CONSULTATION PAPER
ON
IPv6 MIGRATION BYELAW 2082 (2025)

Nepal Telecommunications Authority
Kantipath, Jamal, Kathmandu

JUNE 2025

Preface

The Internet Protocol (IP) is a protocol, or set of rules, for routing and addressing packets of data so that they can travel across networks and arrive at the correct destination. Every device or domain that connects to the Internet is assigned an IP address, and as packets are directed to the IP address attached to them, data arrives where it is needed. Currently there are two version of IP being used: IPv4 and IPv6. The IPv4 uses a 32-bit address scheme allowing to store 2^32 addresses (4.19 billion addresses). The increasing end-users connected to the Internet leads to the exhaustion of IPv4 addresses. That's also why the new Internet addressing system, IPv6, is being deployed to fulfill the need for more Internet addresses. Traditionally, the internet in Nepal has been mostly based on the IPv4. Some major ISPs have been providing Internet service based on the IPv6. Almost all the new devices that uses internet are IPv6 capable, but still the IPv6 has not scaled as expected. Mainly the IPv6 is preferred over the IPv4 because of Security, Scalability and Connectivity reasons.

Also, to build the favorable environment for the 5G and IoT market in Nepal, there is a need of internet network based on IPv6. To promote and encourage the IPv6 Migration among the telecom operators and ISPs of Nepal, NTA intends to formulate a Bylaw related to IPv6 Migration.

NTA has issued this consultation paper to request concerned stakeholders, experts, researchers and any other interested parties to send their comments/ suggestions or inputs either in electronic form or in written form on the various issues raised in consultation paper within 30 days from the date of the publication of this consultation paper. The comments and inputs provided by the stakeholders will enable the Authority in formulating the new IPv6 Migration Byelaws. The consultation paper shall be available on NTA's website (www.nta.gov.np). In case any further clarification or information, please write to info@nta.gov.np or contact Mrs. Roja Kiran Basukala, Deputy Director, NTA (Email: rkbasukala@nta.gov.np).

Mr. Bhupendra Bhandari
Chairman, NTA

IPv6 Migration Byelaw,2082(2025)

Under the authority vested by Section 62 of the Telecommunication Act, 2053 (1997), the Nepal Telecommunications Authority (NTA) has formulated IPv6 Migration Byelaw, 2082(2025) for the adoption, deployment, and management of IPv6 networks within Nepal. It aims to ensure the smooth transition from IPv4 to IPv6 protocols by defining mandatory reporting requirements, setting standards and best practices for network configuration, facilitating compliance monitoring, and providing provisions for dispute resolution. Ultimately, the goal is to promote the effective and secure implementation of IPv6 networks to support the growth and stability of Nepal's telecommunications infrastructure. This byelaw is applicable to licensee of the NTA.

Chapter 1 Preliminary

1. Short Title and Commencement:

(1) This Byelaw is called as the " IPv6 Migration Byelaw, 2082(2025).”
(2) This Byelaw shall come into force immediately from 2082/04/01(BS) (or after NTA’s Board decision for enforcement)

2. Definitions:

Unless the subject or context otherwise requires, in this Byelaw: -

i. Act means the Telecommunication Act, 2053 (1997).
ii. Regulation means the Telecommunication Regulation, 2054 (1998).

iii. Regulatory authority (or authority) means Nepal Telecommunications Authority (NTA) established under the Telecommunication Act, 2053 (1997)

iv. Licensee means the telecommunications service providers who have obtained license from the NTA.

v. IP (or Internet Protocol) address means a unique numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication.

vi. IPv4 address (or Internet Protocol version 4 address or IPv4), functions as a unique identifier assigned to a network interface for communication within an IPv4 network. It enables devices to exchange data over the Internet or other IPv4-based networks. IPv4 addresses are 32 bits in length and are typically expressed in decimal format, with four sets of numbers separated by periods.

vii. IPv6 address ((or Internet Protocol version 4 address or IPv4) means a unique identifier assigned to a network interface for communication on an Internet Protocol version 6 (IPv6) network. It serves as the numerical label that enables devices to communicate with each other over an IPv6-enabled network. IPv6 addresses are 128 bits in length and are typically represented in hexadecimal notation, separated by colons.

viii. Local Internet Registry (LIR) means an organization responsible for managing and distributing IPv6 address blocks within a specific region. LIRs receive allocations of IPv6 addresses from Regional Internet Registries (RIRs) and are tasked with allocating address space to Internet service providers (ISPs),

ix. Regional Internet Registry (RIR) means an organization responsible for the allocation and registration of large blocks of IPv4 and IPv6 addresses to Local Internet Registries (LIRs) within a defined geographic region. RIRs manage and distribute IPv6 address space according to global policies and guidelines established by the Internet Assigned Numbers Authority (IANA). RIR in this byelaw also refers to APNIC in case of Nepal.

x. Allocation means the process of assigning a block of IPv6 addresses from a Regional Internet Registry (RIR) to a Local Internet Registry (LIR) or an end user.

xi. Assignment means granting a portion of an allocated IPv6 address block to a specific end-user or customer. Once an LIR receives an allocation of IPv6 addresses from the RIR, it assigns individual IPv6 address blocks to its customers based on their requirements.

xii. Routing means the process of directing network traffic to its intended destination. In the context of IPv6, routing involves the transmission of IPv6 packets across interconnected networks to reach their designated destinations.

xiii. Migration means migration from IPv4 to IPv6 refers to the transition process of adopting and implementing Internet Protocol version 6 (IPv6) in place of or alongside IPv4 within a network infrastructure. This migration involves upgrading network devices, software, and systems to support IPv6, transferring existing IPv4-based services and resources to IPv6-compatible counterparts, and ensuring seamless interoperability between IPv4 and IPv6 networks during the transition period.

xiv. Dual Stack means a network configuration that supports both IPv4 and IPv6 protocols simultaneously. In a dual-stack network, devices and network infrastructure are capable of communicating using either IPv4 or IPv6 protocols.

xv. Reporting means providing information or data to the NTA on a regular basis to document progress, outcomes, or for compliance.

xvi. Monitoring means the act of observing, tracking, or assessing the progress, performance, or compliance of a system or process during migration or phase of migration or even before/ after migration.

xvii. Audits means systematic and independent examinations to assess the accuracy, effectiveness, and compliance of processes, systems, or operations during migration or phase of migration or even before/after migration.

xviii. Inventory Assessment means Conducting a thorough evaluation of existing network infrastructure to identify current resources and determine compatibility with IPv6.

xix. Security Assessment means performing an in-depth analysis to identify potential security vulnerabilities and risks associated with the transition to IPv6.

xx. Compatibility Testing means evaluating the compatibility of existing network equipment and applications with IPv6 to ensure seamless integration.

xxi. Performance Evaluation means measuring the performance of the network after IPv6 implementation to ensure it meets operational standards and performance metrics.

xxii. Independent Assessors means ensuring that network assessments are conducted by individuals or organizations with the necessary expertise and impartiality.

xxiii. Documented Assessment Methodology means using a well-documented approach that outlines procedures, tools, and techniques for conducting network assessments.

xxiv. Risk Assessment means identifying and prioritizing potential risks and vulnerabilities to develop mitigation strategies.

xxv. Vulnerability Scanning and Penetration Testing (VSPT) means Regularly scanning for and testing vulnerabilities to proactively identify and address security issues.

xxvi. Network Performance and Capacity Evaluation (NPCE) means Assessing the network's ability to handle current and future traffic loads effectively.

xxvii. Security Controls Assessment means evaluating the effectiveness of security measures and recommending improvements.

xxviii. Accurate documentation means keeping detailed records of the assessment process, findings, and remediation actions

xxix. Prompt Remediation means Addressing identified vulnerabilities and weaknesses quickly to maintain network security and performance.

xxx. Audit Trail Maintenance means maintaining a detailed log of assessment activities for review and compliance verification.

xxxi. Continuous Improvement means regularly updating and improving assessment processes based on new developments and lessons learned.

xxxii. Periodic IPv6 Audits means conducting regular audits to track progress and compliance with IPv6 deployment requirements.

xxxiii. Compliance Monitoring means regularly checking for adherence to the byelaws to ensure that standards are being met.

xxxiv. Compliance verification means verifying that all aspects of IPv6 deployment meet the required standards.

xxxv. Penalties means implementing consequences for failure to comply with the bylaws.

xxxvi. Appeals Process means providing a process for disputing enforcement actions.

xxxvii. NAT64 means a mechanism used in IPv6 transition to facilitate communication between IPv6-only clients and IPv4 resources.

xxxviii. DNS64 means a component of IPv6 transition mechanisms that enables DNS servers to resolve domain names to IPv6 addresses (AAAA records) when only IPv4 addresses (A records) are available.

xxxix. GRE means a tunnelling protocol used to encapsulate packets from one network protocol within packets of another protocol. It enables the creation of virtual point-to-point connections over an IP network, allowing the transport of multiprotocol traffic between remote sites.

xl. ISATAP means an IPv6 transition mechanism that allows IPv6 packets to be transmitted over an IPv4 network using tunnelling. It enables automatic tunnelling between IPv6 hosts and routers across an IPv4 infrastructure, facilitating the coexistence of IPv4 and IPv6 networks.

xli. OSPFv3 means a routing protocol used for IPv6 networks to determine the best path for routing packets between routers. It is an extension of OSPF for

IPv4 and supports the routing of IPv6 packets by exchanging routing information and maintaining a routing table of network paths.

xlii. BGP-4 means an exterior gateway protocol used to exchange routing information between autonomous systems on the internet. It enables routers in different networks to communicate and make informed routing decisions based on policies, network conditions, and routing preferences.

xliii. IS-IS means a routing protocol used to establish and maintain routing tables within an autonomous system. It operates by exchanging routing information between routers, enabling the efficient forwarding of packets within large-scale networks. IS-IS supports both IPv4 and IPv6 routing.

xliv. Stakeholder means any individual, group, organization, or entity that has an interest or concern in the implementation, adoption, or outcomes of the byelaws related to IPv6 deployment. This may include, but is not limited to, licensees operating IPv6 networks, enterprises utilizing IPv6 technologies, government agencies overseeing regulatory compliance, industry associations representing networking or telecommunications sectors, technical experts providing expertise on IPv6 transition mechanisms, and end-users or consumers relying on IPv6-enabled services.

xlv. Enterprise means a business or organization engaged in commercial activities, which may include the provision of goods or services, operation of network infrastructure, or utilization of information technology systems. In the context of the byelaw, an enterprise may be a licensee subject to IPv6 deployment requirements, responsible for implementing IPv6 technologies within its network infrastructure, adhering to regulatory standards and best practices outlined in the byelaws, and ensuring the effective transition to IPv6 to support its business operations and service delivery.

Chapter 2 Provision for Allocation and Assignment of IPv6 Addresses

3. Eligibility Criteria

1) Licensee with Valid Operating Licenses within the Jurisdiction:

i. Licensee operating within the jurisdiction of Nepal must possess a valid operating license issued by the regulatory authority NTA.

ii. Licensee must demonstrate compliance with regulatory requirements and industry standards for network operation and management.

iii. Licensee should have a proven track record of providing Internet connectivity services to end-users.

iv. Licensee is required to demonstrate the necessity of IPv6 addresses for their operational requirements.

2) Enterprises with a Demonstrable Operational Need for IPv6 Addresses:

i. Enterprises seeking IPv6 address allocations must demonstrate a legitimate operational need to the NTA for address space/additional address space i.e. beyond what is available through their ISP.

ii. The enterprise should provide documentation to the NTA outlining its network infrastructure, including the number of users, devices, and services requiring IPv6 connectivity through their ISP.

iii. The enterprise must prove to the NTA, enterprise commitment to efficient address space utilization and compliance with IPv6 deployment best practices.

4. IPv6 Address Allocation Application Process:

1) Submission of Formal Application:

i. Licensee/enterprise seeking IPv6 address allocation shall submit a formal application to the NTA after initial level approval of its application (or application process) through ISP Consortium or Steering Committee or equivalent organization. The finalization of application will be done by the NTA.

ii. The application should be submitted in accordance with the prescribed format (RIR prescribe format) and include all required documentation. The details of the application should be as mentioned in the *Application Details.*

2) Application Details:

i. Licensee shall submit the application specifying intended use of the IPv6 addresses, including the specific network infrastructure, services, and applications that will utilize the allocated address space.

ii. Licensee must provide a justification within the application for the requested block size, explaining the anticipated number of users, devices, and services that will require IPv6 connectivity. The justification should be based on realistic projections and growth estimates.

iii. Licensee must follow *Document Requirement* mention in Chapter 2 Section 3.

3) Documentation Requirements:

i. Licensee shall submit detailed network diagram showing current and planned network.

ii. Licensee shall submit addressing plan demonstrating the efficient use of requested IPv6 addresses.

iii. Licensee shall submit proof of organization's legal status and operational capacity.

4) IPv6 Deployment Plan:

i. Along with the application, licensee should submit a documented IPv6 deployment plan outlining their strategy for implementing and managing the allocated address space.

ii. License should specify deployment plan that include timelines, milestones, and resource requirements for IPv6 adoption, as well as measures for ensuring efficient address space utilization and compliance with IPv6 best practices.

5) Review Process:

i. Upon receipt of the application, the NTA will review the submitted documentation (to ensure the licensee/enterprise eligibility criteria for IPv6 address allocation).

ii. The NTA may request additional information or clarification from the licensee/enterprise to support the review process. License should be prepared to provide timely responses to any inquiries or requests for further information.

6) Approval Decision and Notification:

i. If the application meets the eligibility criteria, the NTA will make a decision regarding the approval of the application for IPv6 address allocation and issue a certificate to apply in RIR(APNIC). The

notification of such approval (certificate issuance) will be notified then to the licensee.

ii. In case the eligibility criteria are not meet, the licenses/enterprise would be informed what where missing or where the improvement is necessary in the application.

7) Appeals Process:

i. In the event that an application is denied or requires further review, the applicant may have the option to appeal the decision through established procedures outlined by the RIR(APNIC).

ii. Appeals should be based on valid grounds supported by relevant evidence or documentation and will be considered in a fair and impartial manner by the NTA.

iii. The appeal must be submitted within 30 days of the denial notice.

5. Assignment Policies for IPv6 Address:

1) Assignment to End-Users:

i. Licensee must ensure fair and efficient distribution of IPv6 addresses to their customers.

ii. Licensee should be based on the customer's network requirements and future growth plans.

2) Minimum Assignment:

i. The minimum assignment size that licensee can assign for end-users is /64 for small networks.

ii. For larger networks licensee may assign /48 block, depending on their size and needs.

3) Utilization Requirements:

i. Licensee should ensure that end-users can have efficient utilization of the assigned IPv6 addresses.
ii. Licensee must take care that addresses should be used in accordance with the documented addressing plan.

4) Reclamation of Addresses:

i. Licensee should return RIR any surplus IPv6 addresses, unused or underutilized that are no longer required for their operations. NTA needs to ensure this, if require collaborate with RIR for the purpose.

5) Reporting and Audit:

i. Licensee must submit regular utilization reports as required by the NTA.
ii. NTA needs to audit the use of allocated IPv6 addresses to ensure compliance with the assignment policies for IPV6 Address.

6) Transfer of Addresses:

i. To transfer IPv6 address, licensee must take care and be responsible for it. Licensee must take care that IPv6 addresses should be transferred with prior approval from the RIR.
ii. Transfers must comply with the RIR's policies and any applicable regulations associated to it.

7) Assignment Record Keeping:

i. Detailed records of IPv6 address assignments should be maintained by the licensee.
ii. Records needs to have the assigned address block, date of assignment, and the recipient's details.

Chapter 3 Provision for Address Management

6. Address Space Utilization

1) Utilization Guidelines

i. **Efficient Use:** Licensees must utilize their allocated IPv6 address space efficiently, avoiding wastage or underutilization.

ii. **Subnetting Practices:** Licensees should do subnetting in a manner that supports hierarchical addressing and routing efficiency**.**

iii. **Conservation Measures:** Licensees should adopt measures to conserve address space, including using address aggregation where possible**.**

2) Allocation Principles

i. **Justification for Allocation:** Licensees must provide a detailed justification for the amount of IPv6 address space requested, based on current and projected needs.

ii. **Scalable Allocation:** Licensees should take care that address allocations should be scalable to accommodate future growth while preventing excessive allocation.

iii. **Hierarchical Addressing:** Licensees should use hierarchical addressing to simplify routing and improve the efficiency of address space utilization.

7. Record-Keeping of addresses

1) Maintenance of Records

i. **Accurate Records:** Licensees must maintain accurate and up-to-date records of all allocated and assigned IPv6 addresses.

ii. **Detailed Information:** Licensees should take care that records should include details such as the entity name, contact information, date of allocation, and specific usage of the addresses. Records shall include comprehensive details such as assigned IPv6 prefixes, Subnet masks associated with each prefix, identification of the corresponding end-users or entities to which the addresses have been assigned.

iii. **Retention Period:** Licensees should take care that records must be retained for a minimum period of two years after the address space is no longer in use**.**

3) Storage and Accessibility of records

1) **Storage**: Licensees must store the records of IPv6 address allocations and assignments in a secure and easily accessible manner.
2) **Accessibility:** Licensees should take care that records must be easily accessible to authorized personnel of the NTA (or person authorized by the NTA) for audit and review purposes.

8. Implementation of Best Practices for address management

1) Licensees must implement techniques such as subnet aggregation and address reuse to minimize address wastage and optimize address space utilization.
2) Licensees must employ these best practices; entities can reduce the overall demand for IPv6 addresses and ensure the sustainable use of available resources.

9. Justification for Unused Addresses:

1) NTA reserves the right to request justification for any unused allocated addresses to ensure that address space is being utilized effectively.

2) Licensees must be prepared to provide valid reasons for the non-utilization of allocated addresses, including any plans for future deployment or expansion.

10. Security and Confidentiality:

1) Licensees must protect records of IPv6 address allocations and assignments against unauthorized access, manipulation, or disclosure.
2) Licensees must implement appropriate security measures to safeguard the confidentiality and integrity of these records, including access controls and encryption where necessary.

11. Reporting Obligations of Address Management

1) Reporting Requirements

i. **Frequency of Reports:** Licensees must submit reports on IPv6 address usage to the regulatory authority on a bi-annual basis**.**

ii. **Content of Reports:** Licensees should take care that reports should include the following information:

- Total IPv6 address space allocated and assigned.
- Address space in use and reserved for future use.
- Subnet allocations and assignments.
- Changes in address allocations since the last report.
- Justification for any significant changes in address usage.

2) Reporting Format

i. **Standard Format:** Reports must be submitted by the licensee in a standard format that facilitates easy interas prescribed by the regulatory authority.

ii. **Electronic Submission:** Reports should be submitted by the licensee electronically through a secure online portal provided by the NTA or as specified by the NTA Documentation Standards:

12. Audit Trail:

1) Licensees must maintain an audit trail of any changes made to IPv6 address allocations and assignments, including the reasons for such changes and the individuals responsible for authorizing them. This audit trail serves as a documented history of address management activities and supports accountability and traceability.

13. Continuous Improvement:

1) NTA will continuously review, and update address space utilization guidelines based on industry developments, technological advancements, and feedback from licensees and stakeholder (as RIR).
2) NTA will be regularly assessing utilization practices and identifying opportunities for improvement.
3) NTA will ensure the sustainable management of IPv6 address resources in Nepal.

Chapter 4 Provision for IPv6 Implementation

14. Mandatory IPv6 Implementation:

1) Licensee must implement and support IPv6 on their networks.

15. Timeline for Adoption:

1) Licensee which are still in the process of IPv6 conversion or maintenance must specify a timeline for IPv6 adoption. This timeline should consider factors like network size, infrastructure complexity, and available resources.

16. Regular Reporting of IPv6 of adoption:

1) Licensee must submit regular reports to a designated regulatory authority detailing their progress and compliance with the IPv6 adoption mandate.

17. Detailed Reporting Requirements:

1) License should take care that reports should include information such as the percentage of IPv6-enabled infrastructure, the number of users or customers migrated to IPv6, and any challenges faced during implementation and migration.

18. Technical Standards and Guidelines:

1) License should take care and adhere to legal measures, technical standards, and guidelines for IPv6 implementation, such as those provided by the Internet Engineering Task Force (IETF), Regional Internet Registries (RIRs), and NTA.

19. Resource Allocation:

1) The NTA must allocate necessary resources, including funding for trainings, capacity building and technical assistance, to support licensee in their IPv6 adoption efforts.

20. Incentives

1) The NTA must provide information about financial incentives or grants available to encourage early and efficient migration to IPv6. NTA shall award to licensee who have done good adoption and implementation.

21. Information Dissemination:

1) The NTA must issue guide, disseminate information regarding IPv6 implementation, adoption through various channels such as websites, seminars, workshops, and collaboration with industry associations.

Chapter 5 Provision of Routing and Address Configuration

22. Responsibility for Routing Advertisements:

1) Licensees holding public IPv6 prefixes are responsible for accurately and securely) advertising their address blocks within the global routing system. This includes ensuring that routing advertisements reflect the actual address space assignments and are consistent with routing policies and best practices.

23. Accurate Advertisement of Address Blocks:

1) Licensees who have routing advertisements for IPv6 address blocks must accurately reflect the prefix assignments allocated to the advertising entity. Any discrepancies or inaccuracies in routing advertisements should be promptly corrected to maintain the integrity of the global routing system.

24. Filtering of Routing Advertisements:

1) Licensees advertising IPv6 address blocks should implement filtering mechanisms to prevent unauthorized access and ensure the efficient routing of traffic. This may involve the use of prefix filters, route maps, or access control lists to control the propagation of routing information and protect against route hijacking or spoofing attacks.

25. Authorization and Authentication of Route Announcements:

1) Licensees must ensure routing advertisements should be authenticated and authorized to ensure their legitimacy and authenticity.
2) Licensees must use cryptographic mechanisms such as Resource Public Key Infrastructure (RPKI) or Border Gateway Protocol (BGP) origin validation to validate

route announcements and prevent the propagation of unauthorized or malicious routing information.

26. Compliance with Routing Policy Guidelines:

1) NTA reserve the right to establish specific routing policy guidelines to promote optimal network performance and security. Licences advertising IPv6 address blocks must comply with these guidelines to ensure consistent and reliable routing as per the best practices.

27. Monitoring and Enforcement of Routing Policies:

1) NTA reserves the right to monitor and enforce compliance with routing policies and guidelines. This may involve conducting periodic audits or inspections to verify adherence to routing best practices and address any non-compliance issues identified.

28. Collaboration with Internet Routing Registries (IRRs):

1) Licensees advertising IPv6 address blocks are encouraged to register their routing information with Internet Routing Registries (IRRs) to facilitate route validation and improve the accuracy of routing databases. Collaboration with IRRs helps to ensure the consistency and integrity of routing information across the global routing system.

Chapter 6 Provision relating to Security

29. Mandatory Security Measures:

1) Licensees utilizing IPv6 addresses within their network infrastructure are required to implement appropriate security measures to safeguard their allocated addresses and protect the integrity and confidentiality of their network communications.

30. Deployment of IPv6-Compliant Firewalls:

1) Licensees must deploy IPv6-compliant firewalls to monitor and control incoming and outgoing traffic, enforcing security policies and protecting against unauthorized access, malicious activities, and cyber threats. Firewalls should be configured to inspect IPv6 traffic and apply access control rules based on source and destination addresses, ports, and protocols.

31. Intrusion Detection/Prevention Systems (IDS/IPS):

1) Licensees must deploy Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) to detect and mitigate security incidents, including unauthorized access attempts, malware infections, and network anomalies. IDS/IPS solutions should be capable of analyzing IPv6 traffic and alerting network administrators to potential security breaches or policy violations.

32. Filtering Mechanisms for Traffic Control:

1) Licensees must have filtering mechanisms, such as access control lists (ACLs), packet filters, and content filtering proxies, should be implemented to control the flow of IPv6 traffic and restrict access to authorized resources.

2) Licensees should configure filtering rules to block or allow traffic based on predefined criteria, such as IP addresses, port numbers, and application protocols.

33. Encryption of Sensitive Data:

1) Licensees are encouraged to encrypt sensitive data transmitted over IPv6 networks using robust encryption algorithms and cryptographic protocols, such as IPsec (Internet Protocol Security). Encryption helps protect data confidentiality, integrity, and authenticity, preventing unauthorized interception, tampering, or eavesdropping.

34. Secure Neighbor Discovery (SEND):

1) Licensees must have Secure Neighbor Discovery (SEND) enabled to mitigate risks associated with Neighbor Discovery Protocol (NDP) vulnerabilities, such as address spoofing, Neighbor Cache exhaustion, and router advertisement attacks. SEND enhances the security of IPv6 address resolution and neighbor discovery processes, preventing potential threats and ensuring network integrity.

35. Security Policy Enforcement:

1) Licensees must enforce security policies and guidelines for IPv6 address management and network operations, ensuring compliance with regulatory requirements, industry standards, and best practices. Security policies should be regularly reviewed, updated, and communicated to all stakeholders to maintain a secure and resilient network infrastructure.

36. Regular Security Audits and Assessments**:**

1) Licensees must conduct regular security audits and assessments to evaluate the effectiveness of IPv6 security measures, identify vulnerabilities or weaknesses, and address any security findings promptly. Entities should adopt a proactive approach to security management, continuously monitoring, and improving their security posture to mitigate evolving threats and risks.

Chapter 7 Provision relating to Incident Reporting

37. Mandatory Reporting Requirement:

1) Licensees operating IPv6 networks are mandated to report any security incidents involving their allocated IPv6 addresses promptly to the NTA.

38. Timely Notification of Security Incidents:

1) Licensees must notify NTA upon discovery of a security incident related to IPv6 addresses, without undue delay, providing sufficient details to facilitate timely response and mitigation efforts.

39. Nature and Impact of Incident:

1) Licensee's incident reports should include comprehensive information about the nature and scope of the security incident, describing the type of attack, unauthorized access, or breach detected, as well as the potential impact on network operations, data confidentiality, and service availability.

40. Actions Taken for Mitigation:

1) Licensees must document the actions taken to mitigate the security incident, including containment measures, vulnerability remediation, and restoration efforts aimed at minimizing the impact and preventing further exploitation of vulnerabilities.

41. Collaboration with Stakeholders:

1) Licensees are expected to collaborate with the NTA and other relevant stakeholders during incident response and investigation processes, sharing information, coordinating response efforts, and facilitating forensic analysis as needed.

42. Confidentiality and Data Protection:

1) Licensees must ensure incident reports submitted to the NTA are treated with confidentiality and handled in accordance, ensuring the privacy and security of sensitive information shared during the incident reporting process.

43. Post-Incident Analysis and Review:

1) Licensees should conduct a post-incident analysis and review to identify root causes, lessons learned, and opportunities for improving incident response procedures and enhancing network security posture following the resolution of a security incident.

44. Continuous Monitoring and Reporting:

1) Licensees must maintain ongoing monitoring and reporting mechanisms to detect and respond to security incidents effectively, demonstrating a commitment to proactive risk management and maintaining the integrity and security of IPv6 networks.

Chapter 8 Transition and Coexistence with IPv4

45. Dual Stack Requirements

1) General Requirements

i. **Network Compatibility**:

a. Licensees must take care that all network devices must support both IPv4 and IPv6 protocols simultaneously.

b. Licensees must take care that devices should be capable of processing both types (IPv4 and IPv6) of traffic efficiently without significant performance degradation.

ii. **Firmware Updates**:

a. Licensees should ensure all network software and firmware are updated to support dual stack functionality.

b. Licensees should ensure regular updates are applied to address security vulnerabilities and performance improvements.

iii. **Routing Protocols**:

a. Licensees should implement and configure routing protocols that support both IPv4 and IPv6, such as OSPFv3, BGP-4, and IS-IS.

b. Licensees should ensure routers and switches are configured to handle both IPv4 and IPv6 traffic.

2) Addressing and DNS Requirements

i. **IP Address Allocation**:

a. Licensees should assign both IPv4 and IPv6 addresses to network interfaces during the transition period.

b. Licensees should maintain a clear and organized IP address management strategy to avoid conflicts.

ii. **DNS Configuration**:

a. Licensees should ensure DNS servers are capable of resolving both A (IPv4) and AAAA (IPv6) records.
b. Licensees should implement split-horizon DNS to provide appropriate responses based on the requesting client's network.

3) Security Requirements

i. **Firewall and Security Policies**:

a. Licenses should update firewall rules to accommodate both IPv4 and IPv6 traffic.
b. Licenses should conduct regular security audits to ensure policies are enforced effectively for both protocols.

ii. **Monitoring and Logging**:

a. Licenses should implement logging mechanisms to monitor both IPv4 and IPv6 traffic.
b. Licenses should ensure security information and event management (SIEM) systems can process logs from both types of traffic.

46. IPv6-Only Networks

1) Deployment Guidelines

i. **Planning and Assessment**:

a. Licensees should conduct a thorough network assessment to identify IPv4 dependencies.

b. Licensees should develop a detailed deployment plan outlining the transition to an IPv6-only environment.

ii. **Infrastructure Readiness**:

a. Licensees should ensure all network infrastructure components, including routers, switches, ONU and access points, are IPv6-compliant.
b. Licensees should verify that all critical applications and services support IPv6.

2) Support Mechanisms

1) **Translation and Tunnelling Mechanisms**

a. Licensees should implement NAT64 and DNS64 to facilitate communication between IPv6-only clients and IPv4 resources.
b. Licensees should use tunnelling mechanisms such as 6to4, GRE, ISATAP, or Teredo as interim solutions to connect IPv6 networks across IPv4 infrastructure.

2) **Training and Documentation**:

a. Licensees should provide comprehensive training for network administrators and support staff on IPv6 technologies and troubleshooting.
b. Licensees should maintain detailed documentation of the IPv6 network design, configuration, and operational procedures.

3) Application and Service Adaptation

i. **Application Support**:

a. Licensees should ensure all applications are tested and validated for IPv6 compatibility.

b. Licensees should work with application vendors to address any IPv6 compatibility issues.

ii. **User Transition Support**:

a. Licensees should provide clear communication and support to end-users during the transition to IPv6-only networks.

b. Licensees should implement user feedback mechanisms to identify and resolve issues promptly.

47. Compliance Monitoring for transition and coexistence

i. **Regular Audits**:

a. NTA should conduct periodic audits to ensure compliance with dual stack and IPv6-only network requirements.

b. NTA should report findings and recommend corrective actions for non-compliance.

ii. **Performance Metrics**:

a. NTA should establish key performance indicators (KPIs) to monitor the effectiveness of IPv6 transition and coexistence strategies.

b. NTA should regularly review and adjust strategies based on performance data.

48. Continuous Improvement

i. **Feedback Mechanisms**:

a. Licensees should implement channels for stakeholders to provide feedback on the transition process.

b. Licensees should use feedback to make iterative improvements to policies and procedures.

ii. **Technological Advancements**:

a. Licensees must get informed about advancements in IPv6 technology and best practices.

b. Licensees should incorporate new techniques and tools to optimize the IPv6 transition process.

Chapter 10 Provision for Standard and Best Practices

49. Best Practices for Configuration

1) Adherence to Industry Best Practices:

i. Licensees managing IPv6 addresses within their network infrastructure are strongly encouraged to follow industry best practices for configuring IPv6 addresses on their network devices. These best practices are designed to enhance security, optimize performance, and ensure interoperability in IPv6 environments.

2) Secure Mechanisms for Address Auto-Configuration:

i. Licensees should utilize secure mechanisms for IPv6 address auto-configuration, such as DHCPv6 (Dynamic Host Configuration Protocol for IPv6) or SLAAC (Stateless Address Autoconfiguration). These mechanisms should be configured to prevent unauthorized address assignments and mitigate the risk of address spoofing or theft.

3) Stateless Address Assignment:

i. Licensees should implement Stateless Address Autoconfiguration (SLAAC) judiciously, ensuring that IPv6 addresses are assigned efficiently and securely without the need for central address assignment servers.

ii. Licensees should configure routers to advertise prefixes and manage address configuration parameters effectively.

4) Implementation of Strong Access Control Lists (ACLs):

i. Licensees should deploy Access Control Lists (ACLs) to control traffic flow and enforce security policies in IPv6 networks.

ii. Licensees should configure ACLs to restrict access to IPv6 addresses and services based on source and destination addresses, ports, protocols, and other relevant criteria. Strong ACLs help protect against unauthorized access, denial-of-service (DoS) attacks, and other security threats.

5) Address Space Segmentation:

i. Licensees are encouraged to segment their IPv6 address space into logical zones or subnets based on functional or security requirements to enhance network security and manageability. Address space segmentation helps isolate network traffic, control communication flows, and limit the impact of security incidents or breaches.

6) Encryption and Authentication Mechanisms:

i. Licensees should implement encryption and authentication mechanisms, such as IPsec (Internet Protocol Security), to protect IPv6 communications against eavesdropping, tampering, and unauthorized access. Strong encryption algorithms and key management practices should be employed to safeguard sensitive data transmitted over IPv6 networks.

7) Regular Security Audits and Assessments:

i. Licensees must conduct regular security audits and assessments to evaluate the effectiveness of IPv6 address configuration practices and identify any vulnerabilities or weaknesses that may compromise network security.

ii. Licensees should promptly address any security findings and implement remediation measures to mitigate risks and enhance the resilience of IPv6 networks.

8) Documentation and Configuration Management:

i. Licensees should maintain accurate documentation of IPv6 address configuration settings, including network diagrams, device configurations, and change logs. Configuration management processes should be established to track changes, updates, and revisions to IPv6 address settings and ensure consistency across network devices.

50. Standard Best Practices

1) Licensees should ensure following points to adopt the standard best practices on IPv6.

i. Train your network operators and security managers on IPv6.
ii. Selectively filter ICMP (RFC 4890).
iii. Might be easier to rate-limit ICMPv6 to a few Mbps.
iv. Block Type 0 Routing Header at the edge.
v. Should be automatically blocked by equipment already (but do it anyway).
vi. Adopt all the IPv4 Best Current Practices.
vii. Implement BCP38 filtering.
viii. Implement the Routing Security recommendations as suggested by ICANN, RIR and similar organizations.
ix. If management plane is only IPv4, block IPv6 to the core devices.
x. If management plane is dual stack, replicate IPv4 filters in IPv6.
xi. Which extension headers will be allowed through the access control device?
xii. Deny IPv6 fragments destined to network equipment when possible.
xiii. Use authentication to protect routing protocols.
xiv. Document procedures for last-hop traceback.

2) For Enterprises

i. Implement privacy extensions carefully.
ii. Only allow Global Unicast address sourced traffic out the border router.
iii. Block ULA and other non-assigned IPv6 addresses.
iv. Filter unneeded services at the firewall.
v. Maintain host and application security.
vi. Use cryptographic protections where it is critical.
vii. Implement ingress filtering of packets with IPv6 multicast source addresses
viii. Avoid tunnels.
ix. If you must tunnel, use static tunnelling NOT dynamic tunnelling.

Chapter 11 Provisions for Network Assessment and Audit

51. Comprehensive Inventory Assessment:

1) Licensees shall conduct a comprehensive inventory assessment of existing network infrastructure, including all devices, routers, switches, and servers, to determine their compatibility with IPv6.

52. Addressing Plan Development:

1) Licenses shall develop an addressing plan that outlines the allocation of IPv6 addresses.

53. Security Assessment:

1) Licenses shall conduct a security assessment to identify potential vulnerabilities and risks associated with IPv6 implementation. Licenses need to evaluate the effectiveness of firewalls, intrusion detection systems, and other security mechanisms in the IPv6 context.

54. Compatibility Testing:

1) Licenses shall test the compatibility of existing network equipment and applications with IPv6. Licenses shall conduct interoperability tests to ensure hardware, software, and services can operate seamlessly with IPv6.

55. Performance Evaluation:

1) Licenses shall evaluate the performance of the network after IPv6 implementation, measuring network latency, throughput, and other performance metrics to ensure the transition to IPv6 does not adversely impact network performance.

56. Follow Standard Best Practices:

1) Licenses shall conduct regular network assessments and audits to ensure compliance with regulatory standards, industry best practices, and security requirements.

57. Defined Scope and Objectives:

1) Licenses shall define the scope and objectives of the network assessment, including specific areas to be evaluated such as network infrastructure, systems, applications, and security controls.

58. Qualified and Independent Assessors:

1) Licenses shall ensure that network assessments are conducted by qualified and independent assessors with expertise in network architecture, security, and performance evaluation.

59. Documented Assessment Methodology:

1) Licenses shall establish a documented assessment methodology outlining the procedures, tools, and techniques to be used during the assessment process.

60. Comprehensive Risk Assessment:

1) Licenses shall perform a comprehensive risk assessment as part of the network assessment process. Identify and prioritize potential risks and vulnerabilities to the network infrastructure and systems.

61. Vulnerability Scanning and Penetration Testing:

1) Licenses shall conduct regular vulnerability scanning and penetration testing to identify and mitigate vulnerabilities and security weaknesses in the networks, including both internal and external testing.

62. Network Performance and Capacity Evaluation:

1) Licenses shall evaluate the performance and capacity of the network infrastructure to ensure it meets customer demands, assessing network latency, bandwidth, reliability, and scalability.

63. Security Controls Assessment:

1) Licenses shall assess the effectiveness of security controls, including firewalls, intrusion detection systems, access controls, and encryption mechanisms. Identify any weaknesses or gaps and recommend remedial actions.

64. Accurate Documentation:

1) Licenses shall maintain accurate and up-to-date documentation of the network assessment process, findings, and remediation actions taken. Produce comprehensive reports highlighting assessment results, identified vulnerabilities, and recommendations for improvement.

65. Prompt Remediation:

1) Licenses shall promptly address identified vulnerabilities and weaknesses through appropriate remediation measures. Establish a process for tracking and verifying the implementation of remedial actions and conducting follow-up assessments to ensure their effectiveness.

66. Audit Trail Maintenance:

1) Licenses shall maintain an audit trail of network assessment activities, including documentation of the assessment process, evidence collected, and actions taken. Make this audit trail available for review by NTA or auditors as needed.

67. Continuous Improvement:

1) Licenses should continuously review and enhance network assessment processes based on industry developments, emerging threats, and lessons learned from previous assessments. Actively seek feedback and input from stakeholders to improve assessment and audit practices.

68. Periodic IPv6 Audits:

1) Licenses should perform periodic audits of IPv6 adoption progress and compliance, which may be conducted by internal or external entities. Evaluate the effectiveness of the transition, identify areas for improvement, and ensure adherence to regulatory guidelines and standards.

69. Audit Roles of NTA:

1) NTA should audit whether licensees have followed points mentioned in *Section 51 to 68 of Chapter 11 Provisions for Network Assessment and Audit* or not. NTA might ask for internal audit report of the NTA.

Chapter 12: Provisions for Raising Awareness and Education

70. Public Awareness Campaigns:

1) NTA needs to develop public awareness campaigns to educate end-users, businesses, and organizations about the benefits of IPv6 adoption and the implications of remaining on IPv4.

71. Resources and Training Programs:

1) NTA needs to provide resources, training programs, and workshops to enhance technical knowledge and skills related to IPv6 deployment and migration strategies.

72. Engagement with Educational Institutions:

1) NTA needs to engage/collaborate with educational institutions and research organizations to include IPv6-related topics in relevant curricula and jointly research on IPv6 topics.

73. Internal Awareness Programs:

1) NTA needs to develop and implement awareness programs to educate employees, stakeholders, and customers about the benefits, importance, and necessity of IPv6 adoption. These programs should address common misconceptions and emphasize the long-term sustainability of IPv6.

74. Training for Technical Staff:

1) NTA needs to provide training programs and resources to technical staff, network engineers, and support teams to enhance their understanding and proficiency in IPv6 implementation and troubleshooting. This includes both initial training and continuous professional development opportunities.

75. Engagement with Regulatory Organizations:

1) NTA needs to actively engage with other regulatory organizations(international) involved in IPv6 adoption to stay updated on the latest regulations, guidelines, and compliance requirements.

76. Continuous Evaluation and Improvement:

1) NTA needs to continuously evaluate and improve IPv6 awareness and education initiatives based on feedback from employees, customers, and industry partners. Stay updated on evolving best practices, technological advancements, and address any challenges or barriers faced in IPv6 adoption.

77. Advocacy for IPv6 Adoption:

1) NTA needs to Advocate for IPv6 adoption through public statements, reports, and engagements with policymakers. Emphasize the need for timely IPv6 implementation to ensure continued growth and stability of the Internet.

Chapter 13 Compliance and Enforcement

78. Compliance Monitoring

1) Periodic Audits and Reviews:

i. NTA is responsible for conducting regular audits and reviews to ensure compliance with the established bylaws.

2) Scope of Audits:

i. Audits conducted by the NTA may encompass various aspects of IPv6 deployment, including but not limited to:

   a. Examination of address allocation and assignment records to verify adherence to allocation policies and utilization efficiency.

   b. Assessment of routing practices to ensure accurate advertisement of IPv6 address blocks and compliance with routing protocols.

   c. Evaluation of security measures and protocols implemented to safeguard IPv6 infrastructure and address allocations against potential threats and vulnerabilities.

   d. NTA should audit whether licensees have followed points mentioned in *Section 51 to 68 of Chapter 11 Provisions for Network Assessment and Audit* or not. NTA might ask for internal audit report of the NTA.

3) Documentation Review:

i. Licensee's subject to audit may be required to provide documentation and records related to IPv6 address management, routing configurations, security protocols, and incident response procedures for review by the NTA.

4) On-Site Inspections:

i. In addition to documentation review, the NTA may conduct on-site inspections to assess the physical implementation of IPv6 infrastructure, security controls, and compliance with established standards and guidelines.

5) Adherence to Security Protocols:

i. Licensee's audits will focus on ensuring that they adhere to prescribed security protocols and best practices for IPv6 deployment, including the implementation of firewalls, intrusion detection/prevention systems, encryption mechanisms, and access controls and/or related points mentioned in the Cyber Security Byelaw, 2077 of the NTA (based on the situation).

6) Compliance Verification:

i. NTA will verify compliance as per this byelaw through a comprehensive assessment of audit findings and comparison against established standards and benchmarks.

7) Remediation Requirements:

i. Licensees found to be non-compliant during audits will be required to implement remediation measures to address identified deficiencies and ensure alignment with regulatory requirements and best practices.

8) Follow-Up Audits:

i. NTA reserve the right to conduct follow-up audits to verify the effectiveness of remediation efforts and ensure sustained compliance over time.

9) Transparency and Accountability:

i. NTA will maintain transparency and accountability throughout the audit process, providing entities with clear guidelines, expectations, and opportunities for feedback and clarification.

79. Enforcement

1) Penalties:

i. Licensees for the non-compliance will be taken soft or hard action depending upon the case that may range from warning notices to financial penalties. Licensees found to be in persistent non-compliance with the byelaws may be subject to penalties or sanctions as stipulated by the NTA as per Telecommunication Act, 2053(BS) Section 47, including license suspension, depending on the severity of violations. However, the opportunity for clarification will be given before taking any steps.

2) Appeals Process:

i. Licensees subject to enforcement actions have the right to appeal decisions made by the NTA. An appeals process will be established to ensure procedural fairness and provide recourse for entities aggrieved by enforcement actions or penalties imposed.

Chapter 14 Dispute Resolution

80. Dispute Resolution Process:

1) Formal Dispute Resolution Process:

i. NTA shall resolve any formal dispute concerning the interpretation, application, or enforcement of these bylaws by resolution process established by NTA. This process provides a structured mechanism for addressing disagreements and ensuring equitable resolution.

2) Mediation:

i. Initially, disputing parties may be encouraged to engage in mediation facilitated by neutral third-party mediators appointed or approved by the NTA. Mediation aims to facilitate constructive dialogue, identify common ground, and reach mutually acceptable solutions without resorting to formal legal proceedings.

3) Arbitration:

i. If mediation fails to resolve the dispute satisfactorily, the parties may opt for NTA's arbitration as an alternative dispute resolution mechanism. Arbitration involves the appointment of impartial arbitrators who review the evidence presented by both parties and render a binding decision to resolve the dispute. The decision of NTA arbitration is final and enforceable.

4) Referral to Legal Authorities:

i. In cases where disputes cannot be resolved through mediation or arbitration, or if the nature of the dispute warrants legal intervention, the matter may be referred to relevant legal authorities or judicial bodies for adjudication. Legal authorities may include courts or administrative tribunals with jurisdiction over the subject matter of the dispute.

5) Compliance with Decision:

i. Parties involved in the dispute resolution process shall comply with the decisions, rulings, or awards issued by the appointed mediators, arbitrators, or legal authorities. Compliance ensures the effective resolution of disputes and promotes adherence to established bylaws and regulatory standards.

6) Confidentiality and non-disclosure:

i. All communications, discussions, and proceedings related to the dispute resolution process shall be treated as confidential by the involved parties and NTA. Confidentiality safeguards sensitive information and encourages open and candid dialogue during the resolution process.

7) Cost Allocation:

i. Unless otherwise specified in the dispute resolution process, the costs associated with mediation, arbitration, or legal proceedings, including fees for mediators, arbitrators, and legal representation, shall be borne by the disputing parties in a fair and equitable manner.

8) Timely Resolution:

i. The dispute resolution process shall be conducted expeditiously to ensure timely resolution of disputes and prevent undue delays in addressing grievances. Timely resolution minimizes disruption to operations and facilitates the swift return to normal business activities for the involved parties.

Chapter 15 Review Procedures

81. Review Process:

1) Periodic Review by the Regulatory:

i. NTA shall conduct periodic reviews of these bylaws to assess their effectiveness, relevance, and alignment with evolving technological advancements, industry standards, and best practices. Periodic reviews ensure that the bylaws remain up-to-date and responsive to changing needs and circumstances.

2) Pre-defined Review Intervals:

i. Reviews of the bylaws may be conducted at pre-defined intervals established by the NTA. These intervals ensure regular assessment and adjustment of the bylaws, promoting continuous improvement in IPv6 deployment practices.

3) Response to Significant Changes:

i. NTA reserve the right to initiate ad-hoc reviews in response to significant changes in IPv6 deployment trends, emerging technologies, or regulatory requirements. Such changes may include advancements in IPv6 protocol development, new security threats, or shifts in global internet governance frameworks.

4) Stakeholder Consultation:

i. NTA review process may involve consultation with relevant stakeholders, including licensees, enterprises, government agencies, industry associations, and technical experts. Stakeholder input provides valuable insights into the practical implications of the byelaws and helps identify areas for improvement or refinement.

5) **Assessment of Implementation Challenges:**

i. NTA shall assess the implementation challenges encountered by stakeholders in adhering to the byelaws during the review process. This assessment helps identify barriers to compliance and informs the development of targeted strategies or amendments to enhance the effectiveness of the byelaws.

6) **Evaluation of Enforcement Mechanisms:**

i. NTA's review shall evaluate the effectiveness of enforcement mechanisms established to ensure compliance with the byelaws. This evaluation includes assessing the adequacy of penalties for non-compliance, the efficiency of monitoring and enforcement processes, and the responsiveness of dispute resolution mechanisms.

7) **Incorporation of Lessons Learned:**

i. Lessons learned from past implementation experiences, including successes, failures, and best practices, shall inform the review process. Incorporating lessons learned enables the refinement of byelaws to address practical challenges and optimize outcomes in Nepal's transition to IPv6.

8) **Documentation and Reporting:**

i. NTA's shall report and document the outcomes of the review process, including any proposed amendments or recommendations. Transparent reporting ensures accountability and provides stakeholders with insight into the rationale behind bylaw revisions and updates.

9) **Timely Implementation of Revisions:**

i. Upon completion of the review process, any approved revisions or amendments to the byelaws shall be promptly implemented by the NTA.

Timely implementation ensures that stakeholders benefit from the latest regulatory frameworks and guidance in their IPv6 deployment efforts.

Chapter 16 Amendment

82. Amendment Process

1) **Proposal of Amendments:**

i. Amendments to these byelaws may be proposed by the NTA or licensees. Proposals for amendments should be submitted in writing to the NTA accompanied by a rationale explaining the need for the proposed changes.

2) **Public Consultation Process:**

i. Proposed amendments will undergo a public consultation process to gather feedback from interested parties, including licensees, enterprises, government agencies, and the consumers representative/forum representative. The consultation process may include stakeholder meetings, online forums, surveys, or other mechanisms to solicit input.

3) **Review and Evaluation:**

i. NTA will review and evaluate the feedback received during the public consultation process to assess the potential impact of the proposed amendments and consider any alternative suggestions or concerns raised by stakeholders.

4) **Decision-Making Authority:**

i. NTA will have the final authority to approve and implement amendments to this byelaw. The decision-making process will be guided by considerations of

technical feasibility, regulatory compliance, stakeholder input, and alignment with the objectives of promoting IPv6 adoption in Nepal.

5) Transparency and Accountability:

i. Throughout the amendment process, the NTA will maintain transparency and accountability by documenting the rationale behind proposed amendments, summarizing stakeholder feedback, and providing clear justification for the final decisions made.

6) Notification of Changes:

i. Upon approval of amendments, NTA will notify licensees and the public of the changes made to the byelaws. Notifications may be disseminated through official channels, such as the NTA's website, medias, or direct communication with concerned stakeholders.

7) Effective Date of Amendments:

i. The effective date of amendments to the byelaws will be specified by NTA. Amendments may take effect immediately upon approval or be subject to a transitional period to allow stakeholders time to adjust their practices and procedures accordingly.

8) Publication of Updated Byelaws:

i. Updated versions of the byelaws, incorporating approved amendments, will be published and made readily available to licensees and the public.

Chapter 17 Provision for the Steering Committee

For the implementation, adoption, review, amendment, training and necessary processes and activities following committee will be responsible. For the executional purpose the Executive committee will be responsible, and the governance will be conducted by Governance Committee.

83. Execution Committee

i. Director, Regulation Division of NTA , Chair.
ii. Deputy Director, Numbering and Interconnection Section of NTA, Member.
iii. Deputy Director, Technology Research Section of NTA, Member.
iv. Assistant Director, Technology Research Section of NTA, Member.
v. Assistant Director, Numbering and Interconnection Section of NTA, (Member Secretary)

The roles, responsibility and authority of the execution committee will be as defined by NTA or Governance committee.

84. Governance Committee

i. Chairman of NTA, Chair.
ii. Technical Board Member of NTA, Member.
iii. Senior Director, Regulation and Technology Directorate of NTA, Member.
iv. Director, Monitoring Division of NTA, Member.
v. Director, Regulation Division of NTA, (Member Secretary)
vi. Director, Infrastructure Division of NTA, Member.
vii. Expert of the field (2 Experts), Member

Ministry of Communication and Information Technology representative can be requested as an invitee in the governance committee.

Chapter 18 Miscellaneous

1) This byelaw shall be revised regularly as per requirement. Amendment process will be as per the Chapter 16 Amendment.
2) In case of any disputes of the meaning of the sentence(s), or words. Dispute resolution process will be carried as per the Chapter 14 Dispute Resolution. NTA decision will be final for interpreting the meaning

References

Asia Economic Cooperation. (2017). IPv6 Deployment Strategies in APEC Economies APEC Telecommunications and Information Working Group.

APRICOT (2015). IPv6 Single Stack Now or Later? -The ultimate carrier conundrum.

European Data Protection Supervisor. (2011).INTERNATIONAL CONFERENCE OF DATA PROTECTION AND PRIVACY COMMISSIONERS The Use of Unique Identifiers in the Deployment of Internet Protocol Version 6 .

How to get an initial IPv6 block from your RIR. (n.d.). Retrieved May 10 ,2024, from https://www.apnic.net/wp-content/uploads/2017/01/how-to-get-initial-ipv6-block.pdf

ITU (2015). Role of Policy maker and Regulator in IPv6 Migration ITU Asia-Pacific CoE Training on “IPv6 Infrastructure Security” 22-26 June, 2015 Bangkok, Thailand.

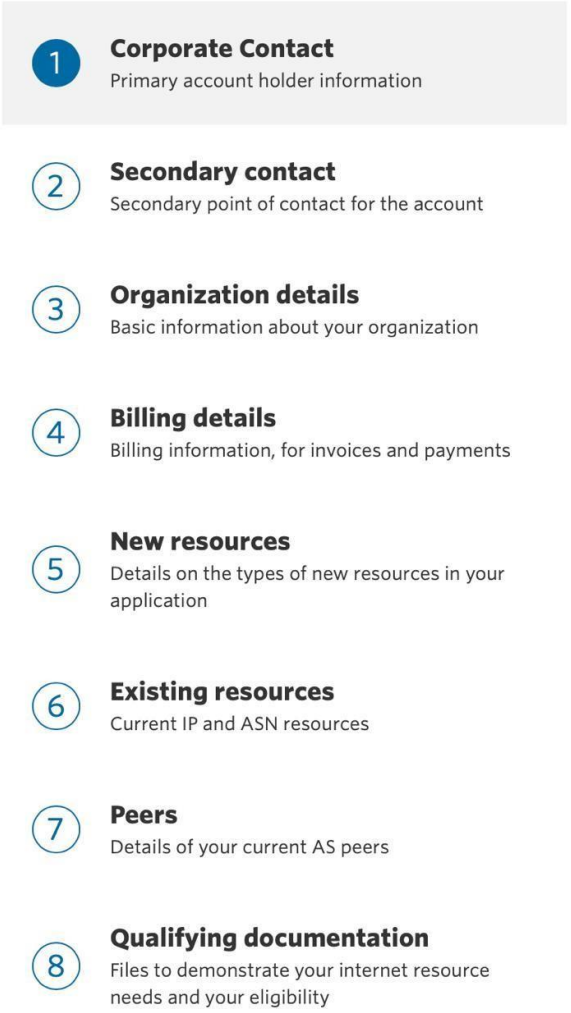
Montgomery, D., Carson, M., Winters, T., Newcombe, M., & Carlin, T. (2020). NIST Special Publication 500-267B Revision 1 USGv6

TELECOM REGULATORY AUTHORITY OF INDIA. (2005).Consultation paper On Issues Relating To Transition From IPv4 To IPv6 in India.

US Federal Energy Regulatory Commission. (2022). Internet Protocol Version 6 (IPv6) Policy.

Annex 1

Fields for Membership form for APNIC (IPv6 or ANS request form)



Source: APNIC

Annex 2

IPv6 block address assignment

IPV6 Global Unicast Address

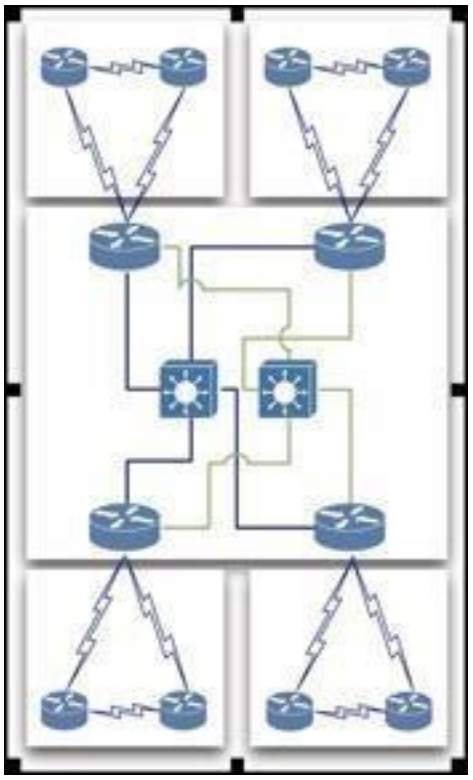
Global Unicast Range: 0010 2000::/3

0011 3000::/3

– All five RIRs are given a /12 from the /3 to further distribute within the RIR region
  - APNIC 2400:0000::/12
  - ARIN 2600:0000::/12
  - AfriNIC 2C00:0000::/12
  - LACNIC 2800:0000::/12
  - Ripe NCC 2A00:0000::/12

Annex 3

Sample Network Topology for Service Provider

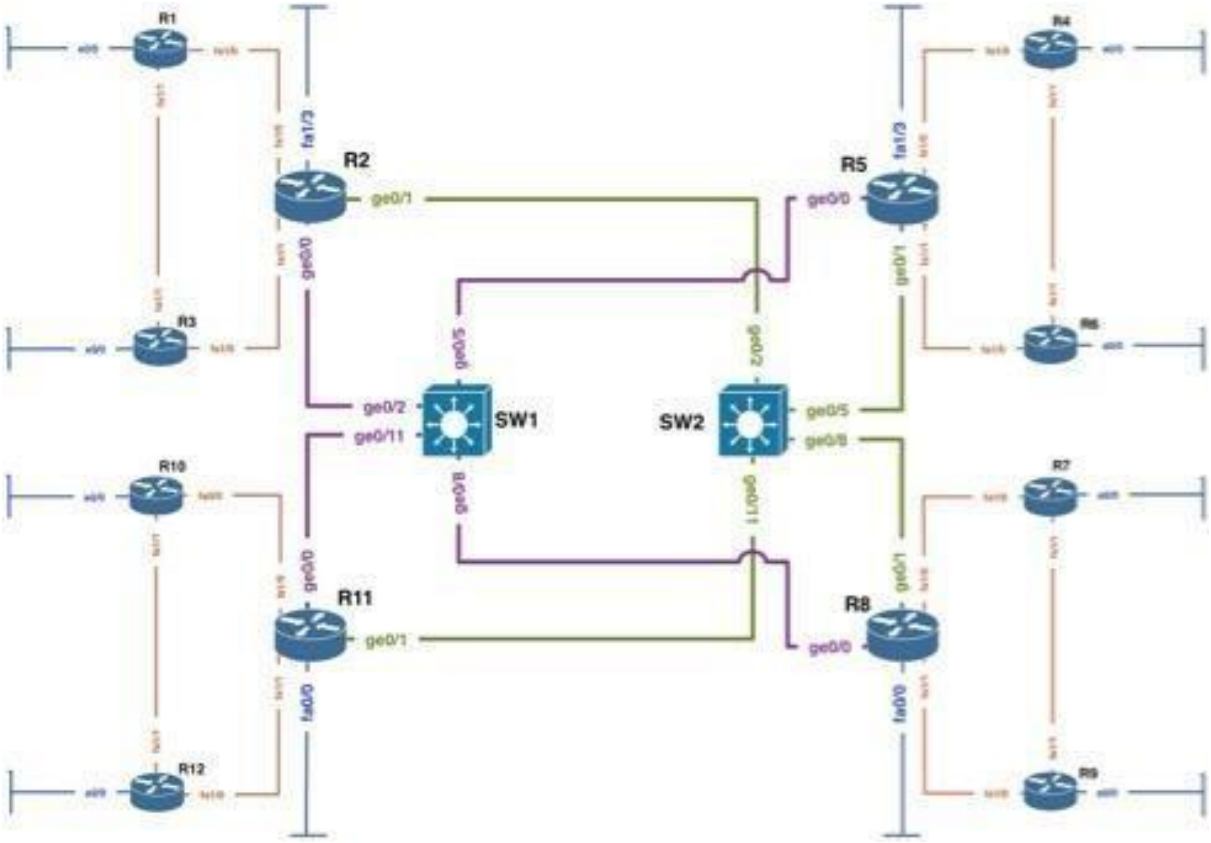


- Scenario:
  - Training ISP has 4 main operating area or region
  - Each region has 2 small POP
  - Each region will have one datacenter to host content
  - Regional network are inter-connected with multiple link

- Regional Network:
  - Each regional network will have 3 routers
  - 1 Core & 2 Edge Routers
  - 2 Point of Presence (POP) for every region
  - POP will use a router to terminate customer network i.e Edge Router
  - Each POP is an aggregation point of ISP customer
- Access Network:
  - Connection between customer network & Edge router
  - Usually 10 to 100 MBPS link
  - Separate routing policy from most of ISP

- Training ISP will connect them on edge router with separate customer IP prefix

- Transport Link:
  - Inter-connection between regional core router
  - Higher data transmission capacity then access link
  - Training ISP has 2 transport link for link redundancy
  - 2 Transport link i.e Purple link A & Green link B are connected to two career grade switch



- Design Consideration:
  - Each regional network should have address summarization capability for customer block and CS link WAN.
  - Prefix planning should have scalability option for next couple of years for both customer block and infrastructure
  - No Summarization require for infrastructure WAN and loopback address

- Design Consideration:
  - All WAN link should be ICMP reachable for link monitoring purpose (At least from designated host)
  - Conservation will get high preference for IPv4 address planning and aggregation will get high preference for IPv6 address planning.
- Design Consideration:
  - OSPF is running in ISP network to carry infrastructure IP prefix
  - Each region is a separate OSPF area
  - Transport core is in OSPF area 0
  - Customer will connect on either static or eBGP (Not OSPF)
  - iBGP will carry external prefix within ISP core IP network
- IPv6 address plan consideration:
  - Big IPv6 address space can cause very very large routing table size
  - Most transit service provider apply IPv6 aggregation prefix filter (i.e. anything other then /48 & <=/32 prefix size
  - Prefix announcement need to send to Internet should be either /32 or /48 bit boundary

- IPv6 address plan consideration (RFC3177):
  - WAN link can be used on /64 bit boundary
  - End site/Customer sub allocation can be made between /48~/64 bit boundary
  - APNIC Utilization/HD ratio will be calculated based on /56 end site assignment/sub-allocation

Annex 4

IPv6 Deployment Best Practices

Addressing Plans – ISP Infrastructure

- What about LANs?
  - /64 per LAN
- What about Point-to-Point links?
  - Protocol design expectation is that /64 is used
  - /127 now recommended/standardised
    - http://www.rfc-editor.org/rfc/rfc6164.txt
    - (reserve /64 for the link, but address it as a /127)
  - Other options:
    - /126s are being used (mirrors IPv4 /30)
    - /112s are being used
      - Leaves final 16 bits free for node IDs
    - Some discussion about /80s, /96s and /120s too

- ISPs should receive /32 from their RIR
- Address block for router loop-back interfaces
  - Generally number all loopbacks out of one /48
  - /128 per loopback
- Address block for infrastructure
  - /48 allows 65k subnets
  - /48 per region (for the largest international networks)
  - /48 for whole backbone (for the majority of networks)
  - Summarise between sites if it makes sense

Addressing Plans – Customer

- Customers get one /48
  - Unless they have more than 65k subnets in which case they get a second /48 (and so on)
- In typical deployments today:
  - Several ISPs give small customers a /56 or single LAN end-sites a /64, e.g.:
  - /64 if end-site will only ever be a LAN

  - /56 for medium end-sites (e.g. small business)
  - /48 for large end-sites
  - (This is another very active discussion area)

Addressing Plans – Advice

- Customer address assignments should not be reserved or assigned on a per PoP basis
  - Same principle as for IPv4
  - ISP iBGP carries customer nets
  - Aggregation within the iBGP not required and usually not desirable
  - Aggregation in eBGP is very necessary
- Backbone infrastructure assignments:
  - Number out of a single /48
    - Operational simplicity and security
  - Aggregate to minimise size of the IGP

- Registries will usually allocate the next block to be contiguous with the first allocation
  - Minimum allocation is /32
  - Very likely that subsequent allocation will make this up to a /31
  - So plan accordingly

IPV6 Addressing Plan

Table 1: Top Level Distribution infrastructure & customer					
Block	**Prefix**	**Description**	**Reverse Domain**	**SOR**	**Registration**
1	2001:0db8::/32	Parent Block	8.b.d.0.1.0.0.2.ip v6.arpa.	N/A	APNIC
2	2001:0db8:0000:0 000::/36	Infrastructure	0.8.b.d.1.0.0.2.ip v6.arpa	No	optional
	2001:0db8:1000:0 000::/36				
	2001:0db8:2000:0 000::/36				
	2001:0db8:3000:0 000::/36				
	2001:0db8:4000:0 000::/36				
	2001:0db8:5000:0 000::/36				
	2001:0db8:6000:0 000::/36				
	2001:0db8:7000:0 000::/36				
3	2001:0db8:8000:0 000::/36	Customer Network Region 1	8.8.b.d.1.0.0.2.ip v6.arpa	Not Yet	Optional
	2001:0db8:9000:0 000::/36				

4	2001:0db8:a000:0000::/36	Customer Network Region 2	a.8.b.d.1.0.0.2.ip v6.arpa	Not Yet	optional
	2001:0db8:b000:0000::/36				
5	2001:0db8:c000:0000::/36	Customer Network Region 3	c.8.b.d.1.0.0.2.ip v6.arpa	Not Yet	optional
	2001:0db8:d000:0000::/36				
6	2001:0db8:e000:0000::/36	Customer Network Region 4	e.8.b.d.1.0.0.2.ip v6.arpa	Not Yet	optional
	2001:0db8:f000:0000::/36				

Table 2: Top Level Summarization option infrastructure & customer

Block	Prefix	Description	Reverse Domain	SOR	Registration
7	2001:0db8:8000:0000::/35	CS Net Summary Region 1	2X/36 arpa domain	N/A	Optional
8	2001:0db8:a000:0000::/35	CS Net Summary Region 2	2X/36 arpa domain	N/A	optional
9	2001:0db8:c000:0000::/35	CS Net Summary Region 3	2X/36 arpa domain	N/A	optional
10	2001:0db8:e000:0000::/35	CS Net Summary Region 4	2X/36 arpa domain	N/A	optional

Table 3: Detail distribution infrastructure					
Block#	**Prefix**	**Description**	**Reverse Domain**	**SOR**	**Registration**
2	2001:0db8:0000:0000::/36	Infrastructure	0.8.b.d.1.0.0.2.ip v6.arpa	No	Optional
11	2001:0db8:0000:0000::/40	Loopback,Transport & WAN [Infra + CS]	0.8.b.d.1.0.0.2.ip v6.arpa	N/A	optional
	2001:0db8:0100:0000::/40			N/A	optional
	2001:0db8:0200:0000::/40			N/A	optional
	2001:0db8:0300:0000::/40				
	2001:0db8:0400:0000::/40				
	2001:0db8:0500:0000::/40				
	2001:0db8:0600:0000::/40				
	2001:0db8:0700:0000::/40				
16	2001:0db8:0800:0000::/40	Region 1 DC	8.8.b.d.1.0.0.2.ip v6.arpa	no	Recommende d
	2001:0db8:0900:0000::/40				

17	2001:0db8:0a00:0000::/40	Region 2 DC	a.8.b.d.1.0.0.2.ip v6.arpa	no	Recommended
	2001:0db8:0b00:0000::/40				
18	2001:0db8:0c00:0000::/40	Region 3 DC	c.8.b.d.1.0.0.2.ip v6.arpa	no	Recommended
	2001:0db8:0d00:0000::/40				
19	2001:0db8:0e00:0000::/40	Region 4 DC	e.8.b.d.1.0.0.2.ip v6.arpa		Recommended
	2001:0db8:0f00:0000::/40				

Table 4: Data Center Prefix Summarization options

Block#	Prefix	Description	Reverse Domain	SOR	Registration
16	2001:0db8:0800:0000::/39	Region 1 DC Summary	8.8.b.d.1.0.0.2.ipv6.arpa	no	Recommended
17	2001:0db8:0a00:0000::/39	Region 2 DC Summary	a.8.b.d.1.0.0.2.ipv6.arpa	no	Recommended
18	2001:0db8:0c00:0000::/39	Region 3 DC Summary	c.8.b.d.1.0.0.2.ipv6.arpa	no	Recommended
19	2001:0db8:0e00:0000::/39	Region 4 DC Summary	e.8.b.d.1.0.0.2.ipv6.arpa		Recommended

Table 5: Further detail loopback, Transport & infrastructure WAN

Block#	**Prefix**	**Description**	**Reverse Domain**	**SOR**	**Registration**
11	2001:0db8:0000:0000::/40	Loopback,Transport & WAN [Infra + CS]	0.8.b.d.1.0.0.2.ipv6.arpa	N/A	optional
20	2001:0db8:0000:0000::/48	Loopback		N/A	optional
	2001:0db8:0001:0000::/48			N/A	optional
21	2001:0db8:0002:0000::/48	Link A Transport			
22	2001:0db8:0003:0000::/48	Link B Transport			
	2001:0db8:0004:0000::/48				
	2001:0db8:0005:0000::/48				
	2001:0db8:0006:0000::/48				
16	2001:0db8:0007:0000::/48				Recommended
	2001:0db8:0008:0000::/48				
17	2001:0db8:0009:0000::/48				Recommended

	2001:0db8:000a:0000::/48				
18	2001:0db8:000b:0000::/48				Recommended
	2001:0db8:000c:0000::/48				
19	2001:0db8:000d:0000::/48				Recommended
23	2001:0db8:000e:0000::/48	WAN Prefix Infra Link			
	2001:0db8:000f:0000::/48				

Table 6: Further detail Customers Link WAN					
Block#	**Prefix**	**Description**	**Reverse Domain**	**SOR**	**Registration**
27	2001:0db8:0010:0000::/48	WAN Prefix CS Link Region1		N/A	optional
	2001:0db8:0011:0000::/48				
	2001:0db8:0012:0000::/48				
	2001:0db8:0013:0000::/48				
28	2001:0db8:0014:0000::/48	WAN Prefix CS Link Region1			

	2001:0db8:0015:0000::/48				
	2001:0db8:0016:0000::/48				
	2001:0db8:0017:0000::/48				
32	2001:0db8:0018:0000::/48	WAN Prefix CS Link Region2			
	2001:0db8:0019:0000::/48				
	2001:0db8:001a:0000::/48				
	2001:0db8:001b:0000::/48				
33	2001:0db8:001c:0000::/48	WAN Prefix CS Link Region2			
	2001:0db8:001d:0000::/48				
	2001:0db8:001e:0000::/48				
	2001:0db8:001f:0000::/48				
37	2001:0db8:0020:0000::/48	WAN Prefix CS Link Region3			
	2001:0db8:0021:0000::/48				

	2001:0db8:0022:0000::/48				
	2001:0db8:0023:0000::/48				
38	2001:0db8:0024:0000::/48	WAN Prefix CS Link Region3			
	2001:0db8:0025:0000::/48				
	2001:0db8:0026:0000::/48				
	2001:0db8:0027:0000::/48				
42	2001:0db8:0028:0000::/48	WAN Prefix CS Link Region4			
	2001:0db8:0029:0000::/48				
	2001:0db8:002a:0000::/48				
	2001:0db8:002b:0000::/48				
43	2001:0db8:002c:0000::/48	WAN Prefix CS Link Region4			
	2001:0db8:002d:0000::/48				
	2001:0db8:002e:0000::/48				

	2001:0db8:002f:0000::/48				

Table 7: CS link WAN Summarization options					
Block#	**Prefix**	**Description**	**Reverse Domain**	**SOR**	**Registration**
24	2001:0db8:0010:0000::/45	WAN CS Link Region1 Summary		N/A	optional
25	2001:0db8:0010:0000::/46	WAN CS Link Region1 POP1 Summary			
26	2001:0db8:0014:0000::/46	WAN CS Link Region1 POP2 Summary			
Block#	**Prefix**	**Description**	**Reverse Domain**	**SOR**	**Registration**
29	2001:0db8:0018:0000::/45	WAN Prefix CS Link Region2 Summary			
30	2001:0db8:0018:0000::/46	WAN CS Link Region2 POP1 Summary			
31	2001:0db8:001c:0000::/46	WAN CS Link Region2 POP2 Summary			
Block#	**Prefix**	**Description**	**Reverse Domain**	**SOR**	**Registration**
34	2001:0db8:0020:0000::/45	WAN Prefix CS Link Region3 Summary			

35	2001:0db8:0020:0000::/46	WAN CS Link Region3 POP1 Summary			
36	2001:0db8:0024:0000::/46	WAN CS Link Region3 POP2 Summary			
Block#	**Prefix**	**Description**	**Reverse Domain**	**SOR**	**Registration**
39	2001:0db8:0028:0000::/45	WAN Prefix CS Link Region4 Summary			
40	2001:0db8:0028:0000::/46	WAN CS Link Region4 POP1 Summary			
41	2001:0db8:002c:0000::/46	WAN CS Link Region4 POP2 Summary			

Table 8: Further detail loopback

Block#	**Prefix**	**Description**	**PTR Record**	**SOR**	**Registration**
20	2001:0db8:0000:0000::/48	Loopback		N/A	optional
43	2001:0db8:0000:0000::1/128	Router1 Lopback	Yes	No	No
	2001:0db8:0000:0000::2/128	Router2 Loopback	Yes	No	No
	2001:0db8:0000:0000::3/128	Router3 Loopback	Yes	No	No

	2001:0db8:0000:0000::4/128	Router4 Loopback	Yes	No	No
	2001:0db8:0000:0000::5/128	Router5 Loopback	Yes	No	No
	2001:0db8:0000:0000::6/128	Router6 Loopback	Yes	No	No
	2001:0db8:0000:0000::7/128	Router7 Loopback	Yes	No	No
	2001:0db8:0000:0000::8/128	Router8 Loopback	Yes	No	No
	2001:0db8:0000:0000::9/128	Router9 Loopback	Yes	No	No
	2001:0db8:0000:0000::10/128	Router10 Lopback	Yes	No	No
	2001:0db8:0000:0000::11/128	Router11 Loopback	Yes	No	No
	2001:0db8:0000:0000::12/128	Router12 Loopback	Yes	No	No

Table 9: Further detail infrastructure WAN					
Block #	**Prefix**	**Description**	**PTR Record**	**SOR**	**Registration**
23	2001:0db8:000E:0000::/48	WAN Prefix infra Link		N/A	optional
Note:	*Allocation will be /64 and assignment will be /126 or /127*				

55	2001:0db8:000E:0000::/64		Yes	No	No
	2001:0db8:000E:0001::/64				
	2001:0db8:000E:0002::/64				
	2001:0db8:000E:0003::/64				
	2001:0db8:000E:0004::/64				
	2001:0db8:000E:0005::/64				
	2001:0db8:000E:0006::/64				
	2001:0db8:000E:0007::/64				
	2001:0db8:000E:0008::/64				
	2001:0db8:000E:0009::/64				
	2001:0db8:000E:000A::/64				
	2001:0db8:000E:000B::/64				
	2001:0db8:000E:000C::/64				
	2001:0db8:000E:000D::/64				
	2001:0db8:000E:000E::/64				
	2001:0db8:000E:000F::/64				
	2001:0db8:000E:0010::/64				
	2001:0db8:000E:0011::/64				
	2001:0db8:000E:0012::/64				
	2001:0db8:000E:0013::/64				

	2001:0db8:000E:0014::/64				
	2001:0db8:000E:0015::/64				

End of Document