Contents

Section 1. Introduction ..................................................................................................................... 1
  1.1 Defining Readiness and its Challenges ........................................................................... 1
  1.2 Prior ATIS Initiatives on IPv6 ........................................................................................ 3

Section 2. Organizational Readiness Plan .................................................................................... 3
  2.1 Steps an Organization Needs to Take to be IPv6 Ready (Business) ......................... 3
  2.2 Steps an Organization Needs to Take to be IPv6 Ready (Technical) ....................... 7
  2.3 Establish a Training Program ..................................................................................... 11

Section 3. Characterization of the Levels of Readiness .......................................................... 11

APPENDIX A: ATIS IPv6 Readiness Plan Study Group Members ........................................... 18
APPENDIX B: Revision History ................................................................................................... 19
Section 1. Introduction

This whitepaper is the product of the Alliance for Telecommunications Industry Solutions (ATIS) IPv6 Readiness Plan Study Group (AIRP-SG), a group of subject matter experts commissioned by the ATIS Technology and Operations (TOPS) Council. The AIRP-SG engaged in the development of this readiness plan in response to the industry’s need to develop a guide for transitioning to IPv6, in light of the previous reports produced by the ATIS IPv6 Task Force (IPv6-TF) and the public announcement in June 2007 by the American Registry for Internet Numbers (ARIN) that the exhaust of IPv4 addresses is imminent.

This whitepaper is intended to be used by a variety of organizations (service providers, enterprise, network providers, etc) to:

- Provide a tool for organizations to make an assessment of current capabilities and to identify steps towards IPv6 readiness, and
- Provide means for organizations to illustrate IPv6 readiness utilizing defined levels of readiness.

1.1 Defining Readiness and its Challenges

Readiness, in terms of IPv6, means being prepared for when business drivers warrant implementing IPv6 within a network. While there are many drivers for IPv6, the ultimate driver will be when the inevitable exhaust of the IPv4 address pool impacts the operation and growth of an existing IP network. At that time, business continuity requirements will dictate the implementation of IPv6.

One of the more significant challenges to date in transitioning to IPv6 is that, aside from the issue of IPv4 address pool exhaust to gain stakeholders attention, there is no short term business driver or business case for aggressive IPv6 transition planning and implementation. This is largely due to the efficiency of the workarounds associated with extending the lifespan of the IPv4 address pool, such as Classless Inter-Domain Routing (CIDR) and Network Address Translator (NAT) technologies. It has been challenging for planners and operators to develop and justify an IPv6 business case. However, the short term exhaust of IPv4 address pool will eventually be upon stakeholders, and without appropriate planning this will likely catch some stakeholders off-guard. The end result potentially will cause negative impacts to their businesses in one form or another.

Announcements from the Regional Internet Registry (RIRs) and Internet Assigned Numbers Authority (IANA) have warned that IPv4 addresses are quickly running out, and will not be as readily available as they have been in the recent past. When the IPv4 address pool eventually exhausts, the impact will be similar to the effects associated with the change of length of the date field to accommodate the year 2000 (Y2K). Y2K was a fixed date, and deadline to have compliant software was generally agreed upon. Y2K compliance became
an absolute requirement for all systems at the same time. The primary motivator in being ready for Y2K was business continuity; thus the business case for Y2K centered on business continuity and risk management.

Unlike the fixed date of Y2K, IPv4 exhaust is going to affect different stakeholder segments and different networks at different times. Tier-1 backbone providers, large enterprise and government networks will be among the first affected, followed by smaller ISPs, enterprise networks, and eventually will reach the consumer. When the impact of IPv4 exhaust comes, IPv6 “compliance” will become a business continuity requirement. If a network is not IPv6 capable, operations may still continue but there will be costs associated with implementing workarounds. Those workarounds will have to be maintained with associated recurring costs, and eventually it may become more efficient to simply transition to IPv6.

From most stakeholders, until IPv4 address pool exhaust becomes a more imminent issue, IPv6 is seen as purely strategic. However, IPv6 is quickly becoming a requirement not only to enable IP networks to ensure global connectivity into the future, but to ensure growth as well. The public IP network and private networks will eventually need to transition to IPv6. The conclusion of ATIS’ previous IPv6 Task Force\(^1\) regarding transitioning to IPv6 is that it’s not a matter of if the industry is going to transition, but when. The recommendation of the ATIS IPv6 Task Force is to start working on IPv6 as soon as possible to ensure a smooth transition for when it makes business sense depending on individual network conditions and requirements.

The transition to IPv6 will also be a necessary activity for enterprises and service providers which currently provide services that rely on the ongoing availability of contiguous IP address resources. Enterprises must meet the expectations of their internal and external customers that expect their mail, web and other services to be available to the entire Internet. This will require services to be reachable via IPv6, as well as IPv4, as organizations will have no choice but to use IPv6 in the future. Service providers have similar service implications as the current service model and Internet structure depends on the hierarchical address assignment model to scale. IPv6 allows service providers to continue to grow their business with new customers and maintain the hierarchical address assignment model.

The first ATIS report on IPv6 identified organizational activities and recommendations for the transition to IPv6. This ATIS Readiness Plan for IPv6 Transition will extend those recommendations into actionable steps that organizations can use as a tool to assist in transition planning. The benefit of such a plan is ensuring that a common measure is available to plan and assess IPv6 readiness for that point in time when it makes sense for each individual organization and network.

\(^1\) See Section 1.2 for additional information on ATIS initiatives regarding IPv6.
1.2 Prior ATIS Initiatives on IPv6

ATIS has issued through the TOPS Council’s IPv6 Task Force (IPv6-TF) two reports investigating and providing recommendations to the industry on IPv6 (May 2006) and challenges associated with IPv6 transition (July 2007). The report and recommendations with respect to various aspects of IPv6, entitled the “ATIS Internet Protocol version 6 (IPv6): Report & Recommendation, May 2006,” reviewed IPv6 deployment, transition challenges and the market drivers behind deployment of IPv6. This initial report notes that industry’s transitioning to IPv6 will stem from three critical drivers: 1) deployment of IMS for peer-to-peer multimedia, 2) continued adoption of IPv6 by large enterprises such as federal and state governments, corporations and universities, and 3) wide-scale deployment of IPv6 for consumer and home networking demands. In order to ensure end-to-end interoperability during the transitional phase, the IPv6-TF highly recommended the general adoption of a dual-stack transition approach complemented with tunneling technologies. Additionally, the report strongly encouraged the industry to prepare for IPv6 transition now, not later.

The second report on transition challenges, the “ATIS IPv6 Task Force Report on Transition Challenges, July 2007” proposes steps forward, to the extent possible, to address the numerous transition challenges identified in its first report such as Address Allocation Policies, Site Multi-homing, Quality of Service (QoS), Security, Interoperability between IPv4 and IPv6, Network Address Translation (NAT), and the impacts on existing network traffic and routing. Notably, the second IPv6-TF report observes that of those issues remaining to be resolved, most significant is the need for organizations to make key internal business decisions with respect to IPv6. While IPv6 is of unquestionable importance to the industry, its wide-scale advancement has been preempted by more pressing technical and operational priorities demanding the industry’s focused attention.

Section 2. Organizational Readiness Plan

The following subsections contain an overview of what steps need to be taken both in terms of physical infrastructure readiness and business readiness for an organization to begin transition to IPv6 interoperability. These steps are not intended to be prescriptive, and may be used by organizations that have already started an internal process for assessing IPv6 readiness. The steps are also intended for use by a host of organization types and may be enhanced for the particular needs of a service provider or enterprise environment.

2.1 Steps an Organization Needs to Take to be IPv6 Ready (Business)
2.1.1 Identify Drivers and Business Requirements to Migrate to IPv6

An organization should identify the reasons to adopt IPv6. What are the drivers? What are the business requirements? It should link IPv6 interoperability to specific goals or objectives of the organization. For example:

- Business continuity when IPv4 addresses are depleted.
- The need for address space to support the explosion of internet enabled devices and proliferation of peer-to-peer always on applications.
- Government mandates and policies to implement IPv6.
- Customer demands.
- Applications support in:
  - Seamless mobility.
  - Ad-hoc networking.
  - Control and sensors applications.
  - Home and personal networks and services and devices.
  - Secure peer-to-peer applications.
  - IP Multimedia System (IMS).
- Global communications.
- Migration of supply chains to IPv6 (e.g., outsourcing).

2.1.2 Identify Associated Benefits, Costs, and Risks

2.1.2.1 Benefits

Identify how IPv6 transition benefits the organization. What line of business and what programs benefit from IPv6 transition? Is IPv6 a key enabler for certain line of business and programs? For example, how does IPv6 transition:

- Increase business opportunities (e.g. new service opportunities, maintain existing services).
- Improve network efficiency and cost savings (e.g. eliminate of mitigation techniques to work around depletion of IPv4 addresses, etc.).
- Improve network performance.
- Simplify operations (e.g. auto-configuration, etc.).
• Provide strategic advantages.

2.1.2.2 Costs

Identify what costs associate with IPv6 transition. For example:

• Planning and Engineering (Including planning, system engineering, design, testing, implementation, and deployment, etc.).

• Infrastructure changes/upgrades. Consider the minimality if done through lifecycle management process.) Changes may include:
  o Hardware and Software.
  o Applications.
  o Operational Support Systems.

• Personnel Training (Including training designers and operations in skills associated with IPv6 and interworking between IPv4 and IPv6).

• Operational costs once deployment started.

2.1.2.3 Risks

Identify what risks are associated with IPv6 transition. These may include business, legal, or technical risks. For each of the risks identified, there should also be mitigating actions that can be used to minimize or prevent those risks and contingency actions that can be taken in the event the mitigating actions are not successful. For example:

• Business risks.
  o Can we achieve the identified benefits and the return on investment?

• Legal risks.
  o Privacy risks may develop due to the existence of unique identifiers in IPv6 addresses which may provide the potential to track network activity. Network operators must, therefore, be aware of any legal requirements to safeguard the privacy of their users.

• Technical risks.
  o Security risks may develop if IPv6 and the associated transition mechanisms are not implemented or managed properly. Different transition mechanisms will have different security concerns. For example, malicious IPv6 packets can be carried within IPv4 tunnels. Some security devices do not provide
IPv6 detection or filtering capability, and malicious users might be able to get IPv6 traffic through these security devices undetected.

- Reliability risks may occur when introducing IPv6 into the infrastructure as this is a non-trivial change. Can the same level of reliability be maintained?
- Interoperability risks may develop due to the initial IPv6 implementation (i.e. unproven IPv6 stack interoperability with other IPv6 stacks, or possible interaction issues with SIP protocols or mobility protocols).

2.1.3 Develop a Business Case and Budget to Implement IPv6

Provide both the quantitative and qualitative reasons for the identified benefits, costs, and risks in a business case for IPv6 transition. The business case should highlight major program activities, specific solutions, and impacts.

2.1.4 Establish a Transition Group to Oversee the IPv6 Transition

Once established, a transition management “office” will plan, coordinate, track and communicate the progress of IPv6 transition throughout the entire organization. The office will also ensure adequate resources (e.g. staffing, training, budget, etc.) are allocated to support the IPv6 program successfully. This type of centralized management office is especially critical in large, distributed organizations. In particular, the transition management office will:

- **Identify the members of the Transition Group** and clearly define their roles and responsibilities.
- **Build awareness** of IPv6 within the organization. Employees should know what is IPv6 and how does it impacted their work areas and why is it important to the organization as a whole.
- **Leverage executive authority** within the organization to sponsor the transition program and set policy. This can provide a significant boost to the overall priority of the transition program when competing for resources.
- **Establish and manage a governance structure** to ensure a smooth implementation and the success of the IPv6 transition program.
- **Identify the areas that will be impacted by IPv6** within the organization. Define milestones to be completed and by when.
- **Establish working team structure** to address the impacted areas. The Transition Group will assign a lead to each working team. The transition management office will also establish the objectives for the working team and ensure that each working team is staffed and trained appropriately and sufficiently.
• **Track transition progress via defined metrics/milestones** that provide executive management the confidence that benefit is being achieved by IPv6 and the transition is progressing as defined.

• **Develop and communicate clear policy and enforcement procedures** to ensure that all impacted areas within an organization include IPv6 in their future plans. IPv6 policies should be released and emphasized on a timely basis. Identify methods or tools for review and enforcement of policies. An example of an IPv6 policy could be that all acquisition and procurement should be of IPv6-capable/ready assets only. An example of an enforcement procedure could be that only business cases for IPv6 compliant projects will be approved.

• **Develop an Overall Comprehensive IPv6 Transition Plan for the whole organization** to ensure that all IPv6 plans are synchronized, consistent, and well prioritized.

• **Communicate the progress of IPv6 transition** throughout the organization.

2.2 Steps an Organization Needs to Take to be IPv6 Ready (Technical)

### 2.2.1 Inventory All IP Aware Assets

Perform an **inventory assessment** in an organization’s current infrastructure. The result of this analysis provides an initial view of those components that may require transition to IPv6. Following is a sample list of components to inventory:

- Address allocation needs for both present and future.
- Networks (e.g. IP, DSL, wireless, VoIP, CPE).
- Network Services (e.g. DNS, DHCP, AAA, NTP, etc.).
- Network Management (e.g. MIBS, SNMP, NetFlow, MRTG, etc.).
- Applications (e.g. VoIP applications, databases, etc.).
- Operational Support Systems and Business Support System.
- IP based/aware services.

### 2.2.2 Develop a Design for IPv6 Transition

Develop an **overall IPv6 design** for various impacted areas. The IPv6 design should be standard based and should provide as much IPv4 feature parity as applicable to support a smooth transition. The design should take into account for any new networks and services as well as traffic growth that an organization foresees. Following is a list of
areas that an organization should consider when developing its IPv6 design. The list highlights some of the major areas to considered; and is not meant to be an exhaustive list.

- **IPv6 Addressing Plan** – Understand all addressing requirements within the organization. The addressing plan should outline the organization’s IP addressing needs for the next few years and the address allocation, management, and acquisition processes. For example:
  - What are the addressing needs for an organization’s own infrastructure, its intranet, its extranet, sites not managed by the organization, and services (e.g. layer 3 VPN) it supports or offers?
  - What is the IP address usage forecast?
  - How should IPv6 addresses be allocated to support infrastructure and end users’ needs?
  - How should IPv6 addresses be allocated to support efficient and scalable routing?
  - Should the organization obtain a Provider Independent (PI) IPv6 prefix or a Provider Aggregatable (PA) IPv6 prefix?
  - Under what conditions does the organization plan to use Stateless Address Auto-configuration (SLAAC) or Stateful Configuration for the hosts that it supports?
  - Will privacy extensions be used?
  - How will an organization manage privacy extensions used by an end user?
  - How will the aspect of multiple prefix addresses on a single interface be managed and utilized?

- **IPv6 Routing** – Understand the impacts to the current routing infrastructure.
  - What changes are required to add to the current routing infrastructure to support IPv6?
  - How do we operate in an IPv4 and IPv6 network environment concurrently?

- **IPv6 Interconnection** – Consider how the organization inter-connects with other organizations.
  - In the case of ISPs, how should IPv6 peering (e.g. filtering rules, peering policies) be implemented?
  - How does an ISP provide IPv6 connectivity to its customers?
  - In the case of end-user organization, how does it connect its internal sites together?
  - How does it connect to the Internet?

- **Transition Mechanism** – Since IPv4 and IPv6 will co-exist for a substantial period of time during the transition to IPv6, an organization needs to consider the various transition mechanisms that will facilitate the transition to IPv6 while co-existing with
the IPv4 network environment. When selecting a transition mechanism, an organization needs to consider its current network environment, IPv6 traffic forecast, IPv6 capable applications/end systems, and IPv6 deployment plan. Transition Mechanisms fall in three major categories: Dual Stack, Tunneling, and Translation.

- **Dual Stack** is mechanism in which an application, a node, a device or any other network entity supports both IPv4 and IPv6 simultaneously. This enables an incremental migration to IPv6.

- **Tunneling** is the mechanism which encapsulates IPv6 packets within IPv4 packets for traversal over an IPv4 network. As the network becomes IPv6 dominant, the remaining few IPv4 applications could use the reverse mechanism by which IPv4 packets are encapsulated in IPv6 packets.

- **Translation** refers to a method of translating one version of IP to another. It allows IPv6-only node talk to IPv4-only node. Translation may not be generically applicable as all applications may not be translated properly between IPv4 and IPv6.

- **Network Services** – Understand how the network services will be impacted as we transition to IPv6. Network Services include: Domain Name Service (DNS), Dynamic Host Configuration Protocol (DHCP), Authentication, Authorization & Accounting (AAA), and Network Time Protocol (NTP), etc. For example, an organization may need to decide whether to support auto-configuration or DHCPv6 or both. It may consider evolve DNS to dual stack to support IPv6 address queries as well as existing IPv4 queries.

- **Security** - In addition to the similar security threats that exist in the IPv4 world, an organization needs to protect new threats that arise during the transition to IPv6. For example, existing firewalls and network intrusion detection systems do not provide IPv6 detection or filtering capability. Malicious users might be able to tunnel IPv6 traffic through these security devices undetected. Some of the automation features that reduce operational overhead may increase vulnerabilities. For example, malicious users can spoof solicitation, advertisement, and binding messages. Applications that use automated tunneling can traverse firewalls and therefore expose the network to outside world. To minimize these problems, mechanisms and policies need to be developed to provide more secured automated capabilities.

- **OSS, BSS & Network Management** - With the introduction of IPv6, OSS, BSS, and Network Management will need to be modified to support the IPv6 infrastructure. Any system that has an IPv4 address field will be a candidate for modification to support IPv6 address fields as well. Any systems that monitor and manage IPv4 traffic will also need to be able to monitor and manage the IPv6 traffic.
• **New features in IPv6** – IPv6 introduces several new features such as Stateless Address Autoconfiguration (SLAAC), “built in” IPSEC, Mobile IPv6, flow label, etc. An organization should evaluate how it can take advantage of these new features in IPv6.

• **Scalability & Reliability** – As organization introduces IPv6 to its existing network, it must ensure that the IPv6 design itself is a scalable and reliable design. In addition, it must ensure that the IPv6 solution does not introduce negative impacts to its current network environment.

• **Service Level Agreements** – Develop service level agreements that reflect IPv6 policy and transition mechanisms for both IPv4 and IPv6 service requirements.

An accompanying **transition strategy** should also be developed to outline a step by step strategy to transition the organization to IPv6 design. It should address questions such as: What are the dependencies of the different impacted areas; which impacted area should be transitioned first?

### 2.2.3 Develop an Impact Analysis

For each platform and service within the organization, what IPv6 capable is will need ot be defined. The organization’s own IPv6 compliance standard for each platform and service will need to be developed. The organization’s own IPv6 compliance standard should be based on commercial and industry standards. For those platforms and services that need to transition to IPv6:

• Assess when they will be IPv6 ready. This step may require contacting vendors for availability of their IPv6 product roadmap.

• Determine resources required (equipment upgrades, human factor, budget cycle, etc.) to transition to IPv6.

• Identify impact to the supporting services and customers. This may require establishing a relationship between the systems integrator and vendor.

### 2.2.4 Develop an IPv6 Implementation Plan

Develop a plan to implement IPv6 transition throughout the organization. The implementation plan should consist of the following components:

• Develop a list of projects to be implemented. Identify dependencies and prioritize the list of projects.

• Establish an IPv6 testing environment to get hands-on experience with the new technology and to verify architecture, designs, engineering rules, etc. The test
environment will include various IP aware assets that need to be tested or interacted with in an IPv6 environment.

- Conduct field trials to gain experiences in the real network as well as operational processes.
- Prioritize IPv6 deployment. Deploy IPv6 during infrastructure refresh cycle and ensure that all products and services acquired or developed are IPv6 capable.

2.3 Establish a Training Program

Both the business and technical aspects of IPv6 transition training may be necessary to initiate and maintain IPv6 readiness. Depending on the role of the personnel play in the organization, the type of training may vary. Following is a sample of training categories:

- **Awareness Training** provides generalized information about IPv6 and IPv6-related issues. This type of training provides an overview of IPv6 technologies, a basic understanding of the IPv6 technology, as well as business drivers, deployment issues, and potential services/products enabled by IPv6.

- **Architectural Training** provides detailed information about IPv6 technology. It is geared toward individuals who will have primary responsibilities in architecting, designing, and deploying IPv6.

- **Operational Training** provides job specific education targeted to an individual’s job responsibilities. It is geared toward individuals who will have primary responsibilities in supporting a deployed IPv6 network.

- **Specialized Training** provides advanced information in certain technology area. It is geared toward Subject Matter Experts (SMEs) who works in a particular technology area. Examples include: Mobility, Security, etc.

**Section 3. Characterization of the Levels of Readiness**

This section contains a characterization of the levels IPv6 readiness. While some aspects of inventory and product assessment may be easily expressed in terms of ratios or percentages, the overall assessment of an organization may be better expressed in a characterization which is more indicative of the need for executive decision making or business planning.

The IPv6 readiness of an organization can be characterized into the following eight levels characterizing the amount of work completed by an organization to migrate to IPv6:
<table>
<thead>
<tr>
<th>Level</th>
<th>Characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Has not considered IPv4 address exhaustion or IPv6 migration.</td>
</tr>
<tr>
<td>1</td>
<td>Is considering IPv6 migration but has not prepared a program to address it.</td>
</tr>
<tr>
<td>2A</td>
<td>Has an IPv6 program in place and is currently identifying critical issues.</td>
</tr>
<tr>
<td>or</td>
<td></td>
</tr>
<tr>
<td>2B</td>
<td>Has clearly identified there are no drivers and business requirements to migrate to IPv6 and has made a positive decision not to migrate to IPv6.</td>
</tr>
<tr>
<td>3A</td>
<td>Has an IPv6 program in place with a complete plan to address critical issues.</td>
</tr>
<tr>
<td>or</td>
<td></td>
</tr>
<tr>
<td>3B</td>
<td>Has decided not to implement IPv6 but has a significantly complete plan for addressing IPv4 address exhaustion and the potential migration of its customers and supply chains to IPv6.</td>
</tr>
<tr>
<td>4</td>
<td>Has an IPv6 program in place and no unresolved critical issues.</td>
</tr>
<tr>
<td>5</td>
<td>Has completed its IPv6 migration program.</td>
</tr>
</tbody>
</table>

In greater detail the levels of readiness are:

- **Level 0**
  A Level 0 readiness characterization is given to an organization that has not considered the implications of IPv4 address exhaustion or IPv6 migration.

- **Level 1**
  A Level 1 readiness characterization is given to an organization that is actively considering IPv6 migration or IPv4 address exhaustion but has not prepared a plan or program to address it.

  Behaviors expected of a Level 1 organization are:

  - Employing internal or external consultants to make IPv6 migration recommendations or develop IPv4 address space exhaustion remedies.
Discussing IPv6 migration or IPv4 address exhaustion at senior management committees involving CxOs (e.g. CIO, CTO).

Gathering internal and external information with regards to IPv6 migration or IPv4 address exhaustion.

Identification of drivers and business requirements to move to IPv6.

Identification of associated costs and risks with regards to IPv6 transition.

A Level 1 organization will be expected to have completed the following steps:

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1.1</td>
<td>Identify Drivers and Business Requirements to Move to IPv6.</td>
</tr>
<tr>
<td>2.1.2</td>
<td>Identify Associated Benefits, Costs, and Risks.</td>
</tr>
</tbody>
</table>

- **Level 2**

  - **Level 2A**

    A Level 2A readiness characterization is given to an organization that has an IPv6 program in place and is currently identifying critical issues to be implemented within the next five years.

    Behaviors expected of a Level 2A organization are:

    - Development of a business case and set aside a budget to migrate to IPv6. The business case identifies the timescales for implementing IPv6.
    - Establishment of up a “Transition Group” to plan, coordinate, track and communicate the progress of the IPv6 program. The members and roles of the IPv6 Transition Group should be identified.
    - Active identification of critical issues by:
      - Inventorying infrastructure that may be impacted by IPv6 transition.
      - Assessing the current infrastructure’s IPv6 capabilities.
    - Active development of the:
      - IPv6 infrastructure design.
– IPv6 deployment plan.
– IPv6 training plan for relevant network & IT staff.
– IPv6 testing plan.

A Level 2A organization will be expected to have completed the previous steps of a Level 1 organization, plus the following steps:

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1.3</td>
<td>Develop a business case and set aside a budget to implement IPv6</td>
</tr>
<tr>
<td>2.1.4</td>
<td>Establish a Transition Group to oversee the IPv6 transition</td>
</tr>
</tbody>
</table>

- **Level 2B**

A Level 2B readiness characterization is given to an organization if it has clearly identified there are no drivers and business requirements to move to IPv6. It must understand the costs and risks of IPv4 address exhaustion and have made a positive decision not to migrate IPv6. The key characteristic of a Level 2B organization is that it has decided not to migrate to IPv6 and that it is active in efforts to understand and demonstrate that IPv4 address exhaustion will not impact its business. It should also be active to understand how the transition of its supply chains and customers to IPv6 would impact its business if it does not transition to IPv6.

- **Level 3**

- **Level 3A**

A Level 3A readiness characterization is given to an organization that has an IPv6 program in place with a complete plan to address critical issues within 5 years.

Behaviors expected of a Level 3A organization are:

- The presence of a funded IPv6 program in place that has:
  - Inventoried the infrastructure impacted by IPv6.
  - Documented the current infrastructure’s IPv6 capabilities.
  - Engaged in lab testing of the IPv6 design and planned infrastructure.
- Has significantly completed a detailed:
  - IPv6 infrastructure design. (The design should address most of the areas listed in the “design area checklist” in this document.)
  - IPv6 deployment plan.
  - IPv6 training plan.
  - IPv6 field trials plan.

A Level 3A organization will be expected to have completed the previous steps of a Level 2A organization, plus the following steps:

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.2.1</td>
<td>Inventory all IP aware assets</td>
</tr>
<tr>
<td>2.2.2</td>
<td>Develop a design for IPv6 transition</td>
</tr>
</tbody>
</table>

- **Level 3B**

A Level 3B readiness characterization is given to an organization if it has decided not to implement IPv6 but has a significantly complete plan for addressing:

- The impact of IPv4 address exhaustion.
- The impact of the transition of its supply chains and customers to IPv6.

A Level 3B organization would be expected to be planning deployment of the necessary systems and gateways to allow its business to continue without disruption when IPv4 address space has exhausted or its supply chains or customers have transitioned to IPv6.

- **Level 4**

A Level 4 readiness characterization is given to an organization that has an IPv6 program in place and no unresolved critical issues.

Behaviors expected of a Level 4 organization are:
• The completion of:
  - IPv6 infrastructure design. The design should address all the areas listed in the “design area checklist” in this document.
  - IPv6 deployment plan.
  - IPv6 training plan.

• Active implementation of:
  - IPv6 infrastructure deployment.
  - IPv6 field trialing.
  - IPv6 training.

A Level 4 organization will be expected to have completed the previous steps of a Level 3A organization, plus the following steps:

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.2.3</td>
<td>Develop an Impact Analysis</td>
</tr>
</tbody>
</table>

- **Level 5**

A Level 5 readiness characterization is given to an organization that has completed its IPv6 migration program, and a full suite of IPv6 capabilities in its networks and applications.

Behaviors expected of a Level 5 organization are:

  - The completion of the deployment of IPv6 infrastructure.
  - The completion of the field trials of IPv6
  - The significant completion of IPv6 training.
  - Has engaged in-service IPv6 customers.

A Level 5 organization will be expected to have completed the previous steps of a Level 4 organization, plus the following steps:
### 2.2.4 Develop an IPv6 Implementation Plan

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Level</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5</td>
</tr>
</tbody>
</table>

### 2.3 Establish a Training Program

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Level</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5</td>
</tr>
</tbody>
</table>

### Summary of Associated Levels and Steps of Readiness

The following table summarizes the above Levels of Readiness and their associated activities in Section 2 of this Readiness Plan.
# APPENDIX A: ATIS IPv6 Readiness Plan Study Group Members

<table>
<thead>
<tr>
<th>Members</th>
<th>Company</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tom Chu</td>
<td>Alcatel-Lucent</td>
</tr>
<tr>
<td>Ken Biholar</td>
<td>Alcatel-Lucent</td>
</tr>
<tr>
<td>Wayne Zeuch</td>
<td>Alcatel-Lucent</td>
</tr>
<tr>
<td>Liza Fung</td>
<td>AT&amp;T</td>
</tr>
<tr>
<td>Peter Willis</td>
<td>BT Group</td>
</tr>
<tr>
<td>Patrick Grossetete</td>
<td>Cisco</td>
</tr>
<tr>
<td>Craig Pierantozzi</td>
<td>Level 3</td>
</tr>
<tr>
<td>Gordon Beacham</td>
<td>Motorola</td>
</tr>
<tr>
<td>John Abraham</td>
<td>Motorola</td>
</tr>
<tr>
<td>Sean Leach</td>
<td>Neustar</td>
</tr>
<tr>
<td>Ed Lewis</td>
<td>Neustar</td>
</tr>
<tr>
<td>Dwight Jameson</td>
<td>Nortel</td>
</tr>
<tr>
<td>Chris Garner</td>
<td>Qwest</td>
</tr>
<tr>
<td>Michael Fargano</td>
<td>Qwest</td>
</tr>
<tr>
<td>Doug Straub</td>
<td>Qwest</td>
</tr>
<tr>
<td>Fred Rogers</td>
<td>Sprint</td>
</tr>
<tr>
<td>Mark Desterdick</td>
<td>Verizon</td>
</tr>
<tr>
<td><strong>ATIS Staff</strong></td>
<td></td>
</tr>
<tr>
<td>Tim Jeffries</td>
<td>ATIS</td>
</tr>
<tr>
<td>Martha Ciske</td>
<td>ATIS</td>
</tr>
<tr>
<td>Lisa Wiseman</td>
<td>ATIS</td>
</tr>
<tr>
<td>Paige Labourdette</td>
<td>ATIS</td>
</tr>
</tbody>
</table>
# APPENDIX B: Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>12/19/2007</td>
<td>Martha Ciske, ATIS</td>
<td>Creation of Draft Plan Outline, Inclusion of Initial Drafts of Areas of Address (L. Fung) and Scales of Measure (P. Willis), and Introduction (M. Desterdick)</td>
</tr>
<tr>
<td>1.1</td>
<td>2/12/2008</td>
<td>Lisa Wiseman, ATIS</td>
<td>Meeting edits including updates to the Scales of Measure</td>
</tr>
<tr>
<td>1.2</td>
<td>3/4/2008</td>
<td>Martha Ciske, ATIS</td>
<td>Meeting edits to Areas of Address</td>
</tr>
<tr>
<td>1.3</td>
<td>3/24/2008</td>
<td>Martha Ciske, ATIS</td>
<td>Revision of Introduction/Background Sections</td>
</tr>
<tr>
<td>1.4</td>
<td>3/24/2008</td>
<td>Martha Ciske, ATIS</td>
<td>Addition of edits for design checklist (L. Fung)</td>
</tr>
<tr>
<td>1.5</td>
<td>3/25/2008</td>
<td>Paige Labourdette, ATIS</td>
<td>Meeting Edits</td>
</tr>
<tr>
<td>1.6</td>
<td>3/27/2008</td>
<td>Martha Ciske, ATIS</td>
<td>General edits (M. Fargano) and readiness measure updates (P. Willis)</td>
</tr>
<tr>
<td>1.7</td>
<td>4/17/08</td>
<td>Martha Ciske, ATIS</td>
<td>Meeting Edits (Design Checklist)</td>
</tr>
<tr>
<td>1.8</td>
<td>5/8/08</td>
<td>Paige Labourdette ATIS</td>
<td>Meeting and Review Edits (L. Fung, P. Willis, E. Lewis, C. Pierantozzi)</td>
</tr>
<tr>
<td>1.9</td>
<td>5/14/2008</td>
<td>Tim Jeffries, ATIS</td>
<td>Edits for Submission to TOPS Council for Review</td>
</tr>
<tr>
<td>2.0</td>
<td>5/27/2008</td>
<td>Martha Ciske, ATIS</td>
<td>Final Editing Revisions for ATIS Board Review</td>
</tr>
</tbody>
</table>