8-10-2016

Development of a Graduate Course on the Transition to Internet Protocol Version 6

Venu Gopal Kakarla
vgk8931@rit.edu

Development of a Graduate Course on the Transition to Internet Protocol Version 6

by

Venu Gopal Kakarla

Thesis submitted in partial fulfilment
of the requirements for the degree of

Master of Science in
Networking & Systems Administration

Department of
Information Sciences & Technologies

B. Thomas Golisano College of
Computing & Information Sciences

Rochester Institute of Technology
Rochester, New York

August 10, 2016

Rochester Institute of Technology

B. Thomas Golisano College of
Computing & Information Sciences

Department of
Information Sciences & Technologies

Master of Science in
Networking & Systems Administration

Thesis Approval Form

Student Name: Venu Gopal Kakarla

Thesis Title: Development of a Graduate Course
on the Transition to Internet Protocol Version 6

Dr. Charles Border

(Committee Chair) *(Signature)* *(Date)*

Dr. Tae Oh

(Committee Member) *(Signature)* *(Date)*

Dr. Luther Troell

(Committee Member) *(Signature)* *(Date)*

Abstract

Internet and mobile connectivity has grown tremendously in the last few decades, creating an ever increasing demand for Internet Protocol (IP) addresses. The pool of Internet Protocol version 4 (IPv4) addresses, once assumed to be more than sufficient for every person on this planet, has reached its final stages of depletion. With The Internet Assigned Numbers Authority's (IANA) global pools depleted, and four of the five Regional Internet Registries (RIR) pools down to the their last /8 block, the remaining addresses will not last very long.

In order to ensure continuous growth of the internet in the foreseeable future, we would need a newer internet protocol, with a much larger address space. Specifically, with that goal in mind the Internet Protocol version 6 (IPv6) was designed about two decades ago. Over the years it has matured, and has proven that it could eventually replace the existing IPv4.

This thesis presents the development a graduate level course on the transition to IPv6. The course makes an attempt at understanding how the new IPv6 protocol is different than the currently used IPv4 protocol. And also tries to emphasize on the options existing to facilitate a smooth transition of production networks from IPv4 to IPv6.

Acknowledgements

Thanks to,

- My parents and family, who have always supported me through the years. Without their support and patience this thesis would not have been possible.
- My thesis committee chair Dr. Charles Border and committee members Dr. Tae Oh and Dr. Luther Troell, for all their guidance throughout the process of writing this thesis. Without them this thesis would not have been possible.
- My mentors, advisors, librarians, professors, colleagues, and friends, whose daily encouragement and inspiration have helped me progress forward.
- Ms. Tracy Morrow for attending my thesis defense and also for proofreading this document for language and grammar.

— Venu Gopal Kakarla

Copyrights

Table of Contents

Table of Figures

1 Introduction

The depletion of IPv4 addresses is forcing network administrators everywhere to implement a new IPv6 addressing scheme to the already complex networks. The newer IPv6 networks are feature rich and promise to fix a lot of age old issues prevalent among IPv4 networks.

In spite of all these new mechanisms to better manage networks we have not seen any major motivations for people to go ahead with an IPv6 implementation. There have been some successful implementations out there, some of which are pretty large scale. But they have still not been sufficient to convince IT admins to transition to IPv6. [1]

Given the current state of the internet, IPv6 transition is not a choice but a requirement. IPv6 is not going to replace anything in the short term. Most likely it is going to co-exist with the existing IPv4. But it is safe to say that eventually in the long term, we can hope that it will eventually replace IPv4. [1]

This thesis presents the development of a course, that describes the concepts and implementation choices that an enterprise needs to ensure while transitioning all or a portion of their network from IPv4 to IPv6. The course can be broken into two parts. One, specifically understanding the IPv6 protocol and routing, and how it differs from its predecessor IPv4. Two, to focus on the various technologies available to aid in the transition from IPv4 to IPv6. Broadly the transition technologies can be categorized into dual stack, tunneling and translation. These three different approaches aim to make this integration of IPv6 into IPv4 networks possible, thus enabling both the technologies to coexist for a certain period of time. And eventually transition into a pure IPv6 landscape.

1.1 Thesis Statement

The goal of this thesis is to design of a graduate level course on the transition from IPv4 to IPv6 that would build on the knowledge students obtained in the other courses offered by the department of Information Sciences and Technologies in the Master's degree in Networking and System Administration at the Rochester Institute of Technology. After completion of the course students would have an understanding of the issues associated with this transition and be able to design and present a plan for a transition from IPv4 to IPv6.

1.2 Motivations of research

There is no plan B, to tackle the depletion of IPv4 addresses. Despite the long list of the issues with IPv6 and its deployment, there are no alternatives. There is no way we can come up with, implement, and deploy an alternative before the lack of IPv4 addresses becomes a serious problem. The only way forward is IPv6. IPv6 has been in the making for almost two decades. It has matured considerably. Thus it is important that it is not ignored any further.

Benefits of IPv6 is not just an expanded address space, it brings out a lot of new features. Such as a new header format, much better support for extensions, flow labeling, and some authentication and privacy capabilities. These benefits make IPv6 a better match for the way that the internet is used today.

1.3 Purpose Statement

The purpose of this research is to develop a course that allows students to gain a better understanding of the functionality and operations of IPv6 networks specifically in how they differ from IPv4 networks. As part of this course students will learn to identify the risks and understand the transition strategies available, hoping that this would help them navigate through the IPv6 transition while avoiding the pitfalls of a poorly planned strategy.

1.4 Implications of research

This course will be beneficial to anyone interested in incorporating IPv6 into their networks in the near future. The main focus will be on transition strategies employing the techniques of tunneling and translation to help in a smoother and more rapid transition to IPv6. Thus this course will help students to formulate a plan for a rapid IPv6 deployment into current networks. The course will involve applying learnt concepts from previously taken courses in enterprise computing as well as emerging computing and network technologies. Students will focus on the available IPv6 transition strategies in both large and small corporate networks, then device a plan for such a transition and study the process involved and understand some of the issues encountered along the way.

1.5 Approach and Methodology

This thesis and the course proposed, aims to explain some of the answers as to why IPv6 transition is necessary, how it is expected to work, and what benefits are gained from implementing it as compared to IPv4. These answers can be provided along with the development of the graduate course. The development of such a course will involve lectures, hands on labs, written assignments focusing on active learning, quizzes and written exams. Thus the completion of this thesis will involve designing and developing these components of the course. The exact components are further listed in the deliverables section.

1.6 Intended Audience

The primary audience of this course will be students in the Master's degree in Networking and Systems Administration who would be interested in pursuing careers as network managers, network administrators and IT personnel who are responsible for managing an enterprise network. The United States Government Office of Management and Budget (OMB) has also mandated that the various departments make the transition to IPv6 initially by June 2008, then September 2012, and finally September 2014. 2008, 2012 and 2014 have long gone, but a lot of the departments have only inched closer to that goal. This course can also help train students who could potentially support federal agencies in meeting this goal. [2][3][4]

1.7 Deliverables

1. Thesis Report
2. Course Outline
    a. Learning outcomes and Course objectives
    b. Textbook selection
    c. Course syllabus and Course schedule
3. Three Lectures
4. An Exam or Exam Format
5. Two or three Labs
6. One Written Assignment

1.8 Work Plan

Week 01: Acceptance of formal proposal by thesis committee and department.

Week 02: Make decisions, get organized.

Week 03: Develop overall plan, draft a list of course topics

Week 04: Decide on the course outline, textbook, lectures, labs, etc.

Week 05: Write lectures, develop labs.

Week 06: Decide on exam format, Prepare exam.

Week 07: Write thesis report.

Week 08: Submission to thesis committee for approval.

Week 09: Submission to department for approval.

Week 10: Project defense, publication, submission to library.

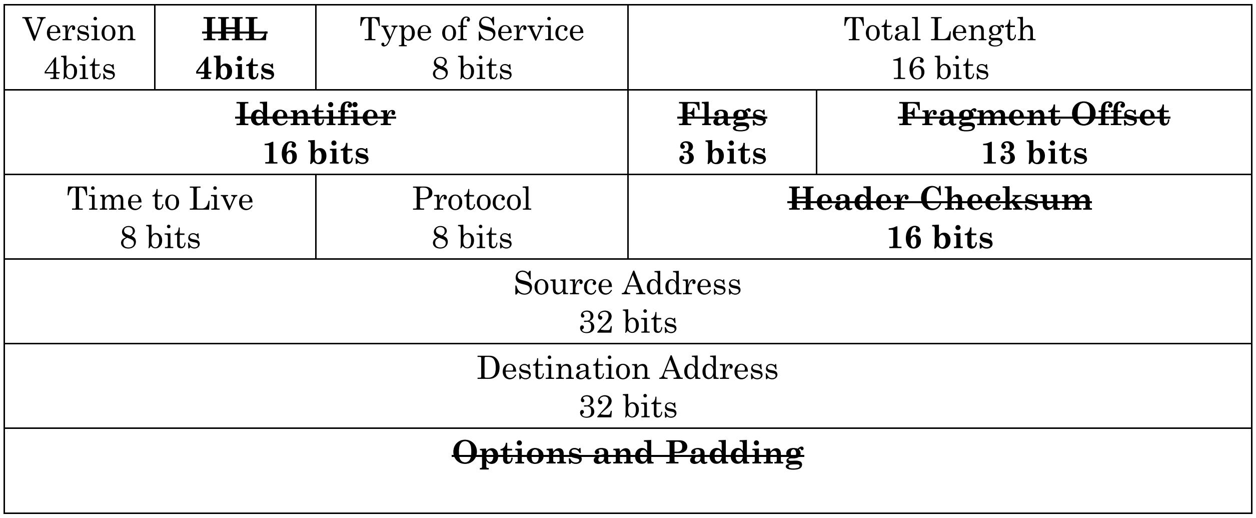
2 Internet Protocol Version 6

2.1 IPv6 Packet Header

In the five layered TCP/IP network stack, IPv6 is a plug in replacement for IPv4. It is supposed to function without much change to the TCP and UDP services. Even though it's a replacement for IPv4, a lot of the fields in the IPv6 header have changed. Some fields have been removed and others modified and even newer fields have been added. Overall, the IPv6 header is much larger than the IPv4 header even though it has a lesser number of fields and is much simpler. This is because of the larger address sizes for the source and destination. IPv6 addresses are 128 bit instead of 32 bit. If we can ignore the quadrupling of the address size, the IPv6 header is much smaller, leaner and simpler. [5][6]

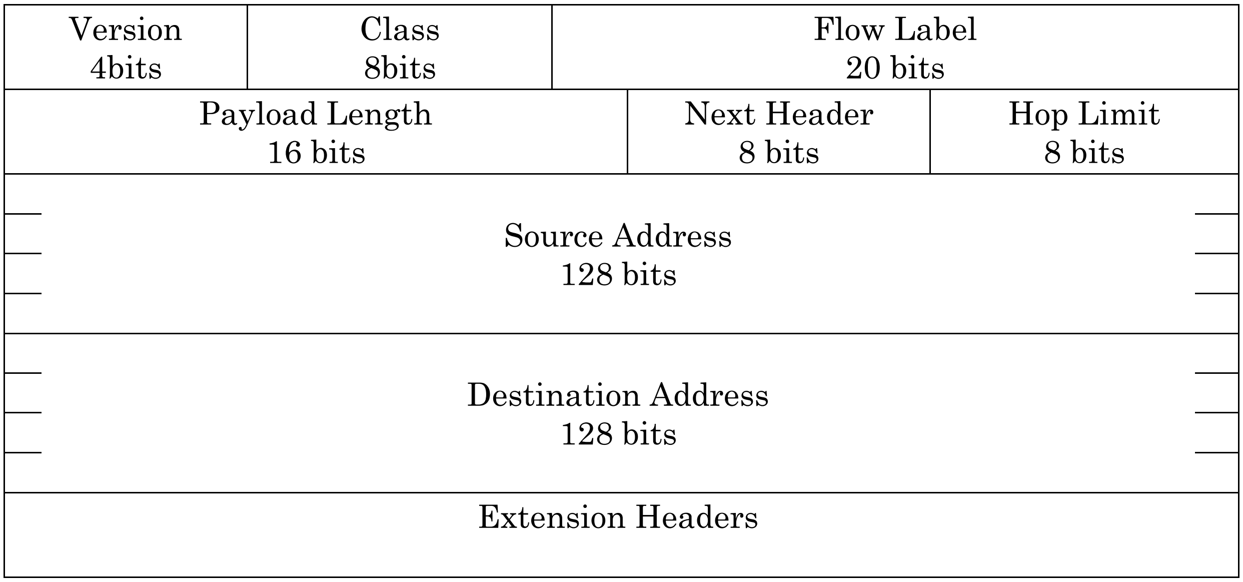
<table>
<tr><td>Version
4bits</td><td>IHL
4bits</td><td>Type of Service
8 bits</td><td colspan="2">Total Length
16 bits</td></tr>
<tr><td colspan="3">Identifier
16 bits</td><td>Flags
3 bits</td><td>Fragment Offset
13 bits</td></tr>
<tr><td colspan="2">Time to Live
8 bits</td><td>Protocol
8 bits</td><td colspan="2">Header Checksum
16 bits</td></tr>
<tr><td colspan="5">Source Address
32 bits</td></tr>
<tr><td colspan="5">Destination Address
32 bits</td></tr>
<tr><td colspan="5">Options and Padding</td></tr>
</table>

Figure 1: IPv4 Packet Header Format



<table>
<tr><td>Version
4bits</td><td>~~<b>IHL</b>~~
<b>4bits</b></td><td>Type of Service
8 bits</td><td colspan="2">Total Length
16 bits</td></tr>
<tr><td colspan="3">~~<b>Identifier</b>~~
<b>16 bits</b></td><td>~~<b>Flags</b>~~
<b>3 bits</b></td><td>~~<b>Fragment Offset</b>~~
<b>13 bits</b></td></tr>
<tr><td colspan="2">Time to Live
8 bits</td><td>Protocol
8 bits</td><td colspan="2">~~<b>Header Checksum</b>~~
<b>16 bits</b></td></tr>
<tr><td colspan="5">Source Address
32 bits</td></tr>
<tr><td colspan="5">Destination Address
32 bits</td></tr>
<tr><td colspan="5">~~<b>Options and Padding</b>~~</td></tr>
</table>

Figure 2: Removed fields from IPv4 Header



<table>
<tr><td>Version
4bits</td><td>Class
8bits</td><td colspan="3">Flow Label
20 bits</td></tr>
<tr><td colspan="3">Payload Length
16 bits</td><td>Next Header
8 bits</td><td>Hop Limit
8 bits</td></tr>
<tr><td colspan="5">Source Address
128 bits</td></tr>
<tr><td colspan="5">Destination Address
128 bits</td></tr>
<tr><td colspan="5">Extension Headers</td></tr>
</table>

Figure 3: IPv6 Packet Header Format

2.1.1 New Fields and Fields changed

- Version has been incremented from four to six, with the size of four bits remaining the same.
- Type of Service has been changed to Traffic Class and Flow Label. Flow label is the only completely new filed introduced in IPv6.
- Time to Live has been renamed to Hop Limit, as we are actually talking of hops and not time.
- Protocol has been renamed to Next Header as IPv6 introduces extension headers.
- Source and Destination Addresses each have their size quadrupled.

2.1.2 Fields removed

- The internet header length filled has been eliminated due to the fact that the IPv6 header is fixed in size.
- Identification, Flags and Fragment Offset have been removed due to the introduction of a dedicated fragmentation extension header.
- Header Checksum has been eliminated to reduce the computation load on routers. In IPv4 due to the TTL value changing at each hop, the checksum changes, causing each router along the way to recomputed the checksum. Elimination of this checksum is not a major problem as the higher layers and lower layers take care of the checksum.

- Options and Padding have been removed as they are no longer required, due to a fixed size header and the availability of extension headers.
- Another change IPv6 brings is the quadrupling of the address size. This means IPv6 addresses are written down using colon separated hexadecimal bits of sixteen. The biggest contiguous substring of zeros can be substituted with two consecutive colons. This can be done only once in an IPv6 address.

2.2 Disruptive Innovations in IPv6

2.2.1 Extension headers

IPv4 packets had up to forty octets as something called options and padding. This was a kind of limitation in the size, hence IPv4 packets with options were hardly seen. Layer security vulnerabilities were discovered in the IPv4 source routing options. Hence source routing was deprecated. [7]

IPv6 kind of extends this with extension headers. Extension headers are optional add-ons to the IPv6 header to implement additional functionality such as source routing, fragmentation, encryption etc. Compared to the IPv4 options the IPv6 extension headers have been improved over the size problem. As they can have up to 255 octets, and then multiple extension headers can be chained in the same packet. [8][9]

2.2.2 Fragmentation

IPv6 also makes a major change in the way it handles packet fragmentation. Unlike fragmentation in IPv4, IPv6 only allows fragmentation at the source node. This means the source will need to know the lowest MTU between itself and the destination. So there is a new protocol for MTU path discovery, which is used to determine the maximum MTU possible without needing to fragment a packet. IPv6 also defines a minimum MTU of 1280 octets. [10]

2.2.3 Autoconfiguration

One of the biggest advantages of IPv6 over IPv4 is autoconfiguration. That means nodes on an IPv6 network can optionally, automatically self-assign themselves IPv6 addresses, which are unique, that is not duplicates of other addresses. This enables something called the stateless addressing of networking, which means that a DHCP server is not required to assign IPv6 addresses. Hence administrator intervention is not needed. This is done by using two new protocols called Neighbor Discovery and Duplicate Address Detection. This new ability of IPv6 networks to autoconfigure, is said to be the main reason for enabling a much faster adoption of IPv6. [11]

2.2.4 Neighbour Discovery and Duplicate Address Detection

One of the most interesting and innovative features of IPv6 is the Neighbor Discovery Protocol. It operates at layer three and is responsible for address autoconfiguration of nodes, discovery of other nodes on the link, determining the link layer addresses of other nodes, duplicate address detection, finding available routers and domain name system (DNS) servers, address prefix discovery, and maintaining reachability information about the paths to other active neighbor nodes. This mechanism is also used for duplicate address detection to avoid address collisions. [12][13]

3 Course Design

In the following section, the various components of this course are presented highlighting how the components are broken down. It tries to elaborate on the different approaches to teaching taken to meet the course objectives. The particular aspects of the course which make it very useful for students are emphasized. Material has been broken into a total of fourteen lectures each spanning a week. This has been done so that the lectures can be aligned with the semester system of instruction at the Rochester Institute of Technology. The typical semester spans sixteen weeks out of which fifteen weeks have regular classroom interaction and the last week, the sixteenth is usually is reserved for the final exams.

3.1 Course Schedule

Week	Topics	Assigned Reading	Activities/Labs
Week 1	Introduction	TB: 1,2 R1: 1,12 R2: 1	Assignment 1 Discussion
Week 2	Technical Fundamentals 1	TB: 3,4 R1: 2,3	Assignment 1 Due
Week 3	Technical Fundamentals 2	TB: 5,6 R1: 7	Lab1
Week 4	Technical Fundamentals 3	TB: 7,8 R1: 4	Lab2
Week 5	Routing 1	TB: 9 R1: 8	Lab3
Week 6	Routing 2	TB: 10	Lab4
Week 7	Routing 3	TB: 15	Lab5
Week 8	Revision, Study, Mid Term		Mid Term Quiz
Week 9	Transition 1	TB: 16 R1: 10	Lab6
Week 10	Transition 2	TB: 17 R2: 3	Lab6
Week 11	Mobility	TB: 11,12 R1: 11	Catchup Lab

Week 12	Security	TB: 13 R1: 5	Assignment 2 Discussion
Week 13	QoS, Network Management	TB: 14,19,20 R1: 6,9	
Week 14	Porting, Case Studies	TB: 21,23 R2: 2	Assignment 2 Due
Week 15	Conclusion, Revision, Study	TB: 24	
Week 16	Finals Week No Class		Final Exam

The TB in the above table refers to the course textbook, specifically "Migrating to IPv6" written by Mark Blanchet. R1 and R2 used above refer to the two reference books namely "IPv6 Essentials" and "Planning for IPv6". Both the reference books are written by author Silvia Hagen.

3.2 Textbook Selection

The textbook selected for this course is "Migrating to IPv6: A Practical Guide to Implementing IPv6 in Mobile and Fixed Networks (2nd ed.)". The book is authored by Marc Blanchet, and published by John Wiley & Sons Ltd in 2016. The course was originally created using the first edition of the book published in 2006, and later updated to use the second edition after it is released in 2016. Out of the many books reviewed to serve as a textbook for this course. This particular book was selected because it not only covered the IPv6 protocol, like other books did. But this was also the only book which covered transition technologies in great detail. So this book also allows the use a single course textbook. Otherwise separate books would have to have been chosen for covering the IPv6 protocol and transition mechanisms separately. The course schedule also lists IPv6 "Essentials (3rd ed.)" and "IPv6 Planning" by

Silvia Hagen for reading. These books are not actually used in the class. But are just provided to support the students with additional reading for each lecture. The chapters in those books are also mapped to the lectures for student's convenience.

3.3 Supplemental Books Selection

The course also refers to a few other supplemental books. It has been ensured that all of these books are available electronically in the RIT's Wallace memorial library, so that the students would not need to purchase them. Among these books, the book "IPv6 Mandates" by Karl Sill is chosen because it takes a project management approach to designing an IPv6 transition plan. It also presents checklists and guidelines to follow, which can support the students in their two written assignments. The Cisco Press book, "Deploying IPv6" by Ciprian Popoviciu, et.al. is chosen because of the examples it provides for implementing the required transition technologies. It also includes Cisco IOS command examples needed by the students to successfully complete the labs component of this course. Since the labs in this course do not include the commands required, this book will prove to be of substantial help to the students.

3.4 Lecture Materials

3.4.1 Lecture 1: Introduction

Lecture 1 covers chapters 1 and 2 of the textbook. The lecture starts with understanding some of the reasons for internet growth in last few decades, and tries to rationalise the reasons for the urgency of transition to IPv6. It talks about some of the statistics showing the rapid rate of IPv4 address space depletion. Then it covers some of the ingenious ways devised to conserve this limited IPv4 address space. It talks about network address translation, variable length subnet masks, classless internet domain routing, and growth of the global routing table. Then it covers some of the real issues prevalent in today's IPv4 networks, issues facing voice over IP and peer to peer networks. Then it talks about the state of IP security in IPv4. Talks about renumbering issues and address collisions over VPN networks. It briefly covers the early history of the internet. And then provides a lot of emphasis on the new features of IPv6. Finally, this lecture also tries to get your hands dirty, by showing the students how to enable IPv6 on different operating systems, such as Windows, Mac OS X, Linux, BSD and Solaris. Examples of commands needed to turn on IPv6 on a Cisco and Juniper router are also included.

3.4.2 Lecture 2, 3, 4: Technical Fundamentals

Lecture 2, 3, 4 cover chapters 3 through 8 of the textbook. The lecture starts with describing the structure of the IPv6 protocol, the new IPv6 header format with a discussion of each field. It also describes what extension headers are, what types of extension headers have been defined, and how they are used. Then the lecture covers IPv6 addressing. Explaining everything about the new address format, address notation, address types. Finally, ICMPv6 is covered starting with ICMPv6 message format, the ICMPv6 error messages This lecture also discusses the extended functionality based on ICMPv6, such as neighbor discovery, autoconfiguration, path MTU discovery.

Provider Prefix	Subnet	Interface Identifier
48bits	16bits	64bits

Figure 4: Unicast Global Address Format

FE80	0	Interface Identifier
16bits	48bits	64bits

Figure 5: Link Local Address Format

FC/FD	Unique Id	Subnet	Interface Identifier
8bits	40bits	16bits	64bits

Figure 6: Unique Local Address Format

0	FFFF	IPv4 Address
80bits	16bits	32bits

Figure 7: IPv4 Mapped Address Format

2002	IPv4 address	Subnet	Interface Identifier
16bits	32bits	16bits	64bits

Figure 8: 6to4 Address Format

0	1
127bits	

Figure 9: Loopback Address Format

FF	l	S	Multicast Group Identifier
14bits			112bits

Figure 10: Multicast Address Format

3.4.3 Lecture 5, 6, 7: Routing

Lecture 5, 6, 7 cover chapters 9 through 15 of the textbook. In this chapter routing protocols are discussed with a focus on IPv6. After going through static routing. The changes made to RIP to become RIPng, OSPF version 3, and Extensions for BGP4 called BGP4+ to handle IPv6 are discussed. Proprietary routing protocols like IS-IS and EIGRPv6 are also touched upon. MPLS for IPv6 is discussed. DHCPv6 and DNSv6 changes like quad A records are also discussed. For the last lecture in the routing series, multicast is extensively studied. Reasons why multicast was not widely used in IPv4 are studied, and the changes made to ensure that the protocol is more widely supported in IPv6 are looked into.

3.4.4 Lecture 8, 9: Transition

Lecture 8, 9 cover chapters 16 and 17 of the textbook. Lecture 8 covers how IPv6 can be deployed in IPv4 dominant networks. Lecture 9 covers how IPv6 dominant networks can be configured to still support IPv4. Starting with interoperability, the different transition mechanisms are defined, such as dual stack, tunneling, and translation techniques. This lecture also highlights how the various mechanisms can be combined together to work towards a smoother transition. The lecture also tries to highlight missing aspects. Finally concluding with security and cost considerations.

3.4.5 Lecture 10: Mobility

Lecture 10 covers chapters 11 and 12 of the textbook. This lecture covers Mobile IPv6. Mobile IPv6 has changed almost completely from Mobile IPv4. These changes are studied. Some concepts which are covered are triangle routing, route optimizations, handoffs and fast handoffs, home agents, etc. The specific extension headers for mobility are introduced. Security considerations are discussed. Finally, this lecture goes through explaining that Mobile IPv6 might be the real reason for the eventual adoption of IPv6, and thus enabling IPv6 to be the foundation for the next generation of smart mobile devices and services.

3.4.6 Lecture 11: Security

Lecture 11 covers chapter 13 of the textbook. The lecture begins with a discussion of various security requirements observed over the years in IPv4. Elaborates on some of the security concepts. Then goes into detail covering the new IP security framework, which is a mandatory part of IPv6 unlike IPv4. It stresses on the various authentication and encryption features of the new IPv6 protocol. Talks about how extended headers are extensively used for IP security model. Then the lecture concludes by briefly talking about the kind of new security needs which might arise in the future with new technologies like internet of things becoming a ubiquitous reality.

3.4.7 Lecture 12: Quality of Service and Network Management

Lecture 12 covers chapters 14, 19 and 20 of the textbook. This chapter covers quality of service enhancements available in IPv6. It highlights some ways to implement it with various service classes. Some configuration examples and performance test results are provided and studied. IPv6 flow routing using the flow label field is extensively studied. Upper layer protocols like transmission control protocol and user datagram protocol are studied. Then network management aspects are covered. Starting with the internet control message protocol. Congestion notification mechanisms are covered. Then different mechanisms to gather management information using SNMP and its MIBs are covered. Some network management tools are touched on.

3.4.8 Lecture 13: Case Studies

Lecture 13 covers chapters 21 and 23 of the textbook. It covers some case studies of successful IPv6 implementations and transitions around the world in big and small companies. Lessons learnt in those transitions are presented. The idea is to show the students that others have faced the issues which they would likely face in their transition. Some project planning, design, management and execution aspects of developing an IPv6 transition plan are also covered.

3.4.9 Lecture 14: Conclusion

Lecture 14 covers chapter 24 of the textbook. Concluding the course, it discusses some future directions in which the internet and the IPv6 protocol are heading. It tries to forecast about the things yet to come. The project management aspects covered in the previous lecture are concluded. Then some mechanisms to test if the transition has been a successful one are presented. Network maintenance topics required after the transition are also covered with an emphasis on some pointers of what issues to watch out for. And finally some time is spent on revision for the final exam.

3.5 Assignments Design

3.5.1 Assignment 1 – Building a business case for IPv6

Assignment 1 has to do with the designing of a business case or business proposal for an IPv6 transition plan. Which is usually the first step in a larger planning process of the IPv6 transition. The intention here is that this business plan can be built upon to a more complete transition plan for Assignment 2. The goal of assignment 1 is to ensure that the student taking this course is convinced that an IPv6 transition is not a choice, but it is inevitable. The only choice is when the transition needs to be made. This assignment hopes to make sure the student gets convinced of the advantages of IPv6 and the reasons why it is needed, early on in the course. So that the course can build on into the technical aspects of the course early on instead of spending time on the rationale behind IPv6.

3.5.2 Assignment 2 – Building a plan for IPv6 transition

Assignment 2 is a buildup of Assignment 1. The goal of the Assignment 2 is for the student to extend the Assignment 1 business case into a more or less complete plan of an IPv6 transition. This assignment is to be done at the end of the course, and in a way is a culmination of the course. The goal is to make sure the student has reached to a point where he feels comfortable with the planning aspects of the course, and is able to use all the various skills he has acquired into one final written paper.

3.6 Mid Term Quiz Design

The midterm component is a quiz of forty short objective and multiple choice questions. Out of the forty questions, ten are easy, ten hard and the rest twenty are chosen to be moderate. Each question typically requires under one minute to answer, and is equivalent to a quarter point. A quiz is chosen specifically and not a written exam because of the fact that the course already has a lot of hands on components like labs and assignments which require the student to come up with plans and designs. And which require a report to be submitted. So since there is a lot of writing already in other components, it was decided to use a quiz to introduce variety in the mix of components. A quiz also helps the course being taught online, so that the student can take it at home, and it's possible to randomize questions from a question bank to eliminate cheating.

3.7 Final Exam Design

Unlike the midterm quiz, the final exam has short essay type questions of around ten in number. With each question weighing a point and each question requiring about five to six minutes to answer, such that the whole exam can be completed in an hour. These questions typically can be answered in about three to five sentences. The questions are generally analytical in nature, requiring the student to not just remember information, but also think and reason. Also these questions are designed such that they can be answered to the point, and will not have an opinion as a typical answer. Some sample questions which can be asked on the final exam are given below.

1. Will IPv6 mean the end of NAT. What is your opinion on the topic?
2. Why was the Header Checksum filed removed from IPv6, even though it was present in IPv4?
3. What is the real goal for the OMB federal government mandate for IPv6?
4. While using IPv4 mapped IPv6 addresses, what is needed to ensure that a client only having IPv4 can communicate with a server only having IPv6?
5. Is it possible for 6to4 to function with dynamically issued IPv4 addresses via DHCP?

3.8 Labs Design

Since this course is primarily targeted for graduate students, a majority of who are working professionally. The laboratory components for this course are designed to be open, unscheduled and structured. By open we mean that the students typically complete these labs without the assistance or presence of an instructor. Unscheduled means that even though there is a scheduled time and place in the networking lab available for the students to work on the activities. If the students choose, they can do the labs independently and alone at any time by taking advantage of the open hours in the lab. Or even at home on an open source and freely available simulation environment like GNS3. The students are encouraged to work at the scheduled time to encourage collective learning and team work, even though the reports are individual and not team based.

And also the labs are designed to be goal oriented and not process oriented. What this means is that step by step instructions and the specific commands and syntax necessary to be typed on the routers are not provided. The labs are divided into activities, and each activity has certain goals. The students are encouraged to find the commands needed and document the steps needed to reach the goals. This was done with the intension that, at the graduate level, it will make students feel more comfortable with investigating the commands and coming up with their own processes to achieve the required goals.

3.8.1 Lab 1 – IPv6 Addressing and SLAAC

Lab 1 primarily deals with addressing, both manual addressing and auto configuration. The students will understand the difference between global unique addressing and unique local addressing. Students will understand that an interface can have both of these types of addresses at the same time. EUI-64 is also experienced. The router solicitation and router advertisement messages used for autoconfiguration are looked at in detail.

3.8.2 Lab 2 – IPv6 Neighbour Discovery

Lab 2 expands on Lab 1 to understand the neighbour solicitation and neighbour advertisement messages. These messages are used for neighbour discovery and duplicate address detection. Neighbour discovery is used in IPv6 instead of address resolution protocol to locate other nodes on the subnet. Duplicate address detection ensures that the auto configured IPv6 addresses are unique. Students also understand how IPv6 supports easy renumbering, by actually performing the numbering change from one provided prefix to another.

3.8.3 Lab 3 – IPv6 Static Routing and OSPFv3

Lab 3 finally explores the routing aspects of IPv6. Both static routing and dynamic routing protocols are experienced. For the dynamic protocol OSPF is specifically configured. Students are asked to compare the new features in OSPF by looking at the packet captures to compare between version 2 and version 3.

3.8.4 Lab 4, 5 – IPv6 BGPv6 and IPv6 Traffic Filtering

Lab 4 focusses on exterior routing protocols specifically Border Gateway Protocol in IPv6. The students are provided with autonomous numbers and are asked to configure BGP zones and test whether the BGP peering works. In lab 5 students work with access lists to preform traffic filtering. The goal is to block IPv6 unique local traffic form reaching a global unicast subnet.

3.8.5 Lab 6 – IPv6 Tunnelling

The last lab, which is lab 6 has students exposed to the various tunnelling options available in IPv6. Tunnels carry either IPv6 traffic over an IPv4 segment or IPv4 traffic over the IPv6 internet. Students first start with configuring manual tunnels. Then automatic tunnels like 6to4, and ISATAP are configured. Finally, two additional weeks are provided for the students to catch up on lab reports if required.

4 Conclusion

RFC 1883 was published in December 1995. This RFC was the first to introduce the IPv6 protocol. Two decades have since past the publication of the RFC, and there is as much fear, uncertainty and doubt today as there was in 1995 about this new protocol. Its predecessor, IPv4 has been doing its job of addressing each and every node present in the ever expanding internet since 1983.

IPv4 was originally introduced when there were no more than a few dozens of interconnected nodes, and all these nodes were all cooperating with each other. That is, they were all connected to the original ARPANET. These nodes were all talking to each other and were managed by people who were all talking to each other. This is what enabled the relatively easy upgrade from the Network Control Protocol (NCP) to IPv4. The typical number of systems which needed to be updated then were less than what is typically found in a small sized enterprise or branch office of today. That is, we are talking of an entity with less than a hundred employees. System administrators back then were also network programmers. And almost all of these system administrators, knew almost all of each other. It was such a small community, that if needed they could gather in a single room. The best part about this small sized community meant that any upgrades needed to be done on the network software, could be done at the same time by everyone involved. And the process of making such a change would be requiring very little synchronisation. And in the very rare case, if something went wrong during the upgrades, everyone can just roll back to the older code, decide to collectively hold off till a newer date, meanwhile the bug or bugs would be located, and a fix would be applied instantaneously. [14]

Nevertheless, back then none of those computer systems and networks were controlling critical systems to the world economy, national defence and communications like todays computers control the banking system, air traffic, medical equipment in hospitals, military communication networks controlling missile systems, etc. So the fact that today's networks are so omnipresent in people's lives and control such important systems affecting people's lives, means that any transition to a newer protocol or technology will need to be made after meticulous planning and study. Also the transition will need to happen while everything is fully functional. This raises the bar on the risk and complexity involved in the required transition to IPv6. Because of these challenges, developing a transition plan for IPv6 is no less complicated than building a space program from scratch. The team which worked on the IPv6 task force at IETF has foreseen this and thus a lot of effort has been spent on transition technologies. It is these technologies which will act as a bridge in the transition years, to make IPv6 and IPv4 interoperate smoothly.

This complex plethora of technologies to help with the transition from IPv4 to IPv6 is the reason for offering this course at RIT. These technologies are so diverse that they require specialist knowledge. This course has attempted to impart that very specialist knowledge, thus will be of great help in increasing the level of expertise among the potential students who would take this course.

5 Appendices

5.1 Course Proposal Form

R·I·T

B. Thomas Golisano College of Computing and Information Sciences

Department of Information Sciences and Technology

NEW (or REVISED) COURSE:

1.0 **Title**: Transition to IPv6

Date: August 10, 2016

Credit Hours: 3

Prerequisite(s): NSSA 602 Enterprise Computing

NSSA 620 Emerging Computing and Network Technologies

Co-requisite(s): None

Course proposed by: Venu Gopal Kakarla

2.0 **Course information:**

	Contact hours per week	**Maximum students per section**
Classroom	1.5	30
Lab	2	15
Active Learning / Active Learning Extended		
Other (specify)	Distance Course	15

Quarter(s) offered *(check)*

[Y] **Fall** [ ] **Intersession** [Y] **Spring** [ ] **Summer**

Students required to take this course: (by program and year, as appropriate)

None

Students who might elect to take the course:

Matriculated students in the following programs,

- MS in Networking and Systems Administration
- MS in Computing Security and Information Assurance
- MS in Information Technology

3.0 Goals of the course *(including rationale for the course, when appropriate)*:

This course mainly focusses on understanding how IPv6 is different from IPv4. Students who are already be familiar with IPv4 will understand the differences and improvements made to the protocol stack. The students will be working on coming up with a transition strategy while developing a plan, working on steps in executing it and at the same time they will learn of methods to verify the progress of their plan, and to make it more complex, they will understand that they will need to do all this while managing a live network. Henceforth it is important that the students be made aware of the risks and limitations of IPv6. The students completing this course will also learn to eventually transition their networks from IPv4 to IPv6. Primarily reducing the fear, uncertainty and doubt. Thus making the whole change less intimidating.

4.0 Course description

This course is a laboratory-based course that focuses on the next generation Internet Protocol Version 6. Topics covered include IPv6 Packet Formats, Extension Headers, Unicast Multicast and Anycast addressing, Scoped addressing, various addressing architectures, static and automatic address configuration using DHCPv6 and Router advertisements, Duplicate Address Detection, Neighbor Discovery using ICMPv6, DNS in IPv6 featured such as DNS Server Discovery are covered. Source Routing, Static Routing, Multicast Routing and Dynamic Routing protocols like RIPng, OSPFv3, IS-ISv6, BGP4 are covered. The various transition technologies covered are divided into deploying IPv6 in IPv4 dominant networks and deploying IPv6 dominant networks with IPv4 support. The first category includes tunneling IPv6 in IPv4, like Static Tunneling, 6to4, ISATAP and using Tunnel Brokers. The later includes tunneling IPv4 in IPv6, DSTM and IP Translation. Special topics include

Renumbering, Multihoming, Mobility, Security, QoS, Network Management, application porting.

(Prerequisite: NSSA 602, NSSA 620) Class 3, Lab 2, Credit 3

5.0 Possible resources (texts, references, computer packages, etc.)

Primary Texts:

1. Marc Blanchet. 2016. Migrating to IPv6: A Practical Guide to Implementing IPv6 in Mobile and Fixed Networks (2nd ed.). John Wiley & Sons, Ltd.

Supplemental Texts:

1. Michael Dooley, Timothy Rooney. 2013. IPv6 Deployment and Management. Wiley-IEEE Press.
2. Karl Sill. 2008. IPv6 Mandates. John Wiley & Sons, Ltd.
3. Ciprian Popoviciu, Eric Levy-Abegnoli, Patrick Grossetete. 2006. Deploying IPv6 Networks. Cisco Press.
4. Silvia Hagen, Vint Cerf. 2014. Ipv6 Essentials (3nd ed.). O'Reilly Media, Inc.
5. Silvia Hagen. 2011. Planning for IPv6 (1st ed.). O'Reilly Media, Inc.
6. Tom Coffeen. 2014. IPv6 Address Planning. O'Reilly Media, Inc.
7. Niall Richard Murphy and David Malone. 2005. IPv6 Network Administration (1st ed.). O'Reilly Media, Inc.
8. Dan York. 2011. Migrating Applications to IPv6 (1st ed.). O'Reilly Media, Inc.

Supporting Materials: None

6.0 Topics (outline):

1. Week 1 Introduction
2. Week 2 Technical Fundamentals 1

   Packet Formats, Extension Headers, Unicast Multicast and Anycast Addressing, Scoped Addresses, Addressing Architecture
3. Week 3 Technical Fundamentals 2

Static address configuration, Automatic address configuration, DHCPv6, Router Advertisements, ARP, Duplicate Address Detection, EUI-64

4. Week 4 Technical Fundamentals 3

   Internet Control Message Protocol, Neighbor Discovery, IPv6 and DNS, Quad A records, DNS Server Discovery
5. Week 5 Routing 1

   Source Routing, Static Routing, RIP, OSPF, IS-IS, BGP,
6. Week 6 Routing 2

   Configuring Routing, Renumbering, Multihoming
7. Week 7 Routing 3

   Multicast Groups, Multicast Routing, Multicast Addressing, Anycast
8. Week 9 Transition 1

   Deploying IPv6 in IPv4 dominant networks, Tunneling IPv6 in IPv4, Static Tunneling, 6to4, ISATAP, Tunnel Brokers
9. Week 10 Transition 2

   Deploying IPv6 dominant networks with IPv4 support, Tunneling IPv4 in IPv6, DSTM, IP Translation
10. Week 11 Mobility
11. Week 12 Security
12. Week 13 QoS, Network Management,
13. Week 14 Porting, Case Studies
14. Week 15 Conclusion

7.0 Intended learning outcomes and associated assessment methods of those outcomes

At the completion of this course, successful students will be able/prepared to:

1. describe technologies emerging in the field of networking and system administration and their impact on large organizations
2. be a key contributing member in the development, management, or research of the computing infrastructure of an enterprise

3. describe and implement technologies important to the management and deployment of large scale computing environments
4. interface and communicate effectively at all levels of an organization
5. design, plan and manage effective computer and network upgrades that meet the operational and business goals of their organizations
6. participate effectively in research positions, leadership positions, or professional careers in computing in both private and public sectors, or alternatively, for admission to other academic programs

8.0 Program or general education goals supported by this course

1. Communication
   a. Express themselves effectively in common college-level written forms using standard American English
   b. Revise and improve written and visual content
   c. Express themselves effectively in presentations, either in spoken standard American English or sign language (American Sign Language or English-based Signing)
   d. Comprehend information accessed through reading and discussion
2. Intellectual Inquiry
   a. Review, assess, and draw conclusions about hypotheses and theories
   b. Analyze arguments, in relation to their premises, assumptions, contexts, and conclusions
   c. Construct logical and reasonable arguments that include anticipation of counter-arguments
   d. Use relevant evidence gathered through accepted scholarly methods and properly acknowledge sources of information
3. Ethical, Social and Global Awareness
   a. Analyze similarities and differences in human experiences and consequent perspectives
   b. Examine connections among the world's populations
   c. Identify contemporary ethical questions and relevant stakeholder positions
4. Scientific, Mathematical and Technological Literacy

a. Explain basic principles and concepts of one of the natural sciences
b. Apply methods of scientific inquiry and problem solving to contemporary issues

c. Comprehend and evaluate mathematical and statistical information
d. Perform college-level mathematical operations on quantitative data
e. Describe the potential and the limitations of technology
f. Use appropriate technology to achieve desired outcomes

5. Creativity, Innovation and Artistic Literacy
   a. Demonstrate creative/innovative approaches to course-based assignments or projects
   b. Interpret and evaluate artistic expression considering the cultural context in which it was created

9.0 Other relevant information *(such as special classroom, studio, or lab needs, special scheduling, media requirements, etc.)*

The following lab will be required for the student's use

- GOL 2160 Networking Lab

10.0 Supplemental information

Other relevant books, journal articles, commercial publications, and websites as selected by the course instructor(s).

APPROVALS:

____ __________________

IST Curriculum Committee Chair   Date

____ __________________

IST Department Chair   Date

5.2 Course Syllabus

NSSA XXX Transition to IPv6

Class Time and Location:	TRF 17:00 – 17:50 GOL XXXX
Course Mode:	On-campus/Online
Prerequisite(s):	NSSA 602 Enterprise Computing NSSA 620 Emerging Computing and Network Technologies

Instructor Information

Instructor:	Venu Gopal, Lecturer, Information Sciences & Technologies.
Contact Information:	Office: GOL-XXXX Phone: 585-475-XXXX Email: xxxxxx@rit.edu
Contact Policy and Preferences	Office hours:
Online Course Material/ Course Webpage	The course materials will all be available through MyCourses

Course Description

NSSA XXX Transition to IPv6

This course is a laboratory-based course that focuses on the next generation Internet Protocol Version 6. Topics covered include IPv6 Packet Formats, Extension Headers, Unicast Multicast and Anycast addressing, Scoped addressing, various addressing architectures, static and automatic address configuration using DHCPv6 and Router advertisements, Duplicate Address Detection, Neighbor Discovery using ICMPv6, DNS in IPv6 featured such as DNS Server Discovery are covered. Source Routing, Static Routing, Multicast Routing and Dynamic Routing protocols like RIPng, OSPFv3, IS-ISv6, BGP4 are covered. The various transition technologies covered are divided into deploying IPv6 in IPv4 dominant networks and deploying IPv6 dominant networks with IPv4 support. The first category includes tunneling IPv6 in IPv4, like Static Tunneling, 6to4, ISATAP and using Tunnel Brokers. The later includes tunneling IPv4 in IPv6, DSTM and IP Translation. Special topics include Renumbering, Multihoming, Mobility, Security, QoS, Network Management, application porting. (Prerequisite: NSSA 815, NSSA 850) Class 3, Lab 2, Credit 4

Course Overview

This course mainly focusses on understanding how IPv6 is different from IPv4. Students who are already be familiar with IPv4 will understand the differences and improvements made to the protocol stack. The students will be working on coming up with a transition strategy while developing a plan, working on steps in executing it and at the same time they will learn of methods to verify the progress of their plan, and to make it more complex, they will understand that they will need to do all this while managing a live network. Henceforth it is important that the students be made aware of the risks and limitations of IPv6. The students completing this course will also learn to eventually transition their networks from IPv4 to IPv6. Primarily reducing the fear, uncertainty and doubt. Thus making the whole change less intimidating.

Course Learning Outcomes

At the completion of this course, successful students will be able/prepared to:

1. describe technologies emerging in the field of networking and system administration and their impact on large organizations
2. be a key contributing member in the development, management, or research of the computing infrastructure of an enterprise
3. describe and implement technologies important to the management and deployment of large scale computing environments
4. interface and communicate effectively at all levels of an organization
5. design, plan and manage effective computer and network upgrades that meet the operational and business goals of their organizations
6. participate effectively in research positions, leadership positions, or professional careers in computing in both private and public sectors, or alternatively, for admission to other academic programs

Program Learning Outcomes

1. Communication
    a. Express themselves effectively in common college-level written forms using standard American English
    b. Revise and improve written and visual content
    c. Express themselves effectively in presentations, either in spoken standard American English or sign language (American Sign Language or English-based Signing)
    d. Comprehend information accessed through reading and discussion
2. Intellectual Inquiry
    a. Review, assess, and draw conclusions about hypotheses and theories
    b. Analyze arguments, in relation to their premises, assumptions, contexts, and conclusions
    c. Construct logical and reasonable arguments that include anticipation of counter-arguments
    d. Use relevant evidence gathered through accepted scholarly methods and properly acknowledge sources of information
3. Ethical, Social and Global Awareness
    a. Analyze similarities and differences in human experiences and consequent perspectives
    b. Examine connections among the world's populations
    c. Identify contemporary ethical questions and relevant stakeholder positions
4. Scientific, Mathematical and Technological Literacy
    a. Explain basic principles and concepts of one of the natural sciences
    b. Apply methods of scientific inquiry and problem solving to contemporary issues
    c. Comprehend and evaluate mathematical and statistical information
    d. Perform college-level mathematical operations on quantitative data
    e. Describe the potential and the limitations of technology
    f. Use appropriate technology to achieve desired outcomes
5. Creativity, Innovation and Artistic Literacy
    a. Demonstrate creative/innovative approaches to course-based assignments or projects

b. Interpret and evaluate artistic expression considering the cultural context in which it was created.

Teaching Philosophy

I enjoy teaching classes based on problem based learning. I feel that students learn best when they can try technologies out to see how they translate into solutions for business problems. My goal in structuring my classes is to create an environment where student feel free to try new things and to try new and innovative things even at the risk of failure.

Audience

This course is meant for students who are network managers or are aspiring to be network managers or anyone who has a stake in running or operating a network.

Course Topics

15. Week 1 Introduction
16. Week 2 Technical Fundamentals 1

    Packet Formats, Extension Headers, Unicast Multicast and Anycast Addressing, Scoped Addresses, Addressing Architecture
17. Week 3 Technical Fundamentals 2

    Static address configuration, Automatic address configuration, DHCPv6, Router Advertisements, ARP, Duplicate Address Detection, EUI-64
18. Week 4 Technical Fundamentals 3

    Internet Control Message Protocol, Neighbor Discovery, IPv6 and DNS, Quad A records, DNS Server Discovery
19. Week 5 Routing 1

    Source Routing, Static Routing, RIP, OSPF, IS-IS, BGP,
20. Week 6 Routing 2

    Configuring Routing, Renumbering, Multihoming
21. Week 7 Routing 3

    Multicast Groups, Multicast Routing, Multicast Addressing, Anycast
22. Week 9 Transition 1

Deploying IPv6 in IPv4 dominant networks, Tunneling IPv6 in IPv4, Static Tunneling, 6to4, ISATAP, Tunnel Brokers

23. Week 10 Transition 2

    Deploying IPv6 dominant networks with IPv4 support, Tunneling IPv4 in IPv6, DSTM, IP Translation

24. Week 11 Mobility
25. Week 12 Security
26. Week 13 QoS, Network Management,
27. Week 14 Porting, Case Studies
28. Week 15 Conclusion

Course Materials

Required Texts:

1. Marc Blanchet. 2016. Migrating to IPv6: A Practical Guide to Implementing IPv6 in Mobile and Fixed Networks (2nd ed.). John Wiley & Sons, Ltd.

Supplemental Texts:

1. Michael Dooley, Timothy Rooney. 2013. IPv6 Deployment and Management. Wiley-IEEE Press.
2. Karl Sill. 2008. IPv6 Mandates. John Wiley & Sons, Ltd.
3. Ciprian Popoviciu, Eric Levy-Abegnoli, Patrick Grossetete. 2006. Deploying IPv6 Networks. Cisco Press.
4. Silvia Hagen, Vint Cerf. 2014. Ipv6 Essentials (3nd ed.). O'Reilly Media, Inc.
5. Silvia Hagen. 2011. Planning for IPv6 (1st ed.). O'Reilly Media, Inc.
6. Tom Coffeen. 2014. IPv6 Address Planning. O'Reilly Media, Inc.
7. Niall Richard Murphy and David Malone. 2005. IPv6 Network Administration (1st ed.). O'Reilly Media, Inc.
8. Dan York. 2011. Migrating Applications to IPv6 (1st ed.). O'Reilly Media, Inc.

Course Schedule

Class meeting sections will be divided into lectures and labs. Tuesday and Thursday classes will be devoted to lectures on new technologies while Fridays will be used for labs and student group work and will meet in the Networking lab GOL 2160.

Week	Topics	Assigned Reading	Activities/Labs
Week 1	Introduction	TB: 1,2 R1: 1,12 R2: 1	Assignment 1 Discussion
Week 2	Technical Fundamentals 1	TB: 3,4 R1: 2,3	Assignment 1 Due
Week 3	Technical Fundamentals 2	TB: 5,6 R1: 7	Lab1
Week 4	Technical Fundamentals 3	TB: 7,8 R1: 4	Lab2
Week 5	Routing 1	TB: 9 R1: 8	Lab3
Week 6	Routing 2	TB: 10	Lab4
Week 7	Routing 3	TB: 15	Lab5
Week 8	Revision, Study, Mid Term		Mid Term Quiz
Week 9	Transition 1	TB: 16 R1: 10	Lab6
Week 10	Transition 2	TB: 17 R2: 3	Lab6
Week 11	Mobility	TB: 11,12 R1: 11	Catchup Lab
Week 12	Security	TB: 13 R1: 5	Assignment 2 Discussion
Week 13	QoS, Network Management	TB: 14,19,20 R1: 6,9	
Week 14	Porting, Case Studies	TB: 21,23 R2: 2	Assignment 2 Due
Week 15	Conclusion, Revision, Study	TB: 24	
Week 16	Finals Week No Class		Final Exam

TB:	Mark Blanchet. Migrating to IPv6: A Practical Guide to Implementing IPv6 in Mobile and Fixed Networks. Wiley (2nd ed.). 2016.
R1:	Silvia Hagen. Ipv6 Essentials (3nd ed.). O'Reilly Media, Inc. 2014.
R2:	Silvia Hagen. Planning for IPv6 (1st ed.). O'Reilly Media, Inc. 2011.

Note any breaks, holidays or planned absences (such as for conferences) during the semester.

Grading / Evaluation

Your overall evaluation is based on the following components:

Grade Scale

Based on the 100% total listed above, letter grades will be assigned as follows:

	Grading Weightage
Lectures	**0%**
Labs	**60%**
Assignments	**20%**
Mid Term Quiz	10%
Final Exam	10%
Total	**100%**

Range	**Grade**
Greater than 90	A
Between 80 and 90	B
Between 70 and 80	C
Between 60 and 70	D
Less than 60	F
Incomplete	I

Late Work

Assignments are due when assigned. Please let me know if an assignment is going to be late.

Attendance and Participation

There is a positive correlation between attending class and doing well in the class. Don't fall behind and don't blow off class.

Expectations

From students

I expect you to come to class prepared to learn and interested in the subject of our course. This will be an interesting class, but it will only be fun if you make it that way. Do the outside reading, take notes in class, don't expect to learn everything on one review of the material.

Time commitment

Since this is a three-credit hour course, you should plan to spend two hours per week in class, two hours in lab, and an additional six to twelve hours on readings, research, discussions, lab write-ups, assignments, etc. The rule-of-thumb is two to three hours per week outside the "classroom" for every credit hour per week in the classroom. If you do the math, it adds to twelve–sixteen hours per week, total.

Writing standards

Written work should adhere to Standard American English. Please proof your papers and e-mail messages before submitting them. I will grade for content, completeness, organization, spelling, grammar, and punctuation, as well as demonstration of knowledge gained in the course and your ability to apply it.

Course Policies

Academic Integrity Statement

As an institution of higher learning, RIT expects students to behave honestly and ethically at all times, especially when submitting work for evaluation in conjunction with any course or degree requirement. The Department of Information Science and Technology encourages all students to become familiar with the RIT Honor Code and with RIT's Academic Honesty Policy.

Statement on Reasonable Accommodations

RIT is committed to providing reasonable accommodations to students with disabilities. If you would like to request accommodations such as special seating or testing modifications due to a disability, please contact the Disability Services Office. It is located in the Student Alumni Union, Room 1150; the Web site is www.rit.edu/dso. After you receive accommodation approval, it is imperative that you see me during office hours so that we can work out whatever arrangement is necessary.

Other Elements

Changes to the syllabus

I have provided this syllabus as guide to our course and have made every attempt to provide an accurate overview of the course. However, as instructor, I reserve the right to modify this document during the semester, if necessary, to ensure that we achieve course learning objectives. You will receive advance notice of any changes to the syllabus through myCourses/email.

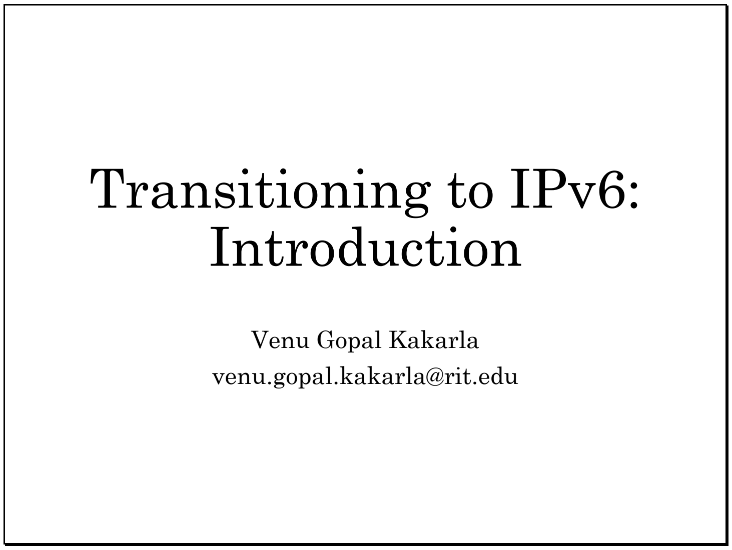
Concluding statement

Most importantly, please be assured that I want students to learn and to receive the good grades they deserve. So please make an appointment with me should you have undue difficulty with your work in the course.

5.3 Lecture Slides

5.3.1 Lecture 1

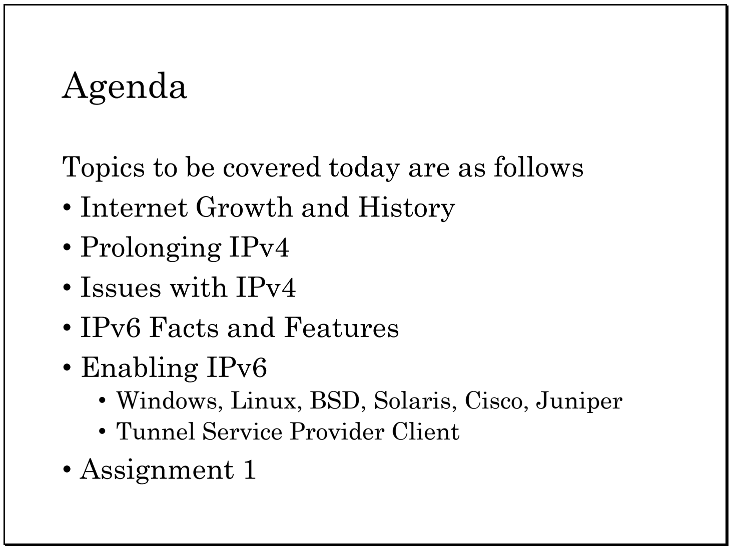
Slide 1



Transitioning to IPv6: Introduction

Venu Gopal Kakarla
venu.gopal.kakarla@rit.edu

Slide 2

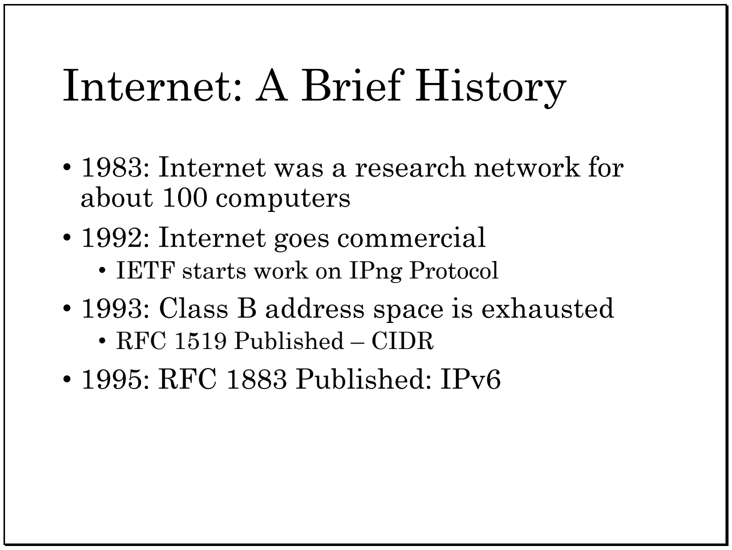


Agenda

Topics to be covered today are as follows

- Internet Growth and History
- Prolonging IPv4
- Issues with IPv4
- IPv6 Facts and Features
- Enabling IPv6
  - Windows, Linux, BSD, Solaris, Cisco, Juniper
  - Tunnel Service Provider Client
- Assignment 1

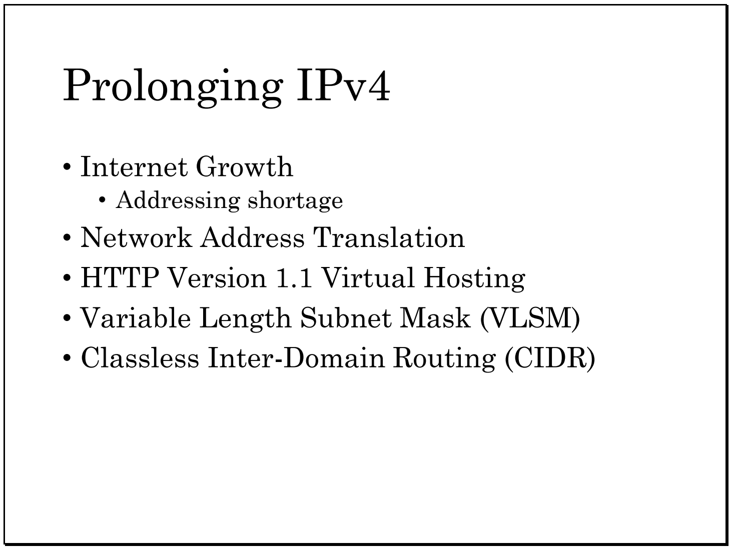
Slide 3



Internet: A Brief History

- 1983: Internet was a research network for about 100 computers
- 1992: Internet goes commercial
  - IETF starts work on IPng Protocol
- 1993: Class B address space is exhausted
  - RFC 1519 Published – CIDR
- 1995: RFC 1883 Published: IPv6

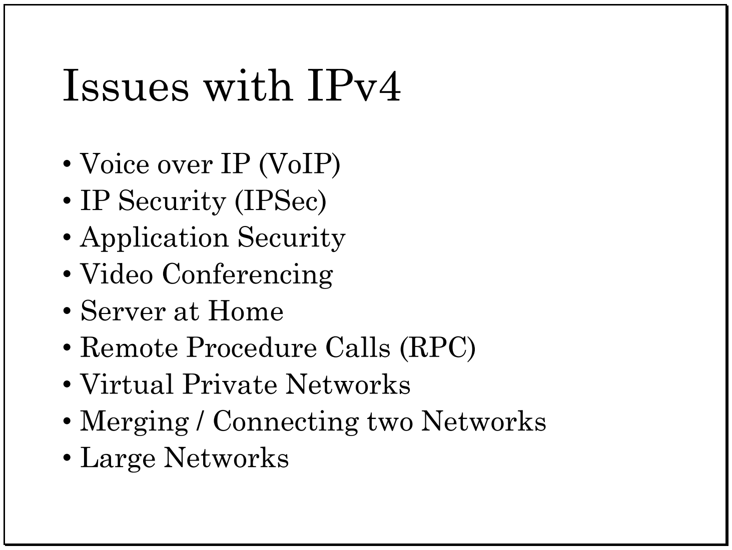
Slide 4



Prolonging IPv4

- Internet Growth
  - Addressing shortage
- Network Address Translation
- HTTP Version 1.1 Virtual Hosting
- Variable Length Subnet Mask (VLSM)
- Classless Inter-Domain Routing (CIDR)

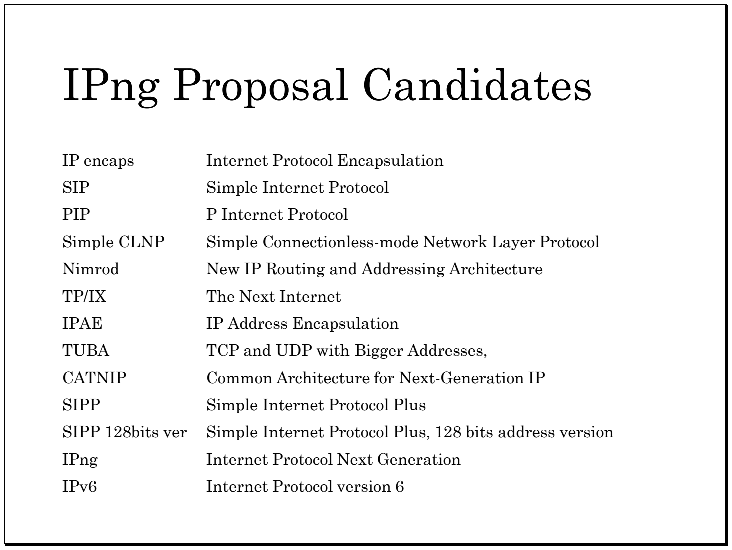
Slide 5



Issues with IPv4

- Voice over IP (VoIP)
- IP Security (IPSec)
- Application Security
- Video Conferencing
- Server at Home
- Remote Procedure Calls (RPC)
- Virtual Private Networks
- Merging / Connecting two Networks
- Large Networks

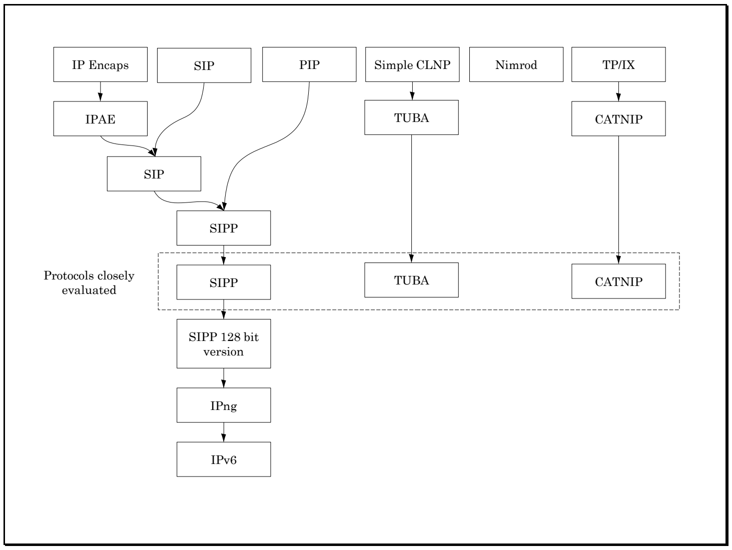
Slide 6



IPng Proposal Candidates

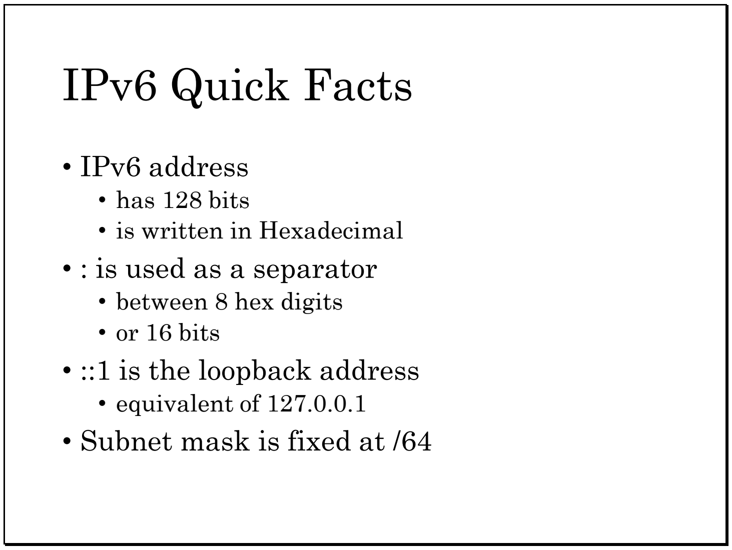
IP encaps	Internet Protocol Encapsulation
SIP	Simple Internet Protocol
PIP	P Internet Protocol
Simple CLNP	Simple Connectionless-mode Network Layer Protocol
Nimrod	New IP Routing and Addressing Architecture
TP/IX	The Next Internet
IPAE	IP Address Encapsulation
TUBA	TCP and UDP with Bigger Addresses,
CATNIP	Common Architecture for Next-Generation IP
SIPP	Simple Internet Protocol Plus
SIPP 128bits ver	Simple Internet Protocol Plus, 128 bits address version
IPng	Internet Protocol Next Generation
IPv6	Internet Protocol version 6

Slide 7



IP Encaps
SIP
PIP
Simple CLNP
Nimrod
TP/IX
IPAE
TUBA
CATNIP
SIP
SIPP
Protocols closely evaluated
SIPP
TUBA
CATNIP
SIPP 128 bit version
IPng
IPv6

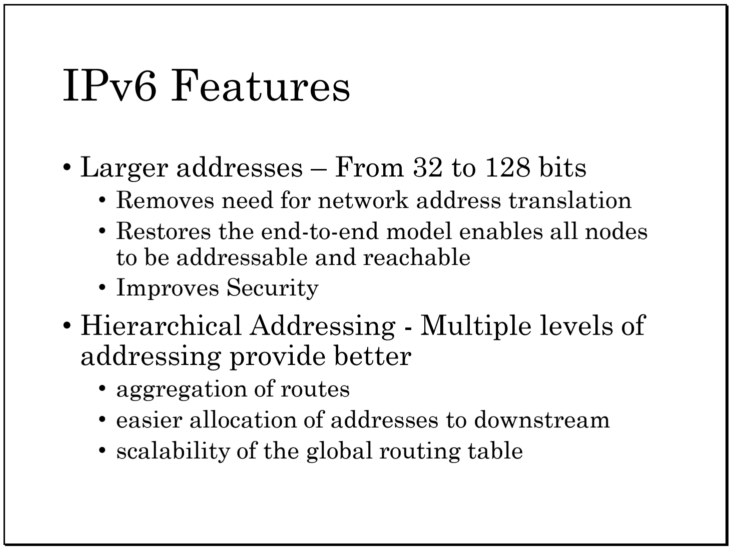
Slide 8



IPv6 Quick Facts

- IPv6 address
  - has 128 bits
  - is written in Hexadecimal
- : is used as a separator
  - between 8 hex digits
  - or 16 bits
- ::1 is the loopback address
  - equivalent of 127.0.0.1
- Subnet mask is fixed at /64

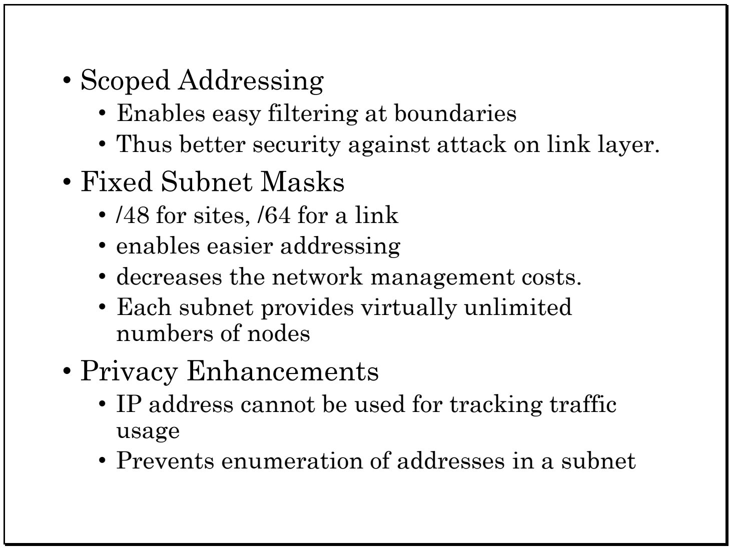
Slide 9



IPv6 Features

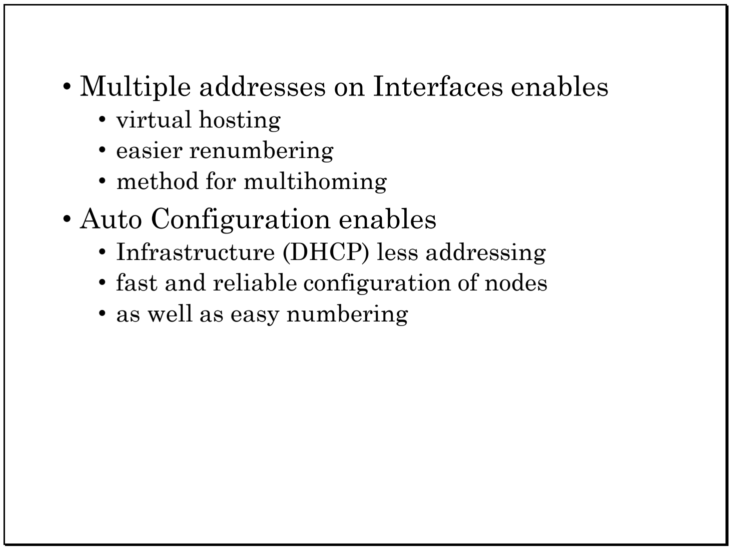
- Larger addresses – From 32 to 128 bits
  - Removes need for network address translation
  - Restores the end-to-end model enables all nodes to be addressable and reachable
  - Improves Security
- Hierarchical Addressing - Multiple levels of addressing provide better
  - aggregation of routes
  - easier allocation of addresses to downstream
  - scalability of the global routing table

Slide 10



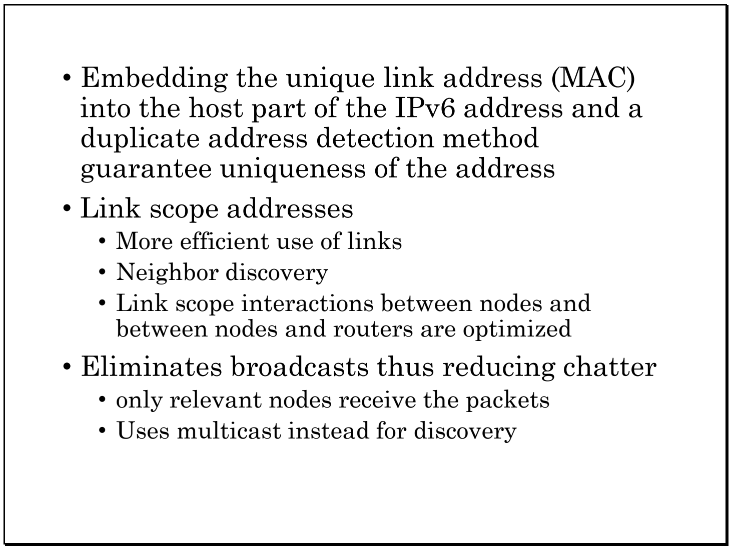
- Scoped Addressing
  - Enables easy filtering at boundaries
  - Thus better security against attack on link layer.
- Fixed Subnet Masks
  - /48 for sites, /64 for a link
  - enables easier addressing
  - decreases the network management costs.
  - Each subnet provides virtually unlimited numbers of nodes
- Privacy Enhancements
  - IP address cannot be used for tracking traffic usage
  - Prevents enumeration of addresses in a subnet

Slide 11



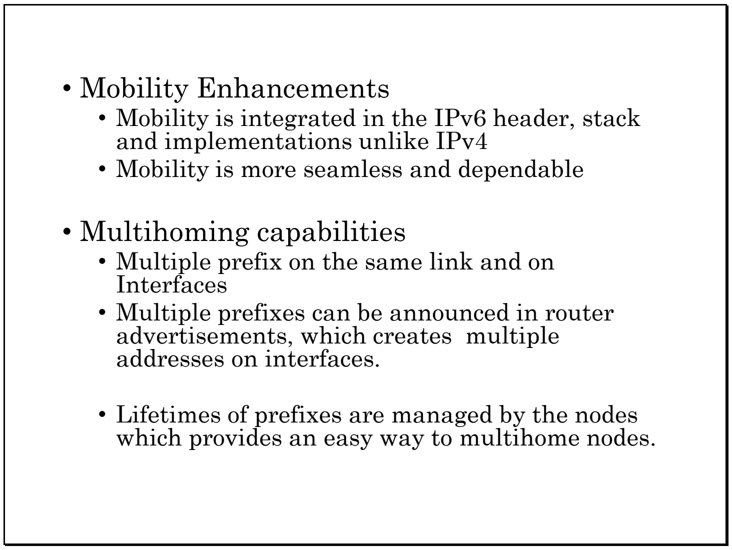
- Multiple addresses on Interfaces enables
  - virtual hosting
  - easier renumbering
  - method for multihoming
- Auto Configuration enables
  - Infrastructure (DHCP) less addressing
  - fast and reliable configuration of nodes
  - as well as easy numbering

Slide 12



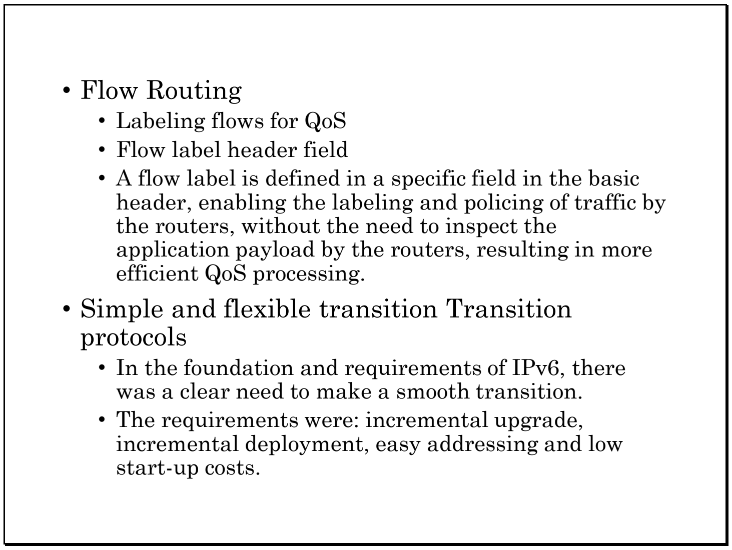
- Embedding the unique link address (MAC) into the host part of the IPv6 address and a duplicate address detection method guarantee uniqueness of the address
- Link scope addresses
  - More efficient use of links
  - Neighbor discovery
  - Link scope interactions between nodes and between nodes and routers are optimized
- Eliminates broadcasts thus reducing chatter
  - only relevant nodes receive the packets
  - Uses multicast instead for discovery

Slide 13



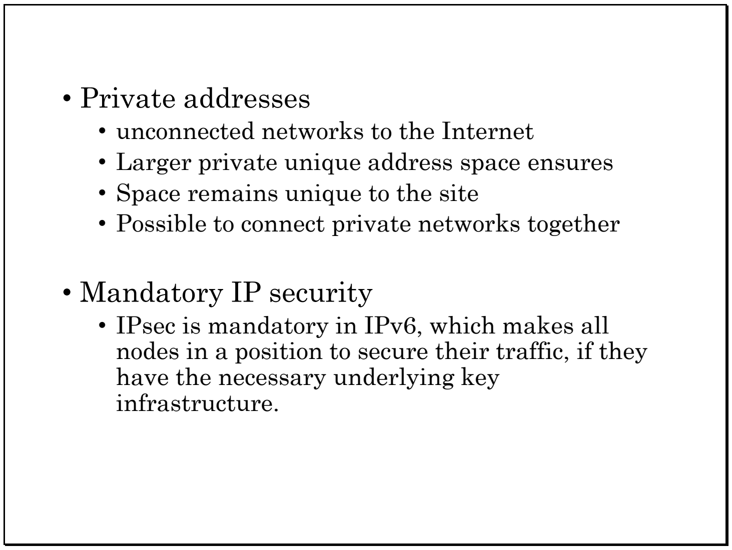
- Mobility Enhancements
  - Mobility is integrated in the IPv6 header, stack and implementations unlike IPv4
  - Mobility is more seamless and dependable
- Multihoming capabilities
  - Multiple prefix on the same link and on Interfaces
  - Multiple prefixes can be announced in router advertisements, which creates multiple addresses on interfaces.
  - Lifetimes of prefixes are managed by the nodes which provides an easy way to multihome nodes.

Slide 14



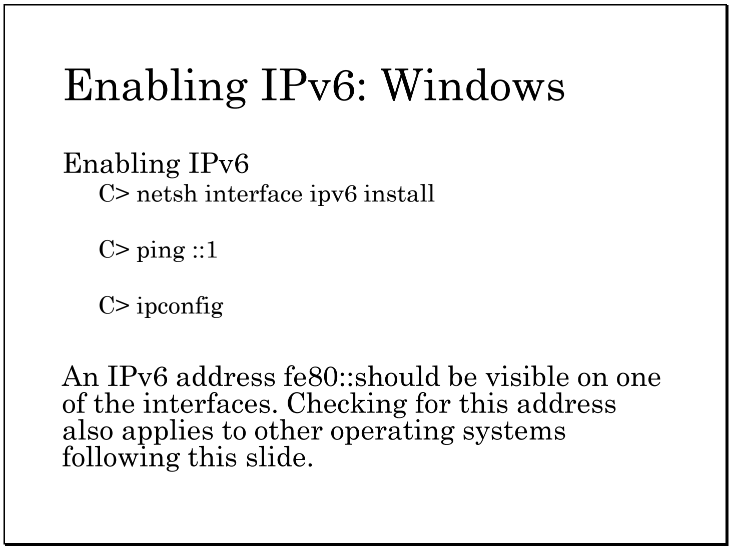
- Flow Routing
  - Labeling flows for QoS
  - Flow label header field
  - A flow label is defined in a specific field in the basic header, enabling the labeling and policing of traffic by the routers, without the need to inspect the application payload by the routers, resulting in more efficient QoS processing.
- Simple and flexible transition Transition protocols
  - In the foundation and requirements of IPv6, there was a clear need to make a smooth transition.
  - The requirements were: incremental upgrade, incremental deployment, easy addressing and low start-up costs.

Slide 15



- Private addresses
  - unconnected networks to the Internet
  - Larger private unique address space ensures
  - Space remains unique to the site
  - Possible to connect private networks together
- Mandatory IP security
  - IPsec is mandatory in IPv6, which makes all nodes in a position to secure their traffic, if they have the necessary underlying key infrastructure.

Slide 16



Enabling IPv6: Windows

Enabling IPv6

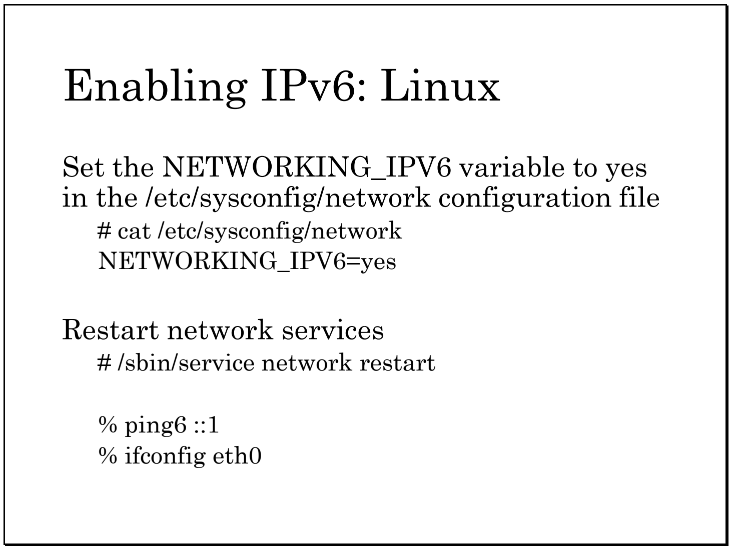
```
C> netsh interface ipv6 install

C> ping ::1

C> ipconfig
```

An IPv6 address fe80::should be visible on one of the interfaces. Checking for this address also applies to other operating systems following this slide.

Slide 17



Enabling IPv6: Linux

Set the NETWORKING_IPV6 variable to yes in the /etc/sysconfig/network configuration file

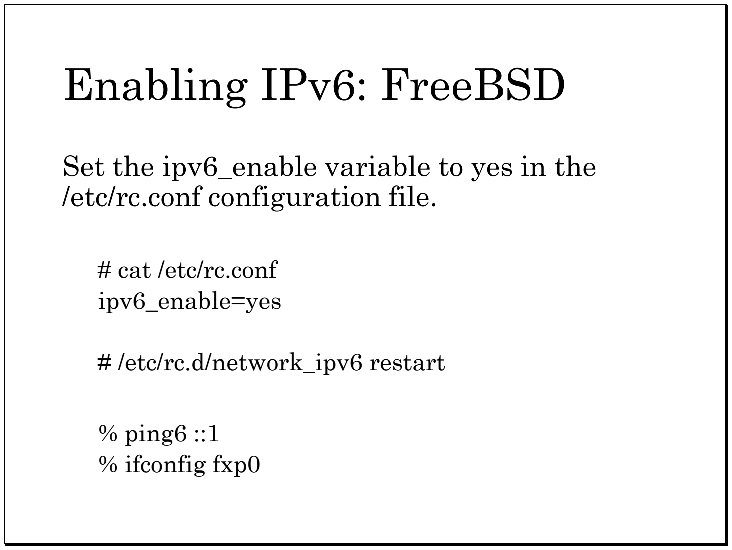
```
# cat /etc/sysconfig/network
NETWORKING_IPV6=yes
```

Restart network services

```
# /sbin/service network restart

% ping6 ::1
% ifconfig eth0
```

Slide 18



Enabling IPv6: FreeBSD

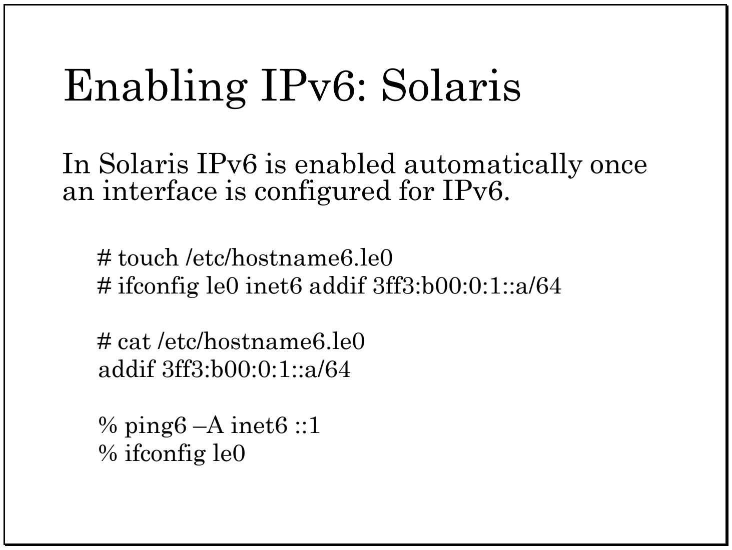
Set the ipv6_enable variable to yes in the /etc/rc.conf configuration file.

```
# cat /etc/rc.conf
ipv6_enable=yes

# /etc/rc.d/network_ipv6 restart

% ping6 ::1
% ifconfig fxp0
```

Slide 19



Enabling IPv6: Solaris

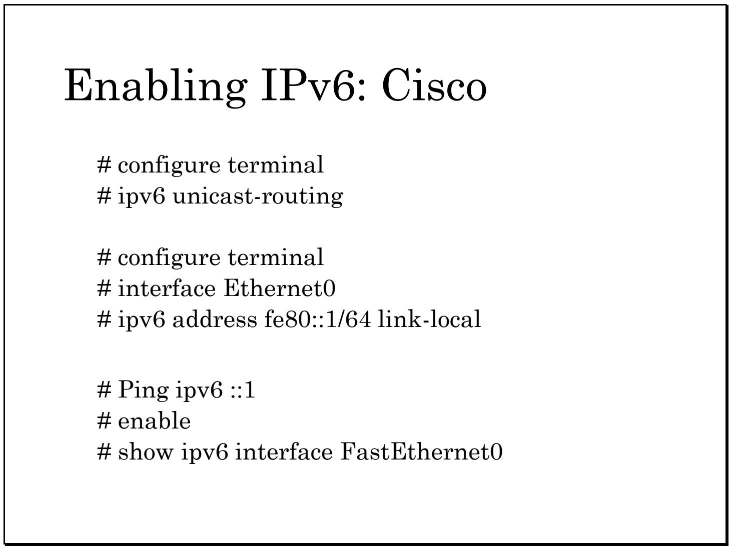
In Solaris IPv6 is enabled automatically once an interface is configured for IPv6.

```
# touch /etc/hostname6.le0
# ifconfig le0 inet6 addif 3ff3:b00:0:1::a/64

# cat /etc/hostname6.le0
addif 3ff3:b00:0:1::a/64

% ping6 –A inet6 ::1
% ifconfig le0
```

Slide 20



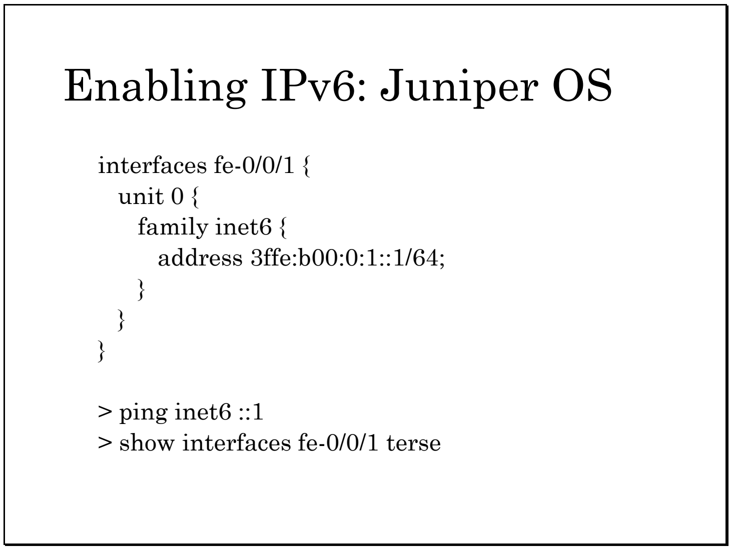
Enabling IPv6: Cisco

```
# configure terminal
# ipv6 unicast-routing

# configure terminal
# interface Ethernet0
# ipv6 address fe80::1/64 link-local

# Ping ipv6 ::1
# enable
# show ipv6 interface FastEthernet0
```

Slide 21

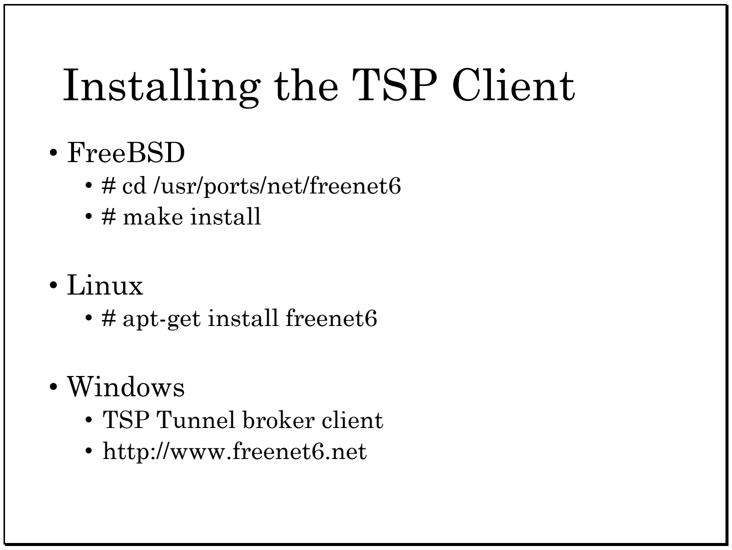


Enabling IPv6: Juniper OS

```
interfaces fe-0/0/1 {
  unit 0 {
    family inet6 {
      address 3ffe:b00:0:1::1/64;
    }
  }
}

> ping inet6 ::1
> show interfaces fe-0/0/1 terse
```

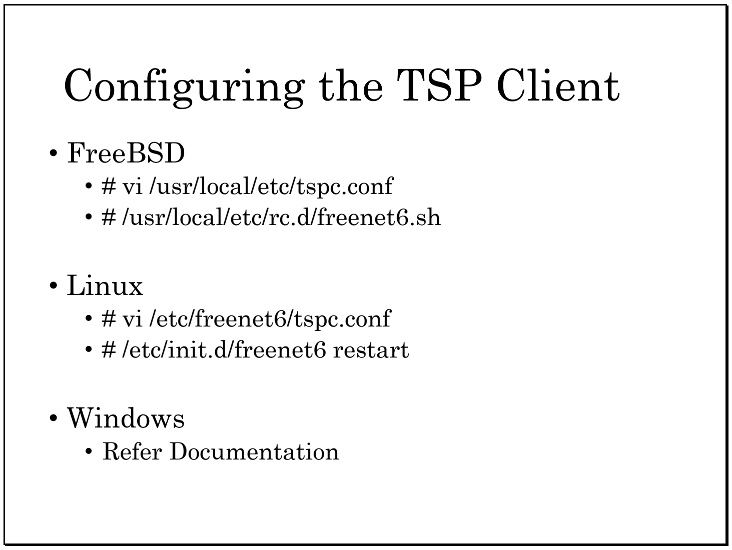
Slide 22



Installing the TSP Client

- FreeBSD
  - # cd /usr/ports/net/freenet6
  - # make install
- Linux
  - # apt-get install freenet6
- Windows
  - TSP Tunnel broker client
  - http://www.freenet6.net

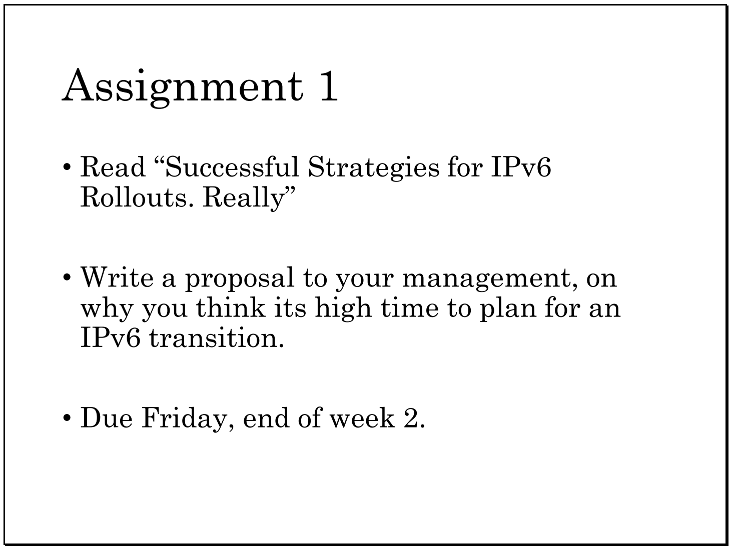
Slide 23



Configuring the TSP Client

- FreeBSD
  - # vi /usr/local/etc/tspc.conf
  - # /usr/local/etc/rc.d/freenet6.sh
- Linux
  - # vi /etc/freenet6/tspc.conf
  - # /etc/init.d/freenet6 restart
- Windows
  - Refer Documentation

Slide 24

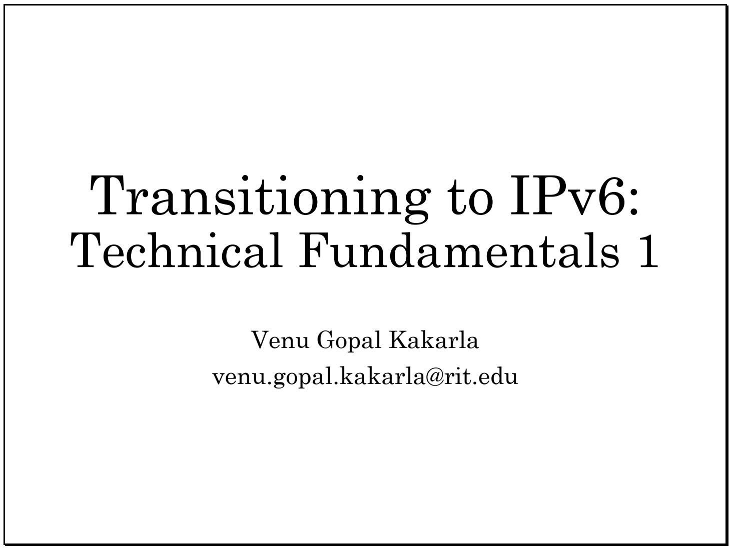


Assignment 1

- Read “Successful Strategies for IPv6 Rollouts. Really”
- Write a proposal to your management, on why you think its high time to plan for an IPv6 transition.
- Due Friday, end of week 2.

5.3.2 Lecture 2

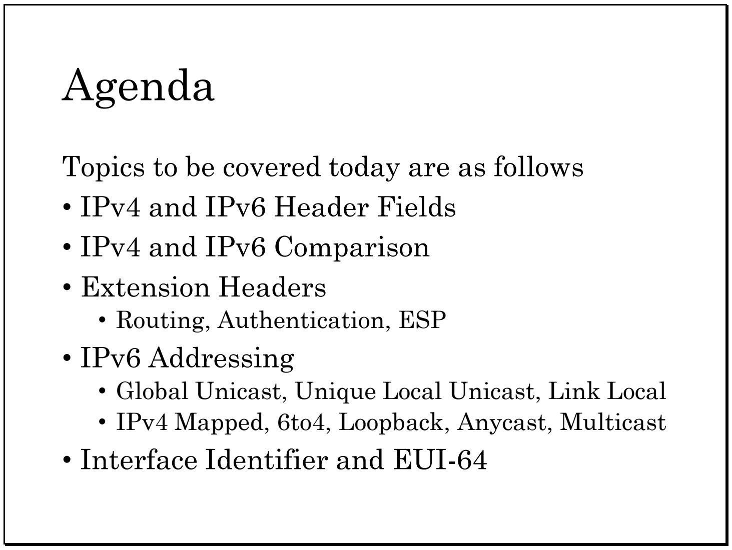
Slide 25



Transitioning to IPv6: Technical Fundamentals 1

Venu Gopal Kakarla
venu.gopal.kakarla@rit.edu

Slide 26

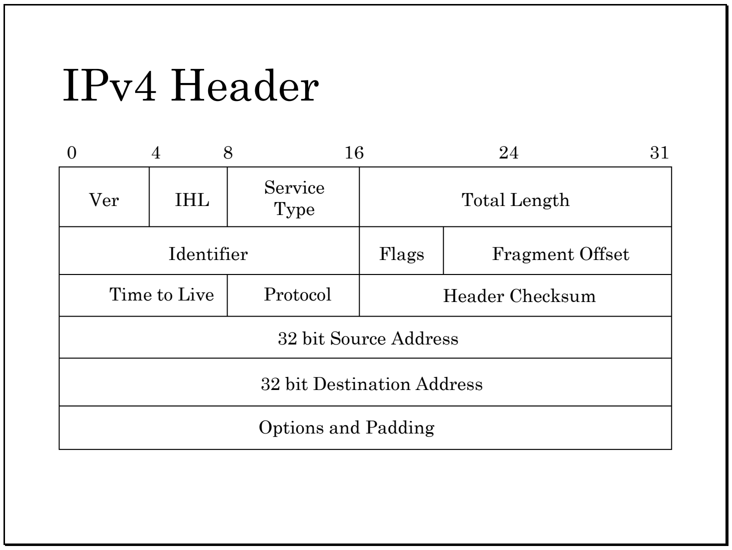


Agenda

Topics to be covered today are as follows

- IPv4 and IPv6 Header Fields
- IPv4 and IPv6 Comparison
- Extension Headers
  - Routing, Authentication, ESP
- IPv6 Addressing
  - Global Unicast, Unique Local Unicast, Link Local
  - IPv4 Mapped, 6to4, Loopback, Anycast, Multicast
- Interface Identifier and EUI-64

Slide 27

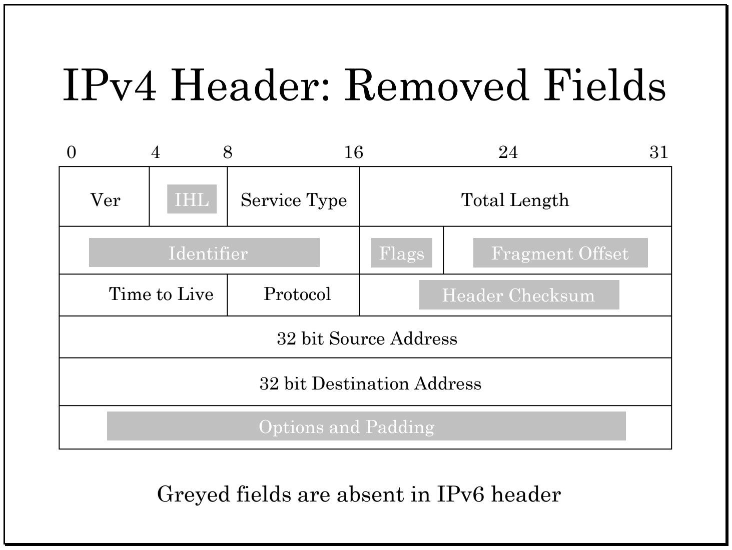


IPv4 Header

0 4 8 16 24 31

<table>
<tr><td>Ver</td><td>IHL</td><td>Service
Type</td><td colspan="2">Total Length</td></tr>
<tr><td colspan="3">Identifier</td><td>Flags</td><td>Fragment Offset</td></tr>
<tr><td colspan="2">Time to Live</td><td>Protocol</td><td colspan="2">Header Checksum</td></tr>
<tr><td colspan="5">32 bit Source Address</td></tr>
<tr><td colspan="5">32 bit Destination Address</td></tr>
<tr><td colspan="5">Options and Padding</td></tr>
</table>

Slide 28



IPv4 Header: Removed Fields

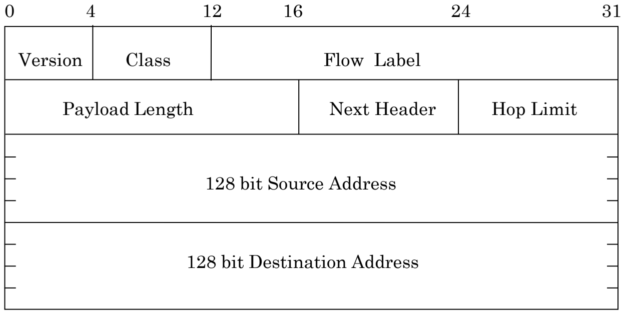
0 4 8 16 24 31

<table>
<tr><td>Ver</td><td>IHL</td><td>Service Type</td><td colspan="2">Total Length</td></tr>
<tr><td colspan="3">Identifier</td><td>Flags</td><td>Fragment Offset</td></tr>
<tr><td colspan="2">Time to Live</td><td>Protocol</td><td colspan="2">Header Checksum</td></tr>
<tr><td colspan="5">32 bit Source Address</td></tr>
<tr><td colspan="5">32 bit Destination Address</td></tr>
<tr><td colspan="5">Options and Padding</td></tr>
</table>

Greyed fields are absent in IPv6 header

Slide 29

IPv6 Header

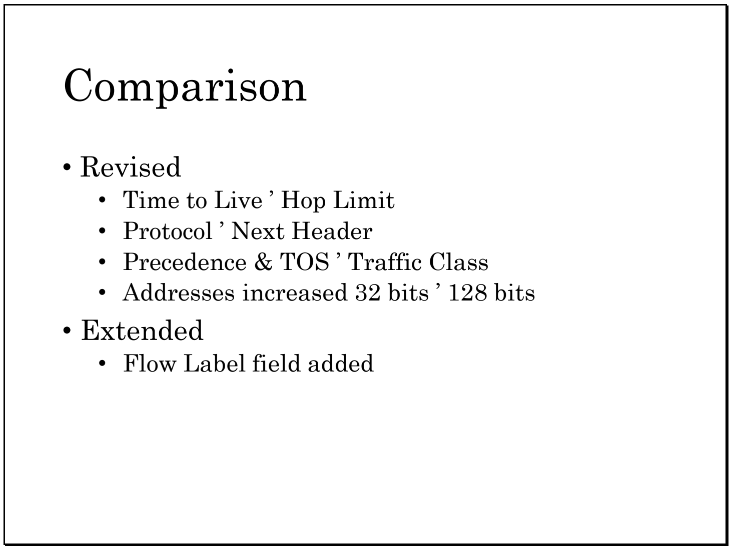


Slide 30

Comparison

- Fragmentation fields moved out of base header
- IP options moved out of base header
- Header Checksum eliminated
- Header Length field eliminated
- Length field excludes IPv6 header
- Alignment changed from 32 to 64 bits

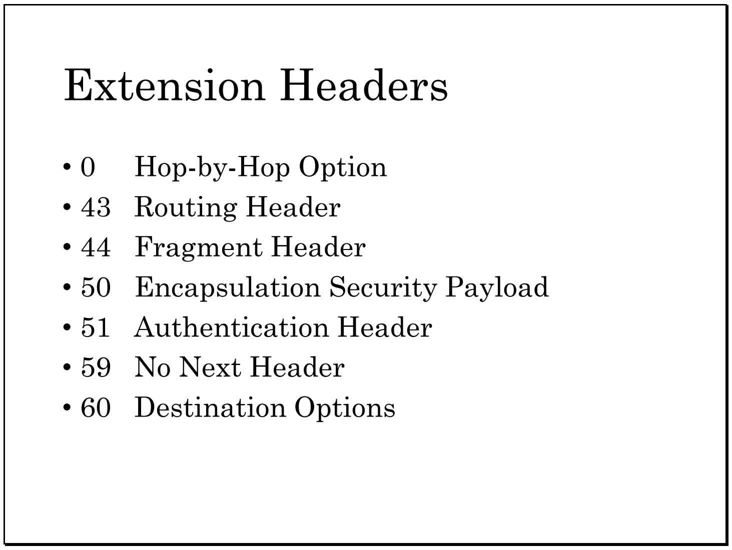
Slide 31



Comparison

- Revised
  - Time to Live ’ Hop Limit
  - Protocol ’ Next Header
  - Precedence & TOS ’ Traffic Class
  - Addresses increased 32 bits ’ 128 bits
- Extended
  - Flow Label field added

Slide 32

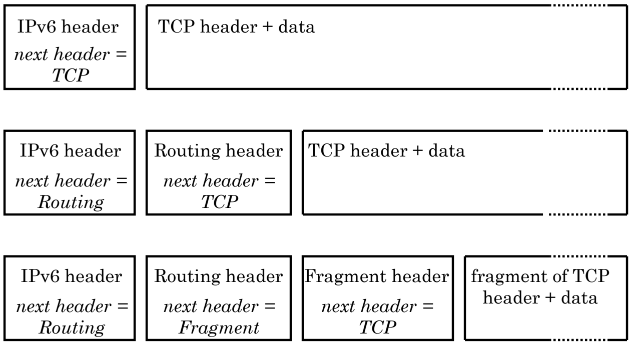


Extension Headers

0	Hop-by-Hop Option
43	Routing Header
44	Fragment Header
50	Encapsulation Security Payload
51	Authentication Header
59	No Next Header
60	Destination Options

Slide 33

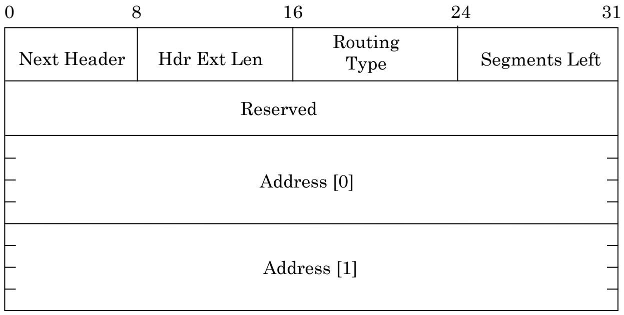
Extension Headers



IPv6 header *next header = TCP*	TCP header + data		
IPv6 header *next header = Routing*	Routing header *next header = TCP*	TCP header + data	
IPv6 header *next header = Routing*	Routing header *next header = Fragment*	Fragment header *next header = TCP*	fragment of TCP header + data

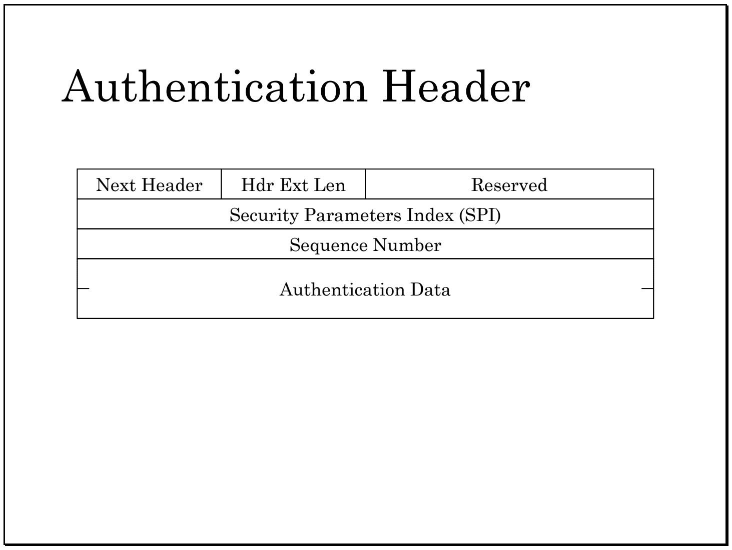
Slide 34

Routing Header



0	8	16	24 31
Next Header	Hdr Ext Len	Routing Type	Segments Left
Reserved			
Address [0]			
Address [1]			

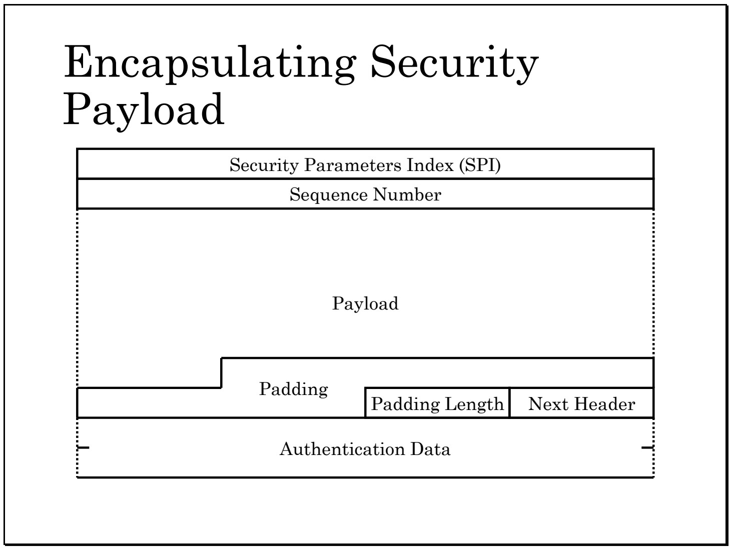
Slide 35



Authentication Header

Next Header	Hdr Ext Len	Reserved
Security Parameters Index (SPI)		
Sequence Number		
Authentication Data		

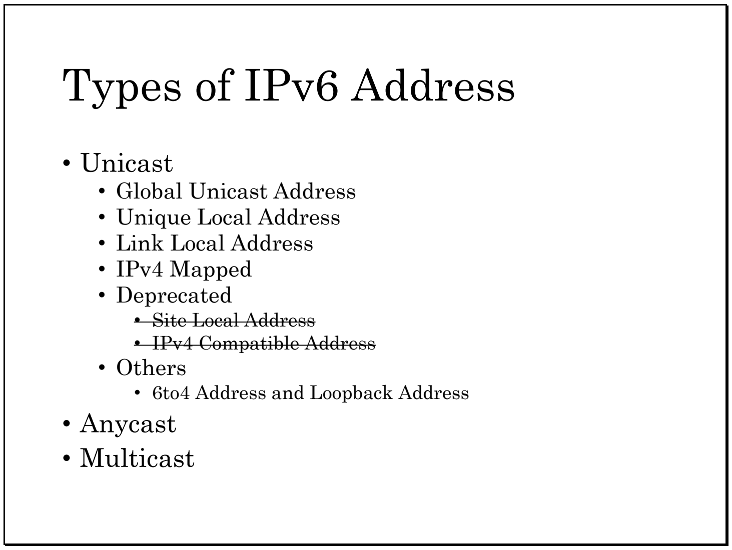
Slide 36



Encapsulating Security Payload

Security Parameters Index (SPI)		
Sequence Number		
Payload		
Padding	Padding Length	Next Header
Authentication Data		

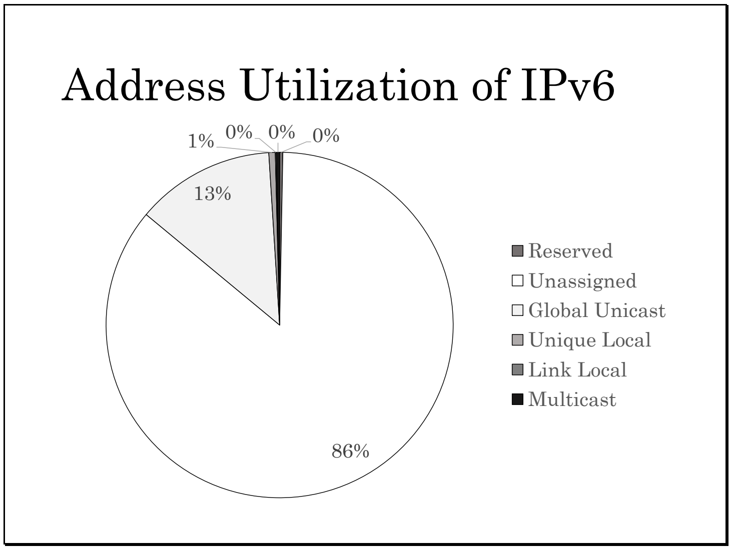
Slide 37



Types of IPv6 Address

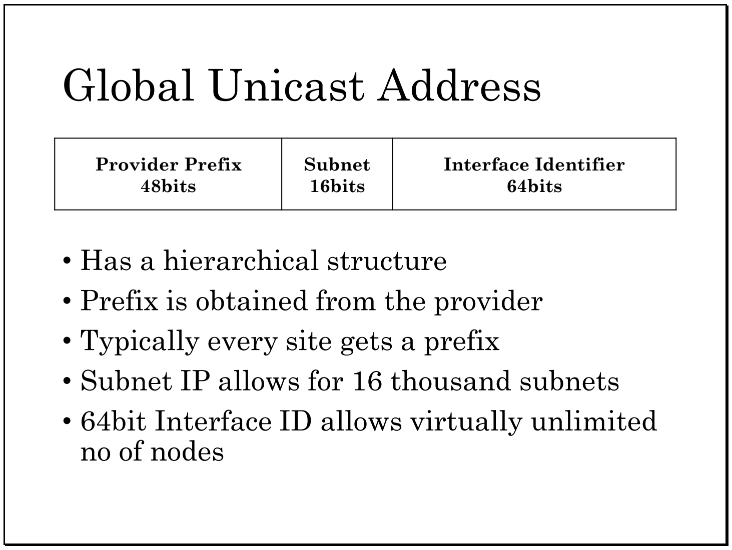
- Unicast
  - Global Unicast Address
  - Unique Local Address
  - Link Local Address
  - IPv4 Mapped
  - Deprecated
    - ~~Site Local Address~~
    - ~~IPv4 Compatible Address~~
  - Others
    - 6to4 Address and Loopback Address
- Anycast
- Multicast

Slide 38



Address Utilization of IPv6

Slide 39

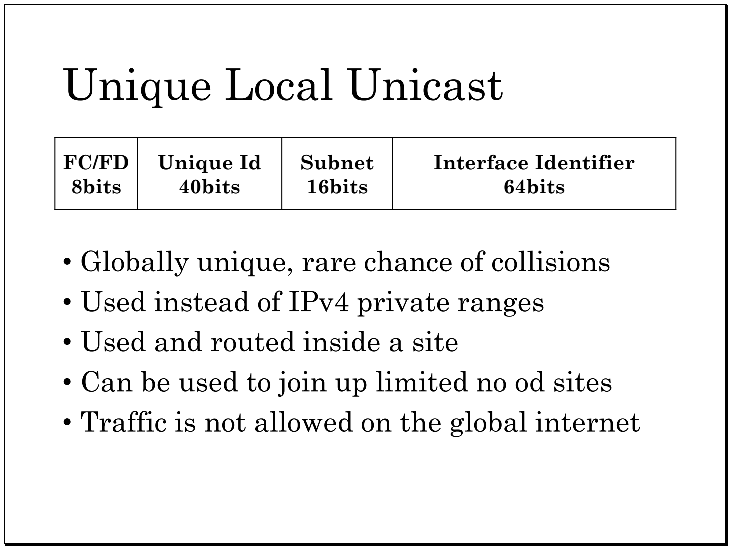


Global Unicast Address

Provider Prefix 48bits	Subnet 16bits	Interface Identifier 64bits

- Has a hierarchical structure
- Prefix is obtained from the provider
- Typically every site gets a prefix
- Subnet IP allows for 16 thousand subnets
- 64bit Interface ID allows virtually unlimited no of nodes

Slide 40

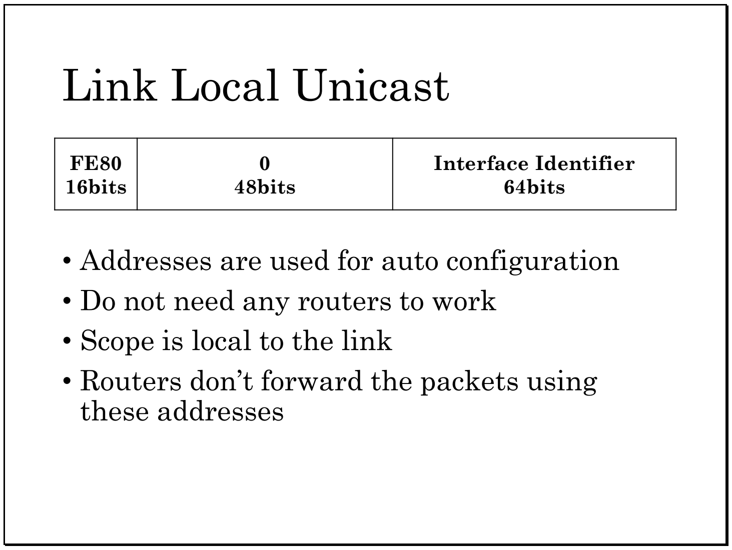


Unique Local Unicast

FC/FD 8bits	Unique Id 40bits	Subnet 16bits	Interface Identifier 64bits

- Globally unique, rare chance of collisions
- Used instead of IPv4 private ranges
- Used and routed inside a site
- Can be used to join up limited no od sites
- Traffic is not allowed on the global internet

Slide 41

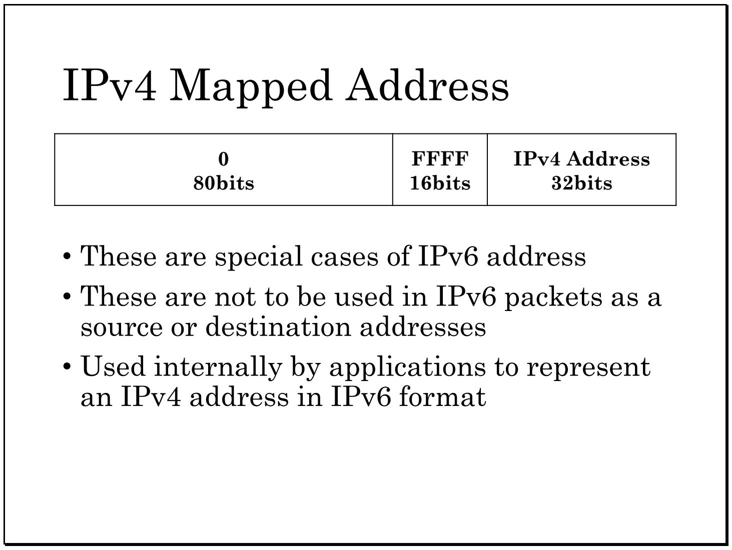


Link Local Unicast

FE80 16bits	0 48bits	Interface Identifier 64bits

- Addresses are used for auto configuration
- Do not need any routers to work
- Scope is local to the link
- Routers don’t forward the packets using these addresses

Slide 42

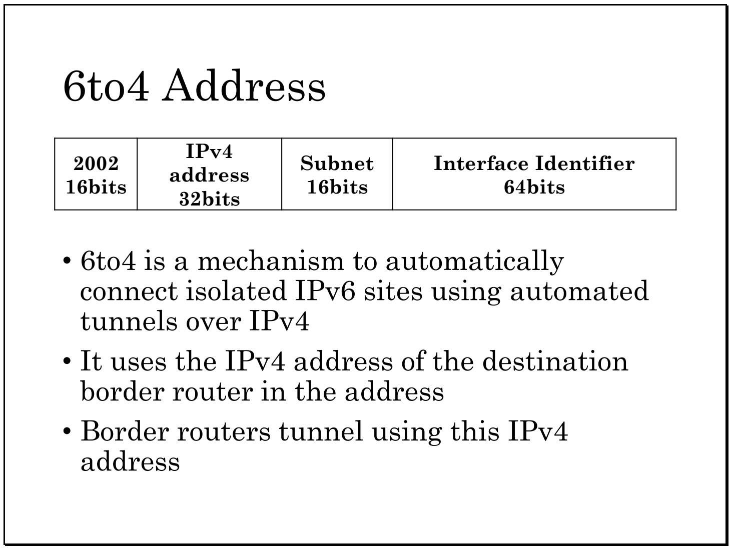


IPv4 Mapped Address

0 80bits	FFFF 16bits	IPv4 Address 32bits

- These are special cases of IPv6 address
- These are not to be used in IPv6 packets as a source or destination addresses
- Used internally by applications to represent an IPv4 address in IPv6 format

Slide 43

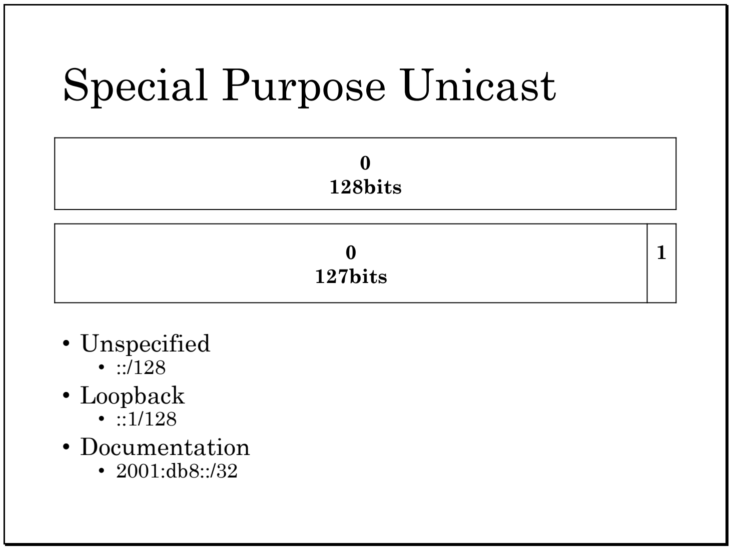


6to4 Address

2002 **16bits**	**IPv4** **address** **32bits**	**Subnet** **16bits**	**Interface Identifier** **64bits**

- 6to4 is a mechanism to automatically connect isolated IPv6 sites using automated tunnels over IPv4
- It uses the IPv4 address of the destination border router in the address
- Border routers tunnel using this IPv4 address

Slide 44



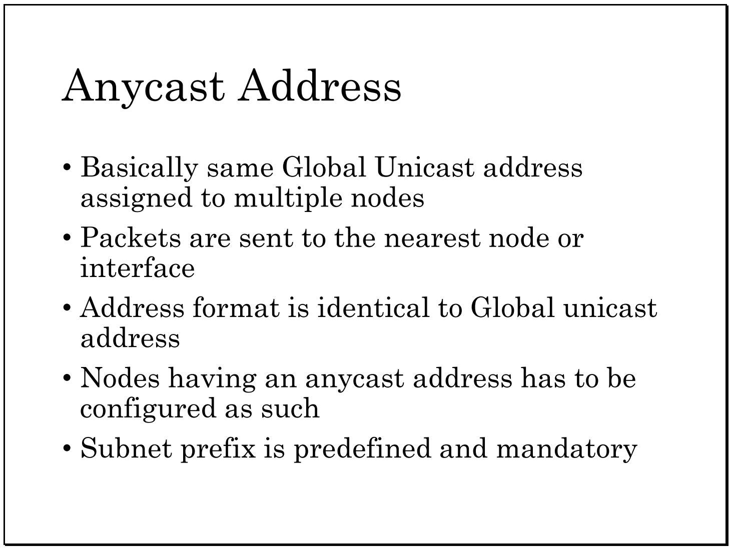
Special Purpose Unicast

0 **128bits**

0 **127bits**	**1**

- Unspecified
  - ::/128
- Loopback
  - ::1/128
- Documentation
  - 2001:db8::/32

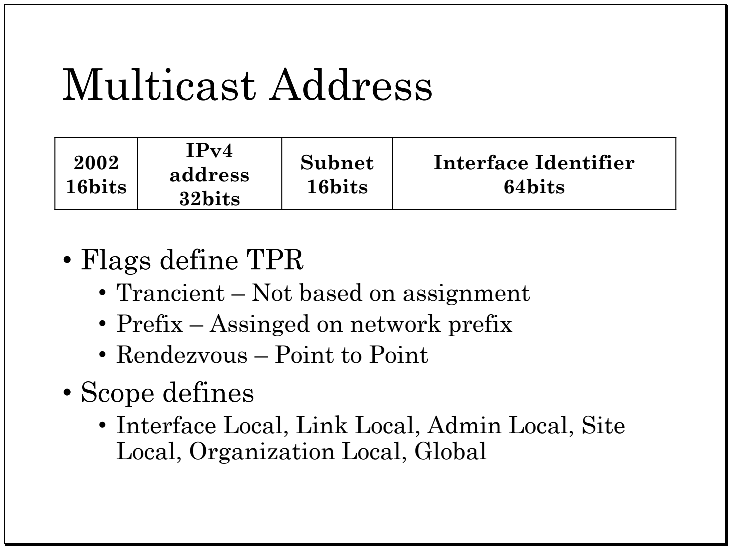
Slide 45



Anycast Address

- Basically same Global Unicast address assigned to multiple nodes
- Packets are sent to the nearest node or interface
- Address format is identical to Global unicast address
- Nodes having an anycast address has to be configured as such
- Subnet prefix is predefined and mandatory

Slide 46

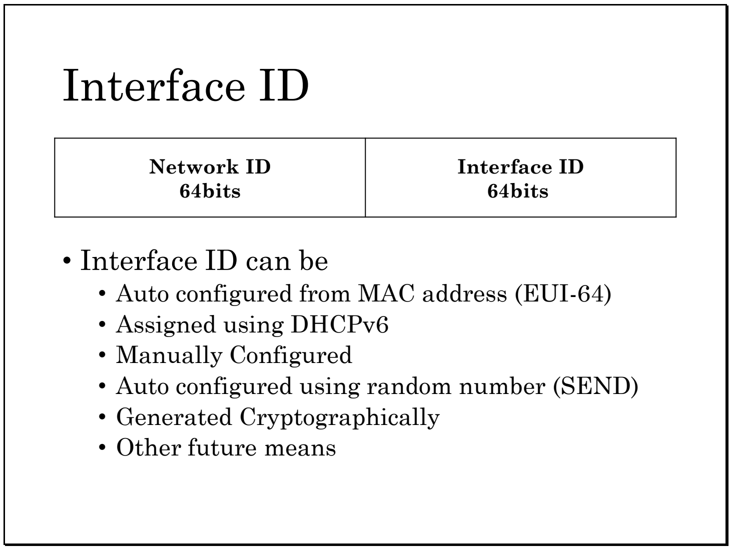


Multicast Address

2002 **16bits**	**IPv4** **address** **32bits**	**Subnet** **16bits**	**Interface Identifier** **64bits**

- Flags define TPR
  - Trancient – Not based on assignment
  - Prefix – Assinged on network prefix
  - Rendezvous – Point to Point
- Scope defines
  - Interface Local, Link Local, Admin Local, Site Local, Organization Local, Global

Slide 47

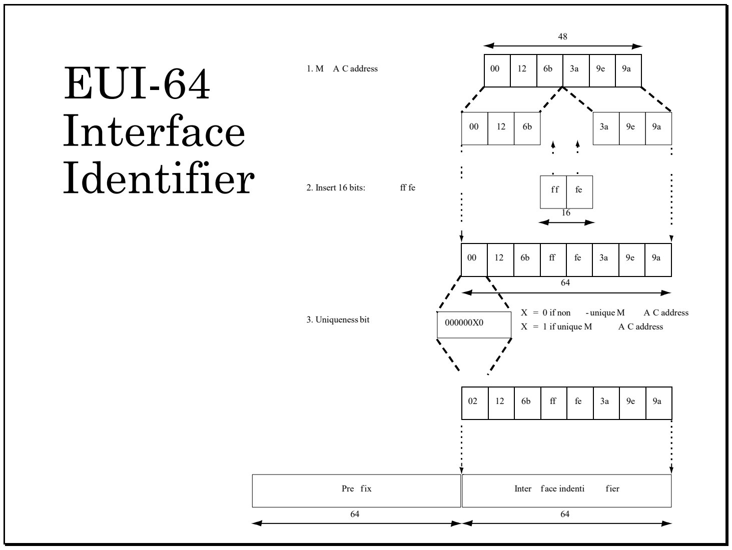


Interface ID

Network ID 64bits	Interface ID 64bits

- Interface ID can be
  - Auto configured from MAC address (EUI-64)
  - Assigned using DHCPv6
  - Manually Configured
  - Auto configured using random number (SEND)
  - Generated Cryptographically
  - Other future means

Slide 48



EUI-64 Interface Identifier

48

1. MAC address

00	12	6b	3a	9e	9a

00	12	6b	3a	9e	9a

2. Insert 16 bits: ff fe

ff	fe

16

00	12	6b	ff	fe	3a	9e	9a

64

3. Uniqueness bit

000000X0

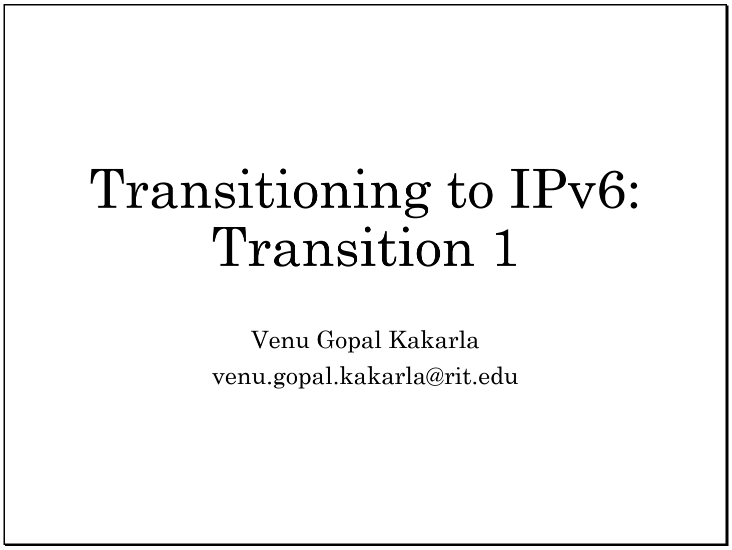
X = 0 if non-unique MAC address
X = 1 if unique MAC address

02	12	6b	ff	fe	3a	9e	9a

Prefix	Interface indentifier
64	64

5.3.3 Lecture 8

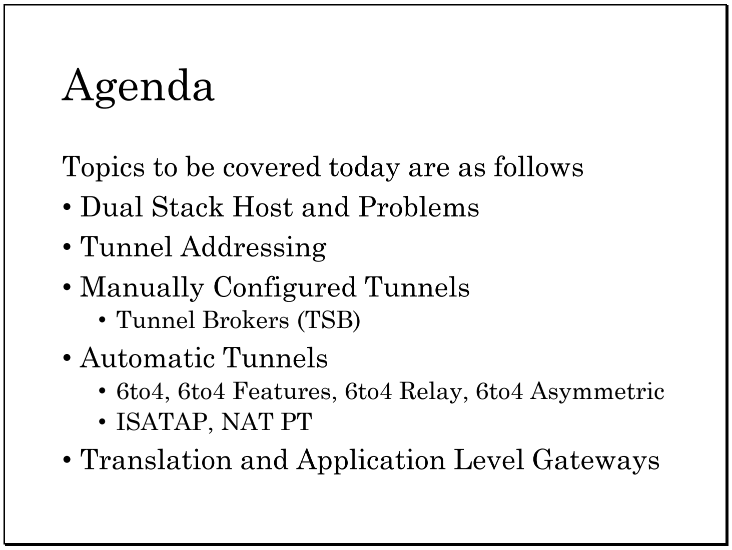
Slide 49



Transitioning to IPv6: Transition 1

Venu Gopal Kakarla
venu.gopal.kakarla@rit.edu

Slide 50

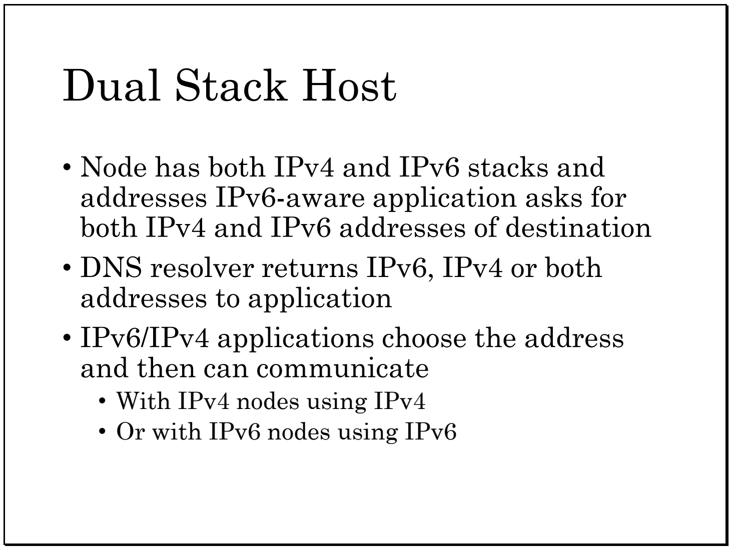


Agenda

Topics to be covered today are as follows

- Dual Stack Host and Problems
- Tunnel Addressing
- Manually Configured Tunnels
  - Tunnel Brokers (TSB)
- Automatic Tunnels
  - 6to4, 6to4 Features, 6to4 Relay, 6to4 Asymmetric
  - ISATAP, NAT PT
- Translation and Application Level Gateways

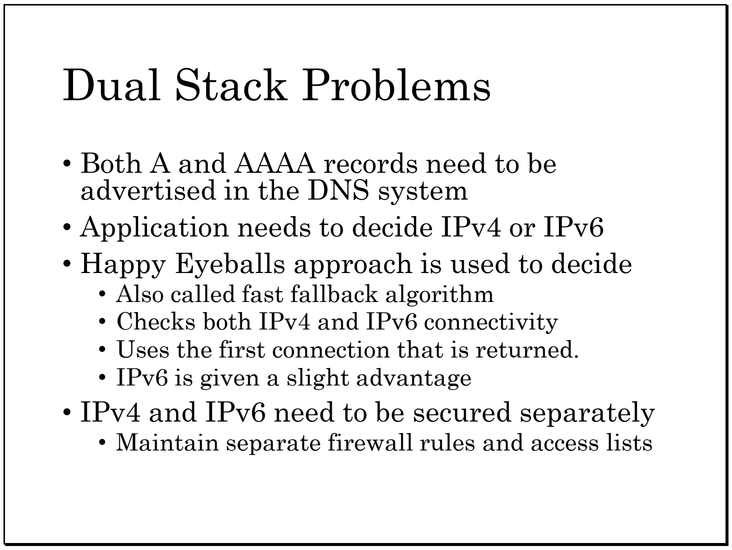
Slide 51



Dual Stack Host

- Node has both IPv4 and IPv6 stacks and addresses IPv6-aware application asks for both IPv4 and IPv6 addresses of destination
- DNS resolver returns IPv6, IPv4 or both addresses to application
- IPv6/IPv4 applications choose the address and then can communicate
  - With IPv4 nodes using IPv4
  - Or with IPv6 nodes using IPv6

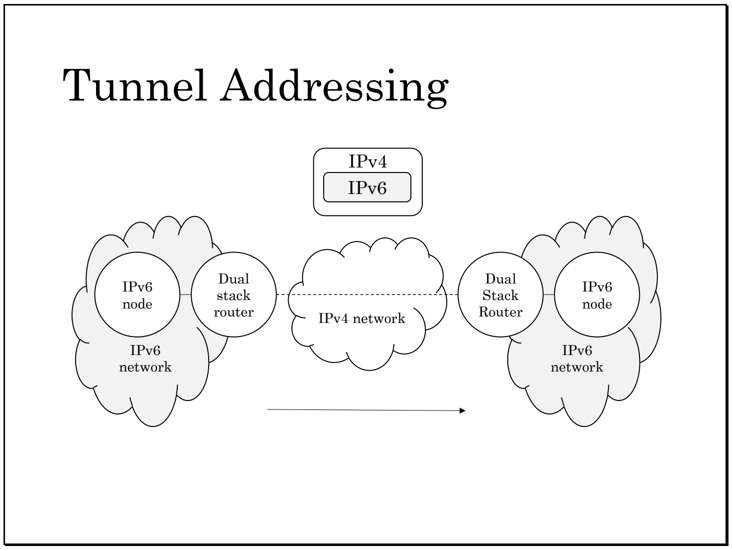
Slide 52



Dual Stack Problems

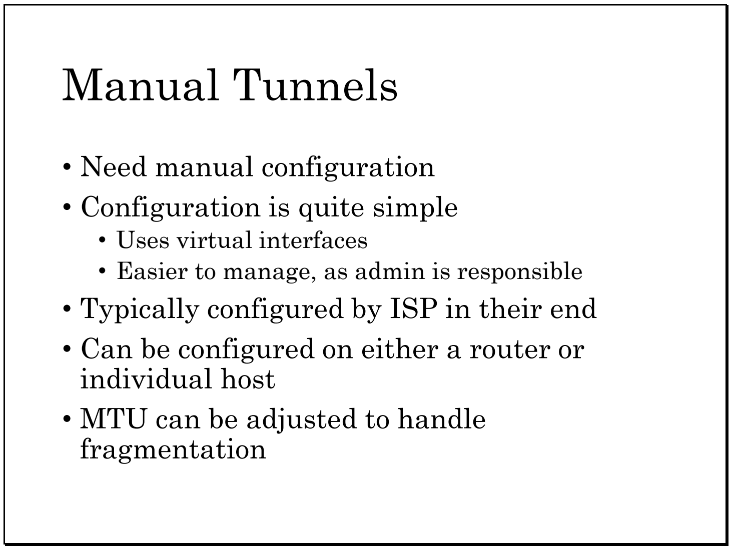
- Both A and AAAA records need to be advertised in the DNS system
- Application needs to decide IPv4 or IPv6
- Happy Eyeballs approach is used to decide
  - Also called fast fallback algorithm
  - Checks both IPv4 and IPv6 connectivity
  - Uses the first connection that is returned.
  - IPv6 is given a slight advantage
- IPv4 and IPv6 need to be secured separately
  - Maintain separate firewall rules and access lists

Slide 53



Tunnel Addressing

Slide 54



Manual Tunnels

- Need manual configuration
- Configuration is quite simple
  - Uses virtual interfaces
  - Easier to manage, as admin is responsible
- Typically configured by ISP in their end
- Can be configured on either a router or individual host
- MTU can be adjusted to handle fragmentation

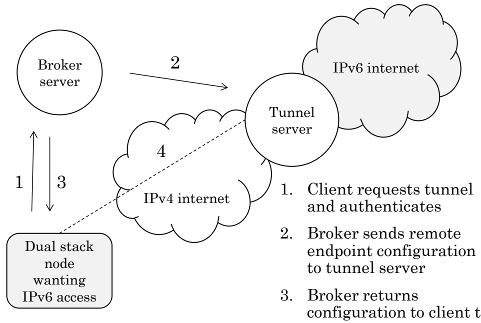
Slide 55

Tunnel Brokers

- Used when the upstream provider or ISP does not support IPv6
- User registers with a broker provider with their IPv4 endpoint address
- A tunnel is requested, provided and configured on the IPv4 gateway
- Possible to traverse over NAT
- Broker can provide an IPv6 prefix if required
- Hexago and Hurricane Electric are brokers

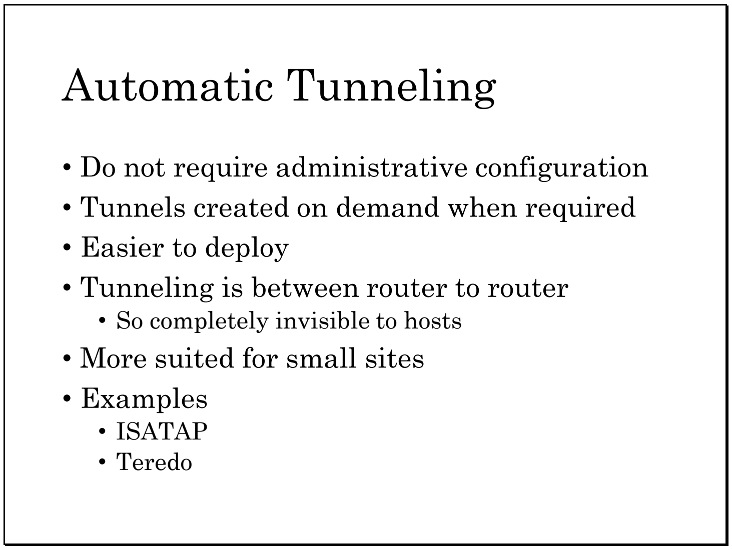
Slide 56

Tunnel Brokers



1. Client requests tunnel and authenticates
2. Broker sends remote endpoint configuration to tunnel server
3. Broker returns configuration to client to create tunnel
4. Tunnel established

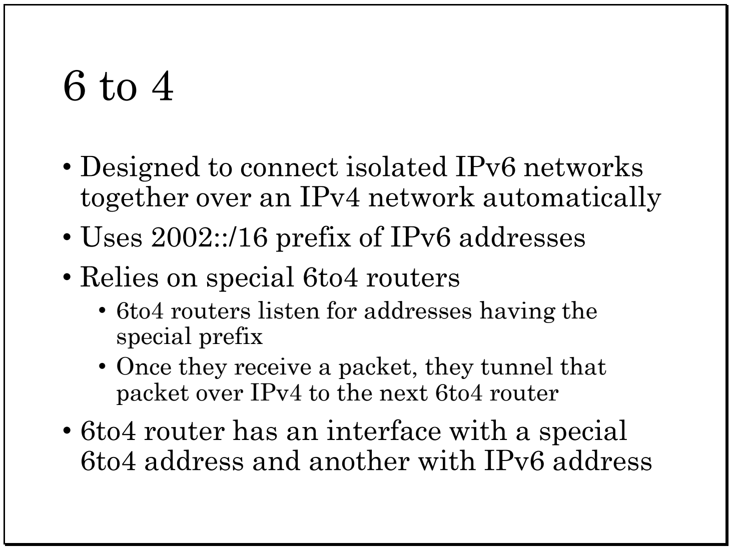
Slide 57



Automatic Tunneling

- Do not require administrative configuration
- Tunnels created on demand when required
- Easier to deploy
- Tunneling is between router to router
  - So completely invisible to hosts
- More suited for small sites
- Examples
  - ISATAP
  - Teredo

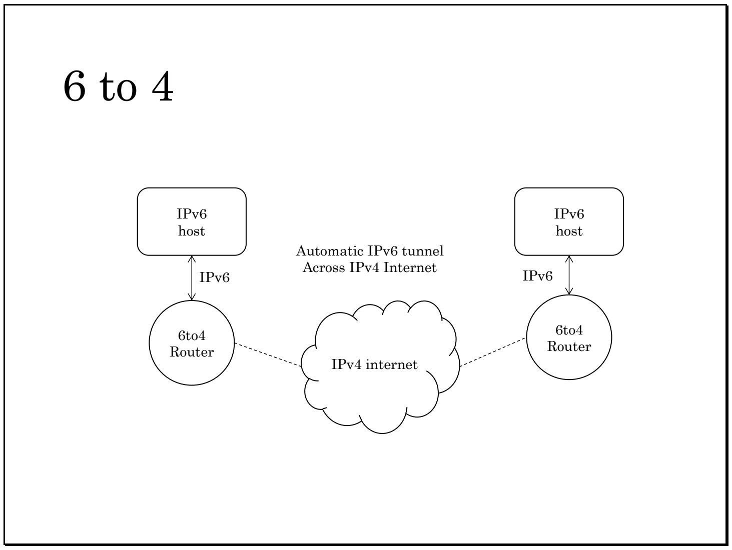
Slide 58



6 to 4

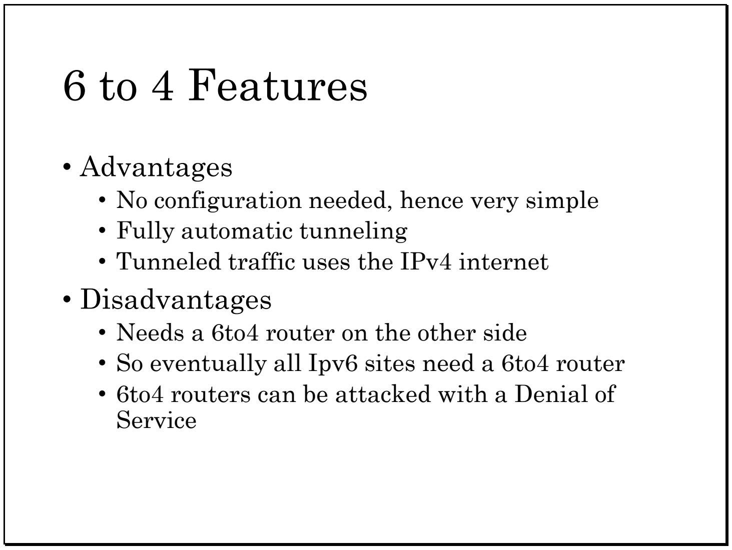
- Designed to connect isolated IPv6 networks together over an IPv4 network automatically
- Uses 2002::/16 prefix of IPv6 addresses
- Relies on special 6to4 routers
  - 6to4 routers listen for addresses having the special prefix
  - Once they receive a packet, they tunnel that packet over IPv4 to the next 6to4 router
- 6to4 router has an interface with a special 6to4 address and another with IPv6 address

Slide 59



6 to 4

Slide 60

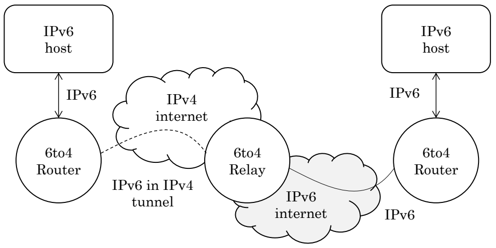


6 to 4 Features

- Advantages
  - No configuration needed, hence very simple
  - Fully automatic tunneling
  - Tunneled traffic uses the IPv4 internet
- Disadvantages
  - Needs a 6to4 router on the other side
  - So eventually all Ipv6 sites need a 6to4 router
  - 6to4 routers can be attacked with a Denial of Service

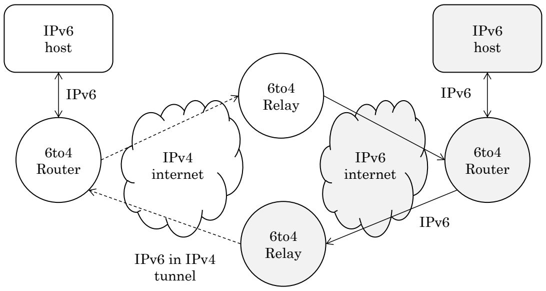
Slide 61

6 to 4 Relay

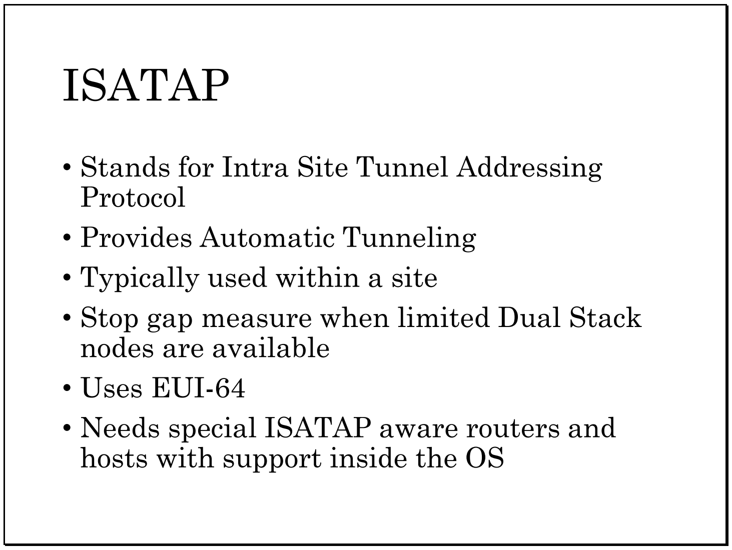


Slide 62

6 to 4 Asymmetric



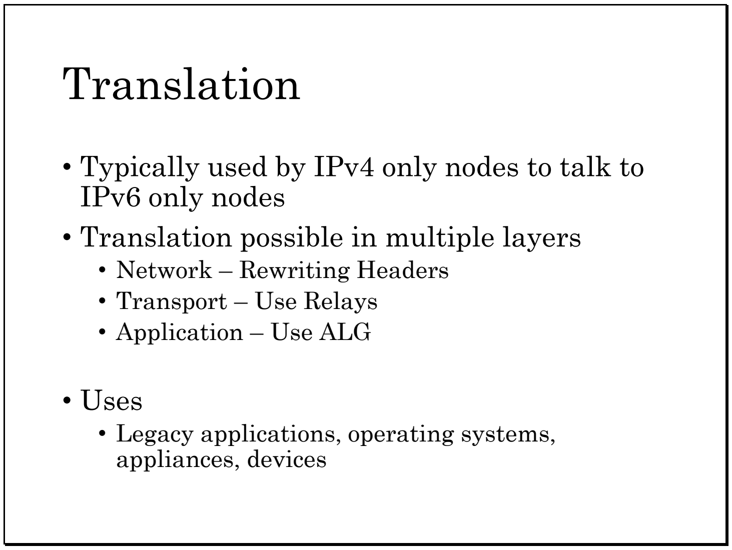
Slide 63



ISATAP

- Stands for Intra Site Tunnel Addressing Protocol
- Provides Automatic Tunneling
- Typically used within a site
- Stop gap measure when limited Dual Stack nodes are available
- Uses EUI-64
- Needs special ISATAP aware routers and hosts with support inside the OS

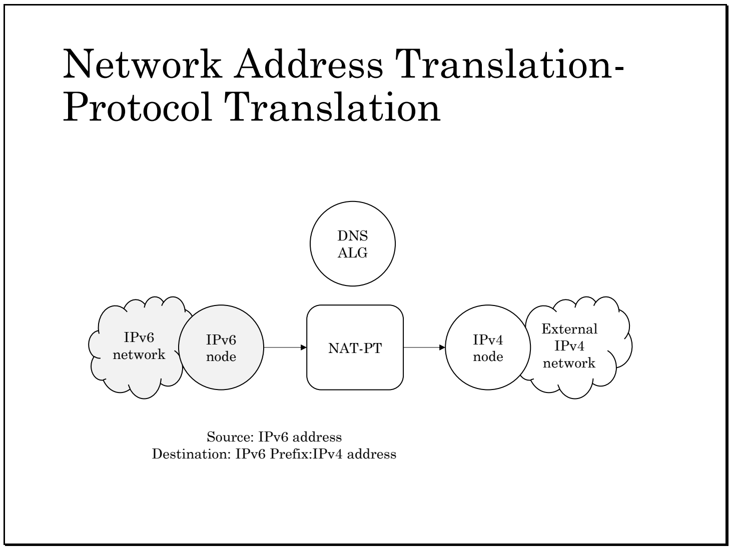
Slide 64



Translation

- Typically used by IPv4 only nodes to talk to IPv6 only nodes
- Translation possible in multiple layers
  - Network – Rewriting Headers
  - Transport – Use Relays
  - Application – Use ALG
- Uses
  - Legacy applications, operating systems, appliances, devices

Slide 65



Network Address Translation-Protocol Translation

DNS
ALG

IPv6
network

IPv6
node

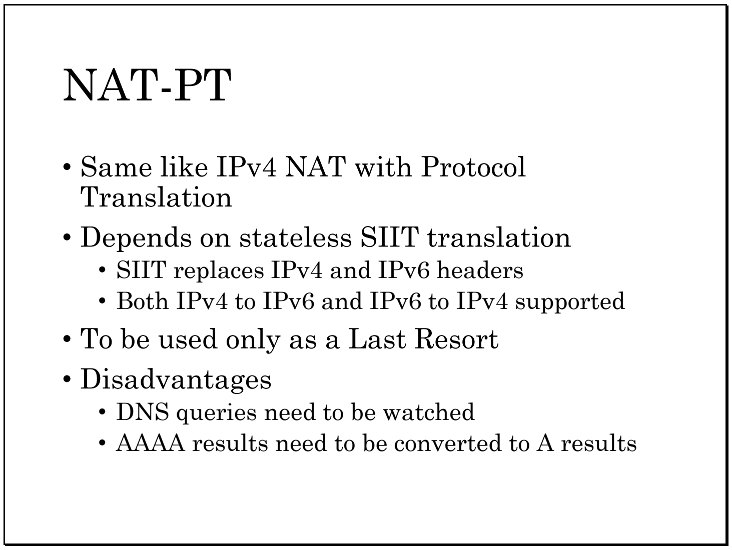
NAT-PT

IPv4
node

External
IPv4
network

Source: IPv6 address
Destination: IPv6 Prefix:IPv4 address

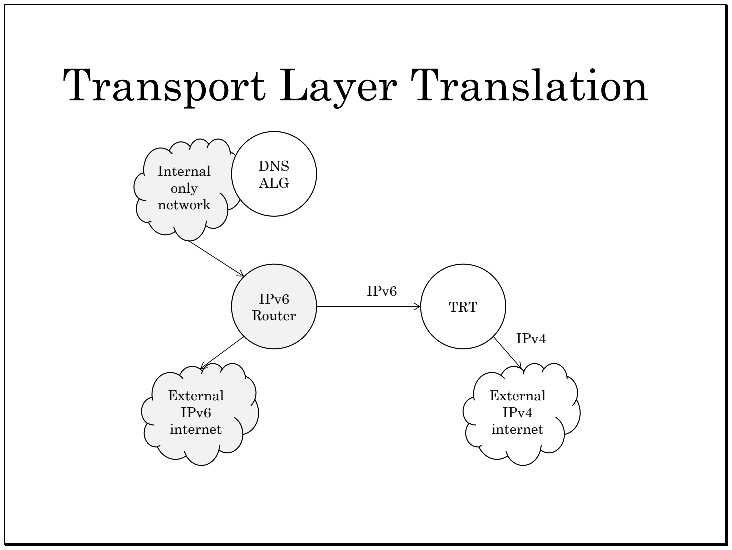
Slide 66



NAT-PT

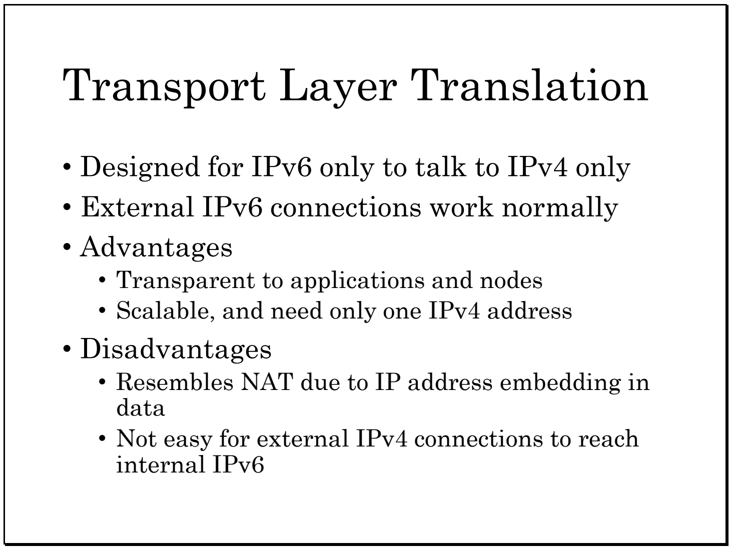
- Same like IPv4 NAT with Protocol Translation
- Depends on stateless SIIT translation
  - SIIT replaces IPv4 and IPv6 headers
  - Both IPv4 to IPv6 and IPv6 to IPv4 supported
- To be used only as a Last Resort
- Disadvantages
  - DNS queries need to be watched
  - AAAA results need to be converted to A results

Slide 67



Transport Layer Translation

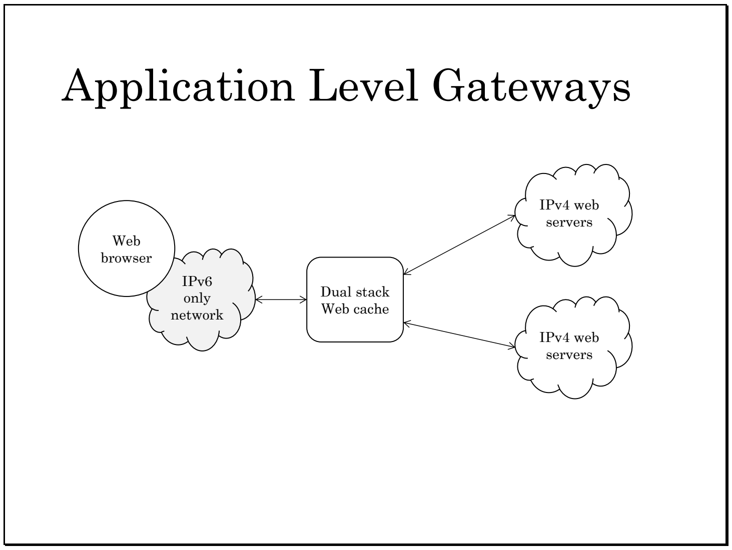
Slide 68



Transport Layer Translation

- Designed for IPv6 only to talk to IPv4 only
- External IPv6 connections work normally
- Advantages
  - Transparent to applications and nodes
  - Scalable, and need only one IPv4 address
- Disadvantages
  - Resembles NAT due to IP address embedding in data
  - Not easy for external IPv4 connections to reach internal IPv6

Slide 69



Application Level Gateways

Web browser

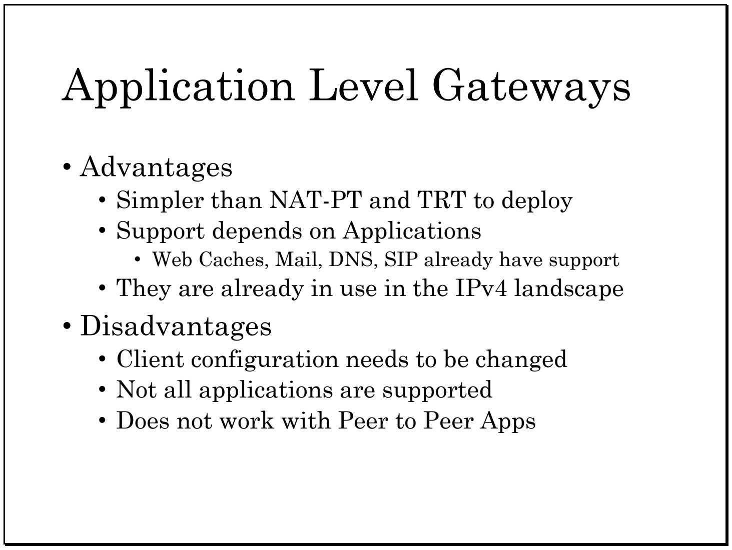
IPv6 only network

Dual stack Web cache

IPv4 web servers

IPv4 web servers

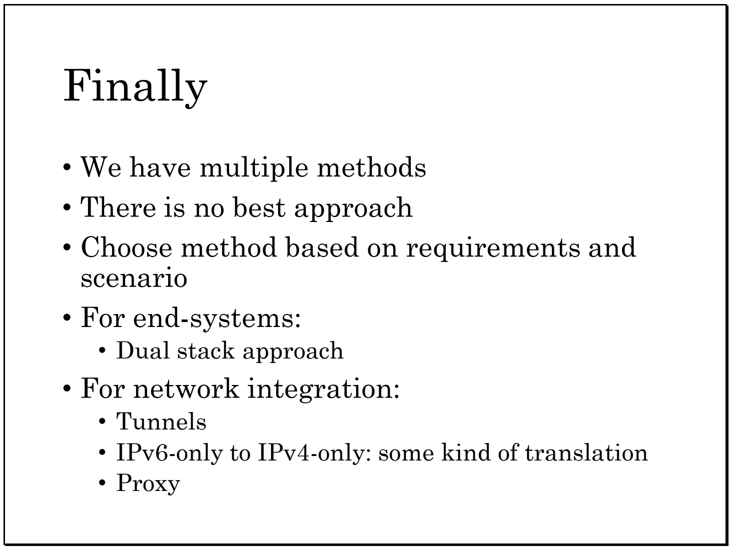
Slide 70



Application Level Gateways

- Advantages
  - Simpler than NAT-PT and TRT to deploy
  - Support depends on Applications
    - Web Caches, Mail, DNS, SIP already have support
  - They are already in use in the IPv4 landscape
- Disadvantages
  - Client configuration needs to be changed
  - Not all applications are supported
  - Does not work with Peer to Peer Apps

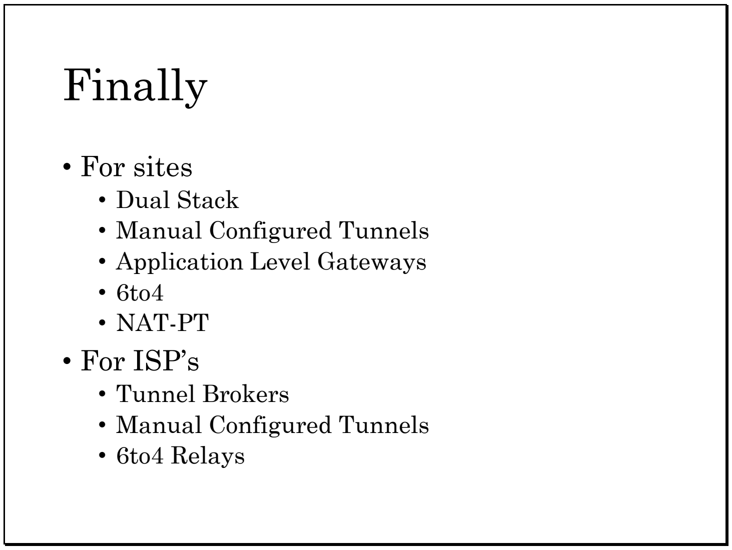
Slide 71



Finally

- We have multiple methods
- There is no best approach
- Choose method based on requirements and scenario
- For end-systems:
  - Dual stack approach
- For network integration:
  - Tunnels
  - IPv6-only to IPv4-only: some kind of translation
  - Proxy

Slide 72



Finally

- For sites
  - Dual Stack
  - Manual Configured Tunnels
  - Application Level Gateways
  - 6to4
  - NAT-PT
- For ISP's
  - Tunnel Brokers
  - Manual Configured Tunnels
  - 6to4 Relays

5.4 Assignments

5.4.1 Writing Assignment 1

4055 xxx – 2016x Transition to IPv6

Writing Assignment 1

Read all instructions carefully before beginning to answer the assignment. You will have until the end of week two at midnight to complete this assignment. Please post your completed assignment to the mycourses dropbox labeled Assignment 1. You may use any resources at your disposal except anyone else in the class. If you have any questions you can please e-mail me.

*Along with this document, you should find a paper in mycourses.rit.edu with the filename "p20-limoncelli.pdf" or "p44-limoncelli.pdf", please read the paper. It should be titled "**Successful Strategies for IPv6 Rollouts. Really.**"*

After you read the paper, write a proposal to the management to the company (real or fictional) you are working at, about why you think it is high time and necessary to start thinking of transitioning to IPv6. Prepare a business case highlighting how you wish it should be done. Remember that you will further develop this business case to a transition plan for Assignment 2.

***

5.5 Mid Term Quiz

4055 xxx Transition to IPv6

2016x Mid Term Quiz

Each question is ¼ points. No of questions is 40. Time available is 50 minutes.

1. Which of the following error reporting messages has been newly introduced in IPv6?
    a. Parameter problem
    b. Packet too big
    c. Destination unreachable
    d. not a, b or c.

2. Which of the following error reporting messages has been removed in IPv6?
    a. Source quench
    b. Packet too big
    c. Destination unreachable
    d. not a, b or c.

3. Which IPv4 protocols are still present in IPv6 with unchanged names?
    a. Internet Group Management Protocol
    b. Address Resolution Protocol
    c. Reverse Address Resolution Protocol
    d. not a, b or c.

4. In IPv6, how does a router inform the source node of a better path?
    a. Router solicitation
    b. Neighbor solicitation
    c. Redirection
    d. not a, b or c.

5. A neighbor solicitation is used by IPv6 host to get what address from what address?
    a. Physical from Internet Protocol
    b. Data link layer from physical
    c. Port from physical
    d. not a, b or c.

6. What IPv6 message contains the router information on the subnet?
    a. Router advertisement
    b. Router information
    c. Router solicitation
    d. not a, b or c.

7. IPv6 gets rid of which of the following protocols?
    a. Internet Control Message Protocol
    b. Internet Protocol
    c. Internet Group Management Protocol
    d. not a, b or c.

8. What does an IPv6 node in a group send to terminate its group membership?
    a. Group membership termination
    b. Group membership query
    c. Group membership report
    d. not a, b or c.

9. If an IPv6 packet has an error in the header or option fields, what kind of error is generated?
    a. Parameter problem
    b. Time exceeded
    c. Destination unreachable
    d. not a, b or c.

10. If an IPv6 packet is not received in specified period of time, what kind of error is generated?
    a. Parameter problem
    b. Time exceeded
    c. Destination unreachable
    d. not a, b or c.

11. IPv6 uses what kind of error message when the hop count field reaches zero and the destination has not been reached?
    a. Parameter problem
    b. Time exceeded
    c. Destination unreachable
    d. not a, b or c.

12. Which of the following IPv6 ICMP error messages have an MTU field to notify the source of packet size?
    a. Parameter problem
    b. Time exceeded
    c. Destination unreachable
    d. not a, b or c.

13. Which for the following IPv6 ICMP error message is sent by the destination to notify the source of a not recognized option?
    a. Parameter problem
    b. Time exceeded
    c. Packet too big
    d. not a, b or c.

14. Where does an error reporting Internet Control Message Protocol packet go to?
    a. Sender
    b. Recipient
    c. Router
    d. not a, b or c.

15. What is used by an IPv6 router to monitor a nodes group membership?
    a. Query
    b. Report
    c. Termination
    d. not a, b or c.

16. IPv6 nodes use echo request and echo reply for what purpose?
    a. Check group memberships
    b. Check inter node communication
    c. Report errors
    d. not a, b or c.

17. What is used by an IPv6 node to join a group?
    a. Group membership termination
    b. Group membership query
    c. Group membership report
    d. not a, b or c.

18. IPv4 has Internet Group Management Protocol, but in IPv6 this is taken care by using what?
    a. Group membership
    b. Router advertisement and solicitation
    c. Echo request and reply
    d. not a, b or c.

19. IPv4 has Address Resolution Protocol, but in IPv6 this is taken care by using what?
    a. Router advertisement and solicitation
    b. Echo request and reply
    c. Neighbor advertisement and solicitation
    d. not a, b or c.

20. What IPv6 message is sent to get information of other routers?
    a. Neighbor advertisement
    b. Neighbor solicitation
    c. Router solicitation
    d. Membership report

21. What IPv6 message is sent to get the MAC address of a node from its IP address?
    a. Neighbor advertisement
    b. Neighbor solicitation
    c. Router solicitation
    d. Membership query

22. IPv6 uses extension headers unlike IPv4. Out of the below list of extension headers which one changes between router hops?
    a. Payload
    b. Fragmentation
    c. Source routing
    d. Authentication

23. IPv6 supports flow routing. Which of the following field is combined with the source address to identify a particular flow?
    a. Hop limit
    b. Next header
    c. Flow label
    d. not a, b or c.

24. During a network congestion, which IPv6 field is used to determine whether a packet needs to be discarded?
    a. Priority
    b. Hop limit
    c. Next header
    d. not a, b or c.

25. Out of the below fields of an IPv6 packet, which is used to limit the packets lifetime?
    a. Priority
    b. Hop limit
    c. Version
    d. not a, b or c.

26. Out of the below fields of an IPv6 packet, which is/are compulsory?
    a. Upper layer data
    b. Base header
    c. Both a and b.
    d. not a, b or c.

27. What kind of IPv6 address is used on a local site with multiple subnets which is not connected to the Internet due to security reasons?
    a. Mapped address
    b. Site local address
    c. Link local address
    d. not a, b or c.

28. What kind of IPv6 address is used on a local network which is not connected to the Internet due to security reasons?
    a. Mapped address
    b. Site local address
    c. Link local address
    d. not a, b or c.

29. What kind of IPv6 address in bit form has 90 zeros, then the 32 bit IPv4 address?
    a. Mapped address
    b. Site local address
    c. Link local address
    d. not a, b or c.

30. What kind of IPv6 address in bit form has eighty zeros, then sixteen ones, then the 32 bit IPv4 address?
    a. Mapped address
    b. Site local address
    c. Link local address
    d. not a, b or c.

31. What kind of IPv6 address is used by a typical node as a unicast address?
    a. Global unicast
    b. Site local address
    c. Link local address
    d. not a, b or c.

32. Out of the below fields of an IPv6 packet, which is used to define its purpose?
    a. Purpose
    b. Type
    c. both a and b.
    d. not a, b or c.

33. Which kind of IPv6 address can be used to reach a group of nodes?
    a. Anycast
    b. Multicast
    c. Unicast
    d. not a, b or c.

34. Which kind of IPv6 address is used to define a group of nodes using addresses that have identical prefixes?
    a. Anycast
    b. Multicast
    c. Unicast
    d. not a, b or c.

35. Which kind of IPv6 address is used to reach a single node?
    a. Anycast
    b. Multicast
    c. Unicast
    d. not a, b or c.

36. How many hexadecimal digits can an IPv6 address have?
    a. Eight
    b. Sixteen
    c. Thirty-two
    d. not a, b or c.

37. IPv6 uses colons ‘:’ to separate octets, what is the maximum no of colons an IPv6 address can have?
    a. Four
    b. Seven
    c. Eight
    d. not a, b or c.

38. To improve human readability of IPv6 addresses, what notation is used?
    a. Hexadecimal numbers and colons
    b. Dotted decimals
    c. both a and b.
    d. not a, b or c.

39. In an IPv6 packet, between where are the options inserted?
    a. Data and base header
    b. Frame header and base header
    c. Extension header and base header
    d. not a, b or c.

40. What is the length of an IPv6 address in bits and octets?
    a. 32 bits and 4 octets
    b. 64 bits and 8 octets
    c. 128 bits and 16 octets
    d. not a, b or c.

5.5.1 Mid Term Quiz Solution Key

1.	b
2.	a
3.	d
4.	c
5.	a
6.	a
7.	c
8.	a
9.	a
10.	b
11.	b
12.	d
13.	a
14.	a
15.	a
16.	b
17.	c
18.	a
19.	c
20.	c
21.	b
22.	c
23.	c
24.	a
25.	b
26.	c
27.	b
28.	c
29.	d
30.	a
31.	a
32.	b
33.	b
34.	a
35.	c
36.	c
37.	b
38.	a
39.	a
40.	c

5.6 Practical Labs

5.6.1 Lab Overview

4055 xxx – 2016x Transition to IPv6
Lab Overview

Introduction

Let us assume that you are a network manager at a big organization. You are really enthusiastic to bring in IPv6 into your corporate network. Currently there are no IPv6 nodes or subnets in your network. So this will be your first attempt to do so.

Your goal is to make sure everything needed to bring in IPv6 to the complex mix that your network is. Before you request an IPv6 prefix from your ISP for connectivity. You would like to experiment in a lab environment. This lab and the following five labs are divided into parts called activities.

Your goal in any IPv6 deployment is to implement a dual stack configuration as much as possible. If implementing a dual stack solution is not possible tunneling is the next best possibility. For the following lab and activity scenarios, we already have IPv4 configured and running. So you will not need to make any IPv4 configurations.

We would like to connect Router1 to the IPv6 internet as our gateway. To simulate an internet connection, we will configure a loopback interface with an IPv6 address from the IPv6 prefix reserved for documentation. So you will have to configure address provided in the diagram on the loopback interface. If we are able to ping this IPv6 address from any other device, we can assume that we are able to access the IPv6 internet.

***

5.6.2 Lab Diagram

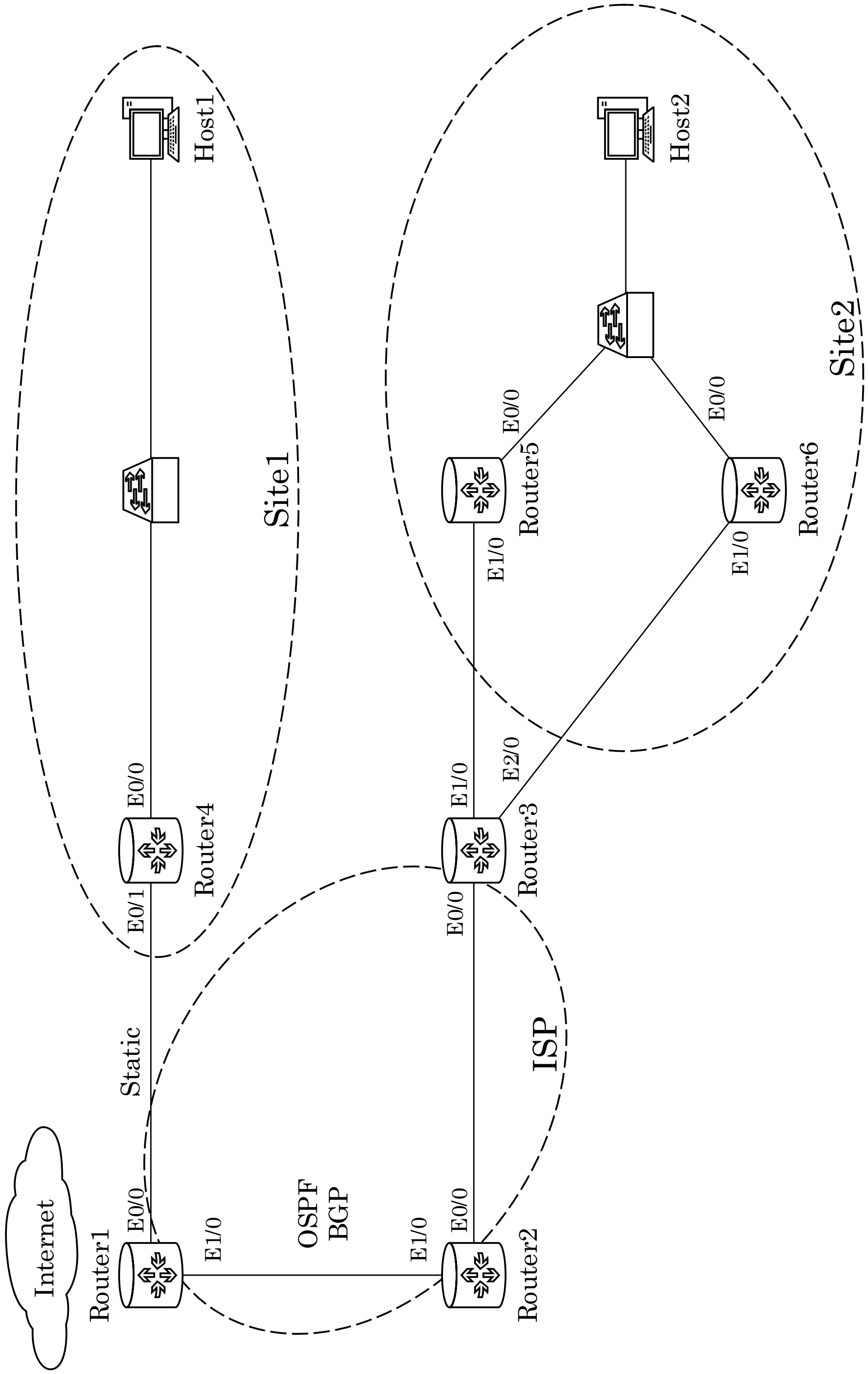


Figure 11: Lab Topology Diagram

5.6.3 Lab 1

4055 xxx – 2016x Transition to IPv6

Lab 1 – IPv6 Addressing and SLAAC

Due Date – End of Week 3

Instructions

- *Read all questions carefully before beginning to answer them.*
- *Submit lab reports on or before the due dates.*
- *Upload your completed reports to the drop box in myCourses. Do not email reports.*
- *If multiple submissions are made, only the most recent one, on or before the due date will be evaluated.*
- *You may use any resources at your disposal except anyone else in the class.*
- *If you have any questions you can either e-mail me or show up at my office in the appointed hours.*
- *Do not forget to save the configuration from all the routers and switches at the end of each lab. You will need to start with those configurations in the next lab.*
- *All reports are to be submitted individually. No group submissions allowed.*

This lab has three parts. Each part should take around 20 minutes.

Activity 1 – IPv6 Unique Local Addressing

Activity 2 – IPv6 Stateless Auto Configuration

Activity 3 – Global Unicast Addressing

Activity 1 – IPv6 Unique Local Addressing

For this lab and the other labs which follow we are using Cisco Routers which support IPv6. Referring to the above topology we will start with the simplest part of the topology. In this case it's Site 1. We can tell from the above topology that Site 1 is running IPv4 and all the routes are configured statically. Verify that this is the case. If this is the case, then we will also use statically configured routes while configuring IPv6. Configure IPv6 between Router4 and Host 1. In this case we will use a private unique local address from the prefix fd00::/8. Refer to the diagram for the required prefix.

Activity 2 – IPv6 Stateless Auto Configuration

IPv6 has a feature called Stateless Auto configuration, where the IPv6 host interface can self-assign itself an IPv6 address based on the address configured on the upstream router connected to the host. In this activity we will test whether this works. So to test this you will need to assign a unique local IPv6 address only on the Router4 interface connected to Host1. Then you can observe if the Host1 automatically gets an IPv6 address from Router4. Use Wireshark on Host1 during this process to capture the traffic between Router4 and Host 1, and demonstrate this. The Host1 uses something called EUI-64, show that the IPv6 address self-configured is derived using EUI-64 method works so you are using that on R4 during the address assignment with /64 mask. Assign this unique local address on R4 using subnetting and then Ping R4's link local and Unique local IPv6 address from H1.

Activity 3 – Global Unicast Addressing

In the previous activity we have tested Site 1 with unique local addressing. And it has been a success. So we have requested our ISP for a Global unicast prefix. And the ISP has provided from their block, to us with a /48 IPv6 address prefix. So in this activity we will use the Global unicast address instead. Unlike IPv4, IPv6 is designed for having multiple addresses on each interface. So we will not need to remove the previously configured Local unicast addresses. We can leave them as it is and configure a new Global unicast address. So we will do this in both Site 1 and Site 2. And unlike last activity where we used EUI-64. This time we will manually configure the address. From now on in the rest of the labs we will only be manually assigning addresses and not using EUI-64. Use the prefix as shown in the diagram, and use the Router number for the last digit of the interface address. For example Router 3 will be <prefix>::3. So ::3 is the interface part of the address. Test tht the multiple address assignment works on the router before assigning Global unicast addresses to Router 5 and Router 6. Use the provided diagram to assign all the required IPv6 addresses.

***

5.6.4 Lab 2

4055 xxx – 2016x Transition to IPv6

Lab 2 – IPv6 Neighbor Discovery

Due Date – End of Week 4

Instructions

- *Read all questions carefully before beginning to answer them.*
- *Submit lab reports on or before the due dates.*
- *Upload your completed reports to the correct drop box in myCourses. Do not email reports.*
- *If multiple submissions are made, only the most recent one, on or before the due date will be evaluated.*
- *You may use any resources at your disposal except anyone else in the class.*
- *If you have any questions you can either e-mail me or show up at my office in the appointed hours.*
- *Do not forget to save the configuration from all the routers and switches at the end of each lab. You will need to start with those configurations in the next lab.*
- *All reports are to be submitted individually. No group submissions allowed.*

This lab has three parts. Each part should take around 20 minutes.

Activity 1 – Router Solicitation and Router Advertisement

Activity 2 – Duplicate Address Detection, Neighbor Solicitation and Neighbor Advertisement.

Activity 3 – Renumbering

Activity 1 – Router Solicitation and Router Advertisement

In lab 1 you have worked with the auto configuration aspects of IPv6. In this lab we will work with concepts of Neighbor discovery. We will specifically be looking at Router solicitation and Router Advertisement messages for this activity. To observe these messages, you will need to modify the router advertisements interval. So, change it from 200 seconds to 30 seconds on Router 4. Then turn on the IPv6 Neighbor discovery debug on Router 4. At the same time turn the Auto configuration off and on in the Ethernet interface on Host 1. Now you will see the router advertisement and router solicitation messages. Explain with screenshots.

Activity 2 – Duplicate Address Detection, Neighbor Solicitation and Neighbor Advertisement.

In the last activity we worked with Router solicitation and router advertisement messages. In this activity we will work on Neighbor solicitation and Neighbor advertisement messages, which are a part of the Duplicate Address Detection mechanism in IPv6. So we now enable the IPv6 Neighbor discovery debug on Router 5 and Router 6. Then we will need to assign new addresses on the Ethernet interfaces of Router 5 and Router 6. Refer to the diagram for the required addresses. Observe the messages after enabling the debug mode. Try to grasp the Duplicate Address Detection process. This process automatically takes place the moment an IPv6 address assignment happens. After this remove the previously assigned IPv6 addresses on Router 5 and Router 6. Then ping Router 6 from router 5, and observe the Neighbor solicitation and Neighbor advertisement between routers. Is the process different between routers compared to between nodes?

Activity 3 – Renumbering

In activity 3, we will attempt to examine the new feature of IPv6 which allows renumbering. To do this we will change the IPv6 address on Router 5 and Router 6 form what was assigned in the previous activity, to a new address shown in the diagram. So let's configure the new IPv6 address on the two routers interfaces. Then let's reconfigure the Router Advertisement interval to forty seconds. To ensure the old addresses expire, we will need to configure a lifetime of 40 on both routers 5 and routers 6. With a screen shot show that the old address on Host 2 is marked as deprecated. Now we will want the addresses to disappear completely. We will reconfigure the lifetime to 0 on both routers. Provide a screenshot to show that the old address is gone from the Ethernet interfaces on the connected hosts.

***

5.6.5 Lab 3

4055 xxx – 2016x Transition to IPv6

Lab 3 – IPv6 Static Routing and OSPFv3

Due Date – End of Week 5

Instructions

- *Read all questions carefully before beginning to answer them.*
- *Submit lab reports on or before the due dates.*
- *Upload your completed reports to the drop box in myCourses. Do not email reports.*
- *If multiple submissions are made, only the most recent submission, on or before the due date will be evaluated.*
- *You may use any resources at your disposal except anyone else in the class.*
- *If you have any questions you can either e-mail me or show up at my office in the appointed hours.*
- *Do not forget to save the configuration from all the routers and switches at the end of each lab. You will need to start with those configurations in the next lab.*
- *All reports are to be submitted individually. No group submissions allowed.*

This lab has two parts. Each part should take around 30 minutes.

Activity 1 – Static Routing

Activity 2 – Open Shortest Path First v3

Activity 1 – Static Routing

Starting with this lab, we will be working with Routing protocols. Before we work with dynamic protocols. We will first configure static routing. Refer to the diagram to see that our ISP has provided us a static IPv6 Global unicast address prefix. So we will use this prefix in our activity. Configure the provided prefix on Router 4. Later we will configure a static route for that prefix towards Router 4. We are assuming our ISP here has connectivity to the IPv6 internet. Thus, Site 1 should be able to access the IPv6 internet. Now configure another Global unicast address on Router 1. And then configure a static route on Router 1 such that the Global unicast address of Router 4 is the net hop. As per the original instructions provided in Lab 1 we will assume we can assume that we can reach the IPv6 internet if we can ping a specific address from Host 1. So ping it and check if you get a response. Do not forget to provide screenshots of your responses.

Activity 2 – Open Shortest Path First v3

In this activity we are going to experiment with the Open Shortest Path Fist dynamic routing protocol. So prior to this activity, we have requested our ISP for IPv6 connectivity between our Site 1 and Site 2. And our ISP has informed us that they are in the process of converting their core network to support Dual Stack. And that they have been running OSPF version 2. To support IPv6 they have planned to upgrade to OSPF version 3. And they have provided us the details needed to enable OSPF between Site 1 and Site 2.

Refer to the diagram to see the prefix provided by the ISP and assign the corresponding IPv6 addresses <prefix>::2/127 on Router 2 and <prefix>::3/127 on Router 3. Use the same prefix to configure the IPv6 address <prefix>::0/127 on Router 1 and <prefix>::1/127 on Router 2. Then configure two OSPF areas. Between Router 1 and router 2, we will use Area 0. And Between Router 2 and Router 3 we will use Area 1. You will also need to make sure the Loopback address of Routers 1 and Routers 2 are set to Area 0. Next we will use Ping to test our OSPF configuration by pinging Router 1 to Router 3. We will Ping the configured loopback interfaces to verify its reachable. Finally use this scenario to show the differences between the OSPF version 2 and version 3 packets, and provide a comparison of the differences in your report.

***

6 Bibliography

[1] M. Blanchet. Challenges and Opportunities in Deploying IPv6 Applications. North American IPv6 Task Force (http://www.nav6tf.org). 2005.

[2] K. S. Evans. Planning for Internet Protocol Version 6 (IPv6). Office of Management and Budget. 2005.

[3] V. Kundra. Transition to IPv6. Office of Management and Budget. 2010.

[4] Planning Guide/Roadmap Toward IPv6 Adoption within the U.S. Government. Federal IPv6 Working Group. 2012.

[5] S. Deering, R. Hinden. Internet Protocol, Version 6 Specification. RFC 2460. 1998.

[6] R. Hinden, S. Deering. IP Version 6 Addressing Architecture. RFC 4291. 2006.

[7] J. Abley, P. Savola, G. Neville-Neil. Deprecation of Type 0 Routing Headers in IPv6. RFC 5095. 2007.

[8] B. Carpenter, S. Jiang. Transmission and Processing of IPv6 Extension Headers. RFC 7045. 2013.

[9] S. Krishnan, J. Woodyatt, E. Kline, J. Hoagland, M. Bhatia. A Uniform Format for IPv6 Extension Headers. RFC 6564. 2012.

[10] S. Krishnan. Handling of Overlapping IPv6 Fragments. RFC 5722. 2009.

[11] S. Thomson, T. Narten, T. Jinmei. IPv6 Stateless Address Autoconfiguration. RFC 4862. 2007.

[12] T. Narten, E. Nordmark, W. Simpson, H. Soliman. Neighbor Discovery for IP version 6 (IPv6). RFC 4861. 2007.

[13] N. Moore. Optimistic Duplicate Address Detection (DAD) for IPv6. RFC 4429. 2006.

[14] J. Postel. NCP/TCP Transition Plan. RFC 801. 1981.

[15] M. Blanchet. Migrating to IPv6: A Practical Guide to Implementing IPv6 in Mobile and Fixed Networks (2nd ed.). Wiley. 2016.

[16] K. Sill. IPv6 Mandates. Wiley. 2008.

[17] C. Popoviciu, E. Levy-abegnoli, P. Grossetete. Deploying IPv6 Networks. Cisco Press. 2011.

[18] S. Hagen, V. Cerf. Ipv6 Essentials (3nd ed.). O'Reilly. 2014.

[19] S. Hagen. Planning for IPv6 (1st ed.). O'Reilly. 2011.

[20] N. R. Murphy and D. Malone. IPv6 Network Administration. O'Reilly. 2005.

[21] D. York. Migrating Applications to IPv6. O'Reilly. 2005.

[22] C. Liu. DNS and BIND on IPv6. O'Reilly. 2011.

[23] M. Dooley, T. Rooney. IPv6 Deployment and Management. Wiley-IEEE Press. 2013.

[24] S. McFarland, M. Sambi, N. Sharma, S. Hooda. IPv6 for enterprise networks. Cisco Press. 2011.

[25] S. Hogg, E. Vyncke. IPv6 Security. Cisco Press. 2009.

[26] P. Loshin. IPv6 Theory, Protocol and Practice (2nd ed.). Morgan Kaufmann. 2004.

[27] Q. Li, T. Jinmei, K. Shima, IPv6 Core Protocols Implementation. Morgan Kaufmann, 2007.

[28] Q. Li, T. Jinmei, K. Shima, IPv6 Advanced Protocols Implementation. Morgan Kaufmann, 2010.

[29] J. J. Amoss, D. Minoli. Handbook of IPv4 to IPv6 Transition: Methodologies for Institutional and Corporate Networks. CRC Press. 2007.

[30] T. A. Limoncelli, V. G. Cerf. 2011. Successful strategies for IPv6 rollouts. Really. Communications of the ACM, Volume 54. April 2011. Pages 44-48.

[31] K. Begnum, C. Border, N. Sijm. An investigation of learning outcomes for MSc programs in Network and System Administration. USENIX Journal of Education in System Administration. Volume 1, Number 1. 2015

[32] S. Frankel, R. Graveman, J. Pearce, M. Rooks. Guidelines for the secure deployment of IPv6. NIST Special Publication. 2010.