IPv6 Transition

Nathan Balon
CIS 537
Advanced Networks

Introduction

IPng or what is otherwise known as IPv6 was created to be the replacement for IPv4. The main reason that IPv6 was created was because of the lack of the of address space that is provided by IPv4. The transition from IPv4 to IPv6 has been a slow process. Since the introduction of IPv6 approximately ten years ago its implementation to date has been limited. What is needed are some methods to ease the transition from IPv4 to IPv6. This paper will explore some of the possible mechanism that can be used in the migration.

As with other technologies it is important that IPv6 provides backward compatibility. In the computer industry almost all products that are produced are backwards compatible. For instance, software that runs on todays computers should also run on future generations of computers, if this wasn't so people would refuse to upgrade their computers. So it is important that IPv6 and IPv4 are able to coexist.

Possible Transfer Solutions

A number of possibilities exist concerning how to efficiently transfer to IPv6. The authors of the book Computer Networks: a Top-Down Approach Featuring the Internet propose three solutions to the problem of transition to IPv6. A number of RFCs have also been written concerning ways to transfer and other possible short term solutions.

"Flag Date"

One solution is to declare a certain time when all of the Internet's infrastructure must changed over to IPv6. This solution is unacceptable since it will be impossible to implement since there are millions of host connected to the Internet. Also, device that do not support IPv6 will still need to work. For example, some embedded devices may not be able to update the version of IP they are using. The users of these device would still want them to work after the transition date. A solution such as this was proposed for the television industry to convert to digital broadcasts by 2008 and this still probably won't be accomplished. A "flag date" when all device must must use IPv6 would never work on this large of scale. This approach might work on a smaller scale such as a company that had an intranet that wasn't connected to the Internet, but then an organization such as this would probably have no incentive to switch.

Dual-Stack

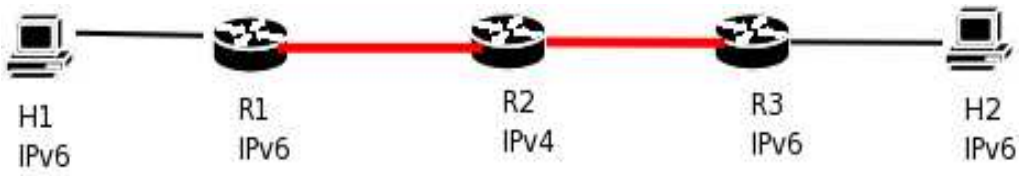
A second possibility is to use a dual stack so that both IPv4 and IPv6 are supported. With this proposal a node would run the software for both versions of the protocol. If a node is communicating with another node that is also running IPv6 then they will send IPv6 datagrams to each other. If one of the nodes only supports Ipv4, then IPv4 datagrams are exchanged. There are some of problems with this solution. To begin, the nodes must determine which version of IP each is using. So there must be some sort of lookup service to determine which version a node is using. James Kruse proposes that DNS could be used to lookup the version of IP that is used by a node. One problem is not every host may have a registered domain name. So using this solution would require that

addition applications are used to lookup the type of IP address. Another problem with this solution is if it is determined that the two nodes that want to communicate are both using IPv6, the routers along there way may not support IPv6. The advantage of this approach is it would be easy to implement. If operating system vendors and router manufacturers incorporated both versions of IP in there new products eventually the dominance of IPv4 would be shifted to IPv6 as equipment was replaced. On the other hand, there is probably little incentive for a vendor to include both versions until there is market pressure on them to do so.

Tunneling

A third possibility is to use tunneling. With this approach an IPv6 datagram is placed inside a IPv4 datagram. This is similar to the tunneling that can be used with multicasting when a router doesn't support a mutlitcast protocol. In the case of tunneling , it is used when an IPv6 packet must pass through a router that doesn't support IPv6. When a router on the path to the destination is discovered that doesn't support IPv6 a tunnel is created. A new IPv4 packet is created and the IPv6 packet is inserted into it. At the other side of the tunnel the IPv6 packet is then removed and forwarded along its way.

The diagram below shows how tunneling would work. If host H1 is sending a packet to host H2 using Ipv6 then it would send an IPv6 packet. When router R1 receives the packet and is going to forward the packet to router R2 a tunnel is created since R2 is not able to process a IPv6 packet. The IPv6 packet is then inserted into an Ipv4 packet and sent to R2 which then forwards this to R3. When R3 receive the packet, R3 can then remove the IPv6 packet from the IPv4 packet and then forward it the H2. The red line in the diagram shows where a tunnel would be created.



One drawback of this is the amount of space that is used by the headers. IP and TCP have both at least 20 byte headers, an IPv6 header is 40 bytes and the link layer header will vary based on the technology that is used. So it is very likely that a packet that a packet that is tunneled will contain close to 100 bytes in header information. If only a small messages sent say 100 bytes of payload, then half of the bandwidth used would be for transmitting header information.

Another, drawback to using tunnels is that the routers instead of creating routing tables and forwarding packets they would also be responsible for creating tunnels which would could degrade the performance of the routers.

RFC 2529

Another possibility is described in RFC 2529, "Transmission of IPv6 over IPv4 Domains without explicit tunnels". The authors of RFC 2529 propose a method to allow to hosts running IPv6 to communicate when the routers between them do not support IPv6. In this scenario IPv6 packets are place within a IPv4 packet. The protocol field is then set to 41 to indicate that a Ipv6 packet is contained within it. How this mechanism work is it maps virtual link layer address to an IPv6 address and uses multicasting. The author states, "its uses IPv4 multicast as a "virtual Ethernet"."

Conclusion

These are some of the proposed solutions to migrating to IPv6. No one solution appears to be best for all applications. Many experts feel that it will still be a number of years until IPv6 is widely deployed.

References

Carpenter, C. and Jung, C. "RFC 2529: Transmission of IPv6 over IPv4 Domains without Explicit Tunnels" 1999.

Hinden, Robert. "IP Next Generation Overview". 1995.

Kruse, James. Computer Networking a Top-Down Approach Featuring the Internet. 2nd ed. Addison-Wesley: Boston, MA. 2003.