Technical Paper

IPv6 Transition Test Challenges

Introduction

While the first RFC for IPv6 has been available for more than six years, IPv6 (Internet Protocol Version 6) has never really reached the phase where the telecommunications industry considered it more than an experimental protocol. This is because the problem, exhaustion of IPv4 addresses, had always been fixed with techniques like Dynamic Host Configuration Protocol (DHCP) and Network Address Translation (NAT). However, this situation is changing due to technical, geographical, and political drivers.

Technically, the third generation of mobile telecommunications is adopting IPv6 as its protocol for multimedia communications. Geographically, because the IPv4 address space has been allocated mainly to North America, Asian and European countries are in need of more addresses. However, because IPv6 is capable of coding addresses up to 128 bits, it will be able to allocate enough addresses among all countries. It is becoming customary to say that IPv6, with an address field of 128 bits compared to 32 bits for IPv4, could assign an address to every grain of sand on Earth.

Agilent Technologies

Politically, some countries realized that IPv6 could be a factor in boosting new applications and helping the economy. Japan, South Korea, and the European community have stated directives for service providers to use IPv6 in new applications and networks.

The purpose of this paper is to review the different test challenges that Network Equipment Manufacturers and Internet Service Providers will encounter when migrating to IPv6.

After reviewing the status of the standardization for transition from IPv4 to IPv6, we have divided this paper into three parts:

- an explanation of tunneling and the associated test challenges.
- an example of a routing protocol working on both protocol stacks and its associated functional test.
- a stress testing scenario of IPv6 islands connected through an IPv4 core network.

IETF and IPv6

Most of the "standardization" regarding IPv6 has been done by the IETF, and the main principles of IPv6 (addressing, security, etc.) have been available for several years. For example, the latest RFC for the IPv6 protocol itself has been available since December 1998, and a previous RFC was finished in December 1995. Most of the issues encountered today are those associated with the transition from IPv4 to IPv6 and mobile IPv6.

Many working groups are involved in IPv6: ipngwg for IP next generation, ngtrans for transition to IPv6, mobileip for IP Mobile, idr-Inter-Domain Routing for Exterior Gateway Routing Protocol. These working groups total more than 180 drafts involving IPv6.

Transition Mechanisms

The topic largely debated among the IETF is the transition from IPv4 to IPv6 and how both versions will coexist for a long time, if not forever. One example is having an IPv6 application running on your home computer reaching an IPv6 server to a remote network through the IPv4 core network. Types of transition mechanisms include:

- Dual-Stack - where both IPv4 and IPv6 protocol stacks coexist in the same terminal or network equipment.
- Tunneling - which is mainly used to tunnel traffic between two IPv6 hosts through an IPv4 network, or vice-versa.
- Translation - which enables an IPv4 host to talk to an IPv6 host.

This paper describes three test scenarios: a functional test scenario for configured and automatic tunneling, a functional test scenario for the routing protocol BGP-4+ based on draft-ietf-ngtrans-bgp-tunnel, and a stress test scenario based on the same draft. The device being tested will be referred to as the System Under Test (SUT).

Tunneling

This section will first discuss the Tunneling concept and then review testing issues for the most common tunnels.

In the early phases of IPv6 development, and Internet service provider will allow access to isolated IPv6 users and communicate with IPv6 islands through an IPv4 network. The method used in this case will be tunneling (ref. Figure 1). Two IPv6 islands are connected to an IPv4 core network. Router A and Router B are Dual-Stack routers. Let us review what happens to the IPv6 packet as it moves across the IPv4 network destined for a host in an IPv6 network:

(a) A packet with an IPv6 address arrives at Router A.

(b) Router A identifies its forwarding table and finds that it can route this IPv6 address by sending it to Router B. It finds that Router B's IPv4 address is 10.1.1.1.

(c) The IPv6 packet is encapsulated in an IPv4 packet and sent into the IPv4 cloud by Router A.

(d) The IPv4 cloud routes the packet using the 10.1.1.1 destination address as if it were a normal IPv4 packet; the packet finally reaches Router B.

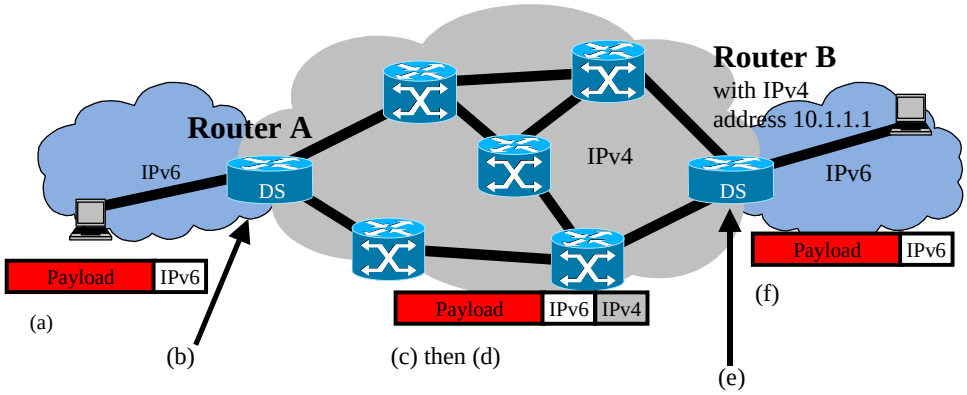

Figure 1: Tunneling Mechanisms

(e) Router B looks at the packet and realizes that it is carrying an IPv6 packet inside. It strips out the IPv4 header and uses the IPv6 header to identify its forwarding table. It finds that it can reach the IPv6 address destination in the IPv6 network to which it is connected.

(f) Router B sends the packet to its destination.

Several drafts and RFCs have already proposed tunneling mechanisms. Here we have focused on two types of tunnels: configured and automatic tunnels based on RFC 2185 "Routing Aspects of IPv6 Transition" and RFC 2529 "Transition Mechanism for IPv6 Host and Routers".

These drafts define two types of addresses: a native IPv6 address represented as 1080:0:FF:0:8:800:200C:417A and an IPv4 compatible IPv6 address where an embedded v4 address is encoded in the first 32 bits of the IPv6 address represented as v6[v4] or 0:0:0:0:0:0:13.1.68.3 or ::13.1.68.3.

Tunneling: How Does It Work?

When a packet with an IPv6 address arrives at Router A, a tunnel is built from Router A to Router B. The tunnel end-point address is determined by the destination address from the tunneled packet (ref. Figure 2).

If the upcoming packet uses an IPv6 native address, then Router A adds an IPv4 header. The IPv4 address will be a predefined value. Thus we say that Router A establishes a CONFIGURED tunnel.

If the upcoming packet uses an IPv4 compatible IPv6 address represented as v6[v4], then Router A extracts the IPv4 address from v6[v4] and uses this address to build the IPv4 header. In this case, we say that Router A establishes an AUTOMATIC tunnel.

Because the IPv4 packet has a global IPv4 destination address, it is routed to Router B. Router B strips out the IPv4 header and forwards the IPv6 packet to the v6 network.

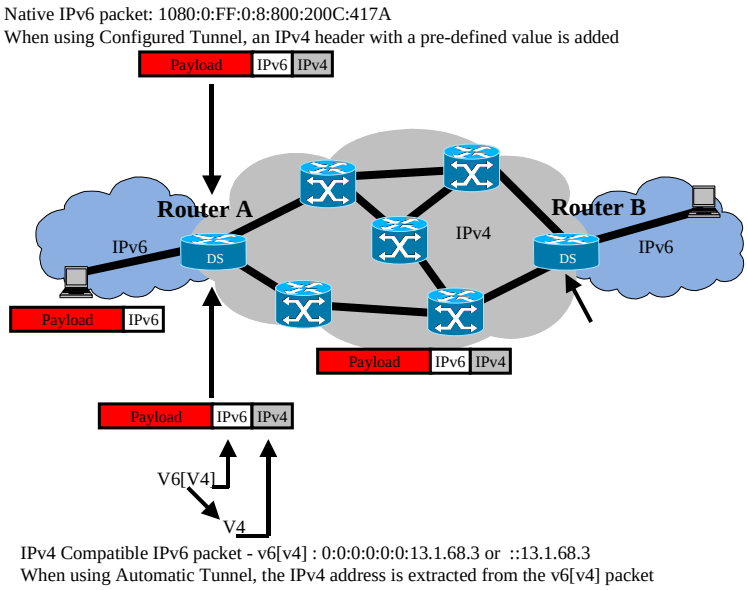

Figure 2: Configured and Automatic Tunneling

Test Scenario: Automatic and Configured Tunneling

The following section describes how test equipment can effectively verify the setup and functionality of Automatic and Configured Tunneling.

The objective is to check the functional behavior of a SUT supporting the configured and automatic tunneling mechanisms. In order to do this, test equipment needs to send IPv6 and IPv4 / IPv6 traffic to capture packets and to emulate an IGPv4 routing protocol.

The following steps should be performed for testing the SUT's automatic tunneling capability (ref. Figure 3):

- Create a routing topology and update the SUT using an IGPv4 (the gray network in Figure 3).
- Generate an IPv6 packet from Port 1A. The destination address is an IPv4 compatible v6 address represented as v6[v4]. We make sure that the v4 address is part of the defined topology.
- Capture the IPv4 packet containing the IPv6 packet on Port 2.
- Verify that the SUT was able to extract the v4 address from the v6[v4] and then build an IPv6 packet encapsulated in an IPv4 packet. The destination address is the v4 part of the v6[v4].

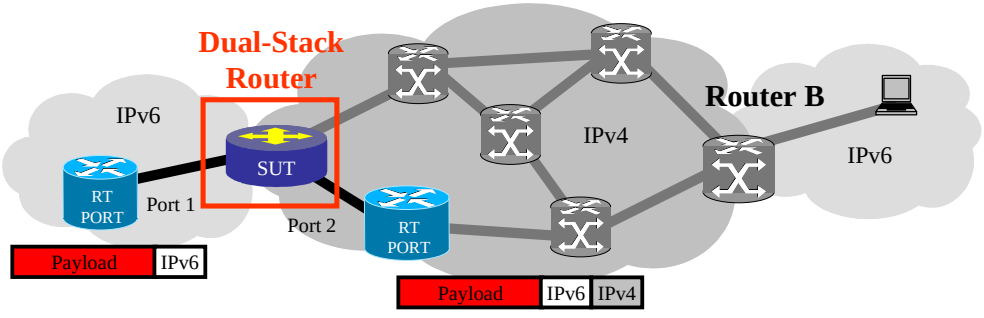

Figure 3: Functional Test Scenario: Configured and Automatic Tunneling

For configured tunnel:

- The IPv4 address of the Dual-Stack Router B is manually configured in the SUT.
- An IPv6 packet is sent from Port 1.
- IPv4 packets containing IPv6 traffic are captured.
- We verify that the SUT correctly builds the IPv4 header with the pre-defined IPv4 address.

Encapsulation and decapsulation of IPv6 is one aspect of testing the transition between the IPv4 and IPv6 protocol stacks. Another aspect is compatibility and the operation of routing protocols on both protocol stacks. This topic will be the main discussion in the second part of this paper.

Functional Routing Test Scenario: Dual-Stack and Tunneling Method based on draft-ietf-ngtrans-bgp-tunnel

This example will illustrate the use of BGP carrying IPv6 reachability information on both IPv4 and IPv6 stacks based on draft-ietf-ngtrans-bgp-tunnel.

As the discussion moves to the topic of Exterior Routing Protocol for IPv6, it is important to mention that BGP-4+ refers to Multi-Protocol BGP (MP-BGP) which carries IPv6 reachability information.

As represented in Figure 4, Dual-Stack MP-BGP-speaker Edge Routers connect IPv6 islands through an IPv4 network. BGP-4+ is used to notify Router B how to reach v6 prefixes like the 20000321 2001:0660:: as specified in Figure 4. BGP-4+ is running on an IPv6 protocol stack. Router B advertises IPv6 addresses to Router A by using BGP-4+ running on IPv4, then Router A updates its routing table.

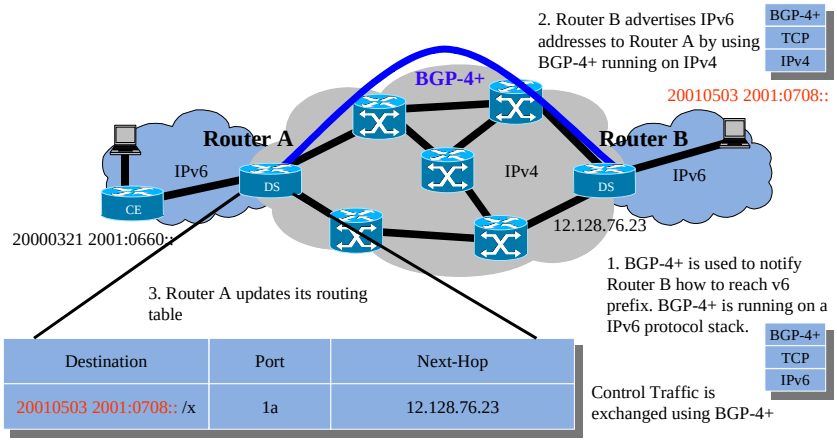

Figure 4: Use of BGP-4+

Functional Routing Test Scenario

The objective is to test the correct implementation of MP-BGP (BGP-4+) carrying IPv6 reachability information over the IPv4 and IPv6 protocol stack in the Dual-Stack of the Edge Router.

The following steps should be followed (Ref. Figure 5):

(a) Simulate a BGP-4+ session between the SUT and Router B.

(b) Advertise a route pool to the SUT from Router B.

(c) The SUT updates its routing table and advertises the route pool to the IPv6 network on Port 1.

(d) Verify that on Port 1, the SUT correctly advertises the route pool on the IPv6 protocol stack.

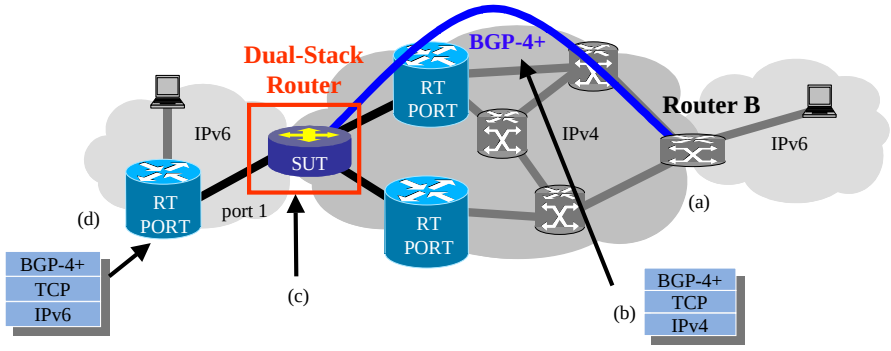

Figure 5: Functional Test Scenario: use of BGP-4+ on both protocol stacks

Stress Test Scenario: Dual-Stack and Tunneling Method based on draft-ietf-ngtrans-bgp-tunnel

Thus far, the discussions in this paper have centered on functional testing. We will reuse the same draft as the previous example to illustrate a stress test scenario.

Here is the complete picture of how this draft works (ref. Figure 6). The IPv6 traffic is forwarded in the IPv4 network using MPLS. The steps are:

(a) A tunnel is built from Router B to Router A by advertising the IPv4 address: 12.128.76.23.

(b) Router A associates 12.128.76.23 with the green label. By label we mean MPLS label which is a four-octet label containing the label value.

(c) An IPv6 packet is sent.

(d) Router A determines that the packet must be sent to Router B. Instead of encapsulating the IPv6 packet in an IPv4 packet, the green label is added.

(e) Router C exchanges the green label with the purple label.

(f) Router D exchanges the purple label with the blue label.

(g) Router B strips and forwards the IPv6 packet to its destination.

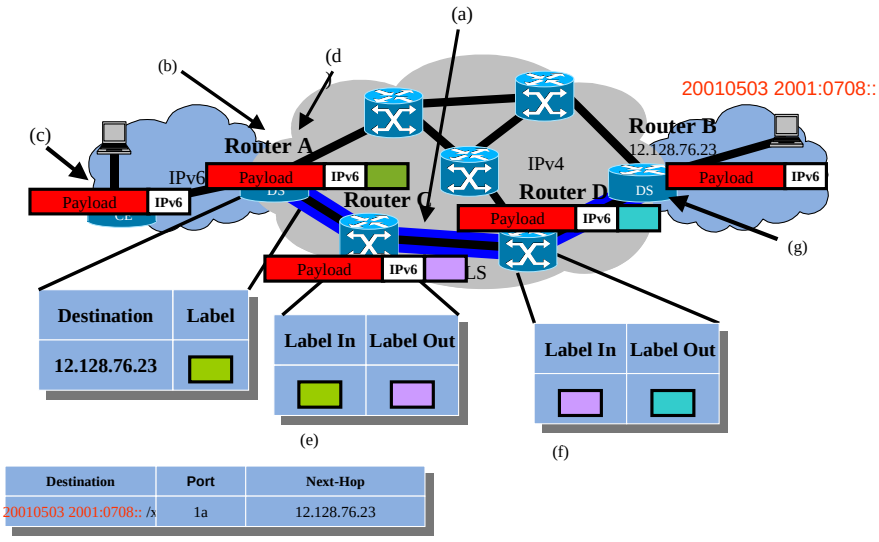

Figure 6: draft-ietf-ngtrans-bgp-tunnel

- In the test lab represented in Figure 7, the first step will be to simulate a tunnel using MPLS between the SUT and Router B.
- The SUT associates the address of Router B with a label (the green label in Figure 7).
- IPv6 packets are sent at wire-rate.
- Real-time QoS measurements like latency, packet loss, and packet throughput are performed.

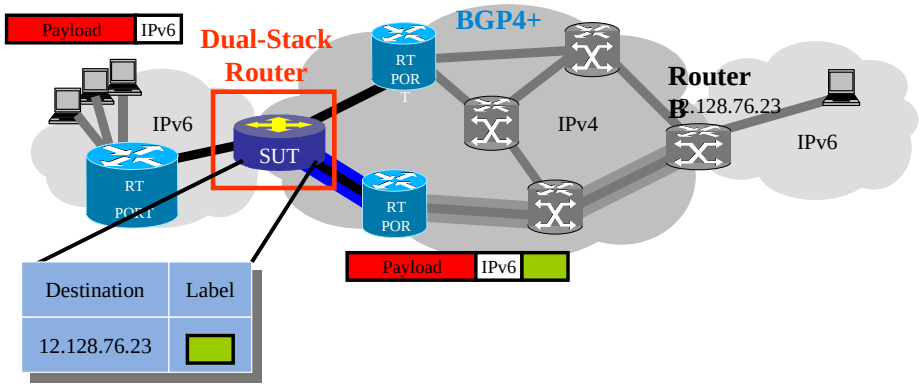

Figure 7: Stress Test Scenario based on draft-ietf-ngtrans-bgp-tunnel

Conclusion

Agilent Technologies is a member of the IPv6 Forum and is therefore committed to providing expertise in dealing with the IPv6 test challenges of router manufacturer and Internet Service Providers. We are also dedicated to providing test equipment that will accompany routers through their life cycle, from functional testing to complex transition and overall performance test scenarios.

For more information on these test tools, please visit www.agilent.com / comms / RouterTester

References

- Connecting IPv6 Domains across IPv4 Clouds with BGP (draft-ietf-ngtrans-bgp-tunnel-02.txt; June 2001)
- Routing Aspects of IPv6 Transition (RFC 2185; September 1997)
- Transition Mechanism for IPv6 Host and Routers (RFC 2893; August 2000)

January 25, 2002
5988-5540EN

Agilent Technologies