The Internet addressing capabilities and the migration of IPv6 are important for cloud computing, as we

shall see in this section. The Internet Protocol, Version 4 (IPv4), provides an addressing capability of

232, or approximately 4.3 billion addresses, a number that proved to be insufficient. Indeed, the Internet

Assigned Numbers Authority (IANA) assigned the last batch of five address blocks to the Regional

Internet Registries in February 2011, officially depleting the global pool of completely fresh blocks of

addresses. Each of the address blocks represents approximately 16.7 million possible addresses.

The Internet Protocol, Version 6 (IPv6), provides an addressing capability of 2128, or 3.4   1038

addresses. There are other major differences between IPv4 and IPv6:

• Multicasting. IPv6 does not implement traditional IP broadcast, (i.e., the transmission of a packet

to all hosts on the attached link using a special broadcast address) and, therefore, does not define

broadcast addresses. IPv6 supports new multicast solutions, including embedding rendezvous point

addresses in an IPv6 multicast group address, which simplifies the deployment of interdomain

solutions.

• Stateless address auto configuration (SLAAC). IPv6 hosts can configure themselves automatically

when they are connected to a routed IPv6 network using the Internet Control Message Protocol

version 6 (ICMPv6) router discovery messages. When first connected to a network, a host sends a

link-local router solicitation multicast request for its configuration parameters; if configured suitably,

routers respond to such a request with a router advertisement packet that contains network-layer

configuration parameters.

• Mandatory support for network security. Internet Network Security (IPsec) is an integral part of the

base protocol suite in IPv6; it is optional for IPv4. IPsec is a protocol suite operating at the IP layer.

Each IP packet is authenticated and encrypted. Other security protocols operate at the upper layers

of the TCP/IP suite (e.g., the Secure Sockets Layer (SSL), the Transport Layer Security (TLS), and

the Secure Shell (SSH)). IPsec uses several protocols: (1) Authentication Headers (AH) – supports

connectionless integrity, data origin authentication for IP datagrams, and protection against replay

attacks; (2) Encapsulating Security Payloads (ESP) – supports confidentiality, data-origin authentication,

connectionless integrity, an anti-replay service, and limited traffic-flow confidentiality; and

(3) Security Associations (SA) – provides the parameters necessary to operate the AH and/or ESP

operations.

Unfortunately, migration to IPv6 is a very challenging and costly proposition. A simple analogy

allows us to explain the difficulties related to migration to IPv6. The telephone numbers inNorth America

consist of 10 decimal digits; this scheme supports up to 10 billion phones, but, in practice, we have fewer

available numbers than that. Indeed, some phone numbers are wasted because we use area codes based

on geographic proximity and, on the other hand, not all available numbers in a given area are allocated.

To overcome the limited number of phone numbers in this scheme, large organizations use private

phone extensions of typically three to five digits. Thus, a single public phone number can translate

to 1,000 phones for an organization using a three-digit extension. Analogously, Network Address

Translation (NAT) allows a single public IP address to support hundreds or even thousands of private

IP addresses. In the past NAT did not work well with applications such as VoIP and virtual private networking (VPN). Nowadays Skype and STUN VoIP applications work well with NAT and NAT-T,

and SSLVPN supports VPN NAT.

If the telephone companies decide to promote a new system based on 40-decimal-digit phone numbers,

we will need new telephones; at the same time we will need new phone books that are much

thicker because each phone number is 40 characters instead of 10. Each individual will need a new

personal address book, and virtually all the communication and switching equipment and software will

need to be updated. Similarly, the IPv6 migration involves upgrading all applications, hosts, routers, and

DNS infrastructure. Also, moving to IPv6 requires backward compatibility, because any organization

migrating to IPv6 should maintain a complete IPv4 infrastructure.

In 2009 a group from Google investigated the adoption of IPv6 [89] and concluded that “… the

IPv6 deployment is small but growing steadily, and that adoption is still heavily influenced by a small

number of large deployments. While we see IPv6 adoption in research and education networks, IPv6

deployment is, with one notable exception, largely absent from consumer access networks.”