HEISON CHAK

VoIP and IPv6

Heison Chak is a system and network administrator at SOMA Networks. He focuses on network management and performance analysis of data and voice networks. Heison has been an active member of the Asterisk community since 2003.

heison@chak.ca

IP ADDRESS SHORTAGE, TRAFFIC PRIoritization, end-to-end security, and NAT issues are problems with VoIP that can be addressed by IPv6. This article will discuss some of these issues. It will also outline some of the hurdles in migrating to the next version of the Internet Protocol.

IPv4 Exhaustion

At a consumption of 5–8% per year, it is predicted that the remaining 25% of available IPv4 addresses could be exhausted as early as July 15, 2011. With Japan having made IPv6 adoption a mandate since 2001, Asia sits in a leading spot in the push for the new protocol. IPv4 addresses are 32-bit, normally written as four decimal numbers.

```
Example: 192.168.1.10
```

IPv6 addresses are 128-bit, represented as eight fields, separated by colons, of up to four hexadecimal digits each.

```
Example: 3ffe:ffff:101::230:6eff:fe04:d9ff
```

The symbol :: is a special syntax used to represent multiple 16-bit groups of continuous zeroes. The large number of addresses (2^{128}) allows a hierarchical allocation of addresses that may make routing and renumbering simpler. Separate address spaces exist for ISPs and for hosts, which is inefficient in use of address space bits but efficient for operational needs.

Third-generation (3G) wireless both in Europe and North America had once been viewed as a big push toward IPv6, since the protocol can facilitate more IP addresses, end-to-end QoS/security, and mobility between 3G and other networks. However, with the slow adoption of 3G networks, ISPs found that they didn't need as many IP addresses as they had once thought. With the exhaustion date closing in, these perceptions may change rapidly in the next few years. The United States government is mandating its agencies' networks to interface with new IPv6 backbones by June 2008, and China plans to showcase its largest IPv6 network at the 2008 Olympics. Commonly known as 6CDO, the IPv6 EU-Chinese Digital Olympics project will demonstrate IPv6 applications in many facets at the Summer Games. This will certainly be an exciting year for IPv6.

End-to-End Communications

With IPv4, NAT is often used to enable multiple hosts on a private network to access the Internet using a single public IP address. Many find this Layer 3 technique convenient and use it widely. Some higher-layer protocols, such as SIP, send network-layer address information inside application payloads. For example, embedded private IP addresses can often be seen in SDP (Session Description Protocol) embedded as a SIP payload. NAT operates only in Layer 3, so the embedded private IP address will not be translated, because it is in Layer 4. Because the private address often become unreachable from the receiving end, the effect could be SIP calls that fail to establish, failed touch-tone inputs, one-way audio, or simply no audio.

Instead of fixing the problem from the root, that is, by not sending embedded Layer 3 addresses in a non–Layer 3 protocol, workarounds are invented to change the embedded private IP address to match the public Internet address on the router. On the endpoint equipment, it may support a static entry of the border router's external IP address or one of the automatic discovery protocols: STUN (Simple Traversal of UDP through NATs), ICE (Interactive Connectivity Establishment), or Traversal Using Relay NAT (TURN). On the router, a SIP-capable ALG (Application Layer Gateway) may be running to examine each SIP/SDP packet and alter the embedded IP.

Although these techniques are widely used to assist devices behind a NAT firewall or router with their packet routing, such altering is actually one of the biggest offenders in data integrity. If you want to implement end-to-end security with IPsec, using one of these techniques will be a challenge, because an ALG on the router altering packets will cause IPsec Authentication Signatures to fail.

With IPv6, end-to-end communication permits nodes to communicate without NAT in a secure fashion. In addition, quality of service can be maintained between IPv4 and IPv6, since there is no difference in QoS for the two protocol versions. There is only a slightly different header definition in IPv6.

Migrating VoIP to IPv6

Unlike the migration from NCP to IPv4 in the early 1980s, IPv4 and IPv6 will interoperate during and after the transition. With the new API (RFC3493, RFC3542) having been available since Linux 2.4, FreeBSD 4.x, Mac OS X 10.2, Windows XP, and Solaris 8, OSes can leave the details of supporting the two versions to the API. Many network vendors (e.g., Cisco, Juniper, Checkpoint) and open source applications (e.g., Apache, Sendmail, Postfix, OpenSSH) also feature IPv6 support.

In order for VoIP to take advantage of IPv6, any VoIP equipment that may be connecting to a network should be made IPv6-aware. Application servers, gateways, and communication end nodes must incorporate the new API. They need to be able to handle both IPv4 and IPv6 traffic, understand how to parse IPv6 URLs, and be able to store the lengthier IPv6 addresses. It's best if they are version-independent whenever possible, parsing addresses and URLs to support both the IPv4 and the IPv6 address syntax required for networking, logging, and SIP URL parsing.

```
IPv6 address syntax:
0::C0A8:010A                         # IPv4-compatible address (192.168.1.10)
1:2:3:4:5:6:7:8/16                   # denotes the address to be /16
0:0:0:0:0:0:0:1                      # loopback
::1                                  # loopback (shorthand)
http://[1:2:3:4:5:6:7:8]:80/index.html  # port 80 URL
```

Open Source VoIP and IPv6

In March 2007, Viagenie in Canada conducted a VoIP call to Consulintel in Spain using CounterPath eyeBeam (previously known as X-Lite) through Asterisk with the IPv6 patch. “Asterisk-IPv6 shows the power of VoIPv6 by avoiding all issues regarding NAT traversal when using IPv4. The presence of NAT for VoIPv4 results in users issues such as non-connecting calls, one-way audio, non-working DTMF. Asterisk-IPv6 solves all these issues and also brings, together with IPv6, true IP mobility, security and autoconfiguration of VoIPv6 phones,” states Marc Blanchet, president of Viagenie. Despite efforts made by Viagenie to make Asterisk IPv6-aware when using the SIP protocol, however, the current version of Asterisk is still not IPv6-ready. SER (SIP Express Router) does seem to be further ahead when it comes to IPv6 support.