



Applications that Benefit from IPv6

Lawrence E. Hughes

Chairman and CTO
InfoWeapons, Inc.



Relevant Characteristics of IPv6

- Larger address space, flat address space restored
- Integrated support for Multicast, support mandatory in all routers
- Better QoS possible with flow label field, improving streaming
- Better support for IPsec in packet headers, no NAT!
- Mobile IPv6 – fascinating opportunities for the future:
 - Mobile Ad Hoc networks (MANET)
 - Networks in Motion (NEMO)
 - Combination of these (MANEMO)

Streaming digitized analog information over the Internet

- Once information is in digital form, it is possible to transmit it in real time over the Internet Protocol (IP).
- This typically is done with a recent transport layer protocol (comparable to TCP and UDP), called RTP (Real-Time Transport Protocol - RFC 3550). RTP can layer over IPv4 or IPv6, but there are significant advantages of layering it over IPv6.
- RTP is used in many streaming applications, including IPTV, Internet Radio and VoIP.

Applications of streaming audio and video information

- *VoIP* (Voice over IP) simulates voice telephony, with varying levels of quality (typically comparable to GSM or landline phone calls). 64 Kbps is adequate for high quality audio. With a good codec, as little as 8 Kbps can provide acceptable voice quality.
- *Internet Radio* (Audio over IP) simulates normal broadcast radio, and there are thousands of stations available today with varying levels of quality (up to Compact Disc level), depending on bandwidth and codec sophistication. Such stations can be received by anyone with a PC including a sound card, an Internet connection and streaming audio software. 64 Kbps to 256 Kbps is adequate for quality stereo music, such as FM radio or CD.
- *IPTV* (TeleVision over IP) simulates a television channel, again with varying levels of quality, up to HDTV. 2 to 4 Mbps is required for SD (Standard Definition) video, while full HD requires 10Mbps or more (depending on format). Smaller images (e.g. in a small window on a PC, or on a phone) or poorer quality images (below broadcast SD) are possible with significantly lower bandwidth requirements.



Typical IPTV system

- The “transmitter” (server) may accept already digitized video information, or encode and compress analog video information (using a video codec). This digital data is then formatted and packetized over RTP, and transmitted over IPv4 or IPv6. If IPv6 is used, multicast is easy to employ, supporting vastly more customers with the same bandwidth.
- The “receiver” (client) accepts the packetized information, decodes it using the same codec used to encode it, and displays it, typically in a window on the PC screen. Optionally, the output could be formatted into a standard TV baseband analog signal (e.g. NTSC) and output to a conventional TV.
- A “set top box” is a headless (no keyboard or display) computer that does all the above steps from the digitized input to a baseband (or even RF modulated) analog TV signal, which is then connected to a TV receiver or monitor. Such a device typically includes a smartcard based authentication and decryption mechanism (to prevent unauthorized use), and some kind of controls (often via remote) to allow selection of one of a number of *channels*. With IPv4, most set top boxes do not use the general Internet, but a “walled garden” IP based network over Coax or Fiber To The Home (FTTH). Other services, such as VoIP and even high speed general Internet access can be bundled along with digitized television service.

A typical commercial (IPv4) IPTV service

- Direct PC TV (www.directv-pctv.com) provides some 9000 channels of video from all over the world, for \$39.95 a month, for display on your PC screen.
- A typical image is 400x226 pixels, requiring about 400 Kbps. The Windows Media Audio 9.1 codec (32 Kbps) is used for the audio track, and VC-1 codec is used for the video track.
- Picture quality (with no QoS) is only fair even with 512 Kbps Internet service, the picture is small (perhaps 2 x 3 inches) and buffering is noticeable. There may be pauses during transmission if the buffer “runs dry” due to lost or damaged packets, or interference from other bandwidth usage on your channel (e.g. file downloads). If this is zoomed to full screen (e.g. 1024 x 768 or even larger), picture quality is very poor.
- Significant bandwidth is required due to all connections being unicast.



Unicast versus Multicast

- Simple IPTV services provide a basic two-party client server connection for each viewer. This is called **unicast**. It uses massive bandwidth, but provides maximum flexibility, by allowing the client to view content any time (“on demand”), and even interact with it (pause, rewind, fast forward, etc). Highly targeted ads could in theory be inserted down to the granularity of individual viewers.
- A more advanced IPTV service can allow any number of clients (potentially millions) to be viewing a single transmitted stream of packets. This is called **multicast**. This is far more efficient of bandwidth and provides for greatest number of viewers for a given amount of bandwidth, but provides the least flexibility for the viewer. In theory, a well designed client could provide time shifting with such a service, in a manner similar to Tivo. This is much more like the traditional television broadcast model than the unicast mechanism above.
- With IPv4, multicast can typically be done only in a LAN or a vendor controlled “walled garden” network. Few general routers on the Internet support multicast.
- With IPv6, all compliant routers must support multicast, so you can count on it being present even over long complicated paths.



IPv6 Support for Multicast

- In IPv6, Multicast Listener Discovery is part of ICMPv6 (which also includes ping and other mechanisms), and is defined in RFC 3810.
- If you wish to subscribe to a given multicast address, MLD is used to inform intervening routers that packets from that multicast address are to pass onwards towards you. As long as at least one subscriber exists downstream from a given router interface, packets will be allowed to pass to that interface. When the last subscriber has “signed off” on that address, packets from it will no longer pass the router.
- This mechanism will work over any IPv6 network, no matter how extensive, so long as all intervening routers are IPv6 compliant.



QoS

- QoS (or Quality of Service) refers to being able to manage bandwidth on a per protocol (or per address, or per “flow”) basis.
- This allows you to guarantee that a given service (such as VoIP or IPTV) can allocate and maintain a minimum amount of bandwidth, regardless of what else is taking place in the channel, assuming enough total aggregate bandwidth is available in the channel. This is key to maintaining quality service. Without QoS, other network activity can cause serious interference with (or even total loss of signal) on critical services, as all bandwidth is on a first-come-first-served basis. A P2P application can easily eat all available bandwidth on a given link if QoS is not deployed.



QoS and IPv6

- It is possible to implement QoS in IPv4, in a vendor controlled “walled garden” network, where they can insure that all routers support it, and have configured it.
- On the general IPv4 Internet, QoS is difficult or impossible to deploy, as QoS is not mandatory, and few routers support it. Typically, bandwidth management is based on service (actually port) and/or user (source or destination address). IPv4 does include a few bits in the packet header for *diffserv* (service differentiation), which allows simple flow tagging.
- In IPv6, all compliant routers must support QoS. IPv6 packet headers also include a new 20-bit field called “flow label” (RFC 3697), which allows *any* flow of data to be tagged, for even better QoS. Due to the size of this field, over 1 million (2^{20}) distinct flows could be differentiated.



Encryption and Key Management

- With any service which someone wishes to provide for a price, there are those who would cheat and obtain it for free (e.g. stolen cable TV service).
- The only foolproof way to prevent this is *encryption* (the reversible scrambling of information based on a *key*).
- IPsec is a simple and efficient way to encrypt data on an IP connection. It uses fast symmetric key cryptography (e.g. using the Advanced Encryption Standard or AES algorithm). This uses the same key to encrypt and decrypt data, hence the sender and receiver must both possess this key. This can be particularly difficult in a multicast environment.
- The Internet Key Exchange standard (IKEv1 is defined in RFC2409, and IKEv2 is defined in RFC 4307) provides a way to securely and efficiently distribute symmetric session keys among communicating participants. It requires a new kind of digital certificate (IPsec certificate), which binds *IP addresses* (IPv4 or IPv6) to a public key (as opposed to a name and e-mail address in client certs, or a Fully Qualified Domain Name like www.hp.com in server certs).



IPsec and IPv6

- IPsec was defined as part of the IPv6 standard. It was so attractive that the IETF tried to retrofit it into IPv4. Unfortunately due to lack of the advanced header mechanisms of IPv6, and the widespread deployment of NAT (Network Address Translation) in IPv4 (due to the depletion of addresses), IPsec does not work well in IPv4. Also, many existing IPv4 routers and firewalls do not support it. Because of this, SSL VPN (a very poor substitute for IPsec, with no IETF standards) is commonly used in IPv4 based networks.
- IPsec, like QoS and Multicast, is mandatory in IPv6 products. It works very well in the IPv6 environment. This means it can be effectively used to prevent unauthorized use of services such as streaming audio and video, even over the general Internet.



Summary

- IPv6 is ideal for services such as IPTV and VoIP (compared to IPv4) because of its flat address space and superior support for:
 - Multicast
 - QoS
 - IPsec
- This is why InfoWeapons (one of the first companies to fully exploit the Next Generation Internet based in IPv6) is working on products to implement reliable, quality audio and video services, with simple to use mechanisms to prevent unauthorized use. These services do not require any “walled garden” to overcome shortcomings of IPv4, hence can be offered to customers worldwide.
- VoIP in particular benefits from these IPv6 advantages, so the first application product released by InfoWeapons is a fully dual stack (IPv4 and IPv6) VoIP (or SIP) server, called SolidPBX. There are existing IP phones (hard and soft) with good IPv6 support that work with it. Our SolidDNS product provides strong ENUM support for VoIP, in addition to dual stack DNS and DHCP, which are required for any dual stack application.



Thank You

See our website at www.infoweapons.com
(naturally over IPv4 *and* IPv6)