

IPv6

Internet Protocol version 6

- Provides Network-Layer Data Exchange Across the Internet
- Vastly Expands Total Number of Addressable Network Devices, Especially for Mobility
- Mu-4000 Identifies Vulnerabilities in IPv6 Deployments

Where is IPv6 Used?

The Internet Protocol Version 6 (IPv6) is the new standard for network layer data exchange across the packet-switched Internet. It supersedes IP version 4 (IPv4) to provide a vast jump in the number of addresses available for networked devices – more than two thousand million million globally routable IPv6 addresses for each globally routable IPv4 address.¹ The pressing requirement is to enable the Mobile Era of the Internet, supporting deployment of millions of VoIP-based cellular telephones and other small, mobile Internet devices. Without IPv6's expanded capacity of addressable devices, most of those new devices would be unable to receive calls and automated transmissions via the Internet. IPv6's new packet header (see Figure 1 below) enables the expanded address space. Many organizations, including large enterprises, service providers and governments are requiring new equipment to be IPv6-ready.

Mu-4000 Identifies IPv6 Vulnerabilities

As a new protocol stack, IPv6 leverages similar vulnerabilities to those in IPv4 and many RFCs unique to IPv6. The shift to IPv6 will be gradual so the bulk of new deployments will simultaneously support both versions of IP using several migration schemes, each of which carries its own potential vulnerabilities. Since IPv6 is new, both product developers and end users have not had time to learn best practices in programming and deployment in native and transitional environments. The Mu-4000 identifies exposures created by the lack of best practices and “vulnerability creep” to help organizations find and expunge weaknesses in new IPv6 deployments. The Mu-4000 mutates all fields of the IPv6 header, all defined extension headers, ICMPv6, and on different classes of addresses.

IPv6 Primer

The primary goal of IPv6 was to vastly expand the number of addressable devices on the Internet. It became clear later that the growth driver behind increasing consumption of IP addresses was a global proliferation of mobile devices and expanded use of embedded systems. Addresses in IPv6 are 128 bits long versus 32 bits in IPv4, which enables greater flexibility in addressing more devices. Short-term demand growth for IP addresses was slowed by widespread use of Network Address Translation (NAT). NAT, however, effectively blocks inbound connections so it does not solve the problem of supporting millions or billions of new mobile devices that want to use the Internet.

Current trends project exhaustion of the primary IANA IPv4 address pool in the 2009 to 2011 timeframe, causing many organizations to accelerate plans for IPv6 deployment. The U.S. Government, for example, has mandated that federal agencies deploy IPv6 in all federal backbones by 2008. All major operating systems natively support IPv6. Other benefits of IPv6 include

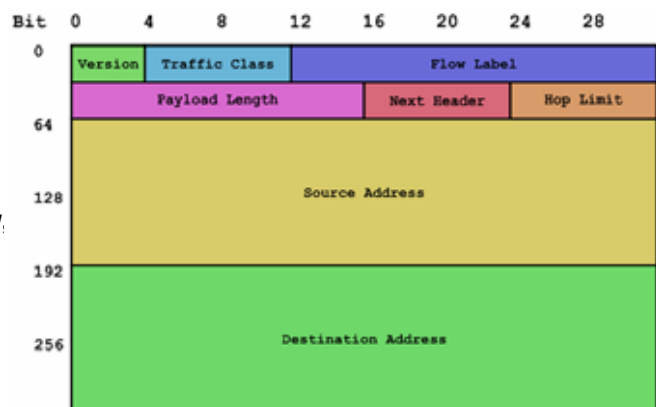


Figure-1: STRUCTURE OF AN IPV6 PACKET HEADER
Source: <http://en.wikipedia.org/wiki/IPv6>

¹The actual number is approximately $((1015/1771) * 292)$ or about 2,837,965,307,452,650,432,575,067,390 IPv6 unicast addresses for each unicast IPv4 address. For reference, the entire IPv4 address space “only” has 4,294,967,296 addresses.

stateless address auto-configuration, better multicast support, better support for high-performance interface with jumbograms, and mandatory network-layer security with IPsec.

Potential Weaknesses of IPv6

There are significant implications for securing IPv6 implementations. One issue is the alleged mandate for IPsec support. From a practical perspective, requiring IPsec will not ensure security because there is no scalable identity management infrastructure on which to deploy IPsec. The larger address space of IPv6 makes scanning certain IP prefixes more difficult than in IPv4. This capability makes IPv6 more resistant to malicious traffic – but it also makes it more difficult to identify unlisted rogue malware machines using distributed attack and new spoofing techniques over IPv6.

POTENTIAL IPv6 WEAK SPOTS

Structural issues with many type-length-value extension headers may be exploitable in IPv6.
Fragmentation support in IPv6 opens up potential attack vectors.
IPv6 addresses contain many more semantics and wider range of accepted variations than IPv4.

BENEFITS OF MU-4000

Rapid identification and detailed auditing of IPv6 weaknesses prior to malicious exploits.
Identification of both IPv4 and IPv6 fragment attacks.
Automates parsing structurally valid addressing in proper context through either multicast or unicast transport.

Table-1.

Transition mechanisms for simultaneous support of IPv6 and IPv4 include dual stack, automatic tunneling, configured tunneling, and proxying and translation. Each presents its own potential vulnerabilities, and devices that support multiple schemes may be exposed even if the end user has not configured all of them. Limited experience programming for IPv6 will create incorrect protocol implementations, and since mobile and embedded devices implement these protocols in hardware or firmware, flawed IPv6 implementations will enable attacks against services comprising millions of new network endpoints.

About the Mu-4000 Analyzer

The Mu-4000 analyzer is a security analysis platform that delivers the industry's first systematic and repeatable process to identify unknown and published vulnerabilities in any IP-based system, application or network device without requiring access to source code. The process, known as “mutate, monitor and manage,” easily integrates with existing security controls. The Mu-4000 subjects the target under analysis to a virtually unlimited number of attack vectors (the “mutations”). It monitors the target and captures results in a database while managing the process in a reproducible and actionable manner. Results include detailed reports and utilities to speed fault remediation. This lifecycle approach enables the creation of security-enabled processes in all phases of product development and deployment. The extensible security analysis platform also enables organizations to integrate their own suites of attacks. The Mu-4000 Analyzer is a self-contained, 2U rack-mountable appliance that is easily configured, operated and managed.

OTHER PROTOCOLS SUPPORTED BY THE MU-4000 (partial list)

ARP	PIM-SM
BGP4	POP3
CDP	RADIUS
DHCP	RTSP
DNP	SIP
FTP	SMTP
HTTP	SNMP
ICMP	SNMP Traps
IGMP	SSL-TLS
IMAP	SSDP
IPv4	SSH
IPv6	Sun RPC
ISAKMP	TCP
LDAP	TFTP
MGCP	TLSv1
PIM-DM	UDP

Table-2.



web: www.mudynamics.com | email: info@mudynamics.com
 address: 686 W. Maude Ave., Suite 104, Sunnyvale, CA 94085, USA
 phone: (866) 276-4640 or (408) 329-6330 | fax: (408) 329-6317