



Verfasst von Paul Stalvig | Technical Marketing Manager

IPv6 – 101: Einführung



Ich bin wahrscheinlich nicht der Einzige, der denkt, dass manche Menschen das Leben unnötig verkomplizieren. Vielleicht spielt dabei die Arbeitsplatzsicherheit eine Rolle, der „Chicken Little“-Effekt, oder die IT-Welt möchte einfach nur öffentlich Aufmerksamkeit erregen, um mehr Geld zu verdienen. Der Millennium-Bug ist hierfür ein hervorragendes Beispiel. Nach der Bewertung der tatsächlichen Fakten und einigen Codekorrekturen ging das Leben mit nur minimalen Unterbrechungen weiter wie zuvor. Die Umstellung auf IPv6 (Internet Protocol Version 6) stellt ein weiteres Beispiel für dieses Phänomen dar. Der Übergang zu IPv6 wird gerade erst untersucht, und schon macht sich manch einer das Leben schwerer als nötig. Man könnte doch einfach ein F5 BIG-IP®-Gerät verwenden, das die gleichzeitige Bereitstellung von IPv4 und IPv6 ermöglicht. Unternehmen, die beim Implementieren neuer Technologien eher zögerlich vorgehen, hätten die Möglichkeit, ihre Netzwerkarchitektur von Grund auf zu erneuern und dadurch langfristig von einem optimalen Netzwerk zu profitieren. Aber halt... wieso sollte sich jetzt etwas ändern, wenn schon zuvor immer lange mit neuen Implementierungen gewartet wurde?

Gibt es denn eine „Killeranwendung“, für die eine unmittelbare Umstellung auf IPv6 erforderlich ist? Derzeit gibt es sie nicht. Allerdings hat die Regierung den Übergang bis zum Jahr 2008 in Auftrag gegeben, und im World Wide Web herrscht ein dramatisches Wachstum vor. In den USA hat der Kongress gesetzlich erlassen, dass alle Regierungsbehörden bis 2008 IPv6-fähig sein sollten. Warum stellt die US-Regierung auf IPv6 um? Es heißt, uns – der Welt – gehen die verwendbaren IP-Adressbereiche aus. Daher müssen wir uns von der Technologie der 1980er Jahre verabschieden und zur Technologie der 1990er übergehen. Zudem werden die IP-Bereiche aufgrund der zunehmenden Verwendung einer Vielzahl alter und neuer Technologien, wie Handys, Laptops, PDAs, usw. förmlich verschlungen.

IP-Adressen

Nachdem ich stundenlang unzählige Bände von IPv6-Literatur durchforstet habe, frage ich mich, worin die Schwierigkeit liegt. Tatsache ist, dass IPv4 mit dem IPv6-Framework einige Verbesserungen, Erweiterungen und neue Hilfsprogramme hinzugefügt werden. Im Prinzip müssen wir uns nur verdeutlichen, dass die Kommunikation zwischen Computern über das Internetprotokoll (IP) erfolgt. Da es sich dabei nicht um Namen, sondern um Zahlen handelt, wird sich an den meisten Merkmalen der IP-Kommunikation nichts ändern. Die Paketkopfzeilen von IPv4 und IPv6 unterscheiden sich beispielsweise nur durch geringfügige Änderungen am Format. Die größte Änderung ist, dass für IPv6-IP-Adressen 128 Bits anstelle von 32 Bits verwendet werden. Das ist einleuchtend. Allerdings werde ich mir nicht die vollständigen IP-Adressen aller Computer merken. Dennoch gibt es tatsächlich einige Personen, die sich die Subnetinformationen (2^n) einprägen, die bis zu $2^{(128-n)}$ Bits einer IP-Adresse ausmachen.



White Paper

Verfasst von Paul Stalvig | Technical Marketing Manager

Sehen wir uns das also einmal genauer an. Eine IPv6-IP-Adresse beinhaltet Informationen im 128 Bit-Format und wird in Binär- oder Hexadezimalschreibweise notiert. Eine IP-Adresse setzt sich aus 16 Blöcken zu jeweils acht Bit zusammen. Meiner Meinung nach wäre es einfacher zu sagen, eine IP-Adresse besteht aus acht 16-Bit-Adressen, da die Hexadezimalnotation durch die 16-Bit-Aufteilung unterbrochen wird. Die Adresse besteht aus einem globalen Routingpräfix, einer Subnetkennung und der Schnittstellen-ID.

Es ist wichtig zu beachten, dass die Trennung der Ziffern nun durch Doppelpunkte anstatt durch Punkte erfolgt. Eine IPv6-Adresse hat also das folgende Format: 2001:DB8:F5F5::F5F5:00:00:C00:201. Wird die Adresse für einen Dienst verwendet, wird der Zusatz anstelle eines Doppelpunkts durch einen Punkt abgetrennt: (2001:DB8:F5F5::F5F5:00:00:C00:201.80 für Internet).

Das zu Dokumentationszwecken zugewiesene Präfix lautet 2001:DB8::/32.

Oktett oder Bytes	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Bits	0-8	9-16	17-24	25-32	33-40	41-48	49-56	57-64	65-72	73-80	81-88	89-96	97-104	105-112	113-120	121-128
Hex	20	01	DB	08	F5	F5	00	00	F5	F5	00	00	C0	00	02	01
Binär	00100000	00000001	11011011	00001000	11110101	11110101	00000000	00000000	11110101	11110101	00000000	00000000	11000000	00000000	00000010	00000001
Dezimal	32	1	219	8	245	245	0	0	245	245	0	0	192	0	2	1
Abkürzungen:																
Kompression																
führer Nullen	20	01*	DB	8	F5	F5	0	0	F5	F5	0	0	C0	0	2	1
Nullunterdrückung	20	01*	DB	8	F5	F5	::		F5	F5	0	0	C0	0	2	1
Mixed Notation																
IPv4-mapped	20	01*	DB	8	F5	F5	::		F5	F5	FF	FF	192	0	2	1

* Diese Zelle wird nicht reduziert, um Verwechslungen in diesem Beispiel zu vermeiden. Wenn das erste Oktett in Hexidezimalschreibweise notiert wäre, könnte es reduziert werden.

Abbildung 1: IPv6-IP-Adresse

Beim Erstellen von IPv6-IP-Adressen werden die ersten 48, 56 oder 64 Informationsbits (je nach Größe der Organisation) hauptsächlich vom Internetdienstanbieter als Routinginformationen zugeteilt. Die verbleibenden Bits sind für das interne Routing verfügbar. Eine Organisation könnte also, sofern DHCP verwendet wird, den Rest der IP-Adresse als MAC-Adresse verwenden. Wenn in einem Subnetz ähnliche Geräte vorhanden sind, wird auch die entsprechende Mac-Adresse sehr ähnlich sein, möglicherweise bis in das letzte Oktett. (Ich denke in diesem Zusammenhang an Intel-Server von Dell, Gateway oder HP. Die MAC-Adresse ist vom Hersteller der Netzwerkschnittstellenkarte vorgegeben. Wenn also verschiedene Server verwendet werden, die Netzwerkschnittstellenkarten jedoch vom selben Hersteller stammen, sind sich diese Nummern wahrscheinlich sehr ähnlich.) Es empfiehlt sich demnach in der Regel, nicht die MACs der Netzwerkschnittstellenkarten zu verwenden, da dies zu viele Probleme beim Überwachen, Warten, bei der Berichterstellung und bei der Sicherheit der Server verursacht.



Bei der ordnungsgemäßen Bereitstellung von IPv6-Adressen bietet die Änderung der ersten Bits einen eindeutigen Verteilungsmechanismus. Werden die ersten Informationsbits geändert, kann eine IP-Adresse erstellt werden, die an jeden Computer im Subnetz gesendet wird, jedoch ausschließlich in der aktuellen Verknüpfung oder im Subnetz.

Kategorien:

Unicast – Dies steht für ein einzelnes IP-Adressziel.

Multicast – Eine Multicast-Adresse wird an mehrere Ziele gesendet (z. B. bei der Übertragung an ein Subnetz). Die Informationen werden, je nach Konfiguration, von allen Computern verarbeitet.

Anycast – Anycast-Adressen werden an mehrere Ziele gesendet, letztendlich jedoch an das erste Gerät auf dem Routingpfad übergeben.

Bereiche:

Global – Globale IPv6-Adressen sind Standardadressen, die für das gesamte Internet gelten. Beispiel: 2001:DB8:F5F5::F5F5:00:00:C00:201

Site-Local – Standortlokale IP-Adressen sind nur für bestimmte Domänen zulässig. Sie werden nicht über das Internet geroutet, sondern nur über das interne Netzwerk eines Unternehmens. Es ist erforderlich, Grenzrouter zu konfigurieren, um den nicht autorisierten Zugriff standortlokaler IP-Adressen auf das Internet oder VPNs zu verhindern. Diese Adressen wurden zuvor als private bzw. RFC 1918-IP-Adressen bezeichnet. Obwohl diese IP-Adressen veraltet sind (und nicht verwendet werden sollten), können verbindungslokale IP-Adressen so geändert werden, dass sie wie standortlokale IP-Adressen funktionieren.

Link-local – Verbindungslokale IP-Adressen sind ausschließlich für die Kommunikation in lokalen Netzwerken zugelassen. Der oder die Router sollten so konfiguriert sein, dass keine anderen Routen zulässig sind. Darin gleichen sie den privaten IP-Adressen – d. h. Adressen, die nicht geroutet werden – mit der Ausnahme, dass sie ausschließlich für bestimmte Netzwerkverbindungen bzw. Subnetze verwendet werden. Wenn standortlokale IPv6-IP-Adressen veraltet sind, können diese Adressen als Ersatz verwendet werden. Beispiel: Fe80:DB8:F5F5::F5F5:00:00:C00:201

Subnetting – Subnetze werden genauso verwendet wie mit IPv4-Adressen. Der einzige Unterschied besteht im Format von 128 Bits anstatt der 32 Bits bei IPv4. Die zusätzlichen 12 Oktette und deren Handhabung



können nach eigenem Ermessen verwendet werden. Das Aussprechen der Ziffernfolge 255.255.255.255.255.255.255.255.255.255.255.255.255.255.255.255.192 kann einem den Atem verschlagen. Ohne die 64 Bits, die den eigenen IP-Bereich (2001:DB8:F5F5:00:00:/64) kennzeichnen, bleibt mit 255.255.255.255.255.255.255.192 ein Bereich von 64 IP-Adressen übrig. Für einige 255er müsste man also doch noch tief Luft holen.

Spezielle Adressen:

Unspecified – Die nicht spezifizierte IP-Adresse wird verwendet, wenn ein Host mit aktiviertem DHCP auf das Netzwerk zugreift. Diese Art von Adresse setzt sich vollständig aus Nullen zusammen und wird mit „::“ dargestellt.

Loopback – Eine Loopback-Adresse entspricht der 127.0.0.1-Adresse von IPv4. Sie wird als „::1“ dargestellt.

Abwärtskompatibilität:

Um den effektiven und effizienten Betrieb zwischen IPv6- und IPv4-Netzwerken zu gewährleisten, stehen mehrere Lösungen zur Verfügung. Sehen wir uns zwei dieser Lösungen an. In der Methodik zur IPv4-Kompatibilität werden zumeist die ersten Bits geändert, und bei den letzten 32 Bits handelt es sich um eine IPv4-IP-Adresse.

Bei IPv4-Mapped IPv6-Adressen befindet sich die IPv4-IP-Adresse in den untergeordneten 32 Bits der IPv6-IP-Adresse. In der Dezimalschreibweise mit Punkten steht die 192.0.2.1-IP-Adresse am Ende (2001:DB8:F5F5::F5F5:00:00:192.0.2.1).

IPv6-zu-IPv4 – Auch in diese IPv6-IP-Adressen sind IPv4-Adressen eingebettet. Zudem verfügen sie auch über die ersten 13 Bits. Die ersten dreizehn Bits lauten „00100000 00000010“ oder in Hexadezimalnotation „2002“. Verwendung von 192.0.2.1 als IPv4-Adresse: Das Ergebnis wäre eine 2002:C000:0201::/48-IPv6-IP-Adresse. Aufgrund dieser Nummerierung wird die resultierende IP-Adresse nicht ordnungsgemäß über das Internet geroutet, sondern nur innerhalb des Netzwerks.

Vergabe und Registrierung:

Die größte Änderung, die nicht sofort ersichtlich ist, liegt in der hierarchischen Verarbeitung der IPv6-Adressbereiche, die sich von der vorherigen zufälligen Methodik unterscheidet. Es ist bekannt, dass in IPv4 jedes Land über einen bestimmten IP-Adressbereich verfügt. Daran ändert sich nichts. Allerdings ändern sich die Quellen, bei denen IP-Adressen erworben werden können.

Die IP-Adressen werden nicht mehr von den einzelnen Unternehmen, Internetdiensteanbietern (Internet Service Provider – ISP) und Personen aus beliebigen verfügbaren Bereichen angefordert. Stattdessen wird der IP-Adressbereich zunächst vom ISP festgelegt und anschließend aufgeteilt (vgl. Abbildung 2). Angenommen, ein Unternehmen verwendet den Internetdiensteanbieter „beispiel.com“. Der IP-Bereich wird bei beispiel.com angefordert. Anschließend stellt beispiel.com die für das Netzwerk geeigneten IP-Adressen aus. Zusammen mit beispiel.com und der Regional Internet Registry (RIR) werden die neuen Daten registriert, wie z. B. die neue IP-Adresse des DNS (Domain Name Services)-Servers. Wie in Abbildung 2 dargestellt, geben die IP-Adressen den Standort an. Die ersten 16 Bits geben die Region an (2001::/16), und die nächsten 16 Bits stammen von beispiel.com (2001:DB8::/32). Die darauf folgenden 16 bis 32 Bits verweisen auf den Bereich des Unternehmens (2001:DB8:F5F5::/48). Bei allen IPv6-Subnetzen und -Adressen belegt dieses Subnetz die ersten 48 Bits. An diesem Punkt wird IPv6 etwas kompliziert für die IT-Mitarbeiter. Was geschieht, wenn zwei ISPs verwendet werden, oder wenn der Wechsel zu einem neuen ISP geplant ist? Unter Umständen könnte hierfür eine vollständige IP-Migration erforderlich sein.

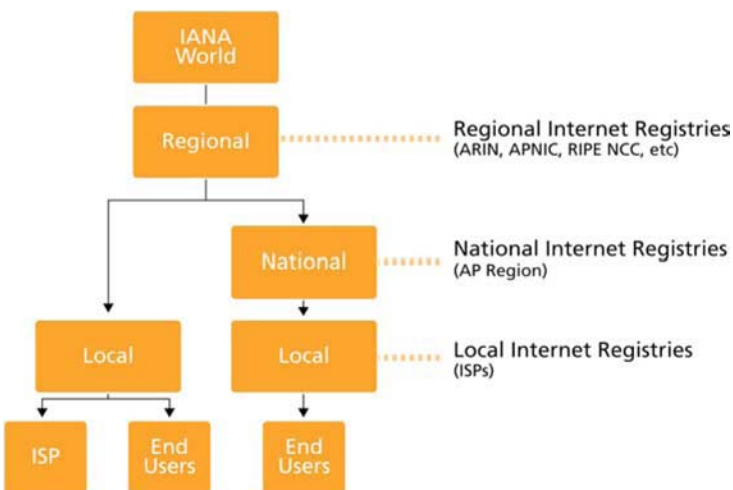


Abbildung 2 IPv6-Registrierung

Wenn eine Organisation aus Redundanzgründen über zwei verschiedene ISPs verfügt, sollte nur ein Adressbereich verwendet werden. Der „Fremdadressbereich“ des sekundären ISPs wird in diesem Fall über dessen Netzwerk geroutet. Dies ist in Bezug auf die Bereiche von Internetdiensteanbietern nichts Neues. Wenn für ein sekundäres Netzwerk eine interne IP-Adressierung erforderlich ist, wird ein kleines bzw. einzelnes Subnetz ausgestellt, das den speziellen Anforderungen des sekundären Netzwerks, und nicht der ganzen Organisation, entspricht. Dadurch können Gesamtkosten gesenkt und Migrationsprobleme vermieden werden.



Wenn eine Organisation den primären ISP wechseln möchte, sollte die Übertragung aller IP-Adressen in eine neue ISP-Routingtabelle oder die Umstellung auf eine neue IP-Adressierung sorgfältig geplant werden. Da jeder ISP über eigene Richtlinien für Netzwerkübertragungen und -routen verfügt, ist es nicht möglich, die genauen Probleme der Organisation im Voraus darzustellen. Die Verwendung von intelligenten, globalen und lokalen Traffic-Managern erleichtert die Migration zu den neuen IP-Adressen (alternativ zur Durchführung einer Umstellung), indem die alten und neuen IP-Adressbereiche sowie der Datenverkehr von den alten und neuen IP-Adressen gleichzeitig bereitgestellt werden. Dies ermöglicht eine reibungslose Migration, und die Auswirkungen auf den Kunden können abgeschwächt werden.

Da jeder ISP auf die IPv6-Migration von Unternehmen vorbereitet sein muss, ist es sinnvoll, wenn der Übergang auf IPv6-Adressen über die ISPs erfolgt. Für jedes IPv6-Routing werden Änderungen erforderlich sein. Im Bereich der Netzwerkrouter stehen interessante Herausforderungen an, da ein Router die Datenpakete nicht mehr fragmentieren kann. Wenn ein Paket für eine angegebene Verbindung zu groß ist, muss der Router eine Nachricht an den Ersteller senden. Der Absender ist dafür verantwortlich, die Pakete anzupassen und erneut zu senden. Es steht zu hoffen, dass die Pakete auf dem Netzwerkpfad nicht für eine andere Verbindung erneut verkleinert werden müssen. Aus dieser Sicht liegt die Hauptaufgabe der Router im Erstellen von Routen, und nicht im Ändern von Paketen. Nun muss der Routingverlauf (der Routingpfad auf beiden Seiten des Routers, der zum Senden der Pakete von der Quelle an das Ziel verwendet wird) von IPv6-Routern aufrechterhalten werden. Dieser Vorgang ist jedoch, im Vergleich zur Fragmentierung, relativ einfach und weniger aufwändig.



Abschluss

Da die Verwendung von IPv6 im Internet zunimmt, ist ein grundlegendes Konzept zur Konfiguration und Verwendung von IP-Adressen für jede Organisation entscheidend. Organisationen müssen eine effektive Migrationsstrategie entwerfen und implementieren. Es müssen nicht nur externe IP-Adressen aktualisiert werden, sondern auch interne IP-Adressen, mit denen Partner über IPSec-Tunnel und Back-End-Verbindungen verbunden sind. F5 stellt eine Methode zum gleichzeitigen Betrieb von IPv4- und IPv6-Diensten bereit, indem der unmittelbare Wechsel zu IPv6 durch eine stufenweise Migrationsstrategie ermöglicht wird.

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 www.f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
info.asia@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com