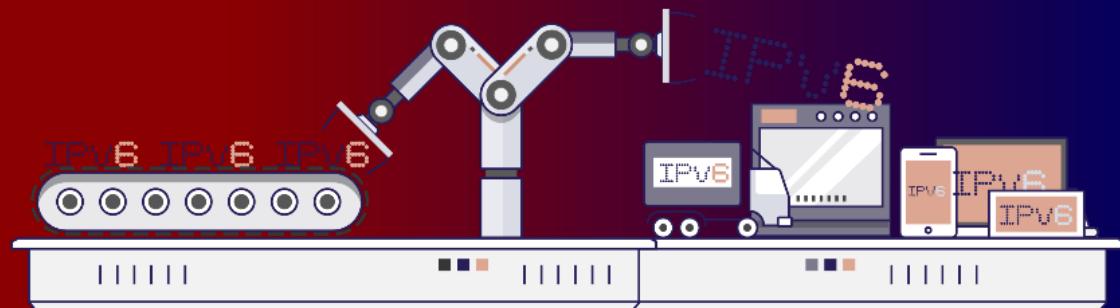




Enterprises: How to deploy —

— IPv6?



VON DER PLANUNG BIS ZUM EINSATZ

OKTOBER 2024 // V 1.4



Dieses Dokument hilft Ihnen, Ihre Aufgaben zu definieren, deren Umsetzung zu planen und IPv6 in Ihrem Unternehmen einzuführen.

Ein umfassender Überblick.

Inhaltsverzeichnis

Vorwort	7
Präambel	8
Leserschaft und Textauszeichnungen	9
I: Einführung	10
• VERGLEICHBARE PROJEKTE	11
• ENTWIRRUNG	11
Der menschliche Faktor	13
• FORTBILDUNGEN	13
• GEGENSEITIGE HILFE	14
Notwendigkeit	15
• EXPOSITION IM INTERNET	15
• ZUGRIFF AUF EXTERNE DIENSTE	18
QUIC ist angekommen	19
• INTERNES NETZ	20
II: Transition Techniken	24
Dual-Stack	26
Transportmechanismen	27
• INTEGRATION IN EINEM IPV4 UNDERLAY	27
MPLS	27
VXLAN	28
SD-WAN	28
• TUNNELLÖSUNGEN	29
• UND IPv6-ONLY?	29
Übersetzungsmechanismen	31
• NAT64 + DNS64	31
Adressierung	32
Topologie	32
MTU ist wichtig	33
Hinweis zur Filterung	33
Welcher Bereich welche Technologie?	34
• CAMPUS	34
NAT64 + DNS64	34
• RECHENZENTRUM	35
Dual-Stack-Server und Anwendungen	36
6/4 Übersetzung	36
Native IPv6-Bereitstellung	37
Singlestack	38
Cloud-Anbieter	38

Externe Übersetzung	38
• WAN	38
Regionale NAT-Plattform	38
III: Einzelteile	40
Warm up	42
Netzwerk	43
• Bereit?	43
• Hardware	44
• LAB	44
• INTERNES ROUTING	46
BGP	47
IGP	47
• FILTERN UND VERFOLGEN	48
Infrastrukturdienste	49
• SIEM	49
• DNS/IPAM/DHCP	49
• VPN, PROXY UND REVERSE PROXY	49
Externe Schnittstelle	49
Interne Schnittstelle	50
• Betriebssysteme	50
IP-Precedence	50
Software-Agenten	52
• ARBEITSPLATZDIENSTE	52
Directory	52
Dateifreigaben und Software-Repositories	53
Kommunikation	53
• ANWENDUNGEN	53
Wie geht man mit einem Dienst um, der über Webbrowser bereitgestellt wird?	55
Anwendungen, die IP verarbeiten	55
IV: Adressplan	57
• ÖFFENTLICH ODER PRIVAT?	58
• KLEINE ORGANISATION	58
ULA	58
Provider Independent (PI) Präfix	59
Nachteile von NPTv6	59
• GROSSE ORGANISATION	60
Verwaltung des direkten Internetzugangs	61
• LOGISCHE GRUPPEN	62
• ADRESSBASTANDTEILE	63
• PRÄFIXGRÖSSE	64
Standard	64

Interconnection	65
• GEMEINSAME DIENSTADRESSEN	65
• ZEITLICHE ENTWICKLUNG	66
• VERWENDUNG DER INTERFACE-ID 0	67
• PRO SCHNITTSTELLENISOLIERUNG	67
• IP IPv4 / IPv6 MAPPING	68
Netz-Präfix-Nummer	69
Hostnummer/Schnittstellen-ID	69
• NATIVE IPv6-NETZE	71
• Internet BGP-Announcement	72
V: Sicherheit und Best Practises	73
Access	75
• DYNAMISCHE ADRESSZUWEISUNG	75
Mechanismen	75
DHCP Identifizierung	76
• ICMP REDIRECT BLOCKING	77
• IPv6 SNOOPING	77
ND-Fragmentierung	78
Zuordnung	78
Quelle	79
Zielort	80
Umzüge	80
ND Unterdrückung	80
Präfix	80
Cache-Poisoning	81
• DHCP ROGUE	81
Physisch	81
Logisch	81
• RA GUARD	82
• RA HOP LIMIT	83
• ANDERE RA-EINSTELLUNGEN	83
• seND (NICHT EINSETZBAR)	85
• MLD	85
• STORM CONTROL	87
• ZU BLOCKIERENDE MULTICAST-GRUPPEN	87
Host	88
• DHCP	88
DHCP DUID	88
DHCP-IAID	89
DHCP ohne RA	89
Unterstützung von DHCP-Optionen im Dual-Stack	89

• SLAAC-ADRESSGENERIERUNGSVERFAHREN	89
Temporäre Adresse	90
Zufallsgenerierte Interface-ID	91
Stable Privacy Address	91
SLAAC-Synthese	91
Verfahren zur Generierung von Link-Local-Adressen	92
• IPv6-STACK NICHT DEAKTIVIEREN	92
• DEAKTIVIERUNG VON ÜBERGANGSMECHANISMEN	93
• DEAKTIVIERUNG VON AUTOMATISCHEN ERKENNUNGSPROTOKOLLEN	93
• BLOCKIERUNG DES LINK-LOKALEN VERKEHRS	94
• VPN	94
• DESKTOP OS KONFIGURATION	95
Windows	95
Linux	95
Network-Manager	96
Systemd Netzwerkd	96
netplan	96
wickedd	97
Linux-Distributionen	97
• MOBIL UND EMBEDDED	98
Android	98
Andere Betriebssysteme	99
Transit	100
• URPF	100
• SCHUTZ DER CONTROL PLANE	100
• OSPF SICHERHEIT	100
Filterung	102
• ICMP	102
• TRANSITION MECHANISMEN	104
• BOGON PRÄFIXE UND ROUTEN	105
• HEADER EXTENSION	106
• Policies	107
Appendix A: Anhang	109
• URL UND LINK-LOCAL IP	110
• MEHRERE PRÄFIXE	111
• CONTAINER	112
Docker	112
Kubernetes	112
• SCADA	113
• NAT64 IN DEN NETZEN DER MOBILFUNKBETREIBER	113
Service Discovery	114

Betrieb auf mobilen Betriebssystemen	114
Hotspots und Teathering	115
• IPv4 PORT SHARING	115
• RFC-ENTWÜRFE ZUR RETTUNG VON IPv4	116
• BEISPIELE FÜR IPV6-IMPLEMENTIERUNGSPROBLEME	116
Nicht gelöschte Routen	116
Unerwartete Verwendung der IPv4-Präfix-Darstellung	117
Inkompatible Eingabefelder	117
• VERSCHWENDUNG VON ADRESSSRAUM	118
• UMWIDMUNG VON ADRESSEN FÜR ANDERE ZWECKE	118
• SRv6	119
• THREAD	120
• SELF-HOSTING UND HEIMANWENDER	120
Adressierung und DNS-Veröffentlichung	120
Flow opening	121
Erreichbarkeitstest	122
• AUTOMATISCHE PORTFREIGABE	122
• ENTWICKLUNG DER ONLINE-SPIELE	123
• WAS IST VON DEN INTERNETPROVIDERN ZU ERWARTEN?	124
Appendix B: Über dieses Dokument	125

Vorwort

Danke

 Dieses Dokument wurde ursprünglich von Jean-Charles BISECCO mit der Unterstützung von Mitgliedern der IPv6-Taskforce verfasst. Es wurde von Axel Semberg in ASCIIDOC überführt, auf Github veröffentlicht und ins Deutsche übersetzt.

Dieses Dokument basiert auf der Arbeit der IPv6-Taskforce, die gemeinsam von Arcep und Internet Society France geleitet wird. Arcep und Internet Society France haben eine Task Force ins Leben gerufen, die sich mit IPv6 befasst und allen Akteuren des Internet-Ökosystems offensteht (Internet Service Provider, Hoster, Unternehmen, öffentlicher Sektor usw.). Sie soll den Übergang zu IPv6 beschleunigen, indem sie den Teilnehmern die Möglichkeit gibt, sich mit spezifischen Fragen zu befassen und best practices auszutauschen.

Dieser von der IPv6 Task Force erstellte Leitfaden soll Bewährtes für die erfolgreiche Umsetzung des Übergangs zu IPv6 vermitteln. Er soll nicht das Fachwissen der IT-Teams Ihres Unternehmens ersetzen, und die Autoren können nicht für Probleme verantwortlich gemacht werden, die aus diesem Leitfaden resultieren.



Treten Sie unserer [IPv6 taskforce](#) bei (französisches Formular, aber wir akzeptieren auch Englischsprachige)

Dieses Dokument gibt nicht den Standpunkt von Arcep wieder, sondern den der Mitarbeiter der Task Force.

 Die neueste Version dieses Leitfadens finden Sie hier:

<https://en.arcep.fr/publications/task-force-ipv6.html>



Präambel

Die Einführung von IPv6 schreitet in allen Teilen der Welt voran, und seine Nutzung ist nicht mehr nur anekdotisch, wie es zu Beginn der 2010er Jahre oft der Fall war. Dieser Leitfaden soll Unternehmen dabei helfen, den Umfang ihrer IPv6-Implementierung zu bestimmen, die Implementierung des Protokolls zu erläutern und eine Reihe von Best Practices bereitzustellen.

Auch wenn es an Dokumentationen über IPv6 und seine Einführung nicht mangelt, konzentrieren sich die meisten davon auf die Netzebene und beziehen sich auf eine horizontale Betrachtung des Datentransports, die in der Regel für einen Betreiber, einen Transitanbieter oder einen Internet-Austauschpunkt gilt.

Die Bereitstellung digitaler Dienste innerhalb eines Unternehmens erfordert jedoch in der Regel ein eher vertikales Modell mit manchmal einzigartigen Konfigurationen in den oberen Schichten, sobald wir uns den vielen Produktionsanwendungen nähern.

Dieser Leitfaden soll IT-Abteilungen, die an der Umstellung auf IPv6 in Unternehmen beteiligt sind, Informationen zur Verfügung stellen, um die Umstellung zu erleichtern.

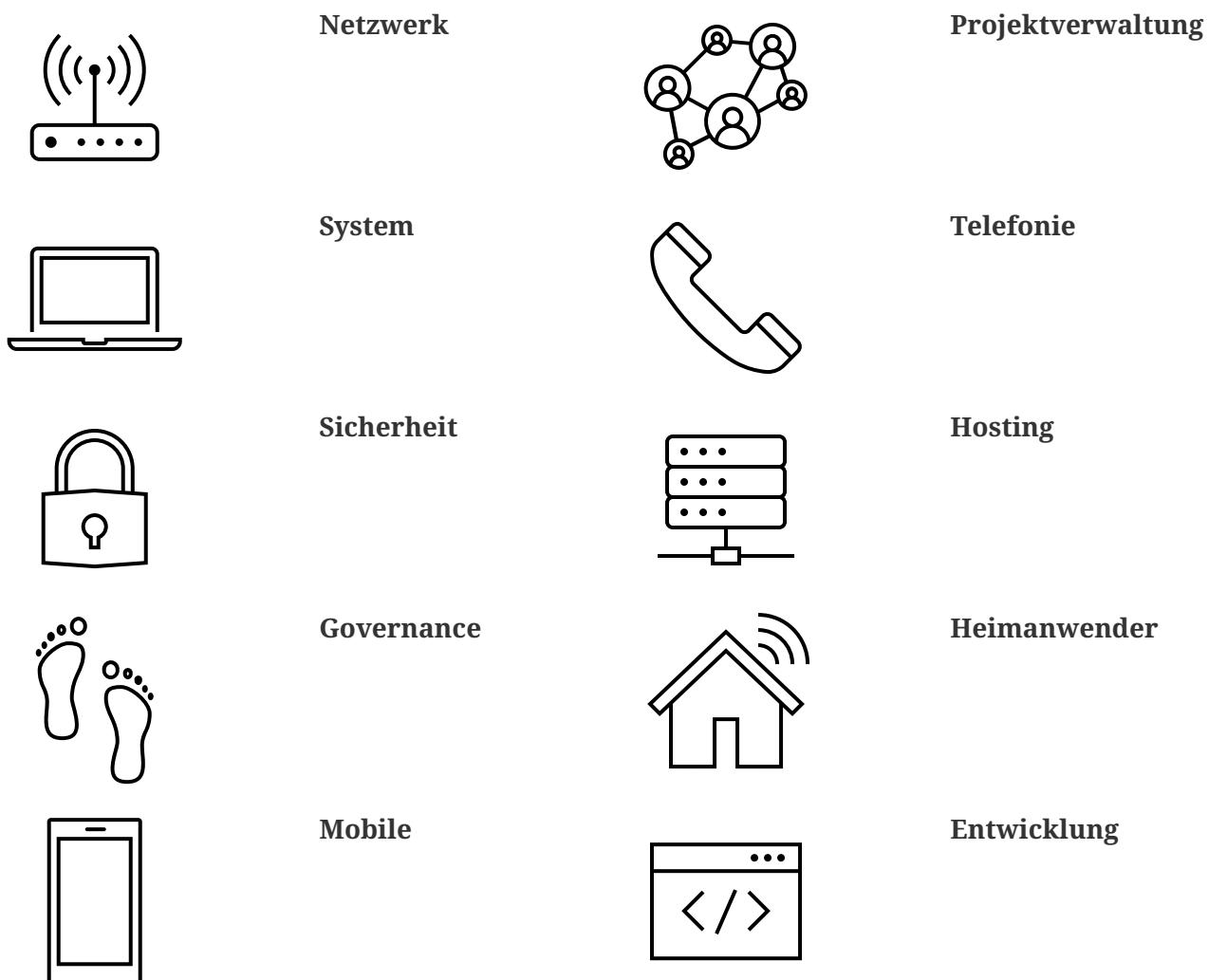
Auch wenn in diesem Dokument auf technische Aspekte eingegangen wird, ist es nicht der Zweck dieses Dokuments, ein IPv6-Lehrbuch zu sein, und es beschränkt sich auf die Details, die für die Behandlung der angesprochenen Punkte erforderlich sind. Es bleibt Ihnen überlassen, IPv6 anhand bestehender Inhalte, reiner Lehrmaterialien, Herstellerdokumentationen, Blogbeiträgen, MOOC, Schulungen usw. zu vertiefen.

Leserschaft und Textauszeichnungen

Dieses Dokument richtet sich in erster Linie an Experten für Informationssysteme, die für den Übergang zu IPv6 zuständig sind.

Er enthält jedoch Abschnitte und Paragraphen, die sich an unterschiedliche Zielgruppen richten.

Auch wenn allen, die eng in Ihr Projekt eingebunden sind, empfohlen wird, das gesamte Dokument zu lesen, gilt dies nicht zwingend für alle anderen. Anhand der Logos am Rand jedes Abschnitts können Sie leicht erkennen, für welche Zielgruppe der jeweilige Inhalt bestimmt ist.



In einigen Abschnitten wird darauf hingewiesen, dass die Auswahlmöglichkeiten für große und kleine Unternehmen unterschiedlich sind. Wenn es nicht möglich ist, eine klare Trennung zwischen den beiden zu ziehen, wird eine Organisation umso mehr in die Kategorie der großen Unternehmen fallen, je komplexer und umfangreicher ihr Informationssystem (IS) ist, auch wenn die Organisation sich selbst nicht als solche klassifiziert, basierend auf ihrer Größe ihres Personals oder ihrer geografischen Ausdehnung.

Teil I: Einführung



Einleitung

Auch wenn die Technologie ein wichtiger Teil dieses Themas ist, ist es ein schwerer Fehler, IPv6 nur darauf zu reduzieren. Die thematische Breite von IPv6 kann aufwändiges Projektmanagement und komplexe technische Entscheidungen erfordern. Die Zuständigkeit für Letztere kann je nach Organisation variieren.

Dieses Kapitel soll Ihnen eine Reihe von Aspekten erläutern, die sich unmittelbar auf den Erfolg des Projekts auswirken können.

• VERGLEICHBARE PROJEKTE

Das Thema IPv6 mag sehr umfangreich sein, aber es ist bei weitem nicht das erste seiner Art. Je nachdem, wie alt Ihr Unternehmen ist, haben Sie vielleicht schon andere Projekte in Angriff genommen, die mit erheblichen Einschränkungen verbunden waren und einen ähnlichen Umfang hatten. Die Erfahrungen aus der Planung und Durchführung jener Projekte könnten Sie davor bewahren, die Fehler zu wiederholen.

Das älteste Beispiel ist die Umstellung auf das Jahr 2000, das in einigen Fällen tiefgreifende Änderungen erforderte, insbesondere bei Datenbanken (Database Management System, DBMS), sowie umfangreiche Tests für Jahreszahlen, die zweistellig kodiert waren.

In jüngerer Zeit erforderte die Einführung von TLS-Zertifikaten - auch für rein interne Anwendungen, die nicht dem Internet ausgesetzt sind - Änderungen an Servern und Proxies/Loadbalancern usw. Von der Konfiguration der Middleware, der Erstellung oder Erweiterung der PKI, der Hinzufügung der Verschlüsselung zu den Audit- und Monitoringsystemen für den Datenverkehr bis hin zur Überwachung der ordnungsgemäßen Einrichtung der gesamten Zertifizierungskette auf den verschiedenen Geräten waren zahlreiche Systeme betroffen.

Auch TLS befindet sich in ständiger Entwicklung und muss regelmäßig geändert werden, wenn Algorithmen veralten, neue Mechanismen hinzukommen usw.

Das letzte Beispiel, das je nach Unternehmensstrategie mehr oder weniger häufig vorkommt, ist die Einführung einer neuen Version eines Betriebssystems und der Migrationszeitraum für Kundenarbeitsplätze mit seinen Anwendungsbewertungen und dem Änderungsmanagement.

Andere Großprojekte sind ebenfalls üblich, wie z. B. die Einführung eines ERP-Systems, aber sie sind eher geschäftsspezifisch und daher von der Kerntätigkeit des Unternehmens abhängig.

• ENTWIRRUNG

Das Internet-Protokoll (IP) ist das zugrunde liegende Element der Kommunikationsinfrastruktur, das eine durchgehende Kompatibilität zwischen den verschiedenen Systemen erfordert. Es gibt nicht die eine Analysemethode, um alle Auswirkungen zuverlässig zu erfassen, so dass eine Kombination mehrerer Methoden erforderlich ist.

Der theoretische Ansatz ist nützlich, wenn Elemente einzeln untersucht werden - z. B.: Hat mein Firewall-Anbieter in Bezug auf IPv6 eine Sicherheitsfunktion ordnungsgemäß implementiert? Wird sich meine Middleware mit einem IPv4- und einem IPv6-Socket gleich verhalten?

Auf der anderen Seite ist eine systemische Analysemethode gut geeignet, um einen Gesamtüberblick über das komplexe Geflecht von miteinander verbundenen Geräten zu erhalten, von denen jedes später sein eigenes System und seine eigene Anwendung hat. Diese Methode muss verwendet werden, um einen verdichteten Gesamtüberblick über die Bausteine des IS in den verschiedenen Schichten zu erhalten.

Da es nicht möglich ist, jedes Element des Informationssystems im Detail zu erforschen, ist es manchmal notwendig, sich auf das Wesentliche zu beschränken, vor allem auf die peripheren Elemente des Ökosystems - wie die Überwachung und die Erfassung von Datenprotokollen -, so dass man sich in der Pilotphase effizienter mit ihnen befassen kann und die gleiche Arbeit nicht zweimal machen muss.

Der Versuch, alles auf einmal zu untersuchen, alles zu inventarisieren, führt nur zu Stagnation und ist nicht die richtige Methode.

Wie ein guter Krimi-Autor müssen Sie genau im richtigen Moment Details über Ihre Figuren preisgeben. Es handelt sich um ein langfristiges Projekt, und es ist zwecklos, tief in das gesamte Ökosystem einzutauchen, da es sich wahrscheinlich geändert haben wird, wenn die Pilotumstellungen und Produktionseinsatz stattfinden.

Apropos Änderungen in den betroffenen Bereichen: Jede dieser Änderungen ist eine Gelegenheit, IPv6 einzuführen. Informieren Sie sich also regelmäßig bei Ihren verschiedenen Abteilungen, um über neue Projekte auf dem Laufenden zu bleiben und diese Gelegenheiten nicht zu verpassen.

Der menschliche Faktor

Sie werden zwangsläufig auf einige Widerstände stoßen, so dass Sie in jedem der beteiligten Teams Unterstützung finden müssen, um voranzukommen. Die kontinuierliche Einbindung der Mitglieder der verschiedenen Teams muss genau zum richtigen Zeitpunkt beginnen. Wenn Sie zu früh damit beginnen, wird die Begeisterung der Mitarbeiter nachlassen und das Projekt an Schwung verlieren; wenn Sie zu spät damit beginnen, wird sich dies auf die Durchlaufzeit des Projekts auswirken. Im Idealfall schafft eine gute Projektplanung die Möglichkeit, die Anzahl der Teilnehmer im Projektteam zu erhöhen, sobald es die Umsetzungsphase beginnt.

Große, abteilungsübergreifende Sitzungen sollten nur der Information dienen, nicht aber dem Brainstorming oder der Diskussion. Andere Vorbesprechungen mit einem oder zwei Vertretern pro Team sind dafür besser geeignet. Spezifische Details, die ein bestimmtes Team betreffen, sollten nur mit diesem Team und möglicherweise mit seinen fachlichen Nachbarn besprochen werden.

All diese Elemente mögen selbstverständlich, wenn nicht gar selbstverständlich erscheinen, aber da an dieser Art von Projekten sehr viele Akteure beteiligt sind, muss eine Hierarchie für den Dialog innerhalb einer großen Struktur geschaffen werden.

Zusammenfassend lässt sich sagen: Bestimmen Sie einen oder zwei Vertreter pro Team und halten Sie sich über künftige Projekte auf dem Laufenden, die Einsatzmöglichkeiten bieten könnten.

Informieren Sie alle Teams in regelmäßigen Abständen auf hohem technischen Niveau über das Projekt, und informieren Sie ein breiteres Publikum auf Informationssitzungen oder in den von Ihnen verschickten Kommunikationsmaterialien über weniger technische Aspekte.

Führen Sie schließlich Einzelgespräche mit den beteiligten Teams, wenn sie sich in der Umsetzungsphase befinden, diesmal in einem größeren Rahmen und entsprechend dem Projektverlauf.

So ist es beispielsweise nicht notwendig, das für die Middleware zuständige Team regelmäßig aufzufordern, sich vorzubereiten, wenn das Netz noch keinen Pilotversuch mit Testservern geplant hat.

• FORTBILDUNGEN

Sie müssen Schulungen für Ihre Mitarbeiter einplanen, um sie auf die Einführung von IPv6 vorzubereiten.

Um den Übergang zu begleiten, müssen Sie auf verschiedenen Rollen, Berufe und Fachkenntnisse, die für einen erfolgreiche IPv6-Einführen erforderlich sind, zugeschnittene Schulungen erstellen.

Vor der Ausarbeitung eines Schulungsprogramms wäre es ratsam, die Mitarbeiter zu befragen, welche Schulungen sie benötigen, um ihre Aufgaben mit IPv6 ordnungsgemäß ausführen zu können. Und in manchen Fällen sogar Module zu erstellen, die auf die besonderen Aspekte und Bedürfnisse des Unternehmens zugeschnitten sind.

Zumindest können Sie davon ausgehen, dass Sie die auszubildenden Personen in mehrere Gruppen einteilen müssen:

- Netzwerk
- Sicherheit
- App-Entwicklung

Idealerweise sollte das Projektteam alle Module mit einem oder zwei Vertretern jeder Zielgruppe testen.

• GEGENSEITIGE HILFE

Zögern Sie nicht, mit Unternehmen und Organisationen ähnlicher Größe, die eine IPv6-Umstellung planen oder durchführen, Kontakt aufzunehmen, um Erfahrungen auszutauschen.

Die IPv6-Taskforce (die gemeinsam von Arcep und der Internet Society France geleitet wird) bietet die Möglichkeit, das Thema mit Gleichgesinnten zu erörtern, was sich auf jeden Fall lohnt. Sie können auch Ihrem lokalen IPv6-Forum beitreten.

Wir zählen darauf, dass Sie uns helfen, diesen Leitfaden zu verbessern und Beispiele für Produkte zu dokumentieren, die in Unternehmen weit verbreitet sind. Siehe den Abschnitt über Feedback am Ende des Leitfadens.

Notwendigkeit

Wir haben bereits Beispiele für Projekte wie TLS und die Umstellung von Betriebssystemen angeführt. Diese Projekte werden in der Regel durch die Notwendigkeit angetrieben, ein Sicherheitsproblem zu lösen oder ein technisches Gerät zu schützen. Andere Projekte werden durch die Einhaltung gesetzlicher Vorschriften angetrieben, wie z. B. die Sicherstellung der Rückverfolgbarkeit von Benutzeraktionen oder die Umsetzung von DSGVO-Anforderungen in Systemen. Natürlich ist die Kosteneffizienz ein Antrieb für andere Projekte, die entweder durch geschäftliche Erwägungen oder durch die Verbesserung des Dienstleistungsniveaus angetrieben werden, wie z. B. bei Orchestrationsprojekten.

Es ist schwierig, ein IPv6-Projekt unter eine dieser Motivationen einzuordnen, und noch schwieriger, IPv4 als potenzielle, kurzfristige "technische Schuld" zu bezeichnen, wie es bei einer veralteten Programmiersprache der Fall sein könnte, für die es keine Entwickler mehr gibt.

In diesem Abschnitt werden daher IPv6-Nutzungsfälle untersucht und ihre Relevanz in Abhängigkeit von der jeweiligen Situation dargelegt.

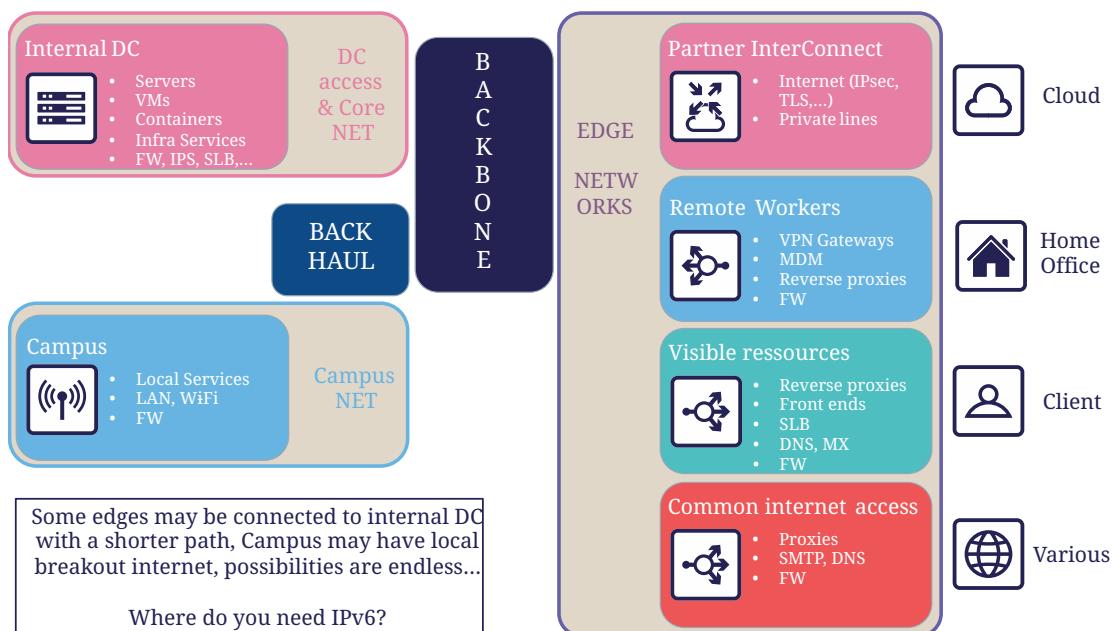


Abbildung 1. Wo brauchen Sie IPv6?

• EXPOSITION IM INTERNET

Den öffentlichen Internetauftritt mit IPv6 zugänglich zu machen, ist wahrscheinlich die größte Priorität, die umgesetzt werden muss.

Dazu gehören Webserver, aber auch DNS, VPN-Gateways...

Die Internetprovider aktivieren nach und nach IPv6 in ihren verschiedenen öffentlichen Netzen. Es begann mit Privatanschlüssen, dann mit Mobilfunkanschlüssen und schließlich mit der gemeinsamen Nutzung von Telefonanschlüssen. Die meisten Smartphones funktionieren jetzt in Mobilfunknetzen nur noch über IPv6, wobei NAT64 die Abwärtskompatibilität zu IPv4 gewährleistet.

Sowohl die Kunden als auch die Mitarbeiter verbinden sich also über IPv6-Verbindungen mit den Infrastrukturen des Unternehmens. Wenn die Internetprovider ihre Einführungsprognosen einhalten, wird wahrscheinlich mehr als die Hälfte der Bevölkerung bis Ende 2023 über eine native IPv6-Verbindung zu Hause und über ihr Mobiltelefon verfügen. In einigen Ländern wird IPv6 bereits für weit mehr als die Hälfte der Kunden angeboten.

Auch wenn IPv4 in absehbarer Zeit nicht verschwinden wird, so ist es doch eine so knappe Ressource geworden, dass sie in immer mehr Fällen von mehreren Teilnehmern unter Verwendung verschiedener Mechanismen geteilt wird. Wenn Sie eine Internetverbindung vertraglich zugesichertem SLA nutzen, ist es wahrscheinlich, dass ein Providergerät die IPv4-Kommunikation die qualitativ beeinträchtigt. Hinzu kommt, dass die Unkenntnis mancher IT-Teams über diese IPv4-Mechanismen die Lösung von Konnektivitäts- und Dienstqualitätsproblemen erschweren kann, während eine IPv6-Verbindung von Ende-zu-Ende ohne Protokolltricks wie NAT44+PAT hergestellt wird.

Wichtig ist zu wissen, dass die Internetprovider dazu übergehen, IPv6 zum Standard auf ihrem öffentlichen Backbone zu machen und IPv4 nur als Dienst bereitzustellen, der mehr und mehr in gekapselter Form übertragen wird.

Wenn Ihr Unternehmen Dienste in Ländern anbietet, die über einen geringeren Bestand an IPv4-Adressen verfügen oder in denen die Gesetzgebung einfach fortschrittlicher ist, kann es notwendig werden, IPv6-fähig zu sein, um mit expandierenden Märkten Schritt zu halten oder um möglicherweise eine künftige gesetzliche Vorschrift zu erfüllen. Einige Länder wie Indien und Frankreich ermutigen ISP, ihren Kunden IPv6 zur Verfügung zu stellen, andere konzentrieren sich auf ihre eigene interne Verwaltung wie die USA und Belgien, China oder Deutschland diese drängen auf eine vollständige Umstellung bis 2025... Seit dem 1. Januar 2021 müssen Betreiber in Frankreich, die 5G-Frequenzen erworben haben, IPv6-Konnektivität anbieten, zumindest als Option.

Neben diesen Aspekten ist ein wichtiger Punkt, dass der IPv6-Transit jetzt realisierbar ist und sich qualitativ der IPv4-Qualität annähert.

Pionieranwender mussten vor Jahren feststellen, dass IPv6 ein Handicap war. Vor einem Jahrzehnt gab es viel weniger Transitstrecken, daher weniger Redundanz und das war suboptimal. Wie viele der frühen Anleitungen empfahlen zu Recht, IPv6 auszuschalten, um den Zugang zu einer bestimmten Website oder einem öffentlichen Streaming-Dienst zu lösen? Dies galt umso mehr, als es das Happy-Eyeballs-Protokoll noch nicht gab und die Browser IPv6-Fehler nicht innerhalb von Millisekunden retten konnten, wie es heute der Fall ist.

IPv6 ist heute kein "Handicap" mehr, das es einmal war: Ganz im Gegenteil, es ist ein Vorteil dank einer echten Ende-zu-Ende-Verbindung.

Außerdem ist die von Google in Frankreich, Kanada und mehreren anderen Ländern gemessene Latenzzeit heute über IPv6 besser als über IPv4, während 2018 noch das Gegenteil der Fall war. Während IPv6-Peering so gut wie IPv4 wird, läuft IPv4 jetzt oft über Carrier-Grade-NAT (CG-NAT), und zwar fast immer in Mobilfunknetzen. Ein kleiner Einflussfaktor für die Verbesserung der Latenzzeit ist die Abschaffung der bei IPv4 erforderlichen Prüfsummenprüfung an jedem Router entlang des IPv6-Pfads sowie die fehlende Fragmentierung durch Router.

Es ist daher wichtig, daran zu denken, dass IPv4 mehr und mehr in einer nicht nativen Weise über CG-NAT weitergegeben wird, insbesondere im Mobilfunk. Damit kommt ein Single-Point-of-Failure (SPOF) und damit ein weiteres Element hinzu, das die Nutzererfahrung beeinträchtigen kann. Die Bereitstellung Ihrer Dienste über IPv6 bedeutet, dass Ihre Kunden nicht mehr von den Übersetzungsinfrastrukturen der Internetprovider abhängig sind.

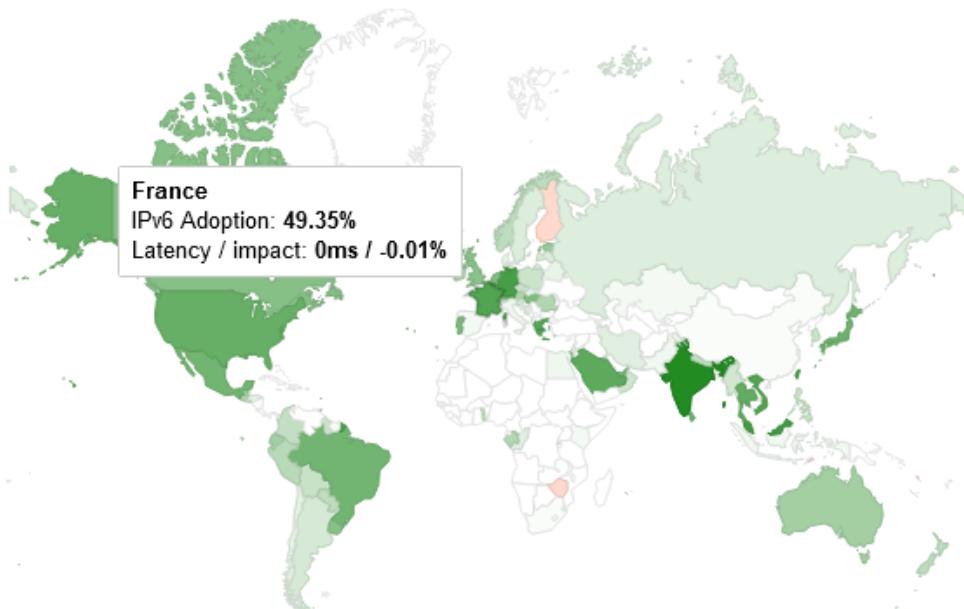


Abbildung 2. Statistiken für den Zugang zu Google-Diensten über IPv6 in Frankreich | Oktober 2021

Immer mehr Kunden erhalten Zugang zu IPv6-Netzen. In Frankreich und Deutschland wird deutlich mehr als die Hälfte der Anfragen auf Google-Dienste über IPv6 gesendet.

IPv4 Waiting List

LIRs in queue	579
Days that first LIR in queue has been waiting	52

We use a waiting list to allocate recovered IPv4 addresses to our members. The table above shows the number of requests already on the waiting list and the number of days that the LIR at the front of the queue has been waiting. This is also shown on the graph below, which should fluctuate over time - falling when recovered addresses become available and are allocated, and rising as new IPv4 requests are added to the waiting list. Both the table and graph are updated every three hours.

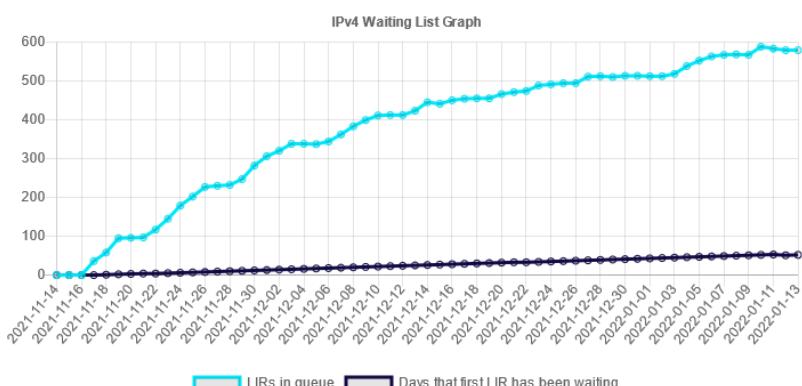


Abbildung 3. RIPE-NCC IPv4-Warteliste Januar 2022

Die Beschaffung von IPv4-Netzen wird immer schwieriger.

• ZUGRIFF AUF EXTERNE DIENSTE

Unabhängig von der Größe ist Ihr Unternehmen immer auch ein Kunde von Diensten Dritter. Hier nimmt die Zahl der IPv6-fähigen Websites und Dienste stetig zu. Der Benutzerverkehr wird in Unternehmen in der Regel über einen User-Proxy weitergeleitet, auch um den Datenverkehr zu filtern, zu schützen und Nachverfolgbarkeit sicherzustellen. Dieser unternehmensinterne Proxy-Dienst läuft in der Regel nur über IPv4, sowohl intern als auch ins Internet. Und das merkt man an der Google-Zugriffsstatistik.

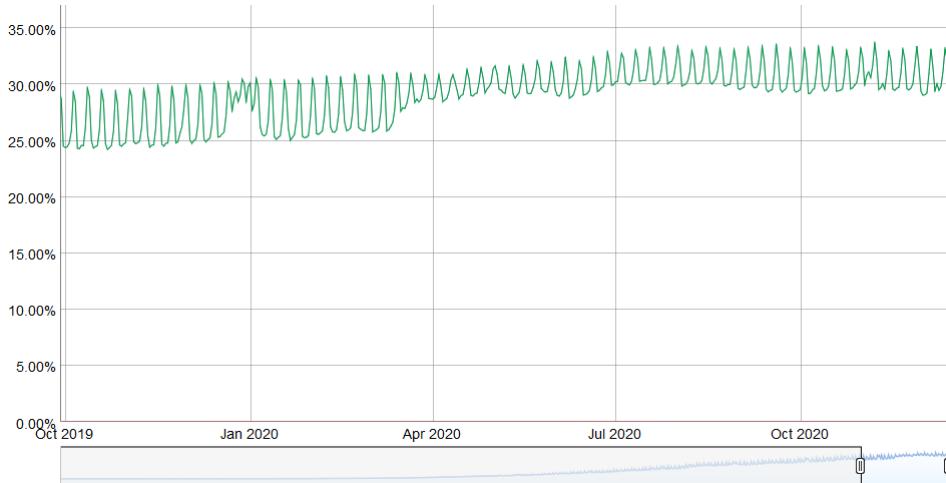


Abbildung 4. Prozentualer Anteil des weltweiten Datenverkehrs, der über IPv6 auf Google-Dienste zugreift

Das Verkehrsaufkommen während der weltweiten COVID-Maßnahmen im März/April 2021 war ähnlich wie in der Woche zwischen Weihnachten und Neujahr. Die prozentuale Veränderung liegt weiterhin im oberen Bereich. Und warum? Ganz einfach: Weil Menschen zu Hause häufiger einen Internetzugang mit IPv6 haben.

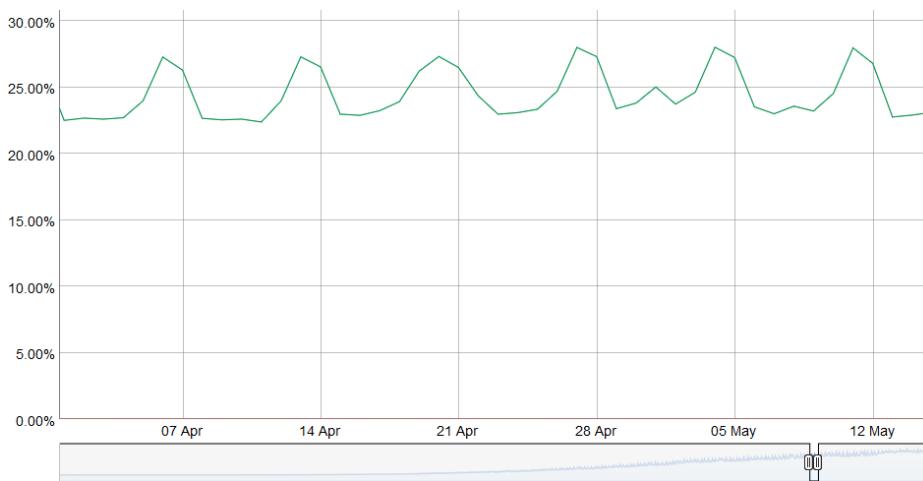


Abbildung 5. Prozentualer Anteil des weltweiten Datenverkehrs, der auf Google-Dienste über IPv6 zugreift, im Detail

Dieses Phänomen kann im Laufe einer Woche beobachtet werden: Hier von Ende April bis Anfang Mai 2019. Spitzenwerte treten immer an Wochenenden auf. Am 1. und 8. Mai, die in vielen Ländern arbeitsfreie Tage sind, kann man in den letzten beiden Wochen Hügel beobachten.

Bis zum Sommer 2024 wird die durchschnittliche weltweite IPv6-Verfügbarkeit voraussichtlich über 50 % liegen. Wird Ihr Unternehmen bis dahin Teil dieser Mehrheit sein?

QUIC ist angekommen

Lassen Sie uns die Gelegenheit nutzen, um einen entscheidenden Punkt beim Zugang zu Internet-Ressourcen anzusprechen und über die Herrschaft des "Connected Mode" zu sprechen. Mit "connected mode" meinen wir nicht die Sucht nach Hyperkonnektivität, sondern einfach Transport-Control-Protocol (TCP).

TCP hat sich dank seiner Kontrollmechanismen lange Zeit durchgesetzt, während UDP im Allgemeinen auf Echtzeitanwendungen beschränkt ist, bei denen eine erneute Übertragung nutzlos ist, wie z. B. bei Sprachübertragungen oder Online-Spielen. Aber, Verbindungen sind immer zuverlässiger, und die Integritätsprüfungen werden in den höheren Schichten für eine zunehmende Anzahl von Datenprotokollen durchgeführt.

Wenn wir also in den Schichten des OSI-Modells nach oben gehen, finden wir den wahrscheinlich größten Kunden von TCP, HTTP. Während HTTP/1.1 seit 1997 in Stein gemeißelt ist, brachte HTTP/2 20 Jahre später Priorisierung, Parallelisierung, Komprimierung und vorausschauendes Caching. HTTP/3 (RFC 9114) bringt eine Abspaltung mit sich, indem es sich von TCP trennt und sich auf ein neues Transportprotokoll, QUIC, stützt.

QUIC ist ein vollwertiges Transportprotokoll, das zwar in UDP verpackt ist, um den Einsatz zu erleichtern, aber das Beste aus beiden Welten vereinen will, indem es Mechanismen anbietet, die die Anzahl der Client/Server-Aushandlungen erheblich reduzieren, und darüber hinaus eine Symbiose mit TLS bildet, das jetzt direkt eingebettet ist. Es zielt daher darauf ab, sichere, parallelisierbare Verbindungen anzubieten und gleichzeitig die Anzahl der Datenpakete und damit der Latenz zu reduzieren.

Einige Anbieter drängen bereits auf UDP in Unternehmen, insbesondere für Kommunikationslösungen. Diese Anbieter fordern ihre Kunden manchmal sogar auf, die Internet-IPv4-Netze der Konferenzdienste im internen Unternehmensnetz zu routen, um den Inhalt der SIP-Nachricht in den oberen Schichten nicht verändern zu müssen, damit UDP-Unterstützung anzubieten und auf jegliche Zwischenverarbeitung zu verzichten. Wie viele Leute haben während des Lockdowns bemerkt, dass diese Lösungen zu Hause auf ihrem eigenen Schreibtisch oder auf ihrem Geschäftsarbeitsplatz besser funktionieren, wenn sie Split-Tunneling VPN anbieten?

Was ist, wenn diese Cloud-Diensteanbieter morgen QUIC und damit UDP für andere Dienste einsetzen? Was müssen Sie tun?

Und nicht nur HTTP/3 bewegt sich in Richtung QUIC, auch das weit verbreitete Netzwerksfreigabeprotokoll SMB macht diesen Sprung, wobei Microsoft an der Implementierung in Azure Files und Windows Server arbeitet.

Werfen Sie einen Blick auf Ihr Netflow-Monitoring, um zu sehen, wie hoch der kumulative Anteil von HTTP(s) und SMB in Ihrem Netzwerk ist. Ein Hinweis: Er ist höchstwahrscheinlich hoch...

Derzeit empfehlen die Firewall-Anbieter, QUIC zu deaktivieren, bis die Unterstützung ordnungsgemäß implementiert ist. Auch die Geräte, die den Datenverkehr entschlüsseln, müssen angepasst werden, da sie bisher auf das TCP+TLS-Paar abgestimmt sind.

Die Neugestaltung Ihrer Egress-Pfade zum Internet bietet die Möglichkeit, IPv6 einzusetzen, was jegliche Paketverarbeitungsschritte auf Proxys beschränken würde.

NAT+PAT vieler QUIC-Streams ist eine Herausforderung. Wenn der Gerätethersteller Application Layer Gateways einführt, um eine spezifische Verarbeitung auf QUIC-Sitzungen anzuwenden, riskiert er, einen Teil seiner Sicherheit zu gefährden. Der RFC-Entwurf draft-duke-quic-natsupp-01 empfiehlt, dass bei NAT keine Optimierung versucht werden sollte.

Auch diese Probleme werden durch eine IPv6-Sitzung beseitigt. Ist das trivial? Denken Sie an die Probleme, die Sie persönlich in Ihrem Heimnetzwerk mit NAT und UDP für dynamische Anforderungen wie Multiplayer-Spiele, P2P oder VoIP in den ersten Tagen erlebt haben. Eine Lösung ist die Beibehaltung von HTTP/2 über TCP, aber für wie lange? Eine Übergangslösung könnte darin bestehen, QUIC ohne Deep Packet Inspection zunächst nur für vertrauenswürdige SaaS-Angebote zuzulassen. Vergessen wir nicht, dass QUIC noch viele andere Dinge als HTTP übertragen kann.

Beachten Sie, dass diese Elemente auch für den Zugriff auf Ihre Ressourcen durch andere Personen oder durch Ihre externen Mitarbeiter gelten. Daher führt der Weg der so genannten "Zero-Trust"-Lösungen zur Abschaffung von VPNs und einer direkteren Offenlegung von Ressourcen, die sich auch auf QUIC verlagern wird.

Dieses Protokoll wurde gerade in RFC 8999, 9000, 9001 und 9002 ratifiziert.

Hinweis zum Proxy: Um von seinen Beiträgen profitieren zu können, muss die Proxyfizierungsschicht sowohl auf der Browser- als auch auf der Proxyseite aufgerüstet werden. Es gibt zwei Modi: einen Tunnelmodus, der effizienteste und der einzige, der den anfänglichen Austausch einer QUIC-Sitzung (mit langem Header) unterstützen kann und einen Vorwärtsmodus, bei dem der Proxy die Rolle des Protokollunterbrechers beibehält, aber erst, wenn die Sitzung aufgebaut ist.



Es wird erwartet, dass das QUIC Transportprotokoll eine schnellere Einführungskurve hat als IPv6. Die Anstrengungen, die unternommen werden, um es in seiner Proxy-Kette oder in seinen Web-Frontends zu unterstützen, sind eine Gelegenheit, parallel an der Einführung von IPv6 zu arbeiten.

• INTERNES NETZ

Was sind die Beweggründe für den Einsatz von IPv6 im internen Netz?

Wie in den vorangegangenen Abschnitten beschrieben, ist die durchgängige Verarbeitung in Zeiten der zunehmenden Auslagerung von Cloud-Ressourcen eindeutig ein Vorteil. Auch hier werden die Anbieter bestimmter Produkte wahrscheinlich Lösungen fördern, die die Zwischenverarbeitung von Paketen einschränken. Beachten Sie, dass die IPv6-Header-Struktur einige Verzögerungen durch die Entfernung der Prüfsumme, die Verwendung von Feldern fester Größe und die Einbeziehung von Flowlable zur einfacheren Verfolgung von Flows während der QoS-Verarbeitung bietet.

Für große Strukturen bedeutet IPv6 auch die Beseitigung der Probleme, die durch die geringe Größe der privaten IPv4-Adressierung verursacht werden.

RFC 1918 bietet 17 891 328 IPv4, das sind nur 70 000 Netze in /24. Viele Organisationen haben die Bestandsgrenze bereits erreicht, und zwar aus mehreren Gründen. Zuteilung nach Unternehmen,

Verschwendungen und Überzuteilung, Nichtabruf von Adressen bei der Stilllegung von Geräten oder Standorten, Wunsch, Routen aus einer Zeit zusammenzufassen, in der Router nur eine kleine Anzahl von Routen unterstützten, Weitergabe an Tochterunternehmen, die weiterverkauft wurden, aber noch über Verbindungen verfügen, usw.

NAT44 kann zwar Verbindungen zu Partnern und neu erworbenen Unternehmen auf komplizierte Weise aufnehmen, doch ist es oft undenkbar, das eigene Unternehmen in sich überschneidende Bereiche aufzuteilen, obwohl auch dies eine Möglichkeit wäre.

Andere nehmen den Weg der "Aneignung von IP-Netzen" und nutzen in ihrem internen IPv4-Netze, die anderen gehören, mit mehr oder weniger Fingerspitzengefühl aus. Es gibt zwei Gruppen:

- Die Vorsichtigen, die doppeltes NAT44 einsetzen und so ein echtes separates Routing am Internetnetzübergang schaffen. Der Verkehr wird zweimal genattet und kann leicht dieselbe Quell- und Ziel-IP haben, wobei das NAT ein anderes NAT maskiert, die Verwirrung ist total; Diese vorsichtigen Leute sind ratlos, wenn ein Cloud-Anbieter ihnen empfiehlt, die öffentliche IP eines Dienstes in ihrem internen Backbone zu routen. Was, wenn sich diese echte öffentliche IP mit einer gefälschten LAN-IP überschneidet? Zumal ein Anbieter neue IPs mit nur wenigen Wochen Vorlaufzeit einführen kann. Science-Fiction-Szenario? Ganz und gar nicht! Ein perfektes Beispiel ist die Verwendung der Kommunikationslösung TEAMS von Microsoft. Der Hersteller empfiehlt, seine öffentlichen IPs bekannt zu geben, aus Gründen, die weiter oben in diesem Dokument erläutert wurden.
- Die Naiven, die IPs nutzen, die niemals im Internet veröffentlicht werden, wie die des US-Verteidigungsministeriums (DoD): 6.0.0.0/8 7.0.0.0/8 11.0.0.0/8 21.0.0.0/8 22.0.0.0/8 26.0.0.0/8 28.0.0.0/8 29.0.0.0/8 30.0.0.0/8 33.0.0.0/8 55.0.0.0/8 214.0.0.0/8 215.0.0.0/8

Nun, das ist nur theoretisch so, da Ende 2019 Abschnitt 1088 des Haushaltsentwurfs des Verteidigungsministeriums vorsah, dass diese ungenutzten IPv4-Netze innerhalb von 10 Jahren verkauft werden würden. (Siehe Anhang) Der Gesetzentwurf wurde jedoch vom Senat nicht angenommen. Aber was ist mit der Zukunft?

Sollten diese Adressen zum Verkauf stehen, würden zweifellos einige in den Händen großer Cloud-Anbieter landen.

Sehr kurz nach der Amtseinführung von Joe Biden begann AS 8003, über Hurricane Electric BGP-Announcements für DoD-IPs zu machen. Offiziell wurde der Washington Post Folgendes dazu berichtet:

Der Digitale Dienst des Verteidigungsministeriums (DDS) hat ein Pilotprojekt zum Announcement von DoD-Internetprotokoll-(IP)-Raum unter Verwendung des Border Gateway Protocol (BGP) genehmigt. Dieser Pilotversuch wird die unbefugte Nutzung des DoD-IP-Adressraums bewerten, evaluieren und verhindern. Darüber hinaus kann dieses Pilotprojekt potenzielle Schwachstellen aufzeigen. Dies ist eine der vielen Bemühungen des DoD, die sich auf die kontinuierliche Verbesserung unserer Cyber-Stellung und -Verteidigung als Reaktion auf fortschrittliche anhaltende Bedrohungen konzentrieren. Wir arbeiten im gesamten DoD zusammen, um sicherzustellen, dass potenzielle Schwachstellen entschärft werden._

Manche sprechen von der Sammlung von Datenverkehr zu Analysezwecken (ein Honeypot), während das DoD den Kampf gegen das Cybersquatting seiner IP-Bereiche hervorhebt. Aber was

wäre, wenn es einfach darum ginge, die Umsetzung des obigen "vorsichtigen" Szenarios innerhalb des DoD selbst zu testen? Und zu simulieren, dass der Verkauf und die Werbung für diese zahllosen IPv4-Netze keine Welleneffekte verursachen würden, bevor sie tatsächlich zum Verkauf freigegeben werden?

Im Juni 2021 hat das DoD [angekündigt](#), dass alle neuen Dienste, die nach den Meilensteinen eingeführt werden, in IPv6 sein sollen.

Am 7. September 2021 wird die überwiegende Mehrheit der Präfixe auf AS749 umgestellt, das dem Verteidigungsministerium gehört, sich aber von seinem üblichen Präfix AS721 unterscheidet.

Wenn Sie sich dem Ende von RFC 1918 nähern, können Sie die Verwendung des für Carrier NAT44 reservierten Bereichs RFC 6598 100.64/10 als eine Möglichkeit zur gemeinsamen Nutzung von IPv4 zwischen Teilnehmern mit einem Carrier Grade NAT untersuchen. Es wird jedoch empfohlen, diese Adressen nicht an Carrier-Geräte wie MPLS-Router zu vergeben oder sie in Cloud-Infrastrukturen zu verwenden, es sei denn, der Provider hat seine Zustimmung erteilt. Es ist es kein Problem, diesen Bereich z. B. für Campus-Netze zu verwenden. Einige Unternehmen tun dies bereits.



Der Bereich 100.64/10 wird de facto von einigen Overlay-Systemen wie der Zscaler Cloud-Proxy-Lösung zum Aufbau von Tunneln verwendet.

Wenn Sie eine Spielernatur sind, können Sie schließlich versuchen, die frühere IPv4 Klasse E (240/4) zu verwenden. Diese IPv4 Klasse befindet sich an der hinteren Grenze von IPv4, hinter dem Multicast-Bereich. Sie ist für eine künftige Nutzung reserviert, die nie eintreten wird, und wird von den Anbietern nicht genutzt, die erkannt haben, dass die zur Standardisierung dieses Bereichs erforderliche Arbeit länger dauern würde, um alle eingesetzten Geräte zu erreichen, als die Umstellung auf IPv6. Im wirklichen Leben sollten Sie es nicht ausprobieren, außer im Labor aus reiner Neugier. Google's GCP erlaubt die Verwendung auf VPC, erwähnt aber mögliche Probleme mit dem Betriebssystem: <https://cloud.google.com/vpc/docs/vpc#valid-ranges>. Sie geben jedoch nicht an, dass Sie möglicherweise nicht einmal in der Lage sind, solche Präfixe auf Ihren BGP-Routern vor Ort zu lernen, obwohl mindestens zwei Anbieter diesen Bereich über einen Befehl unterstützen.

Die Anwendung eines der oben beschriebenen "Schummel"-Szenarien zur Verlängerung der privaten Adressierung oder der kurze Zeithorizont des Erreichens des Endes des RFC 1918-Pools (weniger als ein paar Jahre bei Ihrer Verbrauchsrate) sollte Sie dazu veranlassen, eine IPv6-Einführung ernsthaft in Erwägung zu ziehen.

Denken Sie an die Zeit, die für vergangene und zukünftige NAT44- und Umadressierungsprojekte im Zusammenhang mit der Eingliederung neu erworbener Unternehmen aufgewendet wurde. Haben Sie schon einmal erlebt, dass eine IT-Abteilung beschlossen hat, ihre interne Adressierung mit dem 10.255.0.0/16-Block abwärts zu beginnen, weil ihr Unternehmen eines Tages übernommen werden würde und die neue Muttergesellschaft hoffentlich ihre Adressierung mit 10.0.0.0 begonnen hätte? Schlimmer noch, IP-Adressierungskonflikte während der Strukturintegration verursachen Kosten und Verzögerungen, die oft beträchtlich sind, zusätzlich zu der zusätzlichen Komplexität für den langfristigen Betrieb, falls NAT44 bestehen bleibt.

In this example of mobile connection sharing, IPv4 traffic is altered 3 times!
IPv6 traffic is simply tracked by the destination firewall.

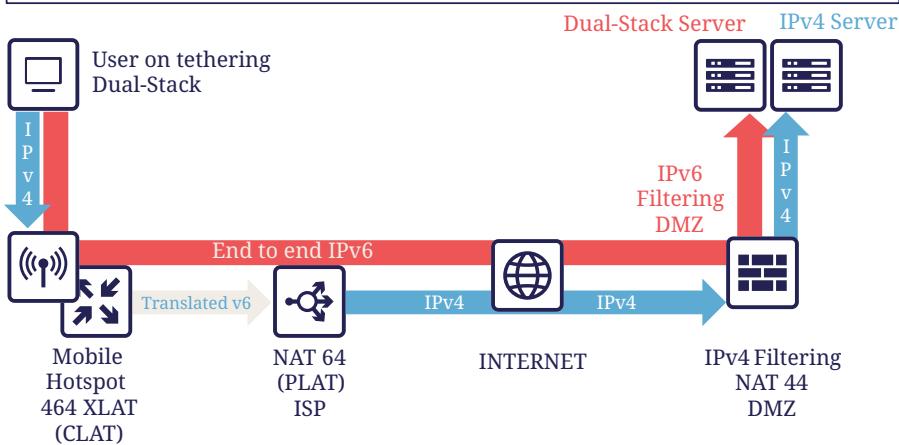


Abbildung 6. Tethering am Smartphone

Teil II: Transition Techniken



Transition Techniken

Die Internet Engineering Task Force (IETF) arbeitet mit Anbietern und Softwareherstellern zusammen, um Mechanismen für den Übergang zu IPv6 bereitzustellen. Diese Mechanismen sind für Netzbetreiber und/oder Unternehmen gedacht.

Zunächst müssen wir die Mechanismen in zwei Verwendungsgruppen unterteilen:

- Diejenigen, die den Transport eines Datenpaketes in ein IP-Netz einer anderen IP-Version ermöglichen. Sie werden in der Regel verwendet, um IPv6-Inseln über IPv4-Transportnetze zu verbinden (oder umgekehrt). Es gibt Systeme, die auf Kapselung und andere, die auf Übersetzung basieren.
- Diejenigen, die es ermöglichen, dass IPv4-Hosts mit IPv6-Hosts kommunizieren oder umgekehrt. Sie beruhen notwendigerweise auf Übersetzung.

Beide ergänzen sich in den meisten Anwendungsfällen.

Dual-Stack

IP-Dual-Stack ist die gleichzeitige Nutzung von IPv4 und IPv6, deren Kooexistenz.

Die parallele Ausführung von IPv4 und IPv6 verursacht jedoch nicht nur für das Netz mit doppelten Routing-Konfigurationsaspekten oder Firewall-Regeln einen Zusatzaufwand. So müssen beispielsweise alle Systembereitstellungsprozesse parallel in v4 und v6 ablaufen. Die Überwachung der Dienstqualität erfordert, dass jeder Dienst sowohl in IPv4 als auch in IPv6 überwacht wird, usw.

Dual-Stack ist daher in einer großen Organisation außerhalb der Netze, in denen die Client-Terminals untergebracht sind, und damit typischerweise auf dem Campus, auf Dauer kaum tragfähig.

Während der Übergangsphase wird IP-Dualstack IPv4-only-Systeme nicht stören, so dass es zu keinen Unterbrechungen oder Störungen bei den Diensten kommt.

Transportmechanismen

In der Anfangszeit von IPv6 wurden Mechanismen entwickelt, um IPv6-Inseln von anderen IPv6-Inseln oder einfach von einem IPv4-Arbeitsplatz aus zu erreichen.

Zu diesen Methoden gehören ISATAP (RFC 5214), Teredo (Microsoft - RFC 4380), 6over4 (RFC 2529), 6to4 (RFC 3056), 6in4 + TB/TSB (RFC 5572), 6rd (RFC 5969), IPv6 GRE (RFC 2473 / 2784), und viele mehr...

Die meisten dieser auf Tunnels basierenden Lösungen verwenden das IP-Protokoll 41 und/oder die UDP-Kapselung, wie es auch bei einem VPN der Fall wäre.

Diese Mechanismen sind nützlich für Strukturen, bei denen die Migration einiger oder aller Teile des Netzes aus technischen Gründen unmöglich ist. Die Netzbetreiber haben sie genutzt, um Fälle zu überwinden, die IPv6 nicht unterstützen, wie z. B. Kabelbetreiber vor DOCSIS 3.1.

Wie bei jeder Tunneltechnik ist der größte Nachteil die mangelnde Sichtbarkeit des Datenverkehrs aufgrund der Kapselung. In Unternehmen erschweren die Anforderungen an die Filterung und die Verwaltung des QoS den Einsatz von Tunnels aufgrund der Komplexität und der geringen Anzahl kompatibler Lösungen, insbesondere von Firewalls.

Die meisten dieser Methoden bergen Sicherheitsrisiken für das Unternehmen und sind auf den Internetprovider ausgerichtet.

In Transportnetzen werden häufig mehrere Technologien übereinander geschichtet, wie dies bei MPLS oder VxLAN der Fall ist. Der Einsatz von Dual-Stack auf allen Transportschichten ist selten sinnvoll. Es ist jedoch wichtig, dies in der höchsten Transportschicht zu implementieren, derjenigen, die für die Netznutzer sichtbar ist, dem Overlay.

• INTEGRATION IN EINEM IPV4 UNDERLAY

Das Unternehmensnetz ermöglicht häufig die Isolierung von End-to-End-Kundenkontexten innerhalb des Unternehmens, sowohl im Backbone als auch im Rechenzentrum.

Während *VRFs lite* auf dem Campus noch vorherrschend sind, werden in den anderen Umgebungen massiv Underlay-basierte Technologien eingesetzt. Es ist dann relativ einfach, IPv6 im Overlay zu übertragen.

MPLS

MPLS ist eine Schlüsselkomponente, die häufig in Unternehmen vorhanden ist, entweder direkt oder in ausgelagerter Form über die Standortzusammenschaltung professioneller Netzbetreiber.

MPLS ermöglicht die Übertragung von IPv6 auf zwei Wegen:

- 6PE (Provider Edge RFC 4798), das v6 in der nativen Tabelle (GRT) der Geräte bereitstellt, nützlich nur, wenn man Dienste über die GRT anbietet (wie Internetzugang oder TV für einen Kunden-ISP);
- 6VPE (RFC 4659), V macht den Unterschied, hier wird einfach VPNV6 neben VPNV4 transitiert, es

ist also das Äquivalent eines L3VPN, die einfachste Methode, die die meisten Anwendungsfälle erfüllt.

Es ist in der Tat möglich, einen IPv6-IGP und LDPv6 zu verwenden, um ein IPv6-Underlay-basiertes MPLS aufzubauen, aber es gibt wenig Nutzen, abgesehen von einer Gelegenheit, die ein weiteres großes Projekt bietet. Vor allem bietet dies kein v6 im L3VPN des Overlay, was das Hauptthema ist, um den Benutzern v6-Zugang zu ermöglichen.

Die 6VPE-Implementierung ist der richtige Weg, denn sie lässt sich leicht auf den aktuellen Geräten einrichten und erfordert nur wenig Konfiguration.

Wenn Ihr MPLS das neue MP-BGP EVPN als Steuerebene anstelle von MP-BGP L3VPN verwendet, ist die IPv6-Unterstützung auch dort kein Problem.

Beachten Sie, dass Sie dank RFC 8950 einen IPv6 Next Hop für IPv4 VPN-Routen haben können, wenn Sie sich für ein IPv6 Underlay entscheiden.

VXLAN

VxLAN wird meist in Verbindung mit EVPN verwendet und löst die Probleme älterer DataCenter Layer-2 SPB Fabrics und hat sich zum Industriestandard entwickelt. Seltener findet man es in Backbones, die MPLS aufgegeben haben, um die Vorteile von EVPN zu nutzen, das vor MPLS als *Controlplane* für VxLAN verfügbar war.

Wie MPLS kapselt auch VxLAN. Daher stellt sich die Frage nach der IPv6-Kompatibilität in dem Overlay, das für die Bereitstellung von Kundendiensten vorgesehen ist. Die Konfiguration eines IPv6-Overlays ist bei den großen Anbietern ausgereift, dennoch ist zu prüfen, ob die Multicast-Mechanismen vollständig unterstützt werden (PIM Snooping, BiDir usw.).

Während das Underlay in IPv4 bleiben kann, ist zu beachten, dass die IETF an der Implementierung von RIFT (Routing in Fat Tree) arbeitet, um den Einsatz von *CLOS Fabrics* im Sinne von Zero Touch Provisioning zu erleichtern. Es zielt auf Fabrics mit iBGP Underlay ab und sieht vor, dass Loopback-Adressen und *Route Reflectors* in IPv6 sein sollten. Es ist schwer zu sagen, ob dies abgeschlossen sein wird, bevor die Fabrics auf SRv6 migrieren (RIFT bietet auch einen Mechanismus für den Austausch von Node-SIDs und SRGB Global Segment Routing Prefixes, um den Einsatz zu erleichtern). Siehe <https://datatracker.ietf.org/wg/rift/documents/>.

SD-WAN

SD-WAN-Produkte arbeiten in der Regel mit DPI und Klassifizierung *ingress*, um QoS anzuwenden und einen Pfad (Internet/MPLS usw.) auszuwählen. Der Datenverkehr wird dann häufig in einem IPSEC-Tunnel verschlüsselt, der für den Client-Kontext spezifisch ist, und an den Zielrouter gekapselt (es sei denn, eine Analyse erfordert beispielsweise die Entkapselung am Hub).

Das Underlay ist so konzipiert, dass es ein bestehendes IPv4-basiertes Netz nutzt, um den Aufwand für die Implementierung dieser Art von Produkt zu begrenzen.

Diese Produkte zielen hauptsächlich auf große Netze ab, die aus kleinen und mittelgroßen Standorten bestehen, mit einer dedizierten Gerätelinie und/oder Integration in bekannte Produktlinien. Auf der Seite der Rechenzentrumskonzentratoren finden wir große Chassis,

ebenfalls aus dedizierten oder bekannten Produktlinien.

Wenn man einige der marktführenden Lösungen auf einem Campus mit mehr als 2000 Nutzern einsetzen will, stößt man oft an die Grenzen dedizierter Produkte, obwohl die Hersteller Fortschritte machen und versuchen, auch das letzte Perzentil der fehlenden Nutzungen abzudecken.

Tatsache ist, dass IPv6 von den Kunden nur selten benötigt wird, da diese Lösungen für ihr internes Netz bestimmt sind. Daher variiert die Kompatibilität der auf dem Markt befindlichen SD-WAN-Lösungen stark von einem Anbieter zum anderen und zwischen den verschiedenen Versionen. Daher ist es wichtig, die Roadmap des Anbieters zu befolgen und die Lösung vor einer v6-Einführung zu testen, aber auch bei jeder neuen Hauptversion, da der Code angesichts der schnellen Entwicklung dieser Lösungen und der Konkurrenz stark verändert werden kann.

Schließlich ist der Local-Internet-Breakout-Aspekt dieser Lösungen ein weiteres Element, das ebenfalls schrittweise IPv6 integriert. Oft mit einer ganzen Schicht von lokalen Sicherheitsdiensten, die gemeinhin als "SASE" bezeichnet werden.

• TUNNELLÖSUNGEN

Es ist nicht immer möglich, IPv6 an einer Transportgrenze durchzulassen, und wie bereits erwähnt, sind nur wenige technische Lösungen auf beiden Seiten der Unternehmens-Hardwareserie nutzbar.

Es bleibt also die Möglichkeit, den IPv6-Verkehr zu tunneln. Dies kann über bekannte Lösungen wie GRE/mGRE oder IPsec erfolgen (letzteres ist jedoch aufgrund der erforderlichen Verschlüsselungsressourcen weniger effizient).

Schließlich können Sie 6in4 auf einem Großteil der auf dem Markt befindlichen Router konfigurieren, wenn Sie mit keiner der oben genannten Lösungen zufrieden sind. 6rd ist ebenfalls häufig verfügbar, zielt aber hauptsächlich auf Nord-Süd-Topologien ab.

Wir raten davon ab, 6to4 (nicht konfigurierbarer Endpunkt), 6over4 (IPv4-Multicast-basiert), ISATAP (basiert auf DNS) und Teredo (UDP-Kapselung) zu berücksichtigen, die nur noch sehr selten verwendet werden.

Die Verfügbarkeit einer bestimmten Methode auf Ihren Geräten in Verbindung mit der Integration mit Ihrem Routing wird Ihre Wahl bestimmen.

• UND IPv6-ONLY?

Wie zu Beginn dieses Kapitels erwähnt, gibt es auch Möglichkeiten, auf IPv4 in Ihrem Backbone zu verzichten. Es beschränkt sich dann auf Nutzernetze, IPv4-as-a-Service, IPv4aaS.

Einige Betreiber gehen bereits dazu über, IPv4 in ihrem Backbone wegzulassen, um IPv4-Adressen einzusparen und sogar IPv4-Adressen zwischen Teilnehmern zu teilen, indem sie Ports aufteilen. Die so genannten Address+Port (AP)-Ansätze sind inzwischen weit verbreitet. Zuerst DS-Lite, dann *Lightweight 4over6* (lw4o6) und in letzter Zeit MAP T/E und 4rd. Die beiden letztgenannten überwiegen bei den heutigen Installationen dank ihrer Aggregationskapazität, die es vermeidet,

eine astronomische Anzahl von Tunneln und ebenso viele Routen im Kernnetz des Internetproviders anschließen zu müssen.

Diejenigen, die noch nicht zu einem IPv6-Backbone übergegangen sind und denen es an verfügbaren IPv4-Adressen mangelt, verwenden einfaches NAT44 auf einer CGN-Kernplattform und nutzen den berühmten 100.64/10-Bereich von RFC 6598.

Diejenigen, die IPv6-only im Backbone nutzen, stellen IPv4 in der Regel über eine der folgenden Methoden bereit:

- 4rd (RFC 7600), das im Gegensatz zu 6rd funktioniert und eine effiziente zustandslose Methode bietet. Es kann im Mesh- oder Hub&Spoke-Modus arbeiten
- MAP (T oder E) (RFC 7599), verfügbar im Übersetzungs- und Kapselungsmodus, ist ebenfalls zustandslos;
- Ältere Implementierungen verwenden DS-Lite und Lw4o6.

Die ersten beiden sind recht ähnlich und verwenden gemeinsame Regeln für eine Domäne, Edge-Router (BR), EA-Bits zur Festlegung der IP-Sharing-Ebene und die Bekanntgabe von Zuordnungsregeln über DHCP an die Endgeräte (CPE).

Die Implementierung dieser Techniken auf der Client-Router-Seite erfolgt in Software, sie sind in unseren Heimroutern zu finden. Es ist jedoch unwahrscheinlich, ein Gerät zu finden, das MAP oder 4rd über seinen ASIC auf der Client-Seite handhaben kann, da High-End-Geräte sich nur mit dem Border-Router-Aspekt befassen.

Was MPLS und VxLAN betrifft, so ist es möglich, IPv4 durch IPv6 auf dem Transport-Underlay zu ersetzen. Sie sollten dies bei der Einführung nur auf der grünen Wiese in Betracht ziehen und erst nach Rücksprache mit Ihrem(n) Anbieter(n).

In besonderen Situationen, in denen der Transport von IPv4 unmöglich ist, gilt das Gleiche wie zuvor. Spezielle Tunnel, um IPv4-Inseln miteinander zu verbinden. So können wir GRE/mGRE und 4in6 einsetzen. 4in6 scheint in Unternehmensroutern noch nicht sehr präsent zu sein.



Sie können IPv6 oft problemlos auf einem IPv4-Underlay transportieren und sollten vielleicht auf ein großes Backbone-Projekt, eine Erneuerung,... warten, um Ihr Underlay auszutauschen. Wenn Sie auf der grünen Wiese starten, sollten Sie ein IPv6-Underlay in Betracht ziehen. Außerdem sollten Sie Ihre Topologie und Ihren Adressierungsplan so gestalten, dass Sie für eine SRv6-Einführung gerüstet sind. Das spart Ihnen später Zeit, wenn Sie nicht jetzt damit starten.

Übersetzungsmechanismen

Der Zweck der IP-Übersetzung besteht darin, den Austausch zwischen Clients und Servern zu ermöglichen, die unterschiedliche Versionen von IP verwenden.

Wenn wir uns an die Dual-Stack-Logik halten, müssen wir überall IPv6 einsetzen. Dies führt jedoch zu einer Menge doppelter Arbeit und funktioniert nur, wenn alle Systeme Dual-Stack-kompatibel sind. Wie kann man IPv6-Clients mit IPv4-Servern kommunizieren lassen? (oder in umgekehrter Richtung)

NAT64 und DNS64 bieten eine gemeinsame Lösung, die bereits weit verbreitet ist und IPv6-Clients den Kontakt zu IPv4-Servern ermöglicht. Umgekehrt ermöglicht SIIT (Stateless IP/ICMP Translation Algorithm) IPv4-Clients den Zugang zu einem reinen IPv6-Netz.

Da der IPv6-Header länger ist, ist es technisch einfacher, die Header-Informationen beim Senden von IPv4-Clients an einen IPv6-Server beizubehalten als umgekehrt. Die Richtung der Einführung ist jedoch eine Frage des Bedarfs, der Strategie, der Zeitplanung und der Konsistenz.

• NAT64 + DNS64

NAT64 (RFC 6146) in Verbindung mit DNS64 (RFC 6147) nutzt das Prinzip des "lügenden" DNS in Verbindung mit einem Übersetzer, um IPv6-Endgeräten den Zugang zu IPv4-Ressourcen zu ermöglichen. Die IETF veröffentlicht einen Leitfaden für den Einsatz (RFC 7269).

Wenn eine Ressource keinen DNS-AAAA-Eintrag hat, synthetisiert der DNS-Server einen aus einem IPv6 /96-Präfix und der im DNS-A-Eintrag zurückgegebenen IPv4 /32-Adresse.

Der Anfragende stellt dann eine Verbindung zu einem synthetischen IPv6-Ziel her.

Irgendwo im Netz (wir werden später sehen, wo) wird ein Gerät, das das Präfix /96 verwaltet, die Verbindung empfangen. Diese NAT64-Plattform entfernt das IPv6/96-Präfix aus dem Ziel und ersetzt den IPv6-Header durch einen IPv4-Header. Dabei wird das Paket mit NAT versehen, eine Quelladresse aus dem NAT-Pool ausgewählt (zusammen mit einem Quellport für den PAT) und das Paket gesendet. Durch das Führen einer Sitzungstabelle führt er die umgekehrte Operation für das zurückkehrende Paket durch.

Beachten Sie, dass der Endpunkt zu keiner Zeit von dem Trick weiß. Dies führt zu Problemen bei P2P-Protokollen sowie bei Protokollen, die die Adresse in die Payload einbetten, wie z. B. SIP, H323, IPSEC AH, SCCP, NFS älter Version 4 usw. Funktionen können als ALG auf NAT64-Plattformen implementiert werden, um das Problem zu lösen, allerdings möglicherweise auf Kosten einer schlechteren Performance.

Die DNSSEC-Validierung durch den Host wird durch dieses Szenario ebenfalls verhindert. Dieses Problem könnte gelöst werden, wenn der Host von NAT64 wüsste (was bei Mobiltelefonen mit APN-Konfiguration der Fall ist oder wenn RFC 7050 verwendet wird, aber letzteres ist bei Desktop-Betriebssystemen nicht sehr nützlich, da sie es noch nicht unterstützen. Es besteht auch der Wunsch, Hosts über DHCPv6 und PCP über das NAT64-Präfix zu informieren).

Auf der Seite der Anwendung funktioniert NAT64, solange sie IPv6-Sockets öffnen kann und einen

Hostnamen und nicht eine direkte IP-Adresse aufruft.

Adressierung

In einem kleinen Netz reicht eine einzige Plattform aus, die in der Regel das WKP-Präfix (RFC 6052 Well Known Prefix) oder ein anderes Präfix (Network Specific Prefix) verwendet, das im Rahmen der Adressierung des Unternehmens mit einem /96 definiert wird.



Beachten Sie, dass bei Verwendung eines ULA-Präfixes NAT64 im Vergleich zu IPv4 immer benachteiligt wird.

Vergessen Sie bei Ihrem Projekt nicht, dass 99% der Verbindungen vom Client-Endpunkt initiiert werden, aber es gibt auch Sonderfälle wie die Fernsteuerung durch den Support. Und natürlich die P2P-Telefonie. Diese erfordern volle IPv6-Kompatibilität.

In einem großen Netz ist es vorteilhaft, mehrere NAT64-Instanzen zu haben, von denen jede ihr eigenes NAT64-Präfix hat. Zu diesem Zweck ist ein Bereich reserviert, der jedoch nicht zwingend erforderlich ist: 64:ff9b:1::/48 (RFC 8215).

Topologie

Die Platzierung dieser NAT64-Instanzen hängt von den jeweiligen Gegebenheiten ab.

Wenn Sie sie direkt an Ihren Standorten einrichten, vermeiden Sie das die Kommunikationsstrecken ins Rechenzentrum. Dazu müssen jedoch so viele NSP-Präfixe verwendet werden, wie Sie Standorte haben, und die DNS64-Konfiguration muss jedes Mal angepasst werden. Über einen entsprechend konfigurierten DNS-Proxy an jedem Standort. (Dies kann *Bind9*, *Unbound* oder eine andere Lösung sein.)

Es ist auch möglich, an jedem Standort dasselbe Präfix zu verwenden, solange es sich um Sackgassen handelt und die Routenanzeigen zum Backbone den NSP filtern. Dies macht die DNS64-Konfiguration einfacher.

Die Einrichtung von NAT64 an den Standorten erfordert in jedem Fall die Beibehaltung eines IPv4-Transits im Backbone. Es ist zu beachten, dass es ohnehin schwierig sein wird, diesen schnell wieder loszuwerden, da die Standorte selten nur Endgeräte enthalten. Die Einrichtung von NAT-Sitzungen an X Standorten bedeutet auch, dass an allen Standorten Sitzungen protokolliert werden müssen. Schließlich müssen zahlreiche NAT-IPv4-Pools eingerichtet und die ACLs zur Filterung angepasst werden.

Andererseits erleichtert die Zentralisierung die Umsetzung auf allen Ebenen, ist aber nicht wünschenswert, wenn sie zu einer Verlangsamung von Datenströmen führt, die innerhalb der Standorte hätten bleiben können.

Ein guter Kompromiss besteht darin, NAT64-Gateways an den größten Standorten einzusetzen, insbesondere an solchen, die Dienste lokal hosten und diese Dienste auch bei einem WAN-Ausfall funktionieren müssen. In anderen Fällen sollte es im Rechenzentrum oder am Backbone-Edge zentralisiert werden.

When users reach the IPv4 server, they use a DNS64 ~~and~~ synthesized record. Translation is done according to the chosen topology.

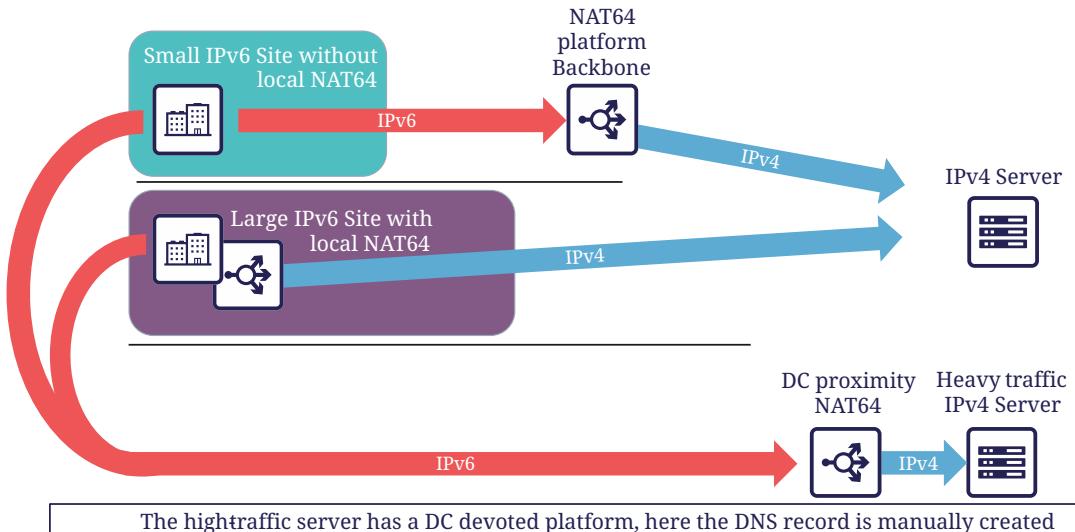


Abbildung 7. Die Verwendung von NAT64

MTU ist wichtig

Der IPv6-Header ist 20 Byte länger als der IPv4-Header, was bedeutet, dass ein großes IPv4-Paket, das zur NAT64-Plattform zurückkehrt, möglicherweise verworfen wird, wenn die Plattform die Fragmentierung nicht richtig handhabt. Da Fragmentierung nur auf der IPv4-Seite auftreten kann, muss man vor der Rückübersetzung oft eine spezielle NAT64-MTU-Einstellung vornehmen, die nicht die reale Schnittstellen-MTU ist, sondern nur die interne Bearbeitung der IP-Pakete beeinflusst.

Die Plattform kann auch eine ICMP-Antwort "Fragmentation Needed" an den IPv4-Server zurücksenden.

Sie müssen möglicherweise die zweite Option für einige Kommunikationen verwenden, und natürlich für solche, die keine IPv4-Fragmentierung unterstützen, wie TFTP. Siehe RFC 7915.

In umgekehrter Richtung müssen Sie sicherstellen, dass PMTU-D mindestens 1280 Bytes lang ist. Stellen Sie also die IPv4-seitige Schnittstelle Ihres NAT64 immer mit einer MTU größer als 1260 ein ($1260 + 20 \text{ Overhead IPv6} = 1280$). Siehe RFC 7269.

Hinweis zur Filterung

Wie lassen sich die Ströme filtern, sobald NAT64 durchlaufen wurde? Wenn NAT64 in der Nähe des Nutzers erfolgt, ist die Identifizierung einer Gruppe einfach. Wenn es zentralisiert ist, erfordert es eine Menge granularer ACLs.

Die Lösung liegt in der Segmentierung von IPv4-NAT-Pools, der Erstellung entsprechender Regeln, so dass Maschinen hinter einem IPv6-Präfix X mit einem dedizierten IPv4-NAT-Pool Y auftauchen, und so weiter. Auch hier gilt: Je mehr Segmentierung es gibt, desto komplexer wird die Umsetzung an den Standorten sein.

Welcher Bereich welche Technologie?

Nachdem Sie nun wissen, was einem Client ermöglicht, mit einem Server zu interagieren, der nicht dieselbe IP-Version spricht, und wie man mit dem Transport umgeht, wollen wir uns die Relevanz der einzelnen Lösungen ansehen.

Ideal ist es, sich zu fragen, was am einfachsten zu migrieren ist.

Welche Arten von Netzteilnehmern sind im Netz vorhanden?

• CAMPUS

Auf der Benutzerseite finden wir in der Regel homogene Workstations mit einem identischen Ökosystem, das pro Standort/geografischer Zone und anderen zentralisierten Bausteinen reproduziert wird. Dieses Ökosystem umfasst Dateispeicher, Authentifizierungsverzeichnis, Messaging und andere Tools für die Zusammenarbeit wie Telefonie, Drucken, Proxy, Workstation Management Agent, Protection Agent und natürlich Geschäftsanwendungen. Letztere sind inzwischen fast systematisch Webanwendungen und stützen sich daher häufig auf den Browser auf der Client-Seite.

Auch die Netzwerkausrüstung folgt häufig wiederkehrenden Architekturmustern, wobei zwei bis drei Generationen auf Organisationsebene nebeneinander bestehen. Leider ist die Campus-Ausrüstung diejenige, die am meisten hinterherhinkt, wenn es um IPv6-Kompatibilität geht, vor allem in Bezug auf die Sicherheitsfunktionen.

Es ist jedoch schwierig, nicht zu erkennen, dass dieser Bereich zwar groß, aber auch relativ homogen ist. Diese Homogenität ist eine Stärke. Durch den Einsatz von IPv6 im Dual-Stack-Verfahren an einem Standort jedes Typs im Pilotbetrieb und durch die Implementierung in den Geräten des Ökosystems "Büro/Arbeitsplatz" wird es möglich, die Einführung zu automatisieren.

Dies kann beim Austausch von Netzkomponenten, bei Umzügen usw. der Fall sein.

Letztendlich ist es sogar möglich, IPv4 aus dem Campus zu entfernen, um die Dual-Stack-Verwaltung loszuwerden. Dies ist das bevorzugte Szenario, wenn Ihre Organisation nicht über ausreichenden privaten IPv4-Adressraum verfügt.

NAT64 + DNS64

Wenn dieser Weg Ihren Bedürfnissen entspricht, müssen Sie die NAT64 und DNS64 genau betrachten. Wir wiederholen die Elemente des Abschnitts über die Topologie:

Wenn Ihre Standorte keine IPv4-kompatiblen Dienste anbieten und/oder nur auf Rechenzentrums- oder Cloud-Server angewiesen sind, besteht keine Notwendigkeit für NAT64 vor Ort, wie dies beispielsweise bei Banken der Fall ist.

Andererseits gibt es an einem großen Industriestandort oft Geschäftsserver vor Ort, so dass die Produktion nicht vollständig von der Zuverlässigkeit des WAN abhängt. Einige dieser Systeme funktionieren nur in IPv4. Dann ist es notwendig, den lokalen Austausch in IPv4 zu ermöglichen.

Wenn nur wenige Clients die betroffenen Anwendungen ausführen müssen und diese auf bestimmte Netze beschränkt sind, erscheint es sinnvoll, den Dual-Stack zu erhalten. Dies kann physisch oder logisch geschehen, z. B. mit Hilfe eines Radius-Servers.

Wenn andererseits viele Arbeitsstationen eine lokale IPv4-Ressource erreichen können müssen, wird die Implementierung eines lokalen NAT64+DNS64 interessant und wird sogar empfohlen, wenn es an privatem IPv4 mangelt.

Dieses NAT64 wird im zustandsabhängigen Modus (mit Sitzungstabellen und Portzuweisung) eingesetzt.

Obwohl es möglich ist, IPv4 mit NAT64 bei jeder Migration eines Standorts auszuschalten, ist eine Komponente problematisch: Die Telefonie. Während die überwiegende Mehrheit der Datenströme an einen Server gesendet wird, besteht bei der Telefonie die Besonderheit, dass direkter P2P-UDP-Verkehr zwischen zwei Benutzern erzeugt wird. Wenn Ihr Gerätehersteller keine Möglichkeit anbietet, der die IPv4- und IPv6-Geräte automatisch zu trennen, um die Übersetzung über einen Dual-Stack-Media-Relay-Server zu erzwingen, wenn ein Anruf zwischen den beiden Domänen aufgebaut wird, müssen Sie IPv6 an allen Standorten einführen, bevor Sie damit beginnen, IPv4 von einigen der Telefone zu entfernen, einschließlich derjenigen mit Fernzugriff (VPN oder andere).

Vergessen Sie nicht, dass einige Dienste möglicherweise eine IPv6-Sitzung zu einer Workstation initiieren müssen, z. B. der Helpdesk, um eine Verbindung zu einer Workstation herzustellen und Fehler zu beheben. Der Helpdesk benötigt daher ebenfalls IPv6-Konnektivität. Und wenn dieser Helpdesk ausgelagert ist, müssen Sie Ihre Verträge überprüfen.

Diese Einschränkung in Verbindung mit SIP- und RTP-Verkehr erzwingt eine Antwort, bevor IPv4 abgeschaltet wird.

• RECHENZENTRUM

Die Ressourcen eines Rechenzentrums, ob vor Ort oder in der Cloud, können sehr unterschiedlich oder relativ homogen sein. Es hängt alles von Ihrem Unternehmen und Ihrer Geschichte ab.

GAFAM (Google-Amazon-Facebook-Apple-Microsoft) haben zwar Möglichkeiten für die Umstellung auf IPv6-only veröffentlicht, doch sind diese in einem Unternehmen nur selten umsetzbar. Um dies zu verstehen, müssen Sie sich nur die Dienste in Bezug auf Volumen und Umfang der Bereitstellung ansehen. Wenn Sie fünfzig oder mehr Dienste auf Hunderttausenden von Servern betreiben, sind Sie zwangsläufig automatisiert und verfügen über einen Orchestrator, der eine Automatisierung erfordert. Es ist dann möglich, eine Pilotmigration zu IPv6 durchzuführen, Dienst für Dienst, und diesen als Basis für Rollout zu nutzen. Ein ähnlicher Ansatz wie der oben erwähnte für Campus, viele Maschinen, aber mit einer ähnlichen Konfiguration. Nehmen wir an, einer der großen Akteur hat ein Verhältnis von 100 000 Maschinen pro Dienst, wie ist das Verhältnis bei Ihnen?

Zählen Sie Ihre Server, VMs und Container auf und teilen Sie sie durch die Anzahl der Anwendungen, die Ihre IT-Abteilung hat. Das Ergebnis wird wahrscheinlich zwischen 3 und 10 liegen. Das ist nicht wirklich etwas, das man als skalierbar bezeichnen kann. Aber lassen Sie sich nicht entmutigen, denn auf diesen Servern läuft oft eine viel geringere Anzahl von Middlewares, etwa zehn. Ihre IPv6-Kompatibilität ist gut, aber Sie müssen trotzdem überprüfen, ob jede

Anwendung ordnungsgemäß funktioniert. Der Abschnitt "Anwendungen" wird Ihnen dabei helfen.

Dual-Stack-Server und Anwendungen

Wie im Abschnitt "Dual-Stack" der Übergangstechnologien erläutert, führt die Beibehaltung von Dualstack auf lange Sicht zu zusätzlichen Kosten. Es ist ideal, IPv6-Konnektivität auf Ihren Server bereitzustellen, um für jedes Szenario auf der Systemseite gerüstet zu sein. Diese Aspekte werden im weiteren Verlauf des Dokuments erörtert. Dual-Stack wird weiterhin für kritische und stark belastete Infrastrukturdiensste empfohlen (DNS, Verzeichnis, Proxy, NAS usw.)

6/4 Übersetzung

Die Lebenszyklen von Anwendungen können 2zwei, drei Jahre oder sogar noch länger sein. Es ist schwierig, so lange zu warten, um Kunden, die nicht über natives IPv4 verfügen, Zugang zu diesen Anwendungen zu bieten.

Wenn Ihre Anwendung dem Internet ausgesetzt ist, können Sie NAT64 auf der Seite des Betreibers für die Clients, die nicht mehr über natives IPv4 verfügen, in den meisten Fällen einfach die Arbeit erledigen lassen. Dies macht jedoch die Fehlerbehebung auf Ihrer Seite komplexer, da Sie keine Kontrolle darüber haben und der Dienst mit einem vom Betreiber abhängigen Leistungs niveau bereitgestellt wird. Wenn es zu langen Latenzzeiten oder Sitzungsabbrüchen kommt, wird der Nutzer Ihnen die Schuld geben, und Ihr Ruf wird in Mitleidenschaft gezogen. Er hat keine Ahnung vom CG-NAT durch seinen Internetanbieter.

Sie haben zwei Möglichkeiten, IPv6 freizugeben: NAT64 oder einen Reverse-Proxy.

Um den Arbeitsaufwand zu begrenzen, können Sie auf vorhandene Geräte zurückgreifen, um die Dinge zu erleichtern. Wenn sich Ihre Präsentationsschicht einfach hinter einer Firewall befindet und keine weiteren Zwischenstationen vorhanden sind, dann scheint statisches NAT64 eine gute Idee zu sein. Sie würden dann jedem Server-IPv4 statisch ein NAT-IPv6 zuordnen und den entsprechenden AAAA DNS-Eintrag veröffentlichen. Sie können sogar IPv6-Präfixe in /120 mit IPv4 /24-Netzen abgleichen, was noch weniger Regeln erfordert. Die Firewall führt NAT+PAT durch und verfolgt die Sitzungen.

IPv4-Server müssen neben der IP auch den Sitzungsport speichern, damit sie die Firewall-Protokolle korrelieren können (siehe RFC 7768).

Für weniger verbreitete Server reicht klassisches NAT64 stateful aus. Denken Sie immer daran, dass dies die Implementierung von DNS64 auf dem Auflösungspfad und die Wahl eines netzwerkspezifischen Präfixes in /96 erfordert, das Sie im Internet offenlegen werden. Dasselbe gilt für das interne Netzwerk.

Hybridisierung ist eine gute Option, statisches NAT64 mit manuell erstelltem AAAA für jeden stark genutzten Front-End-Server und dynamisches NAT64 für alles andere.

Diese NAT64-Verarbeitung erfolgt low level, mit hoher Leistung auf aktueller Hardware. Andererseits erfordert sie eine Synchronisierung der Sitzungstabellen, um die Hochverfügbarkeit des state zu gewährleisten. Dieser Modus eignet sich nicht für Anycast-Server, da eine - wenn auch geringe - Chance besteht, dass der Client während der Dauer der Sitzung von einer NAT64-

Plattform zu einer anderen wechselt. In diesem Fall käme es zu einer Unterbrechung (siehe SIIT unten).

Für granularen Datenverkehr, z. B. wenn der intern zu erreichende IPv4-Server in einem anderen Rechenzentrum steht als die NAT64-Eingangsplattform, können Sie dedizierte IPv4-SNAT-Pools verwenden, um die Grundsätze der granularen Filterung zu beachten (ähnlich wie bei der oben beschriebenen ACL-Problematik).

Mit einem SLB (Load Balancer) auf Layer 4 wird auch NAT64 empfohlen, aber wenn es auf höheren Layern funktioniert (L7 mit oder ohne WAF Application Firewall, z.B. HTTP), dann ist auch bei einer Unterbrechung beim Anwendungsprotokoll die Rekonstruktion der Kommunikation möglich. Dennoch ist es oft nützlich, die IPv6-Adresse des Clients in ein "X-Forwarded-For"-HTTP-Feld zu kopieren, wenn letzteres verwendet wird. Dadurch kann die Sichtbarkeit des Clients bis zum Server zurückverfolgt werden.

Da der öffentliche Zugang zum Rechenzentrum in der Regel aus mehreren dieser Komponenten besteht, sollten Sie zumindest die Geräte mit granularen Regeln auf IPv6 umstellen.

Nehmen wir das Beispiel des Internetverkehrs, der durch eine L4-Firewall und dann durch eine Reverse-Http-Proxy-Anwendungsfirewall (WAF) läuft, bevor er den Server erreicht. Wären wir versucht, IPv6 an der Netzwerk-Firewall abzuschaffen und NAT64 zu verwenden, aber infolgedessen würden bestimmte Erkennungsregeln für Reverse-Proxys nicht mehr funktionieren, da sie immer nur denselben Pool von SNAT-IPs von der Netzwerk-Firewall sehen würden und nicht die IPs der Clients.

Für den internen Zugang zu einer IPv6-inkompatiblen Anwendung können auch NAT64 oder Reverse-Proxy-Methoden verwendet werden. Schließlich ist es für eine interne Anwendung, die mit diesen Ansätzen immer noch nicht funktioniert, immer noch möglich, ein internes VPN zu verwenden, um die IPv4-Insel von einer IPv6-Station aus zu erreichen. Die Verlagerung aller betroffenen Kunden auf eine Virtual Desktop Infrastruktur (VDI) in einem Rechenzentrum ist eine weitere praktikable, aber teure Alternative.

Native IPv6-Bereitstellung

Warum sollte man angesichts des zunehmenden Anteils von IPv6-Kunden nicht in Erwägung ziehen, seine internetbezogenen Dienste nativ in IPv6 anzubieten und eine Übersetzung für IPv4-Kunden zu implementieren?

Dies ist das Prinzip der zustandslosen IP/ICMP-Übersetzung (SIIT), die in ihrer ursprünglichen Version auf eine 1:1-Zwei-Wege-Übersetzung zwischen IPv4 und IPv6 beschränkt ist. Dies erfordert natürlich ebenso viel IPv4- wie IPv6-Adressen auf beiden Seiten und ist daher aufgrund der damit verbundenen Einschränkungen nur in sehr kleinen und spezifischen Umkreisen verwendbar. Zum Beispiel zwischen einigen Servern.

In seiner DC-Variante ermöglicht SIIT-DC den Zugriff auf IPv6-Server von IPv4-Clients aus, ohne eine zustandsabhängige Tabelle zu führen.

Zu diesem Zweck wird ein IPv6/96-Präfix reserviert, um das IPv4 in den letzten 32 Bits abzubilden. So kann das System ohne Einschränkung multipliziert werden und unterstützt Anycast und Dissymmetrie (da es nicht auf Stateful angewiesen ist). Standardmäßig liegt das Präfix im Bereich

64:ff9b:1::/48 (RFC 8215).

Es ist natürlich möglich, mehrere Präfixe zu verwenden, um z. B. die gemappten Pakete mit dem IPv4-Interneteintrag zu verknüpfen, wo sie angekommen sind. Dies ist sehr nützlich, wenn die Internet-Sicherheit zuständsabhängige Systeme hat (IPS usw.).

Man muss jedoch immer so viel IPv4 zur Verfügung stellen, wie es IPv6-Server zu exponieren gibt.

Und wenn auf einem Server irgendwo tief im Rechenzentrum immer noch Bedarf an IPv4 besteht, kann SIIT (Dual Translation) verwendet werden. Der IPv4-Internetverkehr wird in IPv6 übersetzt, durchläuft das Rechenzentrum und wird dann von einem Gerät in der Nähe des Servers erneut übersetzt.

Obwohl wir hier über das Internet sprechen, kann die gleiche Topologie für interne IPv4-Clients implementiert werden.

Singlestack

Eine selten angewandte, aber praktikable Methode in großen Clustern ist die Bereitstellung von Servern, die ihre Dienste nur in IPv6-only parallel zu anderen bestehenden IPv4-only-Servern anbieten. Diese Technik geht zwar nicht in Richtung Homogenisierung der Konfiguration, hat aber den Vorteil, dass sie die bestehenden nicht berührt. Für IPv4-Clients in der Produktion besteht somit kein Risiko einer Unterbrechung oder eines Rückschritts.

Cloud-Anbieter

Während IPv6 in den IaaS-Angeboten der Marktführer nahtlos zur Verfügung steht, ist es bei PaaS-Lösungen noch ein weiter Weg bis dahin.

Zum Beispiel sind die meisten Loadbalancer Services noch nicht kompatibel, und wenn sie es sind (wie AWS NLB ab Ende 2020), dann nur für den Kundenteil und noch nicht für den Backend-Teil. (Was zugegebenermaßen weniger dringend ist).

Externe Übersetzung

Bei Internetdiensten können Sie sich auch auf CDN- und andere Dienste verlassen, die in der Lage sind, im Dual-Stack-Verfahren zu arbeiten, während das Backend nur in einer der IP-Protokollversionen vorliegt.

• WAN

Das WAN selbst bietet den Nutzern keine direkten Dienste an, sondern ist dazu da, den Datenverkehr zwischen den Standorten zu transportieren. Sie können im Abschnitt Transportmechanismen lesen, wie man IPv6-Datenverkehr transportiert.

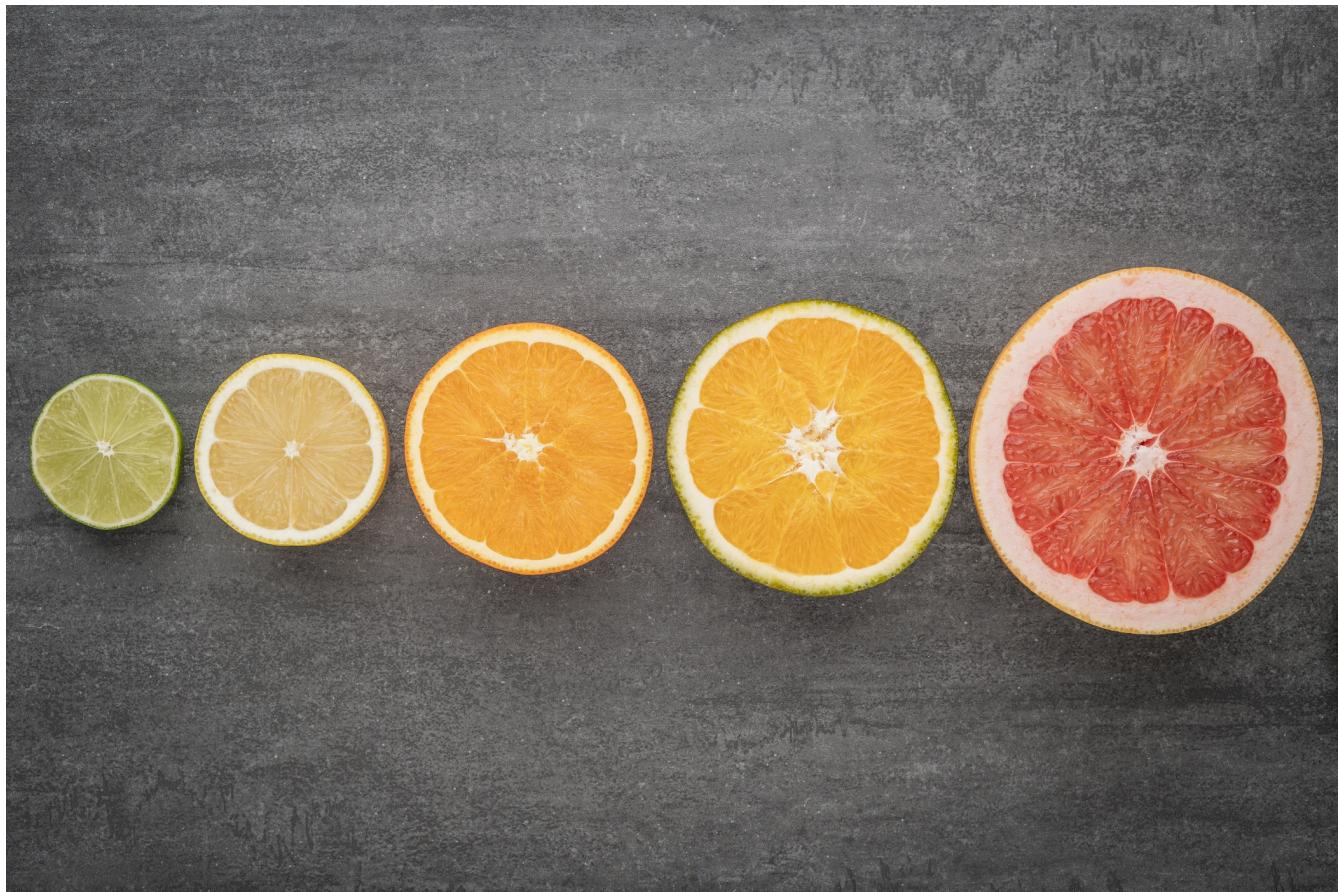
Regionale NAT-Plattform

Abhängig von der Größe Ihrer Standorte und Ihrer typischen Flow Map können Sie die Einrichtung regionaler NAT64-Plattformen auf Ihrem Backbone in Betracht ziehen. Denken Sie daran, dass

dadurch ein zustandsbehafteter Dienst hinzugefügt wird, der die Notwendigkeit symmetrischer Ströme erzwingt.

Ein solcher Dienst kann auch von Ihrem üblichen Netzanbieter über Ihr verwaltetes MPLS bereitgestellt werden, solange Sie den Datenverkehr zwischen den Standorten auf Ihrer Seite nicht verschlüsseln.

Teil III: Einzelteile



Einzelteile

Die Einführung von IPv6 muss logischerweise auf der Infrastrukturebene, dem Netzwerk, beginnen. Und vor jeder Einführung ist es sinnvoll, das Verhalten jeder Komponente zu testen. Nur sehr wenige Unternehmen verfügen über eine durchgängige Labor- und Qualifizierungsumgebung, sowohl horizontal innerhalb derselben Schicht als auch vertikal zwischen den Betriebsschichten. Beispielsweise werden die Prototypen Ihres Campus, Ihres Rechenzentrums und Ihres Sicherheitsnetzes möglicherweise von verschiedenen Teams verwaltet und sind nicht in einer Topologie verbunden, die der Produktionsumgebung nahe kommt. Wenn beispielsweise ein Testserver in einem Netz mit Produktionsroutern läuft, ist das eine vertikale Trennung. Das ist sinnvoll, denn wie soll man sonst ein Problem beheben, wenn alle Stack-Schichten in der Testphase sind - das wäre unbeherrschbar.

Jede Schicht wird ihre eigenen Testumgebungen behalten und auf einer produktiven Netzinfrastruktur basieren. Kurz gesagt, jede Qualifikation läuft selbst auf einer zugrunde liegenden Produktionsumgebung (mit Ausnahme der Grundlage, die die Netzwerkinfrastruktur ist). Dies kann wie folgt dargestellt werden:

sequencing

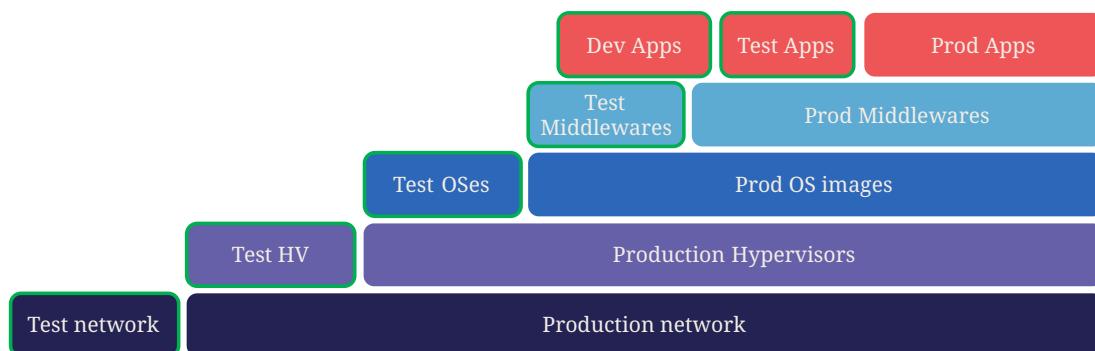


Abbildung 8. Test Stack

Warm up

Bevor Sie sich überhaupt entscheiden, wo Sie anfangen sollen, sollten Sie zunächst sicherstellen, dass alle Ihre aktuellen und künftigen Architekturfestlegungen / Ausschreibungen / Anfragen von Unterauftragnehmern die IPv6-Kompatibilität festlegen und ihr ordnungsgemäßes Funktionieren gewährleisten. Die Umstellung dieser Prozesse nimmt oft viel Zeit in Anspruch, so dass es ratsam ist, sofort mit der Arbeit daran zu beginnen.

Dazu gehören auch Build-, Run- und Lifecycle-Prozesse und alles, was damit zusammenhängt.

Netzwerk

Das Netzwerk ist die erste Säule, mit der wir uns befassen müssen. Beginnen wir mit einigen Fragen zu den Geräten:

- Funktioniert ein Gerät mit IPv6? (Fragen Sie den Gerätehersteller, Integrator, Tester usw.);
- Gibt es Funktionslücken/Einschränkungen bei IPv6 im Vergleich zu IPv4? (z. B.: Verfügt eine Probe über dieselben Erkennungsfähigkeiten, dieselben Regeln und Signaturen, die für die Ausführung von Richtlinien gelten);
- Gibt es eine Leistungslücke zu IPv4? (z. B.: Liegt die Anzahl der pro Sekunde gefilterten Pakete auf einer Firewall in der gleichen Größenordnung? Sind die ASIC-Hardwarefunktionen, wie IPSEC oder TCP-Offloading auf der OS-VM/Hypervisor/Treiber-NIC-Kette oder TLS auf einem Load Balancer gleichwertig?)
- Ist die Geräteverwaltung über IPv6 möglich? Steuerung, Überwachung usw. oder wird IPv6 nur in der Dataplane und nicht auf der Controlplane verwendet?

Die Schwierigkeit der Implementierung steigt mit der Fähigkeit des Geräts, höhere Schichten im OSI-Modell zu nutzen, da immer mehr Funktionen getestet werden müssen und das Risiko der Auslassung/Konfigurationsabweichung ebenfalls steigt.

Es ist daher einfach, mit Routern zu starten, sobald die erforderlichen Routing-Protokolle beherrscht werden. Gleichzeitig vermeiden Sie in den Endnutzernetzen sofort einen dualen Stack zur Verfügung zu stellen, um Zeit für die Herstellung der IPv6-spezifischen Sicherheitsmechanismen in Host-Netzen zu implementieren.

Dann wird die Infrastruktur vernetzt, ohne jedoch den Endanwender zu erreichen.

Im nächsten Schritt schauen wir auf die Geräten für die Filterung und WAN-Optimizer, wo das objektbasierte Modell es ermöglicht, die meisten Richtlinien/ACLs zu doppeln, indem die Objekte bearbeitet werden, um die IPv6-Subnetze/Adressen in Korrelation mit IPv4 widerzuspiegeln.

Der Benutzerzugriff sollte erst aktiviert werden, nachdem die Sicherheitskomponente sowohl für Netzwerkgeräte als auch für Hosts ausgerollt sind.

Der Rest erfordert mehr Arbeit und betrifft die fortgeschrittenen Netzwerkdienste im Rechenzentrum wie Load Balancer, WAF, Probes usw.

• Bereit?

Der Reifegrad der IPv6-Kompatibilität variiert je nach Gerätetyp. Im Allgemeinen sind Routing-Geräte der Carrier-Klasse seit Jahren problemlos. Im Gegensatz dazu treten bei Campus-Geräten manchmal noch einige Fehler auf, insbesondere bei den Sicherheitsfunktionen.

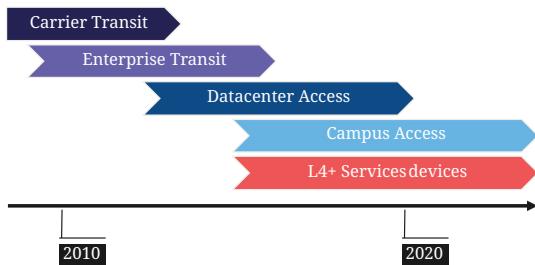


Abbildung 9. Die IPv6-Evolution

Der Reifegrad der Lösungen scheint dem obigen Diagramm zu folgen. Achten Sie auf SD-WAN- und Campus-SDN-Lösungen und lesen Sie den Abschnitt SD-WAN im Abschnitt Transportmechanismen, dessen Punkte auch für Campus-SDN gelten.

Anhand von Versionshinweisen und bekannten Fehlern können Sie erkennen, wann die IPv6-Unterstützung ausgereift ist, wobei der Schwerpunkt auf IPv6-spezifischen Fehlern liegt. Die Entwicklung folgt im Allgemeinen der Normalverteilung und damit einer Gaußschen Kurve.

• Hardware

Überprüfen Sie den Speicherplatz Ihres Routers. Einige Systeme haben nur wenig Platz für die Speicherung von IPv6-Routen. Einige ASICs auf dem Markt speichern IPv6 /48-Routen (und manchmal andere häufige Größen) anders als andere Präfixgrößen.

Die vollständige IPv6-Routingtabelle (BGP Full View) wächst exponentiell, daher sollten Sie bei der Auswahl der Geräte für Internetübergänge etwas Spielraum haben. Wenn Sie wenig Speicherplatz haben, aber dennoch BGP Full View benötigen, können Sie einige Router für IPv6-Peerings und andere für IPv4 einsetzen, wenn die technische und wirtschaftliche Prüfung zufriedenstellend ausfällt.

Da die IPv6-Adressen länger sind, benötigen sie viermal mehr Platz im Speicher. Denken Sie an Routing-Tabellen, ACL, zustandsabhängige Tabellen und Protokolle. Hoffentlich verbrauchen sie oft nur zweimal so viel Platz wie IPv4, solange /64 berücksichtigt werden. Das ist bei Routing-Tabellen und Routing-Entscheidungen häufig.

• LAB

Das Ausprobieren von Funktionen, von den einfachsten wie Routing bis zu den fortschrittlichsten wie Sicherheitsmechanismen, kann in einer Vielzahl von Umgebungen durchgeführt werden. Ob im einzeln oder nicht. Einige Tests, wie z. B. die QoS-Validierung, erfordern ein physisches Chassis und einen Traffic-Generator, während ein OSPFv3-Test höchstwahrscheinlich auf einer virtuellen

Instanz durchgeführt werden kann. Seine Abhängigkeit von ASICs ist begrenzt.

Sie können die Tests wie folgt durchzuführen, wobei die Tests von den linken Spalten auf die rechten Spalten verschoben werden können. Dadurch wird ihre Ausführung jedoch komplexer, was das Risiko erhöht, die letzte Spalte ist für die Produktionstests vorgesehen.

Umgebung Gerät	Virtuelles Labor (Herstellerumgebung oder eveNG,...)	Unabhängiges physisches Labor	Pilotphase in der Produktion
L2 Switch	<ul style="list-style-type: none"> Konfigurationsvalidierung ohne realen Test Einige virtuelle L2-Tests sind je nach Anbieter möglicherweise nicht sehr genau. 	<ul style="list-style-type: none"> Zugangssicherheit (z. B. RA-Guard) MLD-Snooping 802.1x QoS ACL IP-Stacks 	<ul style="list-style-type: none"> Verhalten des Produktionshosts
Wifi AP	N/A	<ul style="list-style-type: none"> Vorherige Elemente (außer IP-Stack...) Erreichbarkeit des Controllers Lokales Routing außerhalb des Tunnels ACL 	<ul style="list-style-type: none"> In der Produktion Host-Verhalten
Router	<ul style="list-style-type: none"> Protokolle (OSPFv3, IS-IS, MP-BGP) FHRP (HSRP, VRRP) Multicast (PIM, MLD,...) DHCPv6-Relay ACL, Route-Map Router / Firewall auch im Zusammenspiel DCI PMTU-Discovery 	<ul style="list-style-type: none"> Vorherige Elemente Zugangssicherheit (RA-Guard usw.) QoS BFD ARP/ND-Inspektion Dual-Stack-Bereitstellung für Zugangsnetze Performance 	<ul style="list-style-type: none"> Verhalten des Produktionshosts Skalierung

Umgebung Gerät	Virtuelles Labor (Herstellerumgebung oder eveNG,...)	Unabhängiges physisches Labor	Pilotphase in der Produktion
FW (zusätzlich zu Router- Funktionen)	<ul style="list-style-type: none"> • Vorherige Elemente • Bearbeiten von Objekten/Regeln in IPv6 • NAT64 • IPv6 Transit-Filterregeln • L7 Nicht-Regressionstests 	<ul style="list-style-type: none"> • Vorherige Elemente • Firewall Hochverfügbarkeit • Transit IPv6-Filterregeln • Controller des Anbieters • IPsec • IPv6-Protokolle + NAT64- Protokolle 	<ul style="list-style-type: none"> • Integration der ACL- Orchestrierung • Integration von IPv6- Protokollen + NAT64- Protokollen • Verhalten des Hosts in der Produktion
Load Balancer (SLB)	<ul style="list-style-type: none"> • Objekt-/Regelbearbeitung in IPv6 • L7 Nicht-Regressionstests • NAT64 	<ul style="list-style-type: none"> • TLS-Offloading • Leistung • IPv6-Protokolle 	
IPS/IDS	<ul style="list-style-type: none"> • Objekt-/Regelbearbeitung in IPv6 	<ul style="list-style-type: none"> • Frühere Elemente 	<ul style="list-style-type: none"> • Prod SIEM- Verarbeitung
WAN Optimierung	<ul style="list-style-type: none"> • Objekt/Regel-Bearbeitung in IPv6 • L7 Nicht-Regressionstests 	<ul style="list-style-type: none"> • Vorherige Elemente 	
Proxy	<ul style="list-style-type: none"> • Objekt/Regel und PAC- Bearbeitung in IPv6 • Gäste 	<ul style="list-style-type: none"> • Vorherige Elemente 	
DNS IPAM DHCP	<ul style="list-style-type: none"> • DNS64 • AAAA-Records • reverse PTR • IPAM IPv6-Blöcke • DHCPv6 mit Optionen 	<ul style="list-style-type: none"> • Vorherige Elemente • Selbstregistrierung der Hosts • Dienst in IPv6 bereitgestellt 	

Um Sie zu unterstützen, hat die RIPE unter [RIPE-772](#) eine Liste von Kompatibilitätspunkten veröffentlicht, die Sie bei der Erstellung einer Ausschreibung überprüfen und anfragen sollten.

Das US-amerikanische NIST hat im Jahr 2020 die Überarbeitung ihres [USGv6-rev1](#) Testprogramms veröffentlicht.

• INTERNES ROUTING

Je nach dem Aufbau Ihres Netzes erfordert die Einführung von IPv6 tiefgreifende Änderungen bei

der Konfiguration der Routing-Protokolle.

BGP

Auch wenn die Implementierung der Adressfamilie IPv6 in MP-BGP die Arbeit in BGP vereinfacht, müssen die Regeln für die Klassifizierung des Typs Access/Präfixlisten/Sets analysiert werden, dass die IPv6-Adressen berücksichtigt werden, um die Route Map/Policy korrekt und vergleichbar zu IPv4 anzuwenden. Um Inkonsistenzen zu vermeiden, sollten Sie Ihre Regeln nach Möglichkeit auf Communities stützen und diese Communities in den Accessnetzen markieren, anstatt überall Listen mit IPv4- und IPv6-Präfixen zu führen. Die Strenge einer IPv4/IPv6-Zuordnungstabelle und Automatisierung ist eine weitere mögliche Strategie, die entweder auf den Routern verteilt oder auf einem Routenserver wie FreeRangeRouting, Bird oder Quagga zentralisiert ist (was wahrscheinlich auch andere Aspekte Ihrer Routingtechnik erleichtert, wenn Sie denen gehören, die häufig BGP optimieren).

IGP

Für IGP kommen zwei Lösungen in Frage. Entweder man verwendet IS-IS von ISO, das IP-unabhängig und flexibler als OSPFv3 ist, aber in Unternehmen nur selten eingesetzt wird. Es ist das IGP, was heute in großen Carrier-Netzen dominiert, vor allem wegen seiner Konvergenz und seiner Fähigkeit zur teilweisen Neuberechnung von Routen.

Darüber hinaus erfordert die Einführung von IPv6 SRv6-basiertem Segment Routing mit IS-IS und seine TLVs, auch wenn OSPF LSAs erstellt wurden, um eine Funktionsäquivalenz zu bieten, aber der Markt und die Hersteller scheinen in erster Linie IS-IS zuzuwenden (erkundigen Sie sich bei Ihren Anbietern).

Die andere Lösung besteht darin, zu OSPFv3 zu wechseln und, sobald es stabil funktioniert, AddressFamilyIPv4 einzubeziehen, um OSPFv2 zu entfernen, Perimeter für Perimeter, wenn die Geräte mit der Bereitstellung von IPv4-Routen in OSPFv3 RFC 5838 kompatibel sind.

Die parallele Beibehaltung der beiden OSPF-Versionen bringt die klassischen Probleme des Dual-Stack mit sich (Homogenität der Konfiguration zwischen IPv4 und IPv6, Konfigurations-Overhead, Gleichwertigkeit der Überwachung usw.).

Für eine große Organisation ist eine IS-IS-Schulung wahrscheinlich den Aufwand wert, vor allem, um Sie auf SRv6 vorzubereiten.

Vergessen Sie nicht, dass nur die IGPs betroffen sind, die Client-Netze übertragen, im Allgemeinen die Accessnetze. Es ist sinnlos, das Underlay-IGP Ihres MPLS oder Ihres VxLAN-EVPN zu ändern, da BGP für IPv6 in der Overlay-Schicht zuständig ist.

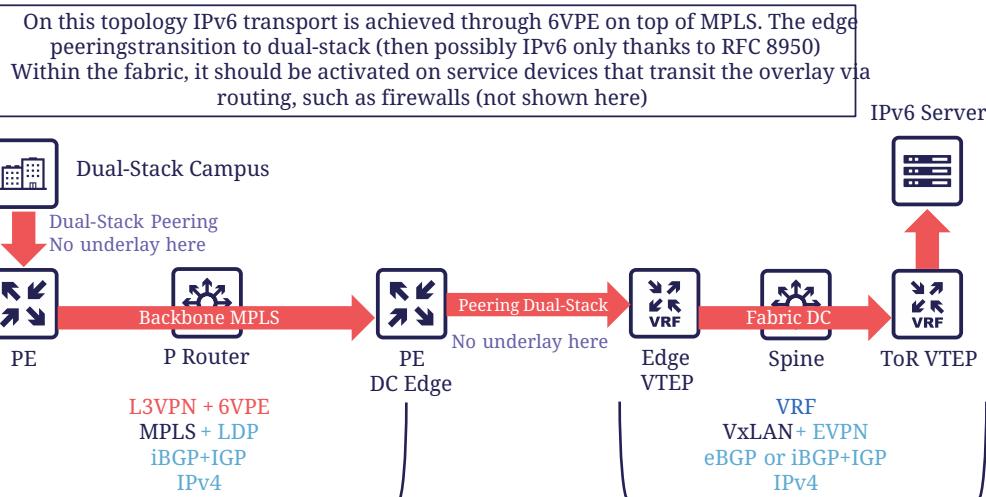


Abbildung 10. 6VPE Topologie

• FILTERN UND VERFOLGEN

Vor der IPv6-Nutzung muss das gleiche Sicherheitsniveau wie bei IPv4 erreicht werden. Der Abschnitt Sicherheit enthält viele Elemente zu diesem Thema. Außerdem finden Sie im Kapitel "IPv4/ IPv6-Mapping" des Abschnitts "Adressplanung" einige Hinweise, die die Umschreibung der Regeln erleichtern können.

Infrastrukturdiene

Viele kritische Dienste gehen Hand in Hand mit dem ordnungsgemäßen Betrieb der Infrastruktur. Einige ermöglichen Konnektivität, andere zielen auf Sicherheitsaspekte ab usw.

Unabhängig davon, welches IPv6-Bereitstellungsszenario Sie für Ihr Unternehmen wählen, wird der Zeitplan für deren Implementierung ähnlich dem der Infrastruktur sein.

• SIEM

Jedes Mal, wenn ein neuer Dienst migriert wird, müssen die Protokollierungen genauso effizient gesammelt und korreliert werden wie bei IPv4. Die Anpassung Ihres SIEM ist daher während des gesamten Projekts unabdingbar, weshalb Sie langfristig Ressourcen für dieses Thema einplanen sollten. Die Transkription von Log-Parsing-Regeln ist recht zeitaufwändig. Es wäre eine gute Idee, wenn die wichtigsten Hersteller fertige Konvertierungsmechanismen anbieten würden.

Vergewissern Sie sich, dass die Protokollquellen die Adresse zwischen eckigen Klammern gefolgt vom Port [IP]:port senden. Ohne Klammern ist es schwierig, beides zu trennen. Sie können sich zwar darauf verlassen, dass die letzte Zahlengruppe der Port ist, aber einige Anwendungen senden ihn zur Vereinfachung nicht, wenn der Quell-Port derselbe ist wie der Server-Port, obwohl dies nicht der Fall sein sollte (selten, aber nicht unmöglich).

Seien Sie vorsichtig mit der Speicherung von IPv6-Adressen, siehe den Abschnitt Anwendungen weiter unten.

• DNS/IPAM/DHCP

Diese Dienste werden häufig von einem System erbracht, mit Ausnahme spezifischer DNS-Zonen, die beispielsweise einer Microsoft Active Directory-Umgebung zugewiesen sind.

In jedem Fall sollten die für Kunden zugänglichen Service-Interfaces solcher Dienste vorrangig auf Dual-Stack umgestellt werden.

Die Management-Schnittstellen der Geräte, müssen nicht sofort in IPv6 bereitgestellt werden. Dies gilt z. B. für NTP-, RADIUS-, TACACS-, SYSLOG-Server. Anders verhält es sich, wenn Ihr Szenario auf eine IPv6-Bereitstellung in den Management-Netzen abzielt.

• VPN, PROXY UND REVERSE PROXY

Diese Dienste haben die Besonderheit, dass sie sowohl interne als auch externe Schnittstellen haben. Die IPv6-Bereitstellung kann unabhängig auf jeder der beiden Seiten implementiert werden, da die Anwendungsfälle unterschiedlich sind.

Externe Schnittstelle

Die Möglichkeit, über das Internet zu kommunizieren, wird es Ihren Nutzern und Kunden ermöglichen, Sie mit einer nativen IPv6-Verbindung zu erreichen, und das in einer Zeit, in der CG-

NAT weit verbreitet ist. Umgekehrt können IPv6-Sites problemlos über Proxy-Browsing erreicht werden.

Daher sollten Ihr VPN-Gateway und Ihr Reverse-Proxy so schnell wie möglich im Dual-Stack-Modus betrieben werden, um zu vermeiden, dass Ihre Datenströme Carrier-Grade-NAT und andere lustige Dinge außerhalb Ihrer Kontrolle durchlaufen müssen. Wir erinnern daran, dass der Reverse-Proxy auch Internet-IPv6-Konnektivität zu IPv4-Servern anbieten kann. Dies ist eine weitere Möglichkeit, die Kontrolle über diese Übersetzung auf der Internet-Seite vom CG-NAT der Internetprovider zurückzuerlangen.

Interne Schnittstelle

Der interne Aspekt geht einher mit der Einführung von IPv6 im LAN. Es wird notwendig sein, die korrekte Definition der PAC-Proxy-Dateien sicherzustellen, so dass die VPN-Regeln umgesetzt werden, insbesondere die für das Split-Tunneling.

• Betriebssysteme

Während die TCP/IP-Stacks der Betriebssysteme IPv6 bereits seit einem Jahrzehnt unterstützen, gibt es die Unterstützung für einige RFCs wie DNS-Server-Informationen über Router-Advertisement (RDNSS) erst seit Kurzem. Beispielsweise beginnt diese Unterstützung in Windows 10 mit Build 1703.

IP-Precedence

Das Konzept der IP-Precendence definiert die Priorität, die den verschiedenen IP-Adresstypen und damit insbesondere die Bevorzugung von IPv6 gegenüber IPv4 oder das Gegenteil.

Die Reihenfolge ist standardisiert, RFC 6724 aus 2012 ersetzt 3484 durch aus 2003. Dies sind die Unterschiede der beiden RFC:

Adresse	Präfix	Ehemalige Prio (RFC 3484)	Neue Prio (RFC 6724)
IPv6 Loopback	::1/128	50	50
Natives IPv6	::/0	40	40
IPv4	::ffff:0:0/96	10	35
6to4	2002::/16	30	30
Teredo	2001::/32	05	05
ULAs	fc00::/7	40	03
site-local	fec0::/10	40	01
6bone	3ffe::/16	40	01
IPv4compat	::/96	20	01

Sie sehen, dass zwischen den beiden Versionen IPv4 gegenüber IPv6-Übergangsmechanismen (6to4, Teredo) bevorzugt wurde und dass Site-Local-Adressen jetzt veraltet sind. Natives IPv6 hat die

höchste Priorität.

Achten Sie auch auf private ULA-Adressen, die eine niedrigere Priorität als IPv4 haben, das kann wichtig sein, falls Sie planen ULA zu verwenden.

```
PS C:\Users\JC> netsh interface ipv6 show prefixpolicies
Recherche du statut actif...

Précédence Libellé Préfixe
-----
 50      0 ::1/128
 40      1 ::/0
 35      4 ::ffff:0:0/96
 30      2 2002::/16
  5      5 2001::/32
  3     13 fc00::/7
  1     11 fec0::/10
  1     12 3ffe::/16
  1      3 ::/96
```

Abbildung 11. IP-Precedence in Windows 10

Ergebnis des Befehls `netsh interface ipv6 show prefixpolicies`. Dieses Verhalten kann mit dem folgenden Registrierungsschlüssel geändert werden:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\tcpip6\Parameters siehe [Link](#)

```
FILES
  /etc/gai.conf

VERSIONS
  The gai.conf file is supported by glibc since version 2.5.

EXAMPLE
  The default table according to RFC 3484 would be specified with the following configuration
  file:

    label ::1/128      0
    label ::/0          1
    label 2002::/16    2
    label ::/96         3
    label ::ffff:0:0/96 4
    precedence ::1/128    50
    precedence ::/0      40
    precedence 2002::/16 30
    precedence ::/96     20
    precedence ::ffff:0:0/96 10

SEE ALSO
  getaddrinfo(3), RFC 3484
```

Abbildung 12. Man-Eintrag Debian 10 (Buster) zur GAI.CONF

Bei vielen GNU/Linux-Distributionen kann das Verhalten in der GetAddressInfo-Datei `/etc/gai.conf` geregelt werden. Hier ein Beispiel der Debian 10 (Buster) Manpage, jedoch kein Hinweis auf den neuen RFC von 2012... <https://man7.org/linux/man-pages/man5/gai.conf.5.html>

Die Änderung der IPv4-Priorität (dargestellt durch ::ffff:0:0/96) kann Ihnen helfen, Fehlfunktionen auf einem Produktionssystem bei der Einführung von IPv6 zu vermeiden. Solange weder eine direkte Konfiguration einer IPv6-Adresse oder eines AAAA-DNS-Eintrag gibt, verwendet das System weiterhin IPv4 für all seine Anfragen. Denken Sie daran, den Normalzustand der IP-Precedence wiederherzustellen, sobald ein stabiler Zustand erreicht ist.

Beachten Sie, dass einige Programme wie z. B. Browser ihre eigene Priorisierung zwischen IPv6 und IPv4 und unabhängig von der IP-Precendence des Betriebssystems vornehmen. Auch die Implementierung des Happy Eyeball-Mechanismus (RFC 8305) kann variieren. (Verzögerung zwischen DNS A- und AAAA-Anfragen, Wartezeit für die Antwort, Timeout des Sockets mit Failover...). Beispiel: Das Tool CURL unterstützt Happy Eyeballs im Vergleich zu seinen

Konkurrenten sehr gut.

Software-Agenten

Betriebssystem-Images werden in der Regel intern mit vorkonfigurierten Agenten ausgeliefert, seltener werden diese Agenten beim ersten Start aufgespielt. In beiden Fällen sind sie ein Teil der Betriebssystembasis und ermöglichen es, die Konformität, Sicherheit usw. zu gewährleisten.

Zu diesen Agenten gehören Backup, Antivirus, Telemetrie und Überwachung, Asset Management, Paket-/Softwaredepolyment usw.

Solange Sie nicht vorhaben, IPv4 ganz aus dem Verkehr zu ziehen, brauchen Sie der Umstellung dieser Dienste auf Dual-Stack keine Priorität einzuräumen; sie kann gleichzeitig mit den Anwendungen erfolgen.

Wichtig ist, dass diese Agenten fehlerfrei arbeiten, wenn eine routingfähigen IPv6-Adresse auf dem System existiert.

Stellen Sie sich die Umstellung nicht wie eine Herkulesaufgabe vor, bei der Sie alles gleichzeitig machen müssen, ohne zu wissen, wo Sie anfangen sollen.

Sobald die Betriebssysteme für den Dual-Stack-Betrieb bereit sind, können Sie sich mit der Umstellung auf IPv6 fortfahren, sobald sein Ökosystem bereit dazu ist. Sofern dies Ihr Umstellungsszenario ist.

• ARBEITSPLATZDIENSTE

Directory

Der Verzeichnisdienst verfügt über LDAP- und Kerberos-Funktionen und beherbergt darüber hinaus gelegentlich bestimmte DNS-Zonen und andere Zusatzdienste. Ihre Allgegenwart innerhalb Ihres Informationssystems macht seine Migration unerlässlich. Das führende Produkt auf dem Markt, Microsoft Active Directory, funktioniert gut im Dual-Stack, es wird sogar von seinem Hersteller seit mehreren Jahren firmenintern mit IPv6-only verwendet.

SPN (Kerberos Service Principal Name)

Im Bestreben, jeden Servers und seinen Dienst hinter einem einzigen Namen zu deklarieren, basieren einige Produkte auf einer reverse DNS-Abfrage. Wenn der Benutzer also ein Service-Ticket für einen Server über einen CNAME und nicht über seinen ursprünglichen Hostnamen anfordert, ruft der Kerberos-Server den ursprünglichen FQDN über Reverse DNS ab. Die alternative, aber mühsame Lösung besteht darin, alle möglichen SPNs jedes Servers zu deklarieren.

Obwohl RFC 4120 von diesem Verhalten (kanonische Auflösung) abrät, wird es wegen seiner Einfachheit in Active Directory verwendet. Daher muss sichergestellt werden, dass der Kerberos-Server (KDC) keine reverse DNS-Abfrage mit einer über einen DNS64 abgerufenen IP ausführt, oder zumindest, dass der DNS-Server weiß, wie er bei DNS64 lügt und eine angemessene Antwort auf diese speziellen



Abfragen erzeugt.

Zu guter Letzt gibt es immer noch einige IP-basierte SPNs anstelle von Hostnamen-basierten SPNs (in der Regel für alte Anwendungen mit, Sie haben es erraten, einer fest codierten Konfiguration oder einfach einer IP-basierten Konfiguration). Dies ist ein seltener Fall, da Windows auf der Client-Seite diese Funktion zwischen Vista und Win 10 1507 nicht mehr unterstützt und ein Downgrade auf NTLM für solche Dienste erzwingt. Dieser spezielle Fall erfordert die Verwendung von zwei SPN pro Maschine und Dienst (IPv4 und IPv6).

Dateifreigaben und Software-Repositories

Unabhängig davon, ob sie für die Benutzer sichtbar sind oder nicht, erzeugen Server, die Dateien bereitstellen, eine hohe Verkehrslast. Wenn Ihr Projekt auf reine IPv6-Clients mit NAT64 abzielt, wäre es eine gute Idee, diese Server auf einen Dual-Stack zu migrieren (oder eine eigene Übersetzungsplattform einzurichten), was die zentralisierte Übersetzungsplattform erheblich entlasten würde.

Dazu gehören SMB, NFS, WSUS, SCCM, Paket-Repositories, EDR-Signatur-Repositories, CMS, Sharepoint, usw.



NFS kleiner Version 4 verwendet den Portmapper-Dienst und unterstützt daher kein NAT64.

Kommunikation

Die E-Mail-Infrastruktur kann noch lange Zeit mit NAT64 auskommen, aber das große Verkehrsaufkommen, das dieses System erzeugt, macht es sinnvoll, zumindest die Client-Zugangsschicht auf IPv6 umzustellen. Für den dem Internet zugewandten Teil, den MTA, besteht keine Eile, es ist nicht zu erwarten, dass SMTP-Server IPv6-only anbieten. Eine Migration erfordert die Überprüfung der Ihrer Lösungen für die Inhaltskontrolle und die Spam-Abwehr.

Auch bei der Telefonie ist es der Anwender Teil des Systems, der schnell migriert werden sollte und zwar viel dringender als das Messaging, um die IPv6-Kompatibilität für die P2P-Kommunikation zwischen Kunden oder zwischen Kunden und der zentraler Infrastruktur herzustellen. Die Dringlichkeit wird durch die bösen Überraschungen von NAT64 mit SIP verstärkt, es sei denn, Sie vertrauen hierfür auf ALGs. Da RTP-Flüsse immer häufiger verschlüsselt werden, sollte Sie sich nicht zu sehr auf ALGs verlassen.

Sie sollten wissen, dass eine wachsende Zahl von SaaS-Anbietern IPv6 unterstützt, abgesehen von einigen wenigen Ausnahmen, wie z. B. ein vor Ort installierter SBC, der mit seinem SaaS-Gegenstück kommuniziert, was nicht sehr störend ist.

• ANWENDUNGEN

Anstatt eine langwierige Qualifizierungskampagne speziell für IPv6 zu starten, ist es besser, die Gelegenheiten zu nutzen, die sich durch größere Upgrades von Anwendungen bieten, um sie für IPv6 zu qualifizieren, dann direkt IPv6-only. Die Rückmeldungen der wichtigsten Hersteller zeigen,

dass es ausreicht, eine Anwendung für IPv6 zu qualifizieren. Es ist sinnlos, alles in IPv4 zu wiederholen, da die aktuellen Methoden und Befehlsaufrufe ohne weiteres Zutun rückwärtskompatibel sind. Dies gilt natürlich nicht für eine Anwendung, die eine alte Programmiersprache verwendet und/oder mit fest kodierten Adressen arbeitet.

Hier finden Sie eine Liste von Fragen, die Sie sich zu jeder Anwendung stellen sollten:

- **Gibt es Installationen der Lösung in IPv6?** (fragen Sie den Hersteller, den Integrator, den Tester...)
- **Ist die verwendete Programmiersprache mit IPv6 kompatibel?** Auf stabile und zuverlässige Weise? (Viele Implementierungsfehler wurden in verschiedenen Sprachen bis 2015 korrigiert);
- **Ist der Code zum Öffnen von Sockets unabhängig von der IP-Protokollversion?** Inet6Address und InetAddress in Java zum Beispiel;
- **Läuft IPv4- und IPv6-Verkehr durch denselben Socket?** Vorheriges Beispiel versus einer Verwendung von IPv4-mapped address (noch in Java);
- **Verarbeitet eine Anwendung IPv6 auf der Client-Seite?** Auf dem Server-Front-End? Auf dem Server-Back-End im Falle einer n-tier-Anwendung? (auch wenn dieser letzte Punkt weniger kritisch ist);
- **Erfolgt der Aufruf einer Anwendung über eine IP-Adresse und nicht über eine DNS-Anfrage?** Nur IPv4-Konfigurationsfeld zum Beispiel;
- **Verwendet eine Anwendung ein Protokoll, das eine IP-Adresse in der Applikationsschicht einbettet?** Wie SIP bei der Telefonie, oder aktives FTP;
- **Initiiert eine Anwendung Verbindungen zu Client-Endpunkten?** Beispiel für aktives FTP mit seinen zwei gleichzeitigen Steuer- und Datensessions, eine in jeder Richtung. Oder Fernsteuerung, sowie SIP, DICOM, etc;
- **Gibt es eine IP-Adressverarbeitung innerhalb Ihrer Anwendung?** Zum Beispiel die Identifizierung des Clients anhand seiner IP-Adresse und nicht anhand seines Benutzernamens;
- **Ist RFC 8305 "Happy Eyeballs v2" korrekt implementiert, um ein schnelles Umschalten zwischen den beiden Protokollen zu ermöglichen?** (Die verwendete aufrufende Funktion und die Standardsprachkonfiguration sollten im Detail untersucht werden, da es leicht passieren kann, dies z.B. in Java nicht korrekt zu implementieren);
- **Wenn die Anwendung nicht IPv6-kompatibel ist, wird dann in der Anwendungsprotokollierung neben der IPv4-Adresse auch der Port festgehalten?** (Um die Verfolgung von NAT64 zu gewährleisten), siehe RFC 7768 von 2016, der seinerseits von RFC 6302 von 2011 inspiriert wurde, der dies ursprünglich für Front-End-Server im Internet empfahl.

Es gibt verschiedene Audit-Tools, einige sind in Entwicklungsumgebungen integriert, andere sind eigenständig, wie z. B. Microsoft checkv4, PortToIPv6, IPv6 code checker, IPv6 care, usw. Diese Tools können entweder den Code prüfen oder Socket-Aufrufe erkennen, wenn der Code ausgeführt wird, und die verwendete Methode identifizieren.

Mobile Anwendungen, die im Google Play Store und im Apple App Store veröffentlicht werden, müssen seit 2016 IPv6-konforme Netzwerkmethoden und -funktionen verwenden, was ein gutes Beispiel für eine schnelle Codeanpassung zeigt.

Nehmen Sie IPv6 unverzüglich in Ihre Spezifikationen und Architekturanforderungen für neue Anwendungen auf. Legen Sie auch einen Termin fest, an dem Upgrades einer bestehenden Anwendung die IPv6-Implementierung enthalten sollten.

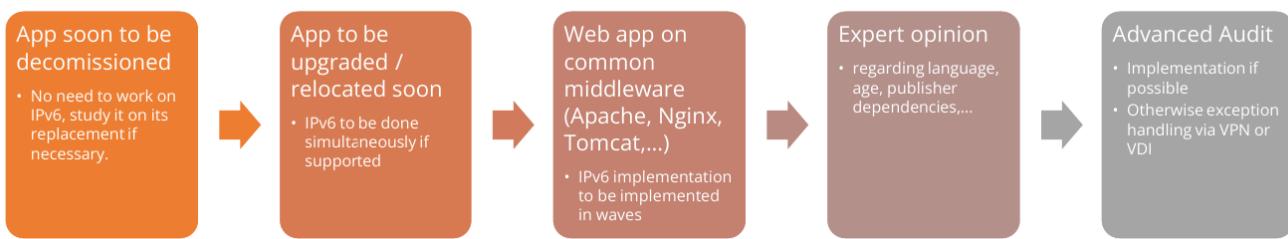


Abbildung 13. Beispiel für die Analyse einer Web App

Wie geht man mit einem Dienst um, der über Webbrowser bereitgestellt wird?

In n-Tier-Architekturen hat das Front-End, auf das die Clients zugreifen, Priorität. Das Backend der Anwendung kann viel länger in IPv4 bleiben.

Idealerweise sollten Sie die Erneuerung von Anwendungen nutzen, um IPv6 zu implementieren.

Das berühmte Dienstprogramm Curl unterstützt IPv6 bereits seit mehr als 20 Jahren.

Anwendungen, die IP verarbeiten

Die IP-Adresse ist ein Schlüsselement in Verzeichnissen; sie kann die folgenden Instrumente umfassen:

- Asset / CMDB / IPAM;
- Infrastruktur-Konfigurations-Orchestrator / Deployment / Konfigurations-Backup;
- Betriebsüberwachung/Messung/Vorfallverfolgung/Helpdesk;
- Skripte zum Sammeln von Informationen;
- Protokollkorrelation (SIEM) / Audit;
- Zugriffsmanagement / Identität.

Die Verwendung von IPv6 erfordert aus verschiedenen Gründen eine Überprüfung der Adressenspeicherung und -verarbeitung:

- Die IPv6-Adresse wird manchmal zusätzlich zu IPv4 vergeben (Dual-Stack);
- Sie ist länger;
- Eine Schnittstelle kann mehrere IPv6-Adressen tragen (Link Local, temporäre GUA, stable GUA, usw.).

Eine Vereinfachungsmethode kann darin bestehen, IPv4-Adressen wie IPv6-Adressen durch das Präfix ::ffff:0:0/96 darzustellen. Auf diese Weise wird der Zusammenhalt und die Vereinfachung des Anwendungscodes erleichtert.

Im Anhang finden Sie im Abschnitt Beispiele ein Umsetzungsprobleme dieser Methode.

In jedem Fall müssen die Adressen in ihrer kanonischen (verkürzten) Form gespeichert werden, um ihre Größe zu verringern. Der Code, der die Kanonisierung durchführt, muss den RFC 5952 genauestens einhalten, damit Sie am Ende immer genau eine Zeichenkette zum Parsen haben. Beachten Sie, dass Adressen auch mit Kleinbuchstaben gespeichert werden müssen (RFC Abschnitt 4.3). Beispiel: ab01::ffff und nicht AB01::FFFF. Die Nichteinhaltung dieser letzten Empfehlung kann sogar zu Problemen bei Anwendungsprotokollen führen, die die IP-Adresse in der Payload tragen, wie SIP.

Teil IV: Adressplan



Adressplan

Der Aufbau dieses zentralen Punktes, des Adressplans, ist ein langer Prozess, der iterativ durchgeführt werden muss.

Der Adressplan muss entsprechend den Besonderheiten Ihrer Organisation erstellt werden. Über die in diesem Abschnitt genannten Punkte hinaus ist es notwendig, sich mit vielen Gesprächspartnern auszutauschen, indem Sie das Ergebnis Ihrer verschiedenen Entwürfe prüfen. Denken Sie in jedem Fall langfristig und lassen Sie am oberen Ende des Blocks etwas Freiraum.

Bevor wir uns mit den Varianten für die Planerstellung befassen, sollten wir uns zunächst mit der Wahl des Präfixes für die Nutzung innerhalb Ihrer Organisation befassen.

• ÖFFENTLICH ODER PRIVAT?

Öffentliche IPv4-Adressen sind rar und ihr Einsatz beschränkt sich daher natürlich auf das Internet. Innerhalb des internen Netzes herrschen die RFC 1918-Bereiche, meist 10.0.0.0/8, vor.

Bei IPv6 stellt sich die Frage nach der Wahl zwischen diesen beiden Optionen.

Je nach Größe und Tätigkeit ist es ideal, wenn Sie einen eigenen Präfix durch Ihre Regional Internet Registry (RIR) zugewiesen bekommen. Ebenso wäre eine große Tochtergesellschaft oder eine Tochtergesellschaft mit einer sehr unabhängigen IT gut beraten, einen eigenen Block beim RIR zu beantragen.

Sie können auch einen Provider Independent Präfix (PI) von einer Sponsor-LIR bekommen, das ist meist nicht teuer.

Die minimale zugewiesene Präfixlänge ist /32. Es ist möglich, größere Blöcke zu erhalten, wenn die Größe der Organisation dies rechtfertigt.

• KLEINE ORGANISATION

Für ein kleines Netz ist es denkbar, das vom ISP bereitgestellte Präfix durch Prefix-Delegation (DHCPv6-PD) zu verwenden. Allerdings ist die Abhängigkeit vom Internetprovider für die Adressierung der eigenen Ressourcen nicht ideal und Sie werden schnell an die Grenzen dieser Variante stoßen, zum Beispiel bei der dauerhaften Adressierung interner Server. Es gibt die Möglichkeit, Präfixe mit DHCPv6-PD zu delegieren, für diejenigen, die mit einer plötzlichen Änderung tolerieren können. In einer idealen Welt könnten sich alle Tools an die Neunummerierung von Präfixen durch den Internetprovider anpassen, aber in der Praxis wird es wohl noch lange dauern, bis alle Konfigurationen so dynamisch sind.

ULA

Die private IPv6-Adressierung erscheint als eine Lösung, dieses "Äquivalent" zum RFC 1918 IPv4 wird ULA für Unique Local Address genannt und entspricht dem Präfix FC00::/7.

Um das Risiko eines Konflikts mit dem selben Präfix einer anderen Organisation zu begrenzen, mit der Sie hypothetisch eines Tages privat Daten austauschen wollen z. B. über einen IPSEC-Tunnel,

wird empfohlen, den Präfix in diesem /7 zufällig zu wählen, anstatt von unten zu beginnen (RFC4193 schreibt diese Zufallsauswahl sogar vor).

Nehmen Sie zum Beispiel ein beliebiges /48 in FC00::/7 und bauen Sie Ihre Adressierung darauf auf. Für eine sehr kleine Organisation ist ein /56 ausreichend. Seien Sie vorsichtig, die Größe darf aus einem Grund, den wir weiter unten sehen werden, nicht zu groß sein. RFC4193 schlägt einen Pseudozufallsgenerierungsalgorithmus vor, um eine 40-Bit-ID zu erhalten, die einen 48-Bit-Präfix ergibt.



In den aktuellen Vorrangregeln hat ULA jedoch eine niedrigere Priorität als IPv4. IPv4 wird daher in einer Dual-Stack-Umgebung bevorzugt (außer beim Verkehr zwischen zwei ULAs).

Es gibt zwei Lösungsmöglichkeiten

- Ändern Sie das Verhalten aller Hosts, um ULA Vorrang vor IPv4 zu geben durch Anpassung der IP-Precedence;
- Beantragen Sie ein unabhängiges PI-Präfix und verwenden Sie es nur intern. Letzteres wird empfohlen.

Provider Independent (PI) Präfix

Unsere empfohlene Lösung: Beantragen Sie ein PI-Präfix der Größe /48 bei einem LIR/Internetprovider. Sie müssen es nicht zwingend im Internet bekannt geben usw. Es wird Ihnen aber ermöglichen, ein LAN mit einem eindeutigen Adressierungsraum zu versehen gleichzeitig und die Probleme mit der ULA- und IPv4-Präferenz zu vermeiden.

In diesem Fall müssen IPv6-Pakete, die diesen PI-Präfix im LAN verwenden, der nicht im Internet announced wird, ein NAT durchlaufen, um im Internet transportiert zu werden. Analog zu IPv4 NAT44 + PAT mit zustandsabhängiger Sitzungstabelle, verwenden Sie Network Prefix Translation IPv6 (NPTv6 | RFC 6296).

Bei der Präfixübersetzung werden die ersten Bits der Adresse ausgetauscht, um ein IPv6-Präfix mit einem anderen Präfix der selben Größe abzulegen. Es finden keine weiteren Änderungen statt, alles ist zustandslos.

Sie müssen lediglich Ihr privates Präfix /56 (oder eine andere Größe) auf das öffentliche Präfix, das vom Internetprovider bereitgestellt wird, abbilden und gleichzeitig die interne Adressierung kontrollieren. Es ist möglich, ein internes /56 auf ein öffentliches, geroutetes /48 Präfix abzubilden, aber natürlich nicht umgekehrt (daher ist es wichtig, keinen zu großen Bereich in Ihrem internen LAN auszuwählen).

Dank NPTv6 kann Ihr Unternehmen von einem ISP zu einem anderen wechseln, ohne im internen LAN IPv6-Adressen ändern zu müssen, und unterstützt die PMTU-D, die Ermittlung der maximal übertragbaren Paketgröße.

Nachteile von NPTv6

Protokolle, die die Adresse in der Payload einkapseln, wie SIP, H323 usw., erfordern immer die

Verwendung eines entsprechenden Application Layer Gateway (ALG) auf dem Gerät, das die Übersetzung durchführt. Wie bei NAT44 können ALGs ein Angriffsvektor sein, siehe insbesondere die jüngsten Slipstreaming-Methoden, die Browser gezwungen haben, bestimmte Zielports zu blockieren.

Sie müssen Ihre DNS-Einträge zwischen der internen DNS-Zone (nicht announced PI oder ULA, je nach Entscheidung) und der externen DNS-Zonen für Internetdienste synchronisieren. So vermeiden Sie einerseits, dass Sie fälschlicherweise einen AAAA-Eintrag mit einer unerreichbaren PI-IP im Internet veröffentlichen, und andererseits, dass Sie intern die Global Routable IP verwenden, da dies die NPTv6-Plattform durchlaufen würde. Zum Beispiel sollte ein LAN-Client, der einen DMZ-Server anfragt, diesen direkt über seine interne Adresse (ULA oder PI) erreichen.

Oh, und vergessen Sie nicht, PTR für beide Adressarten zu erstellen. Dies ist für einige Dienste wie SMTP MX wichtig, da dies Teil der Anti-Spam-Prüfungen ist. Hoffentlich gibt es Mechanismen, die Ihnen eine automatische PTR-Generierung ermöglichen.

• GROSSE ORGANISATION

Beginnen Sie mit der Beschaffung eines öffentlichen PI-Prefix (Provider Independent) oder mehrerer Prefixes im Falle von Tochtergesellschaften oder Niederlassungen auf mehreren Kontinenten.

Vor der Erstellung Ihres Plans müssen einige Besonderheiten berücksichtigt werden.

Ihre öffentlichen BGP-Announcements können gemäß Konvention nicht kleiner als /48 sein. (Ähnliche Situation wie bei /24 IPv4). Es besteht jedoch keine Notwendigkeit, ein Präfix zuzuweisen, das nur den exponierten Servern entspricht; wir werden sehen, warum.

IPv4 und die Allgegenwart von NAT44+PAT haben Praktiken hervorgebracht, die in IPv6 nicht mehr notwendig sind, insbesondere das falsche Gefühl von Sicherheit, das NAT44 im eingehenden Verkehr böte. Der Aspekt der Kommunikationsrichtung ist aufgrund der Anforderung zur Sitzungsverfolgung inhärent vorhanden, d. h. er ist zustandsabhängig. Und obwohl es normal ist, dass es keine automatische Portweiterleitung wie bei Endanwenderroutern gibt, ist es schwieriger, sich gegen die jüngsten Slipstreaming-Angriffe gegen ALGs zu schützen, wie oben erwähnt.

Ein zustandsbehaftetes NAT + PAT-Äquivalent gab es in IPv6, aber seine Verwendung wird nicht empfohlen. In der Tat ist NAT-PT (NAT Protocol Translator RFC 2766, nicht zu verwechseln mit NPTv6) einfach unbrauchbar und wurde archiviert, vgl. RFC 4966, in dem die Gründe für die Einstellung dieses Mechanismus aufgeführt sind.

Sie finden manchmal Sicherheitsempfehlungen, ein internes Netz mit ULA zu betreiben und NAT am Internerübergang zu verwenden, um Ihren Adressplan nach außen hin unsichtbar zu machen.

Diese Empfehlungen erinnern an IPv4-Gewohnheiten sowie an die Tatsache, dass die Verwendung einer privaten internen Adressierung mit NPTv6-Präfixübersetzung zum Internetübergang für ein großes Unternehmen nicht sicherheitsrelevant ist und die Details des internen Plans überhaupt nicht verbirgt, da lediglich die ersten paar Bits der Adresse ausgetauscht werden. Erinnern Sie sich daran, dass NAT keinen Schutz bietet, nur eine Firewall mit den richtigen ACLs und möglicherweise weiteren Prüfungen sind wirksam.

Ihr gesamtes Informationssystem sollte mit Ihrem Präfix adressiert werden.

Verwaltung des direkten Internetzugangs

Die NPTv6-Präfixübersetzung kann auch für andere Situationen verwendet werden. Nehmen wir ein Unternehmen, das auf seinem Campus einen lokalen Breakout (LBO) nutzen möchte, um Internet-Ressourcen (z. B. eine SaaS-Anwendung) ohne den Umweg über sein Rechenzentrum zu erreichen. Der Datenverkehr muss dann von einer Adresse, die dem Unternehmen gehört, zu einer Adresse übersetzt werden, die vom lokalen Internetanbieter des Campus bereitgestellt wird.

Das ein ist ein Grund dafür, Standortpräfixe auf der Grundlage einer geografischen Zuordnung zu verwenden. Dies ermöglicht es Ihnen, nur eine NPTv6-Regel zu haben. Wenn Ihre Standortadressierung fragmentiert ist, müssen Sie jedes lokale /64 auf ein /64 abbilden, das zu dem vom lokalen Betreiber bereitgestellten Präfix gehört (normalerweise ein /48). Das bedeutet mehr Regeln und mehr Arbeit.

Wenn der Campus sehr groß ist und der lokale Netzbetreiber dies zulässt, ist es möglich, dass der Standort seine eigenen /48 (oder mehr) über BGP direkt im Internet announced.

In diesem Fall verwenden die Geräte des Standorts die Adressen eines Präfixes, das wir "Site" /48 nennen. Dieses Präfix wird nicht announced, sondern ein größeres Präfix "Global" /32, das es einschließt, wird vom Rechenzentrum announced. Schließlich announced der Standort lokal und direkt im Internet ein Präfix "LBO" /48 an, das ebenfalls zum globalen /32 gehört. Diese Konfiguration würde zu einem enormen Anstieg der BGP-Fullview im Internet führen, wäre aber nutzbar, wenn Ihr Adressplan eine Routenaggregation am Carrier-Edge vorsieht.

Die lokale Regel von NPTv6 übersetzt das Präfix Site/48 in LBO/48 am lokalen Internetausgang. Der Betrieb der Routing-Entscheidungen von BGP, die more-specific Routen zu bevorzugen, wird es ermöglichen, ohne Konflikt mit IPs zu funktionieren, die alle Ihrem Unternehmen gehören. Wenn wir mehrere Standorte in dieser Situation mit demselben Provider haben, wäre es klug, eine Route-Summary zu verlangen.

Schließlich verlässt ein Teil des Datenverkehrs den Standort direkt über das LBO-Präfix, während ein anderer Teil des Datenverkehrs, der im Rechenzentrum einer weitergehenden Verarbeitung unterzogen werden muss, den Standort über das Site-Präfix verlässt (abhängig von der Konfiguration der Proxeinstellungen der Endgeräte).

Mit dem Aufkommen so genannter "SASE"-Lösungen (Secure Access Service Edge) kann auf die Verarbeitung im Rechenzentrum gänzlich verzichtet werden, so dass die Verwendung von zwei Präfixen bei NPTv6 nicht mehr erforderlich ist.

Der Latenzgewinn durch LBO kann erheblich sein, da der Umweg über das Rechenzentrum und seine Abhängigkeiten nicht mehr erforderlich ist. Allerdings muss das gleiche Sicherheitsniveau in Bezug auf Filterung, Antivirus-Analyse usw. gewährleistet sein. Die Strategien variieren zwischen der Autorisierung eines Teils der Datenströme (Empfänger mit ausreichendem Vertrauensniveau) und dem gesamten Internetverkehr, je nachdem, welches Schutzniveau erreicht werden kann. Dieser wird entweder lokal über VNFs, SASE oder über eine Cloud-Lösung bereitgestellt.

NPTv6 PI+FAI

Here the Local Breakout flows undergo a prefix translation to the local carrier's prefix. The other flows exit through a centralized infrastructure and use the company IP Provider Independent (PI) space.

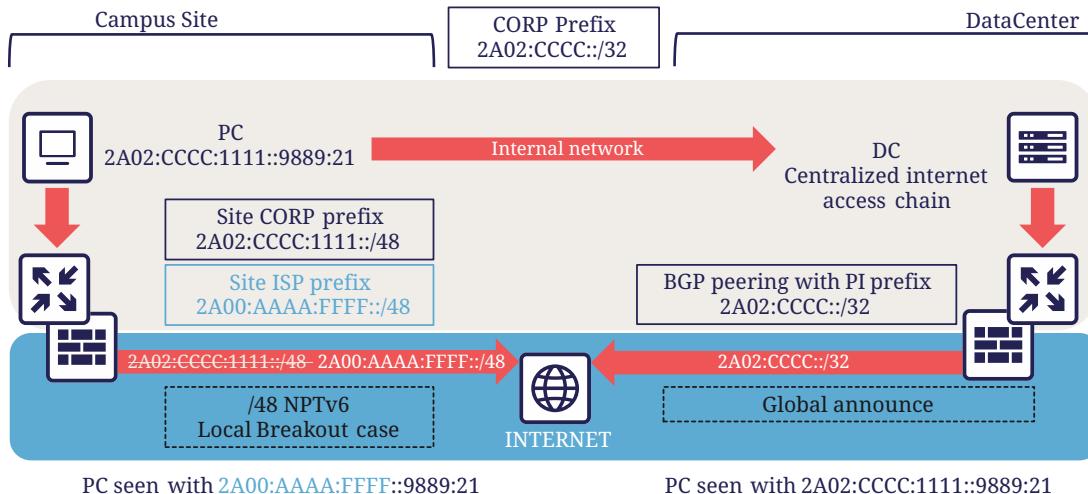


Abbildung 14. Schema von NPTv6 PI+FAI

Für Segmente, die vollständig vom Internet und allen Partnern isoliert werden müssen (z. B. ein SCADA-Netz), ist es möglich, ULA-Adressen zu verwenden. Dies verhindert jedoch keine Rebound-Angriffe von einem anderen internen System aus, da Firewalls ohnehin ausreichen, um den Verkehr am Rande dieser Netze zu blockieren. Der Sicherheitsbeitrag von ULA ist daher fast gleich Null und es bleibt eine subjektive Entscheidung, sie trotzdem zu nutzen.



Es sei noch einmal daran erinnert, dass ULA in den derzeitigen Vorrangregeln eine niedrigere Priorität hat als IPv4. IPv4 wird daher in einer Dual-Stack-Umgebung bevorzugt.

• LOGISCHE GRUPPEN

Bei IPv4 war es üblich, IP-Bereiche nach Standort zuzuweisen, um die Anzahl der Routen durch Summaries zu minimieren. In letzter Zeit haben einige Projekte einen anderen Ansatz gewählt, d. h. die Zuweisung aus einem IP-Block, der einem bestimmten Zweck gewidmet ist, wie z. B. bei einem WiFi-Einführungsprojekt in Behörden oder bei IoT.

Dieser letzte Fall ist für die Filterung von Vorteil, da er sich auf die Nutzung und nicht auf den Standort konzentriert.

Die Auswahl ist besonders wichtig, weil Sie im Gegensatz zu IPv4 keine Maske, sondern nur das Präfix zum Filtern verwenden können.

In IPv4 ist es möglich, wenn auch selten genutzt, z. B. den Platzhalter 0.0.240.0 zu verwenden, um n identische Hosts aus verschiedenen Subnetzen auszuwählen. In IPv6 entfällt dies.

Wenn Geräte eine große Anzahl von Routen unterstützen, würden manuelle Regeln, die auf Routen angewandt werden, komplex werden, um sie mit einem nutzungsorientierten Plan zu implementieren und wir wissen bereits, dass trotz der Automatisierung und SDN auf verschiedenen Perimetern, BGP der Weg bleibt, um "Black Boxes" miteinander zu verbinden. Nichtsdestotrotz wäre es möglich, Skripte und einen Routenserver wie [bird](#) oder [FFRouting](#) zu

verwenden, um automatisch Klassifizierungen vorzunehmen und Policies anzuwenden oder einfach die Communities auf Announcements intensiv zu nutzen.

Die beiden geo- oder typzentrierten Optionen haben Vor- und Nachteile, die durch Automatisierung ausgeglichen werden können (Konsolidierung von Filterregeln und Konsolidierung von Routen und Standorten). Wie bereits bei der NPTv6-Erklärung erwähnt, ist es einfacher, die Adressierung auf den Standort zu stützen.

• ADRESSBASTANDTEILE

Das Slicing kann die Vielfachen von 4 Bits (hexadezimale Zeichen), /32, /48, /52 usw. bevorzugen, um das Lesen zu erleichtern, eine Tendenz, die unserer Gewohnheit entspricht, das IPv4 oktettweise aufzuteilen, und die im konkreten Fall von IPv4 zu Abfall führt.

Jedes Hexazeichen wird als Nibbl, die Gruppierung von 4 Zeichen als Hextet bezeichnet, zum Beispiel: A9B4:

Auch wenn IPv6 eine große Anzahl von Adressen anbietet, dies keine Einladung zur Verschwendug, wir werden z.B. Leetspeak wie "c01d:c01a:c0fe" / "cold cola cofe" innerhalb des Präfixes/der Netz-ID vermeiden.

Man kann sofort daran denken, diese Nibble zu assoziieren mit:

- Rechtsträger / Wirtschaftszweig;
- Geografische Standort-ID;
- Netzwerktyp;
- VLAN- oder VNI-Nummer;
- Betreiber;
- Gerätemodell.

Numerische Elemente können so belassen werden, wie sie sind, was mehr Platz beansprucht, oder in hexadezimaler Form kodiert werden, wodurch die Lesbarkeit für den Menschen entfällt.

Um beispielsweise die VLAN-Nummer zu speichern, haben wir die Wahl zwischen 0 und 4094 (12 Bits):

- 4 0 9 6, das sind 4 Zeichen, also 16 Bits;
- F F E oder 3 Zeichen, um 4094 in Hexadezimal zu bilden, wobei ein freies Nibble im Hextet x F F E bleibt.

Wenn wir einen neuen Adressrahmenplan erstellen, wäre es besser, alles direkt in Hexadezimal zu schreiben, wenn die Aufteilung dies zulässt.

Wenn wir auf die Liste der Bausteine zurückkommen, haben einige von ihnen einen Lebenszyklus, der sich nicht für die Integration in einen Adressplan eignet. So kann sich beispielsweise ein Carrier in der Zwischenzeit ändern, ebenso wie der Hersteller oder das Modell eines Layer-3-Geräts. (Aus Erfahrung wissen wir, dass die Wartung nicht fortgeführt wird, weil "es gut

funktioniert, wie es ist"). Wir werden später eine Ausnahme für Point-to-Point-Netze sehen.

Im Rechenzentrum wird dasselbe mit VLANs passieren, die Verwendung von E-VPN + VxLAN-Technologien mit einer 24-Bit-VNI-Nummer wird das VLAN in den Hintergrund drängen, dasselbe gilt für proprietäre Segmentierungstechnologien, die Begriffe wie Client Tenant, Ressourcenpool usw. integrieren.

Daraus lässt sich ableiten, dass in den Plan nur zeitlich unabhängige und statische Elemente integriert werden sollten, woraus sich ergibt:

- Die Abteilung/Einheit auf einer hohen Ebene, um die Aufschlüsselung der Struktur zu ermöglichen (wie in einem Active Directory).
- Die Lage entweder durch eine Struktur Kontinent / Land / Niederlassung, oder durch die nummerierten Standort-Code.
- Die Art des Netzes mit Unterkategorien, um die Filterung zu erleichtern und einen Teil des Adressplans delegieren zu können.

• PRÄFIXGRÖSSE

Standard

Von Anfang an scheint /64 der unveränderliche Standard für ein Netz zu sein (RFC 4291), insbesondere damit der Autokonfigurationsmechanismus SLAAC funktioniert.

The war front movements (last 20 years)

```
RFC 3513 - "only /64 is valid"  
RFC 3627 - "don't use /127, use /126 if you must"  
RFC 4291 - "reaffirming: only /64 is valid"  
RFC 6164 - "a /127 is OK to use too"  
RFC 6583 - "there are problems with /64"  
RFC 7421 - "/64 is the best!"  
RFC 7608/BCP198 - "every prefix length must be forwardable"  
RFC 4291bis-07 - "fine, /64 and /127 are valid, but nothing else!"  
...  
RFC ???? "?????"
```

Abbildung 15. Ist ein Standard tatsächlich ein Standard?

Die Vorgabe ist eine maximale Präfixlänge von /64, alles andere kann zu unerwartetem Verhalten oder Inkompatibilitäten führen.

Auch bei den Site-Präfixen haben sich die Empfehlungen weiterentwickelt: RFC 6177 passt das Präfix an den tatsächlichen Bedarf an, während früher /48 vorgeschrieben war.

Die Interprovider weisen in der Regel /56 oder /60 für Privatkunden und /48 für Geschäftskunden zu. Die Endnetze sind immer in /64, mit Ausnahme der Point-to-Point-Netze.

Interconnection

Die Netzbetreiber scheinen /125-Verbindungen zu empfehlen. Um zwischen zwei hexadezimalen Zeichen zu unterscheiden, wäre es eine gute Idee, /124 im Plan vorzusehen und die 125 für die Ausfallsicherung bei einem Geräte- oder Anbieterwechsel zu verwenden.

Diese Reservierung hindert Sie nicht daran, die Punkt-zu-Punkt-Schnittstellen auf /127 zu setzen.

Diese Reservierungen für Interconnections und Loopbacks können von der Standortadressierung übernommen werden, oder im Gegenteil von einem /64-Präfix, das für Interconnections in viele /124 aufgeteilt wird.

Im letzteren Fall müssen Sie viele feine Routen in Ihrem Netz bekannt machen.

Der Aufbau von Interconnections mit Link-Locals funktioniert zwar, hat aber viele Nachteile, die in RFC 7404 detailliert beschrieben werden (keine ICMP-Rückmeldung der Schnittstelle, da nicht routingfähig, sondern eine Loopback-Adresse, eine Adresse, die sich bei einem Hardwaretausch ändert, da sie automatisch auf EUI-64 MAC basiert, usw.). Auf der anderen Seite ist einer der großen Vorteile die Entlastung der Routing-Tabellen sowie die Reduzierung der Angriffsfläche. Der Aspekt der Pfadverfolgung mit link-local kann mit RFC 5837 abgerufen werden. Die Wahl wird daher im Allgemeinen zwischen einem Unternehmensnetz versus einem großen ISP oder einem CIX-Austauschpunkt unterschiedlich ausfallen.

Sie können Ihr /124-Präfix mit der BGP AS-Nummer des Drittanbieters, der Router-ID usw. erstellen. Kurz gesagt, alles, was Ihnen bei Ihren täglichen Aufgaben helfen wird.

Seien Sie vorsichtig mit IPAMs, die sich oft weigern, etwas anderes als /64 einzutragen, auch wenn es ist nicht ungewöhnlich ist, lange Präfixe zu haben.

Abgesehen von den ist /64 der derzeitige Standard, und es wäre schade, etwas anderes zu verwenden.

Einige RFC-Entwürfe zielen darauf ab, dass SLAAC etwas anderes als /64 bereitstellen kann, siehe draft-mishra-v6ops-variable-slaac-problem-stmt und draft-mishra-6man-variable-slaac. Diese Entwürfe versuchen, das Problem der Unterteilung eines einzelnen /64 zu lösen, das z.B. von einem Mobilfunkbetreiber über eine 3GPP-Verbindung bereitgestellt wird. Das Ziel ist es, verschiedene Netze auf mobilen Mikroinfrastrukturen zu schaffen, typischerweise ein Router mit mehreren Client-Netzen oder ein angeschlossenes Fahrzeug, dessen verschiedene interne Netze manchmal Ethernet, manchmal BUS verwenden und nicht überbrückt werden können. Es ist sogar notwendig, direkte Austauschnetze mit benachbarten Fahrzeugen (V2V) zu haben. Die Zukunft wird zeigen, ob diese Entwürfe zu einem Internet-Standard werden oder ob sie aufgegeben werden, wenn alle Netzbetreiber anfangen, DHCP-PD auf Mobiltelefonen mit /56 über 3GPP zu unterstützen, wie es bei Hausanschlüssen oft heute schon der Fall ist.



• GEMEINSAME DIENSTADRESSEN

Zur Vereinfachung ist es interessant, den Diensten, bei denen die IP oft manuell eingegeben werden

muss, kurze Adressen zuzuweisen, vor allem natürlich den DNS-Servern, aber auch den Schnittstellen der Router.

Daher sollte die Adresse, die ganz am Anfang einer Organisation steht, pre:fix:0000:0000:..., für diese Zuweisungen verwendet werden, um den Betreibern/Administratoren ihre Arbeit zu erleichtern.

Auf jeder Ebene, jedem Regional-Präfix, jedem Standort... wäre es gut, die 0 und die 1 für Dienste mit verkürzten Adressen zur Erleichterung alltäglicher Aufgaben zu reservieren.

Bitte nicht alle Instanzen desselben Dienstes in dasselbe Präfix aufzunehmen. Es ist keine gute Praxis, z. B. alle DNS- oder SMTP-Relais im selben Präfix zu haben und somit von derselben Route abhängig zu machen. Im Falle eines Routingvorfalls, der dieses Präfix betrifft, können Sie trotz vieler physische und/oder logischer Instanzen des Dienstes einen Blackout bekommen.

• ZEITLICHE ENTWICKLUNG

Um Migrationen auf verschiedenen Ebenen zu ermöglichen, können Migrationsbits implementiert werden.

Ein Netzmigrationsbit kann Änderungen der Hardware, der WAN-Verbindungen usw. erleichtern. Dieses Bit sollte das 64. sein, damit es in /63-Filterregeln berücksichtigt werden kann. Es würde einen schrittweisen Übergang von Subnetzen, VLANs und Geräten ohne weitere Änderungen ermöglichen, da die ACLs in /63 die zwei nutzbaren /64 umfassen würden.

Beispiel: Ein Campus wechselt seinen Core und migriert gleichzeitig zu einem MAN. Die neuen Netze werden mit dem Übergangsbit versehen und parallel zu den alten Netzen geroutet. Dank der breiten Filterung mit diesem Bit können vor der Migration Tests in der neuen Infrastruktur durchgeführt werden. Dadurch werden Big-Bang-Migrationen vermieden und Störungen nach der Migration vermieden.

Bei der nächsten Umschaltung wird das Bit getoggelt. Kein Unterschied zwischen 0 und 1 wird bevorzugt.

Jeder Vorgang, der einen Wechsel der Ausrüstung, des Bedieners, einen Umzug usw. erfordert, wird dadurch erheblich erleichtert.

Es muss jedoch verhindert werden, dass ein Zwillingsnetz angekündigt wird, das ungewollt die globalen Filterregeln ausnutzt. Die Überwachung des Ursprungs von Routen, die zum selben Migrationspaar gehören, ist daher notwendig.

Allgemeiner ausgedrückt: Platz für künftige Dinge schaffen. Dies ermöglicht die Anpassung an neue Architekturen, ohne dass neue Blöcke auf höchster Ebene erforderlich sind.

plan

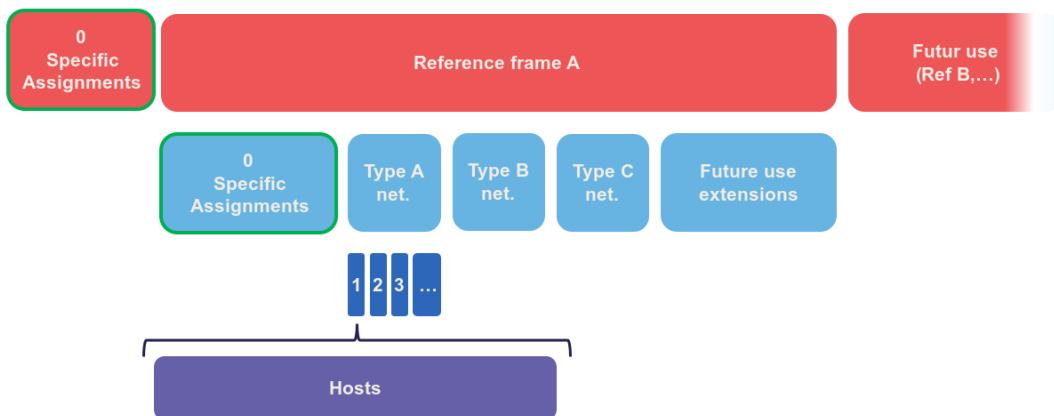


Abbildung 16. Beispiel für eine Adresshierarchie

• VERWENDUNG DER INTERFACE-ID 0

In IPv6 gibt es weder eine reservierte Adresse für das Netzwerk noch eine für Broadcast, alle mathematisch möglichen Adressen können den Hosts zugewiesen werden.

Allerdings sind manchmal falsche Regex in Konfigurationsfeldern von Anwendungen vorhanden. Man kann Systeme finden, die eine Adresse, die auf ::0 endet, zum Beispiel 2001:db8:abcd:1234::/64 nicht unterstützen. Manchmal auf ihrer Schnittstelle oder IP-Konfiguration eines Kommunikationspartners wie der DNS- oder NTP-Serveradresse.

Außerdem empfehlen wir, Adressen mit Interface-ID 0 mindestens für die Server zu vermeiden, deren IP-Adresse in Geräten wie Druckern, Kameras und anderen IoT-Geräten konfiguriert werden.

Die Verwendung von DNS begrenzt das Risiko, außer für DNS selbst. Die Beibehaltung einer 1 am Ende der Adressen Ihrer DNS-Server kann diese Art von Problem verhindern, auch wenn es langsam verschwindet.

Die Verwendung dieser ersten verfügbaren Adresse wirft auch die Frage nach der Verwechslungsgefahr zwischen Adresse und Präfix auf. In IPv4 kann die NetzwerkkAdresse niemals für einen Host verwendet werden (außer im besonderen Fall von /31 RFC 3021 intercos), während in IPv6 dieselbe Adresse für ein Präfix und einen Host verwendet werden kann, wobei die Größe des Präfixes dann der einzige begrenzende Faktor ist. Zum Beispiel gehört ein Host 2001:db8:abcd:1234::/128 zum Netz 2001:db8:abcd:1234::/64.

Aus dem Grund der menschlichen Lesbarkeit ist es besser, die Host-Adresse 0 gar nicht zu verwenden.

• PRO SCHNITTSTELLENISOLIERUNG

Einige technische oder sicherheitsrelevante Gründe können dazu führen, dass mehrere Netzschnittstellen auf Servern eingerichtet werden. So erfordern beispielsweise bestimmte

Sicherheitsstrategien spezielle Management-Schnittstellen. Manchmal werden auch die von Backup-Agenten verwendeten Schnittstellen aus Leistungs- und Separierungsgründen aufgeteilt.

Dies wirft die Frage nach der Wahl der Ausgangsschnittstelle auf. Der IPv4-Stack eines Systems wird eine Metrik verwenden, um die Schnittstelle auszuwählen, die die Route 0.0.0.0/0 trägt, wobei die andere(n) Schnittstelle(n) darauf beschränkt sind, nur das Subnetz zu routen, an das sie jeweils gebunden sind. Es ist dann Sache des Serveradministrators, statische Routen einzurichten, oder des Netzes, NAT durchzuführen, so dass ein Management-Paket über eine NAT-Adresse ankommt, die zum selben Subnetz gehört wie die Management-Schnittstelle.

Was ist mit IPv6? Der kurze RFC 7608 besagt, dass die Routing-Entscheidung auf einem bitweisen Vergleich der Schnittstellen des Rechners mit der Zieladresse beruhen sollte. Die Schnittstelle mit den meisten gemeinsamen Bits gewinnt.

Ein Rechner mit zwei Karten mit den Adressen 2001:db8:abba:CAFE::5 und 2001:db8:abba:1001::5, der ein Paket an 2001:db8:abba:C9D6::6 sendet, verwendet also die erste der beiden Karten.

Dieser Punkt sollte in Ihrem Adressplan berücksichtigt werden, um ein hochrangiges Präfix für Management oder Backup zu reservieren, da dies die Verwendung dedizierter Schnittstellen erleichtert.

Gibt es eine andere Methode, um die Verwendung einer bestimmten Schnittstelle zu einem Off-Link-Präfix zu erzwingen, ohne die Host-Konfiguration zu ändern und ohne einen Plan auf der Grundlage des RF 7608 erstellt zu haben?

Bei IPv4 ermöglicht die Verwendung der DHCPv4-Option 121 (klassenlose statische Routen) die Weiterleitung von Routen an eine Schnittstelle (Anmerkung: diese Option überschreibt die Standardroute, die bekannt gegeben wurde und in eine Option 121 kopiert werden muss, wenn sie bekannt gegeben werden soll).

In IPv6 gibt es nichts Vergleichbares, die Ankündigung eines Präfixes über die Router-Advertisement mit dem L-Bit (on-link) auf 0 führt nicht zum Erlernen einer indirekten Route. Bei DHCPv6 gibt es keine Entsprechung zur DHCPv4 Option 121.

Der RFC 4191 schlägt eine Erweiterung (Typ 24) der RA vor, die es erlaubt, Routen zu propagieren. Er wurde von Microsoft geschrieben und funktioniert seit Windows Vista, der Linux-Kernel implementiert sie ebenfalls seit den Commits 930d6ff und ebacaaa von 2006. Allerdings ist die Option nicht unbedingt aktiviert.

Seien Sie vorsichtig, dieser RFC besteht aus zwei Teilen, einer betrifft den korrekten Umgang mit der RA-Priorität, der andere befasst sich mit zusätzlichen Routen.

Wenn Sie diese Option nicht verwenden können, können Sie versuchen, Präfixe mit der Option "on-link" auf 1 gesetzt zu senden. Die Hosts fügen dann dem Router eine Route für dieses Präfix hinzu. Dies ist jedoch eine Abweichung von der Vorgabe.

• IP IPv4 / IPv6 MAPPING

Wie im Abschnitt über Dual-Stack erörtert, führt die parallele Nutzung von IPv4 und IPv6 zu einem zusätzlichen Konfigurations- und Betriebsaufwand und damit zu zusätzlichen Kosten.

Best Practises können Automatisierungen begünstigen, die diesen Aufwand verringern.

Netz-Präfix-Nummer

Es ist wichtig, eine Datenbank für die Zuordnung zwischen einem IPv4-Netz und dem entsprechenden IPv6-Netz zu haben. Ideal ist es, diese Funktion innerhalb des IPAM zu haben, oder alternativ ein Feld im IPv6-Abschnitt des IPAM zu verwenden, um das zugehörige IPv4-Netz mit seiner Maske anzugeben.

Wenn das IPAM diese Informationen nicht speichern kann, auch nicht durch Tricks, muss ein separates Inventarisierungstool verwendet werden. Dies kann ein anderes IT-Repository, eine spezielle Datenbank usw. sein. Wichtig ist, dass das Repository API-fähig ist, damit es von anderen Systemen angefragt werden kann.

Nehmen wir das Beispiel der Firewall-Filterregeln: Es wäre viel zu umständlich, bei der Einrichtung alle bestehenden Regeln in IPv6 neu zu erstellen und dann den Prozess der Flow Opening Request zu verdoppeln.

Stattdessen ist es möglich, Automatisierungen zu implementieren, die jede Nacht prüfen, ob jedes IPv4-Netz-Objekt eine IPv6 Entsprechung hat, und wenn dies nicht der Fall ist, das Objekt ändern, um das zugehörige IPv6-Präfix hinzuzufügen. Auf diese Weise werden Fehler vermieden, unabhängig davon, ob sie vom Firewall-Administrator oder von Antragstellern stammen, die sich bei der Beantragung bezüglich des IPv6-Präfixes irren könnten.

Mit einer fortschrittlicheren Lösung ist es möglich, Änderungen synchron zu verwalten, ohne sich um den Dualstack zu kümmern.

Hostnummer/Schnittstellen-ID

In der zweiten Hälfte der Adresse befinden sich die 64 Bits für die Host-Identifizierung. Auch hier gibt es Best Practises, um die Zuordnung der IPv4- und IPv6-Adresse eines Dual-Stack-Hosts zu erleichtern.

Diese Praktiken funktionieren natürlich nur bei stateful DHCPv6 oder manueller Adressierung, nicht bei SLAAC oder stateless DHCPv6.

Am einfachsten ist es, die IPv4-Nummer beizubehalten und sie auf IPv6 zu übertragen. Nehmen wir das Netzwerk 10.2.3.128/25 und einen Server 10.2.3.239. Nach der IPv6-Einführung verwendet dieses Netzwerk willkürlich das folgende Präfix 2001:db8:abba:CAFE::/64.

Die Nummerierung des Servers 2001:db8:abba:CAFE::239 erleichtert die Administration und die menschliche Lesbarkeit. Man kann auch das hexadezimale 2001:db8:abba:CAFE::EF verwenden, wenn man will, dass die Werte die gleiche strenge Nummerierung aus binärer Sicht behalten, allerdings geht dabei die Lesbarkeit verloren.

Eine andere Möglichkeit ist die Beibehaltung der Ordnungszahl anstelle der Nummer. Beim Netzwerk sehen wir, dass der Server die 89. nutzbare IPv4 des Netzwerks 10.2.3.128/25 (239-129=110) verwendet. 128 ist die Netzwerknummer und ist hier in IPv4 nicht zuweisbar.

Dieses Ordnungsmuster ergibt 2001:db8:abba:CAFE::110 oder 2001:db8:abba:CAFE::6E in reinem

Hexadezimalformat.

Den Akribischsten unter Ihnen wird aufgefallen sein, dass die Hostnummer ::0 in IPv6 verwendbar ist, da es keine Netzwerknummer und keine Broadcast-Adresse gibt, basierend auf diesem Postulat könnte man auch im Ordinalmodus eine IPv4 .1 Adresse in IPv6 ::0 umwandeln. Dies ist jedoch wegen der Verwechslungsgefahr mit einem Präfix nicht praktikabel und kann auch zu Problemen auf den Systemen führen, z. B. wegen schlecht implementierter Feldprüfungen, wie bereits erwähnt.

Die Wahl zwischen diesen beiden Methoden und den beiden Gegenstücken (dezimal oder hexadezimal) ist von Ihnen zu diskutieren. Die erste Methode in ihrer dezimalen Version ist eindeutig die praktischste, aber andere Kriterien können ins Spiel kommen, wenn wir uns einer orchestrierten Welt nähern.

Hier sind einige Beispiele:

IPv4 Netzwerk	IPv4 Host	IPv6 Hostnummer - Zuordnung	IPv6 Hostnummer - Ordinal
10.2.3.128 25	10.2.3.239	::239 dec ::EF hex	::110 dec ::6E hex 239-129
10.2.4.0 24	10.2.4.239	::239 dez ::EF hex	::239 dez ::EF hex 239
10.5.0.0 23	10.5.0.239	::239 dez ::EF hex	::239 dez ::EF hex 239
10.5.2.0 23	10.5.3.239	Relativ ::1239 dez ::4D7 hex Absolut ::3239 dez ::CA7 hex	::495 dec ::1EF hex (256+239)
10.6.0.0 16	10.6.28.239	::28239 dez ::6E4F hex 28 * Byte+239	::7407 dez ::1CEF hex (28x256) + 239
	10.6.28.3	::28003 dez ::6D63 hex 28 * Byte+003	::7171 dez ::1C03 hex (28x256) + 3
10.8.64.0 18	10.8.72.50	Relativ ::8050 dc ::1F72 hex (72-64)=8 Blöcke + 050 Absolut ::72050 d ::11972 hx	::2098 dez ::832 hex (8x256) + 50

Anhand der Beispieltabelle sehen wir, dass bei einem IPv4-Netz, das auf der Ebene des letzten Bytes (/24) aufgeteilt wird, die Ordnungszahl den gleichen Wert hat wie die Abbildung, da die Zählung in beiden Fällen bei 0 beginnt.

Komplexer wird es bei einem IPv4-Netz, das größer als ein Byte ist, im Beispiel ein /23. Wie können wir hier zwischen 10.5.0.239 und 10.5.1.239 unterscheiden? Das Hinzufügen einer 1, um anzuseigen, dass wir uns über das letzte Byte hinaus bewegen, scheint eine gute Methode zu sein. Wir zählen dann alle Adressen der /24, die das Netz bilden, einschließlich der nicht zuweisbaren Adressen, also 256.

Aber das Streben nach Lesbarkeit hätte uns auch dazu bringen können, das vorherige Byte zu kopieren und ::3239 statt ::1239 zu definieren und so von einem relativen zu einem absoluten Verweis überzugehen. Außerdem können wir sogar die IPv4-Nummer des gesamten Hosts in seine IPv6-Hostnummer kopieren, was allerdings nicht die eleganteste Lösung ist.

Die folgenden Beispiele veranschaulichen auch die Notwendigkeit, die 0 der Bytes im "Mapped"-Modus beizubehalten, um keine Duplikate zu erzeugen. 003, 050, usw.

Wie Sie sehen, kommt es darauf an, die technischen Regeln klar zu definieren und sie einzuhalten.

Zusammengefasst:

- Die dezimale Übertragung, d. h. das Kopieren des vollen Bytes oder sogar von 2 Bytes für Netze größer als /24 (usw.), ist eindeutig besser für die Lesbarkeit. Es führt jedoch zu langen Hostadressen.
- Die Verwendung von Hexadezimalzahlen ist wahrscheinlich nur in einer automatisierten Umgebung von Vorteil.
- 2 BE or not 2 BE, die Verwendung von Hexa und 2er-Potenzen macht streng das Hirn an.
- Auch diese Lösungen ermöglichen die Erstellung von ACLs usw., ohne dass die Arbeit doppelt gemacht werden muss.

Die Zuordnung kann auch über die DNS-Einträge A und AAAA der einzelnen Server erfolgen, was dann eine andere Form der Genauigkeit erfordert.

Was die Hosts betrifft, so scheint es derzeit kein Produkt zu geben, das es ohne vorherige Konfiguration ermöglicht, dieselbe Hostnummer in IPv4 und IPv6 auf der Grundlage einer integrierten IPAM-Zuordnung zuzuweisen.

• NATIVE IPv6-NETZE

Wenn Sie ein natives IPv6-Netz einrichten, gelten die vorherigen Regeln für Hosts nicht. Sie können dann einen Teil der 64 Bits zur Angabe von Hostdetails verwenden.

Zum Beispiel ein Buchstabe zur Bezeichnung eines Desktop-Servers, ein anderes Zeichen zur Angabe eines Druckers. Dies sollte Sie an die bestehenden technischen Regeln / Namenskonventionen für Hostnamen erinnern.

In einem Rechenzentrum kann man sich vorstellen, das mit einer VM verbundene Unternehmen zu markieren, usw.

Mit einer CMDB bleibt dies jedoch komplex und redundant, zumal die Adresse bei Bedarf nicht einfach geändert werden kann.

Die andere Lösung, zumindest auf der Serverseite, besteht darin, die Schnittstellen-ID so festzulegen, dass sie statisch ist und nicht von der MAC-Adresse abhängt (und sich daher nicht ändert, wenn die Karte - physisch oder virtuell - ausgetauscht wird, und den Hersteller in der Adresse nicht preisgibt). In Verbindung mit SLAAC für die Erzeugung der Interface-ID. Diese Lösung ist immer einfacher als eine manuelle Konfiguration.

Im Allgemeinen ist es nur in kleinen Mehrzwecknetzen an kleinen Standorten notwendig, eine Bereichssegmentierung zu definieren.

• Internet BGP-Announcement

Was soll im Internet announced werden?

Auf diese Frage werden einige antworten: "So wenige Ressourcen wie möglich". Stellt die direkte Ankündigung einer /32-DMZ anstelle einer /44-DMZ wirklich eine Verringerung der Angriffsfläche dar? Wird es bei der Implementierung von Stateful- und IPS-Firewalls eine Rolle spielen? Das Ende-zu-Ende-Ziel von IPv6 wird wahrscheinlich sowieso dazu führen, dass breite Advertisements geschaltet werden.

Betrachtet man den Inhalt der BGP-IPv6-Tabelle, so stellt man fest, dass die meisten Advertisements /32, /40, /44 und /48 sind.

Adds and Wdls per Prefix Length

/28	+1	-0
/29	+41	-13
/30	+3	-2
/31	+1	-3
/32	+131	-110
/33	+49	-31
/34	+53	-58
/35	+35	-11
/36	+141	-26
/37	+4	-3
/38	+28	-3
/39	+4	-9
/40	+436	-55
/41	+8	-2
/42	+9	-9
/43	+26	-3
/44	+147	-74
/45	+42	-6
/46	+67	-126
/47	+8	-3
/48	+871	-969
/52	+2	-0
/56	+23	-27
/128	+4	-0

Die /48-Einträge machen mit 54.000 Routen die Hälfte aller Einträge aus, nicht aber das Volumen der eindeutigen Adressen, da jedes /32 65.536 (2e16) mal mehr Adressen enthält als eine /48.

<http://bgp.potaroo.net/v6/as6447/>

<https://bgp.potaroo.net/index-v6.html>

<https://www.cidr-report.org/v6/as2.0/>

Die letzte URL zeigt den Wochenbericht mit den beobachteten Eintragungen und Löschungen von Präfixen an.

Wöchentliches IPv6 Delta

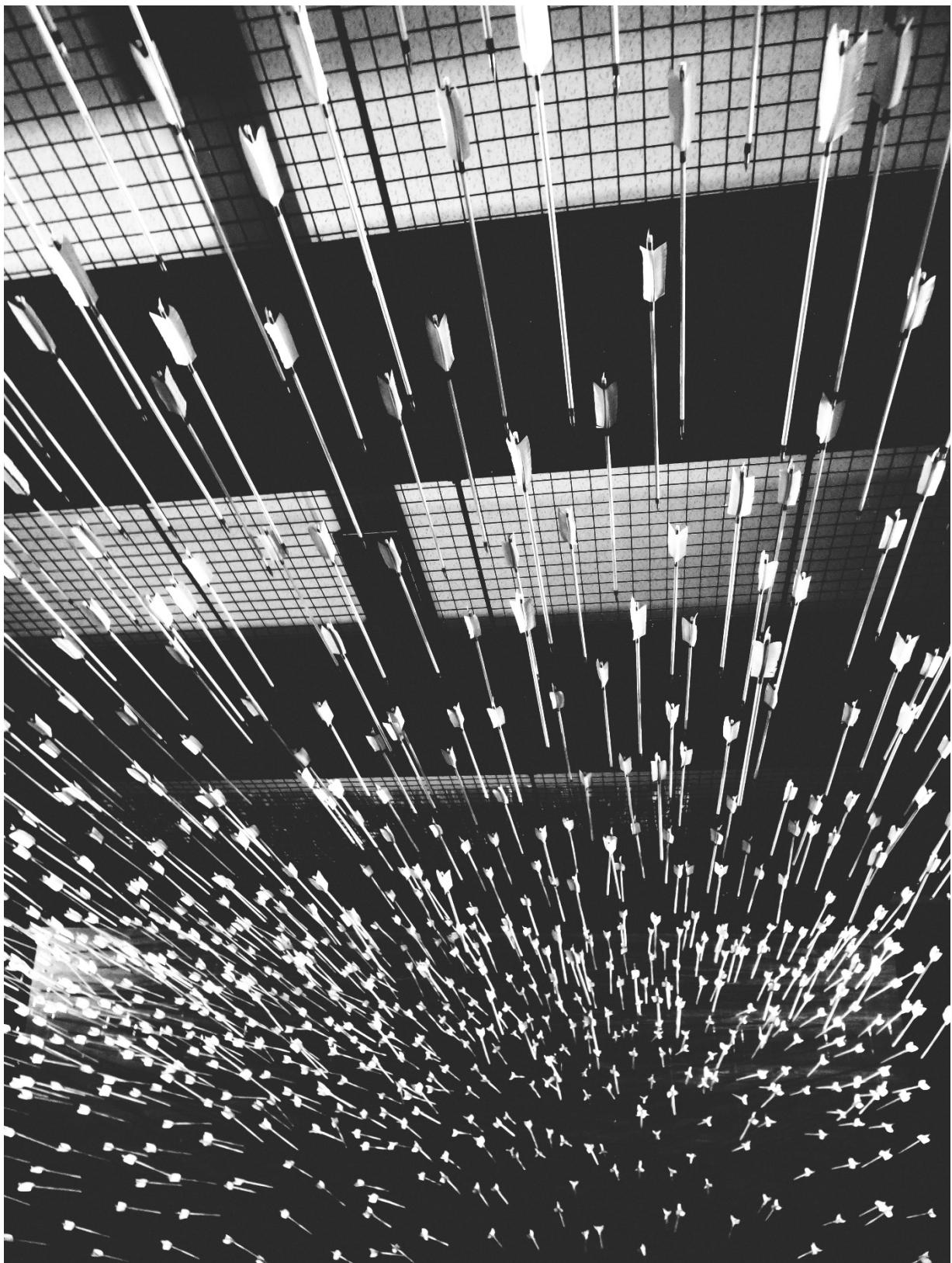
<https://cidr-report.org/v6/as2.0/>

Einige Anti-DDoS-Lösungen funktionieren, indem sie das angegriffene Präfix über ein "reinigendes" Netzwerk erneut ankündigen. Da /48 das kleinste ist, müssen Sie bei dieser Art von Lösung nominal mehr ankündigen.



Idealerweise advertise Sie in großem Umfang entsprechend der geografischen Lage Ihrer Internetknoten. IPv6-Peering kann auch eine Gelegenheit sein, mit RPKI-Routensignierung zu experimentieren, falls Sie dies noch nicht tun, oder mit RTBH und Flowspec zu experimentieren.

Teil V: Sicherheit und Best Practises



Sicherheit und Best Practises

Mit der Einführung der neuen Version des IP-Protokolls kommt die Anforderung, Sicherheitsregeln auf verschiedenen Ebenen zu implementieren. Viele dieser Regeln entsprechen den Best Practises von IPv4, andere sind spezifisch für IPv6.

Es ist besonders wichtig, dass Sie die IPv4-Sicherheitsmechanismen und die IPv6-Funktionen beherrschen, insbesondere die Varianten der Adresszuweisung und die Verwendung des des Neighbor Discovery Protocol (RFC 4861), bevor Sie mit diesem Abschnitt beginnen.

Um Ihnen die Zuordnung der Regelumsetzung auf Ihren Geräten zu erleichtern, sind sie in folgende Bereiche unterteilt:

- TRANSIT für jedes L3-Gerät (Router, FW usw.);
- ACCESS befasst sich mit der letzten Meile, den Geräten der Host-Träger und ihren Besonderheiten. Er befasst sich speziell mit NDP und der Interaktion mit der OSI-Schicht 2 (MAC);
- HOST bezieht sich auf Endgeräte, hauptsächlich Computer und Server;
- FILTERING für Firewalls.

Access

• DYNAMISCHE ADRESSZUWEISUNG

Zur Verfolgung von Endgeräten innerhalb einer Organisation wird DHCPv6 stateful wegen seiner Fähigkeit gegenüber der automatischen Adresszuweisung auf der Grundlage von SLAAC bevorzugt. Server können statische Adressierung verwenden. Einige Geräte, vor allem Android-Geräte, unterstützen DHCPv6 nicht, was manchmal zu Ausnahmen führen muss, siehe dazu das entsprechende Kapitel.

Zunächst sei daran erinnert, dass die Verwendung von Router Advertisements (RA) erforderlich ist, auch bei DHCPv6 stateful. Dieses RA liefert zumindest die Link-Local-Gateway-Adresse und die Zeitgeber. Nur eine vollständige und nicht empfohlene manuelle IPv6-Konfiguration erlaubt es, auf RA zu verzichten.

Mechanismen

Mehrere Bits werden verwendet, um Hosts anzuzeigen, wie sie sich verhalten sollen:

- A - "Autonomous Address Autoconfiguration" sagt dem Host, dass er sich selbst konfigurieren soll (SLAAC RFC 4862);
- M - "Managed Address Config" gibt auf der Gegenseite an, DHCPv6 stateful (RFC 3315) zu verwenden, um seine Adresse zu beziehen;
- O - "Other Config" gibt an, dass andere Optionen außer der IPv6-Adresse von einem Zustandslosen DHCPv6 (RFC 3736) geholt werden können, diese Optionen können DNS-Server, NTP, Domänensuffix, usw. beinhalten;
- L - "On-Link" zeigt an, dass das RA und der Präfix sich auf demselben L2-Link befinden. Dieses Bit wird auf 0 zurückgesetzt, wenn die Ankündigung einen Router überquert, um Störeffekte einer falsch konfigurierten L2-Erweiterung oder ungewolltes Relaying zu vermeiden. Im Gegensatz zu IPv4 geht ein IPv6-Host nicht davon aus, dass ein Host, der sich im gleichen Präfix wie er befindet, direkt in L2 erreicht werden kann (außer bei link-lokalen Adressen). Siehe RFC 5942.

Beachten Sie, dass die Bits A und L innerhalb des Präfixes gesendet werden, nicht im RA-Bereich.

Methode	Bit A+ Auto	Bit M Manage d	Bit O Other	Resultierende Adressen	Optionen	
SLAAC	1	0	0	-temporary (kurzlebig) -Link-Lokal	SLAAC	RDNSS RFC 6106
Stateless DHCPv6	1	0	1	-temporary (kurzlebig) -Link-Lokal	SLAAC	DHCPv6

Methode	Bit A+ Auto	Bit M Manage d	Bit O Other	Resultierende Adressen	Optionen
Stateful DHCPv6	0	1	Redundant mit M	-DHCPv6 -Link-Lokal	DHCPv6
DHCPv6 Stateful + SLAAC (Wahl des Host-Betriebssystems)	1	1	Redundant mit M	-OS Wahl -Link-Lokal	DHCPv6 oder RDNSS je nach Betriebssystem

Die dritte Methode (Stateful DHCPv6) ist dank ihrer Fähigkeit zur Gerätenachverfolgung ideal für Unternehmen.

Vergewissern Sie sich, dass Sie nicht versehentlich den letzten Fall nutzen, in dem die Dinge zufällig sind.

Wenn ein System einer RA mit auf 1 gesetzten A- und M-Bits präsentiert wird, konfigurieren die meisten Betriebssysteme beide und verwenden nur eine der Methoden für ausgehende Verbindungen (hauptsächlich SLAAC temporäre Adresse + Privacy Extensions) oder lassen RFC 7608 entscheiden, indem sie die längste übereinstimmende Adresse des Hosts mit dem Ziel vergleichen. Nur verwenden, wenn Sie Adresslotterie mögen. Dies ist ein übliches Verhalten von Heimroutern. RFC 4862 erwähnt in seinem Abschnitt 5.6, dass die zuletzt erhaltenen Informationen verwendet werden sollten.

Es ist möglich, einem Client über DHCP mehrere Adressen in verschiedenen Präfixen zur Verfügung zu stellen; dieser Fall wird hier nicht behandelt.

Interessanter Punkt: Wenn Sie jemals eine Infrastruktur mit dem zweiten Fall (zustandsloses DHCP) einrichten, dann müssen Ihre Server keine Leases synchronisieren, sondern nur die Konfiguration der Optionen für jedes Präfix.

Beachten Sie, dass einige Betriebssysteme wie Windows eine DHCP-Anfrage senden, auch wenn das RA angibt, SLAAC zu verwenden.

DHCP Identifizierung

DHCPv6 verlässt sich nicht auf die MAC-Adresse wie bei IPv6, sondern der Host gibt eine Kennung namens DUID an. Dieser Bezeichner wird später im Abschnitt "Hosts" des Sicherheitskapitels näher erläutert.

DHCPv6 bietet Optionen, die in IPv4 als Unteroptionen 82 existieren, und führt einige neue ein.

- Herstellerklasse (Option 16) ermöglicht es dem Client-Gerät, seinen Hersteller, sein Modell, seine Version usw. zu senden;
- Vendor Specific (Option 17) für proprietäre Optionen;
- Interface-ID (Option 18), die es ermöglicht, den Namen einer Schnittstelle und das VLAN zu identifizieren. (Circuit-ID in DHCPv4);

- Remote-ID (Option 37) RFC 4649, mit der der physische Port, die einem VPN zugewiesene Benutzer-ID und insbesondere die MAC abgerufen werden können;
- Subscriber-ID (Option 38) wird eher von Internetprovidern für andere Identifikationsinformationen verwendet.

Missverständlich werden diese Optionen auch bei DHCPv6 oft als Option 82 bezeichnet, während es bei DHCPv4 die Option 82 ist.

Es ist möglich, die MAC des Clients in der Option Remote-ID bei Zugangsgeräten (Switches, AP usw.) anzugeben. Dies ist wichtig, da so die MAC-Adresse der Hosts erfasst werden kann.

Weitere Empfehlungen in Bezug auf DHCPv6 zur Erleichterung der Identifizierung von Endgeräten finden Sie im Abschnitt "Hosts".

• ICMP REDIRECT BLOCKING

Das *Neighbor Discovery Protocol* umfasst fünf Nachrichtentypen:

- *Router Solicitation* und *Advertisement*;
- *Neighbor Solicitation* und *Advertisement*;
- *Redirect*.

Mit diesem neuesten Nachrichtentyp kann das Gateway angeben, dass ein anderer Router verwendet wird, um ein bestimmtes Ziel zu erreichen, und dass der Host seine Routing-Tabelle entsprechend aktualisieren sollte.

ICMP-Redirect (Typ 137) sollte blockiert werden, da es einem Angreifer ermöglichen könnte, den Verkehr umzuleiten. Diese Option sollte nur verwendet werden, wenn ein Netzwerksegment zwei Router hat, die unterschiedliche Ressourcen erreichen; ein sehr seltener Fall.

• IPv6 SNOOPING

Erinnern wir uns zunächst kurz an den Zweck der beiden häufigsten Nachrichtentypen im NDP.

Die Nachrichten "Neighbor Solicitation" (135) und "Advertisement" (136) werden verwendet, um die Verbindung mit Schicht 2 innerhalb eines Netzwerksegments herzustellen, wobei in der Regel die MAC-Adresse eines Hosts auf der Grundlage seiner IP-Adresse abgefragt und beantwortet wird. Wie ARP in IPv4.

Die Abfrage erfolgt im Multicast-Modus, im Unicast-Modus kann auch geprüft werden, ob ein Host noch erreichbar ist, wobei in diesem Fall angegeben wird, wer gefragt wird (Zieladresse).

Wenn diese Adresse nicht angegeben ist (::/128), handelt es sich um eine DAD-Nachricht (Duplicate Address Detection)

Die Antwort auf eine Neighbor Solicitation hat ein "Override"-O-Bit, das standardmäßig auf 1 gesetzt ist, um anzugeben, dass ein vorhandener Eintrag in einem ND-Cache überschrieben werden soll. Der RFC gibt an, dass das Setzen des Bits auf 0 für Proxified-Antworten auf Aufforderungen

oder für Anycast-Dienstadressen gedacht ist.

Praktisch ergeben sich die folgenden zwei Beispiele:

- Ein ND-Proxy (ARP-Proxy-Äquivalent) überschreibt mit seiner Antwort nicht eine direkte Antwort, die der betroffene Host direkt hätte senden sollen.
- Zwei Server mit der gleichen Anycast-Adresse in einem Segment werden nicht versuchen, die sie betreffenden Einträge zu überschreiben.

Das S-Bit "Solicited" gibt an, dass die Antwort für eine Unicast-Anfrage mit Zieladresse, d. h. eine Erreichbarkeitsanfrage, bestimmt ist.

Das Bit R "Router" schließlich zeigt an, dass der Host ein Router ist. Wenn es auf 0 gesetzt ist, wird die Erkennung der Unerreichbarkeit des Nachbarn zu dem Schluss kommen, dass der Host nicht mehr in der Lage ist, ein Routing durchzuführen. Es wird dann eine Router-Solicitation eingeleitet und auf einen anderen verfügbaren Router umgeschaltet (basierend auf Prioritäten, falls mehrere vorhanden sind).

Bevor wir überhaupt über Router Solicitation und Advertisement sprechen, werden Sie bereits bemerkt haben, was ein Angreifer mit den NDP-Nachbarschaftsinformationen anstellen kann. Es wird daher dringend empfohlen, zumindest in der Infrastruktur der Zugangsebene auf dem Campus/Benutzerseite geeignete Antispoofing-Mechanismen zu implementieren.

NDP erzeugt Multicast-Gruppen, die Solicited-Node Multicast genannt werden. Jeder Host erstellt eine Multicast-Gruppe für jede zugewiesene Adresse, die ein standardisiertes Präfix FF02:0:0:0:1:FF00::/104 und die letzten 24 Bits der Adresse enthält. Diese Multicast-Adressen werden für DAD verwendet, aber auch, um einen MAC/IP-Abgleich durchzuführen, ohne alle zu stören, wie es beim ARP-Broadcast in IPv4 der Fall ist.

Der erste Kontakt zwischen zwei IPv6-Knoten im selben Netz ist daher immer ein Multicast.

ND-Fragmentierung

RA-Nachrichten können groß sein, wenn sie viele Präfixe enthalten und daher eine Fragmentierung erfordern. In RFC 6980 heißt es, dass es dann besser ist, mehrere Nachrichten zu senden, anstatt das Paket zu fragmentieren. Es gibt nur wenige Gründe, so viele Präfixe und Optionen in einer RA zu haben, das 1280 Byte Größe erreicht werden, dem IPv6-Minimum.

Daher sollten NDP-Protokollfragmente blockiert werden.

Zuordnung

Die Sicherheitsmechanismen beruhen Switch-intern auf dem Aufbau einer Tabelle mit Beziehungen zwischen IP, MAC und physischem Standort, in der Regel dem Switch-Port.

Der einfachste Weg ist die Nutzung von DHCPv6-Snooping, das die von DHCPv6 zurückgegebenen IPv6-Zuweisung nutzt, um eine Steuertabelle, die sogenannte Bindingtable, zu erstellen.

ND, DHCPv6 und andere Prüfungen werden nicht immer auf die korrekteste Weise implementiert. Einige funktionieren perfekt mit Header-Erweiterungen und sogar Fragmentierung. Andere wiederum funktionieren nur im einfachsten Fall. Diese Diskrepanz ist häufig auf die ASIC-Fähigkeiten des Geräts zurückzuführen. Bei einigen Produktlinien wird die Funktion in der Control-Plane ausgeführt und ist mit den Hardware-Optimierungsoptionen daher nicht kompatibel.

Auf der Konfigurationsebene können diese Funktionen Teil eines einheitlichen Pakets sein, andernfalls die Summe mehrerer Optionen, die unabhängig voneinander zu aktivieren sind, und manchmal sogar nebeneinander bestehen (all-in-one + separat) und die Aktivierung einer Art die andere aufheben.

Prüfen Sie daher die Dokumentation des Herstellers sorgfältig und testen Sie mit einem Paketfälscher wie [scapy](#).

Jedes Alarm-/Sicherheitsevent im Zusammenhang mit diesem Regelsatz sollte einen Alarm in Ihrem SIEM auslösen.

Denken Sie daran, die Wiederherstellung der Bindingtable so einzurichten, dass sie sofort gefüllt wird, wenn der Switch neu gestartet wird. In der Regel ist es möglich, sie regelmäßig zu exportieren und/oder aktive Leases vom DHCP-Server zu holen (wenn Sie sich auf Stateful DHCPv6 verlassen).

Es ist möglich, einen Teil dieser Sicherheitsmerkmale ohne DHCP zu nutzen, allerdings beeinträchtigt der Verlust einer sicheren Lernquelle das Schutzniveau (RFC 6620). Heutzutage gibt es Unternehmen, in denen DHCP in Verbindung mit statischen Leases innerhalb des Rechenzentrums verwendet wird, um dieses Sicherheitsniveau auf der Server-Hosting-Zugriffsebene zu gewährleisten. Es ist dann keine manuelle Hostkonfiguration mehr erforderlich.

Ohne DHCP baut das Gerät die Tabelle auf der Grundlage der ausgetauschten DAD-Nachrichten während der automatischen SLAAC-Zuweisung auf.

Beachten Sie, dass bei L3-Fabric-basierten Lösungen das Signalisierungsprotokoll der für den Aufbau der Tabelle erforderlichen Informationen enthält und eine Überprüfung nur für bestimmte Konfigurationen erforderlich ist. In einer EVPN+VxLAN-Infrastruktur wird das MAC/IP-Paar beispielsweise bereits über EVPN-Routen des Typs 2 angekündigt.

Aus dieser Tabelle können dann verschiedene Prüfungen abgeleitet werden, hier die wichtigsten:

Quelle

Ein Paket mit einer unbekannten, nicht zugewiesenen Quelladresse wird verworfen. Der Switch kann versuchen, den DHCP-Server und/oder seinen Nachbarn über NDP zu fragen, ob die Adresse bekannt ist, bevor er den Verkehr verwirft.

Diese Prüfung setzt das Vorhandensein einer Bindingtable voraus, sie führt selbst keine ND-Prüfung durch.

Vergessen Sie nicht, den Verkehr über die lokale Link-Adresse zuzulassen, manchmal über einen zusätzlichen Befehl, und vertrauenswürdige Ports für statische Ressourcen wie manuell adressierte Server.

Zielort

Wenn ein Paket eintrifft, überträgt das Gerät es und führt gegebenenfalls eine ND-Auflösung durch, wenn der Empfänger in der Bindingtable bekannt ist. Andernfalls wird das Paket verworfen.

Dieser Mechanismus ermöglicht es, Datenverkehr an eine missgebildete oder nicht existierende Adresse zu kontern, zum Beispiel für lokale Denial-of-Service-Zwecke.

Umzüge

Wenn ein Host zu einem anderen Anschluss wechselt, kann die physische Standortverfolgung eine ND-Solicitation an den Host an der zuvor bekannten Position in der Bindingtable initiieren. Erhält er eine Antwort, so ist der Neuankömmling ein Spoof.

Dadurch wird der Angriff dann unwirksam, wenn der ursprüngliche Host online ist und antworten kann.

ND Unterdrückung

Zur Optimierung des Datenverkehrs und zur Begrenzung des Multicast-Verkehrs ist es möglich, das Zugangsgerät anstelle des betreffenden Hosts auf NS Neighbor Solicitation-Anfragen antworten zu lassen. Diese Funktion kann zumindest für Multicast-Anfragen, aber auch für Unicast aktiviert werden. ND/ARP-Unterdrückung ist eine übliche Funktion bei EVPN/VxLAN-Verbindungen (wo das Lernen anders abläuft), kann aber auch bei einigen Campus-Produkten eingesetzt werden.

Bedenken Sie jedoch, dass eine der Verwendungen von Unicast-Anfragen (die mit der Zieladresse) darin besteht, die Erreichbarkeit eines Hosts zu prüfen. Es ist daher nicht sinnvoll, im Namen des Hosts für etwas anderes als Multicast zu antworten, es sei denn, das Gerät unterscheidet zwischen Unicast-Anfragen mit und ohne Zieladresse und handelt nur im letzteren Fall.

Mit anderen Worten, ein Gerät sollte niemals ein Neighbor Advertisement mit auf 1 gesetztem S-Bit anstelle des Hosts senden müssen.

Eine mögliche Ausnahme ist WiFi, wo die Überwachung der Funkverbindung mit der Station durch den Zugangspunkt die Beantwortung anstelle der Station selbst für einen Erreichbarkeitstest zulassen kann. Dabei wird einem weniger gesprächigen Medium, dem Funkkanal, Vorrang eingeräumt.

Präfix

Auf der Grundlage von Informationen aus den folgenden Quellen:

- Router-Ankündigung;
- DHCP-Präfix-Delegation;
- Manuelle Konfiguration, falls erforderlich.

Mit der Präfixkontrolle können Sie ein Paket blockieren, dessen routingfähige Quelladresse nicht zu dem im L2-Segment verwendeten Präfix gehört. So wird Adress-Spoofing auf der Zugriffsschicht blockiert, noch bevor URPF später z. B. beim Routing verwendet wird.

Cache-Poisoning

Wie sein Vorgänger ARP Cache Poisoning ist es möglich, den ND-Cache von Hosts zu füllen, was zu einem Überlauf führt. Insbesondere bei 2^{64} möglichen Adressen in einem Netzwerk hat ein Angreifer viele Möglichkeiten.

Ein gängiger Angriff besteht darin, sich in einem Neighbor Advertisement als Router auszugeben und das R-Bit auf 0 zu setzen, was bedeutet, dass die Route nicht mehr verwendet wird. Der Angreifer kann auch einen Man-in-the-Middle-Angriff versuchen, indem er sich als Host oder Router ausgibt.

Die Binding Security verhindert dieses Verhalten, aber es wird dennoch empfohlen, eine Begrenzung der Cache-Größe für Netzwerkgeräte festzulegen. Wenn Sie eine granulare Begrenzung berechnen wollen, denken Sie daran, dass es nicht ausreicht, Hosts, sondern Adressen zu zählen. Jeder Host hat mindestens 2 und kann mehr haben (SLAAC mit temporären Adressen zum Beispiel). Moderne Betriebssysteme verfügen in der Regel über akzeptable Vorgabewerte.

Für weitere Informationen siehe RFC 6583.

• DHCP ROGUE

Physisch

Der in RFC 7610 beschriebene DHCP-Shield-Mechanismus umfasst die Definition der physischen Ports, die DHCP-Server-Datenverkehr empfangen dürfen. Im Allgemeinen handelt es sich um Uplink-Ports. DHCP-Verkehr von nicht definierten Ports wird verworfen.

Das Gerät muss den gesamten Inhalt jeder Nachricht, die vom DHCP-Server kommt, analysieren. Auch hier ist je nach ASIC und Implementierung Vorsicht geboten.

Wenn das Gerät diese Funktion nicht unterstützt, ist es immer noch möglich, eine ACL zu verwenden, die den Verkehr mit dem Quellport UDP 547 und dem Zielport UDP 546 blockiert, aber es wird nicht mit einem gefälschten fragmentierten Paket funktionieren.

Logisch

Der ausführliche RFC 8415, der sich mit DHCPv6 befasst, enthält einen Abschnitt über die Sicherung des Datenaustauschs zwischen dem Server und den Clients und/oder Relays.

IPsec kann zur Authentifizierung oder sogar Verschlüsselung des DHCP-Austauschs zwischen Servern und Relays verwendet werden (RFC 8213). Die kryptografische Konfiguration kann manuell oder auf der Grundlage einer PKI vorgenommen werden.

Die Verwendung von IPsec kann auch anderen Verwaltungsverkehr wie Syslog, SNMP, NTP, RADIUS usw. schützen.

Achtung, die Unterstützung von IKEv2 mit Pre-Shared Secrets ist in diesem RFC nicht zwingend vorgeschrieben.

Die Verwendung eines einfachen gemeinsamen Schlüssels ermöglicht es einem Angreifer, Pakete

wiederzugeben. RDM schränkt das Risiko des Wiederholens ein, allerdings nur auf der Client-Seite und nicht zwischen einem Relay und dem Server.

In vielen überholten RFCs wurden andere Authentifizierungsmechanismen vorgeschlagen. Heute bildet RFC 7227, der sich mit der Implementierung von DHCP-Optionen befasst, die Grundlage für viele Vorschläge. Sie können etwas über die Projekte DHCPv6Sec und Secure-DHCPv6 finden.

Der letzte in RFC 8415 verfügbare Sicherheitselement, RKAP (Reconfiguration Key Authentication Protocol), verhindert die Neukonfiguration eines Clients durch einen böswilligen Server. Bei der ersten Antwort wird ein eindeutiger Schlüssel an den Client gesendet. Der Server verwendet dann HMAC-MD5, um seine Nachrichten zu signieren.

RKAP ist jedoch neu und in der Praxis noch nicht nutzbar.

Die Rekonfiguration ist übrigens eine neue Funktion, mit der Sie Clients dazu zwingen können, DHCP erneut anzufordern (ohne auf das Auslaufen ihres Lease oder einen Neustart zu warten). Diejenigen unter Ihnen, die jemals Hunderte von PoE-Geräten neu starten mussten, damit sie eine neue Option über DHCP berücksichtigen, werden diese Funktion begrüßen. Hüten Sie sich davonr selbst DDoS auszulösen, indem Sie diese neue Funktion in einem zu großen Segment ausprobieren...

Kurz gesagt, implementieren Sie IPsec zwischen Ihren Relays und dem Server und überlassen Sie der DHCPShield-Komponente die Sicherheit der Relay-/Client-Seite nur in Bezug auf den Uplink-Ports von autorisierten DHCP-Server-Nachrichten.

Und schließlich sollten Sie immer daran denken, dass DHCPv6 demselben Client mehrere IPv6 zur Verfügung stellen kann (DUID).

• RA GUARD

Router Advertisement-Nachrichten sind ein zentraler Punkt von IPv6, es muss sichergestellt werden, dass sie von einem autorisierten Router ausgegeben werden.

RFC 6105 empfiehlt, eines oder mehrere der folgenden Elemente in Zugangsgeräten manuell zu setzen, um eine RA-Nachricht zu validieren oder zu blockieren:

- Physischer Anschluss;
- MAC-Adresse des Routers;
- Gateway-IP;
- beworbenes Präfix;
- RA-Priorität;
- Hop-Count-Grenze;
- Wert der Bits M - Managed und O - Other.

Am einfachsten ist es, nur Uplink-Schnittstellen zuzulassen, wobei es oft auch möglich ist, eine TTL-Grenze festzulegen.

Der RFC schlägt auch einen so genannten zustandsabhängigen Lernmodus vor, bei dem das Gerät die RA-Quelle(n) für einen bestimmten Zeitraum lernt. Danach würde es keine neue RA-Quelle mehr akzeptieren.

Dieser zustandsbehaftete Modus wird allmählich in Geräte implementiert.

Wenn der Router auf einen Zwilling umschaltet, der ein Protokoll vom Typ NHRP verwendet, muss sichergestellt werden, dass das Fehlen eines gespeicherten Nachbarn dazu führt, dass das Gerät in den Lernzustand zurückfällt, oder dass sich die kontrollierten Elemente nicht ändern (z. B. eine virtuelle MAC oder IP).

Wenn das Gerät den RA-Guard nicht unterstützt, können Sie zumindest Router Advertisements mit einer ACL an den Zugangsports blockieren.

• RA HOP LIMIT

Um zu verhindern, dass ein Router Advertisement aus dem Segment herausspringt, erinnert uns Abschnitt 6.1 von RFC 4861 an die grundlegenden Kontrollen, die bei ND-Nachrichten durchzuführen sind. Solche Kontrollen wie die Löschung von RA mit einem Hop-Limit unter 255 sollten automatisch funktionieren, ohne dass eine spezielle Sicherheitskonfiguration erforderlich ist. Der ND Shield Entwurf <https://tools.ietf.org/html/draft-gont-opsec-ipv6-nd-shield-00> schlägt vor, weiter zu gehen.

Diese Sicherheit erinnert Sie vielleicht an das, was in BGP mit GTSM (Generalized TTL Security Mechanisms) RFC 5082 existiert. GTSM verwirft eine BGP-Nachricht, wenn ihre TTL/Hop-Limit kleiner als 254 ist, da sie diesmal mit Sicherheit nicht vom Nachbarn stammt (außer natürlich bei Verwendung der BGP-Multihop-Option).

Vergessen Sie nicht, die Konfiguration der Zwischengeräte so anzupassen, dass sie in bestimmten Konfigurationen wie einer L2-Netzerweiterung oder einfach bei der Verwendung von L3-Rechenzentrums-Switches in MLAG die Hop-Limitierung nicht einfach herabsetzen.

Seien Sie vorsichtig, denn in den Dokumentationen einiger Hersteller wird erwähnt, dass der Wert des RA-Hop-Limits bearbeitet werden muss, und oft wird ein Wert von 64 als Standard angegeben. Dies ist in Wirklichkeit das Feld *current hop-limit* (CHL), das den Hosts, die die RA empfangen, den Wert für das Hop-Limit angibt, den sie auf ihrer Seite konfigurieren.

• ANDERE RA-EINSTELLUNGEN

Nachdem wir die spezifischen Punkte zu den Modi Sicherheit und Adresszuweisung gesehen haben, wollen wir uns nun einige der anderen Einstellungen der Router-Anzeige ansehen. Diese Parameter müssen auf jeder Schnittstelle konfiguriert werden.

- RA-Intervall: Verzögerung in Sekunden zwischen zwei unaufgeforderten RA-Übertragungen, mit einem Mindest- und einem Höchstwert.
 - Der Höchstwert muss zwischen 4 und 1800 liegen. Der Standardwert ist 600s;
 - Das Minimum muss zwischen 3s und $\frac{3}{4}$ des Maximalwerts liegen. Der Standardwert ist 1/3 des Maximalwerts oder 3s, wenn der Maximalwert weniger als 9s beträgt.

- RA-Lebensdauer: Lebensdauer, nach der der Router als nicht mehr benutzbar angesehen wird. Der Wert muss zwischen dem MAX-Intervall und 9000 Sekunden liegen. Der Standardwert ist das dreifache max. Intervall.
 - Ein Wert von 0 bedeutet, dass der Router standardmäßig nicht verwendet werden soll;
 - Im Falle einer Punkt-zu-Punkt-Verbindung zwischen zwei Routern, z. B. BGP-Peering, wird die RA-Lebensdauer normalerweise ignoriert, da die Lebensdauer des Nachbarn über das Routing-Protokoll selbst überwacht wird.
- MTU: es ist möglich, den Hosts die MTU der Verbindung mitzuteilen, der Standardwert ist 0.
 - Wenn an einem Standort Probleme mit Path-MTU-D auftreten, können Sie diesen Wert vorübergehend so einstellen, dass das Problem in der ausgehenden Richtung behandelt wird, während Sie das Problem prüfen. Dies ist schneller, als jeden einzelnen Host zu konfigurieren.
- Prefix: der Router kündigt ein oder mehrere routingfähige Präfixe an, jedes mit:
 - *Lifetime* : die Lebensdauer der Route, die in Sekunden seit der letzten Ankündigung oder über eine feste Zeit angegeben werden kann. Diese letzte Option kann verwendet werden, um ein Präfix sauber stillzulegen, bevor es aus der Konfiguration entfernt wird. Der Standardwert ist 2592000 verbleibende Sekunden, also 30 Tage. Es wird nicht empfohlen, den Wert 0xffffffff zu verwenden, der dazu führt, dass die Route permanent gültig ist, was eine gute Möglichkeit ist, ein schwarzes Loch zu bauen, wenn der Router seine lokale Link-Adresse ändert;
 - *On-Link* (Bit L) : wie bereits oben erwähnt, zeigt es an, dass der Router auf dem Link ist, standardmäßig 1.
- SLAAC
 - *Lifetime* : die bevorzugte Gültigkeitsdauer der Adressen, die die Hosts selbst konfigurieren; auch dies kann in verbleibenden Sekunden oder mit einem festen Datum/Uhrzeit konfiguriert werden. Der Standardwert ist 7 Tage (604800 s). Auch hier ist es nicht empfehlenswert, unendlich (0xffffffff) zu verwenden. Schließlich ist zu beachten, dass der Wert nicht größer sein darf als die Gültigkeit der Route des zugehörigen Präfixes;
 - Wenn Sie nicht DHCP stateless mit SLAAC verwenden, können Sie DNS-Serveradressen über RDNSS angeben (obligatorisch für Android).
- Priorität
 - Die Routerpriorität kann Niedrig, Normal (Standard) oder Hoch sein. Sie können diese Option immer dann verwenden, wenn Sie nahtlos zwischen Gateways wechseln möchten, ohne dass Sie dieselbe IP beibehalten müssen. Es kann eine gute Praxis sein, die Priorität auf "Hoch" zu setzen, um die Auswirkung eines unerwünschten Eintrages zu verringern.

Weitere Felder sind im RFC enthalten, werden aber nicht verwendet und sind auf den meisten Plattformen nicht konfigurierbar (Reachable Time und Retransmit Time).

Gut zu wissen, dass die Hersteller einen Statusbefehl implementieren, um alle Präfixe anzuzeigen, die für die entsprechende Schnittstelle ausgegeben werden.

• seND (NICHT EINSETZBAR)

Die *Secure Neighbor Discovery* dient der Authentifizierung von NDP-Nachrichten innerhalb einer Organisation und wurde ursprünglich in RFC 3971 beschrieben.

Das Protokoll stützt sich auf:

- Adressen, die aus einer kryptografischen RSA-Datenbank (CGA) generiert werden RFC 3972;
- PKI und Vertrauensanker;
- Pseudozufallsuhr und Nonce (Anti-Replay).

Wenn ein Host eine Verbindung herstellt, gibt der Router den Zertifizierungspfad und den "Vertrauensanker" an, was zu einer sechsten Art von ND-Nachricht führt, der *Certificate Path Solicitation*. Siehe RFC 6494 über Zertifikatsprofile und -verwaltung und RFC 6495, X.509-Felder.

Das Vorhandensein von Zertifikaten bedeutet ein höheres Nachrichtengewicht und neue Risiken im Zusammenhang mit der Fragmentierung, siehe RFC 6980.

Wenn man sich den RFC im Detail ansieht, stellt man fest, dass ähnliche Probleme wie bei 802.1x bestehen. Wenn der RFC damit beginnt, uns daran zu erinnern, dass IPsec nicht praktikabel war, weil NDP der erste Kontakt mit einem Netzwerk ist, gibt es kein Abhilfesystem, wie es bei 802.1x der Fall ist.

Der Host muss mindestens einen Vertrauensanker vorkonfiguriert haben.

Netzwerkgeräte beginnen damit, SeND zu implementieren, aber es gibt immer noch keine Unterstützung für SeND in Betriebssystemen, abgesehen von einigen wenigen akademischen Projekten.



SeND ist daher zur Zeit leider nicht verwendbar und kann nur innerhalb einer Organisation mit verwalteten Arbeitsplätzen, wie 802.1x, eingesetzt werden.

• MLD

IPv6 nutzt Multicast, während es in einem IPv4-Netz selten verwendet wird. Dort ist es oft auf Erkennungsprotokolle wie mDNS, SSDP, LLMNR oder sogar bei der Implementierung von OSPF beschränkt.

Infolgedessen ist Multicast innerhalb eines Netzsegments nicht immer gut implementiert. Wir sprechen hier nicht einmal von Multicast-Routing, sondern nur von einem Austausch auf demselben L2-Segment.

MLDv1 (RFC 2710) ist das Äquivalent zu IGMPv2 und verwendet drei Arten von Nachrichten:

- *Listener Queries*, entweder allgemein, um alle Knoten zu fragen, ob sie Mitglieder mindestens einer Multicast-Gruppe sind, oder spezifisch, um die Mitglieder einer Gruppe anhand einer bestimmten Adresse zu identifizieren;

- *Listener Reports*, um Hosts auf Anfragen antworten zu lassen;
- *Done* um mitzuteilen, dass sie nicht mehr Teil einer Gruppe sein müssen.

MLDv2 (RFC 3810) baut auf IGMPv3 auf und fügt Quellenfilterung (SSM) hinzu, so dass Quellen ein- oder ausgeschlossen werden können.

Die Hosts senden Berichte über Zustandsänderungen zusätzlich zu den periodischen Berichten, und der Nachrichtentyp "done" verschwindet (er wird von der Zustandsänderung übernommen).

Die Nachrichten werden erneut übertragen, um sie robust gegenüber Paketverlusten zu machen. Eine Robustheitsvariable gibt an, wie oft die Nachrichten erneut übertragen werden sollen. Der Standardwert ist zwei, es kann sinnvoll sein, diesen Wert z. B. bei WLAN zu erhöhen.

MLDv2 ist abwärtskompatibel mit MLDv1, wobei zu beachten ist, dass es auf ICMPv6 aufbaut, im Gegensatz zu IGMP, das direkt auf IPv4 aufsetzt.

MLD ermöglicht es, die Bedürfnisse der Clients zu kennen und sie insbesondere im Falle von geroutetem Multicast an den PIM-Agenten weiterzuleiten. Ohne einen anderen Mechanismus verhält sich der Multicast-Verkehr jedoch wie Broadcast-Verkehr innerhalb des Netzsegments. Er wird an alle Ports gesendet.

MLD-Snooping optimiert die Zustellung von Multicast-Verkehr, indem es ihn nur an Hosts, die ihn anfordern, und an Router, die den Dienst bereitstellen, sendet. L2-Geräte analysieren den Inhalt des MLD-Austauschs, um Tabellen zu erstellen, die Ports und Multicast-Adressen zuordnen. In MLDv1 basiert diese Zuordnung auf der Ziel-Multicast-Adresse, in MLDv2 wird sie um die Quelladresse(n) ergänzt, SSM ist dann erforderlich.

Daher ist es wichtig, dass die MLD-Querier-Funktion auf dem Router (mrouter) aktiv ist und dass die L2-Geräte die MLD-Berichte verwenden, um Snooping durchzuführen. Ohne "mrouter" wird der Status auf allen Switches repliziert, was unerwünscht ist.

Wenn bei MLD mehrere Router versuchen, eine Anfrage zu stellen, wird derjenige mit der kleinsten link-local IP zum Abfrager. Diese kleine Optimierung vermeidet die Probleme, die manchmal bei IPv4 mit IGMP auftreten, wo derjenige gewinnt, der die meisten Anfragen stellt.

Vernachlässigen Sie nicht die Optimierung durch Snooping und überprüfen Sie, ob es auf der gesamten Übertragungsstrecke ordnungsgemäß funktioniert. Nutzen Sie die Gelegenheit, um gleichzeitig IGMP auf IPv4 zu überprüfen.

In Rechenzentrumsumgebungen sollten Sie sich die Zeit nehmen, die Verteilung der zugrundeliegenden Multicast-Bäume in EVPN+VxLAN-Netzen zu berücksichtigen. Die Best Practise ist im Allgemeinen, Netzwerke auf mindestens zwei Underlay-Bäume zu verteilen und dedizierte Bäume für Netzwerke mit intensiven Multicast-Hosts (Cluster, Videosender usw.) zu erstellen. Diese Praxis kann auch für andere Overlay/Underlay-basierte Topologien gelten.

Zusammenfassend lässt sich sagen, dass MLDv2 zwar technisch nur bei Verwendung von SSM erforderlich ist, seine Fähigkeit, den Verlust von mindestens einem Paket zu tolerieren, jedoch einen Vorteil gegenüber V1 darstellt (siehe Robustheitswert). Snooping ist eine Optimierungsanforderung, die auch einen Angriff über unbekannte Multicast-Adressen oder ohne Client-Hosts vermeidet.

Wenn wir über IPv6 und Multicast sprechen, denken wir sofort an Well-Known-Multicast-Gruppen, wie "alle Router" (ff02::2) oder "alle DHCP-Server" (ff02::1:2). Wir vergessen jedoch Solicited-Node Multicast, mit dem wir uns bereits beschäftigt haben.

Zur Erinnerung: Jeder Host erstellt eine Multicast-Gruppenadresse, die auf den letzten 24 Bits jeder konfigurierten Adresse und dem Präfix F02:0:0:0:0:1:FF00::/104 basiert. Diese Adressen dürfen nicht von MLD-Snooping verarbeitet werden, da sie die Tabellen (mit mindestens einer Gruppe pro Host) schnell überlasten könnten. Diese Umgehung ist manchmal standardmäßig aktiviert, manchmal muss ein Befehl wie nd-workaround auf die MLD-Snooping-Konfiguration angewendet werden. Erkundigen Sie sich bei Ihrem Hersteller und werfen Sie einen Blick auf den Inhalt des MLD-Snooping-Inhalts, während die Hosts kommunizieren.



• STORM CONTROL

Klassischere und einfachere Sicherheit, Implementierung von Storm Control für Multicast und unknown Verkehr zumindest auf den Uplinks der Zugangsgeräte. Der dritte Punkt über Broadcast betrifft nur IPv4.

Seien Sie sich bewusst, dass es immer noch besser ist, einen hohen Wert wie 30 % des Links zu haben, als gar keine Konfiguration, während Sie beobachten, um sie nach der Untersuchung des Verkehrs zu verfeinern.

• ZU BLOCKIERENDE MULTICAST-GRUPPEN

Es gibt einige Multicast-Adressen, die direkt auf den Zugangsgeräten blockiert werden können. Sie finden diese im Abschnitt "Deaktivieren von automatischen Erkennungsprotokollen" im Host-Teil.

Host

Abgesehen von seltenen Ausnahmen (Firewall mit Profil) werden die Einstellungen, die Sie auf einen Host anwenden, unabhängig von dem Netz, mit dem er verbunden ist, wirksam. Leider ist es nicht möglich, Profile zu erstellen, z. B. SLAAC auf der Hostseite zu deaktivieren, wenn das in der RA empfangene Präfix das Firmenpräfix ist.

Seien Sie daher vor allem bei Rechnern vorsichtig, die eine Verbindung zu Netzwerken außerhalb Ihres Unternehmens herstellen können. Ein Benutzer mit einem Laptop zu Hause wird es beispielsweise schwer haben, etwas zu tun, wenn der Administrator SLAAC vollständig deaktiviert hat.

Andererseits können Sie Ihre Server so weit wie möglich härten.

• DHCP

DHCP DUID

Der DHCP Unique IDentifier ermöglicht es dem DHCP-Server, den Client zu identifizieren und seine Lease zu verfolgen. Es gibt mehrere Methoden, diesen Identifikator zu erstellen, wobei die einfachste die Hardware-Adresse (MAC) ist.

Diese DUID ist normalerweise innerhalb eines Systems unabhängig von der Netzwerkschnittstelle beständig. Ein Laptop mit einer DUID, die aus der MAC seiner kabelgebundenen Ethernet-Karte gebildet wird, verwendet beispielsweise denselben Wert, wenn er eine Anfrage über die WLAN-Karte stellt.

Die möglichen Varianten im ursprünglichen RFC 8415 sind:

- *Link-Layer-Adresse* (DUID-LL);
- *Link-Layer-Adresse plus Zeit* (DUID-LLT);
- *Anbieterbasierte Unternehmensnummer* (DUID-EN);
- *Universell eindeutiger Bezeichner* (DUID-UUID) RFC 6355.

Die erste ist explizit, die zweite fügt Zeitpunkt der ersten Erzeugung hinzu, sie wird gespeichert und ändert sich nicht, merken Sie sich das.

Die dritte ist nach Wahl des Herstellers.

Die vierte, UUID, versucht, die Persistenz für ein System zu garantieren, das aus dem Netz oder in mehreren Phasen gestartet wird. Der Start eines Servers in PXE mit einem leichten Bootstrapper, der dann zu einem echten Betriebssystem wechselt, ist ein interessanter Fall:

Sie hat mehrere Schnittstellen, so dass wir nicht garantieren können, dass die DUID-LL auf der gleichen Schnittstelle basiert. Der Hersteller unterscheidet sich zwischen der Firmware der PXE-Karte, dem Light-Bootstrapper und dem Betriebssystem.

Die UUID kann konsistent nachverfolgt werden, wenn die gesamte Kette auf denselben

Informationen beruht, z. B. der dem UEFI bekannten System-Seriennummer.

Die meisten Betriebssysteme verwenden standardmäßig DUID-LLT, es gibt keinen Grund, dies zu ändern.

DHCP-IAID

Während eine DUID für ein System eindeutig ist, ist die IAID für eine bestimmte Schnittstelle eindeutig. Hier gibt es keine besondere Konfiguration.

DHCP ohne RA

Wenn das *Router Advertisement* angibt, ob DHCPv6 verwendet werden soll oder nicht, was ist zu tun, wenn kein RA vorhanden ist?

RFC 4862 besagt, dass ein System in Ermangelung von RA DHCP durchführen kann. Dies ist in den meisten Betriebssystemen implementiert. Gut zu wissen ist auch, dass einige Betriebssysteme DHCPv6-Anfragen senden, auch wenn sie vom Router angewiesen werden, nur SLAAC zu verwenden.

Unterstützung von DHCP-Optionen im Dual-Stack

Was passiert, wenn ein Dual-Stack-Host sowohl in DHCPv4 als auch in DHCPv6 bestimmte Optionen empfängt, die sich inhaltlich unterscheiden, und zwar mit widersprüchlichem Inhalt?

Gilt der Vorrang, d. h. der erste, der die Option anbietet? Es könnte interessant sein, dies zu überprüfen.

• SLAAC-ADRESSGENERIERUNGSVERFAHREN

Ursprünglich war geplant, dass die SLAAC-Adresse aus der System-MAC-Adresse in Form von EUI-64 gebildet wird. Dies wirft jedoch viele Probleme auf:

- Da die MAC-Adresse eindeutig ist, kann ein Host im Internet verfolgt werden, unabhängig davon, von welchem Netz (Präfix) aus er sich verbindet;
- Es ist einfacher, einen Adressenscan in einem Netz durchzuführen, da die Verwendung von EUI-64 eine gewisse Vorhersagbarkeit dessen bietet, was häufig in den ersten Bits gefunden werden kann;
- Die Kenntnis der MAC-Adresse ermöglicht es, den Hersteller zu kennen, so dass es beispielsweise möglich ist, die Marke und das Modell des Geräts zu erraten, mit dem man spricht, indem man den Hersteller und das während des Austauschs verwendete Protokoll korreliert;
- Ein Wechsel der Netzwerkschnittstelle führt zu einer Änderung der SLAAC-Adresse.

Zwei RFCs schlagen Ansätze zur Begrenzung dieser Probleme vor, siehe:

- RFC 4941 *Privacy Extensions for Stateless Address Autoconfiguration in IPv6*;
- RFC 7217 *A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless*

Address Autoconfiguration (SLAAC).

Temporäre Adresse

Die temporäre Adresse ist ein Zusatz zur stable Adresse (RFC 4941). Sie ändert sich je nach den Einstellungen des Betriebssystems mehr oder weniger häufig, wobei die vom Router Advertisement SLAAC angekündigten Lebensdauern eingehalten werden.

Einige Systeme erstellen beispielsweise alle 25 Minuten eine neue Adresse und deaktivieren die vorherige Adresse 5 Minuten nach der Erstellung der neuen Adresse und wenn keine Sitzung mit der ältesten temporären IP-Adresse existiert. Neue vom Host initiierte Sitzungen verwenden daher nie länger als 30 Minuten eine Adresse.

Der Host bleibt jedoch jederzeit über seine stable Adresse erreichbar, und nur die stable Adresse unterliegt der DNS-Selbstregistrierung.

Die Verwendung temporärer Adressen kann aufgrund ihrer kurzen Lebensdauer Probleme verursachen.

Im RFC wird der Fall erwähnt, dass ein Server prüft, ob ein PTR-Reverse-DNS-Eintrag für den Client existiert, bevor er den Zugriff zulässt. Es lassen sich aber leicht weitaus häufigere Fälle finden:

Stellen Sie sich vor, Sie authentifizieren sich auf einer Website mit einer temporäre Adresse in der 24. Minute ihrer Gültigkeit, um Zugang zu einem Kundenbereich zu erhalten.

Zwei Minuten später fordert uns der Server erneut auf, uns zu authentifizieren, obwohl wir seit der Verbindung ununterbrochen gesurft haben.

Dieser Fall ist durchaus plausibel, denn wenn der Server aus Sicherheitsgründen vom Kunden verlangt, zusätzlich zu seinem Cookie dieselbe IP zu haben, wird er die Sitzung ablehnen. Ähnlich verhält es sich, wenn ein Front-End-L4-Load-Balancer damit beginnt, den Client an einen anderen Server umzuleiten, der nichts von der Web-Sitzung des Clients weiß, weil er glaubt, es handele sich um einen neuen Client aufgrund einer neuen IP. Derzeit gibt es keinen Mechanismus, der es Browsern erlaubt, einem Server, für den eine Browser-Registerkarte aktiv ist (oder kürzlich aktiv war), die IP-Änderungsinformationen mitzuteilen.

Auch bei einem P2P-Online-Spiel mit selbst gehostetem Matchmaking könnten die Spiele nach wenigen Minuten unterbrochen werden.

Bei einem Spiel wäre es wünschenswert, dass der Entwickler die Sitzungen über die stable Adresse aufbaut, aber bei einem Browser würde dies den Wert der temporären Adresse völlig zunichte machen, da der Webverkehr den Großteil der Verfolgungsmöglichkeiten ausmacht.

Wenn wir einen Schritt zurückgehen, können wir sagen, dass die Nachverfolgung (z. B. Werbung) sich mit der Identifizierung des /64-Präfix begnügen wird, der ausreicht, um einen Haushalt auf die gleiche Weise zu identifizieren wie eine heutige IPv4-Adresse. Es ist jedoch nicht ausgeschlossen, dass Werbetreibende anfangen werden, IPv6-Adressen über eine Woche hinweg zwischenzuspeichern, um diejenigen als stable zu kennzeichnen, die mehrmals gesehen wurden, und somit zwangsläufig eine EUI-64- oder stable privacy Adresse verwenden. Dies gibt ihnen schließlich die Möglichkeit, den einzelnen Nutzer statt des Haushalts zu verfolgen, und zwar ohne

Cookies! Darüber sollte man nachdenken...

Erst kürzlich, im Februar 2021, wurden in RFC 8981 Änderungen an temporären Adressen vorgenommen.

In der Liste der Änderungen finden wir die Möglichkeit, nur temporäre Adressen zu haben ohne stable. Der RFC schreibt immer noch keinen Mechanismus vor, um Präfixe von der Verwendung temporärer Adressen auszuschließen, aber er empfiehlt es. Microsofts Antwort ändert sich vielleicht nicht <https://social.technet.microsoft.com/Forums/azure/en-US/e36e82e9-1911-4f4d-91a2-c62f6e04c9c1/ipv6-turn-off-privacy-extensions-temporary-addresses-for-certain-prefixes-ie-ula-in-win-10?forum=win10itpronetworking>

Zufallsgenerierte Interface-ID

Anstatt seine MAC in EUI-64 zu verwenden, generiert der Host seine Adresse auf der Grundlage eines Pseudozufallsbezeichners. Dieser Bezeichner ändert sich beim Neustart. Systeme, die die Speicherpersistenz unterstützen, können ihre Adresse zusätzlich zur Pseudo-Zufallszahl auf die vorherige Adresse stützen.

Stable Privacy Address

Dieser Mechanismus ermöglicht es Ihnen, immer dieselbe IPv6-Adresse zu erhalten, solange Sie sich im selben Netz/Präfix befinden und sie bei der Verbindung zu anderen Netzen zu ändern. Dies wird dadurch erreicht, dass die Adresse neben dem empfangenen Präfix auch von internen Konstanten des Gerätes abgeleitet wird.

Insbesondere die folgenden:

- Über RA empfangenes Präfix;
- Schnittstellennummer (wie vom Betriebssystem gesehen);
- DAD-Zähler (0, wird bei Konflikten erhöht);
- Geheimschlüssel, der beim ersten Mal zufällig generiert und gespeichert wird;
- Optional die Netzwerkkennung, in der Regel die Wifi SSID.

So ist es unmöglich, die Maschine zu verfolgen, wenn sie sich in verschiedenen Netzen bewegt und auch unmöglich, die MAC aus der Adresse zu ermitteln. Andererseits wird der stabile Aspekt innerhalb jedes frequentierten Netzes die Arbeit des Administrators erleichtern, der DHCPv6 stateful vermeiden möchte.

SLAAC-Synthese

Hier finden Sie eine Übersicht über die Verfolgbarkeit nach Adressentyp. Vergessen Sie nicht, dass die globale Adresse routingfähig ist und daher potenziell überall im Internet sichtbar ist.

SLAAC-Modus	Lokales Tracking	Globales Tracking	Informationen über das Gerät	Tracking aus demselben Netzwerk über die Zeit
EUI-64 (MAC)	YES	YES	YES (Hersteller)	YES
Randomisiert (Änderung bei Neustart)	NO	NO	NO	Über mehrere Stunden/Tag je nach Standby VS-Neustart
Stable Privacy (abgeleitet von Präfix)	YES	NO	NO	YES
NO (für host-initiierte Sitzung)	NO (für host-initiierte Sitzung)	NO (für host-initiierte Sitzung)	Normalerweise weniger als ein Tag (für host-initiierte Sitzung)	

Idealerweise sollten Sie das Standardverhalten des Betriebssystems für Rechner beibehalten, die möglicherweise eine Verbindung nach außen herstellen. Dieses Verhalten variiert im Allgemeinen zwischen Randomized oder Stable Privacy, mit oder ohne temporäre Adresse.

Bei anderen Rechnern ist es möglich, SLAAC vollständig zu deaktivieren, da die Verwendung von DHCPv6 stateful und/oder die manuelle Konfiguration (z. B. von Servern) diesen Mechanismus nutzlos macht. Wir folgen dann der Logik der Verringerung der Angriffsfläche für das Protokoll und schließen die Tür.

Verfahren zur Generierung von Link-Local-Adressen

Obwohl sie nur lokal gilt, profitiert die lokale Verbindungsadresse ebenfalls von den drei oben erwähnten automatischen Konfigurationsmodi.

Die Konfiguration folgt im Allgemeinen der globalen Adresse auf Consumer-Betriebssystemen, wenige Systeme bieten eine spezifische Konfigurationsgranularität nach Adressklassen.

Die Server- und netzorientierten Systeme basieren jedoch im Allgemeinen auf EUI-64.

• IPv6-STACK NICHT DEAKTIVIEREN

Wenn Sie aus irgendeinem Grund verhindern wollen, dass ein Host in IPv6 kommuniziert, deaktivieren Sie seinen IPv6-Stack nicht. Verwenden Sie stattdessen die folgenden Optionen:

- Ändern Sie die Rangfolge, um IPv4 Vorrang zu geben;
- Deaktivieren Sie SLAAC auf dem Host und sperren Sie ihn ggf. für DHCPv6;
- Stellen Sie die OS-Firewall so ein, dass jeglicher IPv6-Verkehr untersagt wird.

Wenn Sie den IPv6-Stack deaktivieren, kann es bei einigen Programmen zu Anomalien kommen.

Windows verlangt beispielsweise seit mehreren Jahren, IPv6 nicht zu deaktivieren, da sonst einige der häufig verwendeten Komponenten nicht mehr ausgeführt werden können. Unter Linux kann das einfache Fehlen des Loopbacks ::1 ebenfalls zu Überraschungen führen. Neuere Kernel lassen die Verwendung des ::1 Loopbacks auch bei deaktiviertem Stack zu.

• DEAKTIVIERUNG VON ÜBERGANGSMECHANISMEN

Einige Mechanismen ermöglichen es Hosts, IPv6 über IPv4-Netze auszutauschen:

- TEREDO;
- ISATAP;
- 6to4.

Diese Mechanismen sind nicht mehr von Interesse und die ersten beiden sind sogar verschwunden. Es ist daher ratsam, sie zu deaktivieren.

• DEAKTIVIERUNG VON AUTOMATISCHEN ERKENNUNGSprotokollen

Es ist ratsam, in das Betriebssystem eingebettete automatische Erkennungsprotokolle zu deaktivieren. Wenn sie bei Heimanwendern nützlich sind, stellen sie in einem Unternehmen ein echtes Risiko dar.

Dazu gehören:

- SSDP (Multi OS, ff02::c - UDP 1900) und folgende Adressen FF0X::C, je nach Bereich:
- Node-local : FF01::C (kommt nicht mal raus...)
 - Link-local : FF02::C ;
 - Site-local : FF05::C (veraltet);
 - Organisation-local : FF08::C (veraltet);
 - Global : FF0E::C.
- mDNS (mehrere Betriebssysteme, ff02:fb - UDP 5053)
- LLMNR (Windows, ff02::1:3 - UDP und TCP 5355)

Abgesehen von den Angriffen, die mit diesen Protokollen verbunden sind, unterscheidet sich ihr Betrieb mit IPv6 in einem ganz bestimmten Punkt.

Bei IPv4 hat ein Rechner nur eine IP. Wenn zwei Rechner miteinander zu kommunizieren beginnen, nachdem sie ihren Namen über eines dieser Protokolle aufgelöst haben, wird die Zuordnung von IP und Rechner in der Regel über DHCP-Protokolle aufrechterhalten.

In IPv6 erlauben diese Protokolle den Rechnern, sich gegenseitig über ihre link-local-Adresse aufzulösen. (FE80::/10). Finden Sie also in einem Protokoll heraus, welcher Rechner eine FE80 war...

Dieses Verhalten tritt in der Produktion in Unternehmen auf, die noch nicht einmal IPv6 eingeführt

haben. Es genügt zum Beispiel ein SMTP-Relay zwischen zwei Microsoft Exchange-Servern, die sich im selben Netzwerksegment befinden. Wenn die oben genannten Protokolle nicht deaktiviert sind, sehen Sie in den E-Mail-Kopfzeilen eine Zustellung über FE80. Glücklicherweise gibt SMTP immer noch den Hostnamen an.

• BLOCKIERUNG DES LINK-LOKALEN VERKEHRS

Zu Hause kann die lokale Link-Adresse verwendet werden, um mit Ihrem NAS, Drucker, Chromecast/Airplay-Empfänger usw. zu kommunizieren, nachdem sie über die oben genannten Protokolle erkannt wurde. Die DNS-Autoregistrierung auf dem heimischen Router bevorzugt die globale Adresse.

In einem Unternehmen hat ein Host jedoch keinen Grund, etwas anderes als ICMP (und darauf basierende Protokolle wie MLD) über seine lokale Link-Adresse zu verwenden. Es wird daher empfohlen, den gesamten TCP- und UDP-Verkehr in beiden Richtungen innerhalb der OS-Firewall zu blockieren. Aber lassen Sie, wie gesagt, ICMP zu.



Bei geclusterten Servern ist es durchaus möglich, dass eine Softwarelösung, bei der sich die Rechner im gleichen Netzsegment befinden müssen, die Local-Link-Adressen für den Datenaustausch oder einfach für den Heartbeat verwendet.

Machen Sie eine Ausnahme für DHCP und EAPOL 802.1x auf Systemen, die diese verwenden.

Für mobile Geräte ist es auch interessant, NAT-PMP (RFC 6886) und seinen Nachfolger PCP V2 (RFC 6887) zu öffnen, um den Betrieb von Anwendungen zu ermöglichen, die unaufgeforderten Verkehr empfangen müssen. Typischerweise sind das Konferenzsysteme. Diese beiden Protokolle ermöglichen es, das Gateway aufzufordern, einen Port zu öffnen, was der automatischen Weiterleitung des NAT44-Ports in IPv4 über UPnP-IGD entspricht.

NAT-PMP verwendete ursprünglich auf beiden Seiten den Port 5351, was jedoch bei Rechnern, die sowohl als Client als auch als Server fungierten, zu Problemen führte, z. B. bei der erneuten gemeinsamen Nutzung einer Verbindung. Daher wurden die Clients auf Port 5350 umgestellt. PCP verwendet ebenfalls 5350 auf der Client-Seite und 5351 auf der Server-Seite.

Wir behalten also UDP 5350 und 5351 im Listening und 5351 im Zielbereich.

Wenn Sie weniger Einschränkungen wünschen, können Sie auch nur den Verkehr in der eingehenden Richtung blockieren.

• VPN

Die Einführung von IPv6 in Heimnetzwerken kann ein Risiko für falsch konfigurierte VPN-Sitzungen darstellen. Ein Unternehmen, das kein Split-Tunneling praktiziert und die Route 0.0.0.0/0 bekannt gibt, wenn das System AAAA-DNS-Ressourcen auflösen kann und die Firewall ihn nicht blockiert, kann er über IPv6 mit dem Internet kommunizieren.

Die Auflösung ist möglich, wenn der DNS-Server des Unternehmens auf AAAA-Anfragen antwortet,

auch über IPv4-Verbindungen, oder wenn der Stack des Hosts die Auflösung über IPv6-DNS erlaubt, das dem Host lokal im VPN zur Verfügung gestellt wird.

Wenn Sie Split-Tunneling verwenden, stellen Sie sicher, dass die IPv4- und IPv6-Regeln übereinstimmen.

Auf vielen Websites können Sie einen IPv6-VPN-Leak-Test durchführen.

Beachten Sie, dass "Consumer"-VPNs selten IPv6 unterstützen, aber dennoch eine Standard-IPv6-Route bekanntgeben, um Datenverkehr an ein Blackhole zu senden um ein Datenleck zu vermeiden. Sie können dasselbe tun und ::/0 in Ihrem VPN ankündigen, auch wenn Sie keine echte Konnektivität bieten.

• DESKTOP OS KONFIGURATION

Dieser Abschnitt enthält einige Konfigurationsbeispiele.

Windows

Unter Windows, auch wenn es noch *netsh*-Befehle gibt, wird jetzt empfohlen, *powershell cmdlets* zu verwenden.

Der größte Teil der Konfiguration ist hier zu finden:

<https://docs.microsoft.com/en-us/powershell/module/nettcpip/set-netipv6protocol?>

Einige der Konfigurationen können direkt in der Registry vorgenommen werden, z. B. die DHCP-DUID-Generierungsmethode über den Schlüssel HKLM\SYSTEM\CurrentControlSet\services\TCPIP6\Parameters\Dhcpv6DUID

0001 - DUID-TTL

0002 - DUID-EN

0003 - DUID-LL

Die persistente DUID wird unter demselben Schlüssel angezeigt.

Linux

Hier sind einige Konfigurationen für GNU/Linux.

Einige werden immer auf der Kernel-Ebene angewendet, entweder direkt oder mit Hilfe eines Drittanbieter-Tools.

Der Rest hängt von den Paketen ab, die für die entsprechenden Funktionen zuständig sind. Da das GNU-Ökosystem per Definition reichhaltig und offen ist, gibt es viele Möglichkeiten, Dinge zu tun, sogar innerhalb der gleichen Distribution. Die offizielle Dokumentation der Distributionen ist nicht immer einheitlich.

Konfigurationen können über vorgenommen werden:

- Befehle;
- Konfigurationsdateien;
- Pseudographisches Werkzeug wie nmtui (für Network Manager).

Nachfolgend finden Sie Links zur Kernel-Dokumentation:

<https://www.kernel.org/doc/Documentation/networking/ipv6.txt>

<https://www.kernel.org/doc/Documentation/networking/ip-sysctl.txt>

<https://github.com/torvalds/linux/blob/master/net/ipv6/Kconfig>

Ein besser lesbare Zusammenfassung <https://sysctl-explorer.net/net/ipv6/>

Network-Manager

Network Manager ist ein relativ weit verbreitetes Tool des Gnome-Projekts, das zur Verwaltung von Netzwerken verwendet wird.

<https://wiki.gnome.org/Projects/NetworkManager>

<https://developer.gnome.org/NetworkManager/stable/settings-ipv6.html>

<https://developer.gnome.org/NetworkManager/stable/nm-settings-ifcfg-rh.html>

<https://developer.gnome.org/NetworkManager/stable/nm-settings-keyfile.html>

CLI nmcli <https://developer.gnome.org/NetworkManager/stable/nmcli.html>

Pseudographische nmtui <https://developer.gnome.org/NetworkManager/stable/nmtui.html>

Systemd Netzwerk

systemd-networkd (Netzwerk) und systemd-resolved (DNS) sind omnipräsent, aber nicht unbedingt aktiviert. Achten Sie darauf, die globale Verwaltung (oder die Verwaltung bestimmter Schnittstellen) durch einen anderen Daemon wie Network-Manager zu deaktivieren, um Konflikte mit Networkd zu vermeiden. Auch das Gegenteil ist der Fall.

<https://systemd.io/>

<https://www.freedesktop.org/software/systemd/man/resolvconf.html#>

<https://www.freedesktop.org/software/systemd/man/systemd-networkd.service.html#>

<https://www.freedesktop.org/software/systemd/man/systemd.network.html#> (das Wichtigste)

netplan

Netplan ist kein direkter Verwaltungsdämon, sondern ein Abstraktionswerkzeug, das bei Canonical (Ubuntu) vorhanden ist. Es konfiguriert dann den Network Manager oder Networkd.

<https://netplan.io>

<https://netplan.io/reference/>

Allerdings scheint Netplan keine DHCP-PD-Unterstützung zu bieten, was für einige Anwendungen ein großer Nachteil ist (z. B. wenn man Hypervisor-Pods /64 zur Verfügung stellen möchte). In der Zwischenzeit können Sie es mit einem systemd Override auf diesem Element verwenden.

<https://bugs.launchpad.net/netplan/+bug/1771886>

wickedd

wickedd bietet einen Dienst zur Verwaltung von Netzwerkschnittstellen. Er überwacht die Schnittstellen des Systems, indem er relevante Informationen vom Kernel über netlink, sysfs und andere Schnittstellen abruft.

Auf ihn kann über einen DBus-Dienst zugegriffen werden, der dazu verwendet werden kann, Schnittstellen neu zu konfigurieren, sie hoch- oder herunterzufahren.

Komponenten

Zusätzlich zum Haupt-Daemon wickedd stellt das wicked-Framework mehrere Hilfs-Daemons und Supplicants zur Verfügung:

Komponente	Beschreibung
wickedd-nanny	Ereignisgesteuerter Policy-Daemon, der für Hotplugging zuständig ist.
wickedd-dhcp6	DHCPv6 Client-Antragsteller
wickedd-dhcp4	DHCPv4-Client-Antragsteller
wickedd-auto4	IPv4 autoip-Antragsteller

Außerdem kommuniziert er auch mit dem externen wpa-suplicant für die Unterstützung von Wireless (WPA). wickedd wird von der Suse-Distribution verwendet.

<https://manpages.opensuse.org/Tumbleweed/wicked/wickedd.8.en.html>

Linux-Distributionen

In der Dokumentation jeder Distribution finden Sie Hinweise darauf, welches Tool standardmäßig installiert ist. In den meisten Fällen liegt die Wahl zwischen systemd-networkd und Network-Manager. Conman und WICD zum Beispiel sind aus der Landschaft verschwunden.

Wie so oft, ist die ArchLinux-Dokumentation sehr vollständig. Hier ist ein Link zu den Konfigurationselementen für jeden Typ von Netzwerkmanager https://wiki.archlinux.org/title/Network_configuration#Network_managers

Siehe auch IPv6 Abschnitt <https://wiki.archlinux.org/title/IPv6>

Ubuntu netplan man <http://manpages.ubuntu.com/manpages/jammy/man5/netplan.5.html>

Hier gibt es viele Elemente <http://mirrors.deepspace6.net/Linux+IPv6-HOWTO/>

und <http://www.bieringer.de/linux/IPv6/>.

• MOBIL UND EMBEDDED

Mobile Betriebssysteme können in einem Unternehmensnetz in verschiedenen Formen anzutreffen sein:

- IoT Hardware (Drucker, Raumbuchung)
- Unternehmens Smartphones
- persönliche Smartphones (BYOD)
- Nicht verwaltete Geräte in einem Gastnetzwerk

Android

Android ist jetzt der führende Akteur in diesen Segmenten, und es hat ein ärgerliches Problem: Es unterstützt DHCPv6 nicht.

Überraschend? Diese Wahl scheint Teil einer Vertrauensstrategie zu sein, um die Implementierung von SLAAC durchzusetzen. Die Gründe werden in RFC 7934 genannt: DHCP bietet nur eine Adresse und erlaubt keine temporären Adressen, was die Rückverfolgung erleichtert. Nur eine Adresse zu haben, verhindert auch das Angebot von Tethering/gemeinsamen Verbindungen im WLAN.

Der Bedarf an DHCPv6 ist jedoch vorhanden, die genannten Einschränkungen sind in einem Unternehmensnetz mit Wifi nicht anwendbar. Das Problem der gemeinsamen Nutzung von Verbindungen ist nur hinter einer 3GPP-Mobilfunkverbindung relevant.

Aber wer hat dann diesen RFC geschrieben? Ingenieure von Google und Apple, angefangen mit Lorenzo Colitti.

Das Problem ist seit vielen Jahren bekannt:

<https://www.techrepublic.com/article/androids-lack-of-dhcpv6-support-frustrates-enterprise-network-admins/>

https://www.reddit.com/r/ipv6/comments/3wfpn2/i_am_getting_sick_of_lorenzos_attitude_to_ipv6/

<https://www.nullzero.co.uk/android-does-not-support-dhcpv6-and-google-wont-fix-that/>

<https://issuetracker.google.com/issues/36949094>

<https://issuetracker.google.com/issues/36949085?pli=1>

Was ist zu tun? Selbstverständlich sollten Sie in Ihren Ausschreibungen für Geräte nach DHCPv6-Unterstützung fragen. Ganz gleich, ob es sich um eine Unternehmens-Smartphones oder embedded Geräten handelt.

Android wird von den Herstellern weit über das Open-Source-OS-Projekt (AOSP) hinaus

angereichert, die OEMs integrieren manchmal einen DHCPv6-Client. Dies ist typischerweise bei Android-Druckern/Kopierern der Fall, aber selten bei Telefonen.

Wie lassen sich Android-basierte BYOD-Geräte verfolgen, wenn sie DHCPv6 nicht unterstützen? MDM (Mobile Device Management) Tracking-Tools könnten die Antwort liefern, indem sie alle verwendeten Adressen verfolgen, solange sie Teil einer konfigurierten Präfixliste sind. Zum Beispiel ein /32, das dem Unternehmen von einem RIR zugewiesen wurde. Auf diese Weise wird das Endgerät nur im beruflichen Netz verfolgt, ohne DHCPv6 zu verwenden.

Dasselbe ist für iOS möglich, obwohl es für sie einfacher ist, sich mit einer SSID ohne SLAAC und nur mit DHCPv6 zu verbinden. Ganz zu schweigen davon, dass über MDM die Verwendung der echten MAC für diese SSID und nicht einer zufälligen MAC erzwungen wird. Mobile Betriebssysteme verwenden in letzter Zeit zufällige physische Adressen nicht nur bei der Suche nach SSIDs, sondern auch nach der Verbindung.

Was Gastnetzwerke betrifft, so ist es schwierig, einem Gerät, das SLAAC verwendet und seine temporäre Adresse mehrmals ändert, ein funktionierendes Captive Portal zur Verfügung zu stellen.

Ein zentralisiertes Captive Portal würde mit DHCPv6 funktionieren, was für Android schade ist. Die Implementierung eines NDPmon-Kollektors könnte es ermöglichen, einem Terminal in SLAAC zu folgen, aber diese Lösungen sind im Moment selten.

Es ist daher heikel, aber nicht unmöglich, IPv6-SLAAC-Konnektivität für Gastnetzwerke in Hotels, Krankenhäusern, Flughäfen oder einfach innerhalb einer Organisation bereitzustellen.

Andere Betriebssysteme

iOS unterstützt beide Methoden der Adresszuweisung und stellt im Betrieb kein besonderes Problem dar.

Für andere embedded Geräte ist es gut, DHCPv6-Unterstützung zu verlangen, aber auch die Möglichkeit zu haben, bei der Verwendung von SLAAC den Mechanismus der automatischen Adresszuweisung zu wählen. In der Regel verwenden viele Mikrocontroller-Geräte heute nur EUI-64-SLAAC. Dies hat den Nachteil, dass ein Angreifer die Marke über die MAC-Adresse identifizieren kann, da letztere in IPv6 enthalten ist. Denken Sie also darüber nach, nach einer stable IPv6-Unterstützung für Privacy zu fragen.

Transit

• URPF

Unicast Reverse Path Forwarding (RFC 3704) verhindert, dass ein Paket, dessen Quelladresse nicht mit einer bekannten Route in umgekehrter Richtung übereinstimmt, einen Router durchläuft, und begrenzt so das Risiko von IP-Spoofing.

Es gibt mehrere Modi, je nachdem, ob wir uns auf die Übereinstimmung zwischen der Quellschnittstelle und der besten entsprechenden Route konzentrieren (strict), auf jede Route, die die Adresse umfasst (Feasible) oder ob wir einfach wissen wollen, ob der Router unabhängig von der Schnittstelle mindestens eine passende Route hat (loose).

RFC 8704 bringt Verbesserungen auf der Grundlage von BGP-Informationen für den "feasible mode".

Die Implementierung muss am Rand des Netzes erfolgen, wo keine Gefahr der Asymmetrie besteht. In der Regel sind dies Campus-Cores oder Internetrouter. Die Konfiguration von uRPF ist im Allgemeinen sowohl für IPv4 als auch für IPv6 gleich.

Wenn Sie Multicast-Verkehr routen, sollten Sie auch Multicast-RPF berücksichtigen.

• SCHUTZ DER CONTROL PLANE

Pakete, die für den Router selbst bestimmt sind, sowie Pakete mit bestimmten Header-Optionen, die eine Ausnahme verursachen, müssen an die Kontrollebene weitergeleitet werden.

RFC 6192 befasst sich mit dieser Problematik. Die Verwendung der QoS-Engine zur Begrenzung der Rate des betreffenden Verkehrs auf einige Mb/s ermöglicht es, den Router vor einem Denial-of-Service-Versuch zu schützen. Natürlich muss sofort untersucht werden, ob der Grenzwert erreicht wurde oder kurz davor steht. Diese Sicherheit unterscheidet nicht zwischen legitimem und illegitimem Verkehr.

Außerdem hat der explizit für den Router selbst bestimmte Verkehr keinen Grund, fragmentiert zu werden, Sie können ihn blockieren, wenn er fragmentiert ist.

• OSPF SICHERHEIT

Die Einführung von OSPFv3 ist eine Gelegenheit, MD5 fallen zu lassen und IPsec zur Sicherung des Austauschs zu verwenden. ESP muss unterstützt werden, AH optional (RFC 4552). Alles im Transportmodus.

Hinweis zu anderen Protokollen:

RIPng bietet das Gleiche.

BGP ist nicht spezifisch für v6 und folgt einem anderen Weg durch die BGPsec-Initiative, die darauf abzielt, die Signatur des Routenursprungs und die Pfadvalidierung (AS-Path) von Ende zu Ende

zusammenzufassen. Diese Initiative konzentriert sich auf das öffentliche Routing und scheint derzeit keine Verschlüsselungs- und Authentifizierungskomponente für Unternehmensnetze zu enthalten, die auf einer privaten PKI oder einer manuellen Implementierung der Schlüssel basiert.

IS-IS sieht keine Entwicklung auf der Sicherheitsseite, außerdem ist es IP-agnostisch.

Filterung

Einige Regeln können in Routern und nicht nur in Firewalls integriert werden, obwohl der zustandsbehaftete Aspekt für einige von ihnen weiterhin erforderlich ist.

• ICMP

Während es einen starken Trend zur Beschränkung des zulässigen ICMPv4-Verkehrs gibt, erfordert ICMPv6 einen detaillierteren Ansatz.

RFC 4890 "Border Firewall Transit Policy" erinnert uns daran und schlägt ACLs zur Implementierung vor. Sie finden sie hier:

Erforderlich Zulassen: * Destination Unreachable (Type 1) - Alle Codes; * Packet Too Big (Type 2) – erforderlich für PMTU-Ermittlung; * Time Exceeded (Type 3) - nur Code 0; * Parameter Problem (Type 4) - nur Codes 1 und 2.

Fakultativ:

- Time Exceeded (Type 3) - Code 1;
- Parameter Problem (Type 4) - Code 0;

Zur Kontrolle der Echo-Anfrage und -Antwort (in der Regel für das Internet gesperrt):

- Echo Request (Type 128);
- Echo Response (Type 129).

Außer bei der Verwendung von IPv6-Mobilität ist es ratsam, diese zu blockieren:

- Home Agent Address Discovery Request (Type 144);
- Home Agent Address Discovery Reply (Type 145);
- Mobile Prefix Solicitation (Type 146);
- Mobile Prefix Advertisement (Type 147).

ICMPv6-Fehler- und Informationscodes, die nicht von der IANA zugewiesen wurden, sollten bei externer Filterung (Internet, Partner usw.) gesperrt werden. Ihre interne Sperrung liegt im Ermessen der Administratoren.

Fehlercode: Typen 5 bis 99 und 102 bis 126 sowie 150 (Seamoby).

Informativer Code: Typen 154-199 und 202-254.

ICMPv6 sah Mechanismen vor, die in der Praxis nicht verwendet werden und daher zu blockieren sind:

- Node information :
 - Node Information Query (Type 139);

- Node Information Response (Type 140).
- Router Renumbering (Type 138) This message enables you to change the prefix of all configured interfaces of the router that receives it. Not likely to be used. Not to be confused with DHCPv6 and Prefix Delegation renumbering.
- Experimental codes (Types 100 – 101 and 200 – 201);
- Other unused types (Types 127 and 255).

Im L3-Modus (Router) sollte die Firewall den Transit (über das Gateway hinaus) von Nachrichten blockieren, die nur innerhalb des Bereichs der link-local-Adresse existieren:

- All NDP inkl. reverse.
 - Router Solicitation (Type 133);
 - Router Advertisement (Type 134);
 - Neighbor Solicitation (Type 135);
 - Neighbor Advertisement (Type 136);
 - Redirect (Type 137);
 - Inverse Neighbor Discovery Solicitation (Type 141);
 - Inverse Neighbor Discovery Advertisement (Type 142).
- Multicast NDP tied to routers:
 - Multicast Router Advertisement (Type 151);
 - Multicast Router Solicitation (Type 152);
 - Multicast Router Termination (Type 153).
- Messages related to the unusable SeND protocol:
 - Certificate Path Solicitation (Type 148);
 - Certificate Path Advertisement (Type 149).
- MLDv1 and v2 messages (must arrive via link-local and have a hop-limit of 1):
 - Listener Query (Type 130);
 - Listener Report (Type 131);
 - Listener Done (Type 132);
 - Listener Report v2 (Type 143).

Arbeitet er hingegen als Bridge (L2), muss er die oben genannten Nachrichten zulassen, mit Ausnahme von SeND (solange es nicht verwendet wird).

Sollte erlaubt werden, obwohl es noch fakultativ ist:

- Time Exceeded (Type 3) - Code 1;
- Parameter Problem (Type 4) - Code 0.

Selbst in L2 wird empfohlen, Redirect (Typ 137) aus Sicherheitsgründen zu blockieren. Es sei denn,

er wird tatsächlich verwendet, z. B. wenn ein Segment zwei Router (einen eingehenden und einen ausgehenden) und einen Host hat, dessen Routing-Tabelle nicht angepasst ist.

Schließlich muss DPI die Nutzdaten analysieren, um zu erkennen, ob ICMPv6 missgebildet ist oder zum Austausch von Nachrichten verwendet wird, indem eine Art Tunnel geschaffen wird. Dies sollte zumindest am Internetübergang geschehen.

DPI wird auch in der Lage sein, eine PMTU-D-Rückgabe mit einem Wert unter 1280 zu blockieren. Dies ist unmöglich und würde einen schlecht entwickelten IPv6-Stack zum Absturz bringen.

• TRANSITION MECHANISMEN

Wenn das Deaktivieren von Transition Mechanismen auf Hosts eine gute Praxis ist, ist das Blockieren dieser Mechanismen auf Filtergeräten ebenso nützlich.

Diese Regeln sind sowohl auf ein IPv4- als auch auf ein IPv6-Netz anzuwenden, abhängig von der Richtung der Verkapselung. Siehe RFC 7123.

Es ist daher notwendig, die :

- IPv4-Protokoll #41 (6in4, 6to4, 6over4, 6rd, ISATAP);
- IPv4-Protokoll Nr. 47 (GRE), außer wenn verwendet;
- Teredo:
 - UDPv4-Zielport 3544;
 - Wenn DPI läuft, filtere UDPv6-Pakete mit Teredo-Adresse (die zum Präfix 2001::/32 gehört) in der Payload;
 - DNS-Anfragen an teredo.ipv6.microsoft.com. (über DPI und/oder direkt auf DNS-Servern).
- ISATAP:
 - Filterung von DNS-Anfragen vom Typ A für isatap.* (über DPI und/oder direkt auf DNS-Servern).
- 6to4:
 - IPv4-Protokoll 41, das an 192.88.99.0/24 geht oder von dort kommt;
 - Enger mit DPI, IPv4-Protokollpaket #41 mit 6to4-Adresse (zum Präfix 2002::/16 gehörend) in der Payload.
- 6over4:
 - Pakete mit Protokoll #41 und Ziel 239.0.0.0/8 (Block 6over4 NDP).
- Tunnel Broker / TSP (Tunnel Setup Protocol):
 - TCPv4 und UDPv4 mit Zielport 3653;
 - Möglichkeit der Vorauswahl mit IP proto #41.
- AYIYA:
 - TCPv4 und UDPv4 mit Zielport 5072.

Verwenden Sie DPI, wenn möglich intelligent, filtern Sie zuerst nach der Protokollnummer, bevor Sie sie an das Analyseprogramm senden, um Ressourcen zu sparen.

Wird eine dieser Regeln von einem Rechner innerhalb des Netzes ausgelöst, sollte eine Untersuchung durchgeführt werden, um die Ursache für die Fehlkonfiguration zu ermitteln. Dies gilt insbesondere für Host-gesteuerte Mechanismen wie Teredo und ISATAP.

Bei IPv6 können Sie 4rd, 4over6, usw. blockieren.

• BOGON PRÄFIXE UND ROUTEN

Bei IPv4 ist es abnormal, einige Adressen zu sehen, z. B. ein Paket mit einer Quelladresse von 127.0.0.5 oder eine IP RFC1918, die aus dem Internet kommt... Das Gleiche gilt für IPv6.

Idealerweise sollten Sie die betreffenden Pakete auf den Front-End-Firewalls des Internets blockieren, aber auch jede BGP-Ankündigung mit diesen Präfixen aus dem Internet oder einem Partner filtern (außer in besonderen Fällen)

- Größte nicht zugewiesene Blöcke :
 - 2d00::/8
 - 2e00::/7
 - 3000::/4
 - 4000::/2
 - 8000::/1
- 2001::/23 IETF reserviert;
- 0::/96 Ehemaliges IPv4-Kompatibilitätspräfix;
- ::ffff:0:0/96 Mapped IPv4 address;
- 64:ff9b::/96 NAT64 Well known prefix;
- 64:ff9b:1::/48 Block für lokale NAT64-Plattformen;
- 100::/64 RTBH (Remote triggered black hole filtering);
- 2001:2::/48 Benchmarking;
- 2001:0DB8::/32 Dokumentation;
- 5f00::/8 6bone, entfallen;
- 2002::/16 6to4;
- 3ffe::/16 früher TEREDO;
- 2001::/32 TEREDO;
- 2001:10::/28 ORCHID Overlay Routable Cryptographic Hash Identifiers RFC 4843;
- 2001:20::/28 ORCHID v2 RFC 7343;
- 2001:3::/32 AMT, wird verwendet, um einem Multicast durch einen Tunnel beizutreten RFC 7450;

- 2001:1::1/128 PCP, ermöglicht einen Port dynamisch in der Firewall zu öffnen;
- ff00::/8 Multicast;
- fe00::/9 früher Multicast;
- fc00::/7 Unique Local Address (ULA);
- fec0::/10 früher Site Local, veraltet;
- fe80::/10 Link-local (außer für L2-Bridge-Firewall);
- ::1/128 Loopback (nicht auf einer Host-OS-Firewall blockieren);
- ::/128 (0) unspecified address;
- ::/8 Viele reservierte Adressen, darunter die letzten zwei;

Neben den RFCs sollten Sie auch die IANA-Ressourcen nicht vergessen:

<https://www.iana.org/assignments/iana-ipv6-special-registry/iana-ipv6-special-registry.xhtml>

<https://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xhtml>

<https://www.iana.org/assignments/ipv6-unicast-address-assignments/ipv6-unicast-address-assignments.xhtml>

Es gibt automatisch erstellte Listen, die diese Präfixe enthalten, sowie Präfixe, die von keinem RIR zugewiesen wurden. Die bekannteste ist <https://www.team-cymru.org/Services/Bogons/fullbogons-ipv6.txt>.

Sie können sie direkt verwenden (Bogon + unallocated) oder nur die Informationen über routbare Unicast-Adressen 2000::/3 behalten

Beachten Sie, dass der 2001:4:112::/48 AS112-Block es ermöglicht, die zahlreichen Reverse-DNS-Anfragen (ptr), die mit privaten IPs verbunden sind, zu verbergen. Das AS112-Projekt zielt darauf ab, DNS-Root zu entlasten, und wird von der ICANN durchgeführt, die aus den Anfragen Statistiken erstellt. Sie sollten dieses Präfix also nur dann sperren, wenn Ihre DNS-Infrastruktur das Blackholing selbst durchführt.

• HEADER EXTENSION

IPv6 bringt Header-Extensions (EHs) mit sich. Sie können kombiniert werden und müssen bei einem vom Absender-Host fragmentierten Paket immer auf im ersten Fragment erscheinen. Daher muss jedes 1. Fragment, das nicht den vollständigen IPv6-Header enthält, zerstört werden.

Eine davon ist der HopByHop (proto 0), der von jedem zwischengeschalteten Router behandelt werden muss. Dies macht de facto einen DDoS möglich, insbesondere wenn das Gerät die Bearbeitung an die Steuerungsebene weiterleiten muss. Anstatt das Paket zu zerstören, ist es besser, dieses Feld an der Organisationsgrenze zu ignorieren. Es ist immer noch notwendig, es zu aktivieren, um intern Multicast oder Jumbogram zu betreiben.

Eine weitere besondere Extension ist der Routing Header (proto 43), der dem von IPv4 ähnlich zu sein scheint. Es ist jedoch nur angebracht, seine Unterelemente RHT 0 und RHT1 zu blockieren, die

dem veralteten Source Routing und Nimrod entsprechen. Andere sind relevant wie der SRH (Segment Routing Header) von SRv6.

Blockieren Sie nicht die Extension, die anzeigt, dass das Paket fragmentiert ist (Proto 44), und die zwei Extensions in Bezug auf IPsec : Encapsulation/ESP (Proto 50) und Authentication/AH (Proto 51).

Der folgende RFC-Entwurf beschreibt die empfohlene Politik (ab Abschnitt 3.3) <https://datatracker.ietf.org/doc/html/draft-ietf-opsec-ipv6-eh-filtering>

Sie sollten Pakete nicht einfach ablehnen, weil sie Header Extension enthalten. Idealerweise sollten Sie nur bestimmte Typen zwischen dem Internet und dem internen Netz filtern.

Stellen Sie sicher, dass Ihre ISPs keine Pakete mit Extensions verwerfen, und überprüfen Sie Ihre Router und Firewalls intern, um zu erkennen, wenn ein Paket aufgrund von Extensions in die Steuerebene eskaliert.

Überprüfen Sie diese Regeln alle 2 Jahre, einige Extensions können verschwinden, andere können hinzukommen. Im Moment gibt es noch Geräte, die versuchen, Extensions zu verarbeiten, auch wenn sie nicht in Ordnung sind oder sich wiederholen, was zu Abstürzen führen kann, siehe <https://datatracker.ietf.org/doc/html/draft-kampanakis-6man-ipv6-eh-parsing-01>

Schließlich sollten Sie sich die Zeit nehmen, RFC 7112 zu lesen, um zu verstehen, was passiert, wenn Extensions aneinandergereiht und fragmentiert werden. Daher die Entscheidung, sie alle in das erste Fragment zu zwingen.

• Policies

Da IPv6 eine große Anzahl von Adressen bietet, ist es notwendig, die Art und Weise zu ändern, wie vorübergehende Sperren gehandhabt werden.

Viele Mechanismen werden ausgelöst, um einen Benutzer nach einer bestimmten Anzahl erfolgloser Authentifizierungsversuche vorübergehend zu sperren oder um eine Website nach starkem Datenverkehr von einer einzelnen IP-Adresse mit einem Captcha zu versehen. Dies ist typischerweise das Prinzip eines Tools wie Fail2Ban oder eines ähnlichen.

Ein infizierter Rechner, der Mitglied eines Botnetzes ist, hat immer dieselbe IPv4, bis sein ISP beschließt, sie zu ändern. Er kann jedoch die 2^{64} IPv6-Adressen, die von der /64, zu der er gehört, angeboten werden, nach dem Zufallsprinzip und mit sehr häufigen Änderungen verwenden.

Auf diese Weise können die Sperrlisten schnell gesättigt werden, oder sie können im Gegenteil umgangen werden, indem die IPv6-Adresse zwischen den einzelnen Versuchen geändert wird.

Aus diesen Gründen ist es wichtig, dass Sie Ihre Blockierungsmechanismen immer auf dem /64 aufbauen. Und idealerweise sollten Sie auch einen Malus auf dem übergeordneten /56 auslösen, um Zeit zu sparen, falls ein bösartiger Versuch von einem benachbarten /64 ausgeht. Letzterer gehört wahrscheinlich zum selben Haushalt.



Dies gilt natürlich auch für den umgekehrten Fall, d. h. einen Benutzer zu bitten, sich nach 20 Minuten erneut zu authentifizieren, weil sich seine temporäre IPv6

geändert hat, macht keinen Sinn, solange er sich immer noch im selben /64 befindet.

Appendix A: Anhang



Anhang

Der Anhang enthält technische Ergänzungen und spezifische Informationen für den Heimgebrauch.

• URL UND LINK-LOCAL IP

Die link-local-Adresse im Bereich FE80::/10 weist die Besonderheit auf, dass sie eine Schnittstellenkennung enthält. Dieser Bezeichner verwendet je nach System den Namen oder die Nummer der Schnittstelle.

Linux fügt den Namen der Schnittstelle hinzu, zum Beispiel %eth0, macOS typischerweise mit %en0.

Windows hingegen fügt die Schnittstellennummer, %1 usw. hinzu.

```
C:\Users\JC>netsh interface ipv6 show address

Interface 1 : Loopback Pseudo-Interface 1

Addr Type État DAD Vie valide Pers. Fav. Adresse
-----
Autre     Préféré    infinite infinite ::1

Interface 3 : Ethernet

Addr Type État DAD Vie valide Pers. Fav. Adresse
-----
Public   Préféré    29m51s   9m51s 2a01:cb00:83f5:[REDACTED]:45e1:e8c3:a8c9:739d
Autre     Préféré    infinite infinite fe80::45e1:e8c3:a8c9:739d%3
```

Abbildung 17. netsh interface ipv6 show address

Unter Windows zeigt der Befehl `netsh interface ipv6 show address` alle zugewiesenen IPv6-Adressen an. In powershell zeigen `Get-NetAdapter` und `Get-NetIPAddress` ebenfalls Informationen an.

```
PS C:\WINDOWS\system32> Get-NetIPv6Protocol

DefaultHopLimit      : 128
NeighborCacheLimit(Entries) : 256
RouteCacheLimit(Entries) : 4096
ReassemblyLimit(Bytes)  : 133913120
IcmpRedirects        : Enabled
SourceRoutingBehavior : DontForward
DhcpMediaSense        : Enabled
MediaSenseEventLog    : Disabled
MldLevel              : All
MldVersion            : Version2
MulticastForwarding   : Disabled
GroupForwardedFragments : Disabled
RandomizeIdentifiers : Enabled
AddressMaskReply      : Disabled
UseTemporaryAddresses : Enabled
MaxTemporaryDadAttempts : 3
MaxTemporaryValidLifetime : 7.00:00:00
MaxTemporaryPreferredLifetime : 1.00:00:00
TemporaryRegenerateTime : 00:00:05
MaxTemporaryDesyncTime : 00:10:00
DeadGatewayDetection  : Enabled
```

Abbildung 18. Get-NetIPv6Protocol

Der Powershell-Befehl `Get-NetIPv6Protocol` gibt die globale Host-IPv6-Konfiguration zurück.

Für Entwicklungszwecke oder einfach für den Heimgebrauch werden URLs üblicherweise mit IP gebildet.

In IPv6 hat eine http-URL zum Beispiel die Form `http://[2001:db8:AAAA:BBBB::H]:8080`

Derzeit ist es nicht möglich, link-lokale Adressen innerhalb einer URL in einem gängigen Webbrower zu verwenden. RFC 6874 erzwingt die Verwendung des %-Zeichens vor der Schnittstellenkennung in einer URL (%2, %eth0, usw.)

Die Verwendung von % ist jedoch der HTML-Gemeinschaft vorbehalten, WHATWG
<https://github.com/whatwg/url/issues/392>

Man sollte also immer globale oder lokale Adressen in einem Browser verwenden. Ihre Unterstützung funktioniert normalerweise in anderen Kontexten, wie einem SCP-Client.

Hier ist das Ticket für die Neuimplementierung des Link-Local in Firefox:
https://bugzilla.mozilla.org/show_bug.cgi?id=700999

Und Chrom <https://bugs.chromium.org/p/chromium/issues/detail?id=70762>

Denken Sie daran, dass eine rein lokale Anwendung (z. B. eine Industriesteuerungsschnittstelle) niemals benötigt, dass sich ein Benutzer über die lokale Link-Adresse in einem Browser mit ihr verbindet.

• MEHRERE PRÄFIXE

IPv6 ermöglicht die gleichzeitige Verwendung mehrerer Präfixe in einem Netz, doch obwohl dieser Mechanismus auf niedriger Ebene im Netz und bei den Hosts sehr gut funktioniert, wirft er einige Probleme auf.

Die Datenströme verlassen den Host von einer standardmäßig gewählten Adresse oder von der Adresse, die das längste gemeinsame Präfix mit dem Ziel hat. Dieser unkontrollierte Aspekt macht die Konfiguration komplexer.

Welche Adresse sollte automatisch im lokalen DNS registriert werden?

Sicherheitssysteme, sei es auf der Zugangsebene (L2-NDP) oder auf der Verkehrsebene (FW, ACL usw.), müssen in der Lage sein, sich im laufenden Betrieb anzupassen.

Multi-homing bis zu den Hosts kann in einer kleinen Struktur interessant bleiben, um einen Wechsel bei einem Providerwechsel zu ermöglichen. Für Netze mittlerer Größe ist die Kombination (PI oder ULA) + NPTv6 die bessere Wahl. Letzteres ist zustandslos und leicht zu konfigurieren.



Es wurde ein Mechanismus entwickelt, der es einem Client und einem Server ermöglicht, ihre unterschiedlichen Adressen über eine Header-Erweiterung auszutauschen und im Falle eines Fehlers zu wechseln, ohne die obere Schicht zu beeinträchtigen und daher ohne Zeitüberschreitung. Dies war Shim6. Sie konnten sich sogar über Adressen authentifizieren, die mit kryptografischen Mechanismen (CGA) erzeugt wurden. In der Praxis wurde Shim6 fallen gelassen, so dass wir im Bereich von Timeout + Aufbau einer neuen Sitzung bei Verlust eines Pfades

bleiben, oder von einem Protokoll der oberen Schicht berücksichtigt werden. Was das OSI-Modell betrifft, so ist anzumerken, dass IP diese Art von Mechanismus ohnehin nie bereitstellen sollte; dies ist die Aufgabe von TCP und jetzt QUIC.

• CONTAINER

Docker

Docker betreibt standardmäßig eine Bridge, eine Docker0-Schnittstelle, und fügt Ports zu NAT44-Regeln hinzu, die auf veröffentlichte Container-Ports verweisen. Es können zusätzliche Bridges erstellt werden, um Container voneinander zu isolieren.

Der Overlay-Modus nutzt VxLAN und ermöglicht die Kommunikation zwischen Hosts, ohne sich um die Konfiguration des zugrunde liegenden Netzes kümmern zu müssen (zusätzlich zur Möglichkeit der Verschlüsselung, Vereinfachung der SWARM-Verwaltung usw.).

Es ist daher schwierig, IPv6 zu verwenden, da Docker so konzipiert ist, dass es eine vollständige Abstraktion des Netzwerks (und auch des Rests) bietet.

Es gibt mehrere Möglichkeiten, dieses Problem zu umgehen:

- Verwenden Sie den "macvlan"-Modus, bei dem die Container auf Ebene 2 wie VMs behandelt werden. Jeder mit seiner eigenen MAC. Nicht sehr praktisch und vor allem schwierig in das Ökosystem zu integrieren und zu betreiben;
- Der neuere IPvlan L2-Modus stellt die IPs der Container hinter derselben MAC wie der Host über einen leichteren Mechanismus als das klassische Bridging zur Verfügung;
- In seiner L3-Version eliminiert IPvlan vollständig das Schleifenrisiko und stützt sich auf IPv4-Subnetze und IPv6-Präfixe. Die entsprechenden Routen müssen auf den Netzgeräten implementiert werden, wobei jeder Host über ein oder mehrere eindeutige Präfixe verfügt.

Im Jahr 2016 initiierte ein Entwickler ein Projekt zu NAT66 im Bridge-Modus in Docker <https://github.com/robertkl/docker-ipv6nat>

Er weist auch darauf hin, dass durch das Fehlen von NAT alle Ports in IPv6 zugänglich sind und man sich daher Gedanken über die Sicherung des Zugangs im Vorfeld machen muss.

Für große Installationen empfehlen wir den IPvlan L3-Modus.

Brauchen wir wirklich IPv6 in Docker? Wie im Dokument angedeutet, ist es interessant, IPv6-Unterstützung auf dem Frontend bereitzustellen (zum Beispiel SLB-Container wie traefik, hap, envoy, caddy usw.). Darüber hinaus kann das Backend in IPv4 bleiben.

Kubernetes

Kubernetes stellt standardmäßig eine IP pro Pod (Gruppierung von Containern auf einem Host) zur Verfügung. Der Host wird als Node bezeichnet. Achten Sie auf die Bedeutung von Pod, die sich hier von anderen Lösungen unterscheidet. Die Adresse wird dem Block entnommen, der der Node zugewiesen ist.

Die Adressierung ist somit flach und ohne Overlay, was die Kommunikation zwischen den einzelnen Pods erleichtert, unabhängig davon, ob sie sich im selben Node befinden oder nicht. Die Sicht auf die Adressierung ist daher identisch, egal ob man sich innerhalb oder außerhalb der Lösung befindet.

Er ist daher dem IPvlan-3-Modus von Docker sehr ähnlich.

Die Verwaltung des Netzes wird dann von einer der zahlreichen Lösungen von Drittanbietern übernommen, die es auf dem Markt gibt (Open Source oder nicht).

Schließlich erfolgt der Zugriff von außen in der Regel über die Kubernetes-Services-Kombination in Verbindung mit einem Load-Balancer, wobei letzterer meist extern ist.

IPv6 wurde vor kurzem von Docker als stabile Funktion markiert, Kubernetes folgte mit Beta-Unterstützung in 1.21 und stabil in 1.23. <https://kubernetes.io/docs/concepts/services-networking/dual-stack/>

Seit diesen Veröffentlichungen Ende 2021 haben einige Cloud-Anbieter bereits damit begonnen, IPv6 für Containerdienste und andere verwaltete Dienste, die indirekt von Containern genutzt werden, einzuführen.

Denken Sie daran, dass der Load Balancer immer eine Adressübersetzung durchführt, es sei denn, Sie verwenden Headless Services.

Für den ausgehenden Datenverkehr ins Internet ist durch die Verwendung öffentlicher IPv6-Adressen kein Proxying oder NAT erforderlich.

• SCADA

Bei einem SCADA-Netz handelt es sich um ein geschlossenes Netz, wie es häufig in der Industrie anzutreffen ist. Der Sinn einer Migration zu IPv6 ist hier relativ begrenzt. Die Kompatibilität von Industrielösungen mit dem Protokoll wird noch einige Zeit dauern, bis sie vollständig ausgereift ist. Zögern Sie jedoch nicht, diese Kompatibilität in den optionalen Fragen der Ausschreibungen zu erwähnen, und ziehen Sie IPv6 nur dann ernsthaft in Betracht, wenn das gesamte Ökosystem kompatibel und getestet ist. Wenn Ihr SCADA-Netz riesig ist, da Ihr Unternehmen viele Präsenzpunkte umfasst, kann IPv6 Ihnen immer noch die IPv4-Adressierung ersparen. Die Implementierung von 6LoWPAN auf eingebetteter Hardware kann ebenfalls eine wichtige Rolle spielen. Andernfalls können Sie immer noch mit IPv4-Adressüberlagerungen/Überschneidungen mit dem Rest der IT arbeiten, da das Prinzip der SCADA darin besteht, dass sie isoliert ist und nicht an andere Ressourcen weitergeleitet wird. Somit ist die Überlappung nur an den Schnittstellenelementen zwischen dem allgemeinen Informationssystem und dem SCADA-Informationssystem zu handhaben, und das sind aus Sicherheitsgründen nur wenige Elemente.

• NAT64 IN DEN NETZEN DER MOBILFUNKBETREIBER

Schauen wir uns an, was bei der Einrichtung von NAT64 zwischen Smartphones und dem Internet zu beachten ist.

Service Discovery

Der Abschnitt NAT64 des Dokuments erläutert die Implementierung mit Workstations. Einige Methoden werden verwendet, um Hosts mit dem NAT64-Präfix zu versorgen, hauptsächlich auf mobilen Plattformen. Dadurch wird sichergestellt, dass die Endpunkte wissen, dass sie sich hinter einem NAT64 befinden. Die Hauptvorteile dieses Bewusstseins bestehen darin, dass der Host die DNSSEC-Validierung wiederherstellen kann und dass der Betrieb von Adressliteralen nicht nur in der IP-Schicht möglich ist, sondern auch dann, wenn eine Payload sie enthält (z. B. SIP ohne die Notwendigkeit eines ALG).

RFC7051 behandelt dieses Thema, ebenso wie der folgende Entwurf:

<https://tools.ietf.org/id/draft-ietf-v6ops-nat64-deployment-08.html>

Eine Lösung ist der DNS-Eintrag `ipv4only.arpa`, der eine bekannte Antwort auf der Grundlage eines RFC liefern muss. In diesem Fall ein A-Eintrag 192.0.0.170 oder 192.0.0.171.

Wenn die Antwort ein AAAA-Datensatz ist, z. B. `64:ff9b::192.0.0.170` (hier in Dezimalschreibweise, damit Sie es leichter lesen können, wenn Sie sich in den Anhang gewagt haben), dann ist eine NAT64-Plattform mit dem Präfix `64:ff9b::/96` in Produktion. Übrigens macht Android das Gleiche mit dem DNS-Eintrag `ipv4.google.com`.

Das PCP-Protokoll (mit dem Sie einen Port auf Ihrem Heimrouter öffnen können) bietet auch die Möglichkeit, das Vorhandensein eines NAT64-Präfixes abzufragen.

Im RFC werden andere Möglichkeiten genannt, nämlich die Bereitstellung der Informationen im Router Advertisement oder über eine DHCPv6-Option.

Schließlich ermöglicht die gute alte APN-Konfiguration des Netzbetreibers auf dem Handy auch die Weitergabe des Präfixes an Smartphones.

PC-Betriebssysteme unterstützen leider keine dieser Methoden auf ihren LAN-Schnittstellen. DNS64 wird also noch lange Zeit im Unternehmen bleiben.

Betrieb auf mobilen Betriebssystemen

Um die Kompatibilität mit der Verwendung von IPv4-Adressen sowie die Unterstützung von DNSsec-Signaturen usw. zu gewährleisten, müssen mobile Betriebssysteme IPv4 verwenden können.

Obwohl die beiden wichtigsten mobilen Betriebssysteme Mechanismen zur Gewährleistung der IPv4-Kompatibilität implementieren, unterscheidet sich die Umsetzung grundlegend.

Google Android stützt sich auf das Netzwerk und 464 XLAT.

Die Datei `clatd.conf` enthält Anweisungen für die CLAT-Konfiguration des Endpunkts. Eine IPv6-Adresse, die Teil des dem Endpunkt zugewiesenen /64 ist, wird mit einer virtuellen privaten IPv4-Adresse abgebildet (SIIT). (Häufig 192.0.0.4). Der IP-Stack fängt alle IPv4-Pakete ab und übersetzt sie in IPv6. In der anderen Richtung wird ein Paket, sobald es an der für die CLAT reservierten Adresse ankommt, in IPv4 übersetzt. Die Entwicklung kann hier verfolgt werden <https://android-review.googlesource.com/q/project:platform%252Fexternal%252Fandroid-clat>

Apple iOS macht sich die eher begrenzte Offenheit seines Systems zunutze, um das Problem auf den oberen Ebenen zu lösen. So wandeln die Frameworks (CFNetwork auf der unteren Ebene, das Cocoa-URL-Ladesystem auf der höheren Ebene) sowie die obligatorische Browsing-Rendering-Engine WebKit jede IPv4-Adresse direkt in die Adresse um, die durch die Synthese des NAT64-Präfixes mit dieser Adresse zurückgegeben wird. Auf diese Weise wird kein einziges IPv4-Paket wirklich erzeugt. Dieser Weg ist aus energetischer Sicht effizienter.

Hotspots und Teathering

Bei der gemeinsamen Nutzung, die auch als Hotspot oder Tethering bezeichnet wird, wird Dual-Stack-WiFi für Hosts bereitgestellt, die nicht wissen, dass nur IPv6 an den Router geliefert wird, in diesem Fall ein Smartphone.

Wenn 464 XLAT zur Rettung kommt, wird das Telefon als CLAT in Verbindung mit dem NAT64 (PLAT) des Betreibernetzes handeln. Gleicher Betrieb auf Android und iOS:

Anstatt ein zustandsabhängiges NAT44 gefolgt von einem NAT46 durchzuführen, wird eine zustandslose Zuordnungsregel (SIIT) zwischen dem IPv4-Netz des Hotspots (meist /24) und einem Teil des /64-IPv6-Netzes, das ihm gehört, erstellt. Somit ist keine Zustandstabelle und kein Portwechsel auf der Telefonseite erforderlich. Der Verkehr durchläuft dann das Stateful NAT64 des Netzbetreibers, um im Internet wieder auf IPv4 umzuschalten.

Denken Sie daran, dass der IPv6-Header länger ist und das erste Gateway den Datenverkehr möglicherweise fragmentieren muss. Wundern Sie sich also nicht, wenn das Hochladen einer Datei durch CLAT verlangsamt wird. Die derzeit auf dem Markt erhältlichen ARM-SoCs bieten Hardware-Unterstützung für alle 464 XLAT-Operationen, um solche Probleme zu vermeiden.

• IPv4 PORT SHARING

Die Address + Port-Techniken werden kurz in dem Abschnitt über die Übergangsmechanismen behandelt. (4rd und MAP-T/E für die neuesten Verfahren). Hosts hinter einem Heimrouter, die einen solchen Mechanismus verwenden, wissen nicht, dass nur ein Teil der 65.535 Ports ihrem WAN zugewiesen ist.

Das ist nicht weiter besorgniserregend, es sei denn, ein Programm verlangt die Öffnung eines Ports (UPnP, NAT-PMP) und der Router vergisst, dass er nicht auf alle Ports Zugriff hat. Manchmal gibt er einen Port zurück, der außerhalb des dem Teilnehmer zugewiesenen Bereichs liegt. Das ist wie russisches Roulette bei einigen P2P-Börsen.

In RFC 6269 werden die Probleme im Zusammenhang mit der gemeinsamen Nutzung erörtert, darunter auch das hier erwähnte Problem, das bei Betreibern auftritt, die die gemeinsame Nutzung zu schnell und zu locker umgesetzt haben.

Ein ISP sollte IPs nicht mit mehr als 16 Kunden teilen.

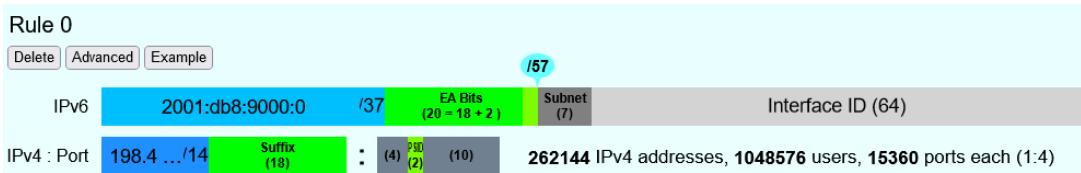


Abbildung 19. MAP A+P Simulation der gemeinsamen Nutzung von Ports

In diesem Beispiel wird IPv4 zwischen vier Kunden geteilt <http://map46.cisco.com/MAP.php>

• RFC-ENTWÜRFE ZUR RETTUNG VON IPv4

Einige Leute bemühen sich, die Lebensdauer von IPv4 zu verlängern, indem sie Wege finden, seine Adressierungsmöglichkeiten zu erweitern.

Es gab mehrere Entwürfe, von denen die jüngsten zu sein scheinen:

<https://www.ietf.org/id/draft-schoen-intarea-unicast-0-00.html>

<https://www.ietf.org/id/draft-schoen-intarea-unicast-127-00.html>

<https://www.ietf.org/id/draft-schoen-intarea-unicast-240-00.html>

Es versteht sich von selbst, dass die Aktualisierung aller IP-Stacks von PC-Betriebssystemen, Smartphones, Routern usw. zur Unterstützung dieser Änderungen wesentlich mehr Aufwand erfordern würde als die Umstellung auf IPv6.

Dennoch wird 240/4 offiziell von mindestens zwei großen Herstellern sowie von Google GCP unterstützt.

Der EzIP-Vorschlag befindet sich in seiner neunten Auflage, wenn Sie NAT lesen möchten:

<https://datatracker.ietf.org/doc/html/draft-chen-ati-adaptive-ipv4-address-space-09>

• BEISPIELE FÜR IPV6-IMPLEMENTIERUNGSPROBLEME

Hier sind einige Beispiele für Implementierungsfehler, die bei der Verwendung von IPv6 auftreten.

Nicht gelöschte Routen

Bei IPv4 hat man entweder Konnektivität oder nicht. Wie können Sie sicher sein, dass die IPv6-Konnektivität verfügbar ist, sobald Sie auf Dual-Stack umstellen? Happy Eyeballs kann helfen, aber es erzeugt eine Verzögerung und ist nicht dafür ausgelegt, eine längere Abwesenheit von IPv6-Konnektivität zu kompensieren.

Beispielsweise haben die ISP-Router mit LTE-Backup oft nur IPv4 auf dem Backup-Link. Wenn das Backup ausgelöst wird, senden einige Router weiterhin RAs, um sich als Standard-Router zu deklarieren und ein IPv6-Präfix anzukündigen, das nicht mehr nutzbar ist, da die IPv6-Konnektivität vollständig unterbrochen ist.

Dieses Problem tritt auch bei der Umnummerierung auf. Bei IPv4 macht NAT44 das lokale Netz unabhängig von der WAN-Addressierung. Bei IPv6 ist dies nicht mehr der Fall (außer bei der Kombination von ULA und NPTv6). In den seltenen Fällen, in denen ein ISP sein Netz umnummert, kann es daher zu einem vorübergehenden Verlust der Konnektivität kommen, solange die alten RA-Informationen noch im Cache gespeichert sind.

In Abschnitt 6.3.5 von RFC 4861 heißt es, dass Hosts das Präfix löschen müssen, wenn der Timer abläuft oder wenn der Router sich nicht mehr als Standard ankündigt. In unserem Fall existiert der Router jedoch noch und ist über seine lokale Link-Adresse erreichbar. Die Hosts werden warten, bis der Präfix-Timer abgelaufen ist, bevor sie die Schnittstellenadresse(n) mit dem alten Präfix löschen. Die Endpunkte werden also weiterhin Pakete an den Router senden, allerdings mit einer Quelladresse, die zum alten Präfix gehört... Sie werden vergeblich auf eine Antwort warten und ohne aggressive Timer-Einstellungen kann es leicht 1800 Sekunden oder eine halbe Stunde dauern. Wir können den Betreibern nur empfehlen, die Ablaufzeiten auf einen Wert unter einer Minute zu senken.

Wer mit IPv6-Multihoming spielen will, wird schnell auf ähnliche Failover-Probleme stoßen.

Unerwartete Verwendung der IPv4-Präfix-Darstellung

Um Ihr Informationssystem zu vereinfachen, haben Sie beschlossen, in Ihrer CMDB nur die IPv6-Notation zu verwenden. So verwenden Sie in Ihren Konfigurationsskripten usw. das Präfix ::ffff:0:0/96, um ein IPv4 anzugeben.

Seltsamerweise erstellt Ihr Skript zwar eine ACL-Regel/Richtlinie, kann sie dann aber bei der Überprüfung nicht finden und beendet die Ausführung mit einem Fehler. Der betreffende Ablauf funktioniert jedoch.

Tatsächlich hat das konfigurierte System einfach beschlossen, die Notation eines IPv4 mit ::ffff:0:0/96 zurück in die klassische IPv4-Notation zu übersetzen.

Diese Art von Verhalten gab es schon bei einigen F5-Produkten, zum Beispiel: <https://cdn.f5.com/product/bugtracker/ID669888.html>

Praktisch, aber bei Automatisierungen zu berücksichtigen.

```
PS C:\WINDOWS\system32> ping ::ffff:c0a8:1
Envoi d'une requête 'Ping' 192.168.0.1 avec 32 octets de données :
Réponse de 192.168.0.1 : octets=32 temps<1ms TTL=64
Réponse de 192.168.0.1 : octets=32 temps<1ms TTL=64
```

Abbildung 20. Diese automatische Konvertierung können wir in gängigen Tools wie Windows ping finden

Inkompatible Eingabefelder

Bei der Eingabe einer IPv6 sind die Feldprüfungen manchmal unzureichend. Die folgenden Fehler können in grafischen Umgebungen und seltener in einer Befehlszeilenumgebung auftreten.

Ein völlig inkompatibles Feld lehnt eine Adresse ab, die nicht in der IPv4-Form vorliegt, aber auch Feinheiten können die Prüfungen überlisten. Zum Beispiel wird manchmal das [], das die Adresse vom Port trennt, nicht beachtet.

So kann die Eingabe von [2001:db8::2D5E]:8443 von der Software in 2001:db8::2D5E:8443 umgewandelt werden.

• VERSCHWENDUNG VON ADRESSSRAUM

Ja, es gibt viele IPv6-Adressen! Das Internet ist voll von klugen Berechnungen, die uns erklären, dass 2E128 gleich $3,4 * 10^{38}$ Adressen sind, d.h. 667 Sextillionen pro m² terrestrischer Oberfläche. Die Zahl liegt außerdem nahe an der Avogadro-Konstante ($\sim 6,02 \cdot 10^{23}$).

Mit Sätzen wie "wir könnten jedes Sandkorn bis zu 2 km tief adressieren" glauben wir natürlich, dass wir alles tun können.

Eine IPv6-Adresse ist jedoch weder ein Nummernschild noch eine Telefonnummer. Sie ist meist auf der Grundlage eines /64-Präfixes aufgebaut. Außerdem gehören diese Präfixe zu einer Teilmenge, die für das globale Routing reserviert ist und vom RIR zugewiesen wird.

Ein großes Unternehmen, das ein /29 erhält, kann also logischerweise 34 Milliarden Netze schaffen. Wenn wir nun die Anzahl der Einrichtungen in /48 zählen, sind es 524.288.

Die indische Post mit ihren 160.000 Postämtern ist also beruhigt... Nun, es sei denn, jemand beschließt, dass das Guest-WiFi und das IoT-Projekt für intelligente Gebäude jeweils ihre eigenen /48 pro Standort benötigen, weil Sicherheit/Politik/Delegation/interne Organisation (streichen Sie das Unwichtige) dies erfordern. Das wird Sie zum Lachen bringen, aber schauen Sie sich IPv4 an, diese Art der Argumentation ist viel zu weit verbreitet.

• UMWIDMUNG VON ADRESSEN FÜR ANDERE ZWECKE

Die riesige Anzahl möglicher Adressen hat die Ingenieure auf Ideen gebracht, wie man sie auf der Grundlage der genauen Identifizierung des Benutzers und/oder der Ressource, auf die zugegriffen werden soll, manipulieren kann.

Hier sind einige Beispiele:

- Einem Server für jeden Client, der sich mit ihm verbindet, unterschiedliche IPv6-Adressen zuweisen? Im Falle eines DDoS können wir nur die betroffene Adresse blockieren, ohne die anderen Clients zu beeinträchtigen, die sich mit demselben Rechner verbinden. Der zukünftige Freund von RTBH?
- Eine Authentifizierung direkt in die Adresse aufnehmen, die sich mit der Zeit weiterentwickelt? Dies ist das Prinzip des IPv6 TOTP, das von diesem SSH-Server-Projekt bereitgestellt wird, dessen IP sich alle 30 Sekunden ändert. <https://github.com/mikroskeem/tosh>
- Direkte Zuweisung von Daten wie z. B. Streaming-Video-Chunks und nicht mehr der Server, der sie hostet; dies ist z. B. der Gegenstand des folgenden Patents <https://patents.justia.com/patent/11134052>

Wenn jedem Server eine große Anzahl von Adressen zugewiesen wird, kann der NDP-Cache schnell überlastet werden.

Diese Verwendungszwecke sind weiterhin möglich, wenn wir dem Server direkt ein /64-Präfix

zuweisen, wie in RFC 8273 beschrieben. Dies ist, was wir bereits mit Containern tun, wie oben am Beispiel von Kubernetes-Knoten beschrieben. Diese /64 könnten auch von Load Balancern gehandhabt werden.

Für Systeme mit regelmäßigm Adresswechsel bedeutet dies, dass jedes Mal eine Sitzung neu aufgebaut werden muss, aber schließlich wäre es nie mehr als eine neue Verwendung der 0-RTT von QUIC zum Beispiel.

• SRv6

Segment-Routing breitet sich bei Netzbetreibern und GAFAMs rasch aus. Derzeit ist SR-MPLS führend, aber Prognosen zeigen, dass sein Gegenstück, das auf einer einfachen IPV6-Datenebene basiert, in einigen Semestern die Führung übernehmen wird.

Die Beherrschung des IPv6-Transports und dieses sektordominanten IGP, IS-IS, wird schnell zu einem Muss für jedes große Netz.

Zusätzlich zu den Beiträgen der SR in Bezug auf die dynamische und adaptive Topologie, die Telemetrie und die Möglichkeit, dienstorientierte Felder (Sicherheitsgruppe, Anwendungskennung...) in den SRH-Header aufzunehmen, wird sie zweifellos die erste sein, die die Gesamtheit der bestehenden Stacks von Schichtenprotokollen ersetzt.

So wird es über das Backbone hinaus wahrscheinlich das Paar VxLAN + EVPN im Rechenzentrum sowie die geschlossenen SDN-Campus-Lösungen ersetzen. Sie bietet einen echten End-to-End-Service ohne Kompromisse.

Die Dienstfelder werden dann eine echte dynamische Anwendung von Richtlinien ermöglichen, die nicht mehr auf Adressbereichen usw., sondern auf zusätzlichen Informationen basieren. All dies geschieht ohne proprietäre Technologie, sondern kann sowohl von physischen als auch von virtuellen Dienstgeräten (VNF) genutzt werden.

Später werden diese Felder wahrscheinlich vom Host selbst eingefügt, so dass Informationen, die direkt von der Anwendung bereitgestellt werden, an ihn weitergegeben werden können. Der 1st-Hop-Router wird weiterhin für das Hinzufügen des ausgewählten Pfads zuständig sein. Auf der Serverseite haben wir die Integration der VTEP-Terminierung (VxLAN und manchmal GENEVE) gesehen, die von den Top-of-Rack-Switches zu den Servern selbst herunterkommt. Auf die gleiche Weise werden wir wahrscheinlich eine vollständige SRv6-Verarbeitung auf Servern erleben, einschließlich der Topologieverwaltung, insbesondere dank der Ankunft von Netzwerkprozessoreinheiten (NPUs, nicht zu verwechseln mit Neural Processor Units) und IPUs (Infrastructure Processing Units).

Die Hersteller drängen die Unternehmen derzeit zur Umstellung auf SR-MPLS, um dann später mit SRv6 zurückzukommen. Möglicherweise werden wir jedoch bald damit beginnen, den Übergang zu SRv6 direkt im Unternehmensnetz und nicht mehr nur in den Netzen der Netzbetreiber zu unterstützen.

• THREAD

Thread ist ein IoT-orientiertes Netzwerkprotokoll, das von der Thread Group <https://www.threadgroup.org/> vorangetrieben wird.



Abbildung 21. Logo von Thread

Sein Zweck ist die Bereitstellung eines Mesh-Kommunikationsnetzes zwischen Hausautomatisierungsgeräten auf der Grundlage von 6LoWPAN. Es nutzt IPv6 mit den Begriffen "Scope", "Routerknoten" und "Children". Besuchen Sie die OpenThread Open Source Projektseite <https://openthread.io/guides/thread-primer/ipv6-addressing>.

Der Smart-Home-Konnektivitätsstandard **Matter** ist mit ihm aufgebaut.

• SELF-HOSTING UND HEIMANWENDER

Anhand der Erfahrungen mit der Implementierung von IPv6 in einem einfachen Heimnetzwerk lassen sich einige der Unterschiede zu IPv4 leicht nachvollziehen. Insbesondere werden wir hier die Exposition der Dienste gegenüber der Außenwelt sehen.

Obwohl diese Beispiele in einer kleinen Struktur verwendet werden können, erinnern wir Sie daran, dass es unerlässlich ist, eine echte Filter- und Analyseschicht am Eingang des Internets auf einem Produktionssystem zu haben, selbst wenn es klein ist.

Adressierung und DNS-Veröffentlichung

Meistens stellen die Netzbetreiber nur ein /64 zur Verfügung, ohne die Möglichkeit, die anderen dem Router zugewiesenen Präfixe zu verwenden (oft in Form eines /56).

Es ist auch unmöglich, die Stabilität des Präfixes im Laufe der Zeit zu gewährleisten (es sei denn, es besteht eine vertragliche Verpflichtung).

Die Adresse jedes auszustellenden Rechners muss daher unabhängig veröffentlicht werden, während wir früher die WAN-IPv4-Adresse veröffentlicht und mit den NAT44-Ports gespielt haben.

Wir beginnen damit, dass wir sicherstellen, dass die Rechner eine stabile Adresse verwenden (in der Regel basierend auf MAC oder stable Privacy, was wünschenswert ist).

Wir werden dann einen dynamischen IPv6-DNS-Dienst verwenden, z. B. Dynu, DuckDNS usw.

Es gibt mehrere Methoden, um das IP/AAAA-DNS-Eintragspaar direkt auf einem Rechner zu verfolgen:

- Abfrageskript mit automatischer Erkennung der Adresse durch den API-Server des DNS-Dienstes;
- Skript, das die öffentliche IP-Adresse über eine Drittanbieter-API abruft (z. B. api6.ipify.org) und dann an den DNS-Dienst weiterleitet;

- Skript, das die IP von der Systemschnittstelle abruft (achten Sie darauf, die öffentliche stabile IP zu verwenden);
- Software-Agent des Dienstes.

Es ist auch möglich, sich auf einen Router und seine NDP-Informationen zu verlassen, aber dann verlassen wir die einfache Verwendung des Heimrouters.

Flow opening

Die Bereitstellung einer Firewall in IPv6 wird von den Betreibern uneinheitlich gehandhabt. Einige haben sie sehr spät im Alles-oder-Nichts-Modus implementiert, andere bieten eine ähnliche Granularität wie bei IPv4.

Nehmen wir das Beispiel einer Orange ISP LiveBox 4. Bei IPv4 wird die Öffnung im Netzwerkbereich vorgenommen.

The screenshot shows the 'Réseau' (Network) section of the configuration interface. At the top, there is a navigation bar with 'Retour' (Back) and 'Réseau'. Below it is a horizontal menu bar with tabs: DHCP, NAT/PAT, DNS, UPnP, DynDNS, DMZ, NTP, and IPv6. The 'DHCP' tab is currently selected. A note below the menu states: 'Les règles NAT/PAT sont nécessaires pour autoriser une communication initiée depuis Internet avec un équipement particulier de votre réseau. Utiles pour certaines applications comme des jeux en lignes ou des serveurs de type FTP ... Assurez-vous que cet équipement a une adresse IP statique (paramétrable dans l'onglet DHCP).'. Another note says: 'Uniquement pour des équipements IPv4.' Under the heading 'Vos règles personnalisées' (Your custom rules), there is a table for defining port forwarding rules:

mon-service	8443	443	TCP	PARX	Toutes	Créer
ex. : 1000	ex. : 1000-2000				IP externes autorisées	

Below the table is a row of buttons: 'Activer' (Enable), 'Application/Service', 'Port interne', 'Port externe', 'Protocole', 'Équipement', and 'IP externe'.

Abbildung 22. IPv4 Orange ISP LiveBox 4 (Frankreich)

Bei IPv4 sind wir daran gewöhnt, unterschiedliche Ports für intern und extern zu haben, was eine Änderung der Ports auf den Servern vermeidet, aber verhindert, dass mehrere Rechner auf demselben externen Port veröffentlicht werden (es sei denn, Sie gehen über einen zwischengeschalteten Reverse Proxy).

Bei IPv6 ist die Situation genau umgekehrt: Jeder Rechner hat seine IP und damit seine 65535 Ports, aber man muss zwangsläufig intern und extern die gleiche Portnummer verwenden, weil es keine Übersetzung (PAT) gibt.

Bei Orange ISP befindet sich die Konfiguration im Bereich der Firewall.

[Retour](#)

Pare-feu

[Annuler](#)[Enregistrer](#)

Ouverture de ports dans le pare-feu (pour équipements IPv6).

The screenshot shows a configuration page for opening ports in a firewall. At the top, there are input fields for 'mon-service-v6' (IP address), '443' (port number), 'TCP' (protocol), 'PARX' (equipment), and 'Toutes' (all). Below these is a note 'ex. : 1000-2000'. To the right, a button 'Créer' (Create) is visible, with the text 'IP externes autorisées' (Authorized external IPs) below it. A table below the form has columns: 'Activer' (Activate), 'Application/Service' (Application/Service), 'Port' (Port), 'Protocole' (Protocol), 'Équipement' (Equipment), and 'Adresse IP externe' (External IP Address). The 'Activer' column contains a checked checkbox.

Abbildung 23. IPv4 Orange ISP LiveBox 4 (Frankreich)

Erreichbarkeitstest

Der Test kann über einen Online-Port-Scanner wie <http://www.ipv6scanner.com/> durchgeführt werden.

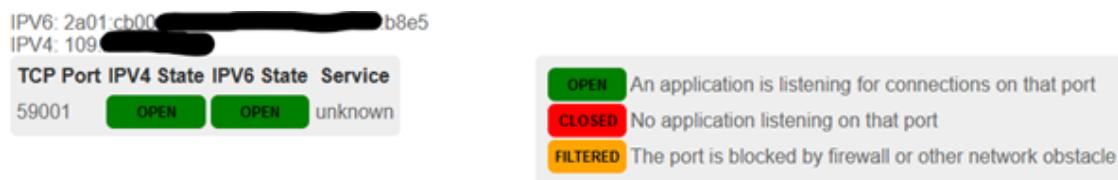


Abbildung 24. Ergebnis des Port-Scans"

Hier ist alles in Ordnung, ansonsten denken Sie daran, dass Happy-Eyeballs V2 die Verbindung auf IPv4 zurückschaltet, wenn keine v6-Antwort kommt.

Einige Anbieter bieten keine guten Firewalls an. Dies ist der Fall bei Iliad Free, das sich lange hinter der Tatsache verbirgt, dass der RFC zu CPE zwar eine zustandsabhängige Filterung empfiehlt, aber nicht vorschreibt. Free bietet erst seit 2020 eine IPv6-Firewall an und die ist sehr schwach. Viele Kunden fordern auf dem Bugtracker <https://dev.freebox.fr/bugs/index.php?string=ipv6&project=9&type%5B%5D=&sev%5B%5D=&pri%5B%5D=&due%5B%5D=&reported%5B%5D=&cat%5B%5D=&status%5B%5D=open&opened=&dev=&closed=&duedatefrom=&duedateto=&changedfrom=&changedto=&openedfrom=&openedto=&closedfrom=&closedto=&do=index> die Implementierung einer echten Firewall.

• AUTOMATISCHE PORTFREIGABE

Wie bereits erwähnt, ermöglicht PCP V2 die Öffnung eines Ports durch den Router auf Anfrage einer Anwendung. Im Allgemeinen für P2P-Anwendungen.

9413 23.6.. 2a01:cb00:83f5.. fe80::a21b:29ff:feff:ba60	PCP v2	122 Map Request: 8999 -> 8999 [TCP]
14499 25.4.. 192.168.0.85 192.168.0.1	PCP v2	102 Map Request: 8999 -> 8999 [TCP]
14500 25.4.. 2a01:cb00:83f5.. fe80::a21b:29ff:feff:ba60	PCP v2	122 Map Request: 8999 -> 8999 [TCP]
14506 25.4.. 2a01:cb00:83f5.. fe80::a21b:29ff:feff:ba60	PCP v2	122 Map Request: 8999 -> 8999 [TCP]
21000 27.4.. 192.168.0.85 192.168.0.1	PCP v2	102 Map Request: 8999 -> 8999 [TCP]
21010 27.4.. 2a01:cb00:83f5.. fe80::a21b:29ff:feff:ba60	PCP v2	122 Map Request: 8999 -> 8999 [TCP]

<

```

> User Datagram Protocol, Src Port: 50061, Dst Port: 5351
< Port Control Protocol, Map Request
  Version: 2
  0... .... = R: Request
  .000 0001 = Opcode: Map (1)
  Reserved: 0
  Requested Lifetime: 3600
  Client IP Address: 2a01:cb00:83f5 [REDACTED]:739d
< Map Request
  MappingNonce: 821daa8a932c7342435fbbe9
  Protocol: 6
  Reserved: 0
  Internal Port: 8999
  Suggested External Port: 8999
  Suggested External IP Address: 2a01:cb00:83f5 [REDACTED]:739d

```

Abbildung 25. Wireshark PCP v2 IPv6

Beispiel einer Wireshark-Aufnahme von PCP V2 mit dem Filter "udp.port eq 5351". Wir stellen fest, dass sowohl in IPv4 als auch in IPv6 Anfragen geöffnet werden.

21000 27.4.. 192.168.0.85 192.168.0.1	PCP v2	102 Map Request: 8999 -> 8999 [TCP]
21010 27.4.. 2a01:cb00:83f5.. fe80::a21b:29ff:feff:ba60	PCP v2	122 Map Request: 8999 -> 8999 [TCP]

<

```

> User Datagram Protocol, Src Port: 61001, Dst Port: 5351
< Port Control Protocol, Map Request
  Version: 2
  0... .... = R: Request
  .000 0001 = Opcode: Map (1)
  Reserved: 0
  Requested Lifetime: 3600
  Client IP Address: ::ffff:192.168.0.85
< Map Request
  MappingNonce: 7d56ab9ec158d0b777f5d08d
  Protocol: 6
  Reserved: 0
  Internal Port: 8999
  Suggested External Port: 8999
  Suggested External IP Address: ::ffff:0:0

```

Abbildung 26. Wireshark PCP v2 IPv4

Beachten Sie, dass bei der IPv4-Version der Anfrage die interne IP als IPv6-Darstellung von IPv4 geschrieben ist und dass die WAN-Adresse auf 0.0.0.0 gesetzt ist, da es sich ohnehin um das IPv4-WAN des Routers handelt (wiederum in derselben Form mit ::ffff:)

Dies ist weit entfernt von dem schweren XML von UPnP-IGD, das den Austausch vieler Pakete erfordert.

• ENTWICKLUNG DER ONLINE-SPIELE

Derzeit integriert die Spieleindustrie IPv6 nicht in ihre Kommunikation zwischen Spielern und Servern. Die Auswirkungen von IPv4 CG-NAT und anderen IPv4aaS-Mechanismen könnten mit einer Anstrengung der Studios vermieden werden.

Spiele, bei denen die Partei von einem eigenen Server verwaltet wird, sollten ihren Server auf Dual Stack umstellen und IPv6 bevorzugen, wenn es verfügbar ist.

Bei P2P-Spielen, bei denen einer der Spieler der Gastgeber des Spiels ist, wäre es sinnvoll, in den Algorithmus für die Gastgeberwahl ein gewichtetes Element aufzunehmen, das auf der

Verfügbarkeit des Dual-Stacks basiert, wenn beispielsweise mindestens 40 % der Spieler im Spiel über aktives IPv6 verfügen.

• WAS IST VON DEN INTERNETPROVIDERN ZU ERWARTEN?

Die Regulierungsbehörden sollten die Betreiber auffordern, zusätzlich zu IPv6 bei Festnetzanschlüssen (xDSL, FTTH, 4/5G-Festnetz, Low Orbit SAT usw.) die folgenden Mechanismen zu implementieren:

- Eine fein abstimmbare Firewall, die dynamisch auf dem Adressensatz-Tracking für jeden Host und der Übereinstimmung mit der MAC-Adresse in der NDP-Tabelle basiert;
- Bereitstellung von mindestens zwei /60-Präfixen zusätzlich zum Standard-Präfix auf eine einfache DHCPv6-PD-Anfrage von einem anderen Router. Es wäre praktisch, wenn die Netzbetreiber auch die Möglichkeit hätten, statische Routen auf mindestens einem dokumentierten IPv4-RFC1918-Block auf ihrer Seite zu implementieren;
- IPv6-Renumbering-Management zur Vermeidung von Blackouts, typischerweise durch Anpassung der RA-Timer;
- Klare Informationen in der Modemschnittstelle über den IPv4- und IPv6-Zugangsmodus sowie den gemappten Portbereich im Falle eines IPv4-A+P-Sharing-Ansatzes (4rd, MAP-x, etc.);
- Die Option, einen Router eines Drittanbieters zu verwenden, wenn die IPv4-A+P-Sharing-Mechanismen den Router des Providers noch exklusiver machen.

Bei der mobilen Konnektivität wäre es wichtig, PCP v2 auf den Endpunkten zu unterstützen, insbesondere bei der gemeinsamen Nutzung von APN. Dies würde es den Kunden ermöglichen, bei der Nutzung von Hotspots die Vorteile von IPv6 durchgängig zu nutzen. Die Unterstützung von DHCP-PD wäre auch sehr praktisch für spezielle Fälle der gemeinsamen Nutzung mehrerer Netze mit mehreren /64.

Appendix B: Über dieses Dokument

Dieses Dokument wurde im Rahmen der ARCEP IPv6-Arbeitsgruppe verfasst, deren Hauptautor Jean-Charles BISECCO allen Mitgliedern für ihre Beiträge und Korrekturen danken möchte. Die ASCIIDOC-Version wird von Axel Schemberg bei [Github](#) bereitgestellt.

IHRE HILFE IST WILLKOMMEN

Diese Anleitung soll im Laufe der Zeit aktualisiert werden, Ihr Feedback ist uns wichtig.

Sie können uns Ihre Ideen zur Verbesserung sowie Ihr Feedback übermitteln:

- Stellen Sie Fragen oder diskutieren Sie auf Github: <https://github.com/optimismus/HowToDeployIPv6/discussions>
- Erstellen Sie ein Issue auf Github <https://github.com/optimismus/HowToDeployIPv6/issues>
- Treten Sie [IPv6 task-force](#) bei
- Kontaktieren Sie den Autor unter IPv6@arcep.fr / IPv6@jclb.net

Die neueste Version ist unter folgender Adresse zu finden:

<https://en.arcep.fr/publications/task-force-ipv6.html>

LIZENZ

Dieses Dokument wird unter der folgenden Lizenz veröffentlicht:

IPv6 Transition Guide © 2022 von Jean-Charles BISECCO ist lizenziert unter



[CC BY-SA 4.0](#) Attribution-ShareAlike 4.0 International

<https://creativecommons.org/licenses/by-sa/4.0/>

Symbole stammen von <https://github.com/ecceman/affinity>

Die Kapitelbilder stammen von unplash.com

Valentin Betancur / Alex Padurariu / Andre Taissin / Erol Ahmed / Possessed Photography / Austris Augsts

ÜBERSETZUNGEN

Dieses Dokument wurde zunächst auf Französisch und Englisch veröffentlicht. Wir sind offen für Übersetzungen in andere Sprachen, um die Einführung von IPv6 an so vielen Orten wie möglich zu erleichtern.

Die Übersetzungen können dem offiziellen Verzeichnis hinzugefügt werden.

Die Übersetzer erhalten Zugang zu den Deltas zwischen dieser Version und zukünftigen Versionen.



IPv6 Task -force