IPv6 an der RWTH Aachen

Protokollüberblick, Status Quo und nächste Schritte

Christoph Viethen
Abt. Netze, IT Center

viethen@itc.rwth-aachen.de

IT Center | RWTH AACHEN UNIVERSITY

IPv6 – was war das noch gleich?

IPv6 – was war das noch gleich? (1)

Fast Facts

- Das *Internet Protocol* in aktueller Version (Nachfolger von IPv4)
- Ursprung in den frühen 1990er Jahren (IPv4: Ende 1970er)
- Viele damals innovative Features wie Multicasting, IPsec, Mobilitäts-Unterstützung, Methoden zur Autokonfiguration von Hosts … (aber wenig Interesse an konsequenter weltweiter Einführung)
- Auffälligstes Merkmal (aus Nutzersicht): l ä n g e r e IP-Adressen (128 bit vs. 32 bit) → viel größerer Adressraum
- Heute: Einführung als nötig erkannt, getrieben von IPv4-Adressknappheit

IPv6 – was war das noch gleich? (2)

Adressen und deren Schreibweisen

- Voll ausgeschrieben (8 x 2 Bytes hex. = 16 Bytes = 128 bits)

```
2A00:8A60:0D0C:1234:83BC:C144:BB37:6221
2A00:8A60:0000:0004:0000:0000:0000:0001
```

- Abkürzungsregeln (stets optional)
  - Beliebig viele (oder wenige) führende (!) Nullen jeder Gruppe weglassen:

```
2A00:8A60:00: 004:    0:0:0:  1
2A00:8A60: 0:0004:0000:0:0:001
```

(ohne Leerzeichen – stehen hier nur zur Verdeutlichung)

  - Aufeinanderfolgende(*) Blöcke vom Wert 0 an höchstens einer Position komprimieren:

```
2A00:8A60:0:4::1
2A00:8A60::4:0:0:0:1
```

← (*) es genügt auch ein einziger

IPv6 – was war das noch gleich? (3)

Adressen und deren Schreibweisen

Keine Angst. :-) IPv6-fähige Software hat die „Abkürzungslogik“ schon eingebaut (bzw. nutzt die entsprechenden APIs des Betriebssystems) – man wird Sie schon verstehen …

```
$ ping6 2A00:8A60:0000:0004:0000:0000:0000:0001
PING 2A00:8A60:0000:0004:0000:0000:0000:0001(2a00:8a60:0:4::1) 56
data bytes
64 bytes from 2a00:8a60:0:4::1: icmp_seq=1 ttl=62 time=0.317 ms
^C

$ ping6 2A00:8A60:00:004:0:000::1
PING 2A00:8A60:00:004:0:000::1(2a00:8a60:0:4::1) 56 data bytes
64 bytes from 2a00:8a60:0:4::1: icmp_seq=1 ttl=62 time=0.324 ms
^C
```

… und Groß-/Kleinschreibung ist bei IPv6-Adressen auch nicht relevant.

IPv6 – was war das noch gleich? (4)

Adressen und deren Schreibweisen

Adresstypen für unterschiedliche Verwendungszwecke und mit unterschiedlicher „Reichweite“ ihrer Gültigkeit (*scope*)

- Link-local: `FE80::/10` → wichtig für’s „Neighbor Discovery Protocol“
- Global unicast: `2000::/3` (heute) → „normale“, weltweit sichtbare IPv6-Adressen
- Multicast: `FF00::/8` → Multicast-Gruppen-Adressen
- Unique local: `FD00::/8` → RFC 1918 in modern …

→ Ein IPv6-Host wird ganz typischerweise *mehrere* IPv6-Adressen haben.

Die gute Nachricht …

… oder: „Warum Sie IPv6 lieben werden“

Die gute Nachricht … (1)

IPv6 ersetzt „nur“ das *Netzwerk*-Protokoll (Layer 3 nach OSI)

Protokolle höherer Schichten (TCP, UDP, HTTP, FTP, DNS …) weitestgehend unverändert:

- Grundlegende Funktionalität / -logik wie bisher
- Anpassungen / Ergänzungen nur dort, wo IPv6-Adressen „wörtlich“ verwendet werden sollen; Beispiele:

  URIs („host subcomponent“)

  ```
  http://[2a00:8a60:d0c:0815::42]:8080/
  ```

  DNS-Einträge („resource records“)

  ```
  halo.rz.rwth-aachen.de.    IN    A       134.130.3.110
                             IN    AAAA    2a00:8a60:0:1000::3:110
  ```

- Routing im Netz funktioniert praktisch genauso wie bisher (entweder statische Routen oder IGPs/EGPs wie OSPF oder BGP usw.), mit Anpassungen für die größere Adresslänge

Die gute Nachricht … (2)

Softwarehersteller hatten Zeit …

- Solider Support in den Netzwerk-Stacks gängiger Desktop- und Server-Betriebssysteme oft schon seit mehreren Produktgenerationen vorhanden
- Mobil-Betriebssysteme holen in letzter Zeit stark auf
  - aktuelle Versionen mit recht brauchbarer IPv6-Unterstützung (von Mobilfunk-Netzbetreibern gefordert)
  - Problem installierter Gerätebasis mit alten Versionen ohne Update-Möglichkeit
- APIs (mit IPv6-Fähigkeiten) zum Teil schon seit > 10 Jahren in Betriebssystemen vorhanden, daher *sollte* Applikationssoftware heutzutage IPv6-Support haben (typischerweise solider Support bei Webbrowsern, E-Mail-Programmen usw.)

→ Fragen Sie Ihren Softwareanbieter! Und sagen Sie ihm, dass IPv6 ja inzwischen immerhin volljährig ist … :-)

Die „nicht so gute“ Nachricht …

… oder: „Ohne Fleiß kein Preis.“

Die „nicht so gute“ Nachricht … (1)

IPv6-Hosts können nicht *direkt* mit IPv4-Hosts kommunizieren

- Insbesondere wegen unterschiedlicher Adresslänge keine unmittelbare *same-layer interaction* möglich

- Heute typisches Deployment-Szenario: Hosts mit IPv4 + IPv6 (**Dual Stack**)
  → Behebt nicht (zeitnah) das Problem der Adressknappheit im IPv4-Bereich!
  → Konnektivität des IPv4-Stacks unabhängig von der des IPv6-Stacks (spannendes Debugging bei Problemen)
  → Software auf Endhosts komplexer als in reinen IPv4- oder IPv6-Umgebungen (z.B. *Happy Eyeballs*: Algorithmisches Ausprobieren, ob ein Ziel auf dem IPv4- oder dem IPv6-Weg besser erreichbar ist)

- Zukünftige „saubere“ Lösung: **IPv6 only**
  → IPv4-Inseln werden aus der IPv6-Welt nur noch über „Adapter“ erreicht (heute favorisierter Ansatz: *stateful NAT64*)
  → *heutige* Situation: Protokoll-Adaption kostet Geld :-) und skaliert schlecht (wesentliche Ursache: IPv4 ist noch eine große(!) Insel)

Die „nicht so gute“ Nachricht … (2)

Autokonfiguration: Gut gemeint, aber eine Security-Herausforderung

- Adresse des Default-Gateways sowie die verwendbaren Netzwerk-Adressen werden automatisch aus „Router Advertisements“ (RAs) gelernt

- *Jeder* Hosts im lokalen Netz könnte solche RAs aussenden und so behaupten, der „echte“ Router zu sein und so den Datenverkehr zu sich umleiten
  → Absichtliches oder auch unabsichtliches Fehlverhalten des Netzwerkstacks auf Endhosts kann erhebliche Probleme anrichten

- Bisherige Manipulationsmaßnahmen im lokalen Netz (z.B. *ARP spoofing*) funktionieren auf Basis des Nachfolgeprotokolls NDP prinzipiell genauso gut

- Neuartige Manipulations-/Angriffs-Szenarien aufgrund des großen Adressraums

→ IPv6 ist ein optimistisches Protokoll (die 1990er lassen grüßen) :-)
→ Probleme heute am sinnvollsten durch Intelligenz im Switching-Bereich lösbar (Stichwort: First-Hop Security)

Die „nicht so gute“ Nachricht … (3)

IPv6 lässt einem die Wahl …

- (Unübersichtliche) Vielfalt an RFCs im IPv6-Umfeld
  - 20-jähriger, noch immer laufender „Ideenwettbewerb“ :-)
  - Viele verworfene / nie implementierte Konzepte
  - Sinnvolle Erweiterungen oder Korrekturen nicht immer leicht zu finden
  - Durchaus widersprüchliche Ansätze

→ Aussage „IPv6-fähig“ (z.B. bei Netzwerkequipment) oft von geringem Wert

→ „Richtiger“ Weg muss zum Teil durch lokale Festlegungen abgesteckt werden

- Mehrere Methoden zur Adress-Konfiguration der Endhosts (statisch, SLAAC, DHCPv6)

→ SLAAC (als „typischste“ IPv6-Methode) meist der beste Weg

SLAAC

StateLess Address AutoConfiguration

StateLess Address AutoConfiguration (SLAAC) (1)

Router-Konfiguration und -Verhalten

- Einem lokalen Netz (bei uns meist: einem VLAN) wird grundsätzlich ein IPv6-Adressblock mit 64 bit Präfixlänge (/64 – „ein Slash-64-Netz“) zugeordnet
- Beispielnetz:
  `2A00:8A60:0D0C:0110::/64` (1. Client-Netz, Inst. für Pseudoadressierung)
- Router erhält z.B. die Adresse `2A00:8A60:0D0C:0110::1`
- Router sendet fortan regelmäßig automatisch und auch fallweise (auf Anfrage von Clients, die konfiguriert werden möchten) *Router Advertisements* (RAs) in das lokale Netz aus (als Multicast)
- RAs sind Teil des „Neighbor Discovery Protocols“ (NDP) und basieren auf ICMPv6-Nachrichten

StateLess Address AutoConfiguration (SLAAC) (2)

```
Internet Control Message Protocol v6
    Type: Router Advertisement (134)
    Flags: 0x48
        0... .... = Managed address configuration: Not set
        .1.. .... = Other configuration: Set
        ..0. .... = Home Agent: Not set
        ...0 1... = Prf (Default Router Preference): High (1)
        .... .0.. = Proxy: Not set
        .... ..0. = Reserved: 0
    Router lifetime (s): 1800
    ICMPv6 Option (Prefix information : 2a00:8a60:d0c:110::/64)
        Type: Prefix information (3)
        Length: 4 (32 bytes)
        Prefix Length: 64
        Flag: 0xc0
            1... .... = On-link flag(L): Set
            .1.. .... = Autonomous address-configuration flag(A): Set
            ..0. .... = Router address flag(R): Not set
            ...0 0000 = Reserved: 0
        Valid Lifetime: 2592000
        Preferred Lifetime: 604800
        Prefix: 2a00:8a60:d0c:110::
```

StateLess Address AutoConfiguration (SLAAC) (3)

Verhalten des (ansonsten unkonfigurierten) Hosts:

Auswertung der RA-Nachrichten des Routers

- A-Flag gesetzt? (→ Adresskonfiguration aufgrund des RA erlaubt)
- Default-Router-Adresse (geht aus dem IPv6-Header hervor)
- Präfix und seine Länge (64 bit bei SLAAC) ← linke Hälfte der IPv6-Adresse
- Ermittlung des „host part“ ← rechte Hälfte der IPv6-Adresse
  - EUI-64: „FFFE“ in die Mitte der MAC-Adresse des Ethernet-Adapters einfügen (und anschließend noch das 7. bit invertieren …)
  - *Privacy Extensions* nach RFC 4941: randomisierten 64-bit-Wert verwenden

→ Host hat nun alle nötigen Angaben, um mit dem Netz zu kommunizieren

(Adressen der DNS-Server werden in einem 2. Schritt automatisch ermittelt)

StateLess Address AutoConfiguration (SLAAC) (4)

Wir mögen SLAAC, denn …

- Ideal geeignet für Client-Hosts, deren Hauptzweck Bereitstellung von Konnektivität von Nutzern zum Datennetz / zum Internet ist
  - Größter Teil der Geräte im RWTH-Datennetz fällt in diese Kategorie
  - SLAAC-Funktionalität grob vergleichbar mit Konfiguration aus DHCPv4-Adresspools
- In den meisten Konstellationen auch gut geeignet für Server (EUI-64-Adresse)
  - Server werden typischerweise über den DNS-Hostnamen gefunden – IPv6-Adresse muss nicht „schön“ sein
- Funktioniert hier und heute (Windows, Linux, Apple OS X & iOS, Android …)
  - als Alternative gedachtes DHCPv6 „not quite ready“ für zentral administrierbaren Dienst, aufgrund „DHCP Unique Identifier“ / fragen Sie uns in 2 Jahren nochmal (Stichwort: RFC 6939) :-)

→ Was auch immer Sie von SLAAC halten:
Bitte vermeiden Sie es, IPv6-Adressen händisch zu konfigurieren!

IPv6 an der RWTH

Erreichtes (und Baustellen)

IPv6 an der RWTH – Erreichtes (und Baustellen) (1)

Grüne Ampeln …

- DFN-Anschluss: IPv6 in Betrieb
- Core-Bereiche des Datennetzes: IPv6 in Betrieb
- Zentrale Firewall: IPv6 in Betrieb
- RIPE-Mitgliedschaft und Auswirkungen: ja / alles im Griff ;)
  - Eigenes AS; Umstellung Peerings
  - „PA“-Adressraum (Größe: /32) für RWTH
  - Routing-Umstellung DFN
  - Div. Umstellungen intern auf neuen Adressraum
  - Anpassung IPv6-Netzwerkdatenbank
  - Delegation der DNS-Reverse-Zone
- Adressplan IPv6 (Grobstruktur): vorhanden

IPv6 an der RWTH – Erreichtes (und Baustellen) (2)

Work in progress

- Schulung NOC-Mitarbeiter
  - Erfolgreiche Kooperation mit FZ Jülich
- ACLs
  - Technisch funktionsfähig, aber Management noch aufwendig (manuell)
- Sicherheitsfunktionen / Störungsdiagnosefähigkeit LANs
  - Tests nötig
  - Funktionsumfang abhängig von Aktualität des lokalen Netzequipments
- DNS-Infrastruktur
  - Umstellung auf zeitgemäße Datenbank-Basis
  - Code-Anpassung und Tests laufen
  - Beta-Status des Backends Q2/2016
- Tests mit Pilotnutzern
  - Erweiterung gewünscht → dazu später mehr
  - IPv6-Tests im Serverbereich (Webserver) wären interessant

IPv6 an der RWTH – Erreichtes (und Baustellen) (3)

Work in progress

- Schulung / Awareness Admins an der RWTH
  - IPv6 „zentral“ auszurollen, ist nicht alles
  - Der „Teufel“ steckt im Detail, und viele Herausforderungen liegen in der Administration der lokalen Netze

→ Deshalb sind wir heute hier!

Heutige Veranstaltung als Anknüpfungspunkt für weitere ähnliche Veranstaltungen, mit Fokussierung auf unterschiedliche Details.

Ideen für Themen:

- Debugging von IPv6-Netzen – wie findet und behebt man lokale Störungen?
- Gängige PC-Betriebssysteme in IPv6-Netzen – was kann / sollte man konfigurieren? Wie verhalten sich unterschiedliche OS-Versionen?

  usw.

Bitte senden Sie uns Ihr Feedback mit Ihren Wünschen!

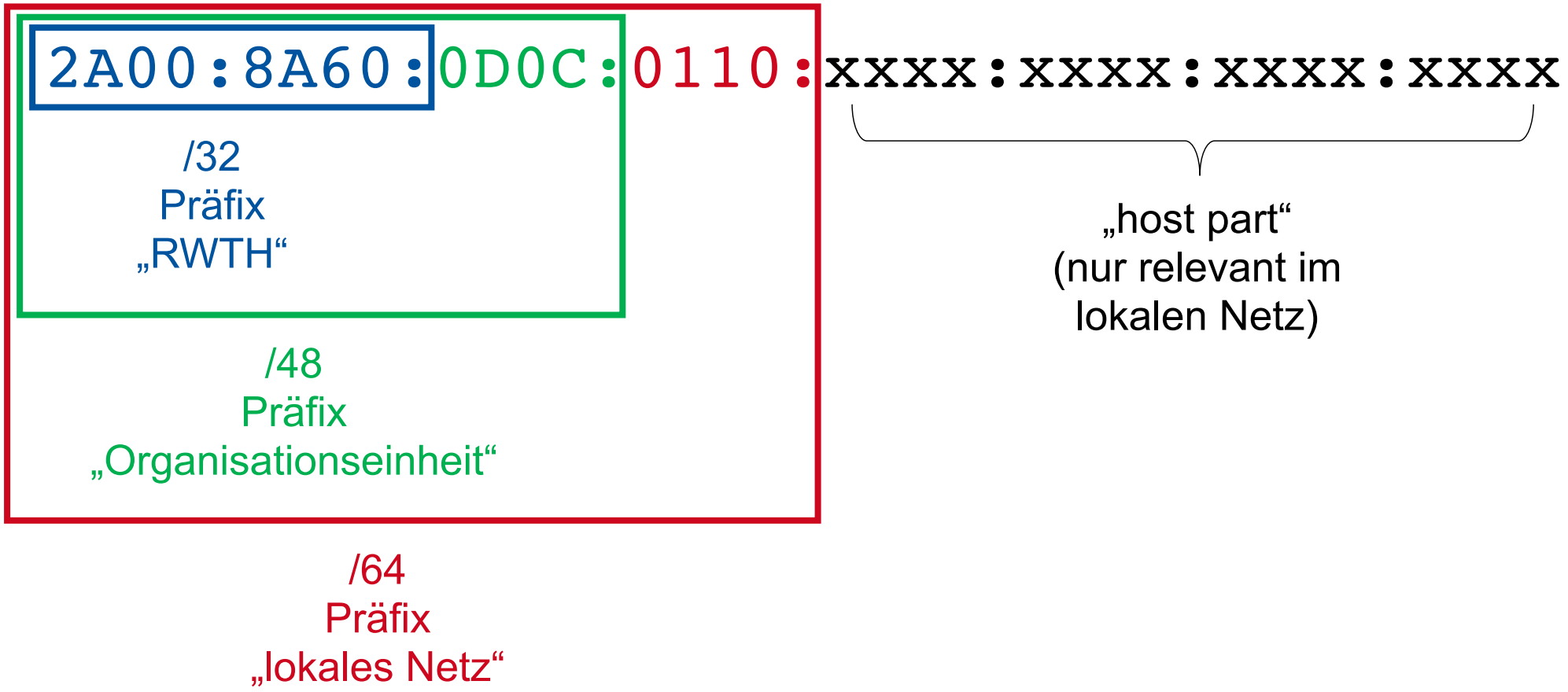
Vergabe von IPv6-Adressbereichen

an der RWTH Aachen

IT Center | RWTH AACHEN UNIVERSITY

Adressvergabe an der RWTH Aachen (1)

IPv6-Adresshierarchie



Adressvergabe an der RWTH Aachen (2)

Zweistufige Adressvergabe

1. Zuordnung von /48-Präfixen zu Organisationseinheiten
   - Aufgabe der RWTH als „Local Internet Registry“ im RIPE-Kontext
   - Durchgeführt durch das IT Center, Abteilung Netze
   - Zuordnung zu externen (Beispiel: Studentenwerk, UK Aachen) wie auch zu internen Organisationseinheiten (Fachgruppen, Institute, …)
   - Sparsame und technisch vernünftige Adressvergabe
   - Versuch, Adressen nach heutigem Ermessen „zukunftssicher“ zu vergeben
   - Maximal(*) ein /48-Präfix je Organisationseinheit

     ((*) eigentlich füllstandsabhängig – wenn ein bestimmter Prozentsatz erreicht ist, dürfen wir weitere Präfixe an die Organisationseinheit vergeben → heute nicht realistisch)

2. Vergabe (und Routing) von /64-Präfixen der einzelnen LANs
   - Tagesgeschäft der Abteilung Netze, IT Center (ähnlich wie bei IPv4)
   - Vergabe einer Teilmenge des der Organisationseinheit zugeordneten /48-Adressraums
   - Feinstrukturierung des IPv6-Adressbereichs an den lokalen Gegebenheiten orientiert
   - Kennzeichnung der vorgesehenen Nutzungsart des Netzes zur Erleichterung der Störungsdiagnose und Implementierung von Sicherheits-Policies

Adressvergabe an der RWTH Aachen (3)

Zuordnung von /48-Präfixen

Was ist eine Organisationseinheit?

- Erste Idee: Orientierung an Institutskennziffern (IKZ)
- Probleme
  - Organisationseinheiten mit mehreren IKZ (z.B. einmal als Lehrstuhl, einmal als Zentrale Einrichtung)
  - IKZ gibt es auf verschiedenen Hierarchieebenen (z.B. Fachgruppe, Institut, Lehrstuhl, Lehr- und Forschungsgebiet)
    - An welche Ebene vergibt man Netzbereiche?
    - Hat es Sinn, untergeordneten Einheiten separate /48-Bereiche zu vergeben, wenn schon eine übergeordnete Einheit solchen Adressraum hat, der mehr als groß genug für alle untergeordneten Einheiten wäre?
- Es gibt keine perfekte Lösung. Derzeit verfolgter Ansatz:
  - Auf Ebene der Fachgruppen (Beispiel: Informatik, Physik, Chemie) /48 zuordnen
  - Lässt sich darin der absehbare Adressbedarf unterbringen → gut so
  - Passt der absehbare Adressbedarf nicht hinein → auf nächsttieferer Hierarchieebene /48-Netze zuordnen
  - Hierarchie der vergebenen /48-Netze möglichst flach halten

Adressvergabe an der RWTH Aachen (4)

Annäherung an eine perfekte Lösung … :-)

- Struktur der RWTH Aachen ist zum Teil unübersichtlich und „gewachsen“
- IPv6-Adressvergabe soll sich an vernünftigerweise zu erwartendem Bedarf orientieren
- Wir möchten keine /48-Bereiche (bis zu 65536 lokale Netze (!)) unnötig vergeben
  - Möglichkeit von „address audits“ durch RIPE
  - Anderswo reicht ein /48 für eine komplette Uni …
  - Wir möchten niemandem Adressen, bei tatsächlichem Bedarf, vorenthalten müssen, nur weil an anderer Stelle verschwendet wurde
- IPv4-Zustände möchte man nie mehr haben …

→ Reden Sie mit uns! Wir schauen uns Ihre IPv4-Netze an, Sie sagen uns, was Sie künftig vorhaben, und so haben wir eine viel bessere Entscheidungsgrundlage.

Adressvergabe an der RWTH Aachen (5)

Wie geht's weiter? Wann geht's weiter?

- Grobstruktur des IPv6-Adressraums ist festgelegt
  - Erster „Buchstabe" nach dem /32-Präfix kennzeichnet u.a. den Fachbereich, z.B. soll `2A00:8A60:1000::/36` einmal Heimat sämtlicher Einrichtungen sein, die der Mathematisch-Naturwissenschaftlichen Fakultät zuzuordnen sind.

  - „Sonderbuchstaben" für Sonderfälle – Client-Rechner, die keiner Organisationseinheit fest zuzuordnen sind, zum Beispiel Nutzer von Eduroam, werden in `2A00:8A60:C000::/36` untergebracht; eindeutig als extern zu betrachtende Einrichtungen erhalten Netze aus `2A00:8A60:E000::/36`.

- /48-Bereiche stellen die „Mittelstruktur" dar
  - Zuordnung zu Org.einheiten erfolgt bei (gemeldetem) Bedarf an IPv6-Adressen
  - Planung im Idealfall im Zusammenspiel mit den jeweiligen Netzverantwortlichen
  - Beginn dieser Arbeiten: sofort
  - Nachricht an Servicedesk (Betreff: „Zuordnung eines /48-Adressbereichs")

Testvergabe von /64-Netzen

Testvergabe von /64-Netzen (1)

Testnutzer werden

Notwendige, nicht hinreichende Voraussetzungen dafür, IPv6-Netze der Größe /64 für‘s lokale Netz zu erhalten:

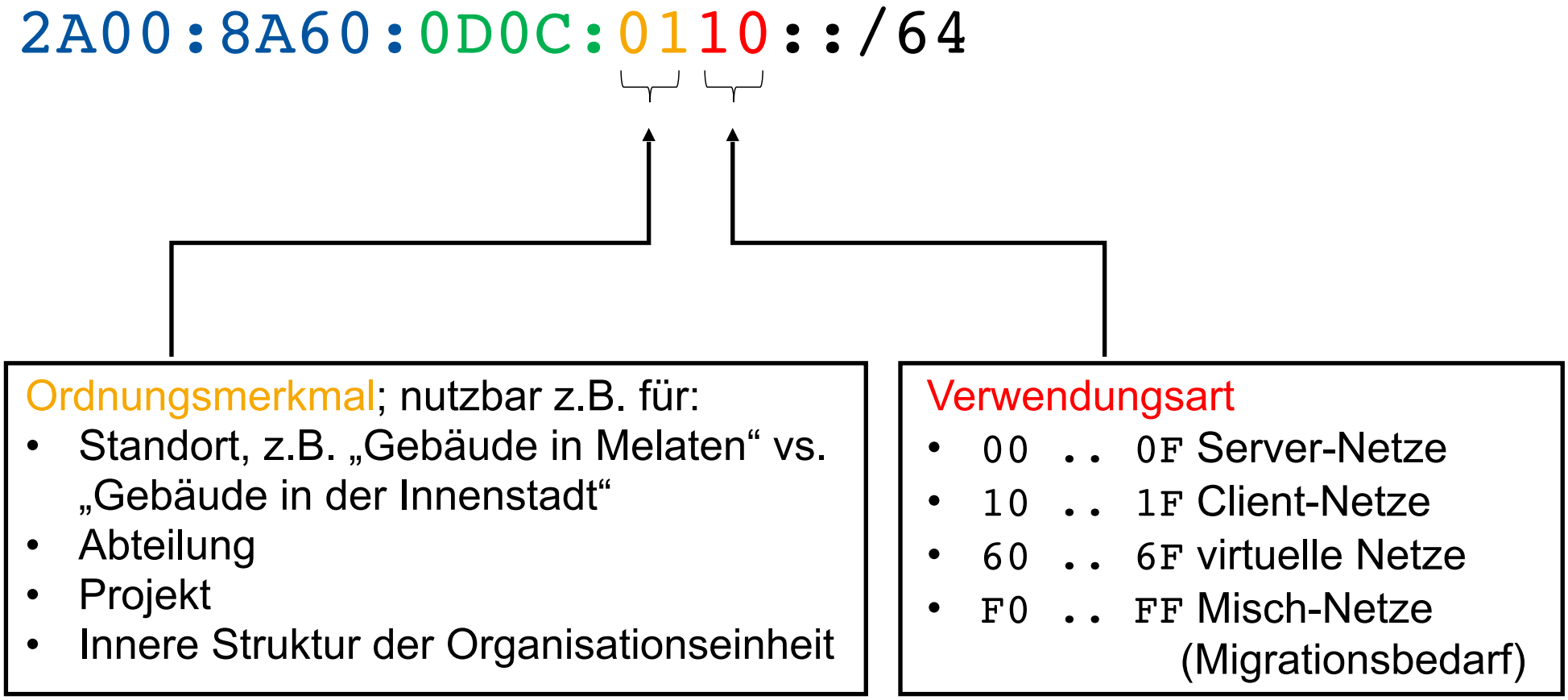
- Zuordnung eines /48-Bereichs ist erfolgt (s.o.)
- *Sämtliches* Netzwerkequipment zwischen unserem Netz-Core und Ihren End-Hosts ist neueren Datums (jünger als 5 Jahre), ist von uns gemanagt und unterstützt First-Hop-Security-Features
- Bewusstsein, dass es sich um Test-Deployments handelt, bei denen durchaus Dinge schiefgehen können (Verbindungsausfälle, verschwundene DNS-Einträge, verirrte Pakete, mehr „Zugang“ in Ihr Netz als erwartet)
- Nicht alle Funktionalität wird von Anfang an verfügbar sein – einiges wird mit Ihrer Hard- und Software vielleicht gar nicht möglich sein

→ Wir werden‘s nie erfahren, wenn wir es nicht ausprobieren! :-)

Die Auswahl der Testkandidaten bleibt uns vorbehalten.

Testvergabe von /64-Netzen (2)

Feinstruktur – wie /64-Netze numeriert werden



Zu guter Letzt …

Eduroam-IPv6-Test (1)

There's a new network in town …

… und es heißt „eduroam-IPv6-test".

- Clients befinden sich in reinem IPv6-Netz

- Benutzt ein NAT64-Gateway zum Übergang in die IPv4-Welt:
  - IPv4-Zieladressen A.B.C.D werden über ein angepasstes DNS („DNS64") in virtuelle IPv6-Adressen der Form 2A00:8A60:C000:EE64::A.B.C.D umgeschrieben
  - IPv6-Client „glaubt" also immer, dass er ein IPv6-Ziel kontaktiert – kein Dual Stack nötig
  - Beim Routing wird anhand einer IPv6-Zieladresse in der genannten Form erkannt, dass das Datenpaket eine NAT-Stufe passieren muss, um dann „hinter" dem NAT als IPv4-Paket weiterübertragen zu werden
  - Der Rückweg erfolgt analog

- **Traffic zu nativen IPv6-Zielen läuft am NAT vorbei und ist schneller / latenz-ärmer :-)))**

Eduroam-IPv6-Test (2)

Weitere Merkmale

- Nachteil: es ist ein NAT – z.B. ist Serverbetrieb in diesem Netz schwierig
- Gibt man als Ziel eine IPv4-Adresse an (und keinen Hostnamen, der im DNS steht), wird der Verbindungsaufbau scheitern (da kein DNS64 erfolgt)
- NAT64 benötigt zusätzlichen Router, was heutzutage (viel IPv4-Traffic) schlecht skaliert
  - Router: gemessen am Datendurchsatz viel teurer als L3-Switches
  - Größere Anzahl nötig, um RWTH-Netz flächendeckend mit NAT64 abzudecken

→ Dieses Problem wird über die Jahre immer kleiner werden
→ Potentiell attraktive Technik für spätere Phase der IPv4→IPv6-Migration

- Weitere Vorteile:
  - reines IPv6, ähnlich implementiert wie (bald) in Mobilfunk-Netzen
  - Testbed für mehrere bei uns neue Technologien: IPv6 im WLAN, NAT64, DNS64
  - Implementiert als Zusammenspiel verschiedener Produkte (BIND9.8, WLCs mit neuem IPv6-tauglichem OS, leistungsfähiger Router) – viele neue Erfahrungen gewonnen

Eduroam-IPv6-Test (3)

Wir sind an Erfahrungsberichten interessiert:

- Läuft es mit Ihrem Mobil-Betriebssystem? Falls nicht, was sind die Symptome?
- Haben Sie Applikationen gefunden, die nicht funktionieren?
- Wie ist die Betriebsstabilität? Genauso wie das „normale“ Eduroam, oder gibt es unerklärliche „Aussetzer“ des neueren Netzes?
- Wie ist die Geschwindigkeit? Merken Sie einen Unterschied beim Ansteuern nativer IPv6-Ziele (Heise, Facebook, Google) und solcher, bei denen das NAT64 durchlaufen werden muss (z.B. Tagesschau, Spiegel)?

Wir hoffen, unser Testnetz für „IPv6 zum Anfassen“ gefällt Ihnen. :-)

Fragen?

Vielen Dank
für Ihre Aufmerksamkeit

Dipl.-Inform. Christoph Viethen

IT Center der RWTH Aachen
Abteilung Netze
Wendlingweg 10
52074 Aachen