ICMPv6 sinnvoll filtern

Benedikt Stockebrand
Stepladder IT Training+Consulting GmbH

Heise/DE-CIX IPv6-Kongress
23. Mai 2014

Ich über mich

- Diplom-Informatiker (Uni Dortmund)
- Internet seit ca. 1993
- Schwerpunkte IT-Betrieb, TCP/IP-Netze, Unix
- Selbständiger Berater und Trainer
- Seit Mitte 2003 Schwerpunkt IPv6
- Autor des Buchs "IPv6 in Practice—A Unixer's Guide to the Next Generation Internet" (Springer 2007)
- 2010 zusammen mit Hans Peter Dittler Erstellung eines IPv6-Leitfadens für das BSI (Bundesamt für Sicherheit in der Informationstechnik)
- 2012 Gründung der "Stepladder IT Training+Consulting GmbH"
- Seit 2013 Betreiber des "BIVBlog" (http://www.stepladder-it.com/bivblog)

ICMP ist Böse. . .

ICMP ist Böse. . .

. . . und ICMPv6 ist sechsmal so Böse

ICMP ist Böse. . .

. . . und ICMPv6 ist sechsmal so Böse

. . . und muss erst recht komplett weggefiltert werden

ICMP ist Böse. . .

. . . und ICMPv6 ist sechsmal so Böse

. . . und muss erst recht komplett weggefiltert werden

. . . und wenn das nicht geht, kann man IPv6 nicht benutzen

ICMP ist Böse. . .

. . . und ICMPv6 ist sechsmal so Böse

. . . und muss erst recht komplett weggefiltert werden

. . . und wenn das nicht geht, kann man IPv6 nicht benutzen

. . . auch wenn man inzwischen wenigstens NAT dafür kaufen kann

ICMP ist Böse. . .

. . . und ICMPv6 ist sechsmal so Böse

. . . und muss erst recht komplett weggefiltert werden

. . . und wenn das nicht geht, kann man IPv6 nicht benutzen

. . . auch wenn man inzwischen wenigstens NAT dafür kaufen kann

. . . und überhaupt war mit BTX alles viel besser.

Sinn und Unsinn von Filtern

Sinn und Unsinn von Filtern

- Jeder Filter ist eine potenzielle Fehlerquelle

Sinn und Unsinn von Filtern

- Jeder Filter ist eine potenzielle Fehlerquelle
- Aber Schutz in der Tiefe ist oft unsere einzige Option

Was kann mein aktueller Filter?

Verbreitete Einschränkungen aktueller Filter:

- Zuordnung von ICMPv6-Paketen zu existierenden Verbindungen
- Zuordnung von ICMPv6-Paketen bei Multicast
- Einschränkungen bei IPv6 Header Extensions/Options
- Einschränkungen bei Tunneln

Informationsbeschaffung

Informationsbeschaffung

- Welche ICMPv6-Typen und -Codes gibt es?

Informationsbeschaffung

- Welche ICMPv6-Typen und -Codes gibt es?
  $\Longrightarrow$ `http://en.wikipedia.org/wiki/ICMPv6`

Informationsbeschaffung

- Welche ICMPv6-Typen und -Codes gibt es?
  $\Longrightarrow$ `http://en.wikipedia.org/wiki/ICMPv6`
  $\Longrightarrow$ `http://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xhtml`

Suchergebnisse. . .

0	Reserved	—
1	Destination Unreachable	[RFC4443]
2	Packet Too Big	[RFC4443]
3	Time Exceeded	[RFC4443]
4	Parameter Problem	[RFC4443]
100	Private experimentation	[RFC4443]
101	Private experimentation	[RFC4443]
102–126	Unassigned	—
127	Reserved for expansion of ICMPv6 error msgs.	[RFC4443]
128	Echo Request	[RFC4443]
129	Echo Reply	[RFC4443]
130	Multicast Listener Query	[RFC2710]
131	Multicast Listener Report	[RFC2710]
132	Multicast Listener Done	[RFC2710]
133	Router Solicitation	[RFC4861]
134	Router Advertisement	[RFC4861]

. . . und mehr Suchergebnisse. . .

135	Neighbor Solicitation	[RFC4861]
136	Neighbor Advertisement	[RFC4861]
137	Redirect Message	[RFC4861]
138	Router Renumbering	[Crawford]
139	ICMP Node Information Query	[RFC4620]
140	ICMP Node Information Response	[RFC4620]
141	Inverse Neighbor Discovery Solicitation Message	[RFC3122]
142	Inverse Neighbor Discovery Advertisement Message	[RFC3122]
143	Version 2 Multicast Listener Report	[RFC3810]
144	Home Agent Address Discovery Request Message	[RFC6275]
145	Home Agent Address Discovery Reply Message	[RFC6275]
146	Mobile Prefix Solicitation	[RFC6275]
147	Mobile Prefix Advertisement	[RFC6275]
148	Certification Path Solicitation Message	[RFC3971]
149	Certification Path Advertisement Message	[RFC3971]

. . . und noch mehr Suchergebnisse

150	ICMP messages utilized by experimental mobility protocols such as Seamoby	[RFC4065]
151	Multicast Router Advertisement	[RFC4286]
152	Multicast Router Solicitation	[RFC4286]
153	Multicast Router Termination	[RFC4286]
154	FMIPv6 Messages	[RFC5568]
155	RPL Control Message	[RFC6550]
156	ILNPv6 Locator Update Message	[RFC6743]
157	Duplicate Address Request	[RFC6775]
158	Duplicate Address Confirmation	[RFC6775]
159-199	Unassigned	—
200	Private experimentation	[RFC4443]
201	Private experimentation	[RFC4443]
255	Reserved for expansion of ICMPv6 informational messages	[RFC4443]

Und jetzt?

Und jetzt?

1. Blacklisting oder Whitelisting?

Und jetzt?

1. Blacklisting oder Whitelisting?
2. Schonmal großzügig aussortieren

Und jetzt?

1. Blacklisting oder Whitelisting?
2. Schonmal großzügig aussortieren
3. Nach Funktion/Aufgabe umsortieren

Und jetzt?

1. Blacklisting oder Whitelisting?
2. Schonmal großzügig aussortieren
3. Nach Funktion/Aufgabe umsortieren
4. . . . und dabei gleich zusammenfassen

Profilbildung

Bezeichnung:	
Types(Codes):	
Von:	**Nach:**
Forwarding? ja/nein	**Hop Limit=255?** ja/nein
Stateful? nein/neu/existierend	
Benötigt wofür?	

MLD (1)

Bezeichnung: Multicast Listener Query	
Types(Codes): 130(0)	
Von: LL Unicast	**Nach:** `ff02::1`, Unicast
Forwarding? nein	**Hop Limit=255?** nein (=1)
Stateful? nein	
Benötigt wofür? Hat eine Router Alert Option; muss durchgelassen werden, wenn MLD-fähige Switches oder Multicast Routing benutzt werden.	

MLD (2)

Bezeichnung: Version 2 Multicast Listener Report	
Types(Codes): 143(0)	
Von: LL Unicast, `::`	**Nach:** `ff02::16`
Forwarding? nein	**Hop Limit=255?** nein (=1)
Stateful? nein	
Benötigt wofür? Hat eine Router Alert Option; muss durchgelassen werden, wenn MLD-fähige Switches oder Multicast Routing benutzt werden.	

MLD (3)

Bezeichnung: Version 1 Multicast Listener Report	
Types(Codes): 131(0)	
Von: LL Unicast	**Nach:** `Gewünschte MC-Adresse`
Forwarding? nein	**Hop Limit=255?** nein (=1)
Stateful? nein	
Benötigt wofür? Hat eine Router Alert Option; muss durchgelassen werden, wenn MLD-fähige Switches oder Multicast Routing benutzt werden.	

MLD (4)

Bezeichnung: Version 1 Multicast Listener Done	
Types(Codes): 132(0)	
Von: LL Unicast	**Nach:** `ff02::2`
Forwarding? nein	**Hop Limit=255?** nein (=1)
Stateful? theoretisch ja	
Benötigt wofür? Hat eine Router Alert Option; muss durchgelassen werden, wenn MLD-fähige Switches oder Multicast Routing benutzt werden.	

Packet Too Big

Bezeichnung: Packet Too Big	
Types(Codes): 2(0)	
Von: Alle Unicast	**Nach:** Alle Unicast
Forwarding? ja	**Hop Limit=255?** nein
Stateful? ja	
Benötigt wofür? Können theoretisch weggefiltert werden, wenn absolut sichergestellt ist, dass keine Fragmentierung benötigt wird; treten dann doch Fragmente auf, wird die Fehlersuche schnell extrem schwierig.	

ICMPv6 Redirect

Bezeichnung: ICMPv6 Redirect	
Types(Codes): 137(0)	
Von: LL Unicast von Router	**Nach:** LL Unicast an Host
Forwarding? nein	**Hop Limit=255?** ja
Stateful? existierend(???)	
Benötigt wofür? Tritt in darauf zugeschnittenen Netztopologien nicht auf.	

Destination Unreachable

Bezeichnung: Destination Unreachable	
Types(Codes): 1(0–7)	
Von: Alle Unicast	**Nach:** Alle Unicast
Forwarding? ja	**Hop Limit=255?** nein
Stateful? ja	
Benötigt wofür? Treten faktisch überall auf. Können theoretisch gefiltert werden, führen dann aber zu extrem langen Timeouts (bis zu 3 Minuten pro Adresse). Evtl. kann auch noch nach ICMPv6 Codes weiter gefiltert werden.	

Time Exceeded (1)

<table>
<tr><td colspan="2">Bezeichnung: Time Exceeded/Hop Limit Exceeded in Transit</td></tr>
<tr><td colspan="2">Types(Codes): 3(0)</td></tr>
<tr><td>Von:
Alle Unicast</td><td>Nach:
Alle Unicast</td></tr>
<tr><td>Forwarding? ja</td><td>Hop Limit=255? nein</td></tr>
<tr><td colspan="2">Stateful? ja</td></tr>
<tr><td colspan="2">Benötigt wofür?
Können theoretisch weggefiltert werden, wenn nirgends dynamische Routing-Protokolle eingesetzt werden und alle Routing-Tabellen garantiert fehlerfrei sind; erleichtern ansonsten aber erheblich die Fehlersuche.</td></tr>
</table>

Time Exceeded (2)

Bezeichnung: Time Exceeded/Fragment Reassembly Time Exceeded	
Types(Codes): 3(1)	
Von: Alle Unicast	**Nach:** Alle Unicast
Forwarding? ja	**Hop Limit=255?** nein
Stateful? ja	
Benötigt wofür? Analog zu “Packet Too Big”.	

Parameter Problem

Bezeichnung: Parameter Problem	
Types(Codes): 4(0–3)	
Von: Alle Unicast	**Nach:** Alle Unicast
Forwarding? ja	**Hop Limit=255?** nein
Stateful? ja	
Benötigt wofür? Deuten auf schwerwiegende Probleme oder Inkompatibilitäten hin; essentiell zur Fehlersuche, sollten aber nur in Ausnahmefällen auftreten.	

Neighbor Discovery (1)

<table>
<tr><td colspan="2">Bezeichnung: Neighbor Solicitation</td></tr>
<tr><td colspan="2">Types(Codes): 135(0)</td></tr>
<tr><td>Von:
LL Unicast,
:: (für DAD)</td><td>Nach:
Unicast,
ff02::1:ffxx:xxxx</td></tr>
<tr><td>Forwarding? nein</td><td>Hop Limit=255? ja</td></tr>
<tr><td colspan="2">Stateful? nein</td></tr>
<tr><td colspan="2">Benötigt wofür?
Muss durchgelassen werden für DAD und Neighbor Discovery; alternativ können in Extremfällen die Neighbor Caches statisch befüllt werden.</td></tr>
</table>

Neighbor Discovery (2)

<table>
<tr><td colspan="2">Bezeichnung: Neighbor Advertisement</td></tr>
<tr><td colspan="2">Types(Codes): 135(0)</td></tr>
<tr><td>Von:
LL Unicast</td><td>Nach:
Unicast, <code>ff02::1</code> (für DAD)</td></tr>
<tr><td>Forwarding? nein</td><td>Hop Limit=255? ja</td></tr>
<tr><td colspan="2">Stateful? ja</td></tr>
<tr><td colspan="2">Benötigt wofür?
Muss durchgelassen werden für DAD und Neighbor Discovery; alternativ können in Extremfällen die Neighbor Caches statisch befüllt werden.</td></tr>
</table>

Autoconfiguration (1)

Bezeichnung: Router Solicitation	
Types(Codes): 133(0)	
Von: LL Unicast	**Nach:** `ff02::2` LL Unicast (in Ausnahmefällen)
Forwarding? nein	**Hop Limit=255?** ja
Stateful? neu	
Benötigt wofür? Wird nur in Verbindung mit Autoconfiguration benötigt.	

Autoconfiguration (2)

Bezeichnung: Router Advertisement	
Types(Codes): 133(0)	
Von: LL Unicast von Router	**Nach:** `ff02::1` LL Unicast (in Ausnahmefällen)
Forwarding? nein	**Hop Limit=255?** ja
Stateful? existierend	
Benötigt wofür? Wird nur in Verbindung mit Autoconfiguration benötigt.	

Echo Request

Bezeichnung: Echo Request	
Types(Codes): 128(0)	
Von: Alle Unicast	**Nach:** Alle Unicast, alle Multicast
Forwarding? ja	**Hop Limit=255?** nein
Stateful? neu	
Benötigt wofür? Zu Diagnose- und Monitoringzwecken hilfreich, kann aber prinzipiell gefiltert werden. Insbesondere Pings an Multicast-Adressen können in manchen Fällen problematisch sein.	

Echo Reply

Bezeichnung: Echo Reply	
Types(Codes): 129(0)	
Von: Alle Unicast	**Nach:** Alle Unicast
Forwarding? ja	**Hop Limit=255?** nein
Stateful? existierend	
Benötigt wofür? Zu Diagnose- und Monitoringzwecken hilfreich, kann aber prinzipiell gefiltert werden. Insbesondere Pings an Multicast-Adressen können in manchen Fällen problematisch beim Connection Tracking sein.	

Fazit

- Manche ICMPv6-Pakete müssen wir durchlassen.
- Der Link-Local Scope und der Hop Limit=255 Trick verhindern auch ohne Paketfilter viel Probleme.
- Connection Tracking hat in existierenden Implementierungen seine Grenzen.
- Multicast bringt einige zusätzliche Überraschungen mit.

Teil I

Anhang

Ressourcen

Protokoll-Interna und Administration

Silvia Hagen
IPv6 – Grundlagen – Funktionalität – Integration
2. Auflage
Sunny Edition, Dezember 2009
ISBN 978-3-9522942-2-2

IPv6 Essentials (2nd edition)
O'Reilly, 2006
ISBN 0-596-10058-2
Vertiefende Beschreibungen der Protokolle

Benedikt Stockebrand
IPv6 in Practice—A Unixer's Guide to the Next Generation Internet
Springer, 2006
ISBN 3-540-24524-3
Einrichtung in Unix (einschliesslich der ekligeren Aspekte)

Ressourcen: Web-Ressourcen

Internet Assigned Numbers Authority (IANA)
`http://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xhtml`
Die offiziell vergebenen ICMPv6 Types und Codes

Internet Engineering Task Force (IETF)
Requests for Comments (RFCs)
`http://www.ietf.org`
Die offiziellen Spezifikationen

BIVBlog: Benedikt's IT Video Blog
`http://www.stepladder-it.com/bivblog/`
Video-Blogs rund um IT im allgemeinen und IPv6 im speziellen

Contact Information

Stepladder IT
Training+Consulting GmbH
Benedikt Stockebrand

Fichardstr. 38
D-60322 Frankfurt/Main

contact@stepladder-it.com

Webseiten:
http://www.stepladder-it.com/
http://www.benedikt-stockebrand.de/

Video Blog:
http://www.stepladder-it.com/bivblog/