IPv6 -
Hohe Braukunst oder laue Pfütze?

Beer-Talk 7. Juni 2012

Rainer Giedat – IT-Security Analyst

Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Warum eigentlich?

Weil dem Internet die Adressen ausgehen!! (Panik!)

IPv4:

Warum eigentlich?

Weil dem Internet die Adressen ausgehen!! (Panik!)

IPv4:

IPv6:

IPv6 – Andere Gründe

- Eingebaute Security:

  → IPSec für alle?

- Sicherheit wider willen:

  → Adressraum zu gross zum Scannen?

- Endlich kein NAT mehr

- Mobile IPv6

Adressraum zu gross?

128 Bit statt 32:

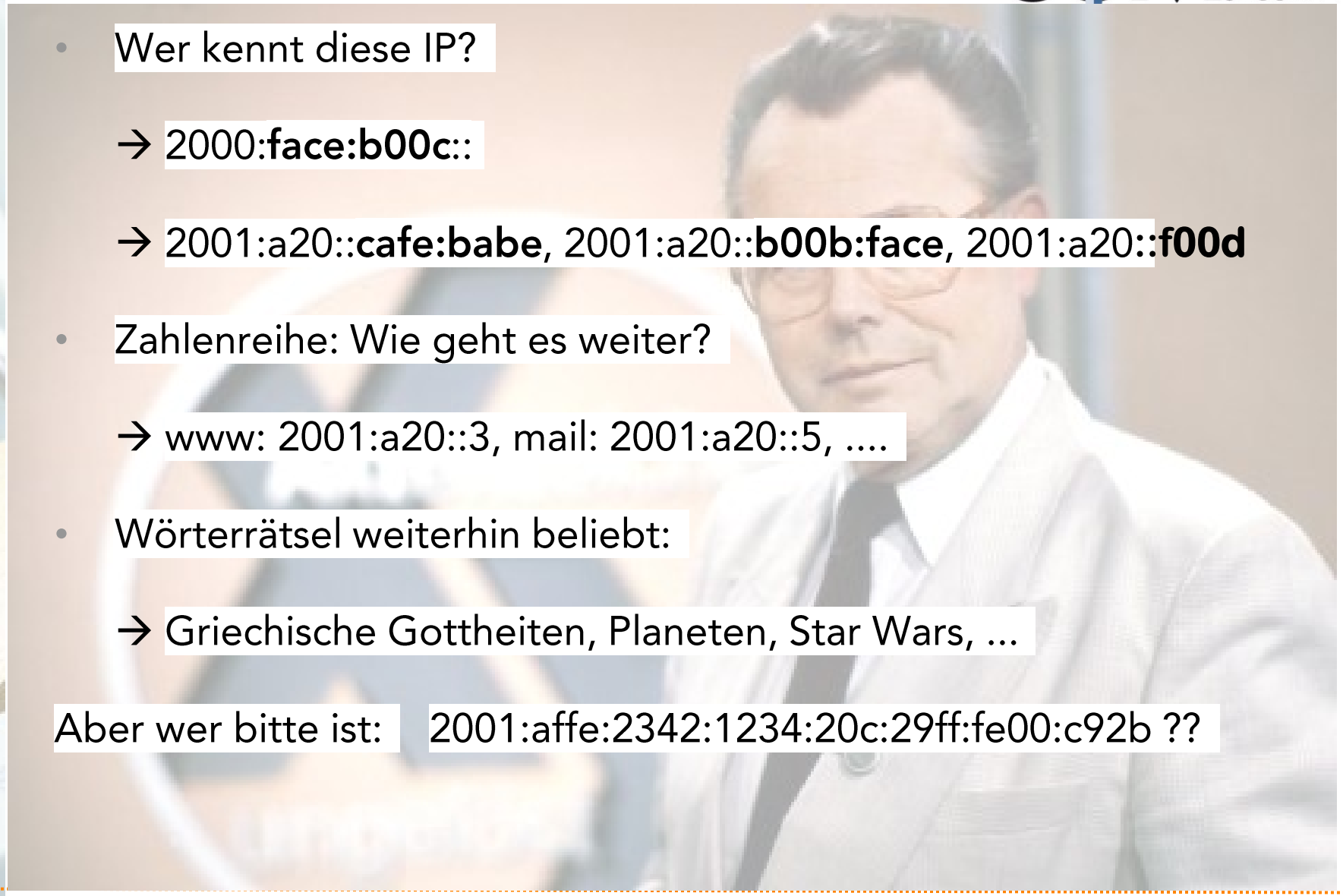
$2^{128} \approx 3{,}4 \cdot 10^{38}$ (340 Sextillionen)

2^{96} (79228162514264337593543950336) mal mehr als IPv4

Kein Netz ist kleiner als 2^{64}!

Das sind18446744073709551616!

Ratekrimi!



- Wer kennt diese IP?

  → 2000:**face:b00c**::

  → 2001:a20::**cafe:babe**, 2001:a20::**b00b:face**, 2001:a20::**f00d**

- Zahlenreihe: Wie geht es weiter?

  → www: 2001:a20::3, mail: 2001:a20::5, ...

- Wörterrätsel weiterhin beliebt:

  → Griechische Gottheiten, Planeten, Star Wars, ...

Aber wer bitte ist: 2001:affe:2342:1234:20c:29ff:fe00:c92b ??

Dynamische Adressen

Aufbau einer IP-Adresse:

<Netzwerkteil>/64:<Host-Teil>/64

- Netzwerkteil wird vorgegeben
- Host-Teil denkt sich jeder selber aus:

  02*<2 byte MAC>***ff:fe***<3 byte MAC>*

Heimspiel

Alter Wein in neuen Schläuchen:

Broadcast ist tot! Lang lebe Multicast!

Spezialadressen:

- All-Nodes: ff02::1 (broadcast)
- All-Routers: ff02::2

Host Discovery im lokalen Netz:

```
# ping6 ff02::1
```

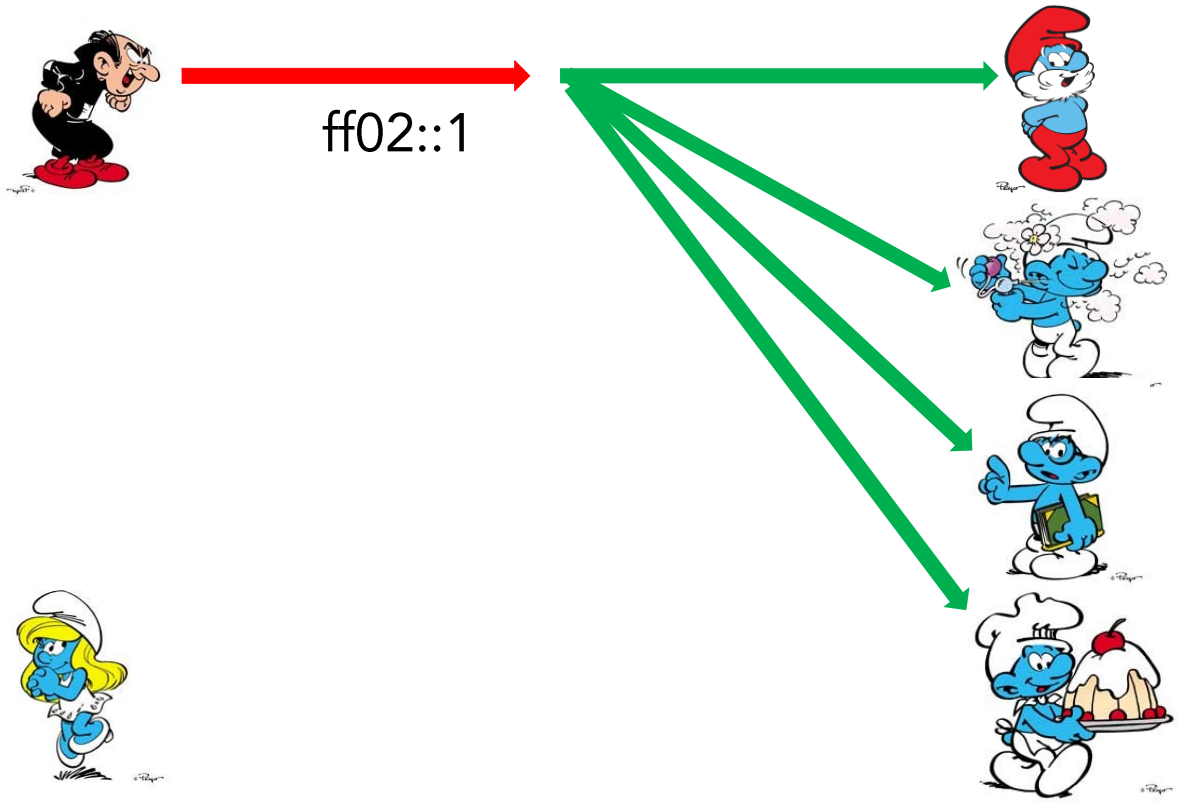
Smurf-Attacke reloaded

→ Angreifer sendet **1** Packet an alle

ff02::1

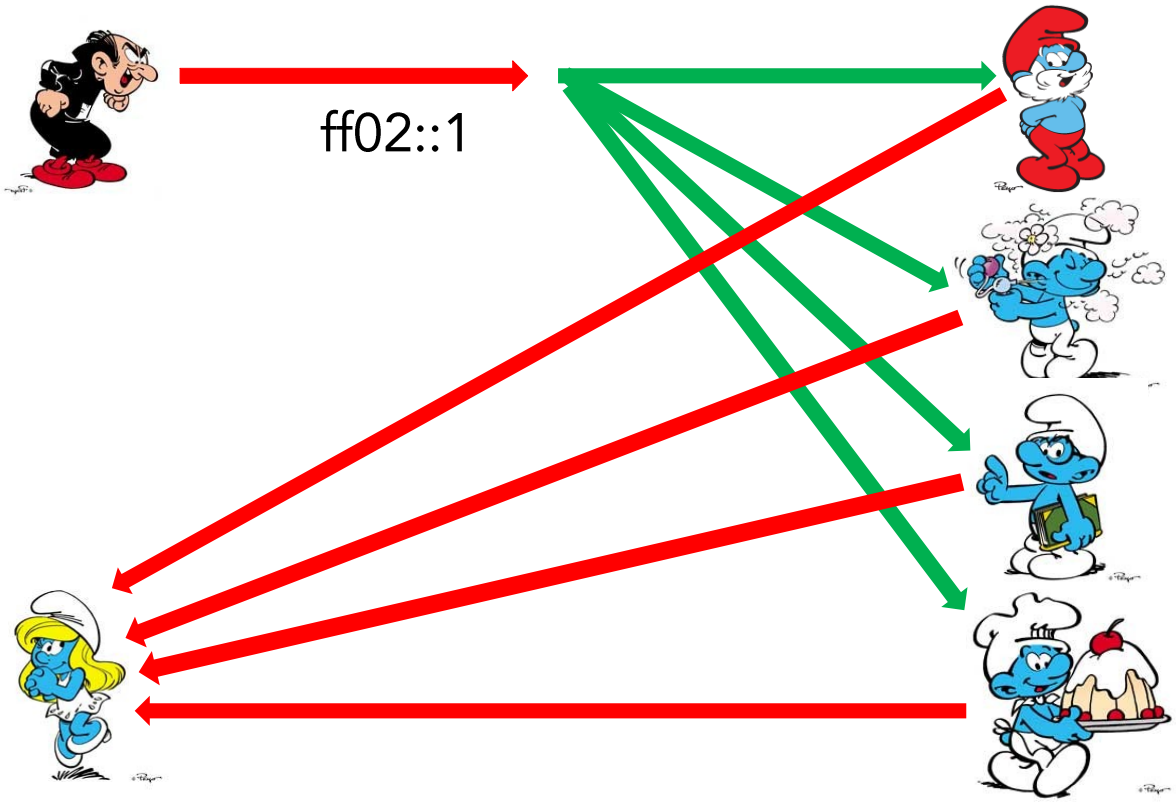
Smurf-Attacke reloaded

→ Angreifer sendet **1** Packet an alle



Smurf-Attacke reloaded

- Angreifer sendet **1** Packet an alle
- Alle Antworten dem vermeintlichen Absender



ARP - Alte Freunde

Wegen Smurf und Host-Discovery, ping ff02::1 manchmal gefiltert

- → Alle 18446744073709551616 können wir nicht testen
- → Bei IPv4 waren das noch weniger...
- → Aus den MACs, die IPv6-Adressen berechnen
- → ARP-Anfragen auf alle IPv4 IPs

ARP - Alte Freunde

Wegen Smurf und Host-Discovery, ping ff02::1 manchmal gefiltert

→ Alle 18446744073709551616 können wir nicht testen

→ Bei IPv4 waren das noch weniger...

→ Aus den MACs, die IPv6-Adressen berechnen

→ ARP-Anfragen auf alle IPv4 IPs

Lösung:

→ **IPv6 Privacy Extension**

IPv6 Privacy Extension

Verwürfelt die Host-Teile der Adressen regelmässig

- Kein IP-Adressen mehr errechenbar!
- Keine eindeutige Zuordenbarkeit mehr!
- Bei manchen OS Standardeinstellung
- Abschaltbar – nicht aber bei MacOS X

ICMPv6 – Absolut notwendig

ICMPv6 komplett abschalten ist keine Alternative

- Duplicate Adress Detection

  → Adressen werden nie doppelt benutzt

- Neighbor Discovery

  → Das neue ARP

- Keine Fragmentierung mehr: Path-MTU-Discovery

DAD DoS

Duplicate Address Detection:

- Wird die Adresse bereits genutzt?

  → Client fragt Nachbarn vor Nutzung

  → Kommt keine Antwort: Gut

  → Kommt Antwort: Neue Adresse ausdenken

DoS: Wir antworten auf alle Anfragen

Kein Client bekommt eine IP! Keine Kommunikation!

Neighbor Discovery Spoofing

- Adressauflösung IPv4 ← → IPv6 (früher ARP)
- Alles auf Layer 3 mit ICMPv6
- Das gleiche wie ARP Poisoning
- Port-Security, DHCP Snooping: hilft alles nix
- Lustiger mit „Override“-Flag

Die Lösung wäre: **SE**cure **N**eighbor **D**iscovery (SEND)

State**L**ess **A**ddress **A**uto **C**onfiguration

- Auf dem Router Präfix (Netz-Adresse) konfiguriert
- Router versendet Informationen an alle
- Hosts generieren sich die IP aus Präfix und ihrer MAC
- Hosts tragen den Router als Default-Router ein

SLAAC - Inhalte

Ein Router Advertisement enthält folgendes:

- Prefix
- Priorität des Routers
- Gültigkeitszeitraum
- Beliebige weitere Options (z.B. DNS nach RFC 5006)

SLAAC als Monkey-in-the-Middle

Angreifer versendet RA mit hoher Priorität

→ Hosts tragen den Router als neuen Default-Router ein!!

Angreifer macht NAT-PT und keinem fällt das auf.

- Alle neuen Verbindungen nun über diesen Router
- Nicht auf Layer 2 verhinderbar
- DHCP-Snooping hilft hier wieder nicht (... logisch ...)
- Gegenmassnahme: RA-Guard oder statische Switch-Konfiguration

SLAAC – Netze Beamen

- Host kann beliebig viele Default-Router haben
- Host kann beliebig viele Adressen haben
- Zwangs-Rollout im internen Netz:

  → IPs entfernter Netze werden lokal!

  → Direkte Kommunikation statt entfernte Netze

  → Vertrauensbeziehungen und Filterregeln umgangen

RA DoS

Was tun, wenn die alten Router nerven?

1. Verkehr wird z.B. immernoch über diese geleitet
2. Wir wollen den Adressraum übernehmen
3. Wir wollen die Erreichbarkeit von aussen verhindern

RA DoS

Was tun, wenn die alten Router nerven?

1. Verkehr wird z.B. immernoch über diese geleitet
2. Wir wollen den Adressraum übernehmen
3. Wir wollen die erreichbarkeit von aussen verhindern

Router Advertisment Denial of Service

„Ich bin dann mal weg“v6: RA mit Lifetime 0

→ Fake RA im Namen des Routers und er ist vergessen!

Redirect Spoofing

Hosts prüfen Redirects auf Plausibilität

Tricksen:

- Ping an das Opfer
- Pong läuft in's Leere
- Redirect auf uns spoofen mit Absender der Routers

→ Der Host wird uns glauben

Hohe Braukunst oder laue Pfütze?

Hohe Braukunst oder laue Pfütze?

Hohe Braukunst! Aber noch naturtrüb…

Hohe Braukunst oder laue Pfütze?

Hohe Braukunst! Aber noch naturtrüb…

Nach dem Filtern sicher lecker!