

IPv6

aktueller Stand und Ausblick

Jens Hektor / Nils Neumann

- **IPv6: aktueller Stand**
- **Cisco IOS IPv6 Feature Mapping**
- **Welche Switche und Router sind für IPv6 geeignet?**
- **First Hop Security**

IPv6: aktueller Stand

- **Dynamisches Routing (OSPFv3) ist auf Backbone-Geräten aktiv**
- **RWTH Firewall filtert IPv6 Datenverkehr**
- **Es gibt bereits ein paar IPv6 Nutzer**
 - Physik
 - UMIC
 - NOC
- **Router und Switch Software ist auf aktuellem Stand mit IPv6 Unterstützung – sofern möglich**
- **Test der IPv4/v6 Konnektivität der ‚neuen‘ Anycast Nameserver läuft aktuell**

■ IPv6 Basis Features

Feature	Catalyst 4500 (Sup7)	Catalyst 6500
ICMPv6	12.2(25)SG	12.2(17a)SX1
IPv6 ICMP Rate Limiting	-	12.2(50)SY
IPv6 MTU Path Discovery	12.2(25)SG	12.2(17a)SX1
IPv6 Neighbor Discovery	12.2(25)SG	12.2(17a)SX1
Netflow v9 for IPv6	-	?!
TFTP IPv6 Support	-	15.1(1)SY
Unicast Reverse Path Forwarding for IPv6	-	15.1(1)SY
IPv6 Stateless Autoconfiguration	12.2(25)SG	12.2(17a)SX1
Syslog over IPv6	12.2(44)SG	12.2(33)SXI

■ IPv6 First-Hop Security Features

Feature	Catalyst 4500 (Sup7)	Catalyst 6500
DHCPv6 Guard	-	-
IPv6 Device Tracking	-	-
IPv6 First-Hop Security Binding Table	-	-
IPv6 ND Multicast Suppress	-	-
IPv6 ND Inspection	-	12.2(50)SY
IPv6 RA Guard	12.2(54)SG	15.2(33)SXI4
IPv6 Snooping	-	-

■ IPv6 Routing Features

Feature	Catalyst 4500 (Sup7)	Catalyst 6500
OSPF for IPv6 (OSPFv3)	12.2(25)SG	12.2(17a)SX1
OSPF for IPv6 Authentication Support with IPsec	-	15.0(1)SY1
IPv6 Route Redistribution	12.2(25)SG	12.2(50)SY
OSPFv3 Fast Convergence	-	15.0(1)SY
IPv6 Static Routing	12.2(25)SG	12.2(17a)SX1
TTL Security Support for OSPFv3 on IPv6	-	-

- **IPv6 First-Hop Security Features (11)**
- **IPv6 Switching Services Features (6)**
- **IPv6 Routing Features (37)**
- **IPv6 Services and Management Features (31)**
- **DHCP Features for IPv6 (19)**
- **IPv6 Multicast Features (30)**
- **restliche Kategorien [Tunnel, VoIP, QoS] (29)**

Insgesamt gibt es über 150 verschiedene IPv6 Features, die vollständig, teilweise oder gar nicht unterstützt werden.

Welche Geräte sind für IPv6 geeignet 1/2

Switch / Router	Anzahl	IPv6	Ersatz
Cisco 2600 Series	4		Cisco 2900 Series
Cisco 2800 Series	23		Cisco 2900 Series
Cisco 2900 Series	19	✓	
Cisco 800 Series	21		Cisco 2900 Series
Cisco Catalyst 2900	9		Cisco Catalyst 2960C
Cisco Catalyst 2940-2970	431		Cisco Catalyst 2960C/(S)/X
Cisco Catalyst 2960C	32	✓	
Cisco Catalyst 2960S/X	60	✓	
Cisco Catalyst 3500/50/60	221		Cisco Catalyst 2960X,3560C/X
Cisco Catalyst 3560C	4	✓	
Cisco Catalyst 3560E	10		Cisco Catalyst 3560X
Cisco Catalyst 3560X	16	✓	

Welche Geräte sind für IPv6 geeignet 2/2

Switch / Router	Anzahl	IPv6	Ersatz
Cisco Catalyst 3750	62		Cisco Catalyst 3750X
Cisco Catalyst 3750X	13	✓	
Cisco Catalyst 4000	2		Cisco Catalyst 4500 Sup7
Cisco Catalyst 4500 (< Sup6)	42		Cisco Catalyst 4500 Sup7
Cisco Catalyst 4500 Sup6/6L	93	?	Cisco Catalyst 4500 Sup7
Cisco Catalyst 4500 >= Sup7/7L	34	✓	
Cisco Catalyst 4900 Series	2		Cisco Catalyst 3750X
Cisco Catalyst 6500 (<Sup2T)	14		Cisco Nexus 7000
Cisco Catalyst Blade Switch 3000	6		Passthrough + Nexus 2k
Cisco Catalyst ME 3400	11		Cisco Catalyst 3750X-12S
Cisco Nexus 5000	7	✓	
Cisco Nexus 7000	6	✓	

■ Betrieb des Dual-Stacks-Netzwerks

- doppelter Aufwand
 - Änderung des Routing, z.B. Umzug
 - Firewalling, z.B. Ändern, Hinzufügen, Löschen
 - Adressvergabe und Pflege von Namenseinträgen (DNS)
 - aufwändigere Fehleranalyse
 - Monitoring
 - Anpassung von Sicherheitssystemen, z.B. Intrusion Detection
- zusätzlich notwendig
 - IPv6 First Hop Security

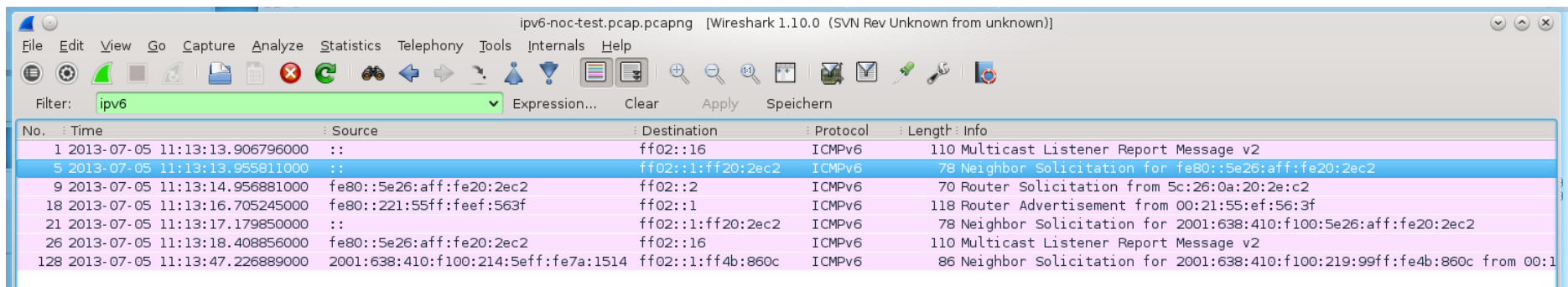
■ Erweiterung > 1000 IPv4-Netzen

- Routing
- Firewalling
- Layer2-Security (First Hop Security)
- SLAAC (Stateless Address Autoconfiguration) /DHCPv6

■ Zentrale Rolle bei Adressvergabe

- Router Announcements (RA)
- Neighbour Discovery (ND)
- Solicitation, Announcements
- Multicast DNS

■ DHCPv6 im Dualstackbetrieb nicht nötig



The image shows a Wireshark capture window titled "ipv6-noc-test.pcap.pcapng [Wireshark 1.10.0 (SVN Rev Unknown from unknown)]". The filter is set to "ipv6". The packet list pane shows several ICMPv6 packets. The selected packet (No. 5) is a Neighbor Solicitation for fe80::5e26:aff:fe20:2ec2.

No.	Time	Source	Destination	Protocol	Length	Info
1	2013-07-05 11:13:13.906796000	::	ff02::16	ICMPv6	110	Multicast Listener Report Message v2
5	2013-07-05 11:13:13.955811000	::	ff02::1:ff20:2ec2	ICMPv6	78	Neighbor Solicitation for fe80::5e26:aff:fe20:2ec2
9	2013-07-05 11:13:14.956881000	fe80::5e26:aff:fe20:2ec2	ff02::2	ICMPv6	70	Router Solicitation from 5c:26:0a:20:2e:c2
18	2013-07-05 11:13:16.705245000	fe80::221:55ff:feef:563f	ff02::1	ICMPv6	118	Router Advertisement from 00:21:55:ef:56:3f
21	2013-07-05 11:13:17.179850000	::	ff02::1:ff20:2ec2	ICMPv6	78	Neighbor Solicitation for 2001:638:410:f100:5e26:aff:fe20:2ec2
26	2013-07-05 11:13:18.408856000	fe80::5e26:aff:fe20:2ec2	ff02::16	ICMPv6	110	Multicast Listener Report Message v2
128	2013-07-05 11:13:47.226889000	2001:638:410:f100:214:5eff:fe7a:1514	ff02::1:ff4b:860c	ICMPv6	86	Neighbor Solicitation for 2001:638:410:f100:219:99ff:fe4b:860c from 00:1

■ RA (Router Announcement)

→ „Angriffe“ finden bereits statt: Windows (ab W7) mit IPv6 aktiv, Internetfreigabe

→ IPv6 Tunnel nach draussen

■ Attack against IPv6 Duplicate Address Detection (DAD)

→ Analog zum IPv4 ARP-flooding: Endgeräte erhalten keine IP

■ Neighbour Cache Attack

→ Von Remote: „ping“ auf grössere Netzbereiche zwingt Router mit Neighbour Discovery messages in die Knie

■ Spielarten diverser Angriffe mit Extension Headern

→ Analog zur IPv4 Fragmentierung

■ LAN Kommunikation bereits jetzt via IPv6