



IPv6

Nico Maas

Universität des Saarlandes

29.08.2012, HIZ

- **Grundlagen**
 - Vergleich IPv4 / IPv6
 - Schreibweisen
 - Adresstypen
 - Spezialadressen
 - Protokolle
- **OS Unterstützung**
- **Evaluierung Switches**
- **Evaluierung Core Router**
- **DualStack Lab**
- **DualStack Lab mit VSS**
- **Security \ RA Flood**
- **ToDo**
- **Quellen**

Grundlagen

IPv4

- 32 Bit
- ≈ 4,3 Milliarden Adressen
- Dezimal Notation
- Trennzeichen .
- 4 Oktette

192.168.2.1

IPv6

- 128 Bit
- ≈ 340 Sextillionen Adressen
- Hexadezimal Notation
- Trennzeichen :
- 8 x 4 Hexadezimal Stellen

2001:0db8:85a3:08d3:1319:8a2e:0370:7344

Verbesserungen

- Vergrößerung Adressbereich
- Vereinfachter Header
 - 320 Bits fester Kopfdatenbereich
 - Ergänzung durch zusätzliche Erweiterungskopfdatenbereiche bei Bedarf
- Stateless Address Auto Configuration
 - Adresszuweisung ohne DHCP Server per Neighbor Discovery Protocols über Router
 - Vermeidung von Konflikten durch Duplicate Address Detection
- Stateful Address Auto Configuration
 - DHCP Server
- Direkte IPSec Unterstützung
- QoS / Multicast / Kein Broadcast
- Verzicht auf NAT zu Gunsten von End2End Security

IPv6 Schreibweisen

- Volle Adresse: 2001:0db8:85a3:08d3:1319:8a2e:0370:7344
- Führende Nullen dürfen weggelassen werden
 - 2001:0db8:0000:08d3:0000:8a2e:0070:7344
 - 2001:db8:0:8d3:0:8a2e:70:7344
- Mehrere aufeinanderfolgende 0 Blöcke dürfen durch :: 1x ersetzt werden
 - 2001:0db8:0:0:0:0:1428:57ab
 - 2001:db8::1428:57ab
- Die letzten 4 Byte dürfen Dezimal notiert werden
 - ::ffff:7f00:1
 - ::ffff:127.0.0.1

IPv6 Schreibweisen

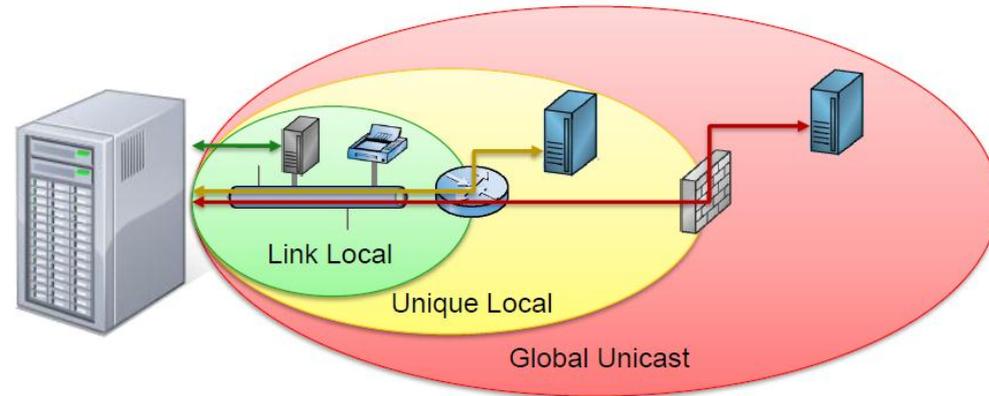
- URL Notation in []
 - `http://[2001:0db8:85a3:08d3:1319:8a2e:0370:7344]:8080/`
- Netznotation / CIDR
 - Präfix/Anzahl der verwendeten Bit für den Präfix – Rest ist Host Anteil
 - `2001:0db8:1234::/48`
 - Von: `2001:0db8:1234:0000:0000:0000:0000:0000`
 - Bis: `2001:0db8:1234:ffff:ffff:ffff:ffff:ffff`
 - /128 ist damit der Host selbst
- Netzgrößen
 - Internet-Provider: /32
 - Geschäftskunden: /48
 - Privatkunden: /56
- Uds: `2001:0638:0200::/48`

IPv6 Typen

- Unicast : 2001:0db8:85a3:08d3:1319:8a2e:0370:7344
 - Netzwerk Präfix => „Netz“ (64 Bit)
 - Device Identifier => „NIC“ (64 Bit)
 - Anfangs eindeutig Identifizierbar => Privacy Extensions
- Multicast: FFXX:0db8:85a3:08d3:1319:8a2e:0370:7344
 - FF => Multicast (8 Bit)
 - XX => Multicast Typ (8 Bit)
 - Group Identifier (112 Bit)
- Anycast
- 6to4 Tunnel
- ISATAP Tunnel
- Teredo Tunnel

IPv6 Typen: Unicast

- Link Local Unicast
 - FE80::/10
 - Im Link eindeutig, kann aber global mehrfach vorkommen. Wird automatisch bei IPv6 für jede Schnittstelle erzeugt, dient zur Netzwerkeinrichtung durch IPv6. Ping auf eine LLU Adresse benötigt die Angabe des „Ping Interfaces“ mit %InterfaceNummer am Ende der Zieladresse. Host erhält hier Informationen über andere IPv6 Hosts und Router.
- Unique Local Unicast
 - FC00::/7
 - Eindeutige lokale Unicast Adresse – sollte jedoch nur im lokalen und abgegrenzten Bereich eingesetzt werden. Router und Firewalls sollen laut RFC 4193 diese nicht ins globale Internet durchreichen.
- Global Unicast
 - 2000::/3
 - Global gültige und eindeutige Unicast Adresse, wird im Internet weitergeleitet



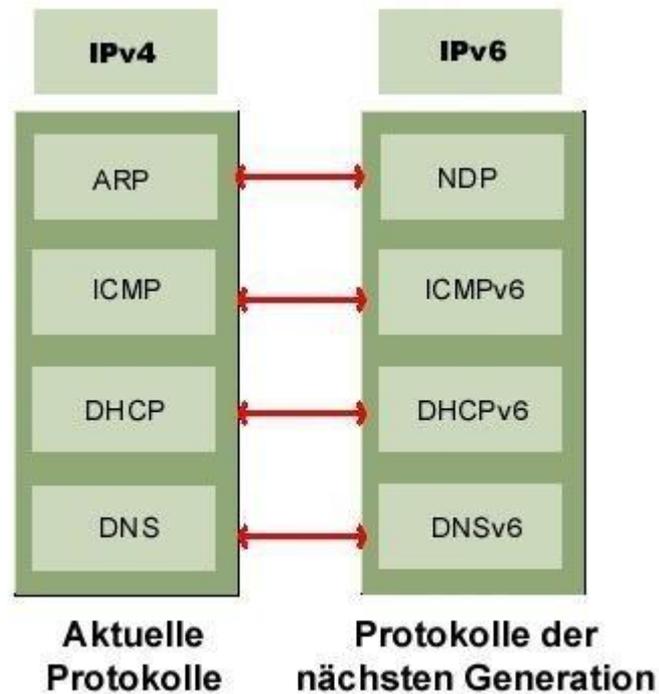
IPv6 Typen: Multicast und Anycast

- Multicast
 - FF00::/8
 - Adressiert eine Gruppe von Netzwerkknoten. Beschrieben in RFC 4291. Prefix definiert auch die Art der MC Adresse: Dauerhaft (well-known) oder Dynamisch sowie die Reichweite. FF05::2 bezeichnet z.B. alle Router im Standort.
- Anycast
 - Spezielle Unicast Adresse
 - Adressiert eine bestimmte Gruppe von Zielen im Netzwerk, z.B. alle Router. Antworten tut jedoch nur das Gerät welches per Routing Table am nächsten / besten erreichbar ist. Eine Anycast Adresse kann niemals als Source Adresse eingesetzt werden.
 - Beispiel: **2001:0db8:85a3:08d3:0000:0000:0000:0000**
 - Alle Router im Netzwerk

IPv6 Typen: Spezial Adressen

- 0.0.0.0
 - 0:0:0:0:0:0:0:0 oder ::/128:
 - Nicht spezifiziert, entspricht in IPv4 0.0.0.0 (RFC 4291)
- 127.0.0.1 / Loopback
 - 0:0:0:0:0:0:0:1 oder ::1/128:
 - Localhost / Loopback / Sweet Home (RFC 4291)
- IPv4-als-IPv6-Adresse
 - 0:0:0:0:0:FFFF:a.b.c.d/96 oder ::FFFF:a.b.c.d/96:
 - Kommt besonders bei IPv6 Servern im IPv4 Netzwerk zum Einsatz. Wird in RFC 4030 beschrieben. Spezieller 96 Bit Präfix.

IPv6 Protokolle



© tecChannel

IPv6 Protokolle: Neighbor Discovery Protocol

- Router Solicitation (ICMPv6 Type 133)
 - Anforderung an alle Router im Netzwerk sich zu melden
- Router Advertisement (ICMPv6 Type 134)
 - Verkündung Anwesenheit im Netz, ausgelöst durch RS oder Zeit
- Neighbor Solicitation (ICMPv6 Type 135)
 - Auflösung IPv6 Adresse auf Link Local Adresse und Überprüfung Erreichbarkeit Host
- Neighbor Advertisement (ICMPv6 Type 136)
 - Antwort auf NS
- Redirect (Type 137)
 - Information eines Routers über besseren ersten Hop für das Routing

Router / Präfix / Hop Ermittlung, Auto Konfiguration der IPv6 Interface Adresse, Adressauflösung, Erkennung doppelter Adressen / Nichterreichbarkeit

IPv6 Protokolle: Internet Control Message Protocol v6

- Destination Unreachable (ICMPv6 Type 1)
 - Ziel nicht erreichbar
- Packet Too Big (ICMPv6 Type 2)
 - Keine Weiterleitung des Pakets, weil Größer als maximale MTU des Links
- Time Exceeded (ICMPv6 Type 3)
 - Hop-Limit / TTL auf 0 abgesunken
- Echo Request (Type 128)
 - Ping
- Echo Reply (Type 129)
 - Pong

ICMPv6 ist wegen der Verknüpfung mit u.a. NDP unerlässlich für die Funktion von IPv6. Ein vollständiges Block von ICMPv6 führt zum Ausfall von IPv6.

IPv6 Protokolle: Dynamic Host Configuration Protocol v6

- Stateful DHCP
 - „Normales DHCP“ mit DHCP Server
- Stateless DHCP \ Auto Configuration
 - Wird vom Router \ Client durchgeführt
 - Router erhält einen Range aufs Interface und vergibt Stateless IP und GW Adresse
 - Vermeidlich „freie“ Adresse wird vom Client per DAD geprüft
 - Daten können durch DHCPv6 Server ergänzt werden (z.B. DNS Server Adresse)
 - Wird von Cisco präferiert da die IOS Software bisher nur begrenzt einen Stateful DHCP zur Verfügung stellt

DHCP unterstützt IPv6 ab Version 4.X

Es ist sinnvoll ein Stateful DHCP in geschlossenen Nutzernetzen anzustreben da ansonsten keine feste Zuweisung von Adressen möglich ist. Stateless ist wenn überhaupt nur in Public Netzen interessant

IPv6 Protokolle: Domain Name System v6

Der DNS funktioniert unter IPv6 wie unter IPv4.

Für IPv6 Adressen werden AAAA Records angelegt.

(Bei IPv4 A Records)

Es können sowohl A also auch AAAA Einträge für einen Namen verfasst werden, so dass das Gerät unter IPv4 und IPv6 Adresse im DualStack Betrieb ohne Proxy erreichbar ist.

Der DNS ist aufgrund der Komplexität der IPv6 Adressen unerlässlich und noch kritischer als unter IPv4.

Unter IPv6 kann der DNS per Stateless / Stateful DHCP oder manuell auf dem Host konfiguriert werden.

Bind unterstützt IPv6 ab Version 9.x

IPv6 OS Unterstützung: Microsoft

- **Windows 9x/ME**
 - IPv6 Stack der Firma Trumpet
- **Windows NT 4.0 / 2000**
 - Es existiert jeweils ein experimenteller Hotfix / Patch
- **Windows XP SP2**
 - Protokollstack per „ipv6 install“ nachinstallierbar. Adressen / DNS per netsh eintragbar
- **Windows Server 2003**
 - Aktiv, aber unfertig
- **Windows Vista / Server 2008**
 - Dual-IP-Layer Architektur, standardmäßig aktiviert, kein Mobile IPv6 Support
- **Windows 7**
 - Wie oben, mit Mobile IPv6 Support
- **Windows 8**
 - Wie oben, bei Dualstack Netzwerk Priorisierung / Nutzung von IPv6

IPv6 OS Unterstützung: Unix

- **Mac OS X**
 - 10.2: Unterstützung
 - 10.3: Vollständig über GUI Konfigurierbar
- **Linux**
 - Kernel 2.2: Experimentell
 - Kernel 2.4: Experimentell
 - Kernel 2.6: Voll nutzbar
- **Solaris**
 - Seit Version 8

IPv6 OS Unterstützung: Mobile

- **Android**
 - Seit 2.1, nur über WIFI, keine Privacy Extensions
 - Seit 2.3.4 IPv6 APNs
- **iOS**
 - Version 4.0 Dual Stack
 - Version 4.3 Privacy Extensions
- **Symbian**
 - Version 7
- **Windows Mobile**
 - Support kommt erst mit dem „Apollo“ Update

IPv6 OS Unterstützung: Netzwerk

- IOS
 - 12.2T Experimental
 - 12.3 / 12.4 Produktion
 - 12.4(6)T EIGRPv6 Unterstützung
 - 12.2(33)SXI4 RA Guard Unterstützung
 - Ältere Router können IPv6 Forwarding nur in Software abbilden, Geschwindigkeitsverlust
 - Ab 12.2(50)SE ist IPv6 im IP Base Package der Switches verfügbar

Evaluierung Switches

SDM Templates (Switching Database Manager)

- Switches mit SDM Unterstützung müssen ggf auf ein dual-ipv4-and-ipv6 Template konfiguriert werden
- Switches mit SDM:

```
--- IOS ---  
CAT2960  
CAT2970  
CAT3550  
CAT3560  
CAT3560E  
CAT3750  
CAT3750-METRO  
CAT3750E  
CBS3020  
CBS3030  
CBS3040  
CGESM  
ME2400  
ME3400
```

Auch die CAT3560V2 und die CAT3750V2 verwenden SDM

Evaluierung Core Router

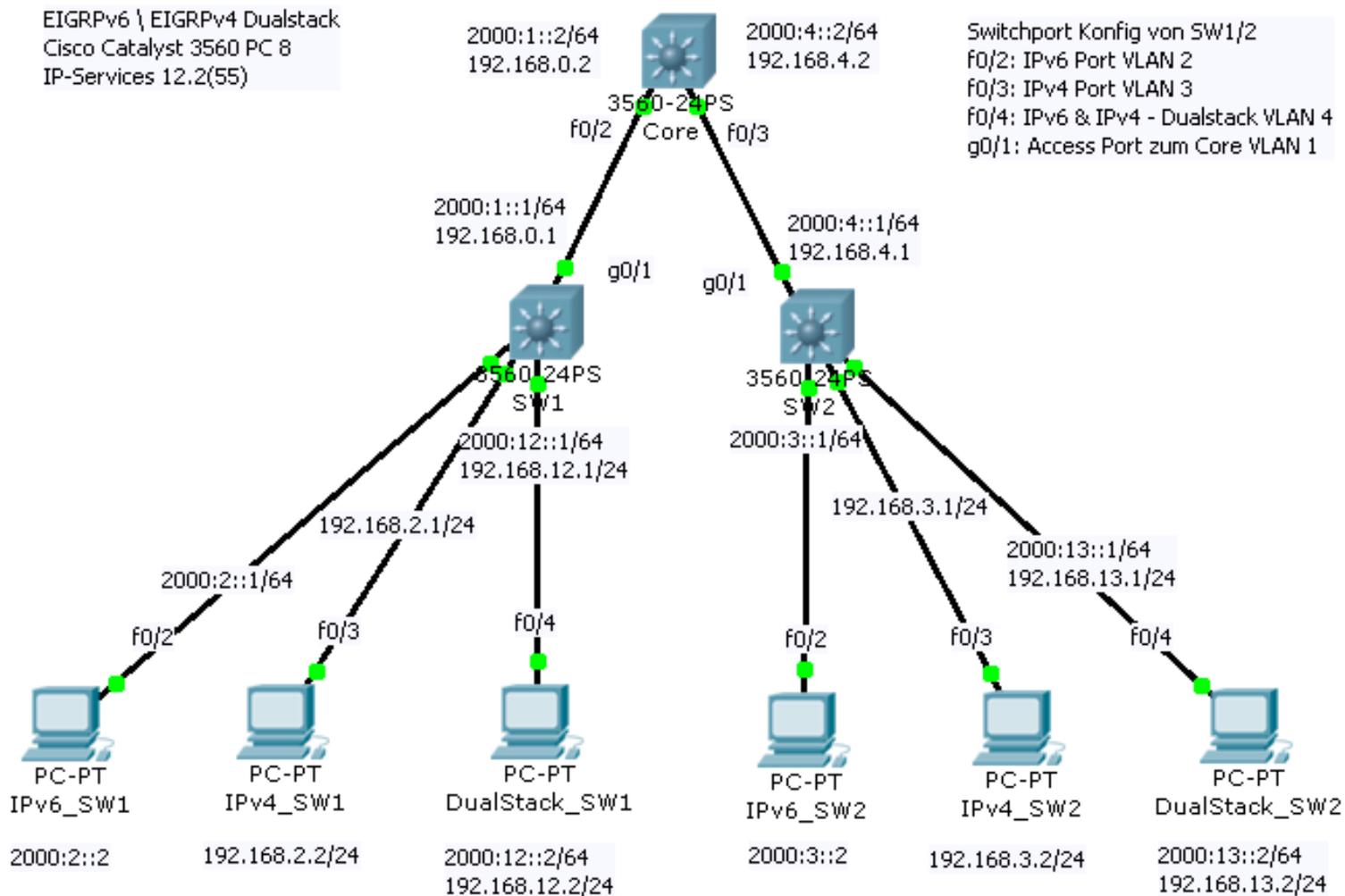
Ergebnis (Mitte 2011)

- **c65evss**
 - IP Services (122-33.SXI1), EIGRPv6, kein RA Guard
- **c65evss-2**
 - Advanced Enterprise Services (122-33.SXJ1), EIGRPv6, RA Guard
- **c65eb36-1**
 - Advanced IP Services (122-33.SXH2a), kein EIGRPv6, kein RA Guard
- **c65eb36-2**
 - Advanced Enterprise Services (122-33.SXI4), EIGRPv6, RA Guard

Ergebnis (Mitte 2012)

- Alle Systeme wurden zwischenzeitlich auf den aktuellen Stand gebracht und unterstützen nun IPv6 in Hardware und Software

DualStack Lab



Bestandteile

- Routing
 - 3x Cisco Catalyst 3560 PC 8 Layer 3 Switch
- Endgeräte
 - 2x Fujitsu Siemens Rechner mit Windows XP SP3
- Verwendete Protokolle
 - EIGRPv4
 - EIGRPv6

Vorbereitung des Switch

- IOS Upgrade
 - Benötigt wird mindestens Feature Set IP-Services, ab 12.2(44)SE
 - Verwendet wurde 12.2(55)SE [c3560-ipservicesk9-tar.122-55.SE]
- DualStack Umstellung
 - Um den DualStack korrekt nutzen zu können / IPv6 Routing, muss ein entsprechendes SDM Template konfiguriert werden.
 - **sdm prefer dual-ipv4-and-ipv6 routing**
 - Reload nicht vergessen!
- IPv6 aktivieren (nicht immer notwendig, auf Interface Ebene als Option)
 - **ipv6 enable**
- IPv6 Routing aktivieren
 - **ipv6 unicast-routing**

Table 8-1 Approximate Number of Feature Resources Allowed by the Indicated Template

Resource	Access	Default	Routing	VLAN
Unicast MAC addresses	4 K	6 K	3 K	12 K
IGMP groups and multicast routes	1 K	1 K	1 K	1 K
Unicast routes	6 K	8 K	11 K	0
▪ Directly connected hosts	4 K	6 K	3 K	0
▪ Indirect routes	2 K	2 K	8 K	0
Policy-based routing ACEs	0.5 K	0	0.5 K	0
QoS classification ACEs	0.5 K	0.5 K	0.5 K	0.5 K
Security ACEs	2 K	1 K	1 K	1 K
VLANs	1 K	1 K	1 K	1 K

Table 8-2 Approximate Feature Resources Allowed by Dual IPv4-IPv6 Templates

Resource	Dual IPv4-and IPv6 Templates			Indirect IPv4 and IPv6 Routing
	Default	VLAN	Routing	
Unicast MAC addresses	2 K	8 K	1.5 K	2 K
IPv4 IGMP groups and multicast routes	1 K	1 K (IGMP) 0 (multicast)	1 K	1 K
Total IPv4 unicast routes:	3 K	0	2.7 K	4 K
▪ Directly connected IPv4 hosts	2 K	0	1.5 K	2 K
▪ Indirect IPv4 routes	1 K	0	1.2 K	2 K
IPv4 policy-based routing ACEs	0	0	0.25 K	0.125 K
IPv4 or MAC QoS ACEs (total)	0.5 K	0.5 K	0.5 K	0.5 K
IPv4 or MAC security ACEs (total)	1 K	1 K	0.5 K	0.625 K
IPv6 multicast groups	1 K	1 K	1 K	1 K
Directly connected IPv6 addresses	2 K	0	1.5 K	2 K
Indirect IPv6 unicast routes	1 K	0.125 K	1.25 K	3 K
IPv6 policy-based routing ACEs	0	0	0.25 K	0.125 K
IPv6 QoS ACEs	0.5 K	0.5 K	0.5 K	0.125 K
IPv6 security ACEs	0.5 K	0.5 K	0.5 K	0.125 K

EIGRP v4 / v6

- Wie OSPFv3 / RIPng wird EIGRPv6 direkt auf die Interface konfiguriert / keine zentrale Konfiguration als “**network**”!
- Der EIGRPv6 Prozess muss aktiviert werden (**no shut**)
- EIGRPv6 benötigt eine **router-id** (wie EIGRPv4 auch)
- Passive Interfaces werden bei EIGRPv6 direkt im Routing Prozess konfiguriert
 - **ipv6 router eigrp 1**
 - **passive-interface f0/1**
- Filterung von Routen erfolgt in EIGRPv6 mit dem **distribute-list prefix-list** Kommando.
- Es gibt kein Äquivalent zu IPv4 **no auto-summary** da in IPv6 kein Konzept für Klassen basiertes Routing existiert

DualStack Lab – Client Interface

EIGRP v4

```
conf t
  int vlan 3
    ip address 192.168.2.1 255.255.255.0
    no shut
  int f0/3
    switchport mode access
    switchport access vlan 3
    spanning-tree portfast
    no shut
end
```

EIGRPv6

```
conf t
  int vlan 2
    no ip address
    ipv6 address 2000:2::1/64
    ipv6 eigrp 1
    no shut
  int f0/2
    switchport mode access
    switchport access vlan 2
    spanning-tree portfast
    no shut
end
```

DualStack Lab – Uplink Interface

EIGRP v4/6 – DualStack Uplink zum Core Router

```
conf t
  int vlan 1
    ip address 192.168.0.1 255.255.255.0
    ipv6 address 2000:1::1/64
    ipv6 eigrp 1
    no shut
  int g0/1
    switchport mode access
    switchport access vlan 1
    switchport nonegotiate
    no shut
end
```

DualStack Lab – Routing aktivieren

EIGRP v4

```
conf t
  router eigrp 1
    network 192.168.0.0
    network 192.168.2.0
end
```

EIGRPv6

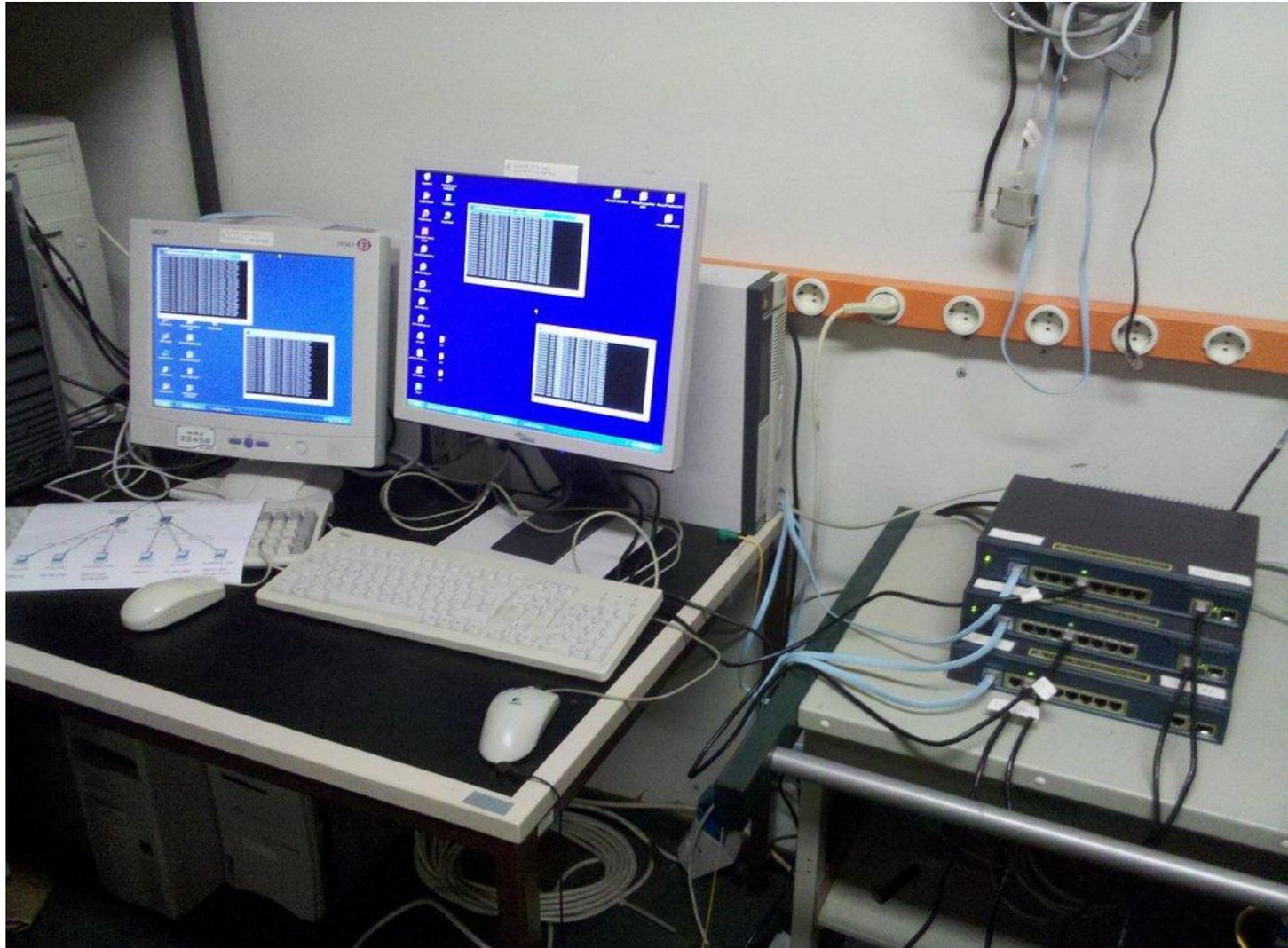
```
conf t
  ipv6 router eigrp 1
    no shut
end
```

DualStack Lab – Client Setup

Windows XP SP3

- IPv6 Installation
 - **ipv6 install**
- IPv6 Konfiguration
 - **netsh interface ipv6 add address “Lan-Verbindung” 2000:2::2**
- IPv6 Ping
 - **ping6 2000:3::2**

DualStack Lab



DualStack Lab

The screenshot displays a Windows 7 desktop environment. The desktop background is blue. On the left side, there is a vertical column of application icons including Paperkorb, Verknüpfung mit Arbeitsplatz, Google Chrome, TeamViewer 6, Mozilla Firefox, Google Earth, Avira AntiVir Control Center, Nero Burning ROM 10, Nero BackItUp 10, Nero MediaHub 10, Nero Vision 10, Nero StartSmart 10, vpn-client, sw1, Uni-SB_VPN-Server_..., sw2, Tera Term Pro, and Skype. On the right side, there are icons for Microsoft Word 2010, Microsoft PowerPoint 2010, Microsoft Outlook 2010, and Microsoft Excel 2010. The taskbar at the bottom contains the Start button, several open windows (Tera Term - COM1.VT, Tera Term - COM2.VT, C:\WINDOWS\system32\cmd.exe, C:\WINDOWS\system32\cmd.exe, Wechseldatenträger ..., Unbenannt - Paint), and the system tray showing the date and time as 14:47.

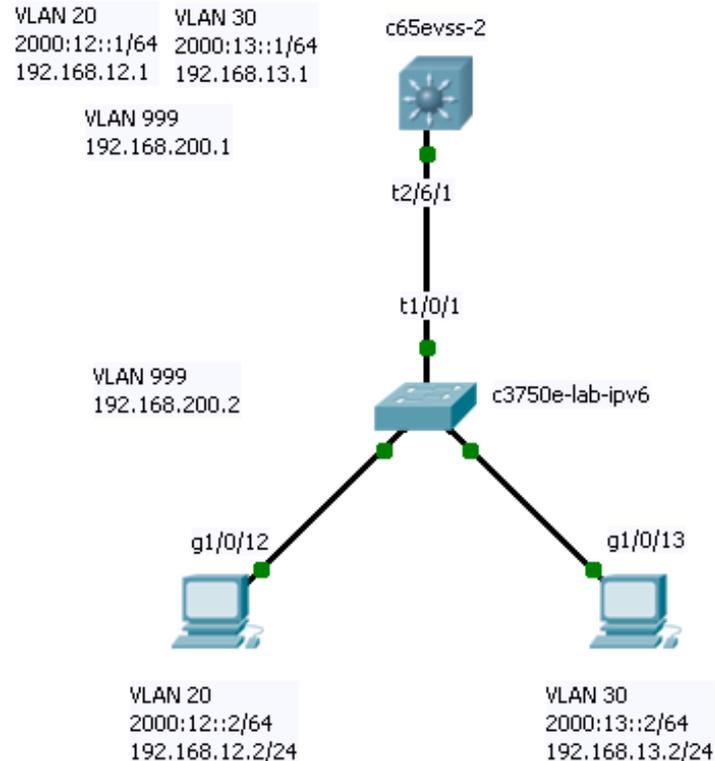
Two command prompt windows are open, both running the command `ping -f 192.168.13.2` and `ping6 -f 2000:13::2` respectively. The output of the first window shows successful ping results to 192.168.13.2, and the output of the second window shows successful ping results to 2000:13::2.

```
C:\WINDOWS\system32\cmd.exe - ping -f 192.168.13.2
Antwort von 192.168.13.2: Bytes=32 Zeit=15ms TTL=125
Antwort von 192.168.13.2: Bytes=32 Zeit=23ms TTL=125
Antwort von 192.168.13.2: Bytes=32 Zeit=29ms TTL=125
Antwort von 192.168.13.2: Bytes=32 Zeit=19ms TTL=125
Antwort von 192.168.13.2: Bytes=32 Zeit=26ms TTL=125
Antwort von 192.168.13.2: Bytes=32 Zeit=15ms TTL=125
Antwort von 192.168.13.2: Bytes=32 Zeit=23ms TTL=125
Antwort von 192.168.13.2: Bytes=32 Zeit=28ms TTL=125
Antwort von 192.168.13.2: Bytes=32 Zeit=29ms TTL=125
Antwort von 192.168.13.2: Bytes=32 Zeit=27ms TTL=125
Antwort von 192.168.13.2: Bytes=32 Zeit=17ms TTL=125
Antwort von 192.168.13.2: Bytes=32 Zeit=23ms TTL=125
Antwort von 192.168.13.2: Bytes=32 Zeit=14ms TTL=125
Antwort von 192.168.13.2: Bytes=32 Zeit=22ms TTL=125
Antwort von 192.168.13.2: Bytes=32 Zeit=29ms TTL=125
Antwort von 192.168.13.2: Bytes=32 Zeit=19ms TTL=125
Antwort von 192.168.13.2: Bytes=32 Zeit=25ms TTL=125
Antwort von 192.168.13.2: Bytes=32 Zeit=14ms TTL=125
Antwort von 192.168.13.2: Bytes=32 Zeit=23ms TTL=125
Antwort von 192.168.13.2: Bytes=32 Zeit=29ms TTL=125
Antwort von 192.168.13.2: Bytes=32 Zeit=17ms TTL=125
Antwort von 192.168.13.2: Bytes=32 Zeit=26ms TTL=125

C:\WINDOWS\system32\cmd.exe - ping6 -f 2000:13::2
Antwort von 2000:13::2: Bytes=32 Zeit=23ms
Antwort von 2000:13::2: Bytes=32 Zeit=29ms
Antwort von 2000:13::2: Bytes=32 Zeit=19ms
Antwort von 2000:13::2: Bytes=32 Zeit=26ms
Antwort von 2000:13::2: Bytes=32 Zeit=16ms
Antwort von 2000:13::2: Bytes=32 Zeit=20ms
Antwort von 2000:13::2: Bytes=32 Zeit=29ms
Antwort von 2000:13::2: Bytes=32 Zeit=18ms
Antwort von 2000:13::2: Bytes=32 Zeit=25ms
Antwort von 2000:13::2: Bytes=32 Zeit=15ms
Antwort von 2000:13::2: Bytes=32 Zeit=23ms
Antwort von 2000:13::2: Bytes=32 Zeit=29ms
Antwort von 2000:13::2: Bytes=32 Zeit=13ms
Antwort von 2000:13::2: Bytes=32 Zeit=27ms
Antwort von 2000:13::2: Bytes=32 Zeit=16ms
Antwort von 2000:13::2: Bytes=32 Zeit=23ms
Antwort von 2000:13::2: Bytes=32 Zeit=30ms
Antwort von 2000:13::2: Bytes=32 Zeit=19ms
Antwort von 2000:13::2: Bytes=32 Zeit=27ms
Antwort von 2000:13::2: Bytes=32 Zeit=28ms
Antwort von 2000:13::2: Bytes=32 Zeit=18ms
Antwort von 2000:13::2: Bytes=32 Zeit=25ms
```

DualStack Lab mit VSS

EIGRPv6 | EIGRPv4 Dualstack
Cisco Catalyst 6509E VSS
Advanced Enterprise Services 12.2(33)SXJ1



c65evss-2
VLAN Routing mittels EIGRPv4 und EIGRPv6 Konfiguration
VLAN mittels GW Adressen für die Rechner

c3750e-lab-ipv6
Terminierung von Access VLAN 20 und VLAN 30 als GW für die Clients

f0/13, f0/14
Dual Stack Windows XP Pro SP3 Rechner

DualStack Lab mit VSS

Stateless DHCPv6 / Autoconfig

```
conf t
  int vlan 40
    ipv6 address 2001:DB8:1234:42::1/64
    ipv6 nd other-config-flag | DHCP Server für weitere Daten
    ipv6 dhcp server dhcp-pool | DHCP Server anbinden
    ipv6 eigrp 1
    no shut
  ipv6 dhcp pool dhcp-pool | DHCP Server Eintrag mit Domain und DNS
    dns-server 2001:DB8:A:B::1
    domain-name example.com
  int g1/0/23
    switchport mode access
    switchport access vlan 40
    spanning-tree portfast
    no shut
end
```

DualStack Lab mit VSS

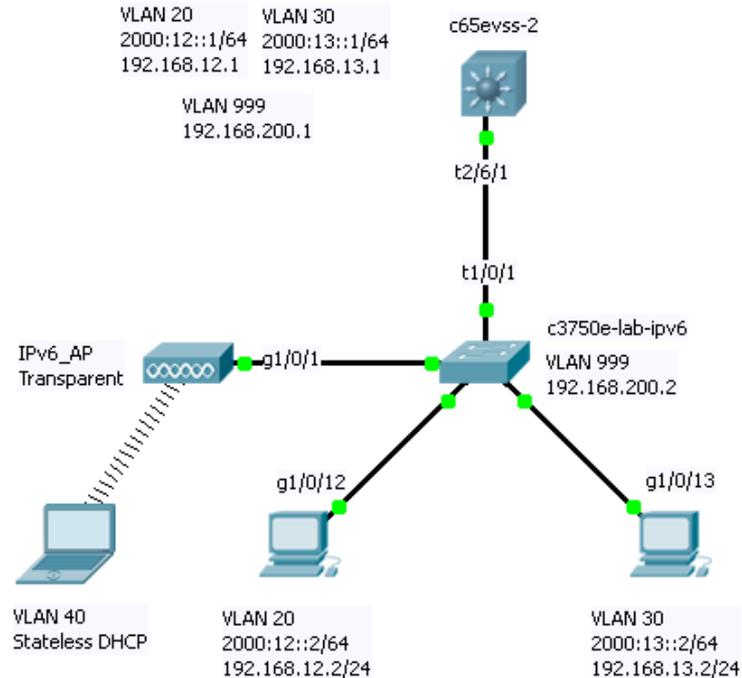
Stateless DHCP / Autoconfig

```
Ping wird ausgeführt für 2001:db8:1234:42:223:54ff:fe09:6adf mit 32 Bytes Daten:  
  
Antwort von 2001:db8:1234:42:223:54ff:fe09:6adf: Zeit=8ms  
Antwort von 2001:db8:1234:42:223:54ff:fe09:6adf: Zeit=15ms  
Antwort von 2001:db8:1234:42:223:54ff:fe09:6adf: Zeit=6ms  
Antwort von 2001:db8:1234:42:223:54ff:fe09:6adf: Zeit=12ms  
  
Ping-Statistik für 2001:db8:1234:42:223:54ff:fe09:6adf:  
Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0 (0% Verlust),  
Ca. Zeitangaben in Millisek.:  
Minimum = 6ms, Maximum = 15ms, Mittelwert = 10ms
```

ipv6 address 2001:DB8:1234:42::1/64

DualStack Lab mit VSS

EIGRPv6 \ EIGRPv4 Dualstack
Cisco Catalyst 6509E VSS
Advanced Enterprise Services 12.2(33)SXJ1



c65evss-2
VLAN Routing mittels EIGRPv4 und EIGRPv6 Konfiguration
VLAN mittels GW Adressen für die Rechner

c3750e-lab-ipv6
Terminierung von Access VLAN 20 und VLAN 30 als GW für die Clients
Terminierung von Access VLAN 40 und PoE für den WLAN AP

IPv6_AP
Transparente Weiterleitung des VLAN 40 an Client, weitergabe der
Stateless DHCP Daten auf VLAN 40

f0/13, f0/14
Dual Stack Windows XP Pro SP3 Rechner

DualStack Lab mit VSS

The image shows three overlapping windows from a Windows operating system. The leftmost window is titled 'Status von Drahtlosnetzwerkverbindung' (Wireless Network Connection Status). It displays connection details for IPv4 and IPv6, signal quality, and activity statistics. The middle window is titled 'Netzwerkverbindungsdetails' (Network Connection Details) and shows a list of network properties for a specific connection. The bottom-right window is a command prompt titled 'Administrator: C:\Windows\system32\cmd.exe' showing the output of a ping command to a specific IPv6 address.

Status von Drahtlosnetzwerkverbindung

Allgemein

Verbindung

IPv4-Konnektivität:	Kein Netzwerkzugriff
IPv6-Konnektivität:	Kein Internetzugriff
Medienstatus:	Aktiviert
Kennung (SSID):	IPv6
Dauer:	00:07:29
Übertragungsrate:	54,0 MBit/s
Signalqualität:	

Details...

Aktivität

Gesendet — — Empfangen

Bytes: 6.218 | 8.669

Eigenschaften Deaktivieren Diagnose

Schließen

Netzwerkverbindungsdetails

Netzwerkverbindungsdetails:

Eigenschaft	Wert
Verbindungsspezifisches...	example.com
Beschreibung	Broadcom 802.11n-Netzwerkadapter
Physikalische Adresse	48-5D-60-2A-97-4F
IPv6-Adresse	2001:db8:1234:42:89d3:689a:48d3:3658
Temporäre IPv6-Adresse	2001:db8:1234:42:4582:85e:87a5:e0fa
Verbindungslokale IPv6-...	fe80::89d3:689a:48d3:3658%13
IPv6-Standardgateway	fe80::224f9ff:fe5b:e400%13
IPv6-DNS-Server	2001:db8:a:b::1

Administrator: C:\Windows\system32\cmd.exe

```
Ping wird ausgeführt für 2000:12::2 mit 32 Bytes Daten:  
Antwort von 2000:12::2: Zeit=15ms  
Antwort von 2000:12::2: Zeit=13ms  
Antwort von 2000:12::2: Zeit=8ms  
Antwort von 2000:12::2: Zeit=16ms  
  
Ping-Statistik für 2000:12::2:  
Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0  
<0% Verlust>,  
Ca. Zeitangaben in Millisek.:  
Minimum = 8ms, Maximum = 16ms, Mittelwert = 13ms
```

Security RA Flood

RA / flood_router6

- Teil des THC-IPv6 Attack Toolkit
- Überflutet das lokale Netz mit falschen RAs
Geräte (Switches, Router, PCs)
verarbeiten die falschen GWs
und fügen diese ihren Listen hinzu
- Führt zu hoher System & Speicherauslastung und schließlich zum Absturz
- DoS Angriff
- Von jedem Port aus möglich
- Schwere Auswirkungen auf Windows, Unix, Mac sowie alle anderen System mit IPv6 Stack
- Entwickelt von THC / Marc „van Hauser“ Heuse

<http://www.thc.org/releases.php>

```
fe80::218:15ff:feee:2d06%12
fe80::218:8ff:feee:f517%12
fe80::218:10ff:fe93:b495%12
fe80::218:e5ff:fe60:e212%12
fe80::218:f4ff:fe14:58ea%12
fe80::218:98ff:fee4:d54d%12
fe80::218:eaff:fe8b:d2cc%12
fe80::218:d2ff:fe45:52a%12
fe80::218:99ff:fe34:b86e%12
fe80::218:1aff:fe11:2ced%12
fe80::218:b4ff:fe03:bc9%12
fe80::218:1ff:fedc:bab9%12
fe80::218:e6ff:feff:2312%12
fe80::218:89ff:fe79:1145%12
fe80::218:a3ff:fe6d:505d%12
fe80::218:23ff:fec6:7d46%12
fe80::218:c2ff:fe05:86d3%12
fe80::218:eef:fe79:ec3e%12
fe80::218:eeff:fe46:806b%12
fe80::218:e2ff:fecf:5568%12
fe80::218:33ff:fe09:721f%12
fe80::218:dbff:fea8:9b5b%12
fe80::218:38ff:fedf:918d%12
fe80::218:62ff:fe1b:50d4%12
fe80::218:c1ff:fe93:7f5c%12
fe80::218:65ff:feb2:62f7%12
fe80::218:b3ff:fe76:2f03%12
fe80::218:3fff:fe96:e6be%12
fe80::218:faff:fede:7e5c%12
fe80::218:14ff:fedc:9143%12
fe80::218:cdff:fe84:18b3%12
fe80::218:5fff:fe7e:e0dd%12
fe80::218:fbff:feea:a08c%12
fe80::218:3cff:fec7:3154%12
fe80::218:5ff:fe66:61e6%12
fe80::218:a1ff:fe18:1d42%12
fe80::218:baff:fe20:83eb%12
fe80::218:b8ff:fe06:cc1a%12
fe80::218:dbff:fe8e:8bf8%12
fe80::218:4eff:fe18:27d1%12
fe80::218:a9ff:fe2a:d675%12
fe80::218:dff:fe26:fe98%12
fe80::218:47ff:feae:ff6f%12
fe80::218:1dff:fecf:a7f3%12
```

Security RA Flood

RA / flood_router6

- Windows XP Pro SP3
- Windows 7
- OpenSuse 10.4
- Ubuntu 10.04.2
- IOS

Security RA Flood

Access Ports \ VLANs

- ACL zum blockieren von RA
 - ipv6 access-list BlockRA
 - 🕒 deny icmp any any router-advertisement
 - 🕒 deny ipv6 any any undetermined-transport
 - 🕒 permit ipv6 any any
- ACL auf Access Ports / VLANs konfigurieren
 - int range f0/1-8
 - 🕒 ipv6 traffic-filter BlockRA in
 - Bei CAT 2960, 3560, 3750, 6500...
 - Undetermined Transport ist erst ab IOS Release 12.2(55) verfügbar
- deny udp any eq 547 any eq 546 // Block Rouge IPv6 DHCP Server

Security RA Flood

Core Router

- RA Guard auf Access Ports konfigurieren
 - int range g0/1-48
 - ⌚ ipv6 nd rguard
- Bei CAT 6500, ab SXI4, nur auf Access Ports anwendbar, nicht auf VLANs

DualStack Lab mit VSS, RA Angriff

EIGRPv6 \ EIGRPv4 Dualstack

Cisco Catalyst 6509E VSS

Advanced Enterprise Services 12.2(33)SXJ1

VLAN 20	VLAN 30
2000:12::1/64	2000:13::1/64
192.168.12.1	192.168.13.1

VLAN 999
192.168.200.1

c65evss-2



t2/6/1

t1/0/1

VLAN 999
192.168.200.2

c3750e-lab-ipv6

g1/0/1



VLAN 999
no ip, Linux
THC Flood RA

g1/0/12



VLAN 20
2000:12::2/64
192.168.12.2/24

g1/0/13



VLAN 30
2000:13::2/64
192.168.13.2/24

c65evss-2

VLAN Routing mittels EIGRPv4 und EIGRPv6 Konfiguration
VLAN mittels GW Adressen für die Rechner

c3750e-lab-ipv6

Terminierung von Access VLAN 20 und VLAN 30 als GW für die Clients

f0/13, f0/14

Dual Stack Windows XP Pro SP3 Rechner

Angriff ohne ACLs auf c3750e:
c3750e: 29% CPU
c65evss-2: 38% CPU
Rechner im Netz frieren ein

Angriff mit ACLs auf c3750e:
c3750e: 23% CPU
c65evss-2: 3% CPU
Rechner im Netz Ok

Noch offene Punkte

- DualStack Labor
- Evaluierung Switches \ Router
 - SDM Template Evaluierung
 - Core Router
 - IOS Versionen + HW IPv6 fähig?
- Cisco VSS Labor
- Subnetting des IPv6 Blockes der UoS
- Reale IPv6 Anbindung an das DFN Netzwerk / erstes Testnetz (10.08.2012)
- DNS & DHCP auf IPv6 / QiP
- NAT-PT oder ähnliche IPv4/v6 Aggregation/Proxytechnik
- Sicherheitskonzept entwerfen / Firewall Regeln entwickeln

Cisco Tools

- IPv6 Knowledge Base Portal
 - <http://www.cisco.com/web/solutions/netsys/ipv6/knowledgebase/index.html#~start>,
- IOS Feature Navigator
 - <http://tools.cisco.com/ITDIT/CFN/>
- IOS Software Download
 - <http://www.cisco.com/cisco/software/find.html?q=&task=default>
- IOS Packaging
 - http://www.cisco.com/en/US/prod/collateral/iosswrel/ps8802/ps5460/prod_bulletin0900aecd80281b17.html
- IPv6 Lab and Techtorial
 - http://www.slideshare.net/feb_989/cisco-i-pv6-laband-techtorial-workshop-v0

Cisco Guides

- Implementing IPv6 for Cisco IOS Software
 - http://www.cisco.com/en/US/docs/ios/12_2t/ipv6/SA_Impv6.pdf
- IOS IPv6 Configuration Guide 12.2SR
 - http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/12_2sr/ipv6_12_2sr_book.html
- IOS 12.2(33)SXI New Features (siehe Mitte der Seite EIGRPv6)
 - http://www.cisco.com/en/US/prod/collateral/iosswrel/ps8802/ps6970/ps6017/ps9673/product_bulletin_c25-503086_ps5460_Products_Bulletin.html
- IOS IPv6 First Hop Security
 - http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-first_hop_security.html
- IOS Implementing DHCP for IPv6
 - <http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-dhcp.html#wp1053979>

Allgemein Web

- EIGRPv6 Konfiguration
 - <http://www.rogerperkin.co.uk/ccie/index.php/ipv6/eigrp-ipv6/>
- NDP
 - http://de.wikipedia.org/wiki/Neighbor_Discovery_Protocol
- ICMPv6
 - <http://de.wikipedia.org/wiki/ICMPv6>
- RA Guard
 - <http://www.gossamer-threads.com/lists/nsp/ipv6/29766>
 - <http://www.mh-sec.de>
 - <http://samsclass.info/ipv6/proj/flood-router6a.htm>
- IPv6 Security
 - <https://wikispaces.psu.edu/display/ipv6/IPv6+security>
 - <http://www.heise.de/netze/artikel/IPv6-Privacy-Extensions-einschalten-1204783.html>

Allgemein Web

- IPv6 Tools
 - <https://www.ultratools.com/ipv6Tools>
- IPv6 Subnet Calculator, Port Scanner, Traceroute, Ping,...
 - <http://www.subnetonline.com/pages/subnet-calculators/ipv6-subnet-calculator.php>
- IPv6
 - <http://de.wikipedia.org/wiki/IPv6>
- IPv6 Sicherheitsvortrag von van Hauser
 - <http://www.heise.de/security/artikel/IPv6-und-die-Sicherheit-1251552.html>
- Grafik Folie 8
 - Naim Mala, Controlware
- Grafik Folie 11
 - http://www.tecchannel.de/netzwerk/lan/2032649/lan_und_wan_ratgeber_richtig_auf_ipv6_migrieren