Monitoring der DualStack Umgebung der AWK Group

Swiss IPv6 Council, 25. November 2013

Gabriel Müller, Senior Consultant

AWK GROUP
Consulting | Engineering | Project Management

www.awk.ch

Fakten und Zahlen

- AWK ist eines der grössten Schweizer Beratungsunternehmen für Informationstechnologie
- Consulting, Engineering und Projektmanagement aus einer Hand
- Über 140 Mitarbeitende, davon 120 Ingenieure, Informatiker und Physiker
- Über 3'000 erfolgreiche Projekte für mehr als 300 Kunden realisiert
- Hauptsitz in Zürich, Niederlassungen in Bern und Basel
- Mitglied der ITIC GROUP, einem internat. Netzwerk unabhängiger Consulting-Firmen
- Unabhängig (vollständig im Besitz der Partner) und produktneutral (keine Interessenbindungen)
- Gegründet 1986

Partner der AWK Group (v.l.n.r): André Arrigoni, Kurt Biri (Managing Partner), Oliver Vaterlaus, Peter Gabriel, Ralph Tonezzer

Agenda

1) Einleitung
2) Umsetzung
3) Demo
4) Zusammenfassung und Ausblick

Einleitung

Einleitung

Motivation

- … sich mit IPv6 zu beschäftigen
  - Seit 2008
  - Passion für Netzwerktechnologien
- … praktische Erfahrungen im Bereich IPv6 zu sammeln
  - Knowhow oft entscheidend für Projekterfolg. Als Projektleiter
    - Aufwandsabschätzungen hinterfragen
    - Lieferobjekte beurteilen
    - Projektmitarbeiter motivieren, Probleme frühzeitig zu kommunizieren
- … für das hier vorgestellte Monitoring-Projekt
  - Erhöhte Anforderungen an das Netzwerk der AWK Group
  - Redundante Netzwerkkonfigurationen ohne Monitoring machen wenig Sinn
- … für den heutigen Vortrag
  - Erfahrungen Teilen
  - Teilnehmer für Praxis-Versuche motvieren

Grau, teurer Freund, ist alle Theorie,
Und grün des Lebens goldener Baum.
(Goethe, Faust I 2038f)

Einleitung

Vision

- Anfang 2013

  „Das Netzwerkmanagement erfolgt zukünftig ausschliesslich über IPv6. Alle relevanten Netzwerkparameter (IPv4 und IPv6) werden über IPv6 abgefragt. Konfigurationen der Netzwerkelemente sollen regelmässig automatisiert gesichert werden. Der Transport erfolgt hier ebenfalls über IPv6“

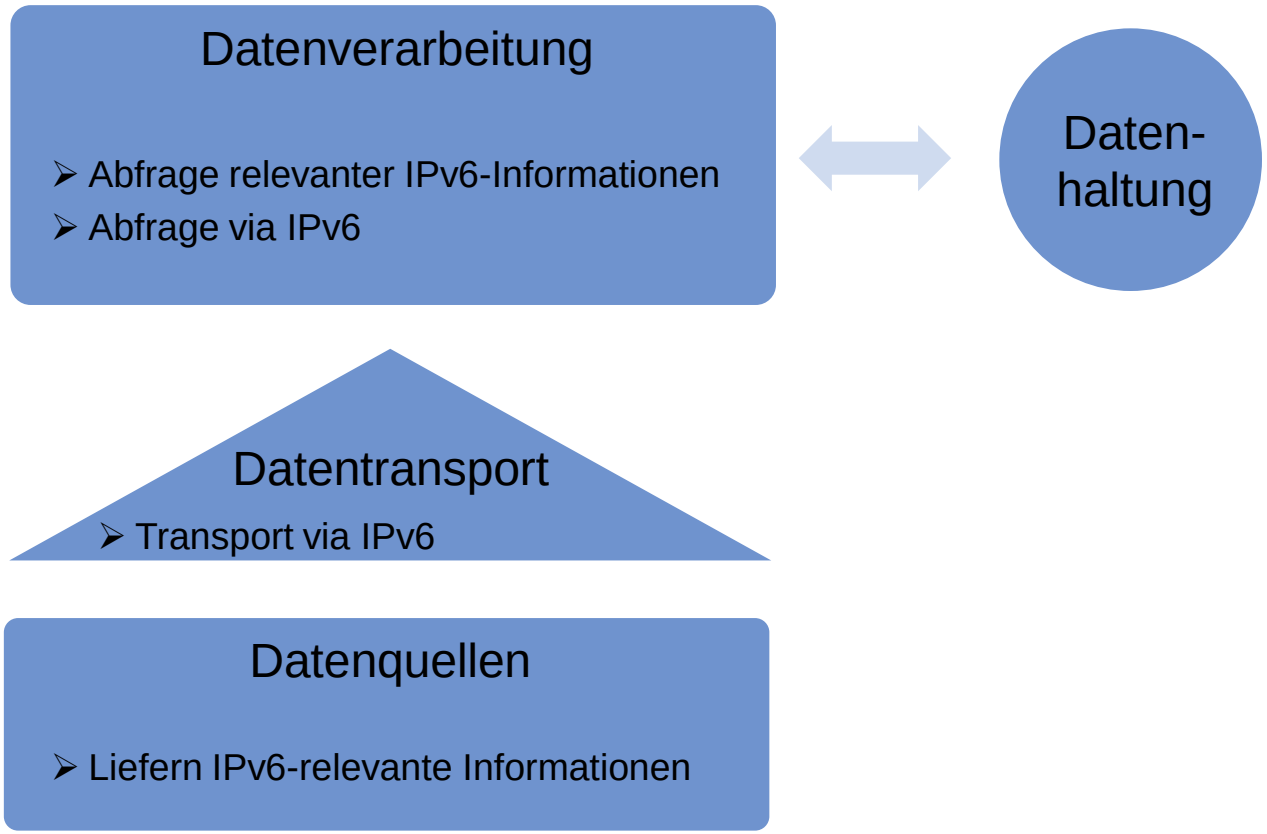
- November 2013

  … nun ja

Einleitung

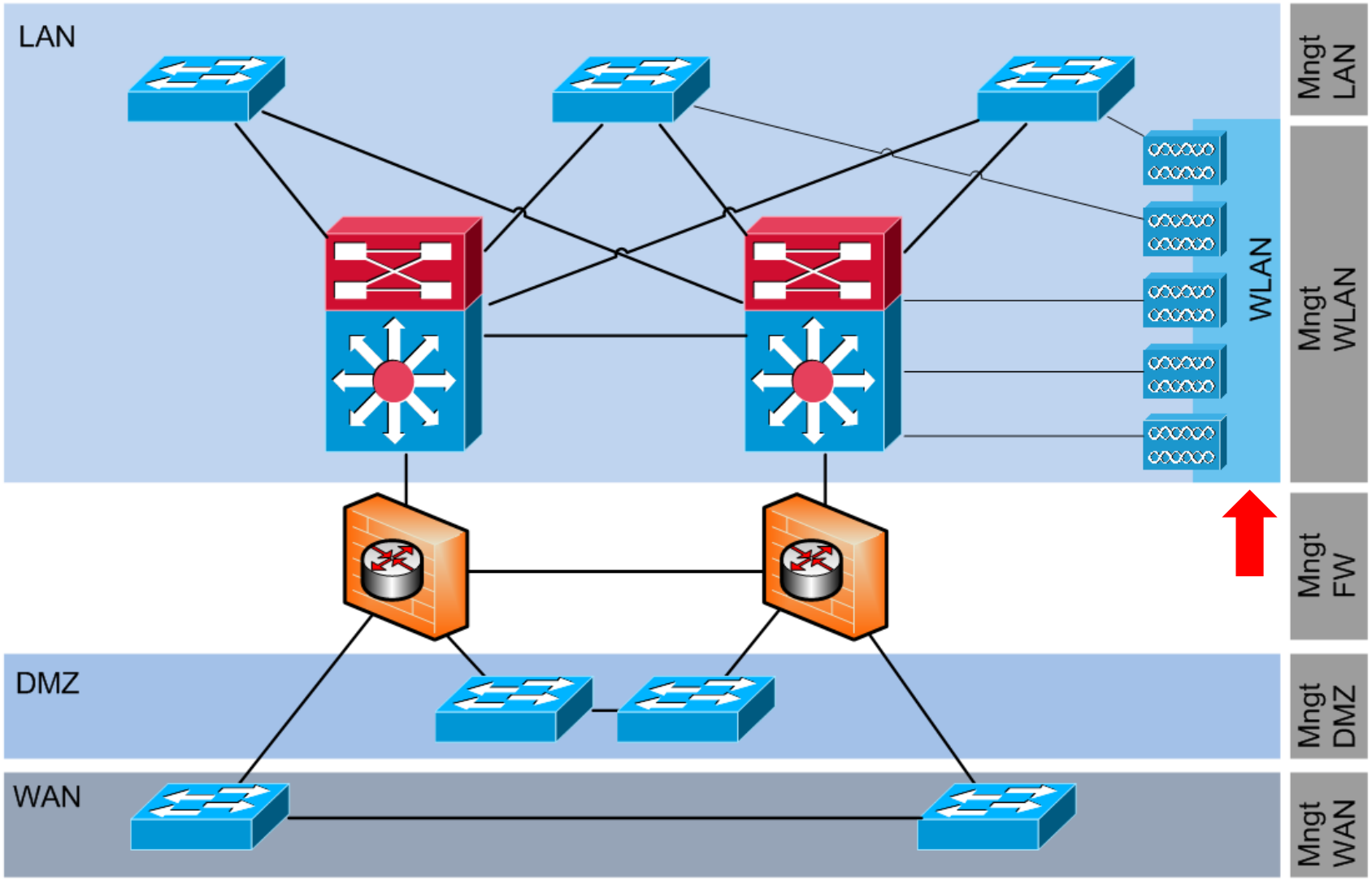
Elemente des Netzwerkmanagements

- Informationen
  - Bereitstellen
  - Transportieren
  - Abfragen
  - Verarbeiten
  - Speichern



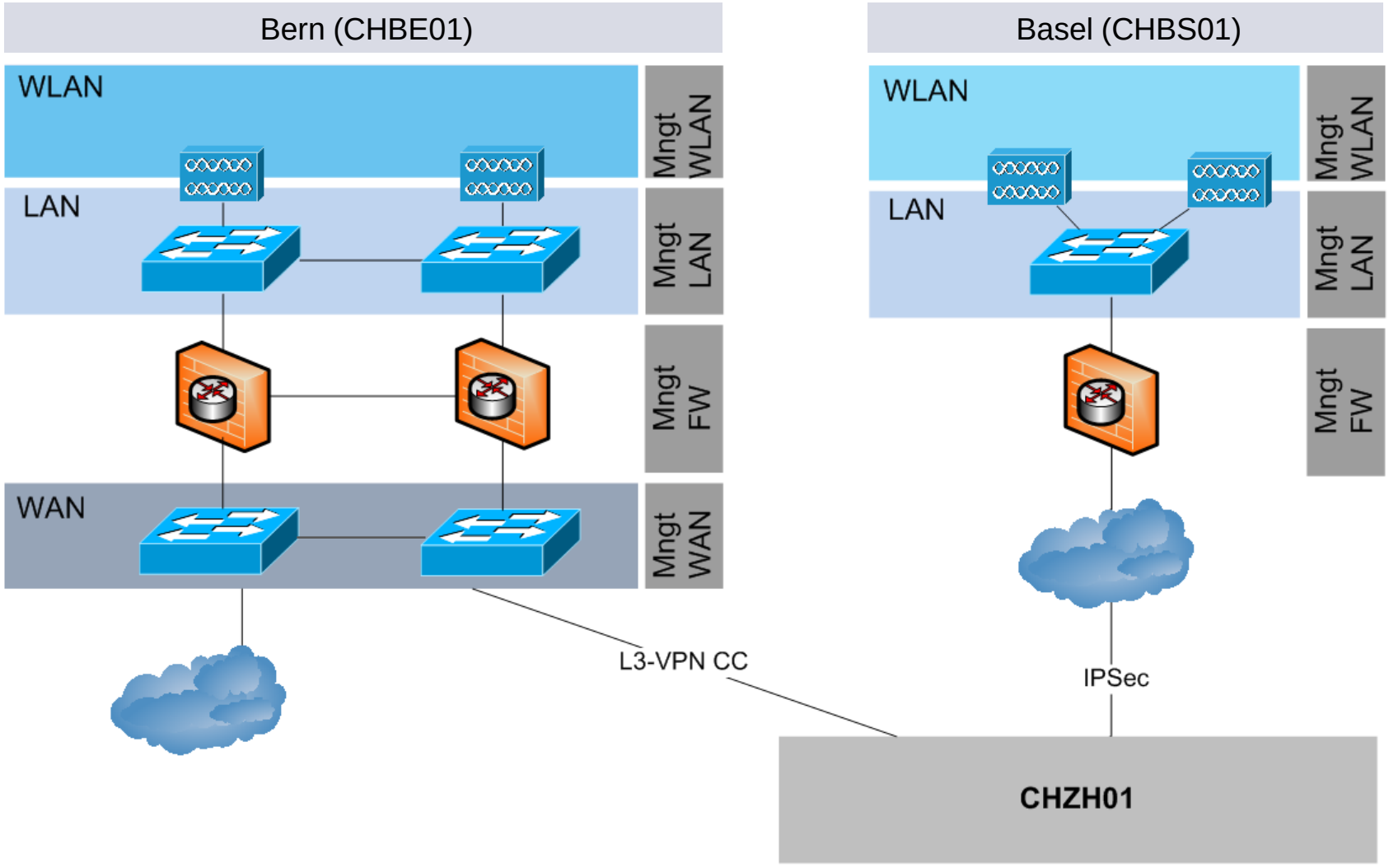
Einleitung

Ausgangslage – Netzwerktopologie Zürich (CHZH01)



Einleitung

Ausgangslage – Netzwerktopologie Bern (CHBE01) und Basel (CHBS01)

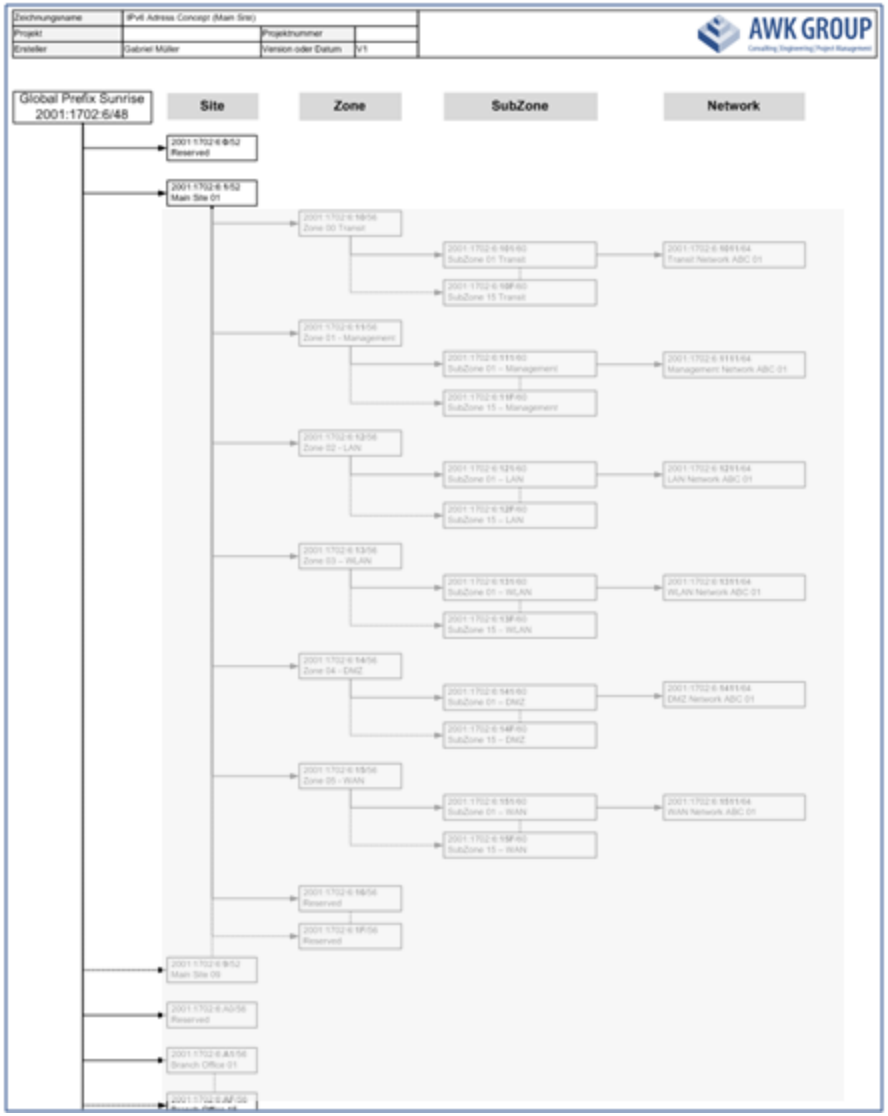


Umsetzung

Umsetzung

Vorbereitungen - Adresskonzept

- 2001:1702:6/48
  - Main Site /52
    - Zone /56
      - SubZone /60
        - Network /64
  - Branch Site /56
    - Zone /60
      - Network /64



Umsetzung

Vorbereitungen - IOS-Updates

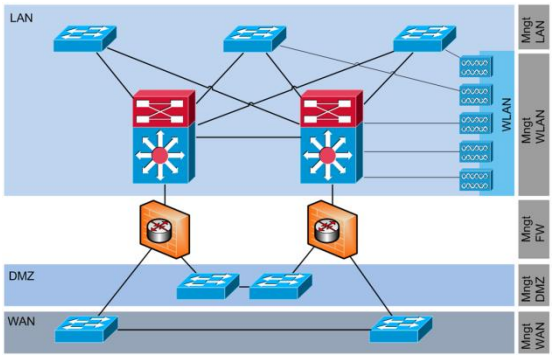
- Anfrage an Integrator (Januar 2013)

  „Für (erweiterte) IPv6-Funktionalität planen wir unsere Switches und Access Points zu upgraden. Gemäss Service-Vertrag würden wir dazu gerne bei XXX die benötigten IOS-Images beziehen. Ganz grob benötigen wir (vorerst) folgende Funktionalität:
  - RA Guard, DHCP Guard
  - Management via IPv6 (ssh, snmpv3, syslog)
  - HRSPv6
  - DHCPv6 relay agent

  Welche IOS-Versionen empfiehlt XXX hier?“
  …

- Empfehlung Integrator
  - Access Points: IOS 15.2.2-JB
  - Layer2-Switches: IOS 15.0.2-SE
  - Layer3-Switches: IOS 15.1.2-SG

- Upgrade des Netzwerks in Zürich Anfang März 2013



Umsetzung

Vorbereitungen - IOS-Updates – Erste Erfahrungen

- Kein IPv6-Support bei den Access Points

IOS 15.2(2)JB

```
CHZH01NAP01(config)#ip?
ip

CHZH01NAP01(config)#interface bvi1
CHZH01NAP01(config-if)#ip?
ip

CHZH01NAP01(config-if)#ip
```

- Seit Ende Juli nun mit IPv6-Support

IOS 15.2(4)JA1

```
CHZH01NAP01(config)#ip?
ip  iphc-profile  ipv6

CHZH01NAP01(config)#interface bvi1
CHZH01NAP01(config-if)#ip?
ip  iphc-profile  ipv6

CHZH01NAP01(config-if)#ip
```

Tipp (IPv4): Ab IOS 15 muss der Default-GW mittels `ip route` konfiguriert werden (`ip default-gateway`-Kommando funktioniert nicht mehr).

Tipp (SNMP): Nach IOS-Update hatten sich die Interface-Indexe geändert

Umsetzung

Vorbereitungen - IOS-Updates – Erste Erfahrungen

- Supported, Not Supported, …

New in Cisco IOS Release 15.0(2)SE

- *…*
- *Support for IOS IPv6 Host mode, which is compliant with the IPv6 Ready Logo Phase-2 Core Protocols test suite. (LAN Lite image for Catalyst 2960, 2960-C and 2960-S switches; IP Base image for Catalyst 3750, 3750v2, 3560, 3560v2 and 3650-C switches).*

```
CHZH01NWS01#show version
...
Switch Ports Model              SW Version            SW Image
------ ----- -----              ----------            ----------
*    1 26    WS-C2960-24TT-L    15.0(2)SE2            C2960-LANBASEK9-M
```

Umsetzung

Vorbereitungen - IOS-Updates – Erste Erfahrungen

- Catalyst 3560

```
CHZH01NDS01#show version
Cisco IOS Software, C3560 Software (C3560-IPBASEK9-M), Version 15.0(2)SE2,
  RELEASE SOFTWARE (fc1)
...
Model number                    : WS-C3560G-24TS-S
System serial number            : FOC0935U0W8
...
CHZH01NDS01#
```

- LLLYYWWSSSS
  - LLL: Produktionsort
  - YY: Produktionsjahr (01 = 1997, 02=1998, …)
  - SSSS: Seriennummernteil
  - ➢ Beachtlich: C3560 von 2005 unterstützen IPv6!

Tipp: Catalyst 2960 / 3560 – IPv6 muss ggf. erst noch aktiviert werden

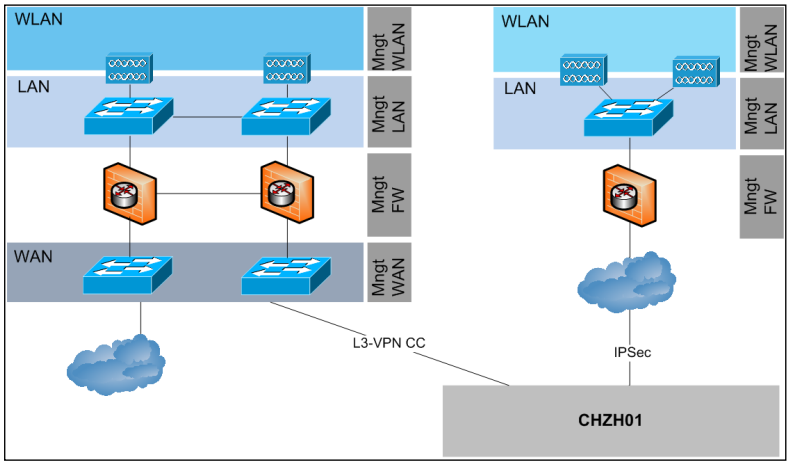
➢ `(config)# sdm prefer dual-ipv4-and-ipv6 [default,routing,vlan]`

Umsetzung

Vorbereitung – IPv6-Anbindung Aussenstandorte

- Kurz- und Mittelfristig:
  - Verwendung von IPv6-Adressen des Präfixes des Hauptstandortes
  - Routing zentral über Zürich
- Langfristig: ?

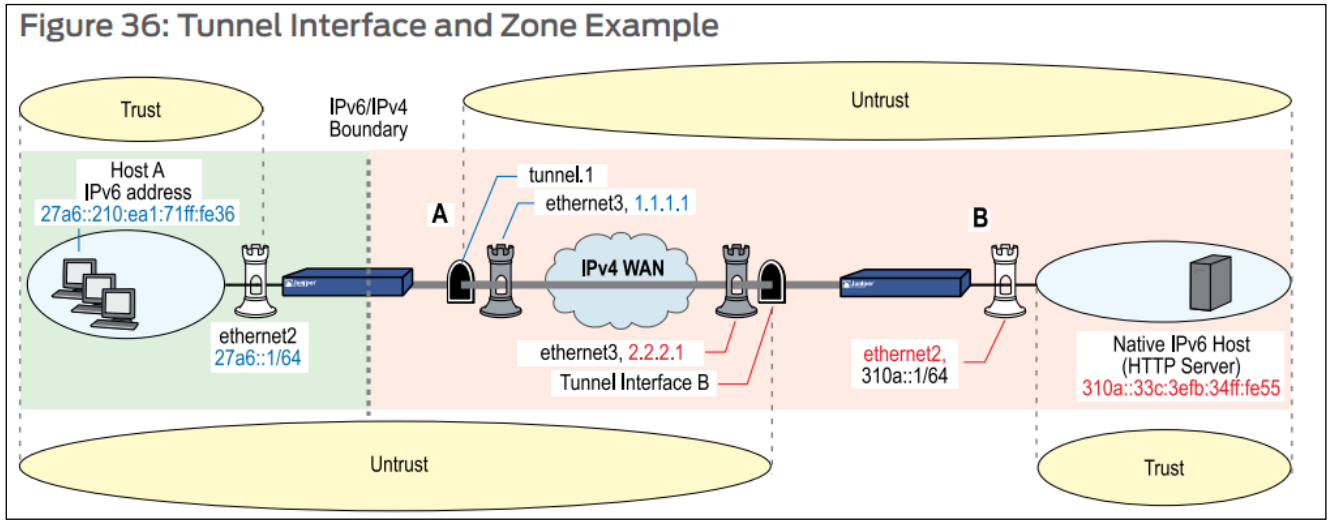
- IPv6 in Bern
  - Über Cablecom (IP VPN)
  - Unterstützt ab Q2-2014
- IPv6 in Basel
  - IPv6 über IPSec-Tunnel



Umsetzung

Vorbereitung – IPv6-Anbindung Aussenstandorte - Erfahrungen

- IPv6 in Basel
  - IPSec Endpunkte
    - Zürich: Juniper SSG-140 / Screenos 6.3.0r8.0
    - Basel: Juniper SRX-210HE / Junos 12.1R6.5
- ScreenOS
  - IPsec 6in4 Tunneling: *„You can use IPsec tunneling, which supports authentication and encryption, to encapsulate packets as the security device transmits them between remote IPv6 island networks over an IPv4 WAN.”*



Quelle: Juniper - Concepts & Examples, ScreenOS Reference Guide, Dual-Stack Architecture with IPv6

Umsetzung

Vorbereitung – IPv6-Anbindung Aussenstandorte - Erfahrungen

- Junos
  - Dokumentation im Web ✗
  - Informationen im Junos Security Buch ✗
  - Hm, Release Notes

IPv6 IPsec
The IPv6 IPsec implementation has the following limitations:
...
• The IPv6 IPsec VPN does not support the following functions:
- *4in6 and 6in4 policy-based site-to-site VPN, IKE*
- *4in6 and 6in4 route-based site-to-site VPN, IKE* ⬅
- *4in6 and 6in4 policy-based site-to-site VPN, Manual Key*
- *4in6 and 6in4 route-based site-to-site VPN, Manual Key* ⬅
- *…*

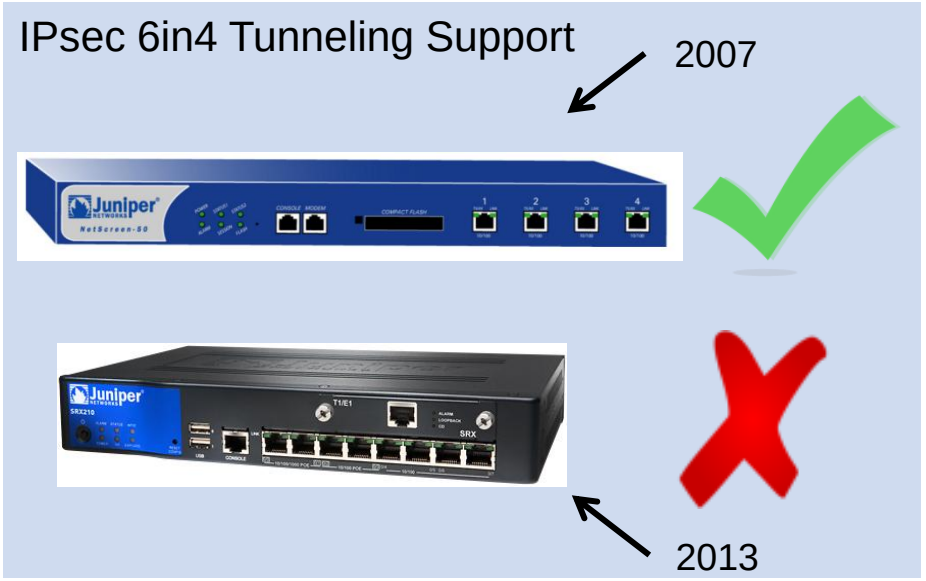
Quelle: https://www.juniper.net/techpubs/en_US/junos12.1/information-products/topic-collections/release-notes/12.1/junos-release-notes-12.1r6.pdf

➢ Vorerst Fokus auf Hauptstandort Zürich

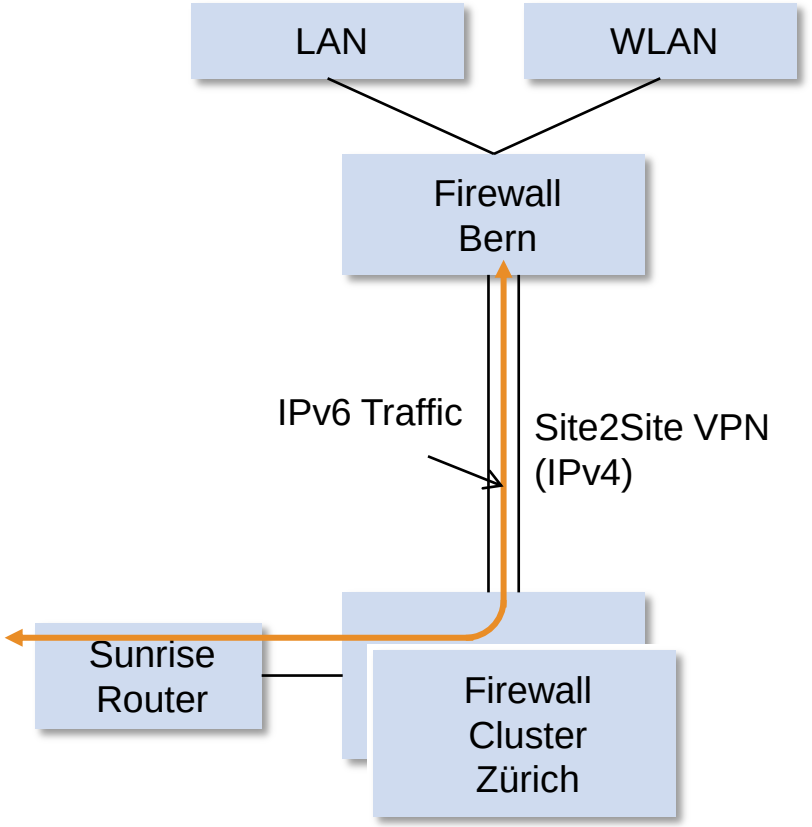
Netzwerk am Standort Bern (Planung)

IPv6-Konferenz 2011

- IPv6 Zugang für Mitarbeiter im Büro Bern
  - Derzeit kein IPv6-Internetzugang in Bern vorhanden
  - IPv6 in IPv4 Tunnel ZH <-> Bern
  - IPv6 Zugang im WLAN in Bern



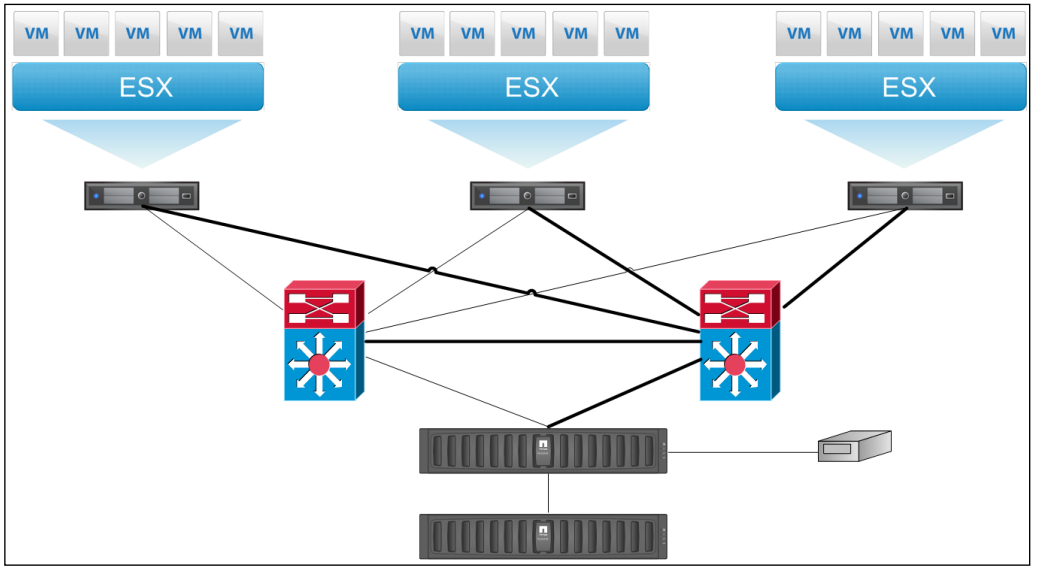
Quelle: https://www.juniper.net



Umsetzung

Vorbereitungen - Server

- Ubuntu 12.04.3 LTS
- Virtuelle Maschine:
  - Intel Xeon CPU 2.13GHz
  - 2GB Ram
  - 15GB HD
  - 2 Netzwerkkarten
    - eth0: Nur IPv4, Admin-Interface
    - eth1: Dualstack



Umsetzung

NTP

- Default-Daemon ntp installiert
- ntp Daemon öffnet v4 und v6 Socket

```
# /etc/ntp.conf, configuration for ntpd; see ntp.conf(5) for help
…
# Use servers from the NTP Pool Project. Approved by Ubuntu Technical Board
# on 2011-02-08 (LP: #104525). See http://www.pool.ntp.org/join.html for
# more information.
server 0.ch.pool.ntp.org
server 1.ch.pool.ntp.org
server 2.ch.pool.ntp.org
server 3.ch.pool.ntp.org


root@Monitoring01:/home/mug# lsof -i | grep ntpd
ntpd      2818            ntp   16u  IPv4  12580      0t0  UDP *:ntp
ntpd      2818            ntp   17u  IPv6  12581      0t0  UDP *:ntp
```

Umsetzung

NTP – Erfahrungen

- Access Points (IOS 15.2(4)JA1)
  - Unterstützen lediglich sntp (simple network time protocol)
  - Cisco‘s aktuelle Implementierung unterstützt kein IPv6

```
CHZH01NAP01(config)#sntp server ?
  Hostname or A.B.C.D  Name or IP address of server

CHZH01NAP01(config)#sntp server 2001:1702:6:1191::101
                                ^
% Invalid input detected at '^' marker.
```

- Catalyst 2960, 3560 und 4500

```
ntp source Vlan1111
ntp server 2001:1702:6:1191::101
```

Umsetzung

NTP – Erfahrungen

- Test: Catalyst 2960 und 3560 (IOS 15.0(2)SE2)

```
CHZH01NAS01#show ntp status
Clock is synchronized, stratum 3, reference is 19.51.5.5
…
system poll interval is 64, last update was 9 sec ago.
```

```
CHZH01NAS01#show ntp associations

  address         ref clock       st   when   poll reach  delay  offset   disp
*~2001:1702:6:1191::101
                  62.2.207.85      2     18     64     1  3.000  55.057  0.119
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
```

- Whois-Abfrage von 19.51.5.5
  - OrgName: Ford Motor Company
- Ändern der NTP-Server Adresse: 2001:1702:6:1191::10**2**
  - Reference nun: 49.63.200.148
  - Descr: Korea Telecom Freetel Corp

NTP Version 4 Release Notes – Nasty Surprises

There is a minor change to the reference ID field of the NTP packet header when operating with IPv6 associations. **In IPv4 associations this field contains the 32-bit IPv4 address of the server**, in order to detect and avoid loops. **In IPv6 associations this field contains the first 32-bits of a MD5 hash formed from the IPv6 address**

Umsetzung

NTP - Erfahrungen

- Test: Catalyst 4500 (IOS 15.2(1)E)

```
CHZH01NCS01#show run | include ntp
ntp source Vlan1191
ntp update-calendar
ntp server 2001:1702:6:1191::101
```

  - NTP über IPv6 funktioniert nicht
  - *debug ntp all* liefert keinerlei Output
  - NTP-Server pingbar, ntp über v4 funktioniert auch problemlos
  - Keine einschränkenden Acces-Lists

```
CHZH01NCS01#ping 2001:1702:6:1191::101 source vlan 1191
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:1702:6:1191::101, timeout is 2 seconds:
Packet sent with a source address of 2001:1702:6:1191::10
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Umsetzung

Rancid

- Zweck
  - Automatische Sicherung der Konfigurationen der Netzwerkelemente
  - Versionierung (CVS)
- IPv6-Spezifische Konfiguration
  - keine, Konfiguration mittels FQDNs
- Im Betrieb
  - Rancid löst FQDNs auf
  - Verbindungsaufbau zu Netzwerkelementen mit SSH (IPv6 wird präferiert)

```
# less var/lib/rancid/CHZH01/router.db
CHZH01NFW01.awkgroup.com:netscreen:up
CHZH01NFW02.awkgroup.com:netscreen:up

CHZH01NCS01.awkgroup.com:cisco:up
CHZH01NCS02.awkgroup.com:cisco:up
…
```

```
# less /etc/hosts
# --- CHZH01 ---

# Core Switches
10.1.224.11             CHZH01NCS01.awkgroup.com   CHZH01NCS01
…
# IPv6
# Core Switches
2001:1702:6:1111::11    CHZH01NCS01.awkgroup.com   CHZH01NCS01
```

Umsetzung

Rancid - Erfahrungen

- Funktioniert problemlos mit
  - Aironet 1142N
  - Catalyst 2960
  - Catalyst 3560
  - Catalyst 4500
- Funktioniert nicht mit
  - Catalyst 2960S

```
CHZH01NAS01(config)#ipv6 access-list
                                   ^
% Invalid input detected at '^' marker.
```

- Begründung Cisco
  - Lanlite-Modell (S)
  - Lanlite Image unterstützt offiziell keine Access Lists

Umsetzung

Rancid - Erfahrungen

- Rancid – Your Network Monitoring Tool (-:

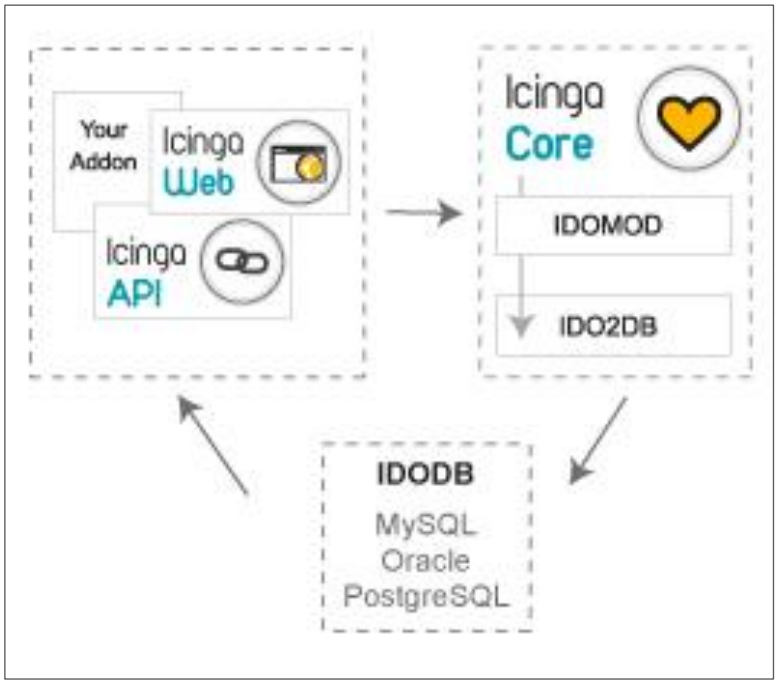
```
Index: configs/chzh01nap03.awkgroup.com
===================================================================
retrieving revision 1.8
diff -u -4 -r1.8 chzh01nap03.awkgroup.com @@ -29,16 +29,22 @@
  !Flash: Directory of flash:/
  !Flash:     2  -rwx        8271  Oct 20 2013 23:35:36 +02:00  config.txt
  !Flash:     3  -rwx           4  Jul 15 2013 10:28:29 +02:00  FOC14314YHN
  !Flash:     4  -rwx    10868774  Oct 20 2013 23:13:14 +02:00  c1140-k9w7-mx.152-4.JA1
+ !Flash:     5  -rwx      295219   Nov 4 2013 19:49:50 +01:00  ap_log_r0_0.log
  !Flash:     6  -rwx        3096  Oct 20 2013 23:35:36 +02:00  private-multiple-fs
  !Flash:     7  drwx         256   Mar 1 2002 01:13:56 +01:00  c1140-k9w7-mx.124-21a.JA1
  !Flash:   155  -rwx         360   Mar 1 1993 01:00:17 +01:00  env_vars
  !Flash:   156  -rwx      186308  Oct 20 2013 23:30:18 +02:00  8001.img
  !Flash:   157  -rwx        8080  Oct 20 2013 23:30:35 +02:00  T2.bin
  !Flash:   158  -rwx       23836  Oct 20 2013 23:30:49 +02:00  T5.bin
  !Flash:   159  -rwx        5672  Oct 20 2013 23:35:36 +02:00  private-config
- !Flash: 32126976 bytes total (15475712 bytes free)
+ !Flash:   160  -rwx      113277   Nov 4 2013 19:49:53 +01:00  event.r0
+ !Flash:   161  -rwx      295219   Nov 4 2013 19:49:54 +01:00  ap_log_r0_1.log
+ !Flash:   162  -rwx      295219   Nov 4 2013 19:49:55 +01:00  ap_log_r0_2.log
…
```

Radio d0 reset: transmitter seems to have stopped

Umsetzung

Icinga

- OpenSource Montoring System
- Gründe für Icinga
  - Icinga Core unterstützt IPv6
  - Modernes Web-Interface
  - Gute Dokumentation
  - Rückwärtskompatible mit Nagios Plugins
  - Unterstützt auch Oracle und PostgreSQL



Architektur (Quelle: https://www.icinga.org)

- In der AWK Group eingesetzt für
  - Host-Alive-Abfragen via ICMP Ping
  - Parameter-Abfragen der Netzwerkelemente mittels SNMP
  - Nicht verwendet: SNMP Traps

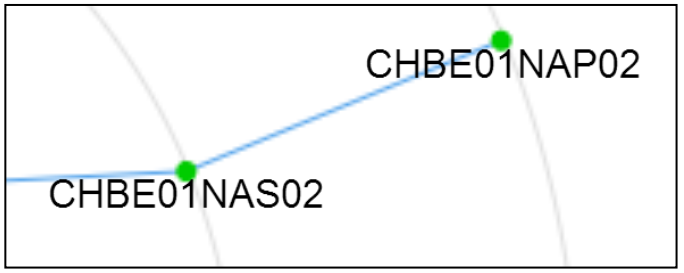
Umsetzung

Icinga

- Host / Service Modell
  - Mittels Host wir ein Netzwerkelement definiert
  - Anschliessend können einem Host Services zugeordnet werden

Host	Service	Status	Last Check	Duration	Attempt	Status Information
CHBE01NAP01	Bridge AWKWLAN - Status	OK	2013-11-20 07:49:41	1d 8h 57m 3s	1/4	SNMP OK - result:1 match:none
	Bridge AWKWLAN NB - Status	OK	2013-11-20 07:49:41	1d 8h 57m 3s	1/4	SNMP OK - result:1 match:none
	CPU Load - Percentage	OK	2013-11-20 07:51:32	22d 6h 20m 40s	1/4	SNMP OK - result:0 match:none
	Radio 0 - Status [2.4GHz]	OK	2013-11-20 07:51:32	22d 6h 20m 40s	1/4	SNMP OK - result:1 match:none
	Radio 1 - Associations [5.0GHz]	OK	2013-11-20 07:49:59	1d 8h 56m 45s	1/4	SNMP OK - result:0 match:none

- Parents
  - Alle Parents ‚down‘
    - ➢ Host ‚unreachable‘ (und nicht ‚down‘)



Umsetzung

Icinga – IPv6

- Host Definition

```
define host{
                host_name       CHZH01NAP01
                alias           Access Point 01
                address         10.1.225.21
                address6        2001:1702:6:1121::21
                parents         CHZH01NCS02
                notes_url       http://monitoring01/munin/CHZH01/CHZH01NAP01/index.html
                use             template_network_generic
}
```

- Plugins mit IPv6-Unterstützung
  - check_ping
  - check_snmp
  - check_multi // noch nicht getestet

Umsetzung

Icinga – IPv6 – Erfahrungen

- IP-Adresse / Hostname als Parameter

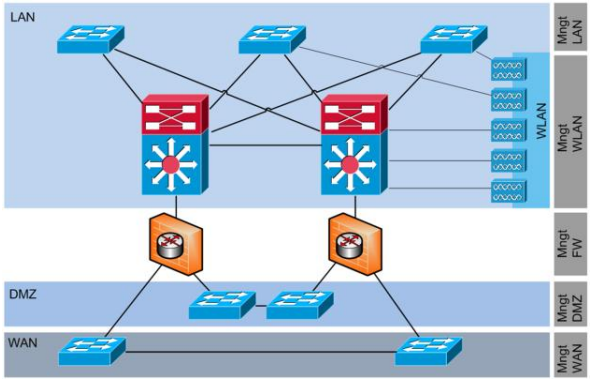
Plugin	IPv6-Adresse	Hostname / FQDN (IPv4 & IPv6)
check_ping	2001:db8::1	foo.example.com
check_snmp	upd6:[2001:db8::1]	udp6:foo.example.com

  - Bemerkungen
    - Bei check_ping kann bei Verwendung des Hostnamen IPv4 mittels Option verwendet werden (-4)
    - Syntax bei check_snmp: Ist lediglich ein Wrapper, es wird net-snmp für die eigentlich SNMP-Abfrage verwendet

Umsetzung

Iciniga – IPv6 – Erfahrungen

- HSRP
  - Schutz vor ‚1st-hop'- Ausfällen
  - IPv6-Support erst mit HSRP Version 2
  - Eine Standby-Gruppe pro Protokol (v4/v6)
- SNMP
  - Zustand von IPv6-Standby-Gruppen kann nicht abgefragt werden
  - Feedback Cisco: Für Catalyst 4500 / Sup 6L-E erst Q2 / 2014




```
interface Vlan1191
 description HSRP DS Interface VLAN 1191
…
 standby version 2
 standby 1191 ipv6 FE80::1191:0:0:10
 standby 1191 ipv6 2001:1702:6:1191::10/64
 standby 1191 timers 1 3
 standby 1191 priority 110
 standby 1191 preempt delay minimum 60
 ipv6 address FE80::1191:0:0:11 link-local
 ipv6 address 2001:1702:6:1191::11/64
 ipv6 nd router-preference High
…
End
```

Hilfreich: VLAN-ID in link local Adresse enkodieren

```
IP6 fe80::1191:0:0:10 > ff02::1:
ICMP6, router advertisement,
length 64
```

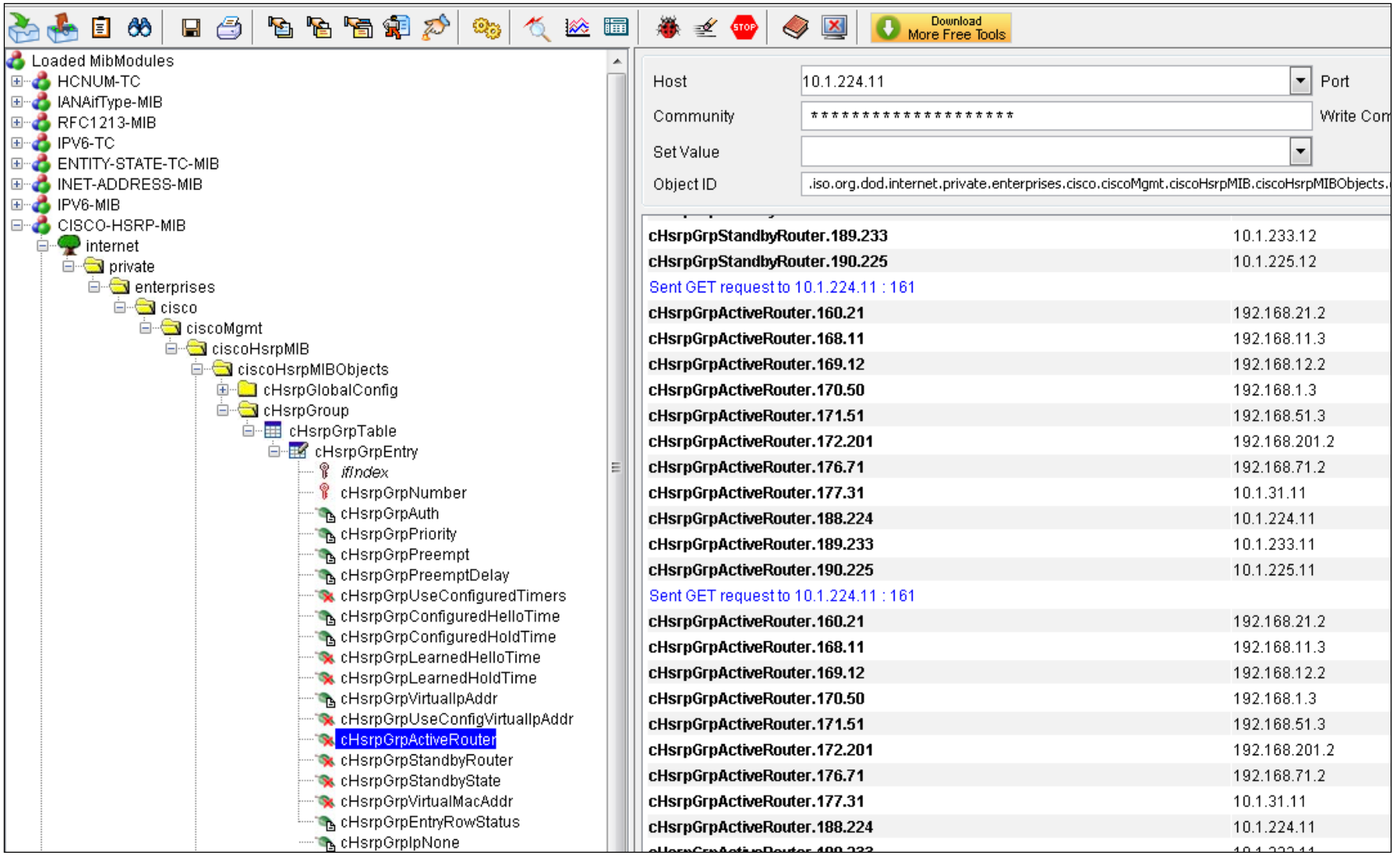
Umsetzung

Icinga – IPv6 – Erfahrungen

```
CHZH01NCS01#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp   Pri P State   Active          Standby         Virtual IP
Vl11        11    110  P Active  local           192.168.11.2    192.168.11.1
Vl12        12    90     Standby 192.168.12.2    local           192.168.12.1
Vl21        21    90     Standby 192.168.21.2    local           192.168.21.1
Vl31        31    110  P Active  local           192.168.31.2    192.168.31.1
Vl50        50    110  P Active  local           192.168.1.2     192.168.1.1
Vl51        51    110  P Active  local           192.168.51.2    192.168.51.1
Vl71        71    90     Standby 192.168.71.2    local           192.168.71.1
Vl201       201   90     Standby 192.168.201.2   local           192.168.201.1
Vl201       1001  90     Standby FE80::201:0:0:22 local          FE80::201:0:0:20
Vl1111      224   110  P Active  local           10.1.224.12     10.1.224.10
Vl1111      1111  110  P Active  local           FE80::1111:0:0:12 FE80::1111:0:0:10
Vl1121      225   110  P Active  local           10.1.225.12     10.1.225.10
Vl1121      1121  110  P Active  local           FE80::1121:0:0:12 FE80::1121:0:0:10
Vl1191      233   110  P Active  local           10.1.233.12     10.1.233.10
Vl1191      1191  110  P Active  local           FE80::1191:0:0:12 FE80::1191:0:0:10
CHZH01NCS01#
```

Umsetzung

Icinga – Erfahrungen



Umsetzung

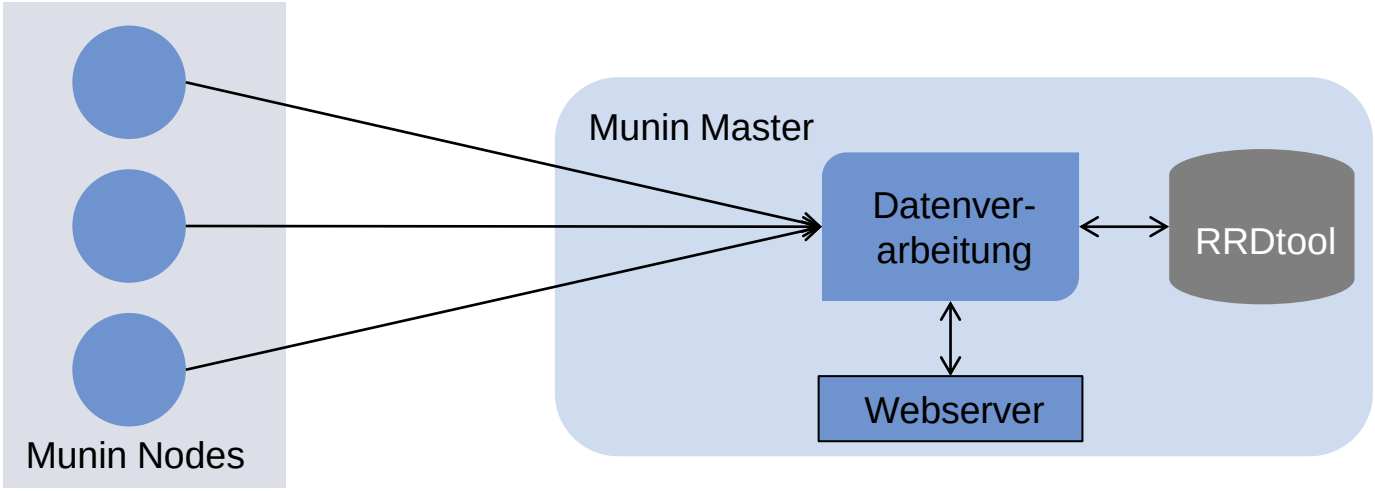
Icinga – Erfahrungen

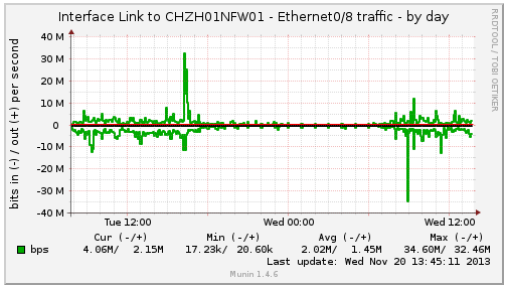
```
.iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.
    - ciscoHsrpMIB.
        -ciscoHsrpMIBObjects.
            -cHsrpGroup.
                -cHsrpGrpTable.
                    -cHsrpGrpEntry.
                        -cHsrpGrpActiveRouter

root@Monitoring01:~# snmpwalk UDP6:[2001:1702:6:1191::11] .1.3.6.1.4.1.9.9.106.1.2.1.1.13
SNMPv2-SMI::enterprises.9.9.106.1.2.1.1.13.160.21 = IpAddress: 192.168.21.2
SNMPv2-SMI::enterprises.9.9.106.1.2.1.1.13.168.11 = IpAddress: 192.168.11.3
SNMPv2-SMI::enterprises.9.9.106.1.2.1.1.13.169.12 = IpAddress: 192.168.12.2
SNMPv2-SMI::enterprises.9.9.106.1.2.1.1.13.170.50 = IpAddress: 192.168.1.3
SNMPv2-SMI::enterprises.9.9.106.1.2.1.1.13.171.51 = IpAddress: 192.168.51.3
SNMPv2-SMI::enterprises.9.9.106.1.2.1.1.13.172.201 = IpAddress: 192.168.201.2
SNMPv2-SMI::enterprises.9.9.106.1.2.1.1.13.176.71 = IpAddress: 192.168.71.2
SNMPv2-SMI::enterprises.9.9.106.1.2.1.1.13.177.31 = IpAddress: 192.168.31.3
SNMPv2-SMI::enterprises.9.9.106.1.2.1.1.13.188.224 = IpAddress: 10.1.224.11
SNMPv2-SMI::enterprises.9.9.106.1.2.1.1.13.189.233 = IpAddress: 10.1.233.11
SNMPv2-SMI::enterprises.9.9.106.1.2.1.1.13.190.225 = IpAddress: 10.1.225.11
root@Monitoring01:~# $
```

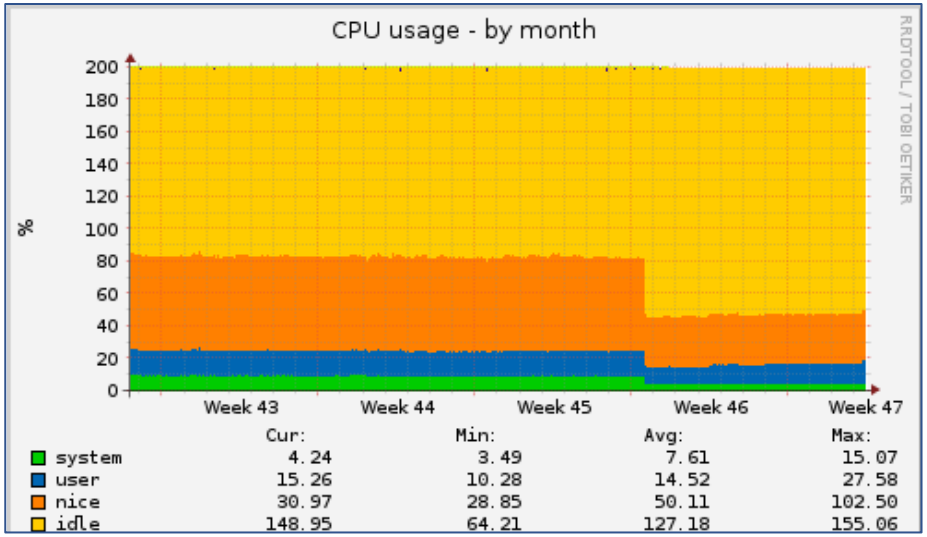
Umsetzung

Munin





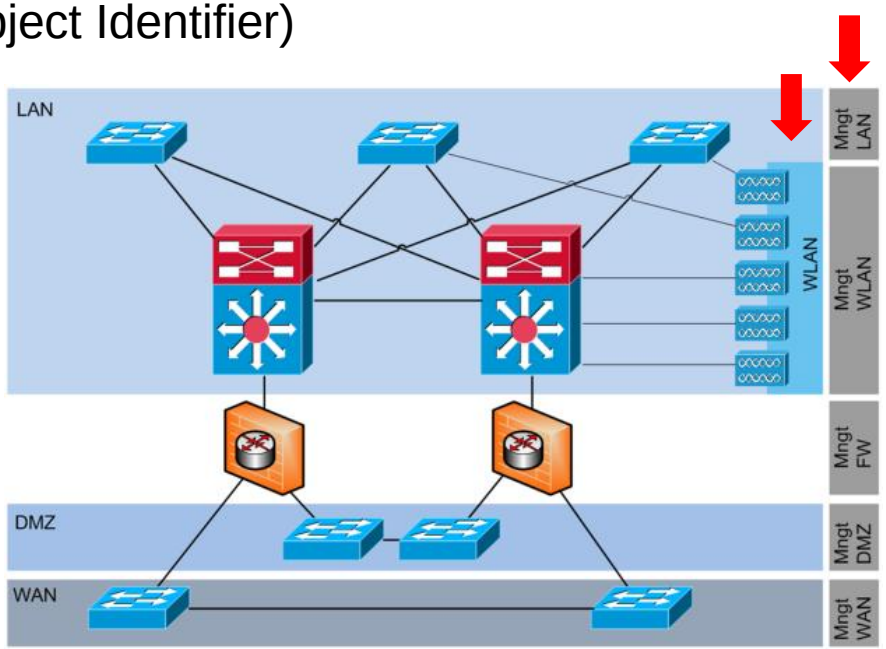
- Nachteile (Version 1.4.6)
  - Keine IPv6 Unterstützung
  - Keine SNMPv3-Unterstützung
  - Skaliert nicht
- Warum dann überhaupt?



Umsetzung

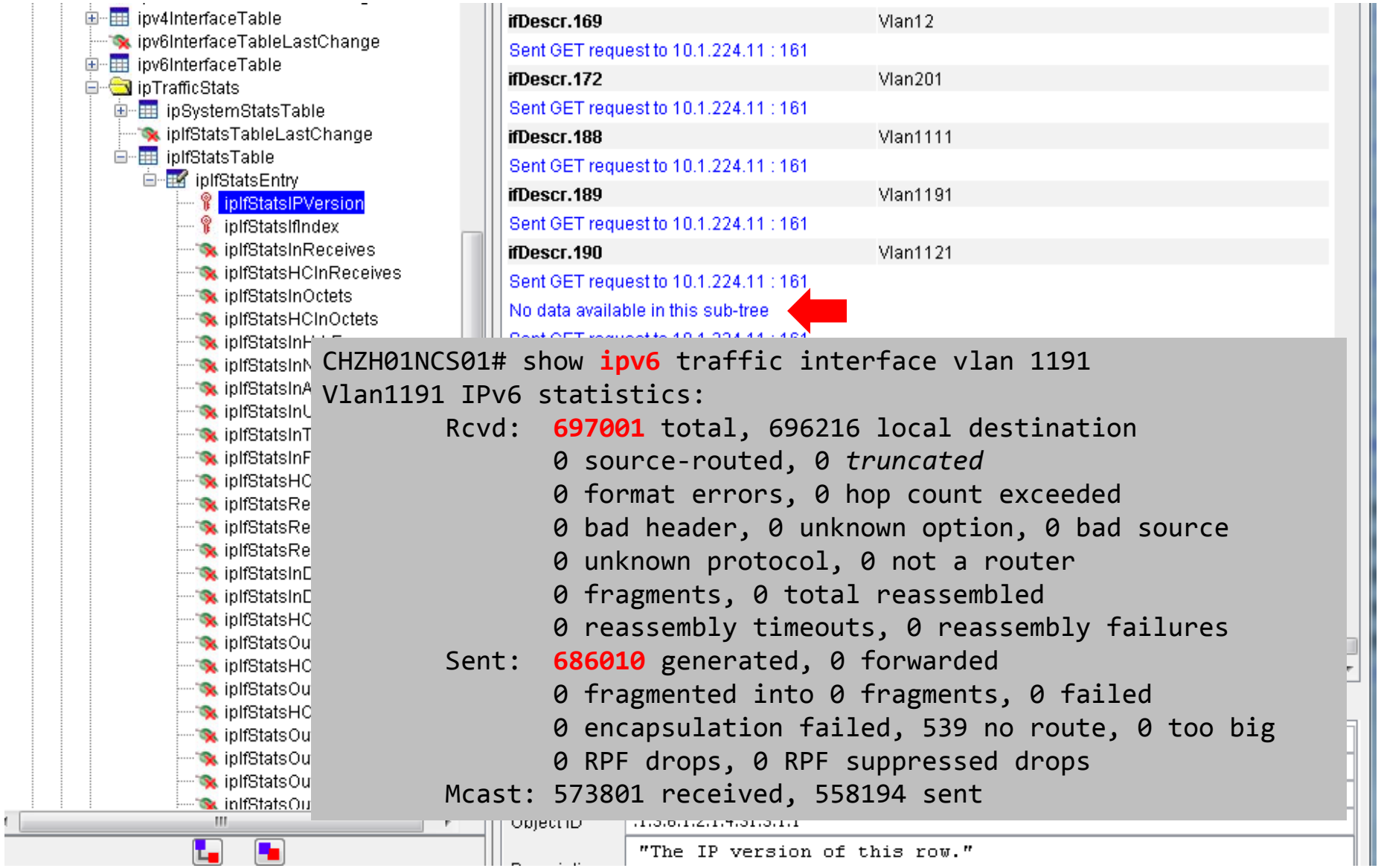
Munin – Erfahrungen

- Ziel: Darstellung von IPv4 und IPv6 Traffic
  - IPv6 Traffic heute
    - AWK WLAN
    - AWK Management Netzwerk
- Vorgehen
  1. Ermittlung der entsprechenden OIDs (Object Identifier)
  2. Erstellung von Graphen



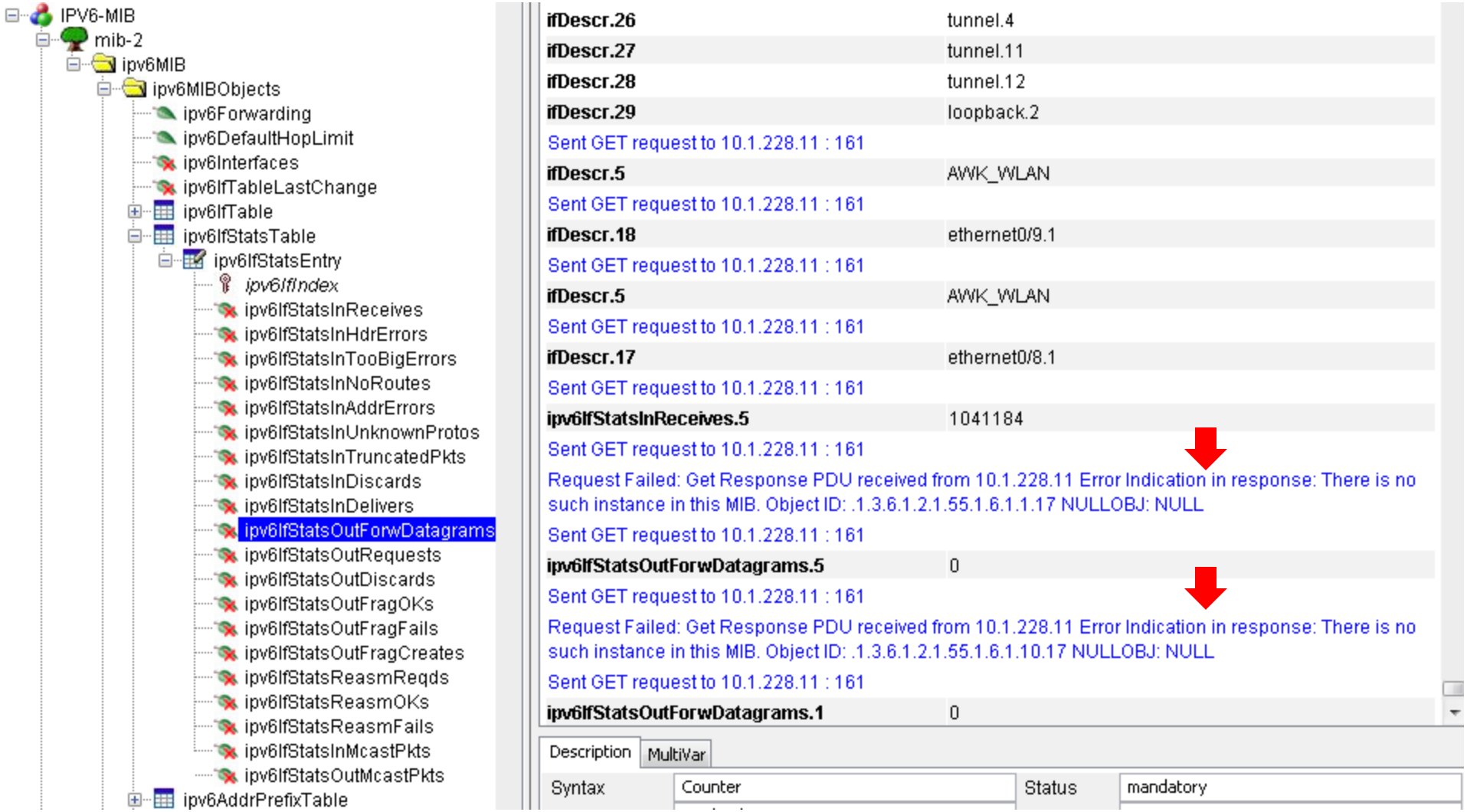
Umsetzung

Munin – Erfahrungen – Catalyst 4500 & IP-MIB



Umsetzung

Munin – Erfahrungen – SSG-140 & IPv6-MIB



Umsetzung

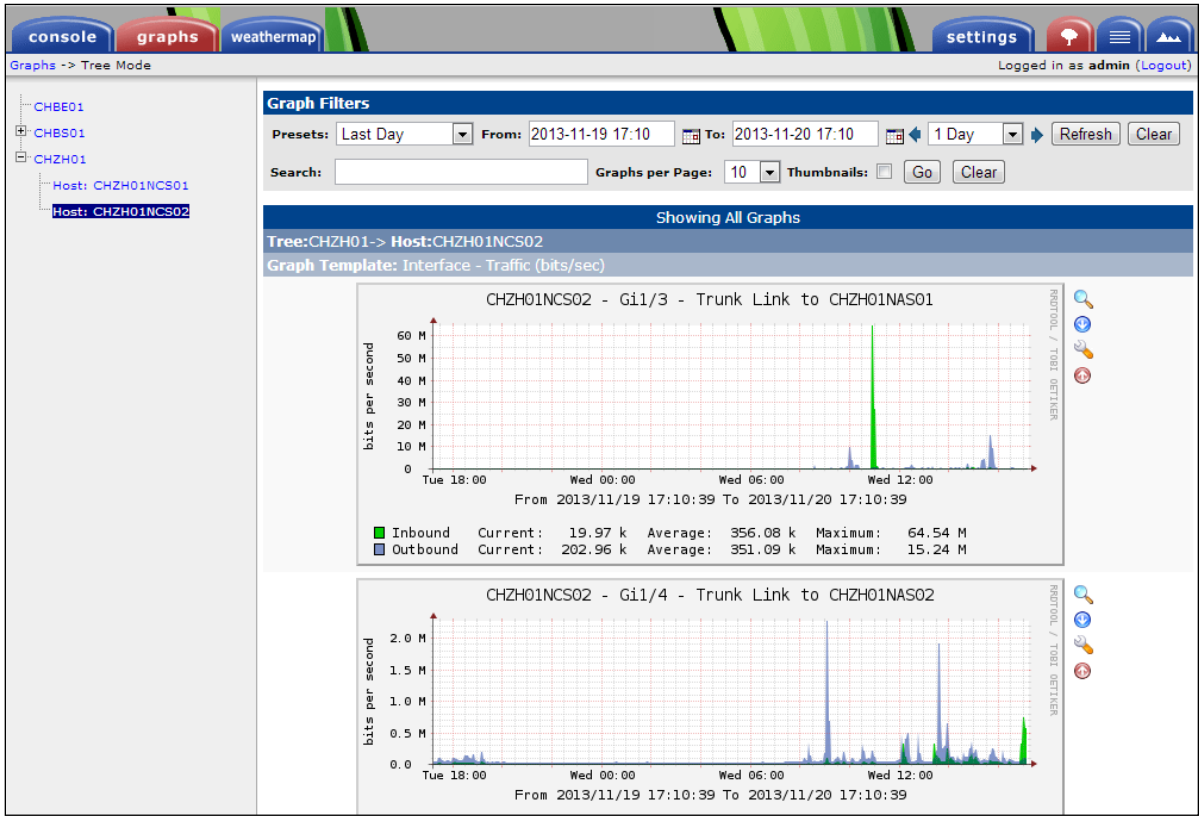
Munin – Erfahrungen – Ubuntu 12.04

- Abfrage möglich mit
  - IP-MIB
  - IPv6-MIB
- /proc/net
  - snmp: IPv4-Zähler System
  - snmp6: IPv6-Zähler System
  - dev_snmp6/
    - eth0 Interface-spezifische Zähler IPv6
    - Eth1 Interface-spezifische Zähler IPv6
- Interface-spezifische Zähler werden bei einem SNMP Walk nicht aufgeführt, nur die System-Zähler

Umsetzung

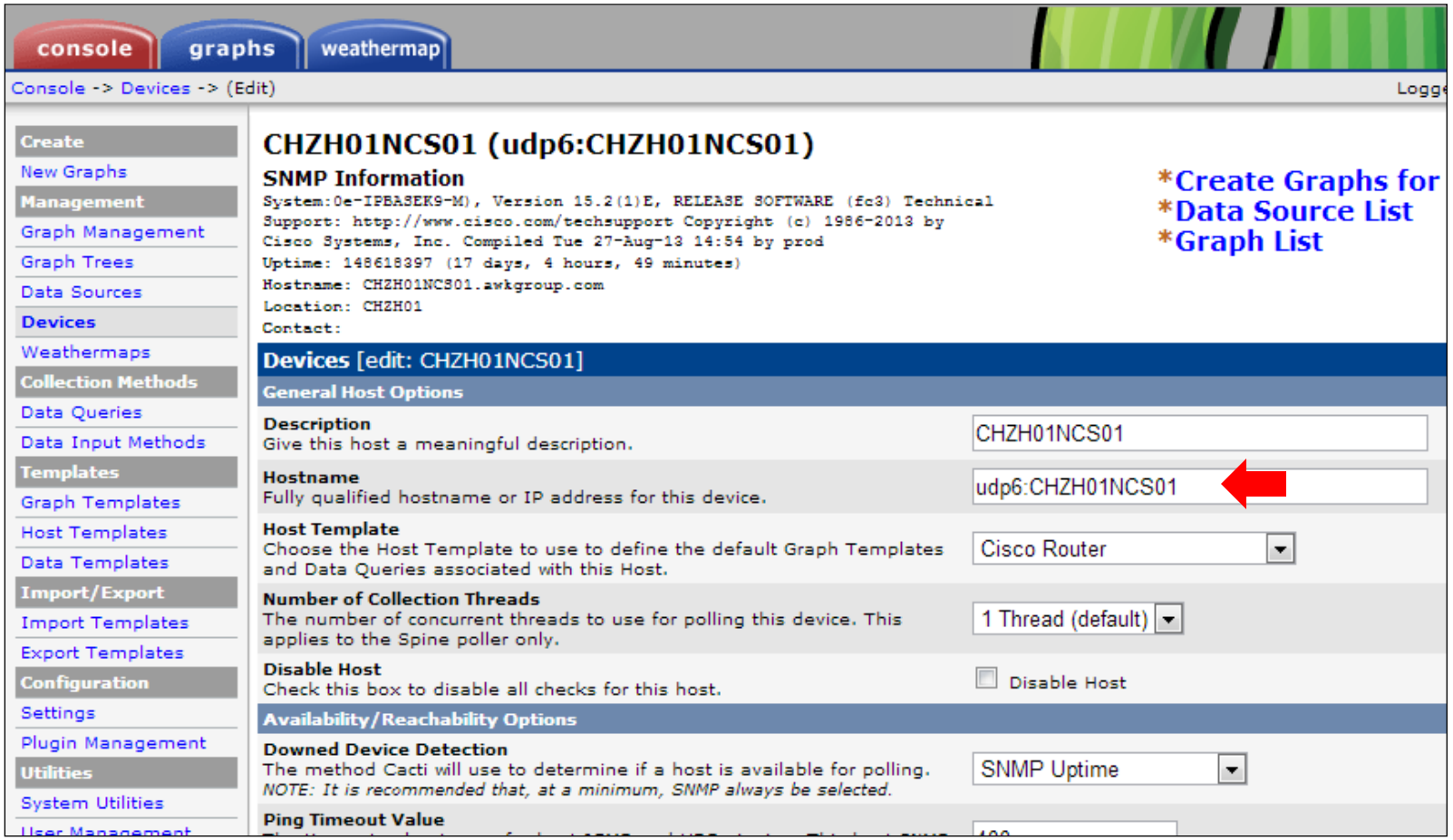
Cacti (Work in Progress)

- Graphische Darstellung von (Netzwerk-)Messwerten
- Sehr ausgereiftes GUI
- SNMPv3-Unterstützung



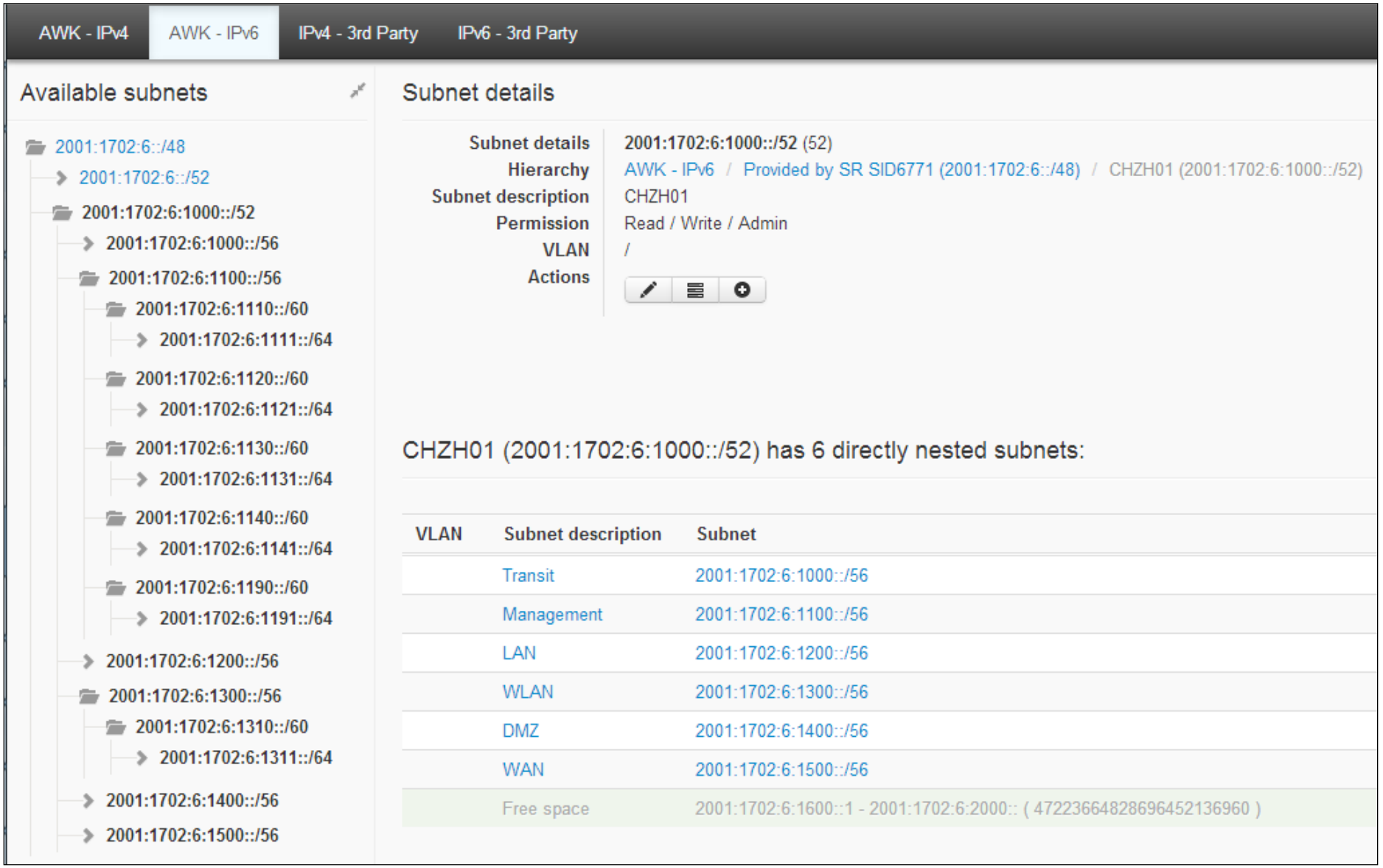
Cacti – Erfahrungen

- Unterstützt SNMP-Abfragen über IPv6
- Eingabe des Hostnamens mit Präfix udp6:



Umsetzung

phpIPAM



Demo

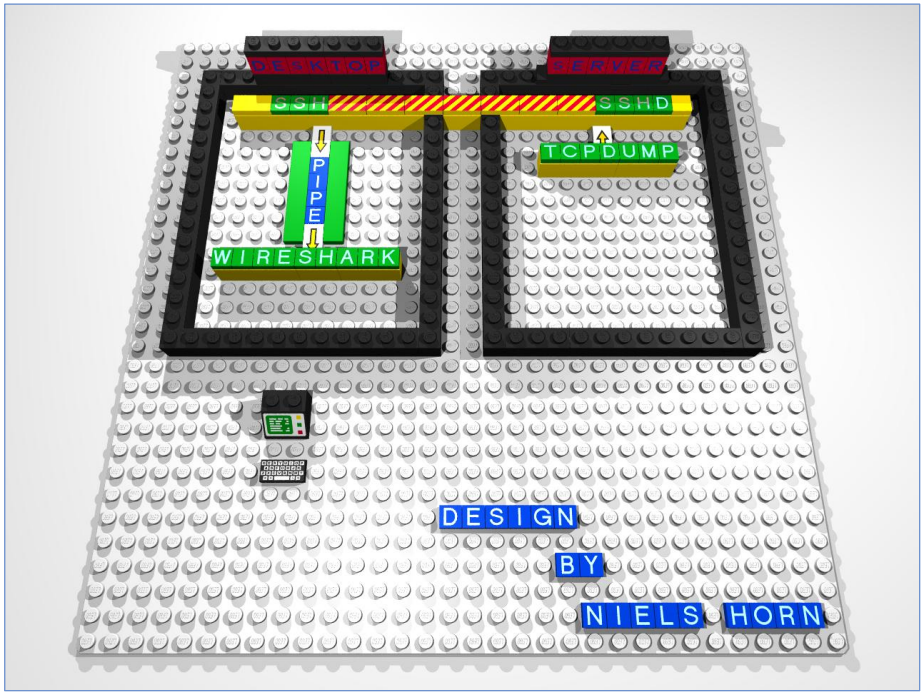
Demo

- Rancid
- Icinga
- Munin
- phpIPAM
- Cacti
- plink
  - ssh chzh01nap01
  - ssh -4 chzh01nap01
  - CHZH01NCS01: shutdown vlan 1191

Demo

Traffic-Tunneling

- plink (Teil der Putty-Tools): Tunneln von (Binär)-Daten:
  - *plink.exe -ssh -pw <Passwort> <username>@<Server-IP/FQDN> "tcpdump -ni eth1 -s 0 -U –w - " | "C:\Program Files\Wireshark\Wireshark.exe" -k -i –*
  - tcpdump wird auf entferntem Server gestartet, raw-Output über den SSH-Tunnel zum lokalen Desktop transportiert und hier in Wireshark angezeigt

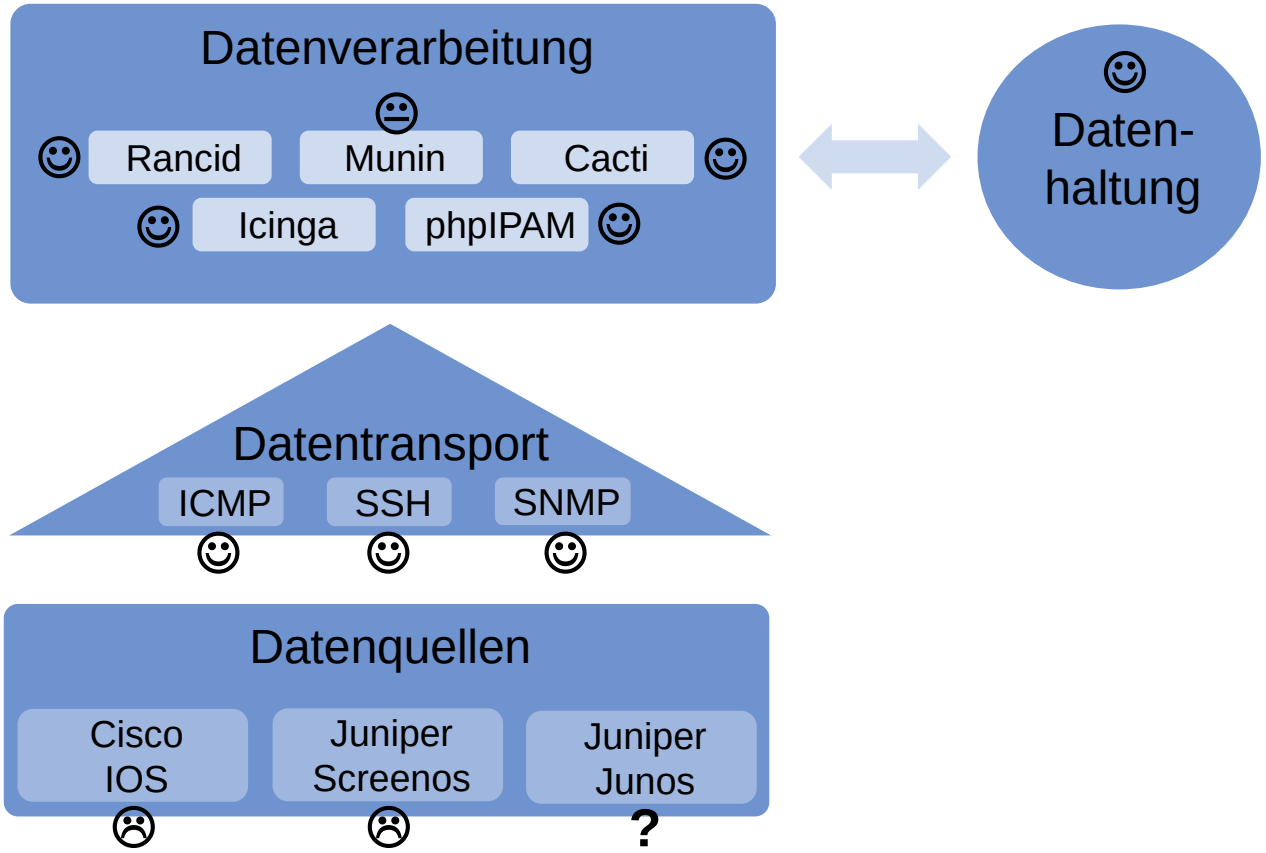


Zusammenfassung und Ausblick

Zusammenfassung

Vorgestellte Anwendungen

- Positiv
- Negativ
  - Verfügbare Informationen
  - OIDs / MIBs
  - Hersteller-Support



- Zusammengefasst
  - Datentransport, Datenverarbeitung und Datenhaltung
  - Bereitstellung IPv6-relevanter Information der Datenquellen

Ausblick

- Aktivitäten 2014
  - Neue Firewalls
  - Security-Features aktivieren
  - IPv6 für Mail-Gateways (IronPort)
  - Dokumentationen aktualisieren
- Knacknuss IPv6-Adressen
  - PI vs. PA
    - Beibehalten des PA-Bereichs
    - Antrag für PI-Bereich
  - /48 gross genug?
    - Eigentlich schon
    - Routing Aussenstandorte?
  - ➢ Je später hier eine Entscheidung getroffen wird, desto aufwendiger

THE END

Vergebens, dass ihr ringsum wissenschaftlich schweift,
Ein jeder lernt nur, was er lernen kann;
Doch der den Augenblick ergreift,
Das ist der recht Mann.

(Goethe, Faust 1, 2038f)

Anhang

HW / SW der Netzwerkelemente

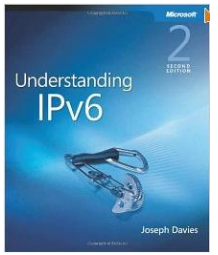
Hersteller	Gerät	SW-Version	Typ
Cisco	AP1142N-E-K9	IOS 12.4(21a)JA1 IOS 15.2(4)JA1	Access-Point
Cisco	C2960S-48TS-S (lanlite)	IOS 12.2(55)SE5 IOS 15.0(2)SE	Layer2-Switch
Cisco	C2960-8TC-S	IOS 12.2(55)SE5	Layer2-Switch
Cisco	C3560G-24TS	IOS 15.0(2)SE2	Layer2-Switch
Cisco	C2960-24TT-L	IOS 15.0(2)SE2	Layer2-Switch
Cisco	C4506-E (Sup 6L-E)	IOS 15.2(1)E	Layer3-Switch
Juniper	SSG-140	ScreenOS 6.3.0r8.0	Firewall
Juniper	SRX210HE	Junos 11.2R4.3 Junos 12.1R6.5	Firewall

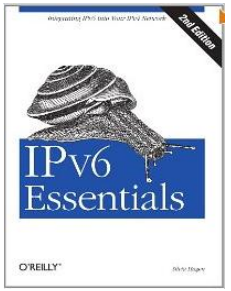
Online Demo-Versionen der vorgestellten Tools

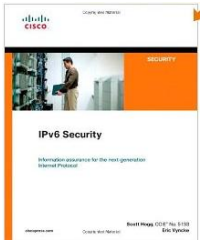
- Icinga
  - http://web.demo.icinga.org/icinga-web/
  - http://classic.demo.icinga.org/icinga/
- Munin
  - http://demo.munin-monitoring.org/munin-monitoring.org/demo.munin-monitoring.org/index.html
- phpIPAM
  - http://demo.phpipam.net/login/

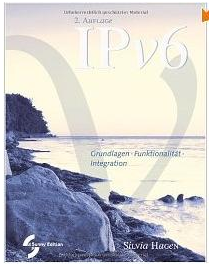
Recommended Reading

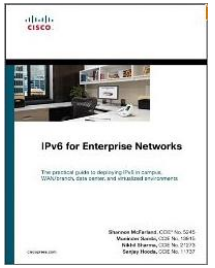
- Understanding IPv6, Second Edition
  - ISBN-13: 978-0735624467
- IPv6 Essentials
  - ISBN-13: 978-0596100582
- IPv6 Security
  - ISBN-13: 978-1587055942
- IPv6. Grundlagen - Funktionalität - Integration
  - ISBN-13: 978-3952294222
- IPv6 for Enterprise Networks
  - ISBN-13: 978-1587142277
- Planning for IPv6
  - ISBN-13: 978-1449305390

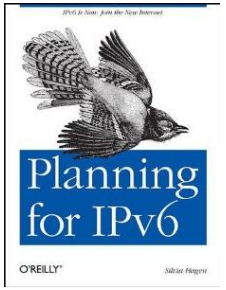












Recommended Reading

- IPv6 Fundamentals
  - ISBN-13: 978-1-58714-313-7
- Junos Security
  - ISBN-13: 978-1-449-38171-4
- ScreenOS Cookbook
  - ISBN-13: 978-0-596-51003-9
- Munin: Graphisches Netzwerk- und System-Monitoring
  - ISBN-13: 978-3-937-51448-2
- Essential SNMP – 2nd Edition
  - ISBN-13: 978-0-596-00840-6