.1.3.6.1.2.1.4.31.1.1 - Hello, anybody there?

Troopers 2015

Gabriel Müller, Senior Consultant

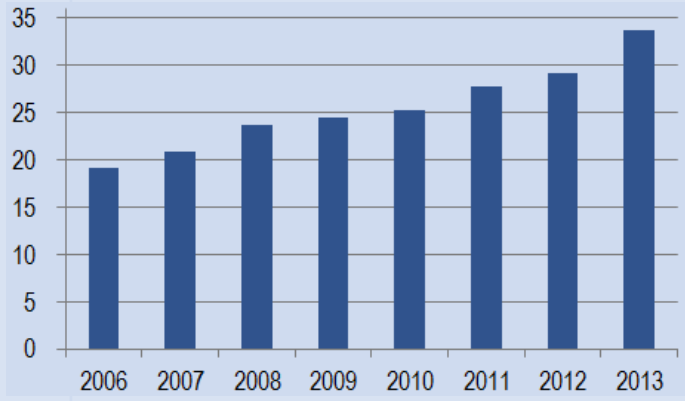
AWK GROUP
Consulting | Engineering | Project Management

Facts and figures

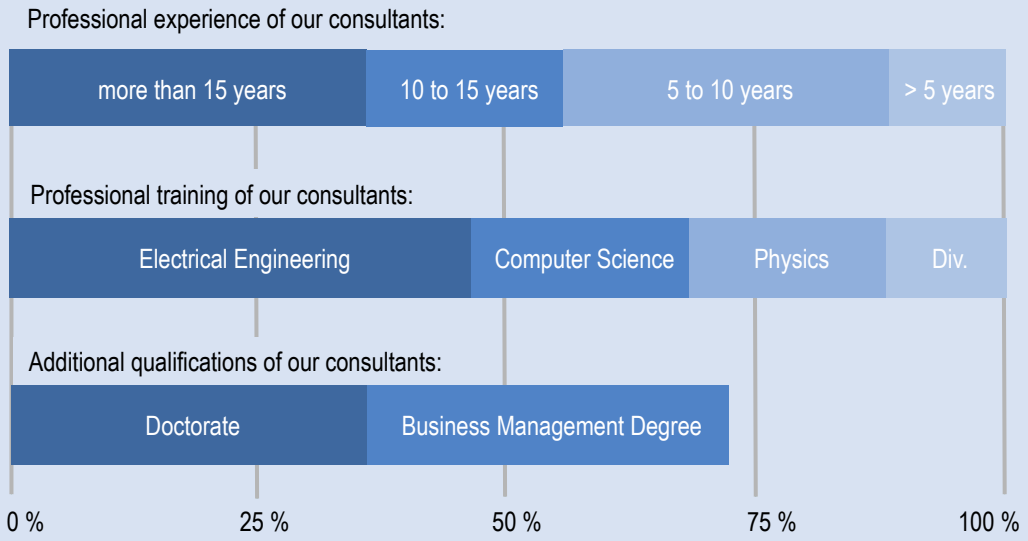
AWK Group AG

Activity	Consultancy, engineering and project management for information technology from a single source
Owner	The share capital is wholly owned by the partners
Founded in	1986
Employees	Over 150 staff
Clients	Over 400
Projects	Over 4,000
Site Locations	Zurich, Berne, Basle, Lausanne
International Network	Member of ITIC GROUP, an international network of independent consultancy firms

Turnover



Background of our consultants



Partners of AWK

From left to right:
André Arrigoni, Ralph Tonezzer, Peter Gabriel, Kurt Biri, Christian Mauz, Oliver Vaterlaus (Managing Partner)

Agenda

1. Motivation
2. SNMP Basics
3. Looking for IPv6 counters and routing information
4. Looking for IPv6 security information
5. Summary
6. Demo

Motivation

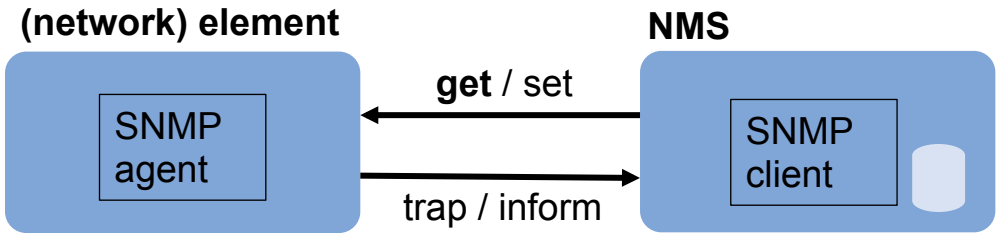
- … for monitoring
- … for monitoring of IPv6 information
- … for monitoring of IPv6 information with SNMP

> *“In theory there is no difference between theory and practice. In practice there is.”*
> (Yogi Berra)

SNMP Basics

Agent and Client

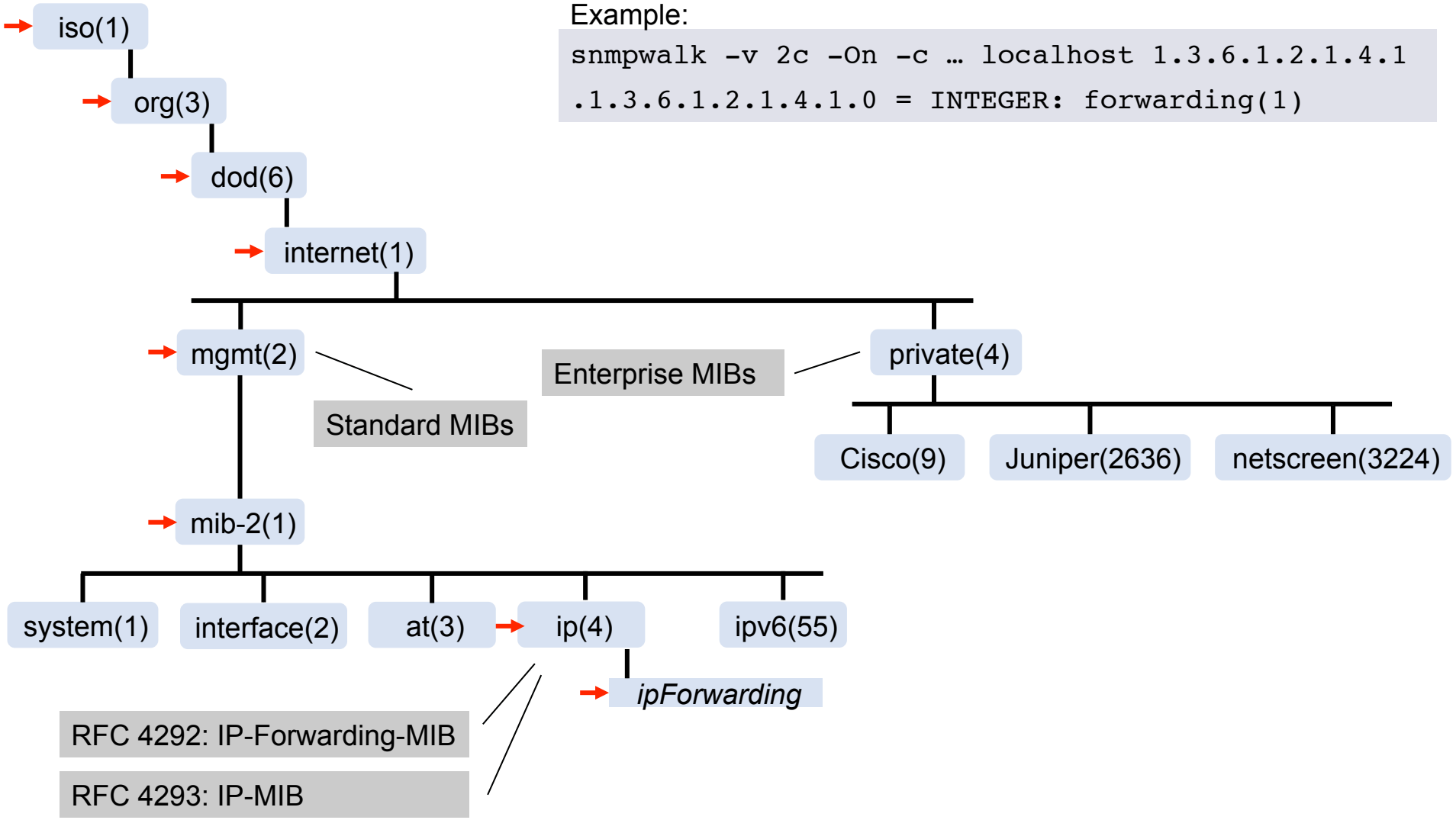
- SNMP Agent
  - Provides management information
    - In form of *management objects (MOs)*
      - Uniquely defined by *object identifiers (OIDs)*
        - *In a tree-like format*
  - *Management Information Base (MIB)* describes information available
- SNMP Client
  - Allows user to retrieve information (get) or set configuration parameters (set)



Note: ‘MIBs’ → MIB Modules (all available modules of a certain element together build the MIB)

SNMP Basics

MIB Tree

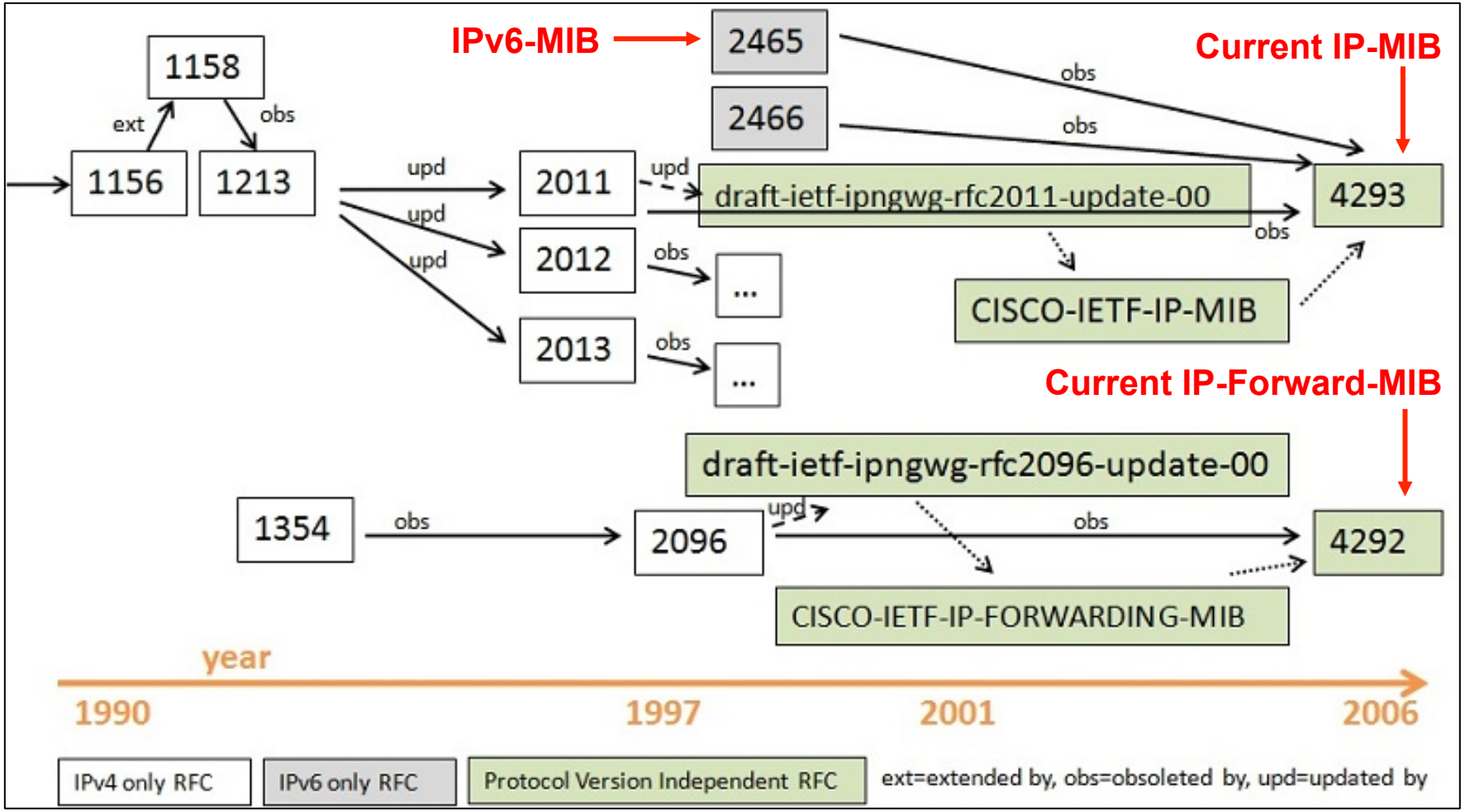


Example:

```
snmpwalk -v 2c -On -c … localhost 1.3.6.1.2.1.4.1
.1.3.6.1.2.1.4.1.0 = INTEGER: forwarding(1)
```

IPv6 MIB Modules

- A bit of history



Source: www.cisco.com

SNMP Basics

IP-MIB (RFC 4293)

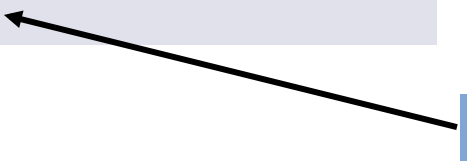
```
+--ip(4) (.1.3.6.1.2.1)        //without .4.24
   +--(Scalars)
   +--ipAddrTable(20)          //deprecated
   +--ipNetToMediaTable(22)    //deprecated
   +--ipv4InterfaceTable(28)
   +--ipv6InterfaceTable(30)
   +--ipTrafficStats(31)
   +--ipAddressPrefixTable(32)
   +--ipAddressTable(34)
   +--ipNetToPhysicalTable(35)
   +--ipv6ScopeZoneIndexTable(36)
   +--ipDefaultRouterTable(37)
   +--ipv6RouterAdvertTable(39)
```

```
|  +--ipSystemStatsTable(1)
   |  +--ipSystemStatsEntry (1)
   +--ipIfStatsTable(3)
   |  +--ipIfStatsEntry(1)
```

SNMP Basics

IP-Forwarding-MIB (RFC 4292)

```
+--ipForward(24) (.1.3.6.1.2.1)
   +--(Scalars)
   +--ipForwardTable(2)          //deprecated
   +--ipCidrRouteTable(4)        //deprecated
   +--ipForwardConformance(5)
   +--inetCidrRouteTable(7)
```



```
|  +--inetCidrRouteEntry(1)
```

SNMP-Basics

IPv6-MIB (RFC 2465)

```
+--ipv6MIB(55)
   +--ipv6MIBObjects(1)
   |  +--(Scalars)
   |  +--ipv6IfTable(5)
   |  +--ipv6IfStatsTable(6)
   |  +--ipv6AddrPrefixTable(7)
   |  +--ipv6AddrTable(8)
   |  +--ipv6RouteTable(11)
   |  +--ipv6NetToMediaTable(12)
```

```
|  +--ipv6IfStatsEntry(1)
```

```
|  +--ipv6RouteEntry(1)
```

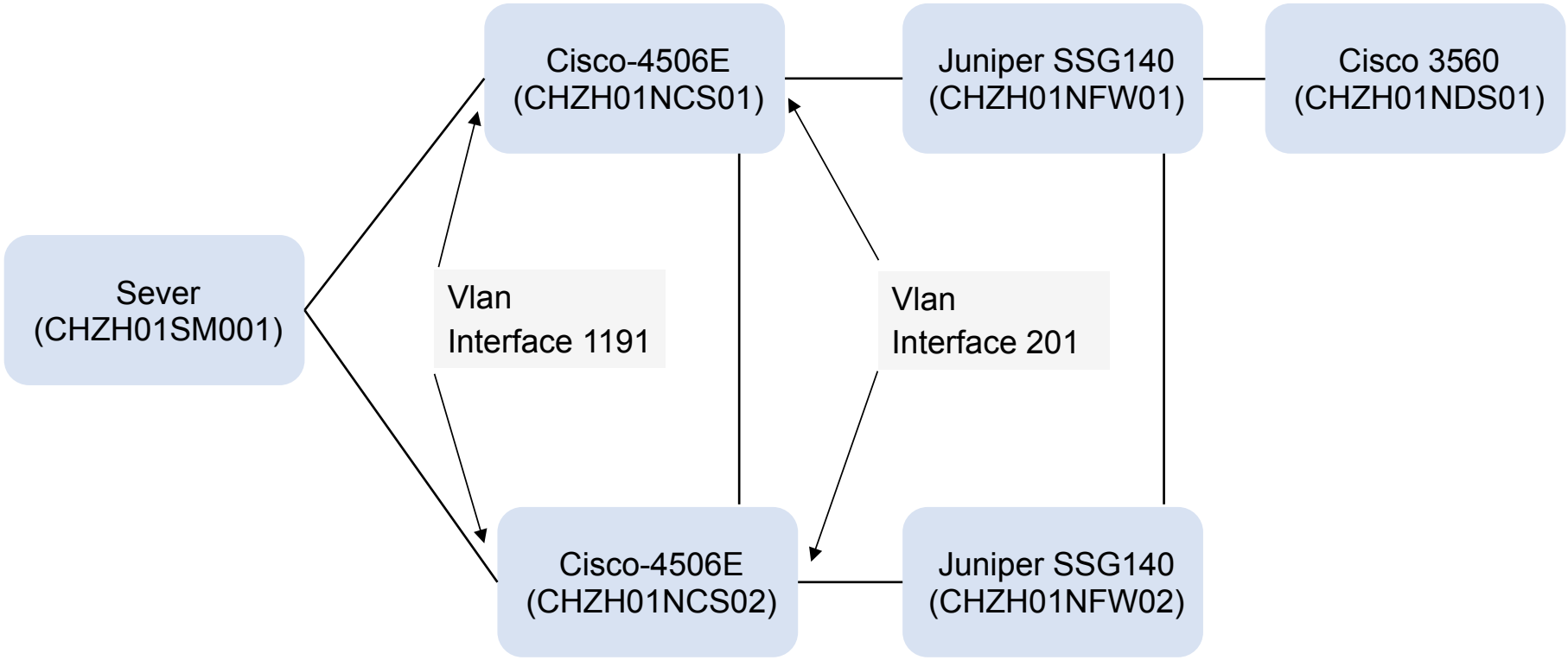
Definiton Datagram: “A self-contained, independent entity of data carrying sufficient information to be routed from the source to the destination computer without reliance on earlier exchanges between this source and destination computer and the transporting network.”
(RFC 1594)

Counters and Routing

Cisco Catalyst 4506E – Sup6-LE – 15.2(2)E1

Counters

- Copying IOS image from SMO01 to DS01
  - Using scp
  - Using ipv6



Cisco Catalyst 4506E – Sup6-LE – 15.2(2)E1

Counters

- Identifying relevant counters at CS01
  - Interface identifier

```
snmpwalk -v 2c -c …  chzh01ncs01 1.3.6.1.2.1.2.2.1.2 | grep 201
IF-MIB::ifDescr.166 = STRING: unrouted VLAN 201
IF-MIB::ifDescr.172 = STRING: Vlan201
IF-MIB::ifDescr.201 = STRING: GigabitEthernet4/10
```

  - Relevant OIDs

```
ipIfStatsHCInOctets                 ipIfStatsHCOutOctets
1.3.6.1.2.1.4.31.3.1.6              1.3.6.1.2.1.4.31.3.1.33

IP Version: unknown (0) - ipv4 (1) - ipv6 (2)

1.3.6.1.2.1.4.31.3.1.6.2.172        1.3.6.1.2.1.4.31.3.1.33.2.172
```

Cisco Catalyst 4506E – Sup6-LE – 15.2(2)E1

Counters

- Reading counter before copying

```
snmpwalk -v 2c -c …  chzh01ncs01 1.3.6.1.2.1.4.31.3.1.6.2.172
IP-MIB::ipIfStatsHCInOctets.ipv6.172 = Counter64: 210390984
snmpwalk -v 2c -c …  chzh01ncs01 1.3.6.1.2.1.4.31.3.1.33.2.172
IP-MIB::ipIfStatsHCOutOctets.ipv6.172 = Counter64: 213247954
```

- Copying the file

```
CHZH01NDS01#copy scp: flash:
Address or name of remote host [2001:db8:6:1191::101]?
Source username [mug]?
Source filename [/home/mug/IOS/c1140-k9w7-tar.152-2.JB.tar]?
Destination filename [c1140-k9w7-tar.152-2.JB.tar]?
Sending file modes: C0664 10352640 c1140-k9w7-tar.152-2.JB.tar
...
10352640 bytes copied in 274.593 secs (37702 bytes/sec)
CHZH01NDS01#
```

Cisco Catalyst 4506E – Sup6-LE – 15.2(2)E1

Counters

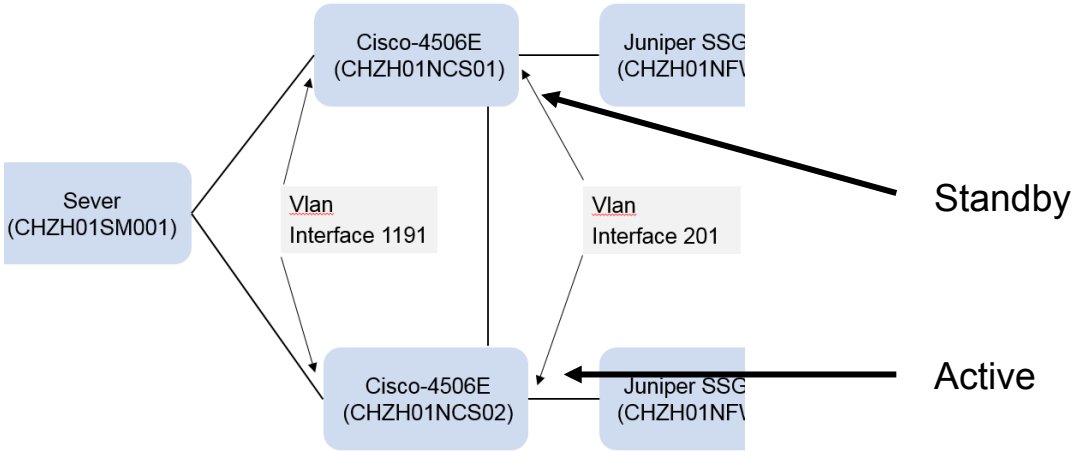
- Reading counters after copying

```
snmpwalk -v 2c -c …  chzh01ncs01 1.3.6.1.2.1.4.31.3.1.6.2.172
IP-MIB::ipIfStatsHCInOctets.ipv6.172 = Counter64: 210435192
snmpwalk -v 2c -c …  chzh01ncs01 1.3.6.1.2.1.4.31.3.1.33.2.172
IP-MIB::ipIfStatsHCOutOctets.ipv6.172 = Counter64: 213291782
```

- What do we expect?
  - About 10Mbytes of traffic on the OutOctets
- Doing the math
  - InOctets: 210435192 – 210390984 = 44208 octets (equals bytes)
  - OutOctets: 213291782 – 213247954 = 43828 octets (equals bytes)
- Any ideas?

Cisco Catalyst 4506E – Sup6-LE – 15.2(2)E1

- Running HSRP on VLAN interface 201




```
CHZH01NCS01#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
…
Vl201       201  90    Standby 192.168.201.2   local           192.168.201.1
Vl201       1001 90    Standby FE80::201:0:0:22local           FE80::201:0:0:20
```

Cisco Catalyst 4506E – Sup6-LE – 15.2(2)E1

Counters

- Checking counters on CS02 (copying the file again)
  - Identifying interface

```
snmpwalk -v 2c -c …  chzh01ncs02 1.3.6.1.2.1.2.2.1.2 | grep 201
IF-MIB::ifDescr.118 = STRING: unrouted VLAN 201
IF-MIB::ifDescr.124 = STRING: Vlan201
```

  - Counters before and after

```
IP-MIB::ipIfStatsHCInOctets.ipv6.124 = Counter64: 215515526
IP-MIB::ipIfStatsHCOutOctets.ipv6.124 = Counter64: 212905664
IP-MIB::ipIfStatsHCInOctets.ipv6.124 = Counter64: 215539474
IP-MIB::ipIfStatsHCOutOctets.ipv6.124 = Counter64: 212928584
```

  - Doing the math
    - InOctets: 215539474 – 215515526 = 23948 octets (bytes)
    - OutOctets: 212928584 – 212905664 = 22920 octets (bytes)

Cisco Catalyst 4506E – Sup6-LE – 15.2(2)E1

Counters

- What to do?
  - Call Cisco (-;
  - In fact: “No IPv4/6 aware HW counters for data plane on Sup6L-E (only traffic which passes control plane is reported). This is a hardware limitation.”
- Ok… so copying the same file to CS01 or CS02 should work, right?
  - Identifying interface

```
snmpwalk -v 2c -c ... chzh01ncs01 1.3.6.1.2.1.2.2.1.2 | grep 1191
IF-MIB::ifDescr.189 = STRING: Vlan1191
```

  - Counters before and after

```
IP-MIB::ipIfStatsHCInOctets.ipv6.189 = Counter64: 419997581
IP-MIB::ipIfStatsHCOutOctets.ipv6.189 = Counter64: 306198179
IP-MIB::ipIfStatsHCInOctets.ipv6.189 = Counter64: 431018580
IP-MIB::ipIfStatsHCOutOctets.ipv6.189 = Counter64: 306986585
```

Cisco Catalyst 4506E – Sup6-LE – 15.2(2)E1

Counters

- Doing the math (remember: we expect to see about 10Mbytes incoming)
  - InOctets: 431018580 – 419997581 = 11020999 Octets (bytes)
  - OutOctets: 306986585 – 306198179 = 788406 Octets (bytes)
- 11020999 / (1024)^2 = 10.51MB

Cisco Catalyst 4506E – Sup6-LE – 15.2(2)E1

Counters

- What about IPv4 Counters

```
snmpwalk -v 2c -c … -OX chzh01ncs01 1.3.6.1.2.1.4.31.3.1  //ipIfStatsEntry
IP-MIB::ipIfStatsInReceives[ipv6][153] = Counter32: 0
IP-MIB::ipIfStatsInReceives[ipv6][172] = Counter32: 1930340
IP-MIB::ipIfStatsInReceives[ipv6][188] = Counter32: 2422612
IP-MIB::ipIfStatsInReceives[ipv6][189] = Counter32: 3111351
IP-MIB::ipIfStatsInReceives[ipv6][190] = Counter32: 100537105
...
IP-MIB::ipIfStatsDiscontinuityTime[ipv6][153] = Timeticks: (0) 0:00:00.00
...
```

  - No information about IPv4 traffic stats available (only IPv6)!
  - Possible solution:
    - IPv4InOctets = ifInOctets – IPv6InOctets
    - IPv4OutOctets = ifOutOctets – IPv6OutOctets

Cisco Catalyst 4506E – Sup6-LE – 15.2(2)E1

Routing Information

- IPv6 Information
  - inetCidrRouteEntry

```
snmpwalk -v 2c -c …  -OX chzh01ncs01 1.3.6.1.2.1.4.24.7.1
…
IP-FORWARD-MIB::inetCidrRouteStatus[ipv6]
         ["00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00"]…         [ipv6]
["20:01:17:02:00:06:10:01:00:00:00:00:00:00:00:10"] … active(1)
…
```

- IPv4 Information
  - ipCidrRouteEntry - Deprecated

```
snmpwalk -v 2c -c …  -OX chzh01ncs01 1.3.6.1.2.1.4.24.4.1
…
IP-FORWARD-MIB::ipCidrRouteNextHop[0.0.0.0][0.0.0.0][0][192.168.201.10] =
IpAddress: 192.168.201.10
…
```

Cisco Catalyst 4506E – Sup6-LE – 15.2(2)E1

HSRP

- HSRP: Host Standby Redundancy Protocol (first hop redundancy protocol)
- On the switch

```
CHZH01NCS01#show standby brief
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
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::1191:0:0:12FE80::1191:0:0:10
```

Cisco Catalyst 4506E – Sup6-LE – 15.2(2)E1

HSRP

- Via SNMP

```
snmpwalk -v 2c -c … -OX chzh01ncs01 1.3.6.1.4.1.9.9.106.1.2.1.1
…
CISCO-HSRP-MIB::cHsrpGrpStandbyRouter[190][225] = IpAddress: 10.1.225.12
CISCO-HSRP-MIB::cHsrpGrpStandbyState[160][21] = INTEGER: standby(5)
CISCO-HSRP-MIB::cHsrpGrpStandbyState[168][11] = INTEGER: active(6)
CISCO-HSRP-MIB::cHsrpGrpStandbyState[169][12] = INTEGER: standby(5)
CISCO-HSRP-MIB::cHsrpGrpStandbyState[170][50] = INTEGER: active(6)
CISCO-HSRP-MIB::cHsrpGrpStandbyState[171][51] = INTEGER: active(6)
CISCO-HSRP-MIB::cHsrpGrpStandbyState[172][201] = INTEGER: standby(5)
CISCO-HSRP-MIB::cHsrpGrpStandbyState[176][71] = INTEGER: standby(5)
CISCO-HSRP-MIB::cHsrpGrpStandbyState[188][224] = INTEGER: active(6)
CISCO-HSRP-MIB::cHsrpGrpStandbyState[189][233] = INTEGER: active(6)
CISCO-HSRP-MIB::cHsrpGrpStandbyState[190][225] = INTEGER: active(6)
CISCO-HSRP-MIB::cHsrpGrpVirtualMacAddr[160][21] = STRING: 0:0:c:7:ac:15
…
```

- Only information about IPv4 standby groups available!

HSRP

- Possible solution
  - Use syslog

```
// Shutting down interface on CS01

CHZH01NCS01(config)#interface vlan 1121

CHZH01NCS01(config-if)#shutdown


// Syslog messages received

Feb 15 19:44:47 chzh01ncs01.awkgroup.com 180: 000180: Feb 15 19:44:46.517 CET:
%HSRP-5-STATECHANGE: Vlan1121 Grp 1121 state Active -> Init

Feb 15 19:44:47 chzh01ncs01.awkgroup.com 181: 000181: Feb 15 19:44:46.521 CET:
%HSRP-5-STATECHANGE: Vlan1121 Grp 225 state Active -> Init

Feb 15 19:44:47 chzh01ncs02.awkgroup.com 146: 000146: Feb 15 19:44:46.523 CET:
%HSRP-5-STATECHANGE: Vlan1121 Grp 1121 state Standby -> Active

Feb 15 19:44:47 chzh01ncs02.awkgroup.com 147: 000147: Feb 15 19:44:46.527 CET:
%HSRP-5-STATECHANGE: Vlan1121 Grp 225 state Standby -> Active
```

C871 – IOS 12.4(24)T8

IP-MIB vs. IP-MIB

- Mission: Find IPv4 and IPv6 counters
  - Checking for IP-MIB support

cisco MIB Locator

Make Selections to get to a Specific Cisco IOS Release:

Release

12.4(24)T8

Platform Family

871

Feature Set

ADVANCED IP SERVICES

New Search

Download all V1 , V2 MIBs

Image Information			
c870-advipservicesk9-mz.124-24.T8.bin	Get list of features for this image from Cisco Feature Navigator		
MIBS Supported in this Image	Details	Download MIB	
ADSL-DMT-LINE-MIB		V1	V2
ADSL-LINE-MIB		V1	V2
ATM-FORUM-TC-MIB		V1	V2
ATM-MIB		V1	V2
ATM2-MIB		V1	V2
BRIDGE-MIB		V1	V2
CISCO-AAA-SERVER-MIB		V1	V2
IP-FORWARD-MIB		V1	V2
IP-MIB		V1	V2

Link: http://tools.cisco.com/Support/SNMP/do/MIBSupport.do?local=en&step=3

C871 – IOS 12.4(24)T8

IP-MIB vs. IP-MIB

- Checking configuration and interface status

```
interface FastEthernet4
 description InternetUplink
 ip address 10.1.0.202 255.255.255.0
 ipv6 address 2001:db8:6:1221::202/64

FastEthernet4 is up, line protocol is up
  Hardware is PQUICC_FEC, address is 001f.9e65.1d24 (bia 001f.9e65.1d24)
  Description: InternetUplink
  Internet address is 10.1.0.202/24

FastEthernet4 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::21F:9EFF:FE65:1D24
  Description: InternetUplink
  Global unicast address(es):
    2001:db8:6:1221::202, subnet is 2001:db8:6:1221::/64
```

C871 – IOS 12.4(24)T8

IP-MIB vs. IP-MIB

- Getting interface identifier

```
snmpwalk -v 2c -c … 10.1.0.202 1.3.6.1.2.1.2.2.1 | grep FastEthernet4
IF-MIB::ifDescr.5 = STRING: FastEthernet4
```

- Getting the counters

```
snmpwalk -v 2c -c public 10.1.0.202 1.3.6.1.2.1.4.31.3.1.6/33.1/2.5
IP-MIB::ipIfStatsHCInOctets.ipv6.5 = No Such Object available on this
agent at this OID
IP-MIB::ipIfStatsHCOutOctets.ipv6.5 = No Such Object available on this
agent at this OID
IP-MIB::ipIfStatsHCInOctets.ipv4.5 = No Such Object available on this
agent at this OID
IP-MIB::ipIfStatsHCOutOctets.ipv4.5 = No Such Object available on this
agent at this OID
```

- Only old version of IP-MIB is implemented!
- Ask Cisco if HW / SW supports IP-MIB according to RFC 4293

C871 – IOS 12.4(24)T8

Routing

- IPv4 information
  - ipCidrRouteEntry - Deprecated

```
snmpwalk -v 2c –c … -OX 10.1.0.202 1.3.6.1.2.1.4.24.4.1
…
IP-FORWARD-MIB::ipCidrRouteNextHop[0.0.0.0][0.0.0.0][0][10.1.11.10] =
IpAddress: 10.1.11.10
```

- IPv6 information
  - inetCidrRouteEntry

```
snmpwalk -v 2c –c … -OX
10.1.0.202
1.3.6.1.2.1.4.24.7.1
IP-FORWARD-
MIB::inetCidrRouteEntry = No
Such Object available on this
```

```
Routerbma#show ipv6 route
IPv6 Routing Table - Default - 8 entries
S   ::/0 [1/0]
     via 2001:db8:6:1221::10
C   2001:db8:6:1221::/64 [0/0]
     via FastEthernet4, directly connected
```

Cisco 2821 – IOS 15.1(4)M1

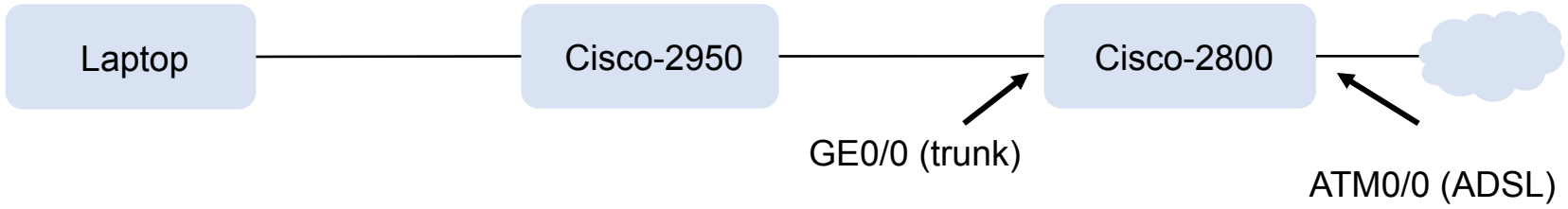
Counters

- Mission: Find IPv4 and IPv6 counters
  - Checking release notes:

```
IPv4 MIB Support (RFC 4293)

Cisco IOS Release 15.1(4)M includes support for the IPv4 MIB as described
in RFC 4293, Management Information Base for the Internet Protocol (IP). …
```

Source: http://www.cisco.com/c/en/us/td/docs/ios/15_1/release/notes/15_1m_and_t/151-4MNEWF.html

  - Test setup




```
IF-MIB::ifDescr.1 = STRING: GigabitEthernet0/0
IF-MIB::ifDescr.15 = STRING: ATM0/0/0.35-aal5 layer
IF-MIB::ifDescr.17 = STRING: GigabitEthernet0/0.12
```

Sub-interface with v4 and v6

Cisco 2821 – IOS 15.1(4)M1

Counters

- Checking for the counters – finally found them (IPv4 and IPv6)

```
snmpwalk -v 2c -c … 212.161.137.149 1.3.6.1.2.1.4.31.3.1.6/33.1/2.17
IP-MIB::ipIfStatsHCInOctets.ipv4.17 = Counter64: 604
IP-MIB::ipIfStatsHCInOctets.ipv6.17 = Counter64: 0
IP-MIB::ipIfStatsHCOutOctets.ipv4.17 = Counter64: 0
IP-MIB::ipIfStatsHCOutOctets.ipv6.17 = Counter64: 10824000
```

- Ok, some testing: Downloading ~12MB (over v4 and v6 each)

```
snmpwalk -v 2c -c … 212.161.137.149 1.3.6.1.2.1.4.31.3.1.6/33.1/2.17
IP-MIB::ipIfStatsHCInOctets.ipv4.17 = Counter64: 38135
IP-MIB::ipIfStatsHCInOctets.ipv6.17 = Counter64: 1236
IP-MIB::ipIfStatsHCOutOctets.ipv4.17 = Counter64: 73654
IP-MIB::ipIfStatsHCOutOctets.ipv6.17 = Counter64: 10826257
```

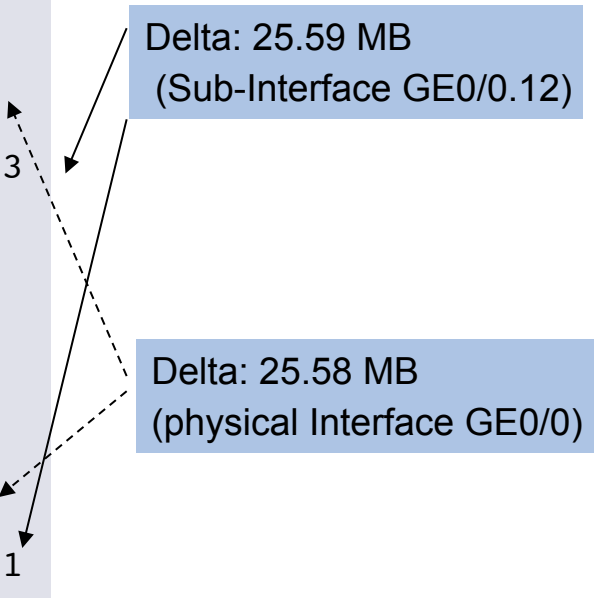
- We should see around 12MB on the OutOctet counters but we only see a few Kb!

Cisco 2821 – IOS 15.1(4)M1

Counters

- Checking IPv4 and IPv6 counter at physical interface GE 0/0
  - Still the same
- Checking Interface Octet counters

```
// Before
IF-MIB::ifInOctets.1 = Counter32: 158368270
IF-MIB::ifInOctets.17 = Counter32: 5766751
IF-MIB::ifOutOctets.1 = Counter32: 190088509
IF-MIB::ifOutOctets.17 = Counter32: 132411973

// After
IF-MIB::ifInOctets.1 = Counter32: 159756432
IF-MIB::ifInOctets.17 = Counter32: 7136661
IF-MIB::ifOutOctets.1 = Counter32: 215876383
IF-MIB::ifOutOctets.17 = Counter32: 158192381
```



- IPv4 and IPv6 counters do not properly count the octets!

Cisco 2821 – IOS 15.1(4)M1

Routing Information

- IPv6 information
  - inetCidrRouteEntry

```
snmpwalk -v 2c -c … 212.161.137.149 -OX 1.3.6.1.2.1.4.24.7.1
…
IP-FORWARD-MIB::inetCidrRouteStatus[ipv6]
        ["00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00"]
        [20:01:17:00:06:01:00:00:00:00:00:00:00:00:00:01"] … active(1)
…
```

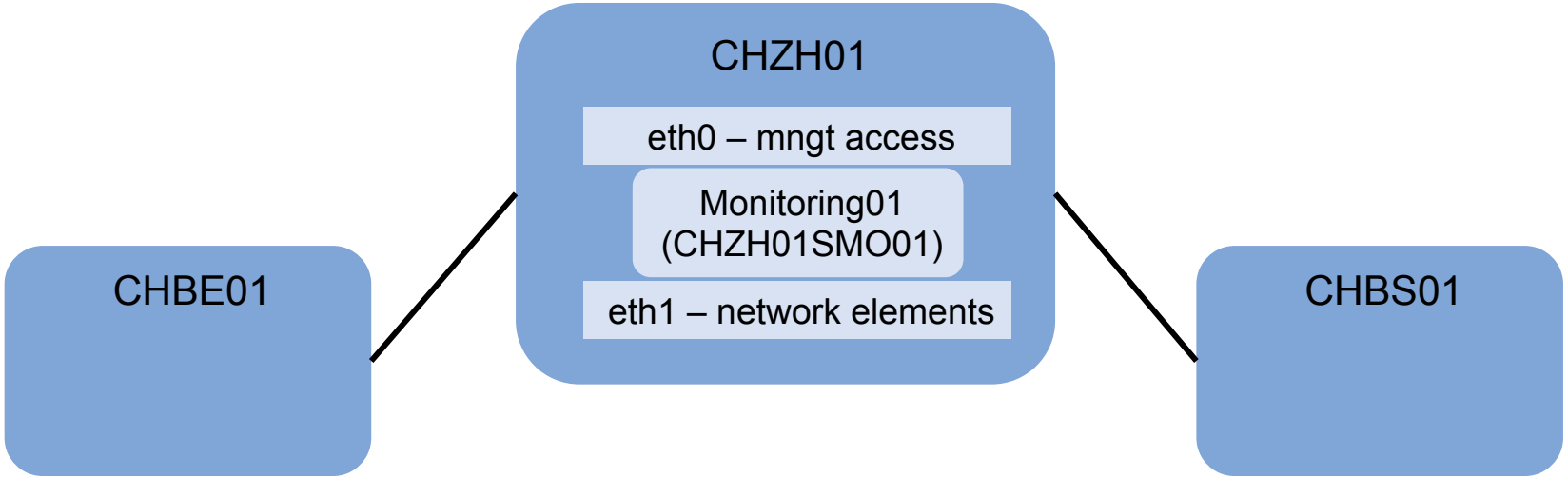
- IPv4 information
  - ipCidrRouteEntry - Deprecated

```
snmpwalk -v 2c -c … 212.161.137.149 -OX 1.3.6.1.2.1.4.24.4.1
…
IP-FORWARD-MIB::ipCidrRouteStatus[0.0.0.0][0.0.0.0][0][194.158.231.177] =
        INTEGER: active(1)
…
```

Ubuntu – 14.04.1 LTS

Counters

- Monitoring01
  - VM running Ubuntu
  - Managing / monitoring network with
    - Cacti
    - Icinga
    - Rancid
    - PHPIpam



Ubuntu – 14.04.1 LTS

Counters

- Checking IPv6-MIB
  - Only displaying results for eth1 here

```
snmpwalk -v 2c -c … chzh01smo01 1.3.6.1.2.1.55.1
IPV6-MIB::ipv6Forwarding.0 = INTEGER: notForwarding(2)
IPV6-MIB::ipv6DefaultHopLimit.0 = INTEGER: 64
IPV6-MIB::ipv6Interfaces.0 = Gauge32: 3
IPV6-MIB::ipv6IfDescr.3 = STRING: eth1
IPV6-MIB::ipv6IfLowerLayer.3 = OID: SNMPv2-SMI::zeroDotZero
IPV6-MIB::ipv6IfEffectiveMtu.3 = Gauge32: 1500 octets
IPV6-MIB::ipv6IfPhysicalAddress.3 = STRING: 0:50:56:b5:60:83
IPV6-MIB::ipv6IfAdminStatus.3 = INTEGER: up(1)
IPV6-MIB::ipv6IfOperStatus.3 = INTEGER: up(1)
```

  - ➢ Very limited information

Ubuntu – 14.04.1 LTS

Counters

- IP-MIB

```
mug@Monitoring01:~$ lsb_release -a
Distributor ID:     Ubuntu
Description:        Ubuntu 12.04.5 LTS
Release:            12.04
Codename:           precise
```

```
mug@Monitoring01:~$ lsb_release -a
Distributor ID:     Ubuntu
Description:        Ubuntu 14.04.1 LTS
Release:            14.04
Codename:           trusty
```

NET-SNMP version: 5.4.3

new 5

```
1  mug@Monitoring01:~$ cat Trace_CHZH01SMO01_Before.txt | g
2  IF-MIB::ifInOctets.1 = Counter32: 616142254
3  IF-MIB::ifInOctets.2 = Counter32: 2244883914
4  IF-MIB::ifInOctets.3 = Counter32: 3774907347
5  IF-MIB::ifInOctets.4 = Counter32: 0
6
7  IP-MIB::ipSystemStatsHCInOctets.ipv4 = Counter64: 0
8  IP-MIB::ipSystemStatsHCInOctets.ipv6 = Counter64: 0
9
10
11
12
13
14
15
16
17 IF-MIB::ifHCInOctets.1 = Counter64: 616142254
18 IF-MIB::ifHCInOctets.2 = Counter64: 2244883914
19 IF-MIB::ifHCInOctets.3 = Counter64: 8069874643
20 IF-MIB::ifHCInOctets.4 = Counter64: 0
21 mug@Monitoring01:~$
```

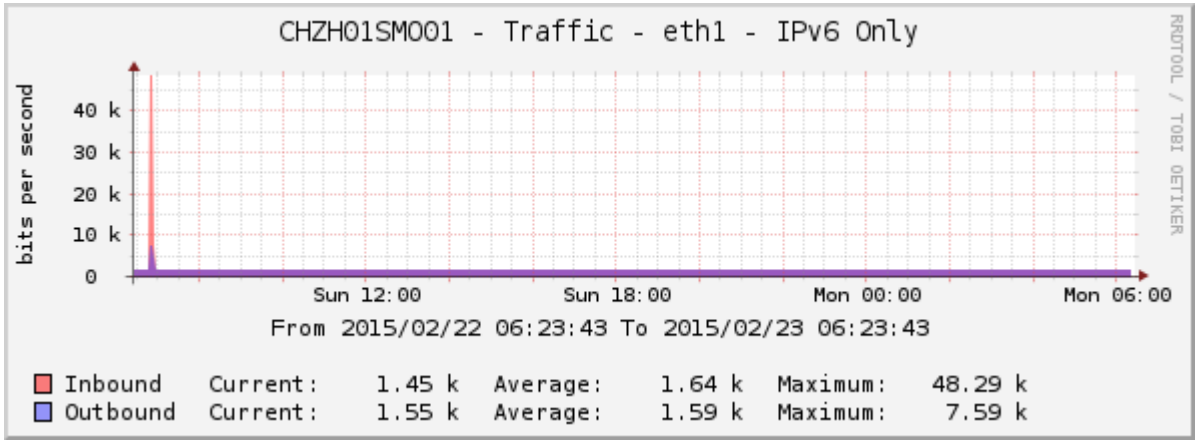
NET-SNMP version: 5.7.2

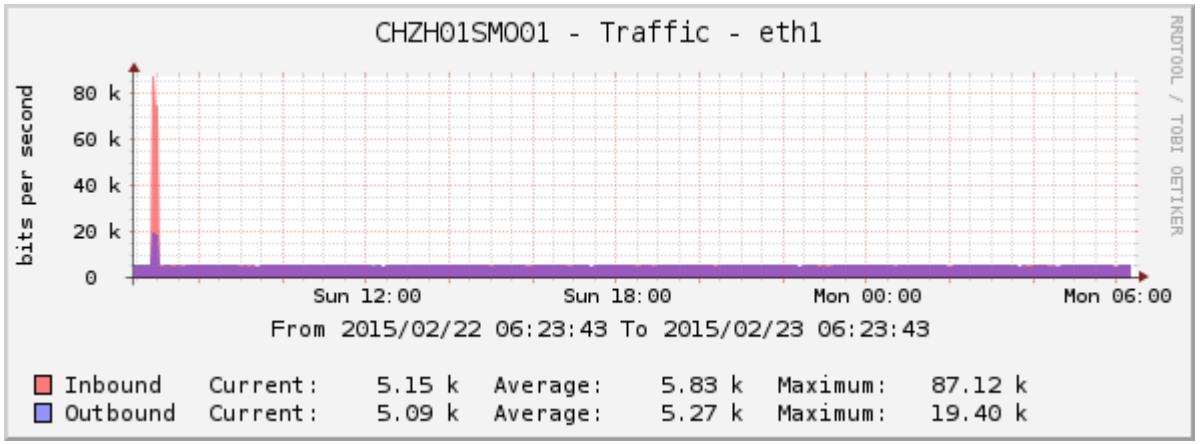
new 6

```
1  mug@Monitoring01:~$ cat Trace_CHZH01SMO01_After.txt | grep
2  IF-MIB::ifInOctets.1 = Counter32: 158469
3  IF-MIB::ifInOctets.2 = Counter32: 983790
4  IF-MIB::ifInOctets.3 = Counter32: 727988
5  IF-MIB::ifInOctets.4 = Counter32: 0
6  IP-MIB::ipSystemStatsInOctets.ipv6 = Counter32: 215416
7  IP-MIB::ipSystemStatsHCInOctets.ipv6 = Counter64: 215416
8
9  IP-MIB::ipIfStatsInOctets.ipv6.1 = Counter32: 5677
10 IP-MIB::ipIfStatsInOctets.ipv6.2 = Counter32: 0
11 IP-MIB::ipIfStatsInOctets.ipv6.3 = Counter32: 209739
12 IP-MIB::ipIfStatsInOctets.ipv6.4 = Counter32: 0
13 IP-MIB::ipIfStatsHCInOctets.ipv6.1 = Counter64: 5677
14 IP-MIB::ipIfStatsHCInOctets.ipv6.2 = Counter64: 0
15 IP-MIB::ipIfStatsHCInOctets.ipv6.3 = Counter64: 209739
16 IP-MIB::ipIfStatsHCInOctets.ipv6.4 = Counter64: 0
17 IF-MIB::ifHCInOctets.1 = Counter64: 158469
18 IF-MIB::ifHCInOctets.2 = Counter64: 983790
19 IF-MIB::ifHCInOctets.3 = Counter64: 727988
20 IF-MIB::ifHCInOctets.4 = Counter64: 0
21 mug@Monitoring01:~$
```

Counters

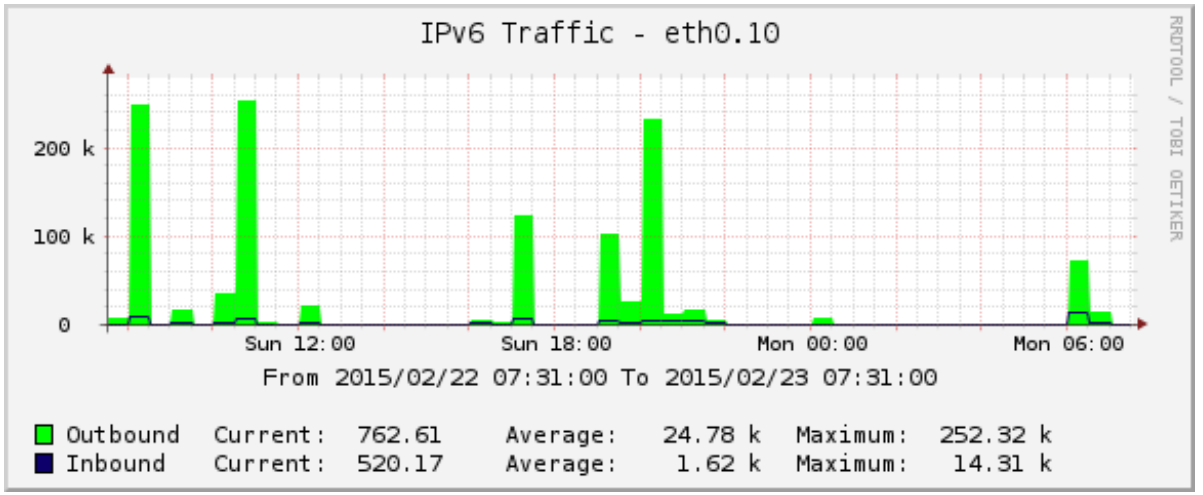
- What is missing again?
  - IPv4 counters!
- At least we can graph IPv6 data
  - Challenge counters

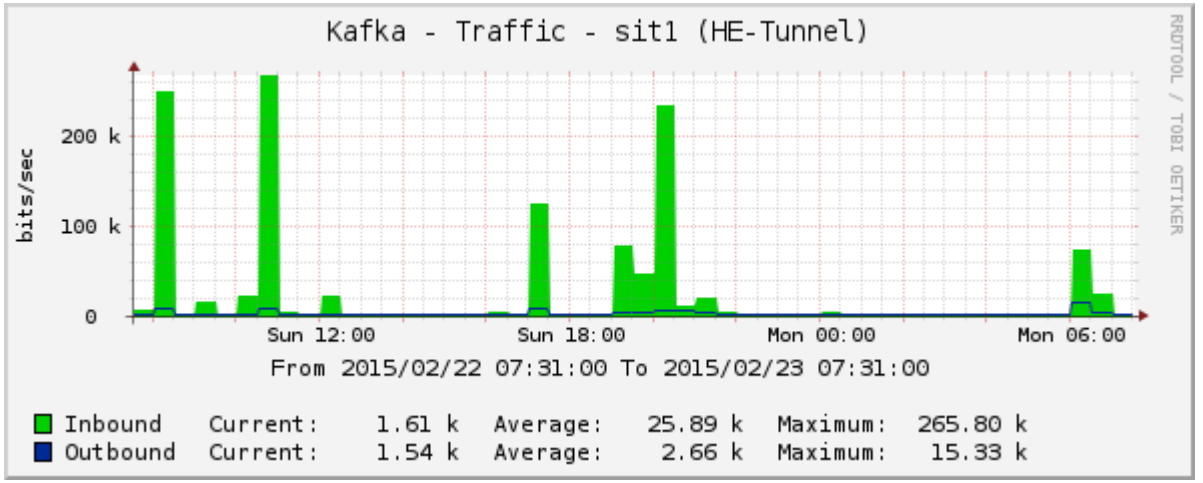




Counters

- Once again: challenge counters





Routing

- Looking for default routes

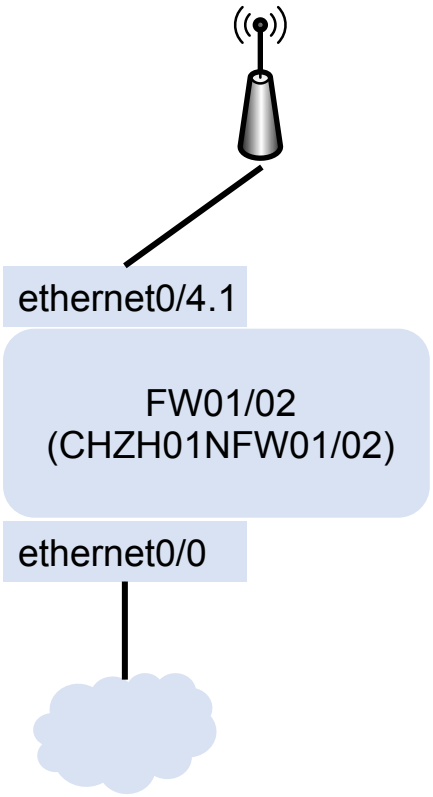
```
snmpwalk -v 2c -c … chzh01smo01 -OX .1.3.6.1.2.1.4.24.7
…
IP-FORWARD-MIB::inetCidrRouteStatus[ipv4]
["0.0.0.0"][0][SNMPv2-SMI::zeroDotZero][ipv4]
["192.168.21.1"] = INTEGER: active(1)
…
IP-FORWARD-MIB::inetCidrRouteStatus[ipv6]
["00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00"][0][SNMPv2-
SMI::zeroDotZero.21][ipv6]
["fe:80:00:00:00:00:00:11:91:00:00:00:00:00:10"] = INTEGER: active(1)
```

  - First time we see IPv4 routing information in current IP-Forward-MIB / MIB location (inetCidrRouteStatus)

Counters

- IPv6 @ AWK
  - Management
  - ‘Public’ WLAN (AWKWLAN)

```
snmpwalk -v 2c -c … chzh01nfw01 1.3.6.1.2.1.2.2.1.2
IF-MIB::ifDescr.1 = STRING: SR_Internet_Uplink
IF-MIB::ifDescr.2 = STRING: ethernet0/1
…
IF-MIB::ifDescr.7 = STRING: AWK_WLAN
IF-MIB::ifDescr.8 = STRING: ethernet0/4.1
…
```

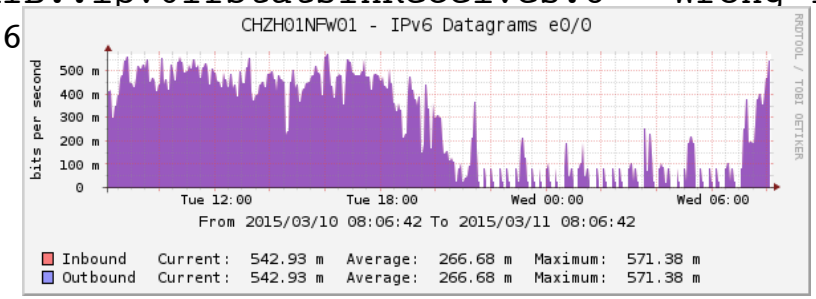


Counters

- Looking at the counters (IPv6-MIB)
  - ipv6IfStatsInReceives: “The total number of input datagrams received by the interface, including those received in error.”

Internet-Uplink
(native IPv6)

```
snmpwalk -v 2c -c … chzh01nfw01 1.3.6.1.2.1.55.1.6.1.1
IPV6-MIB::ipv6IfStatsInReceives.1 = Wrong Type (should be Counter32): INTEGER: 479416
IPV6-MIB::ipv6IfStatsInReceives.2 = Wrong Type (should be Counter32): INTEGER:
2995405
…
IPV6-MIB::ipv6IfStatsInReceives.7 = Wrong Type (should be Counter32): INTEGER:
2067656
IPV6-MIB::ipv6IfStatsInReceives.8 = Wrong Type (should be Counter32): INTEGER:
2067656
```




```
-----SNMP query started-----
1: sysUpTime.0 264 days, 2:52:47.00
-----SNMP query finished-----
```

Counters

- ipv6IfStatsOutForwDatagrams: “The number of output datagrams which this entity received and forwarded to their final destinations.”

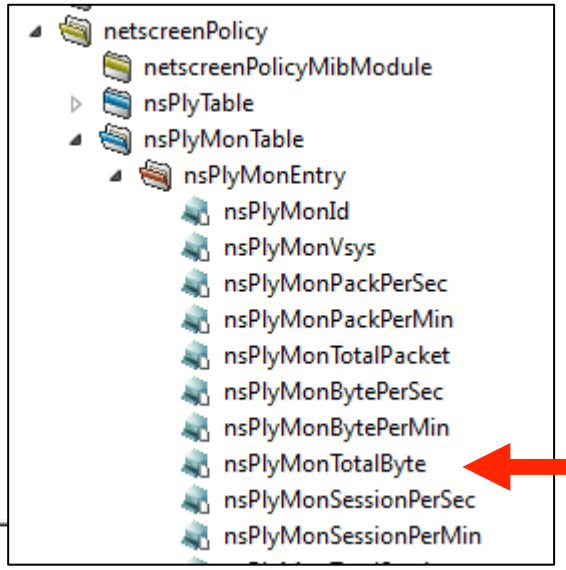
```
snmpwalk -v 2c -c … chzh01nfw01 1.3.6.1.2.1.55.1.6.1.10
IPV6-MIB::ipv6IfStatsOutForwDatagrams.1 = Wrong Type (should be Counter32): INTEGER:
0
IPV6-MIB::ipv6IfStatsOutForwDatagrams.2 = Wrong Type (should be Counter32): INTEGER:
0
…
IPV6-MIB::ipv6IfStatsOutForwDatagrams.7 = Wrong Type (should be Counter32): INTEGER:
0
IPV6-MIB::ipv6IfStatsOutForwDatagrams.8 = Wrong Type (should be Counter32): INTEGER:
0
…
```

  - ➢ No IPv6 traffic information available!

- Any idea how we could get information about IPv6 traffic?
  - Policy counters

Counters

- Policy counters for incoming mail
  - ScreenOS policy statistics



  - Getting policy ID

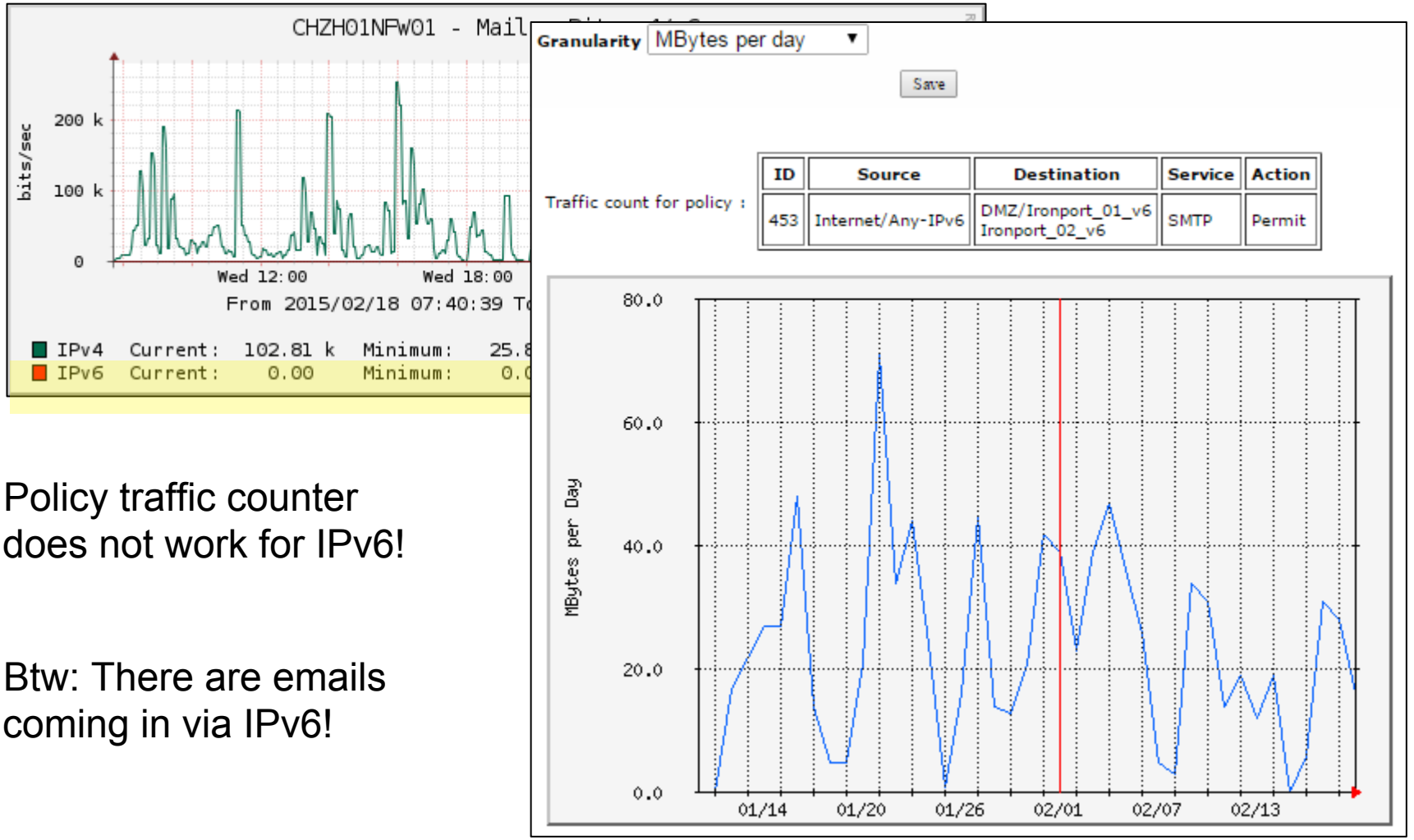
From Internet To DMZ, total policy: 16

ID	Source	Destination	Service	Action
451	Any-IPv6	Any-IPv6	Block_All_EH	
59	Any-IPv4	MIP(194.230.77.200)	HTTP HTTPS	
74	Any-IPv4	MIP(194.230.77.202) MIP(194.230.77.203)	SMTP	
453	Any-IPv6	Ironport_01_v6 Ironport_02_v6	SMTP	

Juniper SSG140 – ScreenOS 6.3.0r17.0

Counters

- Set up the graph



- Policy traffic counter does not work for IPv6!

- Btw: There are emails coming in via IPv6!

Juniper SSG140 – ScreenOS 6.3.0r17.0

Routing

- IPv4 information
  - ipCidrRouteEntry – Deprecated

```
snmpwalk -v 2c -c … -OX chzh01nfw01 1.3.6.1.2.1.4.24.4.1

…

IP-FORWARD-MIB::ipCidrRouteStatus[0.0.0.0][0.0.0.0][0][194.230.77.193] =
INTEGER: active(1)

…
```

- IPv6 information
  - ipv6RouteEntry

```
snmpwalk -v 2c -c … chzh01nfw01 1.3.6.1.2.1.55.1.11.1

IPV6-MIB::ipv6RouteNextHop[STRING: 0:0:0:0:0:0:0:0][0][1] = STRING:
2001:db8:6:0:0:0:0:1

IPV6-MIB::ipv6RouteValid[STRING: 0:0:0:0:0:0:0:0][0][1] = INTEGER: true(1)
```

Counters

- Looking at counters (IPv6-MIB)

```
snmpwalk -v 2c -c … -OX 212.161.178.231 1.3.6.1.2.1.55.1.6.1
IPV6-MIB::ipv6IfStatsInReceives[16] = Counter32: 0
IPV6-MIB::ipv6IfStatsInReceives[18] = Counter32: 0
IPV6-MIB::ipv6IfStatsInReceives[24] = Counter32: 0
IPV6-MIB::ipv6IfStatsInReceives[543] = Counter32: 0
…
IPV6-MIB::ipv6IfStatsOutForwDatagrams[16] = Counter32: 0
IPV6-MIB::ipv6IfStatsOutForwDatagrams[18] = Counter32: 0
IPV6-MIB::ipv6IfStatsOutForwDatagrams[24] = Counter32: 0
IPV6-MIB::ipv6IfStatsOutForwDatagrams[543] = Counter32: 0
```

Counters

- Looking at byte counters (jnxIpv6IfStatsEntry)

```
snmpwalk -v 2c -c … -OX 212.161.178.231 1.3.6.1.4.1.2636.3.11.1.3.1.1
...
JUNIPER-IPv6-MIB::jnxIpv6IfInOctets[615] = Counter64: 264
...
JUNIPER-IPv6-MIB::jnxIpv6IfOutOctets[615] = Counter64: 0
```

  - Very limited access to device, could not challenge counters

  - Again, no counters for IPv4 traffic!

Routing

- IPv4 information
  - inetCidrRouteEntry (current IP-MIB)

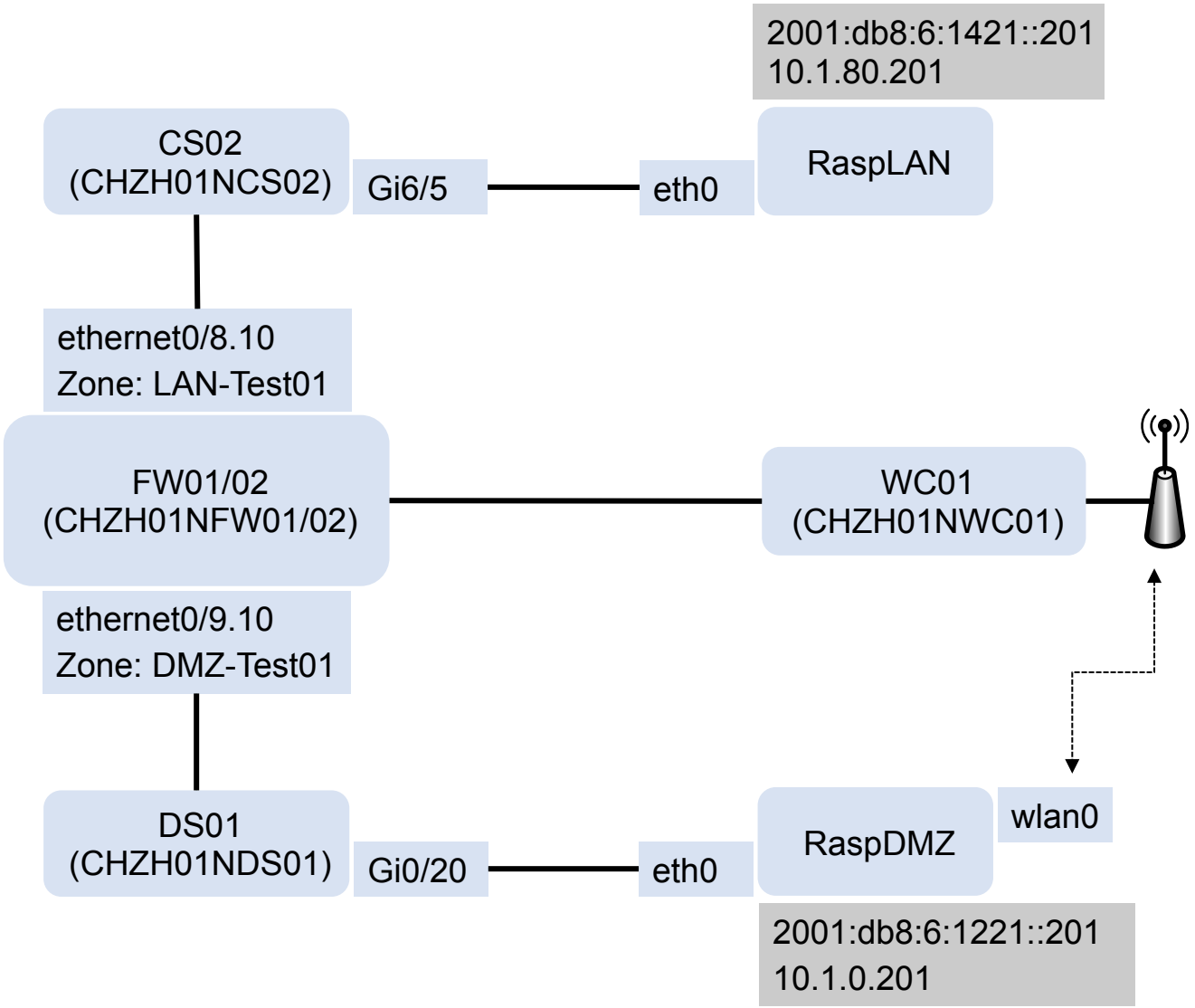
```
muellega@T430s:~$ snmpwalk -v 2c -c arbor -OX 212.161.178.231
1.3.6.1.2.1.4.24.7.1.17  // inetCidrRouteStatus

IP-FORWARD-MIB::inetCidrRouteStatus[ipv4]["0.0.0.0"][0][SNMPv2-
SMI::zeroDotZero][unknown][""] = INTEGER: active(1)

IP-FORWARD-MIB::inetCidrRouteStatus[ipv4]["1.0.0.0"][24][SNMPv2-
SMI::zeroDotZero][ipv4]["212.161.181.166"] = INTEGER: active(1)

IP-FORWARD-MIB::inetCidrRouteStatus[ipv4]["1.0.4.0"][24][SNMPv2-
SMI::zeroDotZero][ipv4]["212.161.181.166"] = INTEGER: active(1)
```

- IPv6 information
  - ipv6RouteEntry

```
snmpwalk -v 2c -c … 212.161.178.231 -OX 1.3.6.1.2.1.55.1.11.1

IPV6-MIB::ipv6RouteNextHop[STRING: 0:0:0:0:0:0:0:0][0][0] = STRING:
0:0:0:0:0:0:0:0

IPV6-MIB::ipv6RouteValid[STRING: 0:0:0:0:0:0:0:0][0][0] = INTEGER: true(1)
```

IPv6 Security

Test Setup


2001:db8:6:1421::201
10.1.80.201
CS02
(CHZH01NCS02)
Gi6/5
eth0
RaspLAN
ethernet0/8.10
Zone: LAN-Test01
FW01/02
(CHZH01NFW01/02)
WC01
(CHZH01NWC01)
ethernet0/9.10
Zone: DMZ-Test01
DS01
(CHZH01NDS01)
Gi0/20
eth0
RaspDMZ
wlan0
2001:db8:6:1221::201
10.1.0.201

Juniper SSG140 – ScreenOS 6.3.0r17.0

Screen Feature

- Described by Juniper as:
  - "ScreenOS SCREEN options secure a zone by inspecting, then allowing or denying, all connection attempts that require crossing an interface bound to that zone."
  - "These options offer protection against IP address and port scans, denial of service (DoS) attacks, and other kinds of malicious activity."
- Quite impressive number of options
  - MIB exists for related counters (NETSCREEN-POLICY-MIB)
  - Let's try a few with IPv6

Screen Counters for Zone DMZ - Test01			
HTTP component detected/blocked!	0	ICMP flood protection	46027
UDP flood protection	2741	WinNuke attack protection	0
Port scan protection	47	IP sweep protection	0
Teardrop attack protection	0	SYN flood protection	0
IP spoof attack protection	0	Ping of Death attack protection	0
Src Route IP option filtering	0	Land attack protection	0
SYN fragment protection	0	TCP packet without flags protection	0
Unknown protocol protection	0	Bad IP option protection	0
Record route IP option detection	0	Timestamp IP option detection	0
Security IP option detection	0	Loose src route IP option detection	0
Strict src route IP option detection	0	Stream IP option detection	0
ICMP fragment protection	0	Large ICMP packet protection	0
SYN and FIN bits set protection	0	FIN bit but no ACK bit protection	0

Source: http://www.juniper.net/techpubs/software/screenos/screenos6.3.0/630_ce_AttackDetection.pdf

Screen Features

- Before we can start

```
snmpwalk -v 2c -c … chzh01nfw01 1.3.6.1.2.1.2.2.1.2
IF-MIB::ifDescr.12 = STRING: AWK_LAN
IF-MIB::ifDescr.17 = STRING: AWK_DMZ
```

- Port scan

```
mug@Monitoring01:~$ snmpwalk -v 2c -c … chzh01nfw01 1.3.6.1.4.1.3224.3.2.1.12
NETSCREEN-IDS-MIB::nsIdsAttkMonPortScan.18 = Counter32: 40

root@RaspDMZ:/home/pi# nmap -p 10-30 rasplan    //IPv4
root@RaspDMZ:/home/pi# nmap -p 10-30 -6 rasplan //IPv6

mug@Monitoring01:~$ snmpwalk -v 2c -c … chzh01nfw01 1.3.6.1.4.1.3224.3.2.1.12
NETSCREEN-IDS-MIB::nsIdsAttkMonPortScan.18 = Counter32: 42
```

Screen Features

- Port Scan (continued)
  - Details needed: Use syslog

```
// IPv4 Port Scan

Feb 19 20:50:51 chzh01nfw01.awkgroup.com CHZH01NFW01: NetScreen
device_id=CHZH01NFW01  [Root]system-alert-00016: Port scan! From
10.1.80.201:34863 to 10.1.0.201:27, proto TCP (zone DMZ - Test01 int
ethernet0/9.10). Occurred 1 times. (2015-02-19 20:50:50)


// IPv6 Port Scan

Feb 19 20:50:57 chzh01nfw01.awkgroup.com CHZH01NFW01: NetScreen
device_id=CHZH01NFW01  [Root]system-alert-00016: Port scan! From
2001:db8:6:1421::201:39774 to 2001:db8:6:1221::201:13, proto TCP (zone DMZ -
Test01 int  ethernet0/9.10). Occurred 1 times. (2015-02-19 20:50:56)
```

  - Comments? (not this slide, but previous one)

Screen Features

- Port Scan (continued)
  - Interface ID mismatch!
    - Interface IDs

```
IF-MIB::ifDescr.17 = STRING: AWK_DMZ
IF-MIB::ifDescr.18 = STRING: ethernet0/9.1
IF-MIB::ifDescr.19 = STRING: ethernet0/9.2
IF-MIB::ifDescr.20 = STRING: ethernet0/9.3
IF-MIB::ifDescr.21 = STRING: ethernet0/9.4
IF-MIB::ifDescr.22 = STRING: ethernet0/9.5
IF-MIB::ifDescr.23 = STRING: ethernet0/9.7
IF-MIB::ifDescr.24 = STRING: ethernet0/9.10
```

    - RaspDMZ connected to ethernet0/9.10

```
Cluster01:CHZH01NFW01(M)-> get arp | include 10.1.80.201
    10.1.80.201  b827eb0889eb    trust-vr/eth0/9.10    …
```

    - Check interface IDs on this slide again

Screen Features

- ICMP flooding

```
mug@Monitoring01:~$ snmpwalk -v 2c -c … chzh01nfw01 1.3.6.1.4.1.3224.3.2.1.9.18
NETSCREEN-IDS-MIB::nsIdsAttkMonIcmpFlood.18 = Counter32: 16544


root@RaspDMZ:/home/pi/thc-ipv6-2.7# ./flood_advertise6 eth0
Starting to flood network with neighbor advertisements on eth0


Feb 19 21:06:34 chzh01nfw01.awkgroup.com CHZH01NFW01: NetScreen
device_id=CHZH01NFW01  [Root]system-alert-00011: ICMP flood! From
fe80::218:50ff:fe94:1647 to ff02::1, proto 58 (zone DMZ - Test01 int
ethernet0/9.10). Occurred 1 times. (2015-02-19 21:06:33)


mug@Monitoring01:~$ snmpwalk -v 2c -c … chzh01nfw01 1.3.6.1.4.1.3224.3.2.1.9.18
NETSCREEN-IDS-MIB::nsIdsAttkMonIcmpFlood.18 = Counter32: 18088
```

Screen Features

- UDP flooding

```
mug@Monitoring01:~$ snmpwalk -v 2c -c … chzh01nfw01 1.3.6.1.4.1.3224.3.2.1.10.18
NETSCREEN-IDS-MIB::nsIdsAttkMonUdpFlood.18 = Counter32: 1247


root@RaspDMZ:/home/pi/thc-ipv6-2.7# ./flood_dhcpc6 eth0
Starting to flood dhcp6 servers locally on eth0


Feb 19 21:09:24 chzh01nfw01.awkgroup.com CHZH01NFW01: NetScreen
device_id=CHZH01NFW01  [Root]system-alert-00012: UDP flood! From
fe80::2e09:0:0:0:546 to ff02::1:2:547, proto UDP (zone DMZ - Test01 int
ethernet0/9.10). Occurred 1 times. (2015-02-19 21:09:23)


mug@Monitoring01:~$ snmpwalk -v 2c -c … chzh01nfw01 1.3.6.1.4.1.3224.3.2.1.10.18
NETSCREEN-IDS-MIB::nsIdsAttkMonUdpFlood.18 = Counter32: 2741
```

Screen Features

- MLD flooding

```
root@RaspDMZ:/home/pi/thc-ipv6-2.7# ./flood_mld6 eth0
Starting to flood network with MLD reports on
 -> not detected


root@RaspDMZ:/home/pi/thc-ipv6-2.7# ./flood_mld26 eth0
Starting to flood network with MLDv2 reports on eth0


Feb 19 21:12:14 chzh01nfw01.awkgroup.com CHZH01NFW01: NetScreen
device_id=CHZH01NFW01  [Root]system-alert-00011: ICMP flood! From
fe80::18:9dff:fe5b:17b9 to ff02::16, proto 58 (zone DMZ - Test01 int
ethernet0/9.10). Occurred 1 times. (2015-02-19 21:12:13)
```

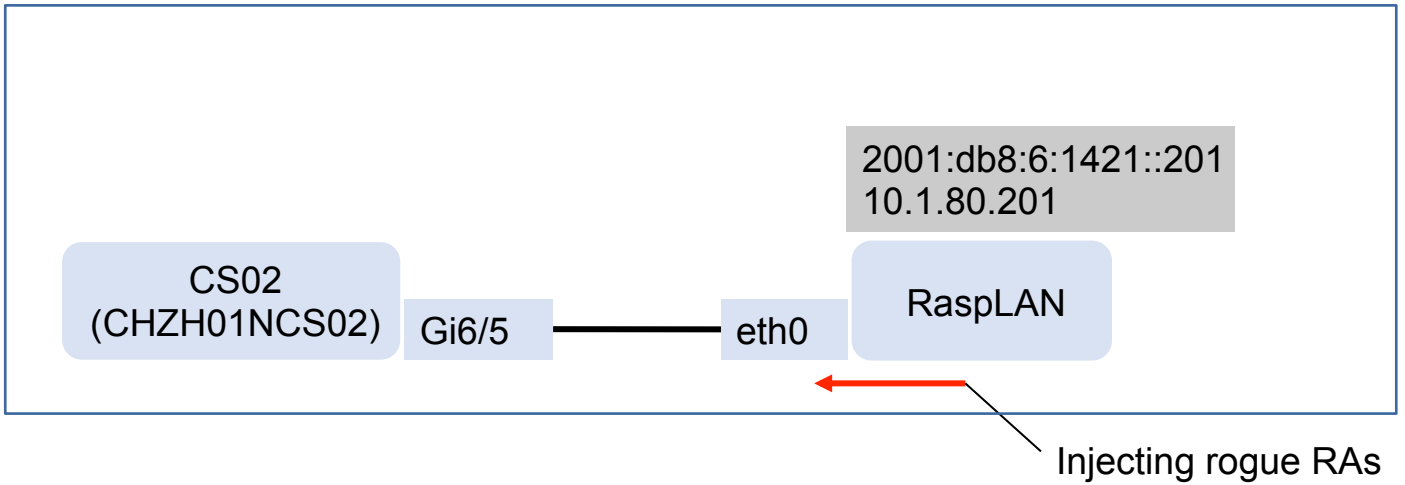
Screen Features

- MLD flooding (continued)
  - Difference MLD vs. MLDv2 (IPv6): ff02::2 vs ff02::16
  - Only listening on ff02::16 ?

```
Cluster01:CHZH01NFW01(M)-> get interface ethernet0/9.10
Interface ethernet0/9.10(VSI):
  description ethernet0/9.10
  number 13, if_info 10584, if_index 10, VLAN tag 1421, mode route
  link up, phy-link up/full-duplex, admin status up
  ipv6 is enable/operable, router mode.
  ipv6 operating mtu 1500, learned mtu 0
  ipv6 Interface-ID: 0210dbfffeff20d0
  ipv6 fe80::210:dbff:feff:20d0/64, link local, PREFIX
  ipv6 2001:db8:6:1421::10/64, global aggregatable, STATEFUL
  ipv6 ff02::1:ffff:20d0, solicited-node scope
  ipv6 ff02::1:ff00:10, solicited-node scope
  vsys Root, zone DMZ - Test01, vr trust-vr, vsd 0
...
```

IPv6 First Hop Security

- Sending evil packets to test
  - RA Guard feature
  - Undetermined Transport feature



- MIB support
  - Checked with Cisco – no MIB / SNMP support
  - Possible solution: use syslog

IPv6 First Hop Security

- RA Guard
  - Config

```
interface GigabitEthernet6/5#
 ipv6 nd raguard
ipv6 snooping logging packet drop
```

  - Injecting RAs

```
root@RaspLAN:/home/pi/thc-ipv6-2.5# ./fake_router26 eth0
Starting to advertise router (Press Control-C to end) ...
```

  - Syslog output

```
Feb 23 20:01:04 chzh01ncs02.awkgroup.com 938: 000944: Feb 23 20:01:03.903
CET: %SISF-4-PAK_DROP: Message dropped A=FE80::BA27:EBFF:FE60:E401 G=-
V=1221 I=Gi6/5 P=NDP::RA Reason=Message unauthorized on port
```

IPv6 First Hop Security

- Undetermined transport
  - Config

```
interface GigabitEthernet6/5#
 ipv6 traffic-filter StopAllRAs in
ipv6 access-list StopAllRAs
 deny icmp any any router-advertisement log-input sequence 10
 deny ipv6 any any log-input undetermined-transport sequence 11
 permit ipv6 any any sequence 20
```

  - Syslog output

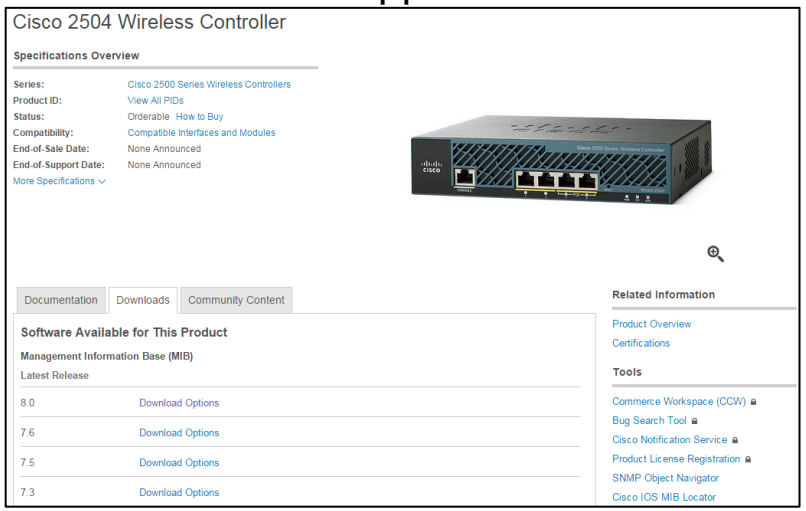
./fake_router26 eth0

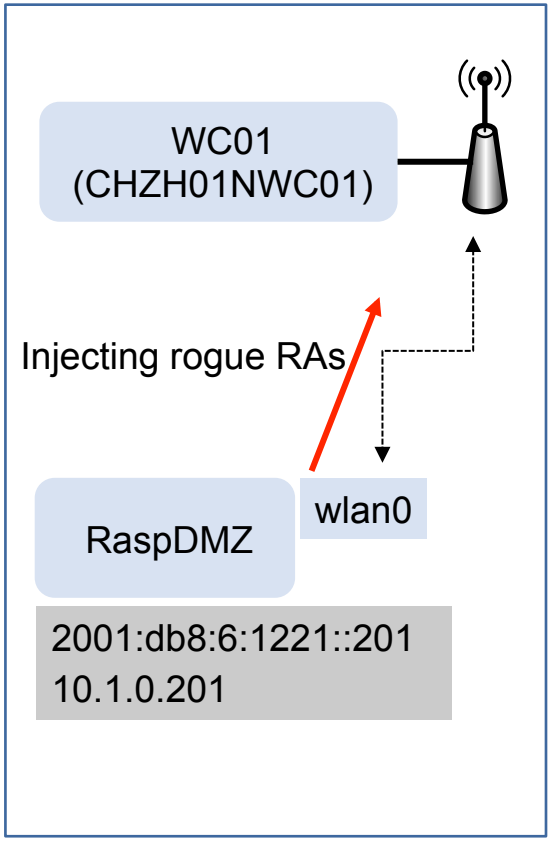
```
Feb 23 19:37:35 chzh01ncs02.awkgroup.com 925: 000931: Feb 23 19:37:34.113
CET: %IPV6_ACL-6-ACCESSLOGDP: list StopAllRAs/10 denied icmpv6
FE80::BA27:EBFF:FE60:E401 (GigabitEthernet6/5 b827.eb60.e401) -> FF02::1
(134/0), 1 packet
Feb 23 19:37:54 chzh01ncs02.awkgroup.com 928: 000934: Feb 23 19:37:53.325
CET: %IPV6_ACL-6-ACCESSLOGNP: list StopAllRAs/11 denied 44
FE80::BA27:EBFF:FE60:E401 (GigabitEthernet6/5 b827.eb60.e401) -> FF02::1,
2 packets
```

./fake_router26 -E D eth0

IPv6 First Hop Security

- WLC implements RA Guard feature
- CISCO-LWAPP-IPV6-MIB
  - allows to query related information via SNMP
  - some sort of ‘semi’-public
    - No hits on google
    - No hits in Cisco SNMP object navigator
    - Only available on product page itself, requires valid support contract to access

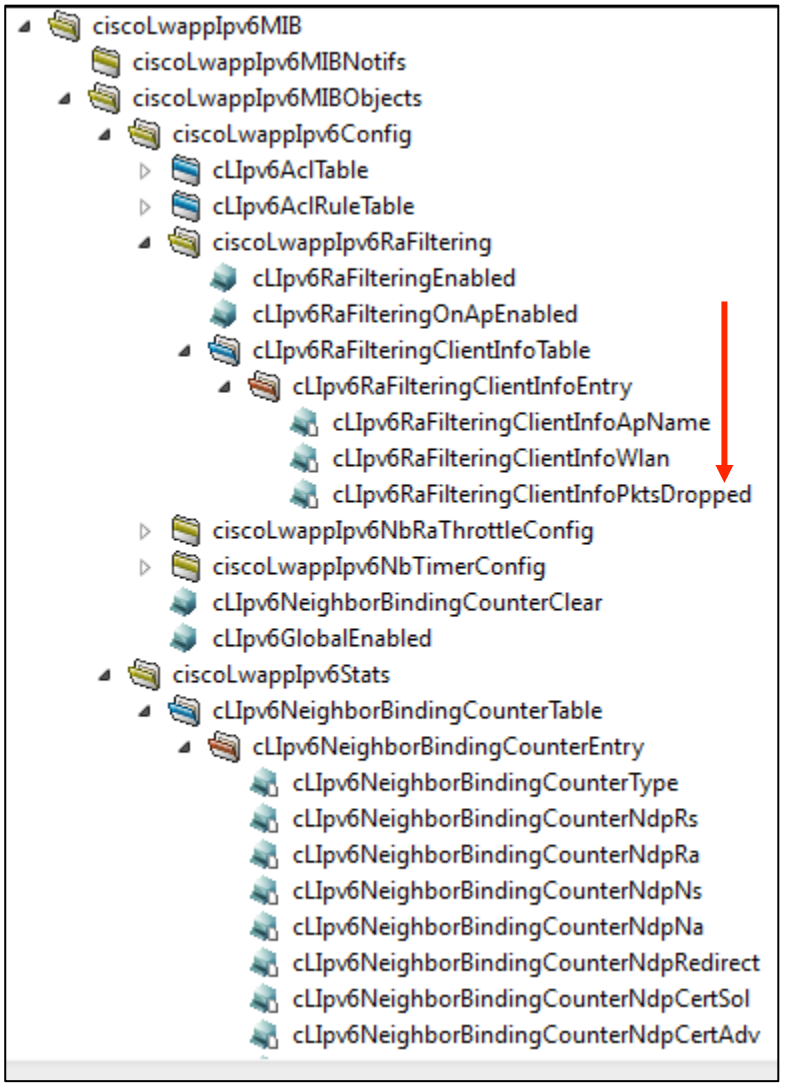




IPv6 First Hop Security

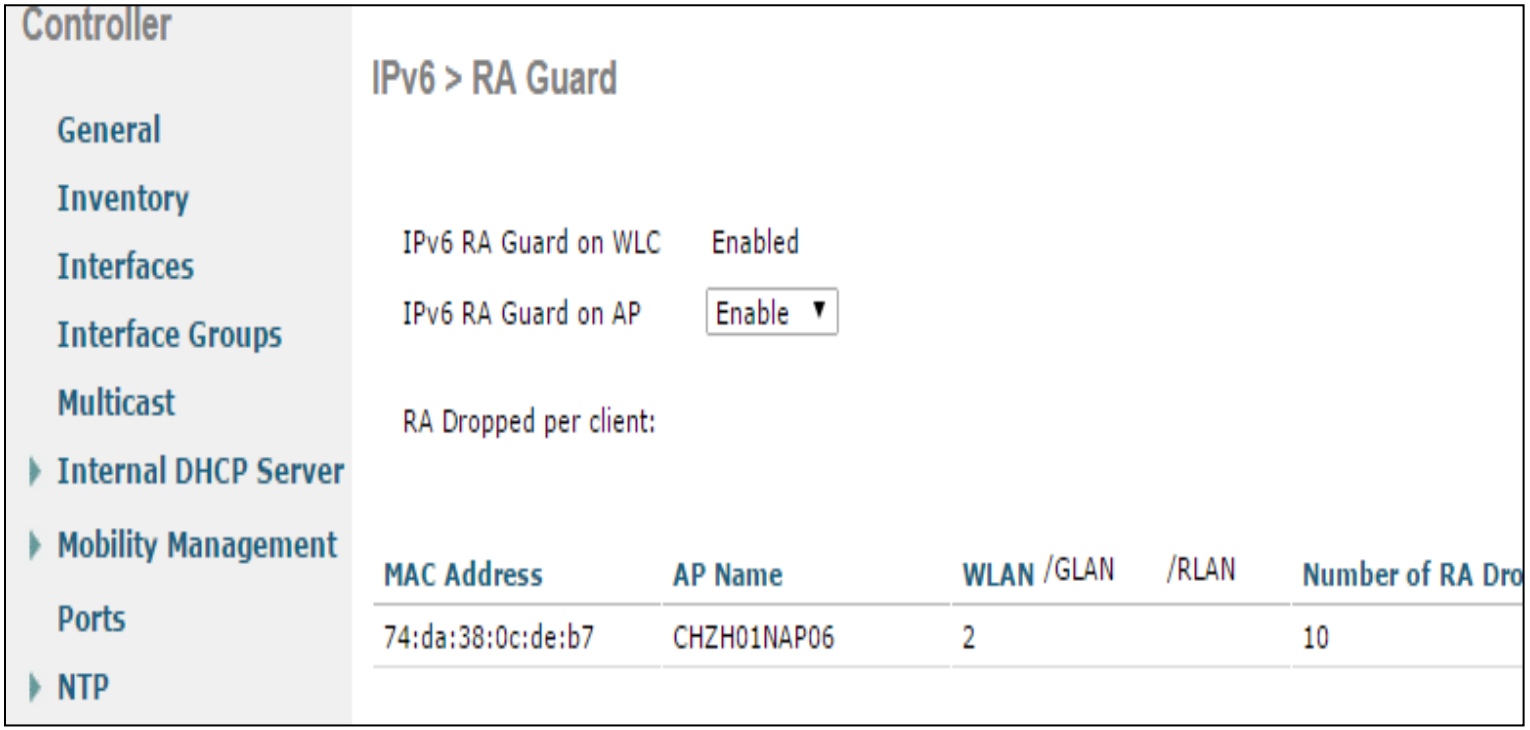
- RA Guard
  - Injecting RAs

```
root@RaspDMZ# ./fake_router26 wlan0
Starting to advertise router (Press Control-C to
end) ...



snmpwalk -v 2c -c … 10.1.225.101 -OX
1.3.6.1.4.1.9.9.9999.1.1.3.3.1.3
…
CISCO-LWAPP-IPV6-
MIB::cLIpv6RaFilteringClientInfoPktsDropped
[STRING: 70:73:cb:e8:a1:b4] = Counter32: 0
CISCO-LWAPP-IPV6-
MIB::cLIpv6RaFilteringClientInfoPktsDropped
[STRING: 74:da:38:c:de:b7] = Counter32: 6
…
```



IPv6 First Hop Security

- RA Guard (continued)
  - GUI



  - Did not detect fragmented RAs
  - Could not find out how to trigger syslog message

Summary

Summary Counters & Routing

Device	Counters IPv4 / IPv6 (Octets per interface in/out	Routing Information IPv4 / IPv6
Cisco 4506E (15.2(2)E1)	Only IPv6 counters, only traffic passing control plane	IPv4: ipCidrRouteEntry (D) IPv6: inetCidrRouteEntry
Cisco 871 (12.4(24)T8)	No interface specific IPv4 & IPv6 counters	IPv4: ipCidrRouteEntry (D) IPv6: n/a
Cisco 28xx (15.2(2)E1)	Counters for IPv4 & IPv6 but wrong values	IPv4: ipCidrRouteEntry (D) IPv6: inetCidrRouteEntry
Ubuntu (14.04 LTS)	Only IPv6 counters, correct values of those counters	IPv4: inetCidrRouteEntry IPv6: inetCidrRouteEntry
Juniper SSG140 (6.3.0r17)	No octet counters (IPv4 & IPv6), counter values wrong	IPv4: ipCidrRouteEntry (D) IPv6: ipv6RouteEntry
Juniper MX960 (12.3R8-S3)	Only IPv6 counters (values could not be challenged)	IPv4: inetCidrRouteEntry IPv6: ipv6RouteEntry

Summary Counters & Routing

- Be reminded
  - IP-MIB: supports IPv4 and IPv6 octet counters (at least the RFC itself)
  - IPv6MIB: only supports IPv6 datagram counters (you need vendor MIB module !)

- What can you do?
  - Long term: push vendors
  - Short term:
    - If you have at least IPv6 counters: IPv4 counters = Octets minus IPv6 Octetes
    - If you do not have IPv6 counters: different (sub)interfaces for IPv4 and IPv6

- What you have to do?
  - Test it !!!

Summary Security

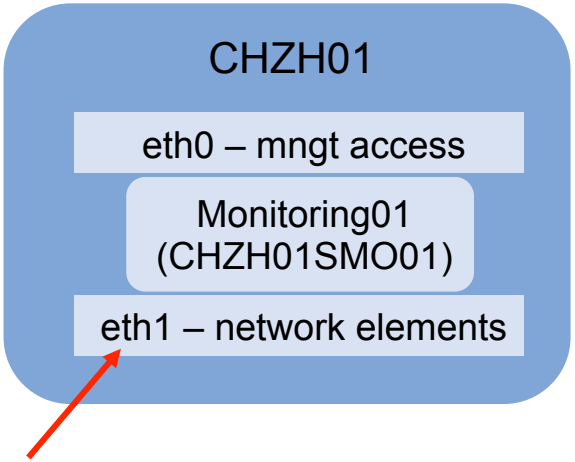
- SNMP
  - (Basic) useful information is often available
  - If not or you need more detailed information, check for syslog capabilities
- Hardware
  - Be prepared to exchange older HW
  - Strongly depends on your network gear and your requirements
  - Testing needed !!!
- Recommendation in general
  - Dualstack networks: only implement (FHS) IPv6 security, if you have similar IPv4 security mechanism already in place

Demo

Demo

Setup Cacti Graph with IPv6 Counters

- Goal: Setup a graph in Cacti which displays the IPv6 traffic of our interface towards the network elements (dualstack network on eth1). To do so we need to
  - Determine OIDs for IPv6 Octets in / out
  - Create data sources in Cacti
  - Create graph in Cacti
  - Download an IOS image on a switch via IPv6
  - Check the graph to see if we can see the traffic



Demo

Lack of IPv6 Capable SNMP Browsers (?)

- SnmpB
- OIDView

Demo

netsnmp CLI Tips & Tricks

- snmptranslate with Tz Option

```
mug@Monitoring01:~$ snmptranslate -Tz -m /var/lib/mibs/ietf/IP-MIB
```

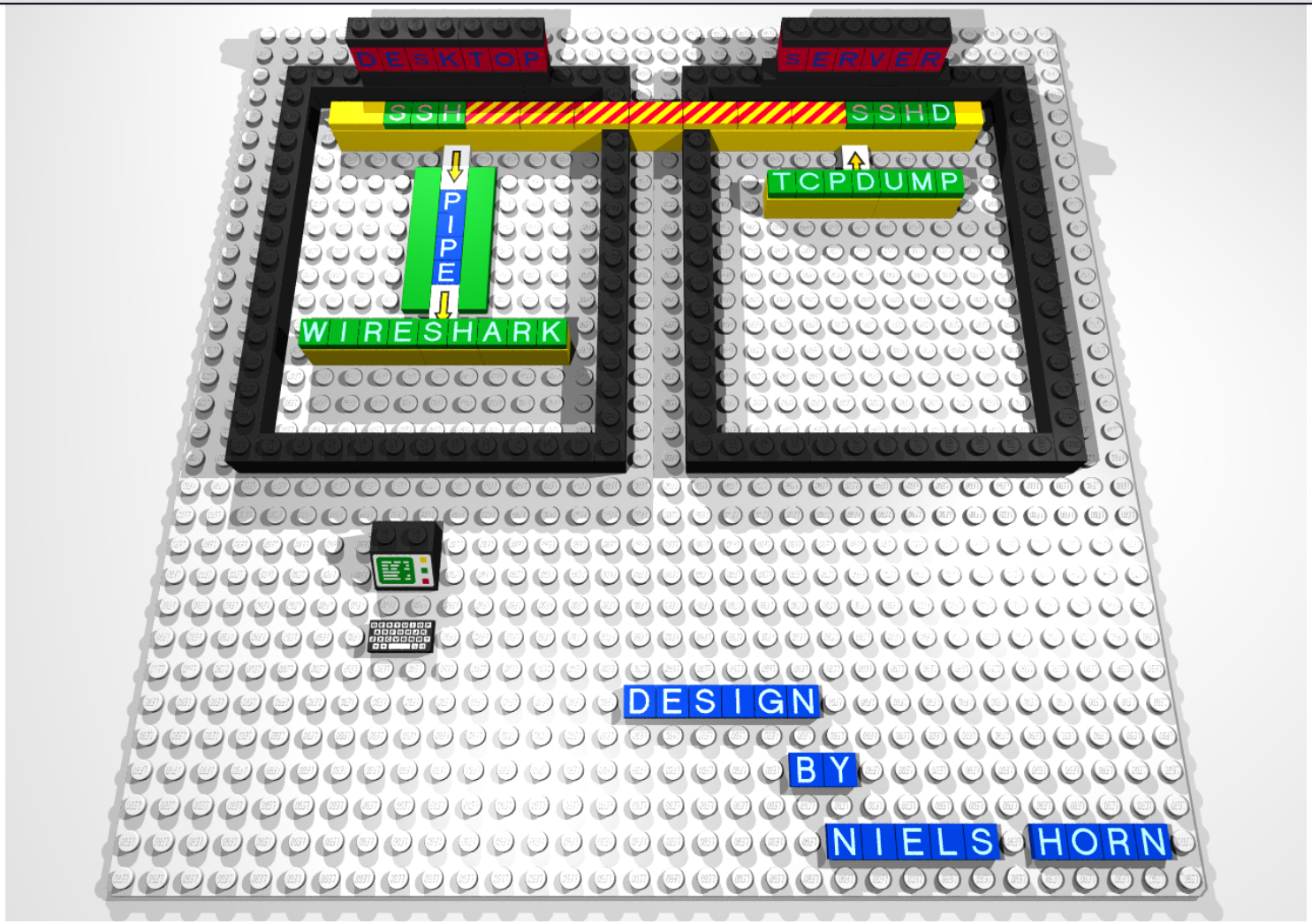
- IP version in OID

```
mug@Monitoring01:~$ snmpwalk -v 2c –c ... -On localhost .1.3.6.1.2.1.4.24.7
```

Demo

Looking at some IPv6 traffic with SSH Tunnel

```
plink.exe -ssh -pw troopers15 root@192.168.21.30 "tcpdump -ni eth1 -
s 0 -U -w -" | "C:\Program Files\Wireshark\Wireshark.exe" -k -i -
```



Appendix

Cisco Catalyst 4506E – Sup6-LE – 15.2(2)E1

IP Address Information

- Information about IP addresses configured on interfaces

```
snmpwalk -v 2c -c … -OX chzh01ncs01 1.3.6.1.2.1.4.34.1.3  //IpAddressTable
IP-MIB::ipAddressIfIndex[ipv6]
        ["20:01:17:02:00:06:10:01:00:00:00:00:00:00:00:20"] …
IP-MIB::ipAddressIfIndex[ipv6]
        ["20:01:17:02:00:06:10:01:00:00:00:00:00:00:00:21"] …
```

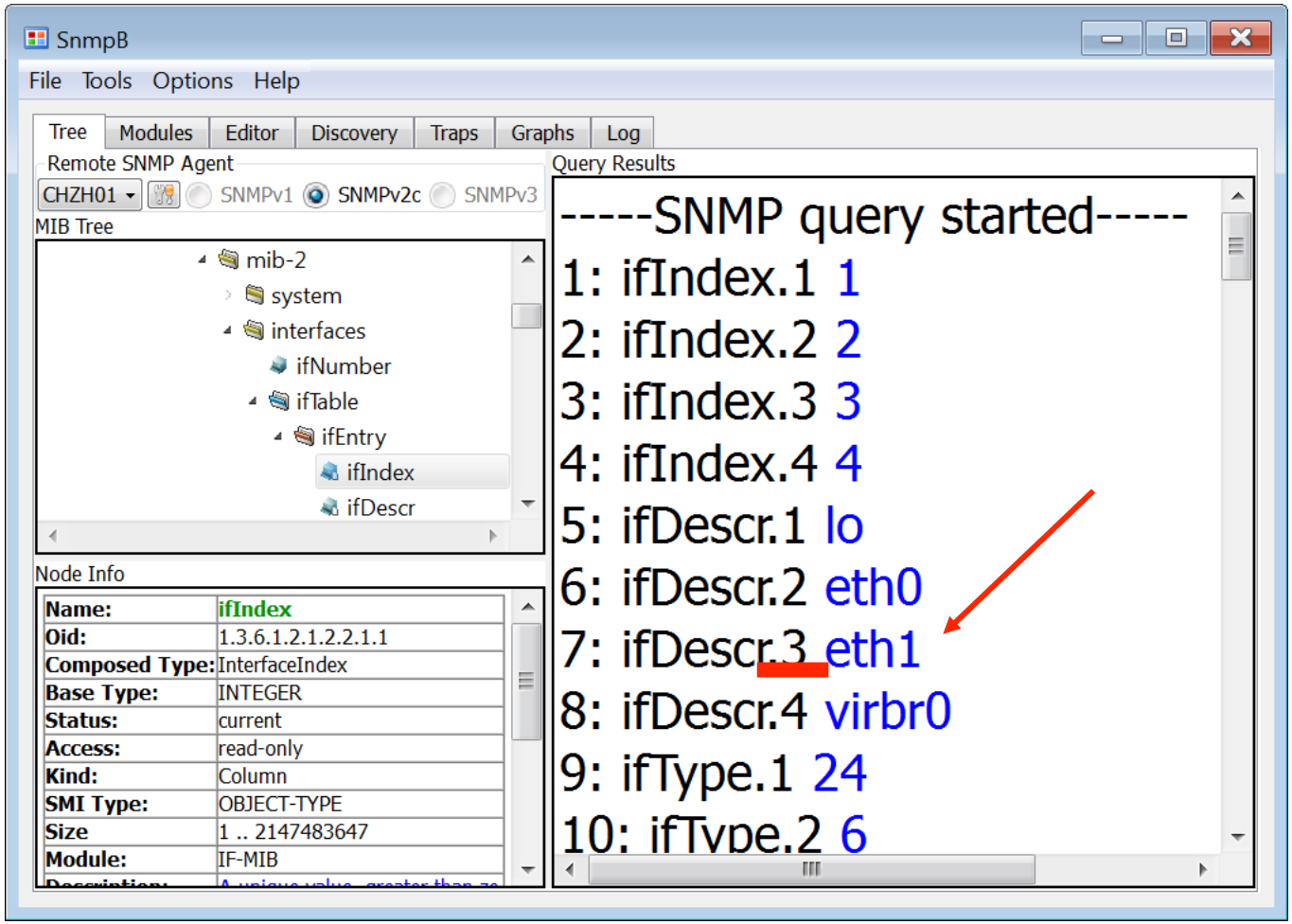
```
snmpwalk -v 2c -c … -OX chzh01ncs01 1.3.6.1.2.1.4.20.1.2  //IpAddrTable
IP-MIB::ipAdEntIfIndex[10.1.224.10] = INTEGER: 188
IP-MIB::ipAdEntIfIndex[10.1.224.11] = INTEGER: 188
```

  - IpAddressTable only contains IPv6 information
  - IPv4 information still contained in deprecated IpAddrTable

Demo (detailed)

Setup Cacti Graph with IPv6 Counters

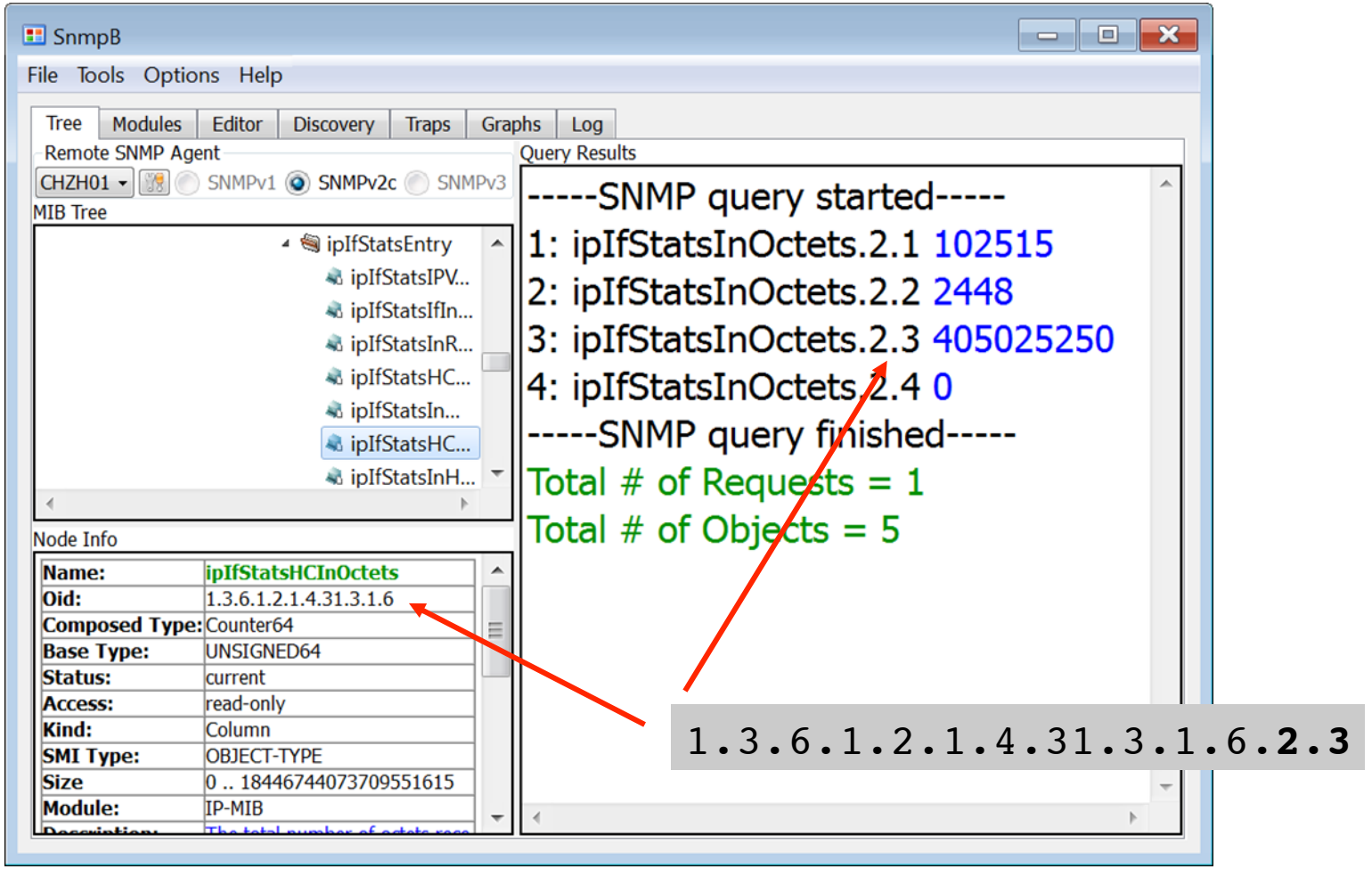
- Determine interface index



Demo (detailed)

Setup Cacti Graph with IPv6 Counters

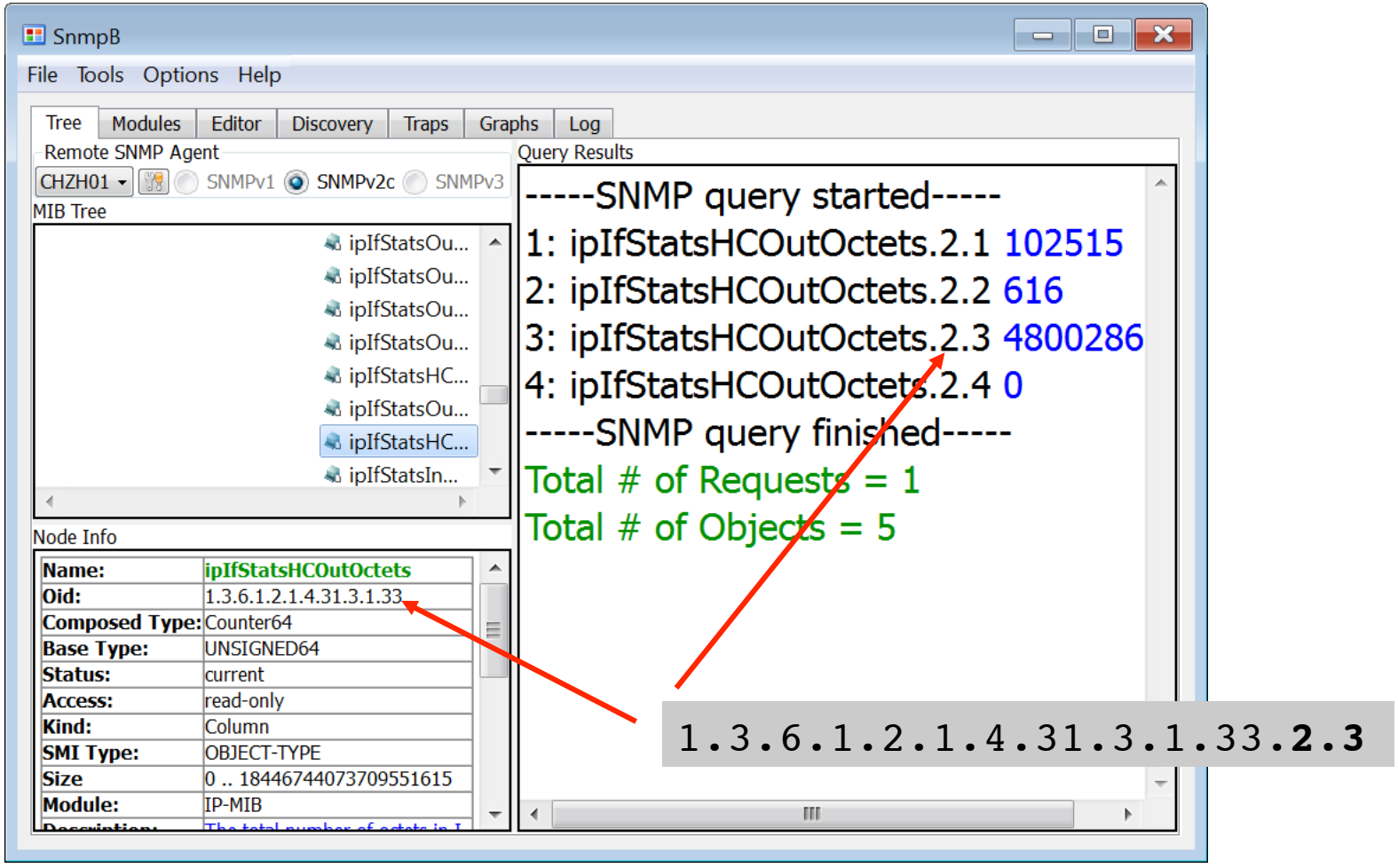
- Determine OID for IPv6 Octets in



Demo (detailed)

Setup Cacti Graph with IPv6 Counters

- Determine OID for IPv6 Octets out



Demo (detailed)

Setup Cacti Graph with IPv6 Counters

- On the console this would look like this
  - Getting interface index

```
mug@Monitoring01:~$ snmpwalk -v 2c –c … localhost 1.3.6.1.2.1.2.2.1 | grep eth1
IF-MIB::ifDescr.3 = STRING: eth1
```

  - Getting OID for IPv6 Octets in

```
mug@Monitoring01:~$ snmpwalk -v 2c -c … localhost 1.3.6.1.2.1.4.31.3.1.6
IP-MIB::ipIfStatsHCInOctets.ipv6.1 = Counter64: 102515
IP-MIB::ipIfStatsHCInOctets.ipv6.2 = Counter64: 2448
IP-MIB::ipIfStatsHCInOctets.ipv6.3 = Counter64: 405149079
IP-MIB::ipIfStatsHCInOctets.ipv6.4 = Counter64: 0
```

  - Validate OID (Octets in)

```
mug@Monitoring01:~$ snmpwalk -v 2c –c … localhost 1.3.6.1.2.1.4.31.3.1.6.2.3
IP-MIB::ipIfStatsHCInOctets.ipv6.3 = Counter64: 405158047
```

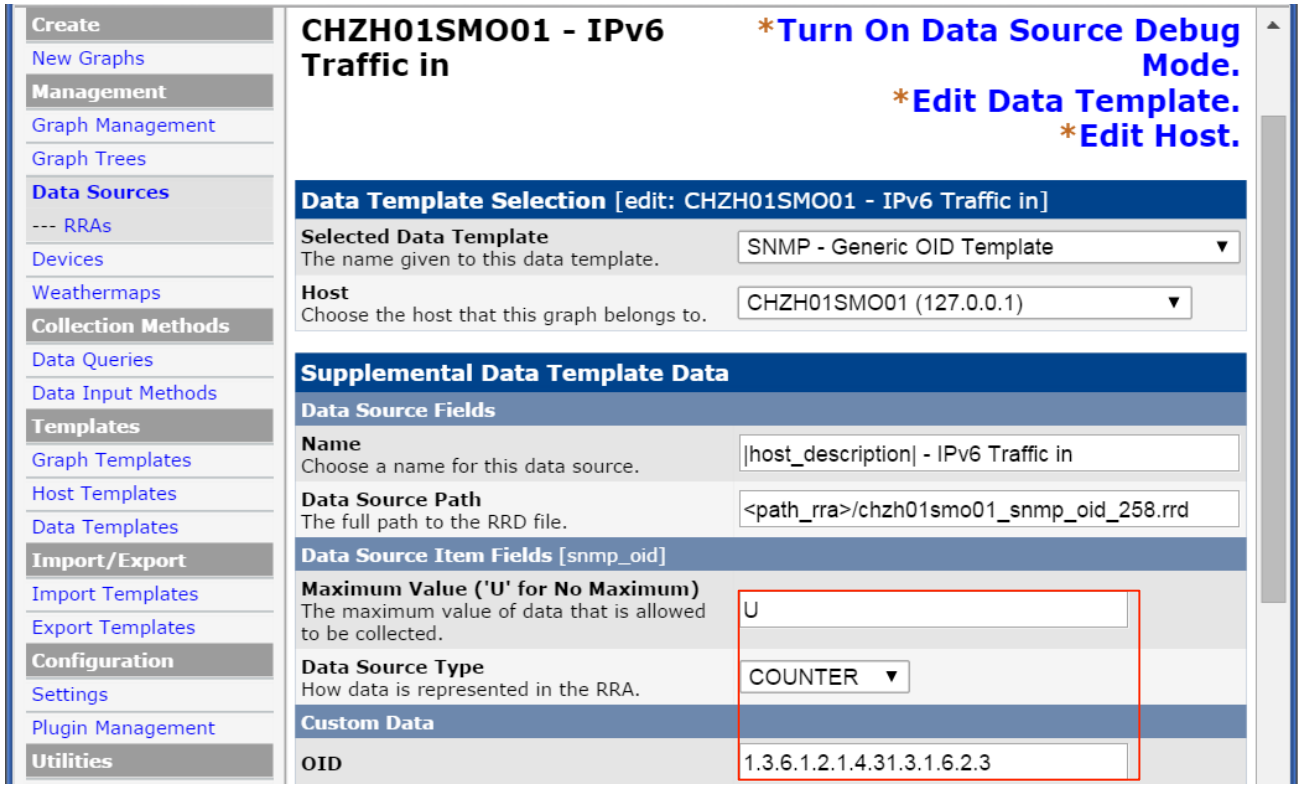
  - Validate OID (Octets out)

```
mug@Monitoring01:~$ snmpwalk -v 2c -c … localhost 1.3.6.1.2.1.4.31.3.1.33.2.3
IP-MIB::ipIfStatsHCOutOctets.ipv6.3 = Counter64: 480142638
```

Demo (detailed)

Setup Cacti Graph with IPv6 Counters

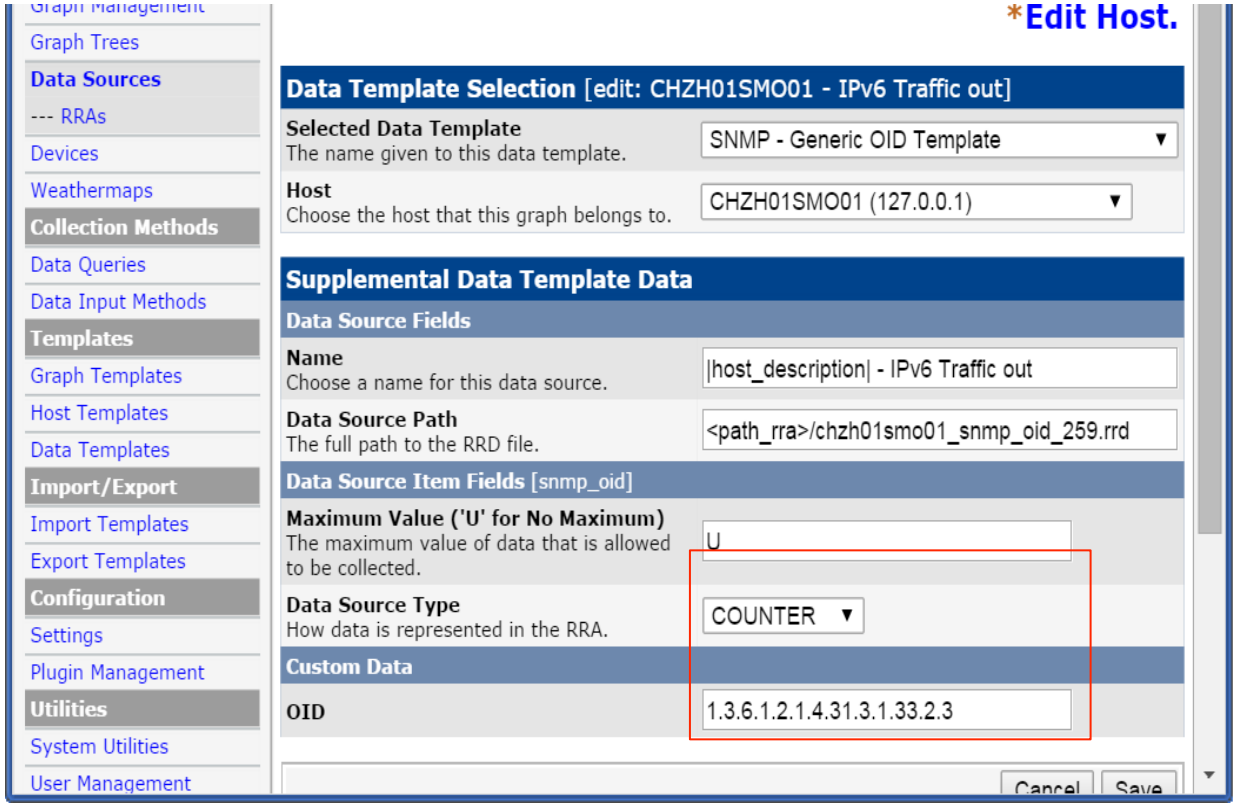
- Console > Data Sources > Add
  - Data Template: Select *SNMP Generic OID Template*
  - *(On next screen) Enter OID*



Demo (detailed)

Setup Cacti Graph with IPv6 Counters

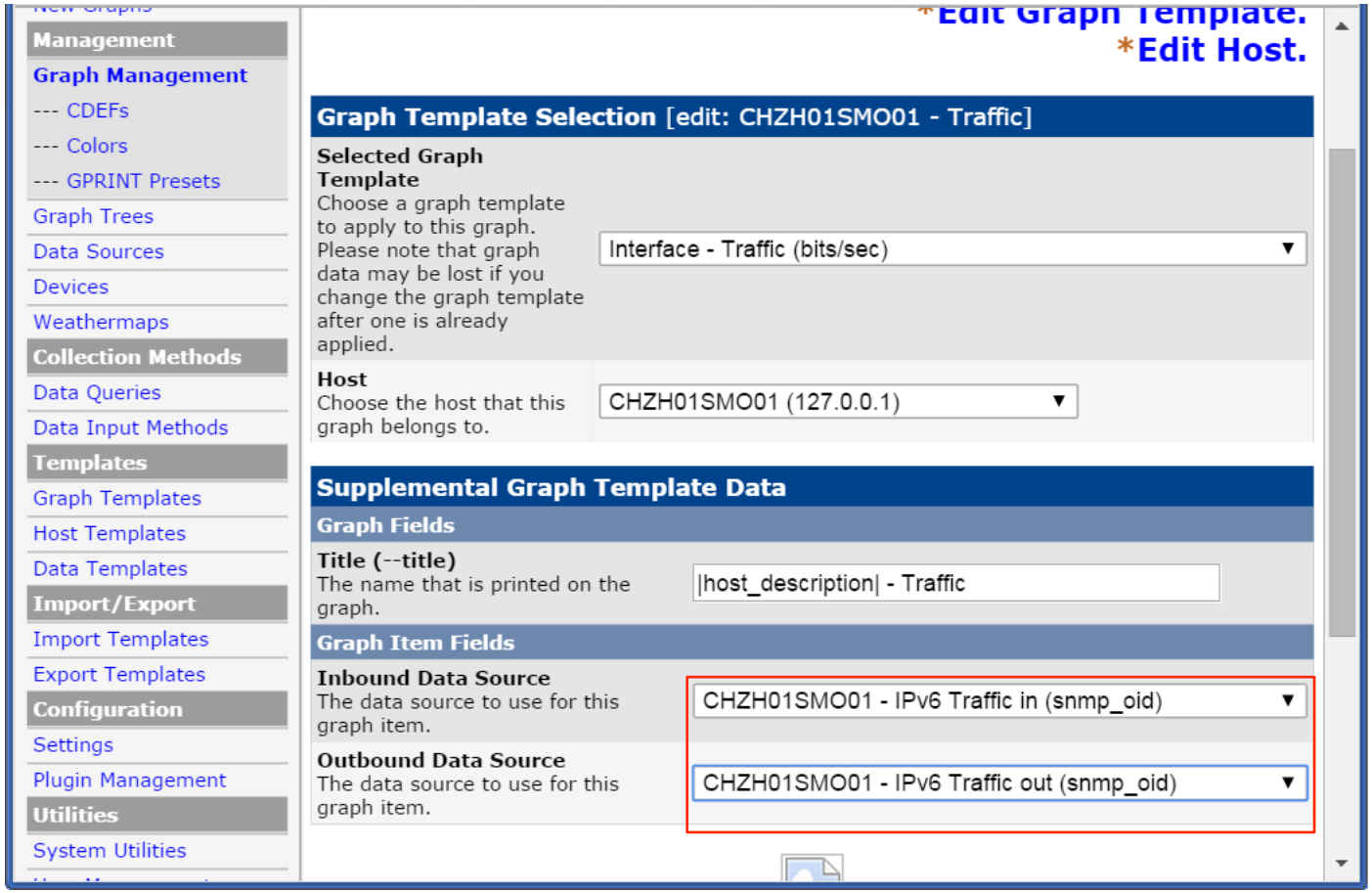
— *Repeat for OctetsOut counter*



Demo (detailed)

Setup Cacti Graph with IPv6 Counters

- Create Graph
  - Graph Management > Add



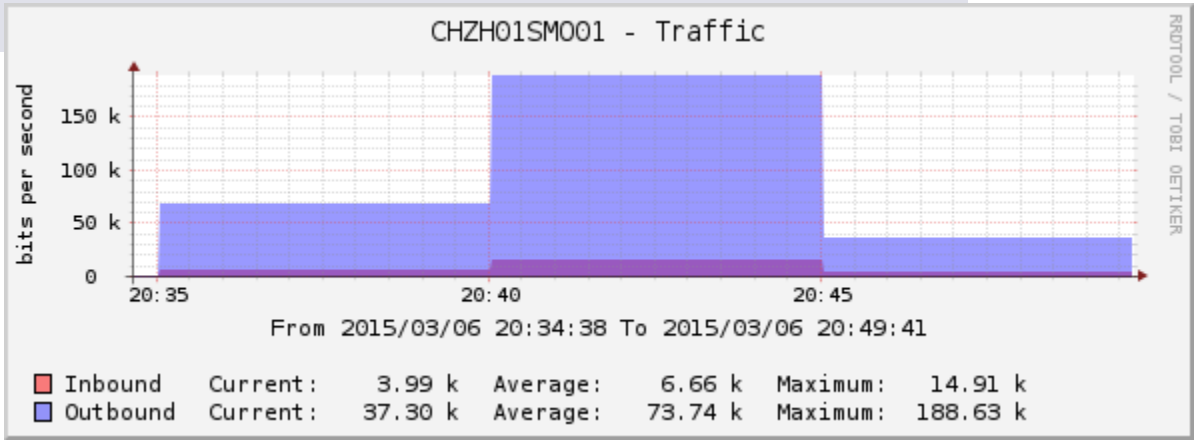
Demo (detailed)

Setup Cacti Graph with IPv6 Counters

- Generate some traffic

```
CHZH01NCS01#copy scp: bootflash:
Address or name of remote host []? 2001:db8:6:1191::101
Source username [mug]?
Source filename []? /home/mug/IOS/c1140-k9w7-tar.152-2.JB.tar
Destination filename [c1140-k9w7-tar.152-2.JB.tar]?
Password:
 Sending file modes: C0664 10352640 c1140-k9w7-tar.152-2.JB.tar
!!!!!!!...
10352640 bytes copied in 28.596 secs (362031 bytes/sec)
CHZH01NCS01#
```

- Looking at the graph

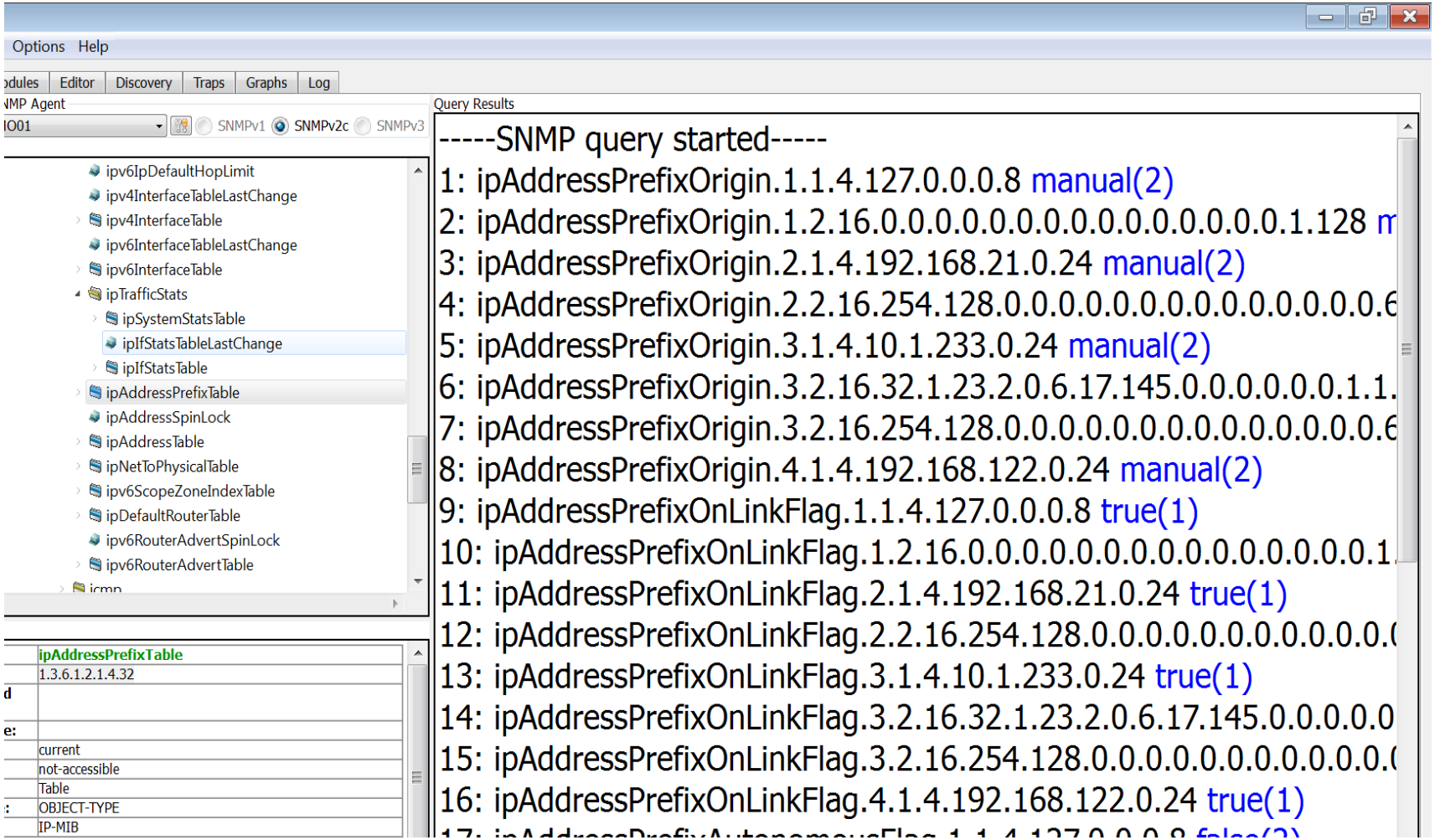


Demo (detailed)

Lack of IPv6 Capable SNMP Browsers (?)

- SnmpB

Where is fe:80:00:00:00:00:00:00:00:00:00:00:00:00:00:00

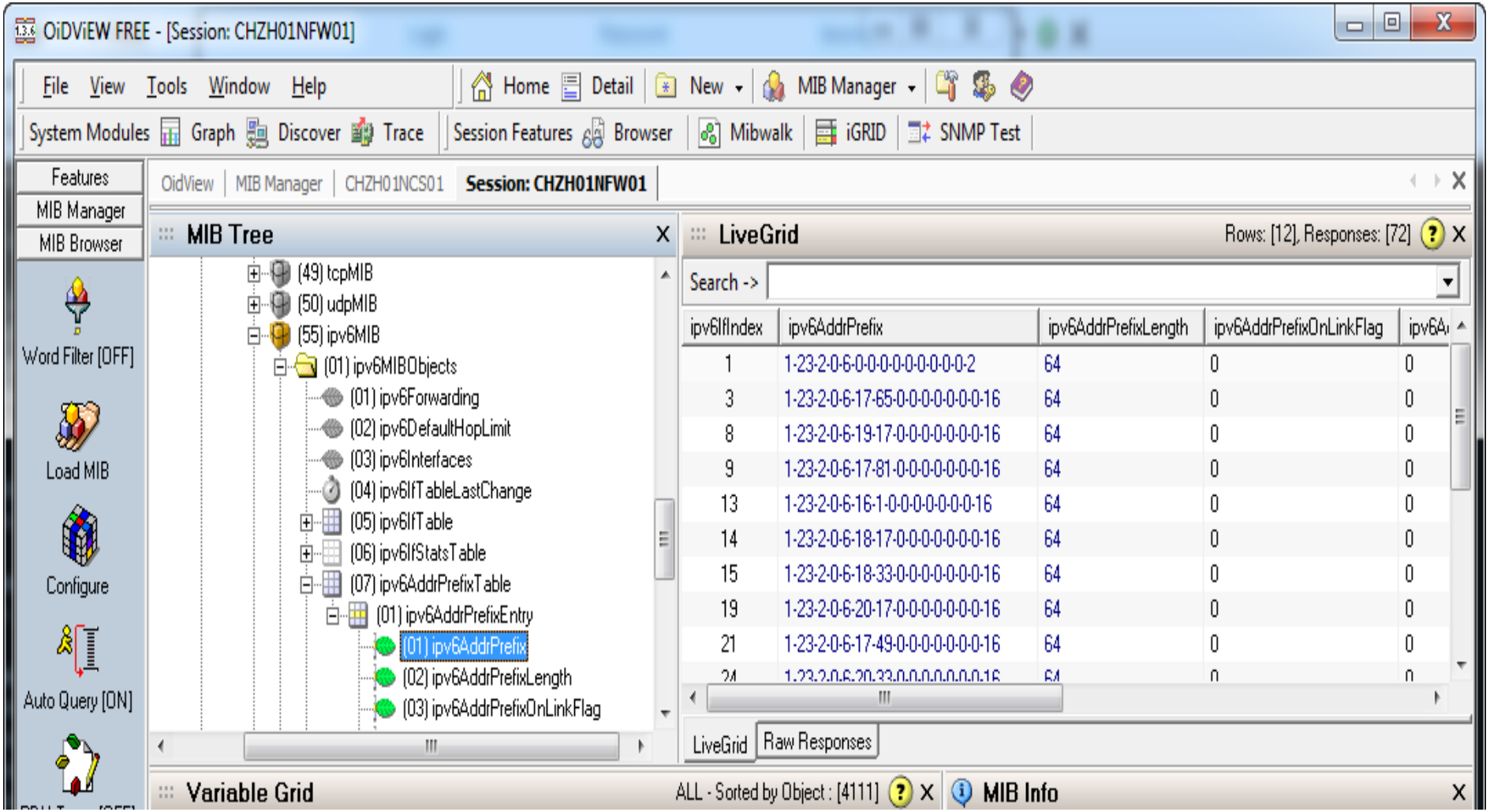


Demo (detailed)

Lack of IPv6 Capable SNMP Browsers (?)

- OIDView

Where is 2001:db8:6:0:0:0:0:2



Demo (detailed)

netsnmp CLI Tips & Tricks

- OX Option
  - Without (IPv6MIB – AddressTable (Juniper MX960))

```
muellega@T430s:~$ snmpwalk -v 2c -c … … 1.3.6.1.2.1.55.1.8.1
…
IPV6-MIB::ipv6AddrStatus.16.' ..............' = INTEGER: preferred(1)
IPV6-MIB::ipv6AddrStatus.16.'............^n&' = INTEGER: preferred(1)
IPV6-MIB::ipv6AddrStatus.18.'..............' = INTEGER: preferred(1)
…
```

  - With OX Option

```
muellega@T430s:~$ snmpwalk -v 2c -c … -OX … 1.3.6.1.2.1.55.1.8.1
…
IPV6-MIB::ipv6AddrStatus[16][STRING: 2001:1704:0:0:0:0:0:b] = INTEGER: …
IPV6-MIB::ipv6AddrStatus[16][STRING: fe80:0:0:0:2a0:a50f:fc5e:6e26] = INTEGER: …
IPV6-MIB::ipv6AddrStatus[18][STRING: fe80:0:0:0:200:ff:fe00:4] = INTEGER: …
…
```

Demo (detailed)

netsnmp CLI Tips & Tricks

- snmptranslate with Tz Option

```
mug@Monitoring01:~$ snmptranslate -Tz -m /var/lib/mibs/ietf/IP-MIB
…
"ipIfStatsEntry"                          "1.3.6.1.2.1.4.31.3.1"
"ipIfStatsIPVersion"                      "1.3.6.1.2.1.4.31.3.1.1"
"ipIfStatsIfIndex"                        "1.3.6.1.2.1.4.31.3.1.2"
"ipIfStatsInReceives"                     "1.3.6.1.2.1.4.31.3.1.3"
"ipIfStatsHCInReceives"                   "1.3.6.1.2.1.4.31.3.1.4"
"ipIfStatsInOctets"                       "1.3.6.1.2.1.4.31.3.1.5"
"ipIfStatsHCInOctets"                     "1.3.6.1.2.1.4.31.3.1.6"
"ipIfStatsInHdrErrors"                    "1.3.6.1.2.1.4.31.3.1.7"
…
```

Demo (detailed)

Netsnmp CLI Tips & Tricks

- IP version in OID

```
mug@Monitoring01:~$ snmpwalk -v 2c –c … -On localhost .1.3.6.1.2.1.4.24.7
.1.3.6.1.2.1.4.24.7.1.7.1.4.0.0.0.0.0.2.0.0.1.4.192.168.21.1 = INTEGER: 2
.1.3.6.1.2.1.4.24.7.1.7.1.4.10.1.224.0.19.2.0.0.1.4.10.1.233.10 = INTEGER: 3
.1.3.6.1.2.1.4.24.7.1.7.1.4.10.1.233.0.24.3.0.0.3.1.4.0.0.0.0 = INTEGER: 3
.1.3.6.1.2.1.4.24.7.1.7.1.4.10.101.224.0.20.2.0.0.1.4.10.1.233.10 = INTEGER: 3
.1.3.6.1.2.1.4.24.7.1.7.1.4.10.101.248.0.24.2.0.0.1.4.10.1.233.10 = INTEGER: 3
.1.3.6.1.2.1.4.24.7.1.7.1.4.10.102.224.0.20.2.0.0.1.4.10.1.233.10 = INTEGER: 3
.1.3.6.1.2.1.4.24.7.1.7.1.4.10.102.248.0.24.2.0.0.1.4.10.1.233.10 = INTEGER: 3
.1.3.6.1.2.1.4.24.7.1.7.1.4.192.168.21.0.24.3.0.0.2.1.4.0.0.0.0 = INTEGER: 2
.1.3.6.1.2.1.4.24.7.1.7.1.4.192.168.122.0.24.3.0.0.4.1.4.0.0.0.0 = INTEGER: 4
.
1.3.6.1.2.1.4.24.7.1.7.2.16.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.3.0.0.19.2.16.254.1
28.0.0.0.0.0.0.17.145.0.0.0.0.0.16 = INTEGER: 3
```

References

Links

- History of IP MIBs (Cisco)
  - http://www.cisco.com/web/about/security/intelligence/ipv6_mib.html
- IPv6 FHS Wiki Cisco
  - http://docwiki.cisco.com/wiki/FHS
- Cisco MIB Explorer
  - http://tools.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&step=2
- Juniper MIB Explorer
  - http://contentapps.juniper.net/mib-explorer/
- Concepts & Examples – ScreenOS Reference Guide
  (Attack Detection and Defense Mechanisms)
  - http://www.juniper.net/techpubs/software/screenos/screenos6.3.0/630_ce_AttackDetection.pdf
- NetSNMP
  - http://www.net-snmp.org/docs/mibs/ip.html (IP MIB)
  - http://www.net-snmp.org/docs/mibs/ipForward.html (IP FORWARDING MIB)
  - http://www.net-snmp.org/docs/mibs/ipv6MIB.html (IPv6MIB)
- IPv6 health check
  - https://www.mythic-beasts.com/ipv6/health-check
- The 20-Minute SNMP Tutorial - Automating System Administration with Perl
  - http://archive.oreilly.com/pub/a/perl/excerpts/system-admin-with-perl/twenty-minute-snmp-tutorial.html

IPv6 MIB Modules

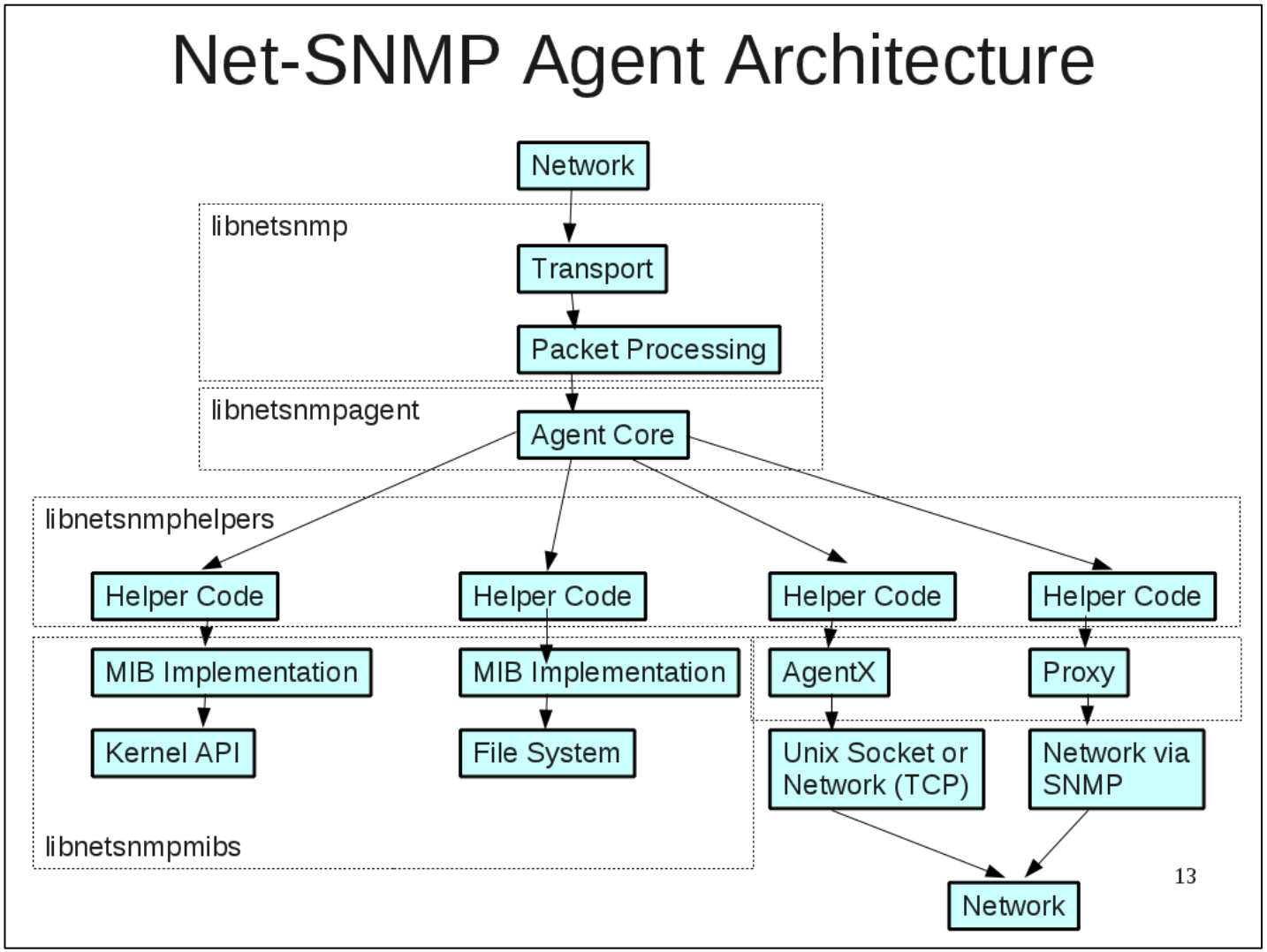
IP Address Types in MIBs

- Representation of IPv6 addresses in MIBs
  - IP-MIB: InetAddressIPv6 (16 octets) (RFC 4001 - INET-ADDRESS-MIB)
  - IPv6-MIB: Ipv6Address (16 octets) (RFC 2465 – IPv6-MIB)

```
InetAddress ::= TEXTUAL-CONVENTION
    STATUS      current
    DESCRIPTION
        "Denotes a generic Internet address...
    SYNTAX      OCTET STRING (SIZE (0..255))

InetAddressIPv6 ::= TEXTUAL-CONVENTION
    DISPLAY-HINT "2x:2x:2x:2x:2x:2x:2x:2x"
    STATUS      current
    DESCRIPTION
        "Represents an IPv6 network address:...

    SYNTAX      OCTET STRING (SIZE (16))

InetAddressType ::= TEXTUAL-CONVENTION (RFC 4001)
    …
   ipv4(1)     An IPv4 address as defined by the
               InetAddressIPv4 textual convention.
   ipv6(2)     An IPv6 address as defined by the
               InetAddressIPv6 textual convention.
   ipv4z(3)    A non-global IPv4 address including a zone
               index as defined by the InetAddressIPv4z
               textual convention.
   ipv6z(4)    A non-global IPv6 address including a zone
               index as defined by the InetAddressIPv6z
               textual convention.
```

```
Ipv6Address ::= TEXTUAL-CONVENTION
     DISPLAY-HINT "2x:"
     STATUS      current
     DESCRIPTION
       "This data type is used to model IPv6 addresses.
        This is a binary string of 16 octets in network
        byte-order."
     SYNTAX      OCTET STRING (SIZE (16))
```

netsnmp Agent



Source: http://www.net-snmp.org/wiki

Test Setup

Picture

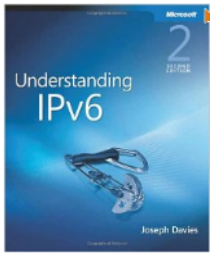
Juniper SRX-210HE – Junos 12.1X44-D35.5

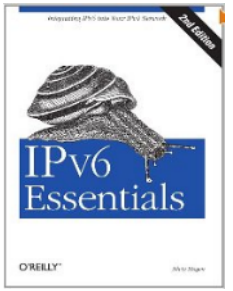
Counting IPv4 octets with policy (from Juniper Support - not validated)

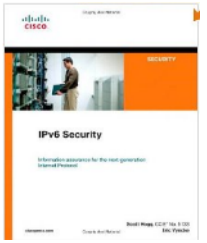
```
set firewall family inet filter ipv4_byte_count term t1 from source-address 0.0.0.0/0
set firewall family inet filter ipv4_byte_count term t1 from destination-address 0.0.0.0/0
set firewall family inet filter ipv4_byte_count term t1 then count ipv4_byte_counter
set firewall family inet filter ipv4_byte_count term t1 then accept
set firewall family inet filter ipv4_byte_count term default then accept
set interfaces ge-0/0/0 unit 0 family inet filter input ipv4_byte_count

// Information than can be optained at the following positions
.1.3.6.1.4.1.2636.3.5.2.1.5 contains your counters
.1.3.6.1.4.1.2636.3.5.2.1.6 contains your filter names
.1.3.6.1.4.1.2636.3.5.2.1.7 contains your counter names

// Get OIDs
snmpbulkwalk jnpr .1.3.6.1.4.1.2636.3.5.2.1.7 | grep ipv4_byte_count
"1.3.6.1.2.1.4.31.3.1.7"
…
```

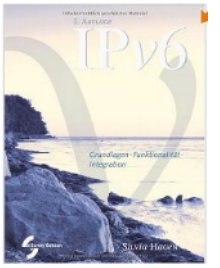
Recommended Reading

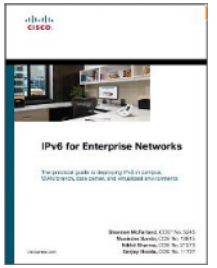
- Understanding IPv6, Second Edition
  - ISBN-13: 978-0735624467
- IPv6 Essentials
  - ISBN-13: 978-0596100582
- IPv6 Security
  - ISBN-13: 978-1587055942
- IPv6. Grundlagen - Funktionalität - Integration
  - ISBN-13: 978-3952294222
- IPv6 for Enterprise Networks
  - ISBN-13: 978-1587142277
- Planning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

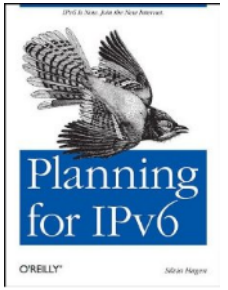












Recommended Reading

- 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
- Essential SNMP – 2nd Edition
  - ISBN-13: 978-0-596-00840-6