AWK GROUP

Consulting
Engineering
Project Management

Tools for Troubleshooting and Monitoring IPv6 Networks

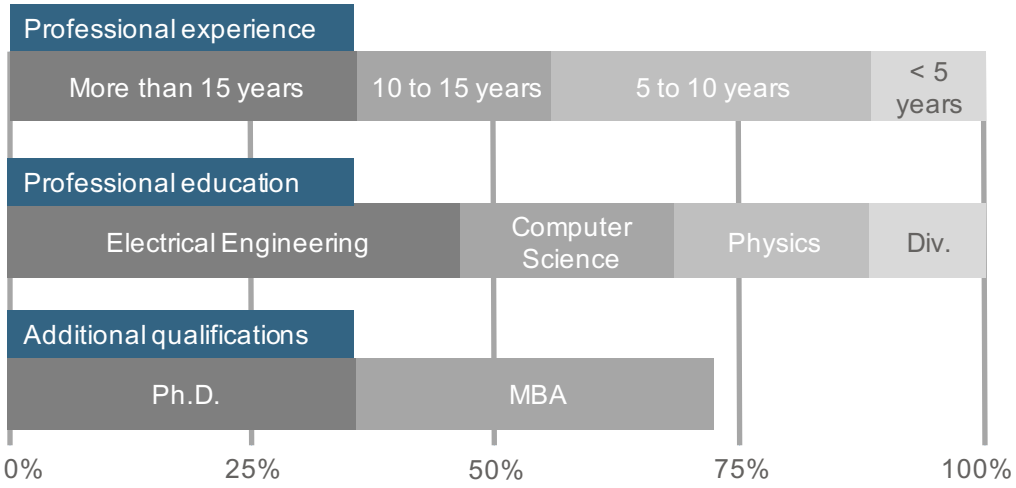
Troopers, 15th of March 2016

Gabriel Müller, Senior Consultant

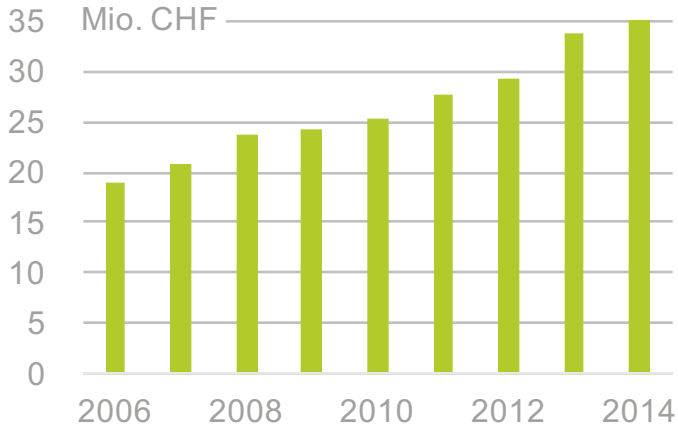
Facts and Figures

Activity	Consulting, engineering und project management for information technology from a single source
Owner	The share capital is wholly owned by the partners
Founded in	1986
Employees	Over 170 staff
Clients	Over 400
Projects	Over 4‘000
Site Locations	Zurich, Berne, Basle, Lausanne

Qualification of our Consultants



Turnover



Partners of AWK

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

Content

Prepare you for the real hard life out there

```
trooper@UbuntuTeacher:~$ ping galileo.troopers
… -> success

trooper@UbuntuTeacher:~$ ping6 galileo.troopers
… -> fails
```

```
trooper@UbuntuTeacher:~$ ping6 <IPv6 address>
… -> fails
trooper@UbuntuTeacher:~$ ping6 –I eth0 <IPv6 link local address>
… -> fails
```

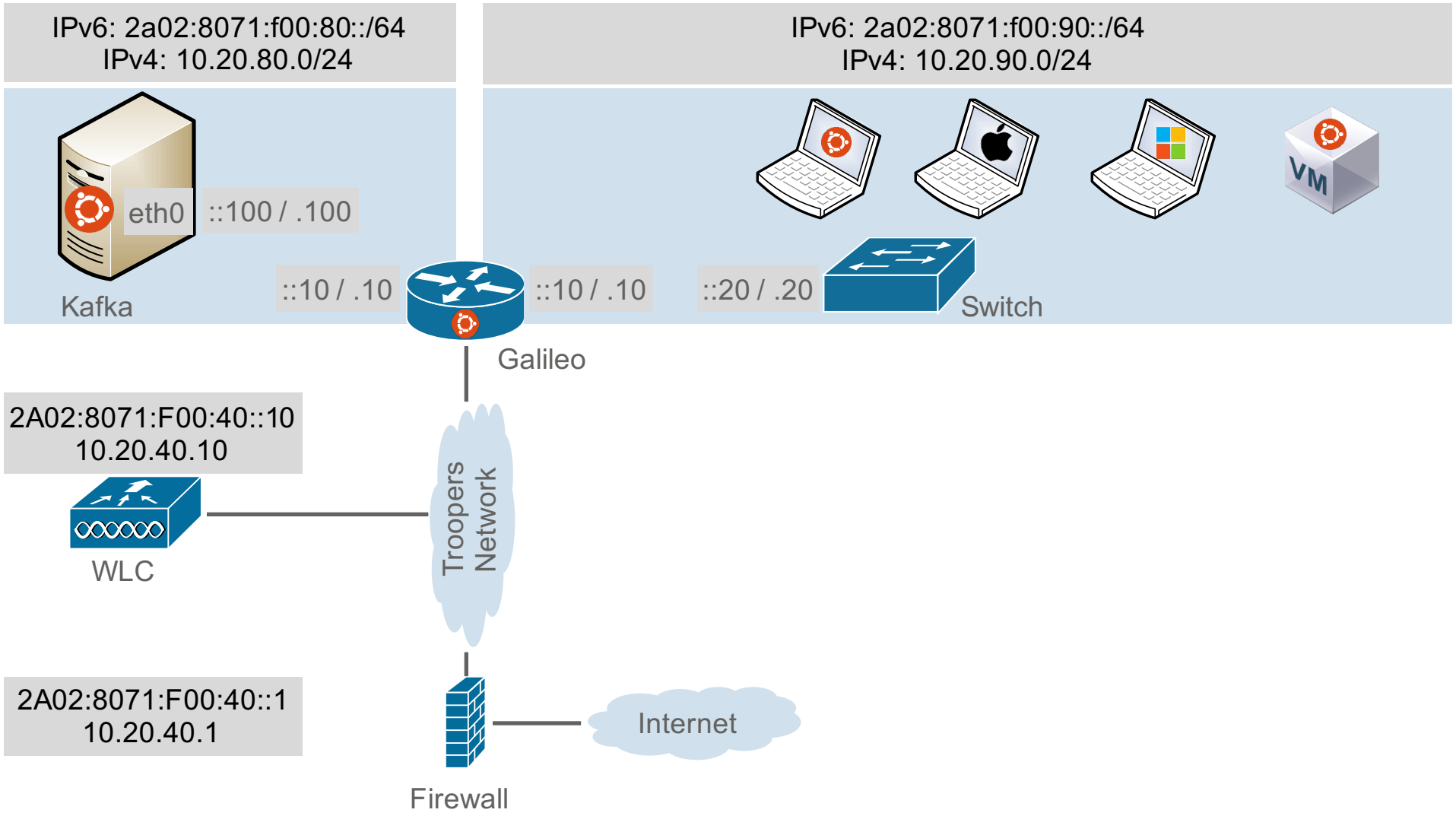
```
trooper@UbuntuTeacher:~$ dmesg
…
[   10.445996] IPv6: eth0: IPv6 duplicate address fe80::20c:29ff:fef7:c14 detected!
…
[  424.570259] IPv6: eth0: IPv6 duplicate address …:4875:f3c:c541:a01d detected!
[  424.953870] IPv6: eth0: IPv6 duplicate address …:20c:29ff:fef7:c14 detected!
[  425.105647] IPv6: eth0: IPv6 duplicate address …:ccc3:fa8f:3052:9409 detected!
[  425.736880] IPv6: eth0: IPv6 duplicate address …:c4f5:c7f3:42fa:5e07 detected!
[  425.736891] IPv6: ipv6_create_tempaddr: regeneration time exceeded - disabled
temporary address support
```

Prepare you for the real hard life out there

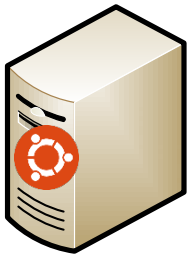
```
trooper@Ubuntu:~$ sudo sysctl net.ipv6.conf.eth0.accept_dad=0
[sudo] password for trooper:
net.ipv6.conf.eth0.accept_dad = 0
trooper@Ubuntu:~$ ping6 -I eth0 fe80::20c:29ff:fef7:c14
connect: Cannot assign requested address

trooper@Ubuntu:~$ sudo ifconfig eth0 down
trooper@Ubuntu:~$ sudo ifconfig eth0 up

trooper@Ubuntu:~$ ping6 -I eth0 fe80::20c:29ff:fef7:c14
PING fe80::20c:29ff:fef7:c14(fe80::20c:29ff:fef7:c14) from fe80:… eth0: 56 data
64 bytes from fe80::20c:29ff:fef7:c14: icmp_seq=1 ttl=64 time=0.207 ms
64 bytes from fe80::20c:29ff:fef7:c14: icmp_seq=2 ttl=64 time=0.103 ms^C---
trooper@Ubuntu:~$ ping6 galileo.troopers
PING galileo.troopers(galileo.troopers) 56 data bytes
64 bytes from galileo.troopers: icmp_seq=1 ttl=64 time=1.13 ms
64 bytes from galileo.troopers: icmp_seq=2 ttl=64 time=1.03 ms
```

Content

The Big Picture



Addressing and Services (1/3)



Kafka

Addressing
IPv6: 2a02:8071:f00:80::100
IPv4: 10.20.80.100
DNS Records
– kafka.troopers (v4 & v6)
– kafka6.troopers (v6 only)
– kafka4.troopers (v4 only)

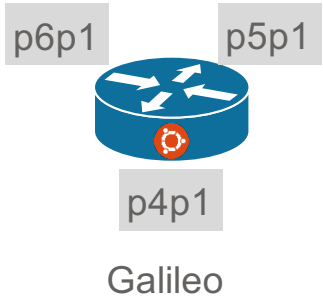
File Services
/home/trooper
- NFS
- SMB
- SCP

System Services
Various
- snmpd (port 161/udp)
- ntpd (port 123/udp)

Web Services
kafka.troopers
- observium (port 80)
- ntopng (port 3000)

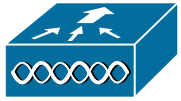
Addressing and Services (2/3)

Addressing
IPv6: 2A02:8071:f00:40::200 (p4p1)
IPv6: 2a02:8071:f00:90::10 (p5p1)
IPv6: 2a02:8071:f00:80::10 (p6p1)
IPv4: 10.20.40.200 (p4p1)
IPv4: 10.20.90.10 (p5p1)
IPv4: 10.20.80.10 (p6p1)
DNS Records
– galileo.troopers (v4 & v6)
– galileo6.troopes (v6 only)
– galileo4.troopers (v4 only)



System Services
Various
- snmpd (port 161/udp)
- DNSv4/v6
- DHCPv4
- SLAAC

Addressing and Services (3/3)

	Addressing	System Services
 Switch	IPv6: 2a02:8071:f00:90::20 IPv4: 10.20.90.20 DNS Records – switch.troopers (v4 & v6) – switch6.troopes (v6 only)	Various - snmpd (port 161/udp)
 WLC	IPv6: 2A02:8071:F00:40::10 IPv4: 10.20.40.10 DNS Records – wlc.troopers (v4 & v6) – wlc6.troopes (v6 only)	Various - snmpd (port 161/udp)
 Firewall	IPv6: 2A02:8071:F00:40::1 IPv4: 10.20.40.1 DNS Records – firewall.troopers (v4 & v6) – firewall6.troopes (v6 only)	Various - snmpd (port 161/udp)

Credentials

	Login Credentials	Service Credentials

Kafka
T2016_UbuntuDesktop
	– User: trooper
	– Password: trooper
	Attention VM image users: Highly recommended to change this asap (-;
		– SNMPv2c:
		  – ROCOMMUNITY (IPv4)
		  – ROCOMMUNITY6 (IPv6)
		– SNMPv3:
		  – Auth: trooper!
		  – Priv: trooper?
		
		– Up to you to set this up

Galileo
Switch
Firewall
	– n/a	– SNMPv2c:
		  – ROCOMMUNITY (IPv4)
		  – ROCOMMUNITY6 (IPv6)
		– SNMPv3:
		  – AuthKey: trooper!
		  – PrivKey: trooper?
		
		– SNMPv3:
		  – AuthKey: trooper!
		  – PrivKey: trooper?

Tools – CLI

- ifconfig / ipconfig
- route
- netstat
- tcpdump / windump
- nmap
- net-snmp (snmpwalk, snmpget, …)
- iperf
- ntpupdate
- traceroute / traceroute6 / tracert
- ping / ping6
- lsof

Hint: Use the manpages of the tools (or -help) to figure out IPv6 related options.

Tools - GUI

- Zenmap
- Wireshark
- SnmpB
- Observium
- Ntopng
- JPerf

Content

A - Set up your stuff

#				VM	Task Description
A01	X	X	X		Download required tools from server (Kafka)
A02				X	Assign static IPv6 address to your Ubuntu guest VM (optional)
A03	X	X	X		Install tcpdump / windump and Wireshark

B - Basics

#				VM	Task Description
B01	X	X	X	X	Check your local routing table. Which is your IPv6 default route?
B02	X	X	X	X	Check your neighbour cache for IPv6 neighbours.
B03	X	X	X	X	Ensure that you have connectivity to the IPv6 internet (ping).
B04	X	X	X	X	Use traceroute to determine the path of IPv6 packets to a target in the internet (e.g. heise.de).
B05	X	X	X	X	Your IPv6 address is assigned dynamically. Which mechanism is used (DHCPv6 or SLAAC)?
B06	X	X	X	X	For DNS lookups of your client, which IP version is used?
B07	X	X	X	X	Install plugins on browser (IPvoo, IPfox,…).
B08	X	X	X	X	Browse to an IPv6 enabled webpage to test plugins (e.g. heise.de).

C – SNMP – Basics

#				VM	Task Description
C01	X	X	X	X	Ensure that generic MIB files are installed on your system and download vendor specific MIB files from server (Kafka) (optional)
C02	X	X	X	X	Setup / configure your client to use the MIB files (optional)
C03	X	X	X	X	Verify that you can query devices (Galileo, Kafka) with SNMP, using IPv4 and SNMPv2c credentials
C04		X	X	X	Verify that you can query devices (Galileo, Kafka) with SNMP, using IPv6 and SNMPv2c credentials
C05	X	X	X	X	Verify that you can query devices (Galileo, Kafka) with SNMP, using IPv4 and SNMPv3 credentials
C06		X	X	X	Verify that you can query devices (Galileo, Kafka) with SNMP, using IPv6 and SNMPv3 credentials
C07		X	X	X	Gather information about hostname, location, interfaces, IPv4/6 counters and IPv4/6 routes from devices (Galileo, Kafka, Firewall) using IPv6 and SNMPv3

C – SNMP – Basics

#				VM	Task Description
C08				X	Setup net-snmp daemon (snmpd) on your Ubuntu VM, configure a SNMPv1/v2 RO community as well as a SNMPv3 user with RO access.
C09				X	How can you restrict / limit access to snmpd to specific IPv4 and IPv6 ranges?
C10				X	Verify that you can query your Ubuntu via snmp locally (localhost), ensure that you can do this with both, IPv4 and v6, using the RO community and the SNMPv3 user.

D – SNMP – Observium

#				VM	Task Description
D01				X	Create a login for your local Observium installation (you need to specify privileges level 10 for admin rights).
D02				X	Add your Ubuntu VM (localhost) to Observium. Ensure that IPv6 is used. In order to do this, you need to add an entry to your /etc/hosts file.
D03				X	Add Galileo and Kafka to your Observium installation. Ensure that IPv6 is used for the snmp queries of Observium.

E – Various

#				VM	Task Description
E01	X	X	X	X	NTP: Query the ntp server (kafka) via IPv4 and v6
E02	X	X	X	X	Port Scanning: Ports which your device is listening for incoming connections on v4/v6
E03	X	X	X	X	Port Scanning: Investigate which well known ports (1-1024) are open on router and server (v4 and v6)
E04				X	ntopng: Change password of your local ntopng installation
E05				X	ntopng: Restart your local ntopng instance and have a look at the traffic breakdowns
E06	X	X	X	X	ntopng: Have a look at the ntopng installation on Kafka
E07	X	X	X	X	Iperf: Test the network performance between your device and Kafka with both IP versions. For IPv4 use port 4 and for IPv6 use port 6 (tcp) and ports 44 and 66 (udp).
E08	X				Jperf: Re-run tests with jperf
E09	X	X	X	X	For the brave: Try to compile snmpb for Ubuntu / OS X / Win7

Content

A01

#				VM	Task Description
A01	X	X	X		Download required tools from server (Kafka)

- Access files via
  - Windows share on Kafka (smb)
  - NFS share on Kafka
  - Use SCP / SSH to download files from Kafka

A02

#				VM	Task Description
A02				X	Assign static IPv6 address to your Ubuntu guest VM (optional)

- Edit /etc/network/interfaces

```
# Static IPv6 address
auto p5p1
…
iface p5p1 inet6 static
     address 2a02:8071:f00:90::1223
     netmask 64
     gateway 2a02:8071:f00:90::10
```

- Ensure that IPv6 address is not allready used!

A03

#				VM	Task Description
A03	X	X	X		Install tcpdump / windump and Wireshark

- Windows & Mac: Download and install installation packages
- Linux: Install with the package manager of your Linux distribution

B01

#				VM	Task Description
B01	X	X	X	X	Check your local routing table. Which is your IPv6 default route?

```
C:\Users\mug>netsh interface ipv6 show route

Veröff.  Typ       Met   Präfix                    Idx  Gateway/Schnittstelle
-------  --------  ----  ------------------------  ---  ---------------------
Nein     Manuell   8    ::/0                       11  LAN-Verbindung* 16
Nein     Manuell   256  ::/0                       12  fe80::222:4dff:fe9b:7c69
…
```

```
Gabriels-MacBook-Pro:~ muellega$ netstat -rn -f inet6
Routing tables

Internet6:
Destination                Gateway                          Flags         Netif Expire
default                    fe80::222:4dff:fe9b:7c69%en4     UGc             en4
::1                        ::1                              UHL             lo0
```

B01

#				VM	Task Description
B01	X	X	X	X	Check your local routing table. Which is your IPv6 default route?

```
trooper@UbuntuTeacher:~$ netstat -rn AF -6
Kernel IPv6 routing table
Destination                    Next Hop                   Flag Met Ref Use If
…
::/0                           fe80::222:4dff:fe9b:7c69   UGDAe 1024 0     0 eth0
…
```

B02

#				VM	Task Description
B02	X	X	X	X	Check your neighbour cache for IPv6 neighbours.

```
C:\Users\mug>netsh interface ipv6 show neighbors
…
Schnittstelle 12: LAN-Verbindung
Internetadresse                                Physische Adresse   Typ
----------------------------------------------  -----------------  -----------
fe80::222:4dff:fe9b:7c69                        00-22-4d-9b-7c-69  Erreichbar (Router)
ff02::1                                         33-33-00-00-00-01  Permanent
ff02::2                                         33-33-00-00-00-02  Permanent
```

```
Gabriels-MacBook-Pro:~ muellega$ ndp -an
Neighbor                        Linklayer Address  Netif Expire    St Flgs Prbs
…
fe80::222:4dff:fe9b:7c69%en4    0:22:4d:9b:7c:69   en4   6s        R  R
```

B02

#				VM	Task Description
B02	X	X	X	X	Check your neighbour cache for IPv6 neighbours.

```
rooper@UbuntuTeacher:~$ ip -6 neigh show
fe80::222:4dff:fe9b:7c69 dev eth0 lladdr 00:22:4d:9b:7c:69 router REACHABLE
2001:470:b5f5:aa:aa00::1 dev eth0 lladdr 00:22:4d:9b:7c:69 router REACHABLE
```

B03

#				VM	Task Description
B03	X	X	X	X	Ensure that you have connectivity to the IPv6 internet (ping).

```
C:\Users\mug>ping -6 heise.de

Ping wird ausgeführt für heise.de [2a02:2e0:3fe:1001:302::] mit 32 Bytes Daten:
Antwort von 2a02:2e0:3fe:1001:302::: Zeit=19ms
Antwort von 2a02:2e0:3fe:1001:302::: Zeit=20ms
```

```
Gabriels-MacBook-Pro:~ muellega$ ping6 heise.de
PING6(56=40+8+8 bytes) 2001:470:b5f5:aa:d863:5996:4b0f:b87f -->
2a02:2e0:3fe:1001:302::
16 bytes from 2a02:2e0:3fe:1001:302::, icmp_seq=0 hlim=57 time=19.355 ms
16 bytes from 2a02:2e0:3fe:1001:302::, icmp_seq=1 hlim=57 time=26.749 ms
```

```
trooper@UbuntuTeacher:~$ ping6 heise.de
PING heise.de(redirector.heise.de) 56 data bytes
64 bytes from redirector.heise.de: icmp_seq=1 ttl=57 time=20.2 ms
64 bytes from redirector.heise.de: icmp_seq=2 ttl=57 time=20.1 ms
```

B04

#				VM	Task Description
B04	X	X	X	X	Use traceroute to determine the path of IPv6 packets to a target in the internet (e.g. heise.de).

```
C:\Users\mug>tracert -6 -d heise.de

Routenverfolgung zu heise.de [2a02:2e0:3fe:1001:302::] über maximal 30 Abschnitte:
  1    <1 ms    <1 ms    <1 ms  2001:470:b5f5:aa:aa00::1
  2    13 ms    11 ms    12 ms  2001:470:25:2a::1
  3    20 ms    21 ms    10 ms  2001:470:0:11d::1
  4    18 ms    20 ms    22 ms  2001:470:0:21c::1
  5    21 ms    21 ms    20 ms  2001:7f8::3012:0:1
  6    18 ms    18 ms    16 ms  2a02:2e0:12:19::101
  7    16 ms    16 ms    17 ms  2a02:2e0:3fe:0:c::1
  8    21 ms    27 ms    17 ms  2a02:2e0:3fe:1001:302::
Ablaufverfolgung beendet.
C:\Users\mug>
```

B04

#				VM	Task Description
B04	X	X	X	X	Use traceroute to determine the path of IPv6 packets to a target in the internet (e.g. heise.de).

```
Gabriels-MacBook-Pro:~ muellega$ traceroute6 -n heise.de
traceroute6 to heise.de (2a02:2e0:3fe:1001:302::) from
2001:470:b5f5:aa:d889:9eaa:fccb:e637, 64 hops max, 12 byte packets
 1  2001:470:b5f5:aa:aa00::1  0.422 ms  0.400 ms  0.386 ms
 2  2001:470:25:2a::1  20.379 ms  13.517 ms  11.624 ms
 3  2001:470:0:11d::1  19.356 ms  11.122 ms  15.015 ms
 4  2001:470:0:21c::1  32.935 ms  27.870 ms  20.469 ms
 5  2001:7f8::3012:0:1  26.697 ms *  24.724 ms
 6  2a02:2e0:12:19::101  156.170 ms  207.931 ms  208.248 ms
 7  2a02:2e0:3fe:0:c::1  16.529 ms !P  16.208 ms !P  17.173 ms !P
Gabriels-MacBook-Pro:~ muellega$
```

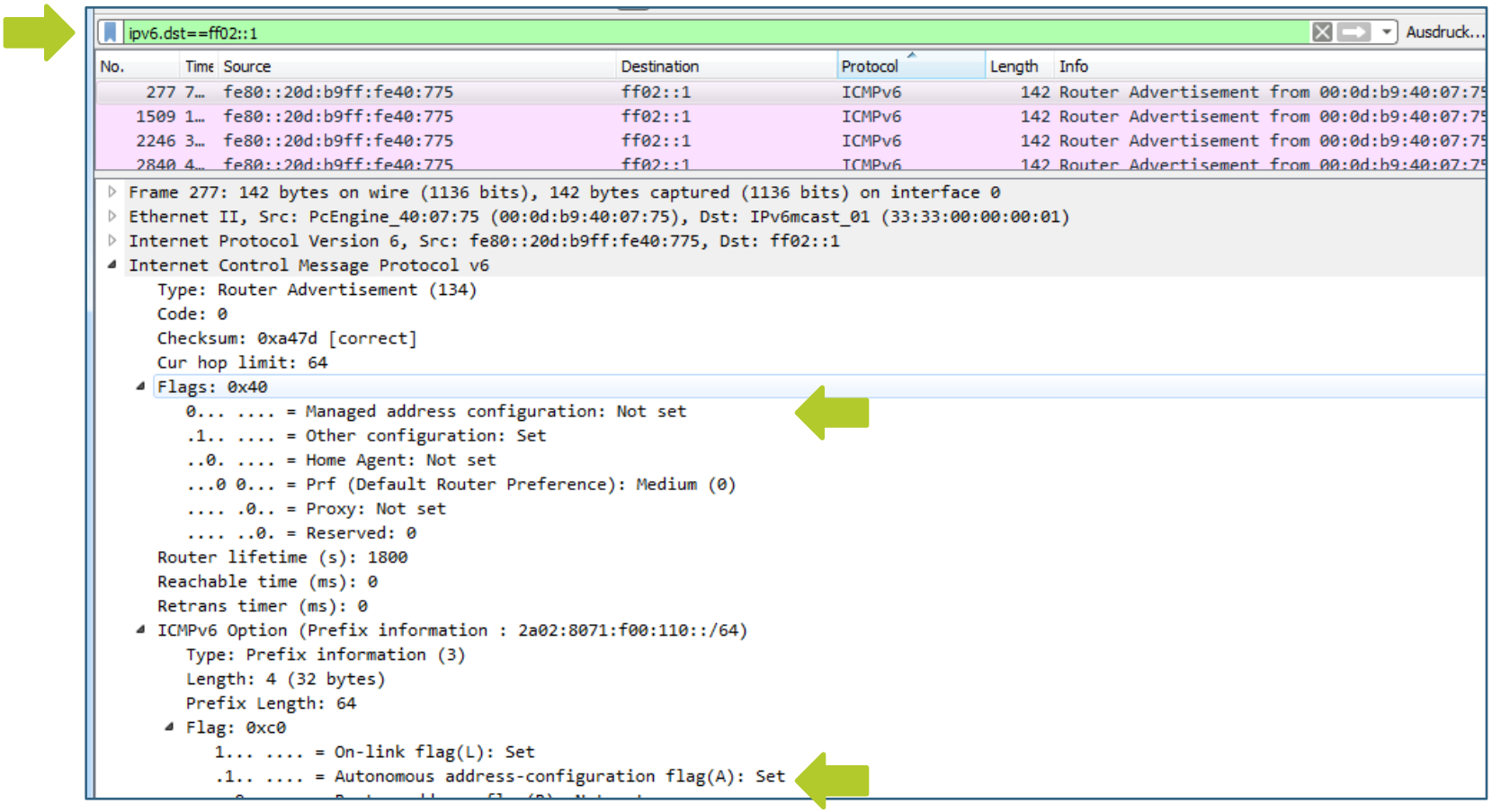
B04

#				VM	Task Description
B04	X	X	X	X	Use traceroute to determine the path of IPv6 packets to a target in the internet (e.g. heise.de).

```
rooper@UbuntuTeacher:~$ traceroute6 -n heise.de
traceroute to heise.de (2a02:2e0:3fe:1001:302::) from
2001:470:b5f5:aa:1c2d:523e:7451:aee2, 30 hops max, 24 byte packets
 1  2001:470:b5f5:aa:aa00::1  0.552 ms  0.433 ms  0.44 ms
 2  2001:470:25:2a::1  12.088 ms  14.235 ms  14.037 ms
 3  2001:470:0:11d::1  35.827 ms  16.079 ms  24.112 ms
 4  2001:470:0:21c::1  31.059 ms  47.556 ms  31.366 ms
 5  2001:7f8::3012:0:1  29.284 ms  20.665 ms  23.36 ms
 6  2a02:2e0:12:19::101  20.586 ms  19.74 ms  22.744 ms
 7  2a02:2e0:3fe:0:c::1  23.622 ms !S  21.95 ms !S  24.546 ms !S
trooper@UbuntuTeacher:~$
```

B05

#				VM	Task Description
B05	X	X	X	X	Your IPv6 address is assigned dynamically. Which mechanism is used (DHCPv6 or SLAAC)?



B06

#				VM	Task Description
B06	X	X	X	X	For DNS lookups of your client, which IP version is used?

dns

No.	Time	Source	Destination	Protocol	Length	Info
277	4…	2a02:8071:f00:110:a994:1c79:cd6:7164	2a02:8071:f00:110::10	DNS	88	Standard query 0x90bf AAAA heise.de
278	4…	2a02:8071:f00:110::10	2a02:8071:f00:110:a9…	DNS	116	Standard query response 0x90bf AAAA

```
▷ Frame 278: 116 bytes on wire (928 bits), 116 bytes captured (928 bits) on interface 0
▷ Ethernet II, Src: PcEngine_40:07:75 (00:0d:b9:40:07:75), Dst: Vmware_8e:47:82 (00:0c:29:8e:47:82)
▷ Internet Protocol Version 6, Src: 2a02:8071:f00:110::10, Dst: 2a02:8071:f00:110:a994:1c79:cd6:7164
▷ User Datagram Protocol, Src Port: 53 (53), Dst Port: 59607 (59607)
◢ Domain Name System (response)
    [Request In: 277]
    [Time: 0.000770000 seconds]
    Transaction ID: 0x90bf
  ▷ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  ▷ Queries
  ◢ Answers
    ▷ heise.de: type AAAA, class IN, addr 2a02:2e0:3fe:1001:302::
```

B07

#				VM	Task Description
B07	X	X	X	X	Install plugins on browser (IPvoo, IPfox,…).

Any idea for Microsoft IE?

Google Chrome

- IPvFoo
- IP Address and Domain Information
  - https://chrome.google.com/webstore/

Mozilla Firefox

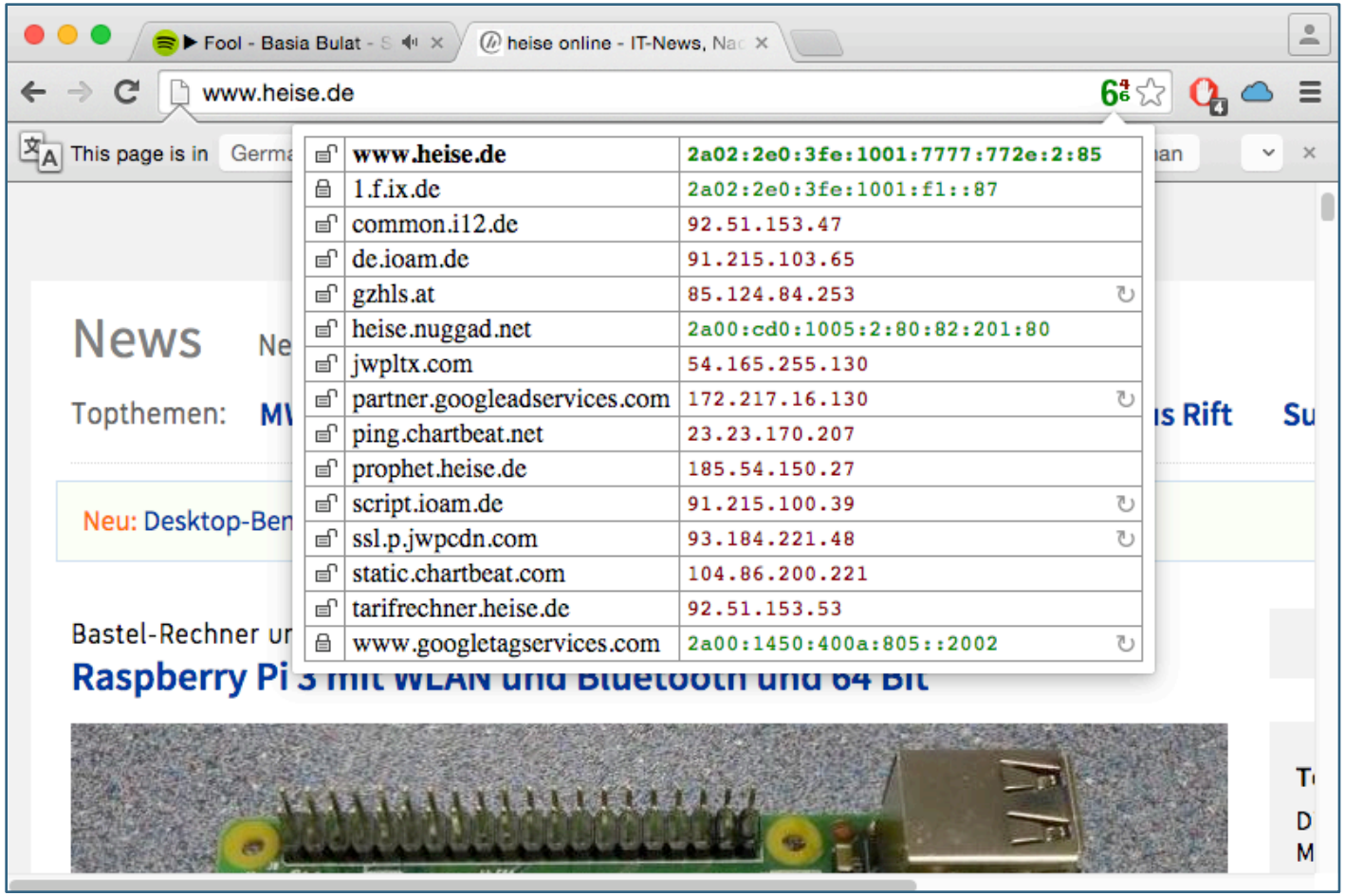
- IPvFox
- IP Address and Domain Information
  - https://addons.mozilla.org/mk/firefox/

OS X Safari

- Safari: TCPIPUTILS
  - http://www.macupdate.com/app/mac/39018/ip-address-and-domain-information

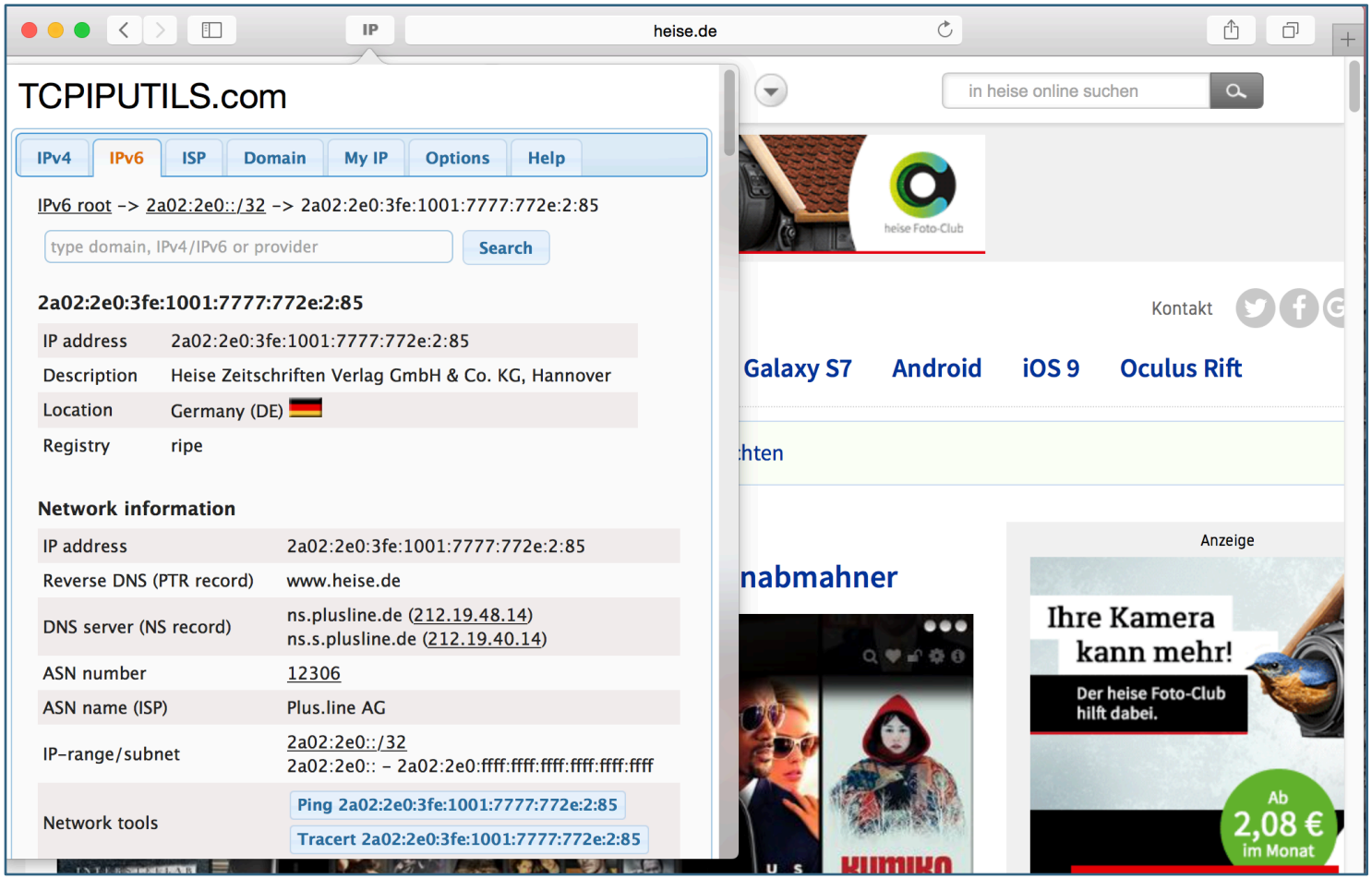
B08

#				VM	Task Description
B08	X	X	X	X	Browse to an IPv6 enabled webpage to test plugins (e.g. heise.de).



B08

#				VM	Task Description
B08	X	X	X	X	Browse to an IPv6 enabled webpage to test plugins (e.g. heise.de).



C01

#				VM	Task Description
C01	X	X	X	X	Ensure that generic MIB files are installed on your system and download vendor specific MIB files from server (Kafka) (optional).

Generic MIB files

- Ubuntu

```
trooper@UbuntuTeacher:~$ sudo apt-get install snmp-mibs-downloader
trooper@UbuntuTeacher:~$ sudo download-mibs
```

- OSX / Windows
  - Download from Kafka: /home/trooper/software/MIBs/Generic

Vendor specific MIB files

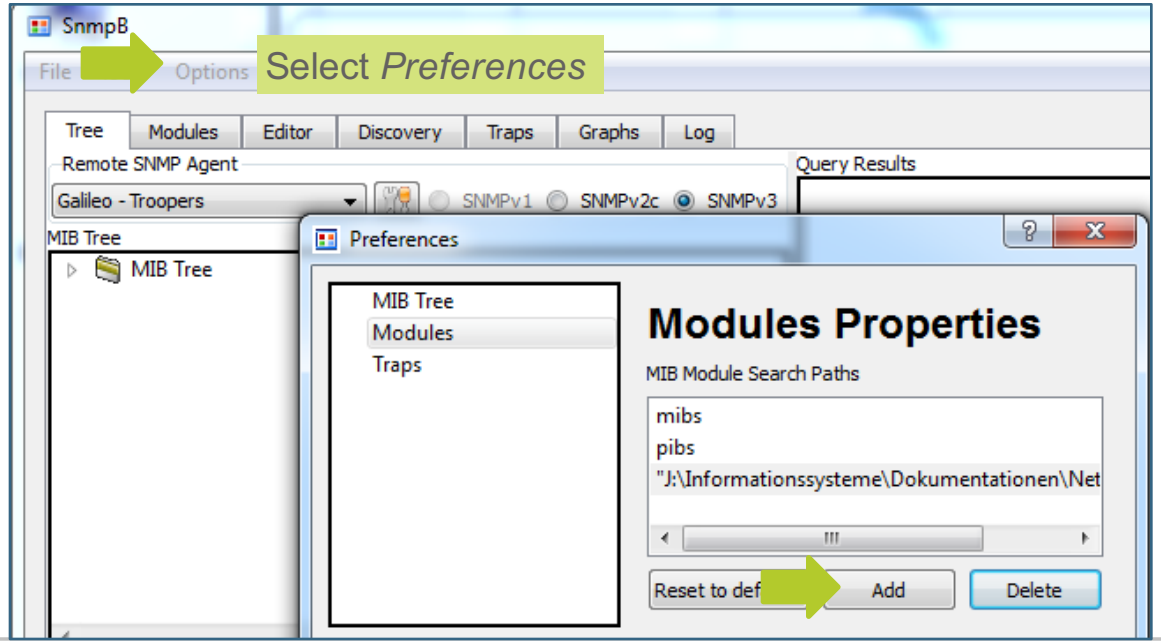
- You will need the Cisco MIBs for the upcoming tasks
  - /home/trooper/MIBs/Cisco

C02

#				VM	Task Description
C02	X	X	X	X	Setup / configure your client to use the MIB files (optional)

Windows (SnmpD)

Check existing MIB stock of SnmpD and copy missing MIB files either to default directory (C:\Program Files (x86)\SnmpB\mibs) or to some other directory. In the later case add the path to the SnmpD configuration.

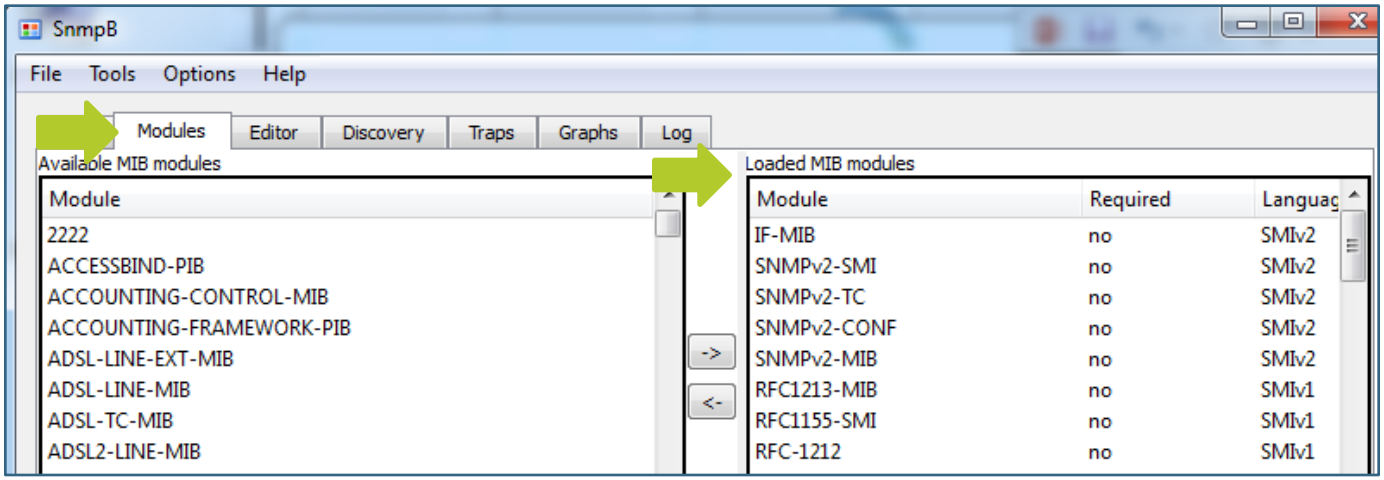


C02

#				VM	Task Description
C02	X	X	X	X	Setup / configure your client to use the MIB files (optional)

Windows (SnmpD)

- Ensure that MIB files do not have a suffix, such as .txt
- Ensure that required MIB files are tin the *Loaded MIB modules* section



C02

#				VM	Task Description
C02	X	X	X	X	Setup / configure your client to use the MIB files (optional)

OSX / Ubuntu

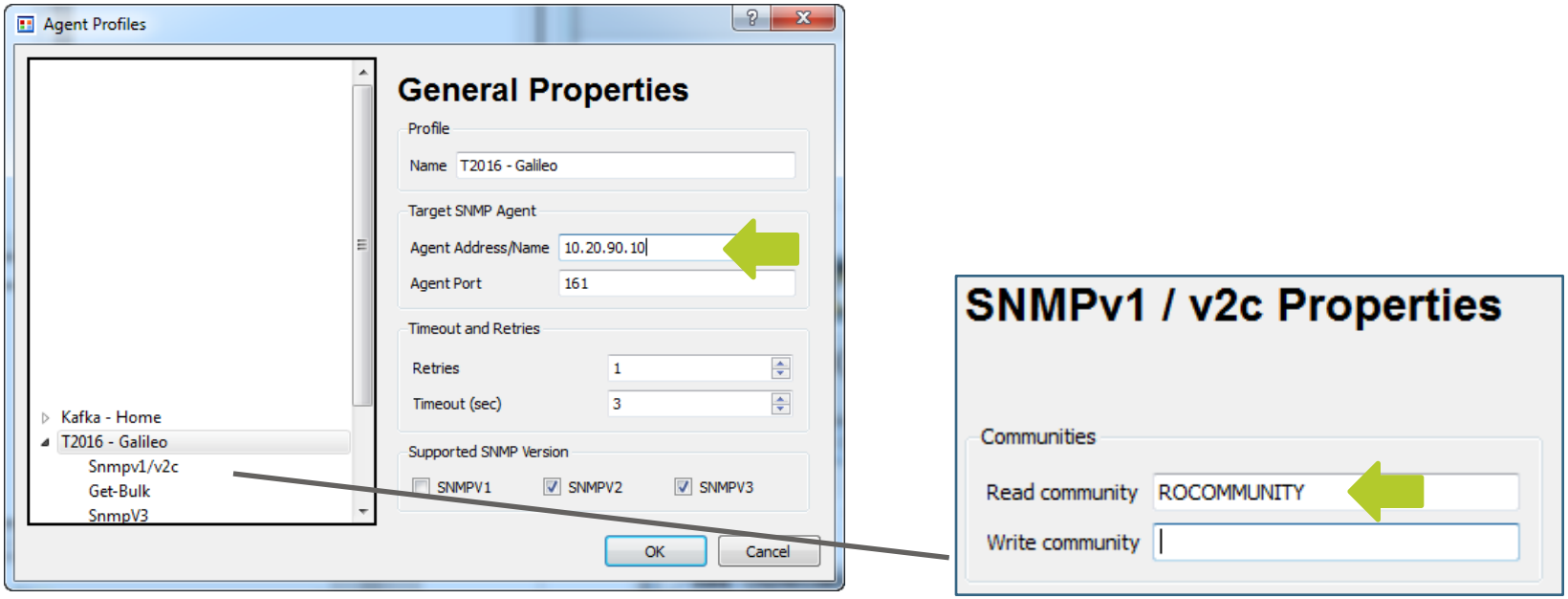
- You have to setup a config file, name it snmp.conf and place it in your local home directory file under snmp, e.g. /home/trooper/.snmp/
- Two different config files have been prepared by us, you can find them on Kafka (/home/trooper/config/snmp):
  - snmp.conf_ubuntu
  - snmp.conf_mac
- They contain a lot of comments, have a look!

C03

#				VM	Task Description
C03	X	X	X	X	Verify that you can query devices (Galileo, Kafka) with SNMP, using IPv4 and SNMPv2c credentials

Windows (SnmpB)

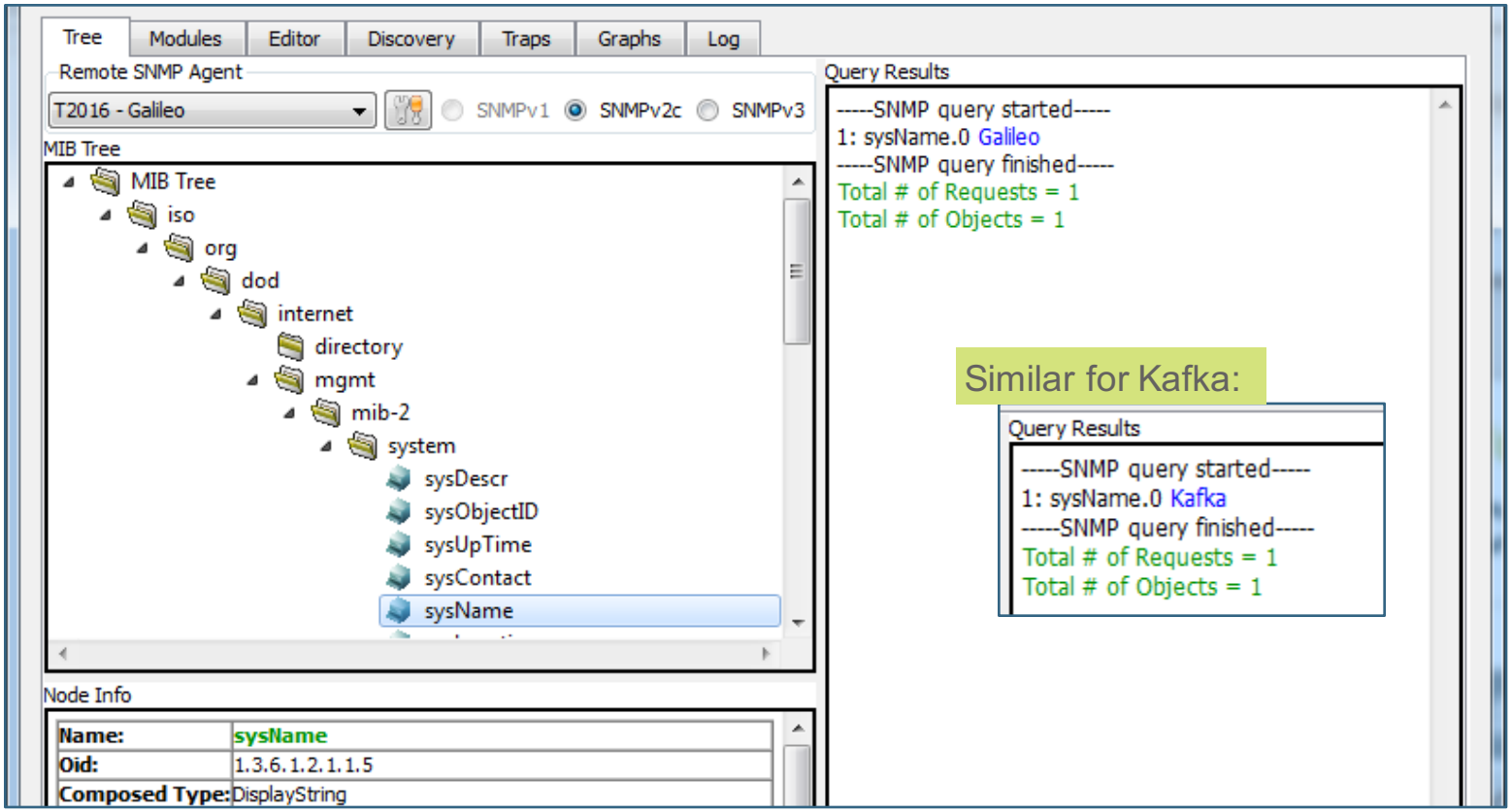
- Add Kafka and Galileo as hosts in the SnmpB configuration and specify the SNMPv2 community.



C03

#				VM	Task Description
C03	X	X	X	X	Verify that you can query devices (Galileo, Kafka) with SNMP, using IPv4 and SNMPv2c credentials

Windows (SnmpB)



C03

Hint: *2>/dev/null* is used to re-direct a lot of error messages you might get if you tell snmp client to load all MIB files.

#				VM	Task Description
C03	X	X	X	X	Verify that you can query devices (Galileo, Kafka) with SNMP, using IPv4 and SNMPv2c credentials

OSX / Ubuntu

```
trooper@UbuntuTeacher:~$ snmpget -v 2c -c ROCOMMUNITY kafka.troopers sysName.0
2>/dev/null
SNMPv2-MIB::sysName.0 = STRING: Kafka
trooper@UbuntuTeacher:~$
```

```
trooper@UbuntuTeacher:~$ snmpget -v 2c -c ROCOMMUNITY galileo.troopers sysName.0
2>/dev/null
SNMPv2-MIB::sysName.0 = STRING: Galileo
trooper@UbuntuTeacher:~$
```

```
rooper@UbuntuTeacher:~$ sudo tcpdump -n -i eth0 udp and ip
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
21:19:33.390169 IP … > …:  C=ROCOMMUNITY GetRequest(28)  .1.3.6.1.2.1.1.5.0
21:19:33.391753 IP … > …:  C=ROCOMMUNITY GetResponse(33)  .1.3.6.1.2.1.1.5.0="Kafka"
```

C04

#				VM	Task Description
C04		X	X	X	Verify that you can query devices (Galileo, Kafka) with SNMP, using IPv6 and SNMPv2c credentials

```
trooper@UbuntuTeacher:~$ snmpget -v 2c -c ROCOMMUNITY6 udp6:kafka.troopers sysName.0
2>/dev/null
SNMPv2-MIB::sysName.0 = STRING: Kafka
trooper@UbuntuTeacher:~$
```

```
trooper@UbuntuTeacher:~$ snmpget -v 2c -c ROCOMMUNITY6 udp6:galileo.troopers
sysName.0 2>/dev/null
SNMPv2-MIB::sysName.0 = STRING: Galileo
trooper@UbuntuTeacher:~$
```

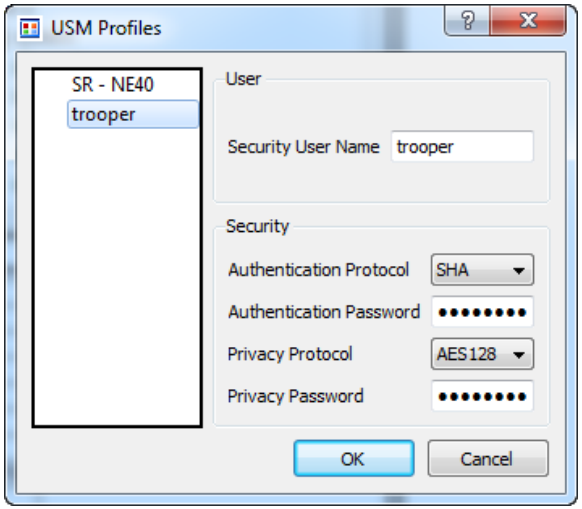
```
trooper@UbuntuTeacher:~$ sudo tcpdump -n -i eth0 udp and ip6
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
21:22:19.533270 IP6 … > …: C=ROCOMMUNITY6 GetRequest(28) .1.3.6.1.2.1.1.5.0
21:22:19.534337 IP6 … > …: C=ROCOMMUNITY6 GetResponse(33) .1.3.6.1.2.1.1.5.0="Kafka"
```

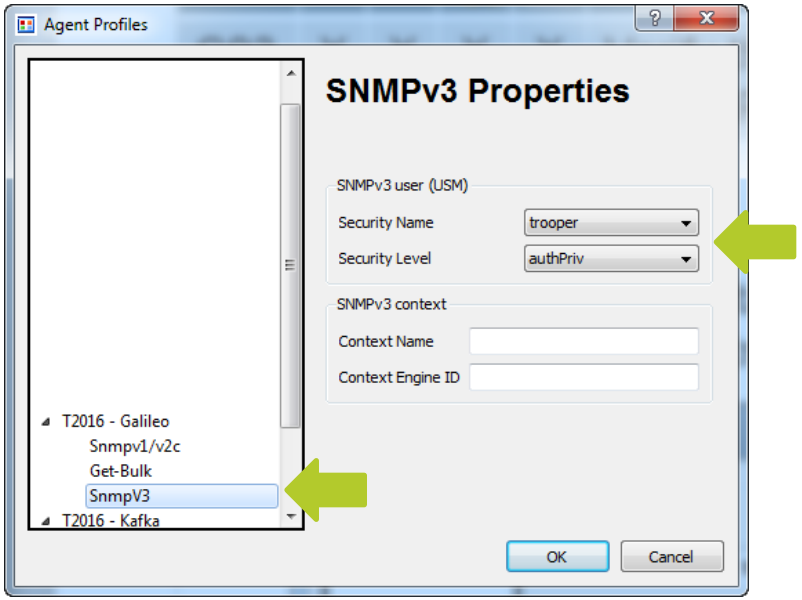
C05

#				VM	Task Description
C05	X	X	X	X	Verify that you can query devices (Galileo, Kafka) with SNMP, using IPv4 and SNMPv3 credentials

Windows (SnmpB)

- Create new USM Profile (SNMPv3). Authentication and Privacy password can be found in this documentation, for protocols use SHA and AES128. Then assign this profile to your host entries for Kafka and Galileo.

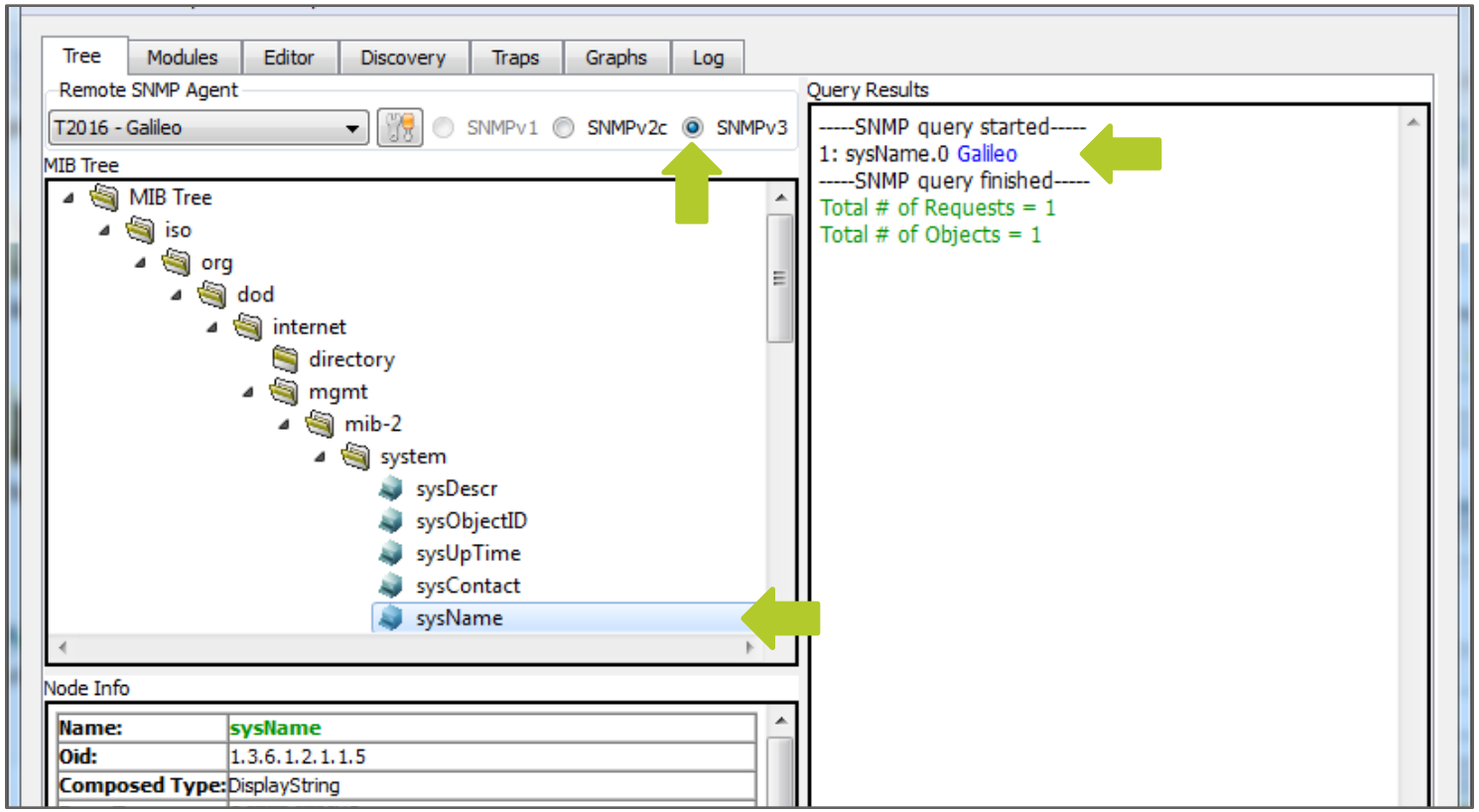




C05

#				VM	Task Description
C05	X	X	X	X	Verify that you can query devices (Galileo, Kafka) with SNMP, using IPv4 and SNMPv3 credentials

Windows (SnmpB)



C05

#				VM	Task Description
C05	X	X	X	X	Verify that you can query devices (Galileo, Kafka) with SNMP, using IPv4 and SNMPv3 credentials

OSX / Ubuntu

```
trooper@UbuntuTeacher:~$ snmpget -v 3 -n "" -u trooper -a SHA -A "trooper!" -x AES -
X "trooper?" kafka.troopers sysName.0 -l authPriv 2>/dev/null
SNMPv2-MIB::sysName.0 = STRING: Kafka
trooper@UbuntuTeacher:~$
```

```
trooper@UbuntuTeacher:~$ snmpget -v 3 -n "" -u trooper -a SHA -A "trooper!" -x AES -
X "trooper?" galileo.troopers sysName.0 -l authPriv 2>/dev/null
SNMPv2-MIB::sysName.0 = STRING: Galileo
trooper@UbuntuTeacher:~$
```

```
rooper@UbuntuTeacher:~$ sudo tcpdump -n -i eth0 udp and ip
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
… F= U= E= 0x800x000x1F0x880x800x530x7D0x800x2F0x240x560xBE0x560x000x000x000x00 C=
Report(32)  .1.3.6.1.6.3.15.1.1.4.0=241 …
```

C06

#				VM	Task Description
C06		X	X	X	Verify that you can query devices (Galileo, Kafka) with SNMP, using IPv6 and SNMPv3 credentials

```
trooper@UbuntuTeacher:~$ snmpget -v 3 -n "" -u trooper -a SHA -A "trooper!" -x AES -
X "trooper?" udp6:kafka6.troopers sysName.0 -l authPriv 2>/dev/null
SNMPv2-MIB::sysName.0 = STRING: Kafka
trooper@UbuntuTeacher:~$
```

```
trooper@UbuntuTeacher:~$ snmpget -v 3 -n "" -u trooper -a SHA -A "trooper!" -x AES -
X "trooper?" udp6:galileo6.troopers sysName.0 -l authPriv 2>/dev/null
SNMPv2-MIB::sysName.0 = STRING: Galileo
trooper@UbuntuTeacher:~$
```

```
trooper@UbuntuTeacher:~$ sudo tcpdump -n -i eth0 udp and ip6
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
… (encrytpted traffic)
```

C07

#				VM	Task Description
C07		X	X	X	Gather information about hostname, location, interfaces, IPv4/6 counters and IPv4/6 routes from devices (Galileo, Kafka, Firewall) using IPv6 and SNMPv3

Tips for MIB Files – net-snmp

- Overview: http://www.net-snmp.org/docs/mibs/
- Hostname: http://www.net-snmp.org/docs/mibs/SNMPv2-MIB.txt
  - sysName.0
- Interfaces: http://www.net-snmp.org/docs/mibs/interfaces.html
  - ifDescr
- Interface Statistics: http://www.net-snmp.org/docs/mibs/ip.html#ipIfStatsTable
  - ipIfStatsTable
- Routes: http://www.net-snmp.org/docs/mibs/ipForward.html
  - inetCidrRouteTable

C07

#				VM	Task Description
C07		X	X	X	Gather information about hostname, location, interfaces, IPv4/6 counters and IPv4/6 routes from devices (Galileo, Kafka, Firewall) using IPv6 and SNMPv3

```
// hostname
trooper@UbuntuTeacher:~$ snmpget -v 3 -n "" -u trooper -a SHA -A "trooper!" -x AES -
X "trooper?" udp6:kafka6.troopers sysName.0 -l authPriv 2>/dev/null
SNMPv2-MIB::sysName.0 = STRING: Kafka
trooper@UbuntuTeacher:~$
```

```
// Interface Description
trooper@UbuntuTeacher:~$ snmpwalk -v 3 -n "" -u trooper -a SHA -A "trooper!" -x AES
-X "trooper?" -l authPriv udp6:galileo6.troopers ifDescr  -OX 2>/dev/null
IF-MIB::ifDescr[1] = STRING: lo
IF-MIB::ifDescr[2] = STRING: p4p1
IF-MIB::ifDescr[3] = STRING: p5p1
IF-MIB::ifDescr[4] = STRING: p6p1
trooper@UbuntuTeacher:~$
```

C07

#				VM	Task Description
C07		X	X	X	Gather information about hostname, location, interfaces, IPv4/6 counters and IPv4/6 routes from devices (Galileo, Kafka, Firewall) using IPv6 and SNMPv3

```
// Interface Statistics
trooper@UbuntuTeacher:~$ snmpget -v 3 -n "" -u trooper -a SHA -A "trooper!" -x AES -
X "trooper?" udp6:firewall6.troopers ipifStatsEntry -l authPriv 2>/dev/null
IP-MIB::ipIfStatsInReceives[ipv4][5] = Counter32: 0
IP-MIB::ipIfStatsInReceives[ipv4][8] = Counter32: 879405
IP-MIB::ipIfStatsInReceives[ipv4][9] = Counter32: 8006
IP-MIB::ipIfStatsInReceives[ipv4][12] = Counter32: 8353279
IP-MIB::ipIfStatsInReceives[ipv6][7] = Counter32: 0
…
IP-MIB::ipIfStatsHCInReceives[ipv4][2] = Counter64: 1949382
IP-MIB::ipIfStatsHCInReceives[ipv4][5] = Counter64: 0
IP-MIB::ipIfStatsHCInReceives[ipv4][8] = Counter64: 879405
…
trooper@UbuntuTeacher:~$
```

C07

#				VM	Task Description
C07		X	X	X	Gather information about hostname, location, interfaces, IPv4/6 counters and IPv4/6 routes from devices (Galileo, Kafka, Firewall) using IPv6 and SNMPv3

```
// Routing Entries
trooper@UbuntuTeacher:~$ snmpget -v 3 -n "" -u trooper -a SHA -A "trooper!" -x AES -
X "trooper?" udp6:firewall6.troopers inetCidrRouteTable -l authPriv 2>/dev/null
IP-FORWARD-MIB::inetCidrRouteIfIndex[ipv4]["0.0.0.0"][0][SNMPv2-
SMI::zeroDotZero][ipv4]["10.1.10.1"] = INTEGER: 2
…
IP-FORWARD-MIB::inetCidrRouteIfIndex[ipv6]
["00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:01"][128][SNMPv2-SMI::zeroDotZero.14]
[ipv6]["00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00"] = INTEGER: 1
IP-FORWARD-MIB::inetCidrRouteIfIndex[ipv6]
["2a:02:80:71:0f:00:01:00:00:00:00:00:00:00:00:00"][64][SNMPv2-SMI::zeroDotZero.5]
[ipv6]["00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00"] = INTEGER: 4
…
trooper@UbuntuTeacher:~$
```

C08

#				VM	Task Description
C08				X	Setup net-snmp daemon (snmpd) on your Ubuntu VM, configure a SNMPv1/v2 RO community as well as a SNMPv3 user with RO access.

Required

- Define on which protocols and which IP addresses snmpd should listen
  - agentAddress
- Define RO communities for IPv4 and IPv6
  - rocommunity / rocommunity6
- Setup SNMPv3 user
  - rouser
- Add administrator details and location information
  - sysLocation
  - sysContact

A working configuration can be found on Kafka: (/home/trooper/config/snmp/snmpd.conf.txt)

C09

#				VM	Task Description
C09				X	How can you restrict / narrow down access to snmpd to specific IPv4 and IPv6 ranges?

snmpd.conf

```
# Restrict snmpd to listen on dedicated interfaces (-> IPs) only
# IPv4
# agentAddress udp:127.0.0.1:161,udp:10.20.80.100:161
# IPv6
# agentAddress udp6:[::1]:161,udp6:[2a02:8071:f00:80::100]:161
```

Firewall

- Control which clients (source IPs) can connect to the snmpd daemon

C10

#				VM	Task Description
C10				X	Verify that you can query your Ubuntu via snmp locally (localhost), ensure that you can do this with both, IPv4 and v6 using the RO community and the SNMPv3 user

```
trooper@UbuntuTeacher:~$ snmpget -v 2c -c ROCOMMUNITY localhost sysName.0
2>/dev/null
SNMPv2-MIB::sysName.0 = STRING: UbuntuTeacher

trooper@UbuntuTeacher:~$ snmpget -v 2c -c ROCOMMUNITY6 udp6:localhost sysName.0
2>/dev/null
SNMPv2-MIB::sysName.0 = STRING: UbuntuTeacher
```

```
trooper@UbuntuTeacher:~$ snmpwalk -v 3 -n "" -u trooper -a SHA -A "trooper!" -x AES
-X "trooper?" -l authPriv localhost sysName.0 2>/dev/null
SNMPv2-MIB::sysName.0 = STRING: UbuntuTeacher

trooper@UbuntuTeacher:~$ snmpwalk -v 3 -n "" -u trooper -a SHA -A "trooper!" -x AES
-X "trooper?" -l authPriv udp6:localhost sysName.0 2>/dev/null
SNMPv2-MIB::sysName.0 = STRING: UbuntuTeacher
```

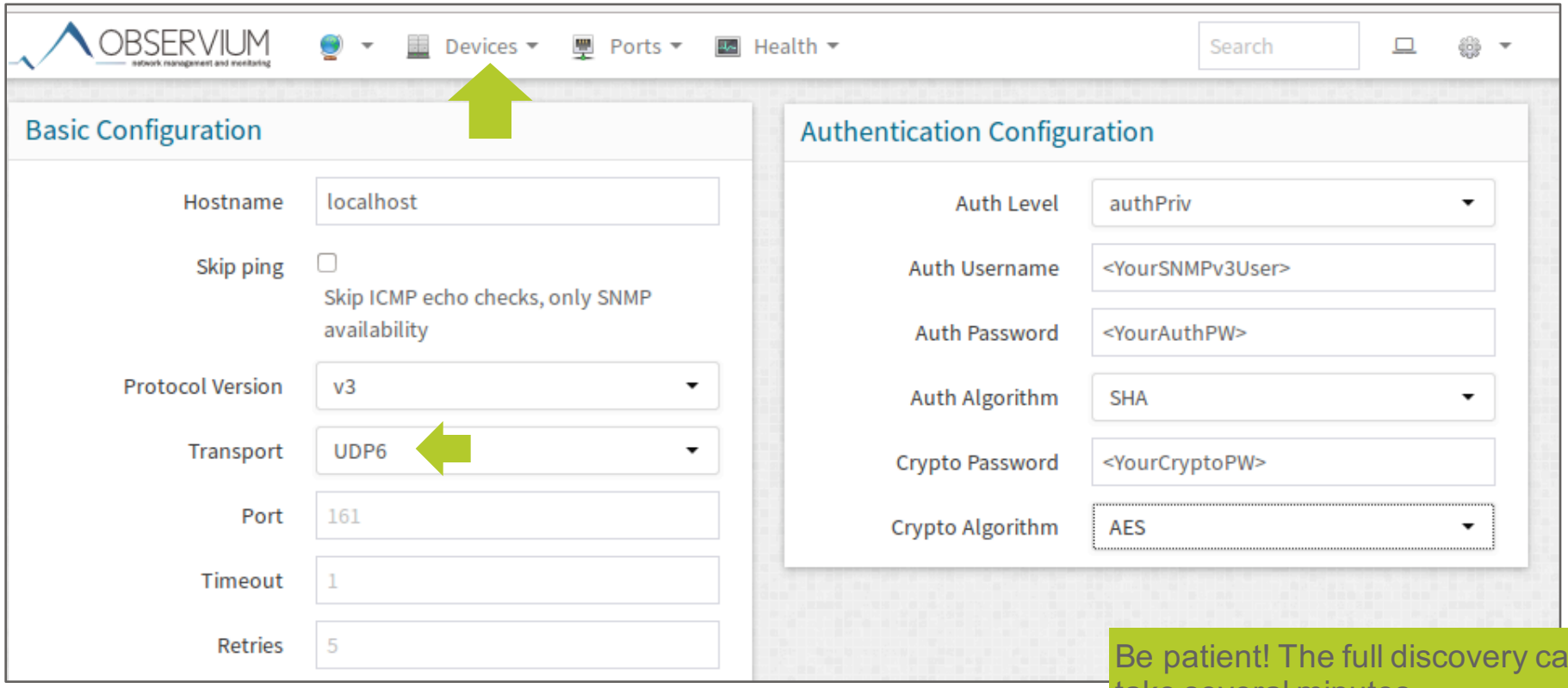
D01

#				VM	Task Description
D01				X	Create a login for your local Observium installation (you need to specify privileges level 10 for admin rights)

```
trooper@UbuntuTeacher:~$ cd /opt/observium/
trooper@UbuntuTeacher:/opt/observium$ sudo ./adduser.php --help
[sudo] password for trooper:
Observium CE 0.16.1.7533
Add User

USAGE:
adduser.php <username> <password> <level 1-10> [email]

EXAMPLE:
ADMIN:   adduser.php <username> <password> 10 [email]

USER LEVELS:
  0 - Disabled (This user disabled)
  …
  10 - Administrator (This user has full administrative access)
```

D02

#				VM	Task Description
D02				X	Add your Ubuntu VM (localhost) to Observium. Ensure that IPv6 is used. In order to do this, ensure you have an IPv6 entry for localhost in /etc/hosts.



Be patient! The full discovery can take several minutes.

D03

#				VM	Task Description
D03				X	Add Galileo and Kafka to your Observium installation. Ensure that IPv6 is used for the snmp queries of Observium.

Similar to D02

- Use SNMPv3 credentials given in the introduction part
  - (trooper / trooper! / trooper?)

E01

#				VM	Task Description
E01	X	X	X	X	NTP: Query the ntp server (kafka) via IPv4 and v6

Windows

```
C:\Users\mug\Desktop>w32tm /stripchart /computer:kafka.troopers /samples:5 /dataonly
kafka.troopers wird verfolgt [10.20.80.100:123].
…

C:\Users\mug\Desktop>w32tm /stripchart /computer:kafka6.troopers /samples:5
/dataonly
kafka6.troopers wird verfolgt [[2a02:8071:f00:80::100]:123].
5 Proben werden gesammelt.
Es ist 04.03.2016 23:33:46.
23:33:46, -00.0432092s
23:33:48, -00.0511911s
23:33:50, -00.0519504s
23:33:52, -00.0541765s
23:33:54, -00.0565454s

C:\Users\mug\Desktop>
```

E01

#				VM	Task Description
E01	X	X	X	X	NTP: Query the ntp server (kafka) via IPv4 and v6

OS X / Ubuntu (IPv6)

```
trooper@UbuntuTeacher:~$ ntpdate -d kafka4.troopers
19 Feb 21:17:24 ntpdate[9998]: ntpdate 4.2.6p5@1.2349-o Thu Feb 11 18:30:41 UTC 2016
(1)
Looking for host kafka6.troopers and service ntp
host found : kafka.troopers
transmit(10.20.80.100)
receive(10.20.80.100)
…
originate timestamp: da71f6da.cd4500f0  Fri, Feb 19 2016 21:17:30.801
transmit timestamp:  da71f6da.ce0bfff5  Fri, Feb 19 2016 21:17:30.804
…
filter offset: -0.00365 -0.00351 -0.00356 -0.00356
         0.000000 0.000000 0.000000 0.000000
delay 0.02643, dispersion 0.00008
offset -0.003659
trooper@UbuntuTeacher:~$
```

E01

#				VM	Task Description
E01	X	X	X	X	NTP: Query the ntp server (kafka) via IPv4 and v6

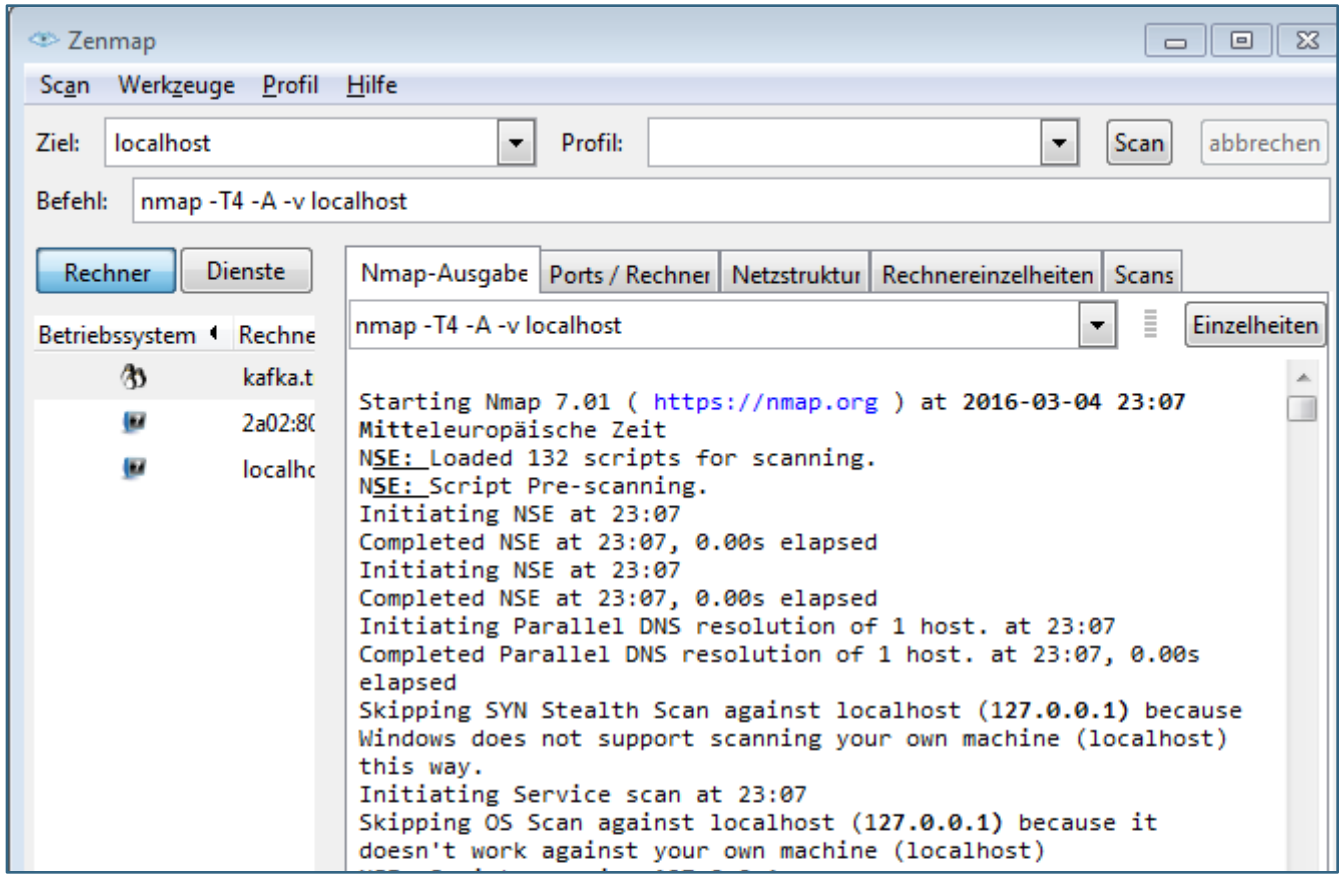
OS X / Ubuntu (IPv6)

```
trooper@UbuntuTeacher:~$ ntpdate -d kafka6.troopers
19 Feb 21:17:24 ntpdate[9998]: ntpdate 4.2.6p5@1.2349-o Thu Feb 11 18:30:41 UTC 2016
(1)
Looking for host kafka6.troopers and service ntp
host found : kafka.troopers
transmit(2a02:8071:f00:80::100)
receive(2a02:8071:f00:80::100)
…
originate timestamp: da71f6da.cd4500f0  Fri, Feb 19 2016 21:17:30.801
transmit timestamp:  da71f6da.ce0bfff5  Fri, Feb 19 2016 21:17:30.804
…
filter offset: -0.00365 -0.00351 -0.00356 -0.00356
         0.000000 0.000000 0.000000 0.000000
delay 0.02643, dispersion 0.00008
offset -0.003659
trooper@UbuntuTeacher:~$
```

E02

#				VM	Task Description
E02	X	X	X	X	Port Scanning: On which ports your device is listening for incoming connections on v4/v6

Windows



E02

#				VM	Task Description
E02	X	X	X	X	Port Scanning: On which ports your device is listening for incoming connections on v4/v6

OS X

```
// IPv4 - TCP
Gabriels-MacBook-Pro:~ muellega$ nmap localhost

// IPv6 – TCP
Gabriels-MacBook-Pro:~ muellega$ nmap localhost -6

// IPv4 – UDP
Gabriels-MacBook-Pro:~ muellega$ sudo nmap localhost –sU

// IPv6 – UDP
Gabriels-MacBook-Pro:~ muellega$ sudo nmap localhost –sU -6
…
PORT    STATE SERVICE
123/udp open  ntp
…
```

E02

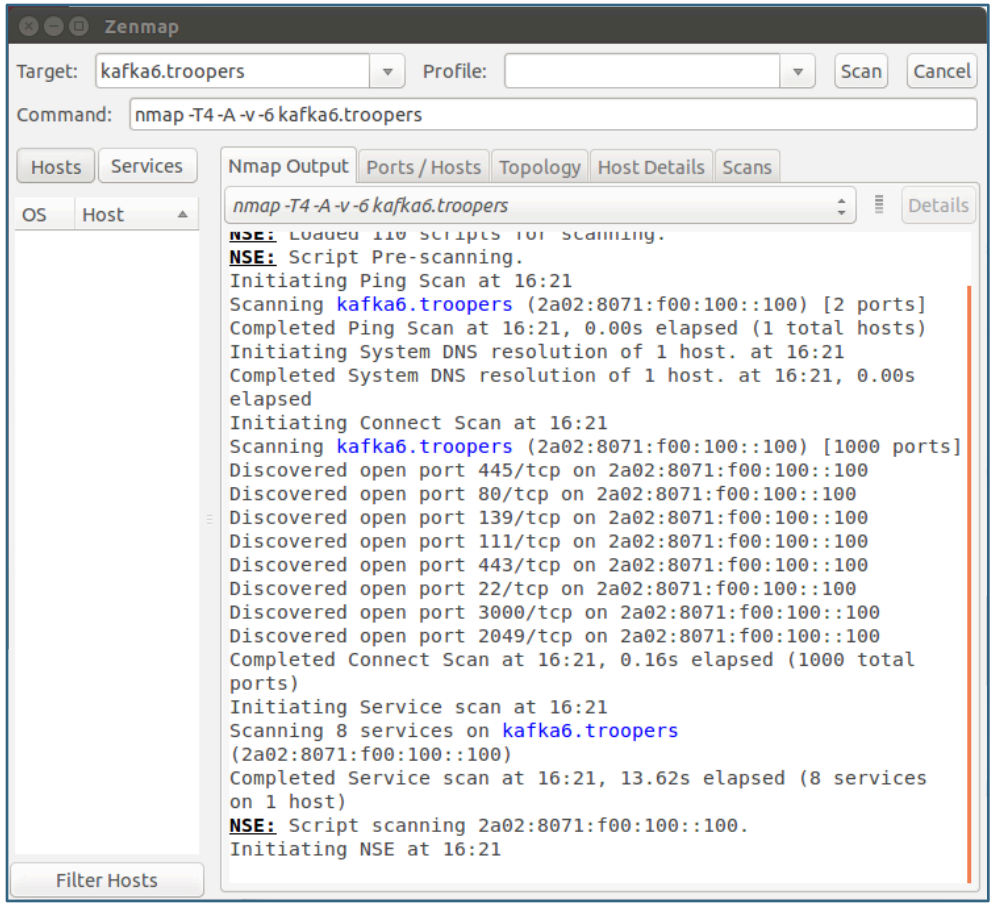
#				VM	Task Description
E02	X	X	X	X	Port Scanning: On which ports your device is listening for incoming connections on v4/v6

Ubuntu

```
trooper@UbuntuTeacher:~$ sudo netstat -plnt -4  // TCP IPv4

trooper@UbuntuTeacher:~$ sudo netstat -plnt -6  // TCP IPv6

trooper@UbuntuTeacher:~$ sudo netstat -plnu -4  // UDP IPv4

trooper@UbuntuTeacher:~$ sudo netstat -plnu -6  // UDP IPv6
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         PID/Program name
udp6       0      0 :::33276               :::*                    4999/rpc.statd
...
udp6       0      0 fe80::20c:29ff:feb3:123 :::*                   13549/ntpd
udp6       0      0 ::1:123                :::*                    13549/ntpd
```

E03

#				VM	Task Description
E03	X	X	X	X	Port Scanning: Investigate which well known ports (1-1024) are open on router and server (v4 and v6)

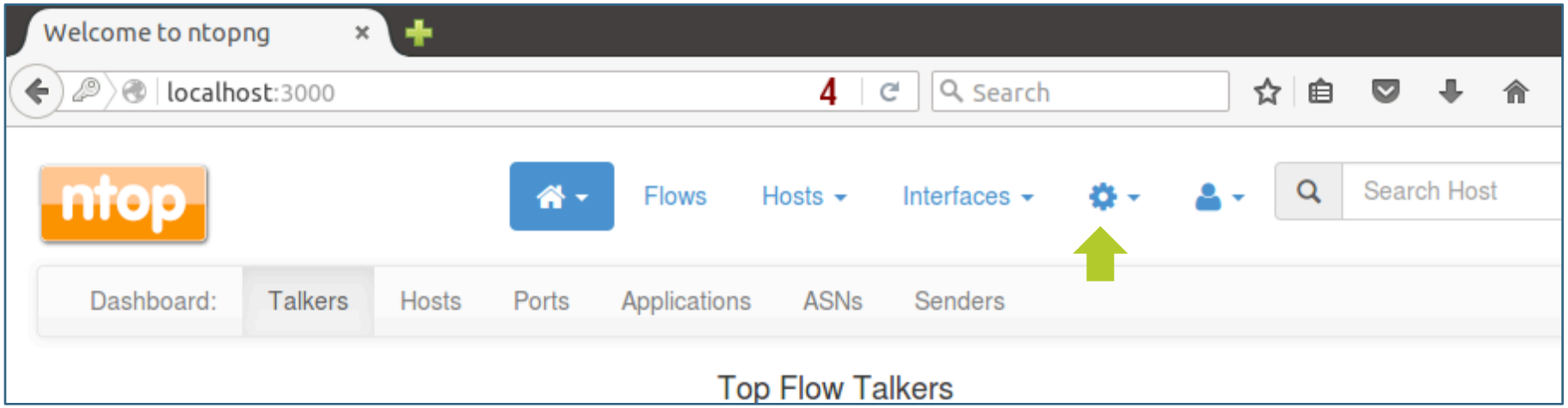


- Instead of kafka6.troopers you can also use its IPv6 address: 2a02:8071:f00:80::100
- In IPv4 scans you do not need option '-6'
- Similar comments apply to Galileo

E04

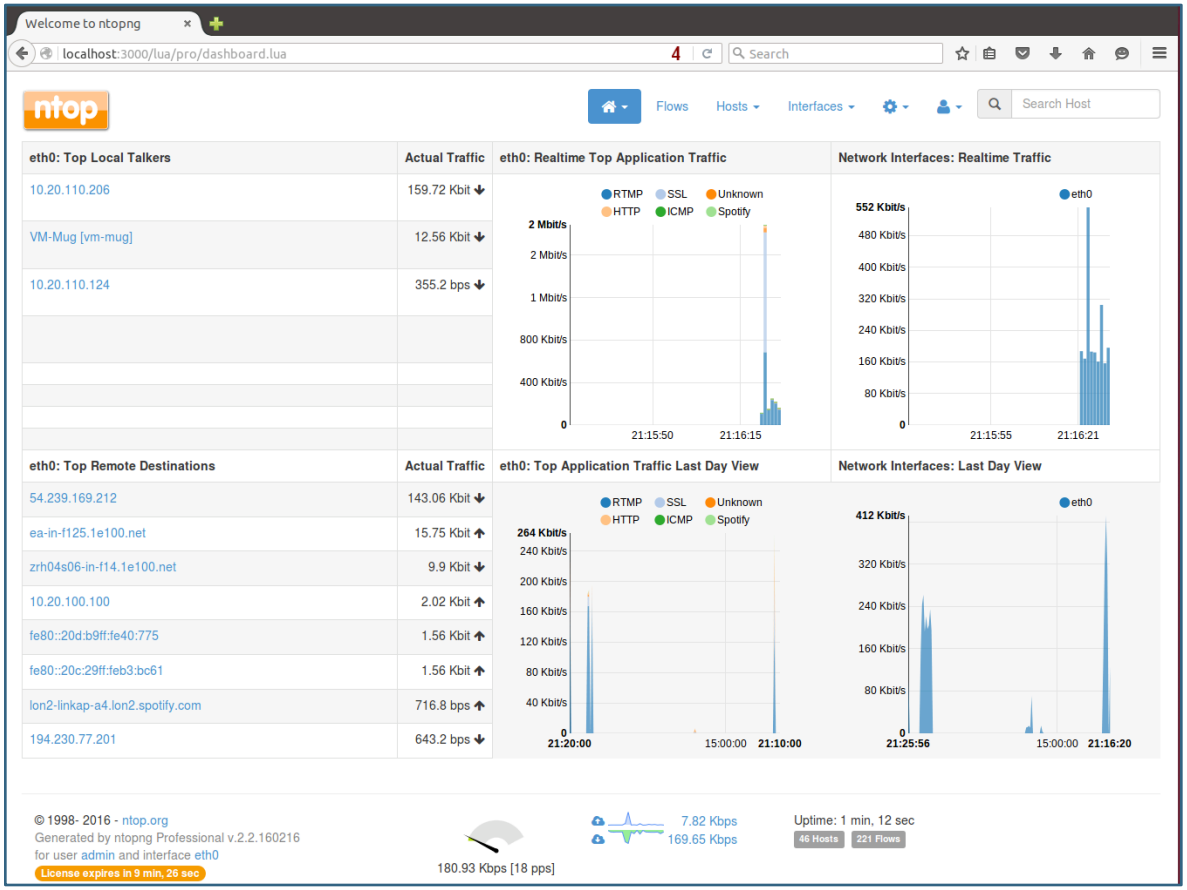
#				VM	Task Description
E04				X	ntopng: Change password of your local ntopng installation

- Connect to http://localhost:3000
- Login with admin / admin
- Go to Settings > Manage Users



E05

#				VM	Task Description
E05				X	ntopng: Restart your local Ubuntu VM and have a look again at the ntopng page



E06

#				VM	Task Description
E06	X	X	X	X	ntopng: Have a look at the ntopng installation on Kafka

- Access web site at: http//kafka6.troopers:3000
- Login: trooper / trooper

E07

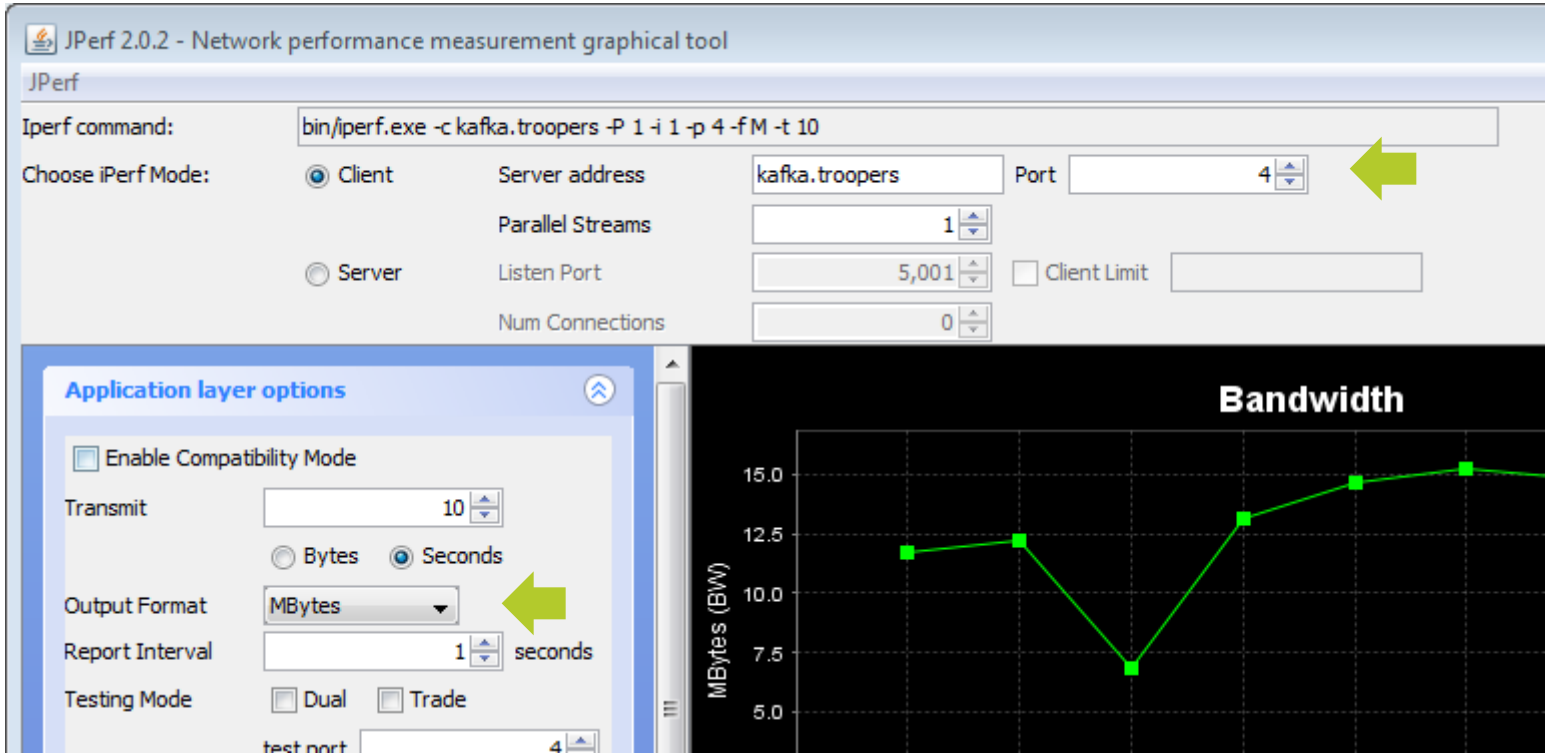
#				VM	Task Description
E07	X	X	X	X	iperf: Test the network performance between your device and Kafka with both IP versions. For IPv4 use port 4 and for IPv6 use port 6 (tcp) and ports 44 and 66 (udp).

```
// IPv4 – TCP
iperf.exe -c kafka.troopers -P 1 -i 1 -p 4  -f M -t 2

// IPv6 – TCP
iperf.exe -c kafka6.troopers -P 1 -i 1 -p 6  -f M -t 2 –V

// IPv4 – UPD
iperf.exe -c kafka.troopers -P 1 -i 1 -p 44  -f M -t 2 -u -b 1000M

// IPv6 – UDP
iperf.exe -c kafka6.troopers -P 1 -i 1 -p 66 -V -f M -t 2 -u -b 1000M
------------------------------------------------------------
Client connecting to kafka.troopers, UDP port 66
…
[284]  0.0- 2.0 sec  9.75 MBytes  4.85 MBytes/sec  2.382 ms    0/ 6958 (0%)
```

E08

#				VM	Task Description
E08	X				jperf: Re-run tests with jperf

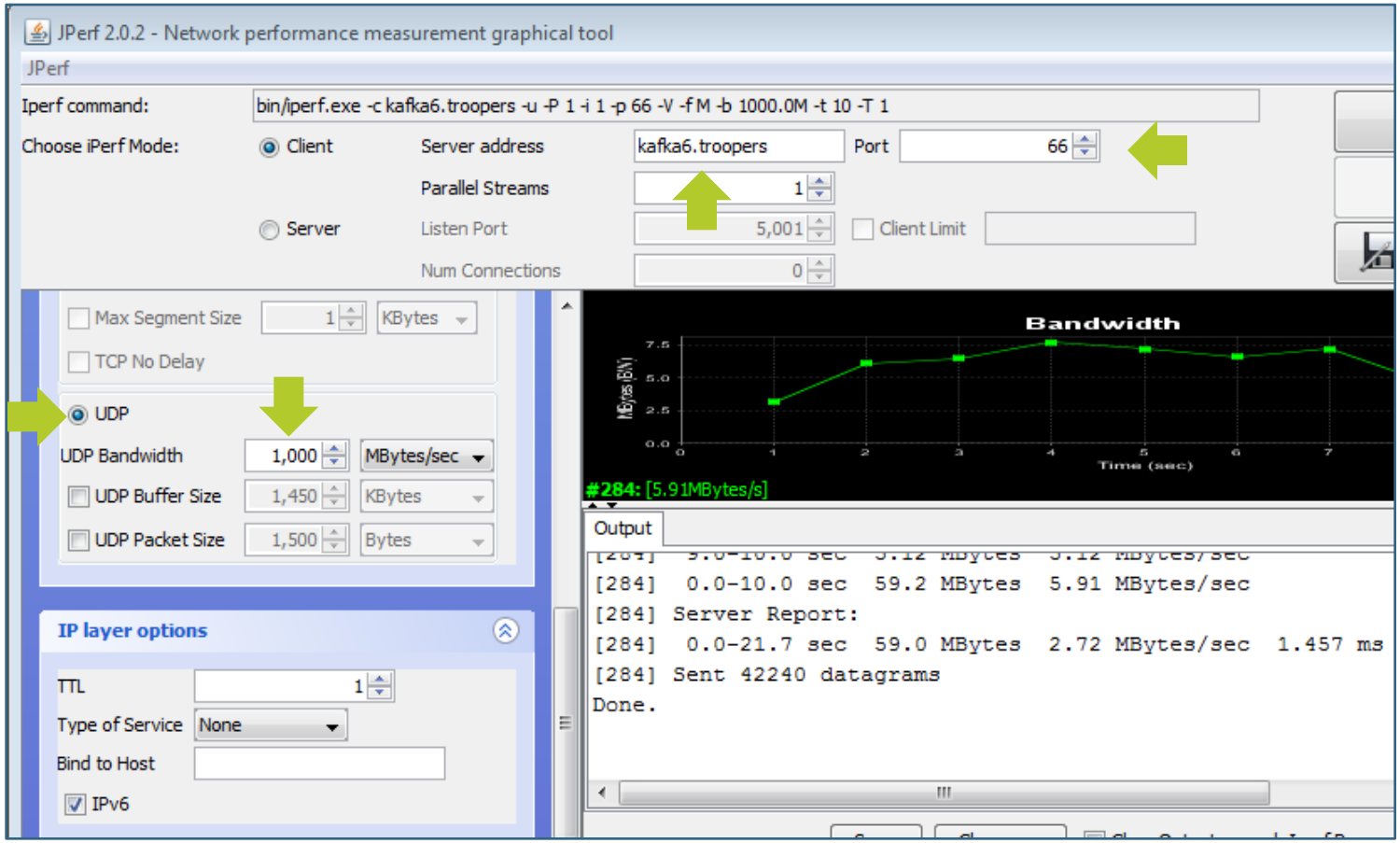
IPv4 - TCP



E08

#				VM	Task Description
E08	X				Jperf: Re-run tests with jperf

IPv6 - UDP



Content

Your Feedback

Good

+ …

To improve

- …

In case of further questions

AWK GROUP

Gabriel Müller
Dipl. El.-Ing. ETH
Senior Consultant

gabriel.mueller@awk.ch

Content

Nice to know

snmptranslate

```
// Convert numerical OID to MIB name entry
trooper@UbuntuTeacher:~$ snmptranslate .1.3.6.1.2.1.2.2.1.2 2>/dev/null
IF-MIB::ifDescr
trooper@UbuntuTeacher:~$

// Find numerical OID given the (incomplete) MIB name entry
// If you have full name, you can omit (-Ib), e.g. SNMPv2-MIB::sysName
trooper@UbuntuTeacher:~$ snmptranslate -On -Ib ifDescr 2>/dev/null
.1.3.6.1.2.1.2.2.1.2

// Find MIB of MIB entry
trooper@UbuntuTeacher:~$ snmptranslate  -Ib sysname 2>/dev/null
SNMPv2-MIB::sysName
trooper@UbuntuTeacher:~$
```

Nice to know

Date and Time (OS X / Ubuntu)

For details about output see:
http://nlug.ml1.co.uk/2012/01/ntpq-p-output/831

```
trooper@UbuntuTeacher:/home/trooper# ntpq -pn
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
 2a02:8071:f00:1 192.33.96.102    2 u   41   64    7    0.925   -2.453   4.615
tropper@UbuntuTeacher:/home/trooper#

trooper@UbuntuTeacher:~$ timedatectl status
      Local time: Fr 2016-02-19 21:39:21 CET
  Universal time: Fr 2016-02-19 20:39:21 UTC
        Timezone: Europe/Berlin (CET, +0100)
     NTP enabled: yes
NTP synchronized: yes
…
 Last DST change: DST ended at
                  So 2015-10-25 02:59:59 CEST
                  So 2015-10-25 02:00:00 CET
 Next DST change: DST begins (the clock jumps one hour forward) at
…
trooper@UbuntuTeacher:~$
```

Nice to know

net-snmp command syntax

- SNMPv1/2 (community string)

```
trooper@UbuntuTeacher:~$ snmpget -v 2c -c <communitystring> <IP/FQDN> <OID/OIDname>
```

  - This is unsecure, everything is transmitted in clear text (check with packet sniffer)
  - Use SNMPv3 (authentication and encryption)
  - Demand SNMPv3 support from vendors (yes, there are still products without SNMPv3 support)

- SNMPv3 (user)

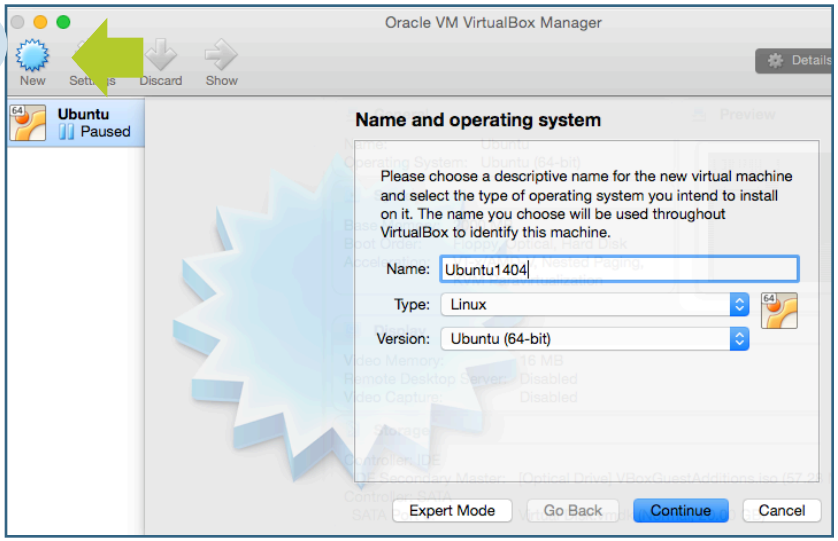
```
trooper@UbuntuTeacher:~$ snmpget -v 3 -n "" -u <username> -a SHA -A "<authKey>" -x
AES -X “privKey" –l authPriv <IP/FQDN> <OID/OIDname>
```

  - This example uses encryption and authentication, for more information see: http://www.net-snmp.org/tutorial/tutorial-5/commands/snmpv3.html

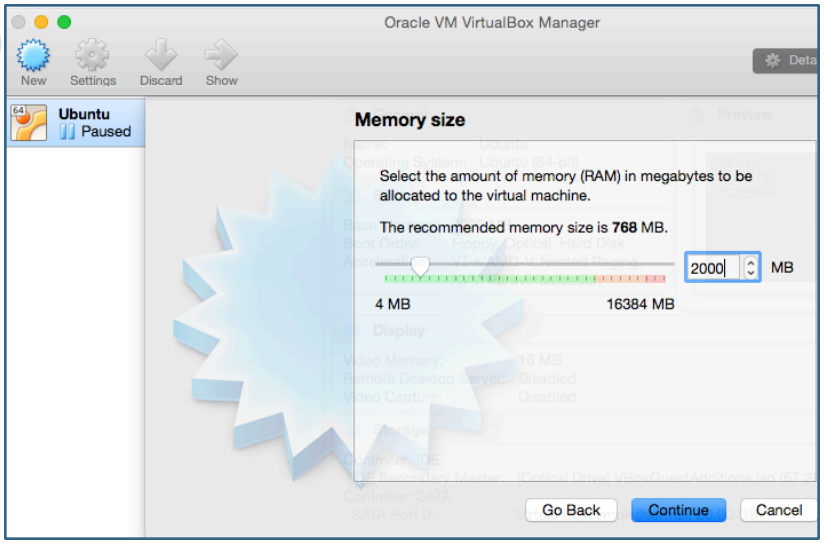
Import VMware Image into VirtualBox

1. New, name it, select Type Linux, Version Ubuntu (64bit), Continue
2. Assign at least 2GB of RAM (the more, the better), Continue
3. Select existing Virtual Disk File (Virtual Disk.vmdk), Create

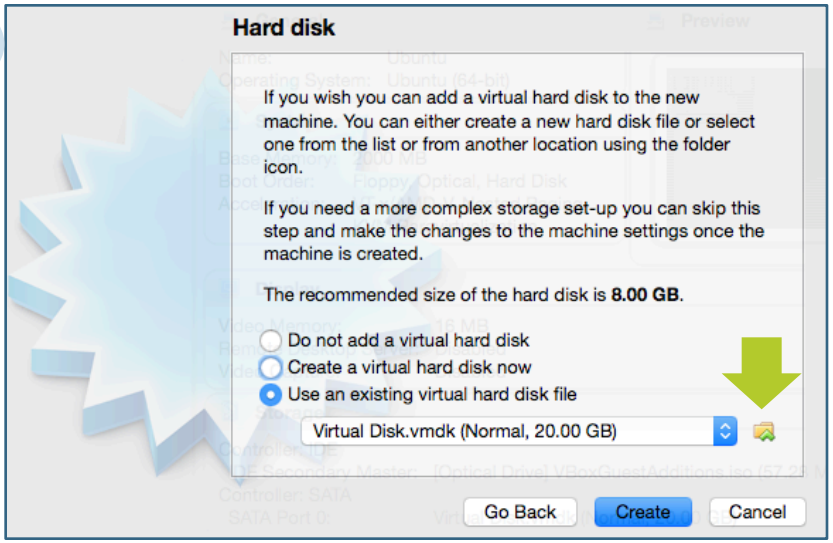
1



2



3



Import VMware Image VMware Fusion

- Add .vmwarevm to folder name
- Fusion now should recognize VM folder