

Consulting Engineering Project Management



Tools for Troubleshooting and Monitoring IPv6 Networks

Troopers, 15th of March 2016

Gabriel Müller, Senior Consultant

AWK Group

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
0.1	

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

Motivation

- Lab Environment
- Your Tasks
- Answers
- Summary
- ► Other



Motivation

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 ...:cc3: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
```



Motivation

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 seg=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 seg=1 ttl=64 time=1.13 ms
64 bytes from galileo.troopers: icmp seq=2 ttl=64 time=1.03 ms
```

Content

Motivation

Lab Environment

- Your Tasks
- Answers
- Summary
- ► Other



The Big Picture





Addressing and Services



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

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)





Addressing and Services



Credentials



Lab Environment Tools – CLI

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

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

Lab Environment Tools - GUI

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



Content

- Motivation
- Lab Environment
- Your Tasks
- Answers
- Summary
- ► Other



A - Set up your stuff

#		Ú	0	VM	Task Description		
A01	Х	Х	Х		Download required tools from server (Kafka)		
A02				Х	Assign static IPv6 address to your Ubuntu guest VM (optional)		
A03	Х	Х	Х		Install tcpdump / windump and Wireshark		



B - Basics

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

C – SNMP – Basics

#		Ú	0	VM	Task Description	
C01	Х	Х	Х	Х	Ensure that generic MIB files are installed on your system and download vendor specific MIB files from server (Kafka) (optional)	
C02	Х	Х	Х	Х	Setup / configure your client to use the MIB files (optional)	
C03	Х	Х	Х	Х	Verify that you can query devices (Galileo, Kafka) with SNMP, using IPv4 and SNMPv2c credentials	
C04		Х	Х	Х	Verify that you can query devices (Galileo, Kafka) with SNMP, using IPv6 and SNMPv2c credentials	
C05	Х	Х	Х	Х	Verify that you can query devices (Galileo, Kafka) with SNMP, using IPv4 and SNMPv3 credentials	
C06		Х	Х	Х	Verify that you can query devices (Galileo, Kafka) with SNMP, using IPv6 and SNMPv3 credentials	
C07		Х	Х	Х	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

#	Ú		VM	Task Description		
C08			Х	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			Х	How can you restrict / limit access to snmpd to specific IPv4 and IPv6 ranges?		
C10			Х	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

#	Ú	VM	Task Description		
D01		Х	Create a login for your local Observium installation (you need to specify privileges level 10 for admin rights).		
D02		Х	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		Х	Add Galileo and Kafka to your Observium installation. Ensure that IPv6 is used for the snmp queries of Observium.		



E – Various

#		Ú		VM	Task Description			
E01	Х	Х	Х	Х	NTP: Query the ntp server (kafka) via IPv4 and v6			
E02	Х	Х	Х	Х	Port Scanning: Ports which your device is listening for incoming connections on v4/v6			
E03	Х	Х	Х	Х	Port Scanning: Investigate which well known ports (1-1024) are open on router and server (v4 and v6)			
E04				Х	ntopng: Change password of your local ntopng installation			
E05				Х	ntopng: Restart your local ntopng instance and have a look at the traffic breakdowns			
E06	Х	Х	Х	Х	ntopng: Have a look at the ntopng installation on Kafka			
E07	Х	Х	Х	Х	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	Х				Jperf: Re-run tests with jperf			
E09	Х	Х	Х	Х	For the brave: Try to compile snmpb for Ubuntu / OS X / Win7			

Content

- Motivation
- Lab Environment
- Your Tasks
- Answers
- Summary
- ► Other



A01

#		Ú	\bigcirc	VM	Task Description
A01	Х	Х	Х		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

#		Ú		VM	Task Description				
A02				Х	Assign static IPv6 address to your Ubuntu guest VM (optional)				
• Ed	Edit /etc/network/interfaces								
# Sta	tic	IPv	6 ac	dre	SS				
auto	p5p1								
iface	p5p)1 i	net6	sta	atic				
	address 2a02:8071:f00:90::1223								
:	netmask 64								
	gateway 2a02:8071:f00:90::10								

• Ensure that IPv6 address is not allready used!

A03

#		Ú	\bigcirc	VM	Task Description
A03	Х	Х	Х		Install tcpdump / windump and Wireshark

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



#		Ú		VM		Task Description						
B01	Х	Х	Х	Х	Chec	k your local routing table.	Whic	h is your IPv6 default route?	?			
C:\Users\mug>netsh interface ipv6 show route												
Veröf	f.	Тур			Met	Präfix	Idx	Gateway/Schnittstelle				
Nein		Man	uell		8 :	:/0	11	LAN-Verbindung* 16				
Nein		Man	uell		256 :	:/0	12	fe80::222:4dff:fe9b:7c69				
•••												
Gabri	els-	Mac	Book	-Pr	o:~ mu	ellega\$ netstat -rn -f in	et6					
Routi	Routing tables											
Inter	net6	5:										
Destination						Gateway		Flags Netif Exp	pire			
default						fe80::222:4dff:fe9b:7c69	%en4	UGc en4				
::1						::1		UHL lo0				





#		Ú	$\textcircled{0}{0}$	VM	Task Description							
B01	Х	Х	Х	Х	Check your local routing table. Which is your IPv6 default route?							
troop	er@U	bun	tuTe	eache	er:~\$ netstat -rn AF -6							
Kerne	l IP	v6	rout	ing	table							
Desti	nati	on			Next Hop	Flag Met Ref Use	If					
•••												
::/0					fe80::222:4dff:fe9b:7c69	UGDAe 1024 0	0 eth0					
•••	••											





#		Ú		VM			Task	Descri	ption		
B02	Х	Х	Х	Х	Check your	neighbour	cache f	or IPv6	neighbo	urs.	
C:\Us	ers\	mug	>net	sh :	interface ip	v6 show ne:	ighbors				
•••											
Schni	ttst	ell	e 12	: Li	AN-Verbindun	g					
Inter	neta	dre	sse				Phys	ische	Adresse	Тур	
											-
fe80:	:222	:4d	ff:f	e9b	: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	
Gabri	els-	Mac	Book	-Pro	o:~ muellega	\$ ndp -an					
Neigh	bor					Linklayer	Address	Neti	f Expire	St Flgs I	Prbs
fe80:	:222	:4d	ff:f	e9b	:7c69%en4	0:22:4d:91	o:7c:69	en4	6s	R R	





#		Ú	\bigcirc	VM	Task Description
B02	Х	Х	Х	Х	Check your neighbour cache for IPv6 neighbours.

rooper@UbuntuTeacher:~\$	ip -6	5 neig	gh 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

#		Ú		VM	Task Description
B03	Х	Х	Х	Х	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

#		Ú		VM				Task Description
B04	Х	Х	Х	Х	Use the	e trad inte	cero rnet	ute to determine the path of IPv6 packets to a target in (e.g. heise.de).
C:\Us	ers\	mug	>tra	acer	t -6	-d]	heise	e.de
Route	nver	fol	gung	y zu	heis	se.de	e [2a	a02:2e0:3fe: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::
Ablau	fver	fol	gung	g be	endet	- •		

C:\Users\mug>

B04

#		Ú	0	VM	Task Description
B04	Х	Х	Х	Х	Use traceroute to determine the path of IPv6 packets to a target in the internet (e.g. heise.de).
Gabri	els.	Mac	Book	-Pr	o:~ 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

#		Ú	\bigcirc	VM	Task Description
B04	Х	Х	Х	Х	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:~\$

#		Ú	\bigcirc	VM	Task Description							
B05	Х	Х	Х	Х	Your IPv6 address is assigned dynamically. Which mechanis used (DHCPv6 or SLAAC)?							
	No. ▷ F ▷ E ▷ I ⊿ I	0v6.dst== Tim 277 7 1509 1 2246 3 2840 4 rame 27 thernet nternet Type: Code: Code: Code: Check Cur h 4 Flags 0. .1 Route Reach Retra 4 ICMPv Ty Le Pr 4 Fl	#f02::1 # Source fe80:: fe90:: sum: 0x o0:	:20d:b9f :20	Destination Protocol Length Info ff:fe40:775 ff02::1 ICMPv6 142 Router Advertisement from 00:0d:b9:40:07:7 sige Protocol v6 isissement (134) isissement (134) isorrect] vert: 0 ; iso isi iso ;: 0 fix information : 2a02:8071:f00:110::/64) iso iso if if if if if bn-link flag(L): Set uutonomous address-configuration flag(A):							

B06

#				\bigcirc	VM		Task	Descript	ion					
B0	6	Х	Х	Х	Х	For DNS looku	ps of your clier	nt, which I	P ver	sion is	s use	ed?		
	No.	ns Tir 277 4 278 4	n€ Sour . 2a0 . 2a0 78: 11	ce 2:8071 2:8071 L6 byte	:f00:1 :f00:1 es on	10:a994:1c79:cd6:7164 10::10 wire (928 bits), 116 byt	Destination 2a02:8071:f00:110::10 2a02:8071:f00:110:a9 tes captured (928 bits)	Protocol DNS DNS DNS on interface (Length 88 116	Info Standard Standard	query query	0x90bf respons	AAAA he ;e 0x90t	eise.de
	⊳ Et ⊳ In ⊳ Us	therne nterne ser Da	t II, t Prot tagran	Src: F tocol N n Proto	PcEngi Versio Dcol,	ne_40:07:75 (00:0d:b9:40 n 6, Src: 2a02:8071:f00: Src Port: 53 (53), Dst P	0:07:75), Dst: Vmware_8 110::10, Dst: 2a02:807 Port: 59607 (59607)	e:47:82 (00:0c 1:f00:110:a994	:29:8e:4 :1c79:cd	7:82) 6:7164				
		International Content of the second s	Name S <u>uest 1</u> 2: 0.0 sactions: 2: 0x8 tions: 2: 0x8 tions:	5ystem (n: 277) 0007700 (n ID: (180 St (1 (180 St (188 St) (188 St	(resp 7] 000 se 0x90b tandar 0 0	onse) conds] f d query response, No err A, class IN, addr 2a02:2	or e0:3fe:1001:302::							



#		Ú		VM	Task Description
B07	Х	Х	Х	Х	Install plugins on browser (IPvoo, IPfox,).

Google Chrome

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

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

Any idea for Microsoft IE?



			0.	. ~			
This page is in Germ	a	🖻 www.heise.de	2a02:2e0:3fe:1001:7777:772e:2:85	18	an	~	×
		a 1.f.ix.de	2a02:2e0:3fe:1001:f1::87				_
News No		🖆 common.i12.de	92.51.153.47				
		🖆 de.ioam.de	91.215.103.65				
		🖻 gzhls.at	85.124.84.253	J			
		🖆 heise.nuggad.net	2a00:cd0:1005:2:80:82:201:80				
TACAAS IN		ig jwpltx.com	54.165.255.130				
Tonthemen: M	, [☐ partner.googleadservices.com	n 172.217.16.130	٦.	Dift		Su
	1	f ping.chartbeat.net	23.23.170.207		SKIIL		3
		f prophet.heise.de	185.54.150.27				
New Deckton Ro		∎ script.ioam.de	91.215.100.39	J			
Neu. Desktop-be		ssl.p.jwpcdn.com	93.184.221.48	J			
		static.chartbeat.com	104.86.200.221				
		a tarifrechner.heise.de					
Bastel-Rechner u	r	a www.googletagservices.com)				
Raspberry P	3	mit WLAN und Blue	100th und 64 Bit				
MISSIO PROCESSION NO.	-				10000000		
and the start							
					and the		٦


B08





C01

#		Ú		VM	Task Description
C01	Х	Х	Х	Х	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





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.

File Options Se	elect Preferences	
Tree Modules Edit Remote SNMP Agent Galileo - Troopers	or Discovery Traps Grap	hs Log Query Results Pv2c
MIB Tree	MIB Tree Modules Traps	Modules Properties
		mibs pibs "J:\Informationssysteme\Dokumentationen\Net <





#		Ú	\bigcirc	VM	Task Description
C02	Х	Х	Х	Х	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

E SnmpB		~		
File Tools Options Help				
Modules Editor Discovery Traps Graphs	Log			
Available MIB modules		Loaded MIB modules		
Module		Module	Required	Languag 📤
2222		IF-MIB	no	SMIv2 =
ACCESSBIND-PIB		SNMPv2-SMI	no	SMIv2
ACCOUNTING-CONTROL-MIB		SNMPv2-TC	no	SMIv2
ACCOUNTING-FRAMEWORK-PIB		SNMPv2-CONF	no	SMIv2
ADSL-LINE-EXT-MIB	->	SNMPv2-MIB	no	SMIv2
ADSL-LINE-MIB		RFC1213-MIB	no	SMIv1
ADSL-TC-MIB		RFC1155-SMI	no	SMIv1
ADSL2-LINE-MIB		RFC-1212	no	SMIv1





#		Ú		VM	Task Description
C02	Х	Х	Х	Х	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

#		Ú	0	VM	Task Description
C03	Х	Х	Х	Х	Verify that you can query devices (Galileo, Kafka) with SNMP, using IPv4 and SNMPv2c credentials
Windo	ows	s (Si	nmp)B)	

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

Agent Profiles	2 <mark>×</mark>	
E	General Properties Profile Name T2016 - Galileo Target SNMP Agent Agent Address/Name 10.20.90.10	
	Agent Port 161	SNMPv1 / v2c Properties
	Retries 1	-
⊳ Kafka - Home	Timeout (sec) 3	
T2016 - Galileo Snmpv1/v2c	Supported SNMP Version	Communities
Get-Bulk	SNMPV1 SNMPV2 SNMPV3	Read community ROCOMMUNITY
Jinnyyy	OK Cancel	Write community



C03

#		Ú		VM	Та	ask Description
C03	Х	Х	Х	Х	Verify that you can query dusing IPv4 and SNMPv2c	levices (Galileo, Kafka) with SNMP, credentials
Wind	ows	(SI	nmp	oB)		
		Tree Ren T20: MIB Tr MIB Tr Note Note	e Mo note SNM 16 - Galile ree MIB MIB MIB A () i i note S MIB A () i i i i i i i i i i i i i i i i i i i	vdules P Agent o Tree so org a (a) d a (a) a (b) a f f f f f f f f f f f f f f f f f f	Editor Discovery Traps Graphs Log Image: Source of the system Image: Source of the system Image: Source of the system Image: Source of the system Image: Source of the system Image: Source of the system Image: Source of the system Image: Source of the system Image: Source of the system Image: Source of the system Image: Source of the system Image: Source of the system Image: Source of the system Image: Source of the system Image: Source of the system Image: Source of the system Image: Source of the system Image: Source of the system Image: Source of the system Image: Source of the system Image: Source of the system Image: Source of the system Image: Source of the system Image: Source of the system Image: Source of the system Image: Source of the system Image: Source of the system Image: Source of the system Image: Source of the system Image: Source of the system Image: Source of the system Image: Source of the system Image: Source of the system Image: Source of the system Image: Source of the system Image: Source of the system Image: Source of the system Image: Source of the system Image: Source of the system Image: Source of the system Im	Query Results SNMP query started 1: sysName.0 Galileo SNMP query finished Total # of Objects = 1 Similar for Kafka: Query Results SNMP query started 1: sysName.0 Kafka SNMP query finished Total # of Requests = 1 Total # of Objects = 1



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.

#		Ú		VM	Task Description
C03	Х	Х	Х	Х	Verify that you can query devices (Galileo, Kafka) with SNMP, using IPv4 and SNMPv2c credentials
OSX /	Ub	unt	u		
troope 2>/de	er@U v/nu	Jbun 111	tuTe	each	er:~\$ snmpget -v 2c -c ROCOMMUNITY kafka.troopers sysName.0

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

#	Ú	\bigcirc	VM	Task Description
C04	Х	Х	Х	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

#		Ú	0	VM	Task Description
C05	Х	Х	Х	Х	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.

USM Profiles	
SR - NE40	User
	Security User Name trooper
	Security
	Authentication Protocol SHA
	Privacy Protocol AES128 -
	Privacy Password
	OK Cancel

		SNMPv3 Properties
	Е	SNMPv3 user (USM) Security Name trooper Security Level authPriv SNMPv3 context
▲ T2016 - Galileo		Context Name Context Engine ID
Get-Bulk SnmpV3 4 T2016 - Kafka		

C05



Windows (SnmpB)





C05

#		Ú	\bigcirc	VM	Task Description								
C05	05 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													
troop	er@U	Jbun	tuTe	each	er:~\$								

```
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

#	Ú	\bigcirc	VM	Task Description					
C06	Х	Х	Х	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

#	Ú	0	VM	Task Description							
C07	Х	Х	Х	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: <u>http://www.net-snmp.org/docs/mibs/</u>
- Hostname: <u>http://www.net-snmp.org/docs/mibs/SNMPv2-MIB.txt</u>
 - sysName.0
- Interfaces: <u>http://www.net-snmp.org/docs/mibs/interfaces.html</u>
 - ifDescr
- Interface Statistics: <u>http://www.net-snmp.org/docs/mibs/ip.html#iplfStatsTable</u>
 - iplfStatsTable
- Routes: <u>http://www.net-snmp.org/docs/mibs/ipForward.html</u>
 - inetCidrRouteTable

C07

#	Ú	0	VM	Task Description
C07	Х	Х	Х	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

#		Ú	0	VM	Task Description								
C07		Х	Х	Х	Gather information about hostname, location, interfaces, IPv4/6 counters and IPv4/6 routes from devices (Galileo, Kafka, Firewall) using IPv6 and SNMPv3								
// Interface Statistics													
troop X "tro IP-MI IP-MI IP-MI IP-MI IP-MI	<pre>// Interface Statistics trooper@UbuntuTeacher:~\$ snmpget -v 3 -n "" -u trooper -a SHA -A "trooper!" -x AES - X "trooper?" udp6:firewall6.troopers ipifStatsEntry -1 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</pre>												
TP_MT	R••i	nTf	Stat	GHC	$InReceives[inv4][2] = Counter64 \cdot 1949382$								
TP_MT	B••i	nT f	Stat	GHC	$InReceives[ipv4][5] = Counter64 \cdot 0$								
	B • • i	DT F	Stat	GHC	InPeceives[ipv4][8] = Counter64. 879405								
		ЪТТ	scal	SAC	THVECETAES[ThA4][0] - CONTRET04: 012402								
•••	0	T 1	L (T	1-									
troop	trooper@UbuntuTeacher:~\$												



C07

#		Ú		VM	Task Description								
C07		Х	Х	Х	Gather information about hostname, location, interfaces, IPv4/6 counters and IPv4/6 routes from devices (Galileo, Kafka, Firewall) using IPv6 and SNMPv3								
// Ro troop X "tr IP-FO SMI::	utin er@U oope RWAR zerc	ig E Jbun er?" RD-M oDot	ntri tuTe udp IB:: Zerc	les each o6:f ine o][i]	er:~\$ snmpget -v 3 -n "" -u trooper -a SHA -A "trooper!" -x AES - irewall6.troopers inetCidrRouteTable -l authPriv 2>/dev/null tCidrRouteIfIndex[ipv4]["0.0.0.0"][0][SNMPv2- pv4]["10.1.10.1"] = INTEGER: 2								
IP-FO	RWAF	RD-M	IB::	ine	tCidrRouteIfIndex[ipv6]								
["00: [ipv6 IP-FO ["2a: [ipv6	<pre>IP-FORWARD-MIB::inetCidrRouteIfIndex[ipv6] ["00:00:00:00:00:00:00:00:00:00:00:00:00:</pre>												
•••													

trooper@UbuntuTeacher:~\$



C08

#	Ú		VM	Task Description
C08			Х	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

#	Ú	\bigcirc	VM	Task Description					
C09			Х	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

#	Ú	VM	Task Description
C10		Х	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

#		Ú		VM	Task Description					
D01				Х	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.phphelp [sudo] password for trooper: Observium CE 0.16.1.7533 Add User										
USAGE	:									
addus	er.p	hp	<use< td=""><td>ernai</td><td>me> <password> <level 1-10=""> [email]</level></password></td></use<>	ernai	me> <password> <level 1-10=""> [email]</level></password>					
EXAMP: ADMIN	LE: :	add	user	•phj	o <username> <password> 10 [email]</password></username>					
USER : 0 - 	LEVE Dis	LS: abl	ed (Thi	s user disabled)					
10 .	– Ad	min	istr	ato:	r (This user has full administrative access)					

D02

#		í 👌	VM			Task Descripti	on				
D02			Х	Add your Ubuntu V used. In order to do localhost in /etc/hos	M (lo o this sts.	ocalhost) to Obso s, ensure you hav	ervium ve an	n. Ensure IPv6 ent	e that ry for	IPv	6 is
Basi	OBSE according	RVIUM uration		▼ 📃 Devices ▼ 💻 Ports ▼	🐱 Hea	alth • Authentication Configu	ration	Search		.	-
		Hostnam	ie lo	calhost		Auth Level	authPriv			•	
		Skip pir	ng 🗆	in ICMP echo checks, only SNMP		Auth Username	<yoursnmpv3user></yoursnmpv3user>				
			av	vailability		Auth Password	<yourauthpw></yourauthpw>				
	Proto	col Versio	on v	3 🗸		Auth Algorithm	SHA				
		Transpo	rt 🛛	JDP6		Crypto Password	<yourcryptopw></yourcryptopw>				
		Po	rt 10	51		Crypto Algorithm	AES			•	
		Timeou	ut 1				······				
		Retrie	es 5				Be pa	itient! The f several min	full disc utes.	cover	y car



D03

#	Ú	\bigcirc	VM	Task Description
D03			Х	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?)





#		Ú		VM	Task Description
E01	Х	Х	Х	Х	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>







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:~$
```





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:~$
```



#		Ú	0	VM		Task Description
E02	Х	Х	Х	Х	Port Sc connec	anning: On which ports your device is listening for incoming tions on v4/v6
Wind	ows		Scal Scal Befe Betr	ienmap n Wer local thl: nr echner iebssyst	kzeuge <u>P</u> rofil host nap -T4 -A -v loc Dienste em • Rechne kafka.t 2a02:8(localhc	Hife Imap-Ausgabe Ports / Rechner Neap-Ausgabe Ports / Rechner Rechnereinzelheiten Scan Bitteleuropäische Zeit NSE: Loaded 132 scripts for scanning. NSE: Script Pre-scanning. Initiating NSE at 23:07 Gompleted NSE at 23:07 Completed NSE at 23:07, 0.00s elapsed Initiating Parallel DNS resolution of 1 host. at 23:07 Completed Parallel DNS resolution of 1 host. at 23:07, 0.00s Completed Parallel DNS resolution of 1 host. at 23:07, 0.00s Skipping SYN Stealth Scan against localhost (127.0.0.1) because Windows does not support scanning your own machine (localhost) this way. Initita

#		Ú	\bigcirc	VM	Task Description						
E02	Х	Х	Х	Х	ort Scanning: On which ports your device is listening for incoming onnections on v4/v6						
OS X											
// IP Gabri	v4 - els-	- TC -Mac	P Book	-Pro	o:~ muellega\$ nmap localhost						
// IP Gabri	v6 – els-	- TC -Mac	P Book	-Pro	o:~ muellega\$ nmap localhost -6						
// IP Gabri	v4 – els-	- UD -Mac	P Book	-Pro	o:~ muellega\$ sudo nmap localhost —sU						
// IP Gabri 	v6 – els-	- UD •Mac	P Book	-Pro	o:~ muellega\$ sudo nmap localhost —sU -6						
PORT 123/u	s dp c	STAT open	E SE nt	RVI(p	CE						



#		Ú		VM		Task Description
E02	Х	Х	Х	Х	Port Scanning: On which connections on v4/v6	ports your device is listening for incoming
Ubun	tu					
troop	er@U	Jbun	tuTe	each	er:~\$ sudo netstat -plnt	-4 // TCP IPv4
troop	er@U	Jbun	tuTe	each	er:~\$ sudo netstat -plnt	-6 // TCP IPv6
troop	er@U	Jbun	tuTe	each	er:~\$ sudo netstat -plnu	-4 // UDP IPv4
troop Activ	er@U e In	Jbun iter	tuTe net	each con:	er:~\$ sudo netstat -plnu nections (only servers)	-6 // UDP IPv6
Proto	Rec	v-Q	Ser	nd-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



#		Ú	0	VM	Task Description
E03	Х	Х	Х	Х	Port Scanning: Investigate which well known ports (1-1024) are open on router and server (v4 and v6)
808 z	enmap				 Instead of kafka6 troopers you can
Target: ka Command: Hosts S OS Hos	ifka6.tro	IA -A -V -G IA -A -V -G Nma NSE Ini Sca Com ela Ini Sca Dis Dis Dis Dis Dis Dis Dis Dis	5 kafka6.t p Output p -T4-A-v i Coauer Scrip tiating pleted tiating pleted tiating pleted tiating covered covered covered covered covered covered covered covered tiating pleted i Scrip tiating pleted tiating pleted to tiating pleted to tiating	▼ F roopers Ports/ -6 kafka6 u 110 S t Pre-s Ping Sc System System Connect afka6.t open p open p Service t scann NSE at	<pre>profile:</pre>



#	Ú	0	VM	Task Description
E04			Х	ntopng: Change password of your local ntopng installation

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

Welcome to ntop	ng ×	+										
(P) (localho	ost:3000				4 ⊂ Search						+	⋒
ntop			*	Flows	Hosts 🗸	Interfaces -	0 -	4 -	Q	Searc	ch Host	
Dashboard:	Talkers	Hosts	Ports	Applications	s ASNs	Senders						
				Тс	p Flow Ta	alkers						



#	Ś	VM				T	ask De	escript	tion				
E05		Х	ntopng: Re ntopng pag	estart yo ge	ur lo	ocal	Ubunt	u VM a	and I	have	e a	look again at	the
		Welcome	e to ntopng × 🔶			ñ.	4 C ^a Q, search Flows Hosts →	Interfaces 🗸 🔹 🔹	_ ☆ 自 ▲ - Q	Search Host	_ @ ≡	=	
		eth0: To	p Local Talkers	Actual Traffic	eth0: Realtin	ne Top Appli	cation Traffic	Network Interfa	aces: Realtime 1	Traffic			
		10.20.11	0.206	159.72 Kbit 🕹	0.000	RTMP HTTP	SSL Onknown	552 Kbit/s		●eth0			
		VM-Mug	[vm-mug]	12.56 Kbit 🕁	2 Mbit/s			480 Kbit/s					
		10.20.11	0.124	355.2 bps 🔸	1 Mbit/s			400 Kbit/s					
					000 // 100			240 Kbit/s					
					800 KDIVS			160 Kbit/s					
					400 Kbit/s			80 Kbit/s					
					0	21:	15:50 21:16:15	0	21:15:55	21:16:21	1		
		eth0: To	p Remote Destinations	Actual Traffic	eth0: Top A	oplication Tr	affic Last Day View	Network Interfa	ices: Last Day	View			
		54.239.1	69.212	143.06 Kbit 🕹		RTMP HTTP	SSL Unknown	412 Kbit/s		eth0			
		ea-in-f12	25.1e100.net	15.75 Kbit 🛧	264 Kbit/s 240 Kbit/s								
		zrh04s06	3-in-f14.1e100.net	9.9 Kbit 🕁	200 Kbit/s			320 Kbit/s					
		10.20.10	0.100	2.02 Kbit 🛧	160 Kbit/s			240 Kbit/s					
		fe80::200	2:09ff:fe40:775	1.56 Kbit 🛧	120 Kbit/s			160 Kbit/s					
		lon2-links	an-a4 lon2 spotify com	716.8 hps	40 Kbit/s			80 Kbit/s					
		194.230.	77.201	643.2 bps 🗸	0	0.00	15:00:00 21:10	0 21:25:51	5	15:00:00 2	1:16:20		
					21.2		10.00.00 21.10	21.20.0		10.00.00 2			
		© 1998- General for user License	2016 - nlop.org ted by ntopng Professional v.2.2.160216 admin and interface eth0 expires In 9 min, 26 sec	180.93 Kb	ops [18 pps]		7.82 Kbps 169.65 Kbps	Uptime: 1 min, 12 sec 46 Hosts 221 Flows					





#		Ú	\	VM	Task Description
E06	Х	Х	Х	Х	ntopng: Have a look at the ntopng installation on Kafka

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



#		Ú		VM	Task Description						
E07	Х	Х	Х	Х	erf: Test the network performance between your device and afka with both IP versions. For IPv4 use port 4 and for IPv6 use ort 6 (tcp) and ports 44 and 66 (udp).						
// тр	7/	- TC	D								
iperf	iperf.exe -c kafka.troopers -P 1 -i 1 -p 4 -f M -t 2										
// IP	// IPv6 — TCP										
iperf	iperf.exe -c kafka6.troopers -P 1 -i 1 -p 6 -f M -t 2 -V										
// IP	v4 -	- UP	D								
iperf	.exe	e - c	kaf	ka.	troopers -P 1 -i 1 -p 44 -f M -t 2 -u -b 1000M						
// IP	v6 -	- UD	P								
iperf	iperf.exe -c kafka6.troopers -P 1 -i 1 -p 66 -V -f M -t 2 -u -b 1000M										
Clien	t co	onne	ctir	ng to	o kafka.troopers, UDP port 66						
	0	0	2 0	202	0.75 MDzztog 4.95 MDzztog 2.292 mg $0/(6059/(0.9))$						
[204]	0.	0-	Ζ.Ο	sec	9.15 MBYLES 4.05 MBYLES/SEC 2.302 IIIS 0/ 0958 (0%)						





#		Task Description
E08	Х	jperf: Re-run tests with jperf

IPv4 - TCP





E08



IPv6 - UDP




Content

- Motivation
- Lab Environment
- Your Tasks
- Answers

Summary

► Other



Summary

Your Feedback

Good



To improve





Summary

In case of further questions





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

gabriel.mueller@awk.ch



Content

- Motivation
- Lab Environment
- Your Tasks
- Answers
- Summary





Other 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
TF-MTB:: 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:~$
```

Other Nice to know

Date and Time (O	S X / Ubuntu)			For det	ails about o	utput see:		
trooper@UbuntuTea	cher:/home/troo	per# nt	na-pa	http://n	lug.ml1.co.u	ik/2012/01/	ntpq-p-outp	ut/831
remote	refid	sttw	vhen pol	l reach	delay	offset	jitter	
2a02:8071:f00:1	192.33.96.102	2 u	41 6	54 7	0.925	-2.453	4.615	
tropper@UbuntuTea	cher:/home/troc	per#						
trooper@UbuntuTea	cher:~\$ timedat	ectl st	atus					
Local time:	Fr 2016-02-19	21:39:2	21 CET					
Universal time:	Fr 2016-02-19	20:39:2	21 UTC					
Timezone:	Europe/Berlin	(CET, +	-0100)					
NTP enabled:	yes		·					
NTP synchronized:	yes							
•••								
Last DST change:	DST ended at							
	So 2015-10-25	02:59:5	59 CEST					
	So 2015-10-25	02:00:0)0 CET					
Next DST change:	DST begins (th	ne clock	, jumps	one hour	forward)	at		

trooper@UbuntuTea	cher:~\$							

Other 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: <u>http://www.net-snmp.org/tutorial/tutorial-5/commands/snmpv3.html</u>



Nice to know

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

	Oracle VM VirtualBox Manager
New Settings Discard Show	Name and operating system
	Please choose a descriptive name for the new virtual machine and select the type of operating system you intend to install on it. The name you choose will be used throughout VirtualBox to identify this machine.
	Name: Ubuntu1404
	Type: Linux
	Version: Ubuntu (64-bit)
	Video Memory: 16 MB Remote Desktop Server: Disabled
	Video Capture: Disabled
	A Marine -
	DE Secondary Master: - [Optical Drive] VBoxGuestAdditions iso (5
	Expert Mode Go Back Continue Canc





Nice to know

Import VMware Image VMware Fusion

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

