



## **ABANS DE COMENÇAR**

- 1. Ves a menú Fitxer i sel·lecciona l'opció Fes una còpia... i desa-la a la carpeta corresponent dins de la professora té compartida amb tu.**
- 2. Reanomena el fitxer de la següent manera:  
"SMX MP05 UF3 NF4 A1.1 Instal·lació i anàlisi interfície NTP  
Nom Cognoms"**

### **Resultat d'aprenentatge**

4. Descriu les tècniques i els procediments de monitoratge de la xarxa local segons unes especificacions donades.

### **Criteris d'avaluació**

- 4.1 Identifica els paràmetres que identifiquen el rendiment d'una xarxa local tenint-ne en compte l'arquitectura i la tecnologia de xarxa de suport.
- 4.2 Enumera les eines maquinari i programari utilitzades en el monitoratge d'una xarxa local tenint-ne en compte les especificacions tècniques.
- 4.3 Explica el funcionament de les eines de gestió de la xarxa per obtenir informació del trànsit i rendiment de les comunicacions de la xarxa local, segons especificacions tècniques de les mateixes eines.
- 4.4 Explica el procés a seguir per monitorar el trànsit d'una xarxa local en funció de les topologies i protocols de xarxa implementats.
- 4.5 Descriu els procediments de resolució d'incidències segons el pla de manteniment preventiu i periòdic.

## **ENUNCIAT**

### **MONITORATGE DE LA XARXA AMB ntop**

**FES UN VÍDEO DE TOTS ELS PASSOS QUE ES DEMANEN.**

#### **1. Instal·lació ntop**

- a) En una màquina Ubuntu GNU/Linux: **apt-get install ntopng**

Si no funciona feu apt-get update i després apt-get upgrade.



CFGM SMX MP05 UF3 NF4 A1

Reconfigura Ntop mitjançant la comanda: **dpkg-reconfigure ntopng**

Especifica quina serà la interfície que utilitzarem per realitzar l'anàlisi de la xarxa i defineix el nom d'usuari que utilitzarà ntopng (per defecte, ntopng)

b) Reinicia Ntop mitjançant la comanda: **/etc/init.d/ntopng start** (posa una captura)

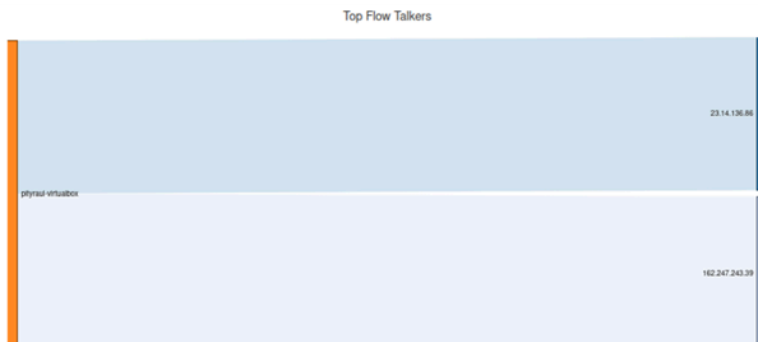
**Starting ntopng (via systemctl): ntopng.service.**

c) Fes **/etc/init.d/ntopng status** (posa captura)

```
● ntopng.service - ntopng - High-Speed Web-based Traffic Analysis and Flow Collection Tool
Loaded: loaded (/lib/systemd/system/ntopng.service; enabled; vendor preset: enabled)
Active: active (running) since Fri 2024-05-10 13:20:58 CEST; 4min 30s ago
Docs: man:ntopng(8)
      file:/usr/share/doc/ntopng/README.Debian
      file:/usr/share/doc/ntopng/UserGuide.pdf.gz
Process: 1232 ExecStart=/usr/sbin/ntopng /etc/ntopng.conf (code=exited, status=0/SUCCESS)
Main PID: 1809 (2/flow_checks)
Tasks: 24 (limit: 5759)
Memory: 177.3M
CPU: 4.706s
CGroup: /system.slice/ntopng.service
        └─1809 /usr/sbin/ntopng /etc/ntopng.conf
```

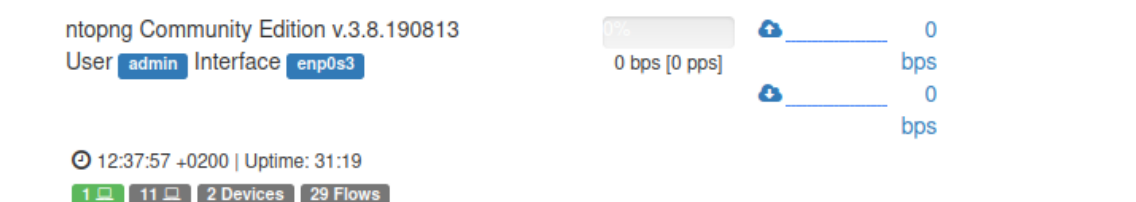
d) Obre el navegador i accedeix a Ntop mitjançant: <http://localhost:3000>

e) Introdueix usuari i contrasenya per defecte admin admin, i després canvia la contrasenya quan t'ho demani per "elteunomcognom1".



## 2. Anàlisi de la interfície de Ntop

a) A la primera pantalla a baix de tot hi ha la següent informació





## A1.1 Instal·lació i anàlisi interfície NTOP



CFGM SMX MP05 UF3 NF4 A1

Entra a tots els links i fes captura de pantalla de cada apartat.

10 - Hosts - Status - Severity - Direction - Applications - Categories - DSCP - Host Pool - Networks - IP Version - Protocol										
	Application	Protocol	Client	Server	Duration	Breakdown	Actual Thpt	Total Bytes	Info	
	DNS	 UDP	pityraul-virtualbox  10.0.2.3	10.0.2.3  domain	00:01 sec	<div>Client Server</div>	0 bps	327 Bytes	us-west1.prod.sumo.prod...	










10 - IP Version- Direction- Filter Hosts									
	IP Address	Flows	MAC Address	Name	Seen Since	Breakdown	Throughput	Total B	
	102.2	1	33:33:00:00:00:02		00:37 sec	Recv	0 bit/s	62 B	
	216.239.38.120	2	RealtekU_12:35:02	www.google.com	02:51	Sent	0 bit/s	1.11	
	216.239.32.36	1	RealtekU_12:35:02	region1.google-analytics...	02:32	Sent Recv	0 bit/s	27.3	
	178.62.197.130	1	RealtekU_12:35:02	www.ntop.org	02:05	Sent Recv	0 bit/s	6.3	













10

IP Version

Direction

Filter Hosts

	IP Address	Flows	MAC Address	Name	Seen Since	Breakdown	Throughput	Total B
	fe80::5371:68a3:2d2b:87b2 	1	PcsCompu_82-F3:C3	pityraul-virtualbox [IPv...	07:41	<div>Sent</div>	80.66 bit/s 	3.36
	10.0.2.3 	4	RealtekU_12:35:02		07:39	<div>Sent Recv</div>	1.01 kbit/s 	89.38
	10.0.2.15 	25	PcsCompu_82-F3:C3	pityraul-virtualbox	07:41	<div>Sent Recv</div>	18.79 kbit/s 	16.7

10 -	Hosts	Status	Severity	Direction	Applications	Categories	DSCP	Host Pool	Networks	IP Version	Protocol				
	Application		Protocol	Client	Server		Duration	Breakdown		Actual Thpt	Total Bytes	Info			
	G+ TLS GoogleDo...		TCP	pityraul-virtualbox  58764	142.250.184.174  https		08:02	<div>Client Server</div>		0 bps	340.14 KB	docs.google.com			
	G+ TLS Google		TCP	pityraul-virtualbox  34466	142.250.200.78  https		03:04	<div>Client Server</div>		0 bps	52.3 KB	play.google.com			
	G+ TLS Google		TCP	pityraul-virtualbox  41298	142.250.178.163  https		04:18	<div>Client Server</div>		0 bps	21.93 KB	ssl.gstatic.com			
	TLS.Cloudfla...		TCP	pityraul-virtualbox  51738	104.16.79.73  https		02:24	<div>Client Server</div>		0 bps	12.36 KB	cloudflareinsights.com			

b) Entra al navegador i obre 3 webs diferents. Anota-les aquí:

Clica el botó Flows i mira si t'han aparegut les webs que has obert al navegador. Fes captura de pantalla i omple la següent taula:

Nom aplicació	Durada connexió	Total Bytes descarregats
MediaMarkt	3:06	1.67
Youtube	3:05	3.42
ZARA	3:04	1.57



c) Entra a una web i ves a mirar la velocitat de pujada i baixada a la pàgina principal. Fes captura de pantalla de la velocitat. (Si no vas ràpid hauràs de tornar a visitar una pàgina web perquè et sortirà velocitat 0).

d) A l'apartat de Hosts indica com es distingeix entre màquina local i màquina remota fent una captura de pantalla.

	IP Address	Flows	MAC Address	Name	Seen Since	Breakdown	Throughput
	fe80::d2f2534:5d4:c17d	1	EliteGro_B4:A1:D0		01:55	Sent	0 bit/s
	fe80::94f29:cc49:5f1b	7	Compalln_Es:B9:F9		04:24	Sent	0 bit/s
	fe80::874:1442:b6e4:aa82	2	EliteGro_B4:92:CD		04:29	Sent, Recd	0 bit/s
	fe80::69d6:648f:898b:fe06	1	EliteGro_B4:93:46	fe80::69d6:648f:898b:fe0...	04:29	Sent, Recd	223.56 bit/s
	fe80::5a2c:2762:991f:4981	3	EliteGro_2B:0D:BC	fe80::5a2c:2762:991f:498...	04:28	Sent, Recd	0 bit/s

e) Per poder fer `ifconfig -a` has d'instal·lar el paquet `net-tools`.

Com a superusuari fes: `# apt install net-tools`

Ara cerca la IP i la MAC de la interfície de la teva targeta de xarxa. (posa captura de pantalla)

```
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::5371:68a3:2d2b:87b2 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:82:f3:c3 txqueuelen 1000 (Ethernet)
    RX packets 679 bytes 744556 (744.5 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 538 bytes 53282 (53.2 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Bucle local)
```

f) Entra a la pantalla on hi ha el teu host (per la IP) i comprova que té la MAC que has vist a l'apartat anterior. (captura de pantalla)

### Local Hosts

	IP Address	Flows	MAC Address	Name	Seen Since	Breakdown	Throughput	Total Bytes
	fe80::5371:68a3:2d2b:87b2	1	PcsCompu_82:F3:C3	plyraul-virtualbox [IPv...	07:52	Sent	80.37 bit/s	2.91 KB
	10.0.2.15	51	PcsCompu_82:F3:C3	plyraul-virtualbox	07:52	Recd	388.91 bit/s	7.83 MB



- g) Indica el trànsit enviat i rebut (Traffic Sent / Received) que et surt a tu (posa captura de pantalla)



- h) Indica els Fluxes de dades (Active Flows) que hi ha com a client i com a servidor. (posa captura de pantalla)

Per què creus que no hi ha gairebé fluxes de dades com a servidor?

### Exemple

Traffic Sent / Received	1,809 Pkts / 145.55 KB —	893 Pkts / 366.81 KB —
Active Flows / Total Active / Low Goodput	As Client	As Server
	6 — / 1,108 — / 1 —	0 — / 2 — / 0 —

- i) A Active Flows ves a la pestanya Applications i fes captura de les aplicacions a les que t'has connectat com a l'exemple següent:

### Active Flows

10 ▾	Hosts ▾	Status ▾	Direction ▾	Applications ▾	Categories ▾	IP Version ▾
Application	L4 Proto	Client	Server	Actual Thpt	Breakdown	
<a href="#">Info</a> DNS.YouTube	UDP	10.0.2.15 :37127	213.176.16	0 bit/s	Server	—
<a href="#">Info</a> DNS	UDP	10.0.2.15 :50837	213.176.16	0 bit/s	Server	—
<a href="#">Info</a> DNS.Google	UDP	10.0.2.15 :57097	213.176.16	0 bit/s	Server	—
<a href="#">Info</a> DNS.Google	UDP	10.0.2.15 :57215	213.176.16	0 bit/s	Server	—
<a href="#">Info</a> DNS.Google	UDP	10.0.2.15 :47348	213.176.16	0 bit/s	Server	—

### Exemple