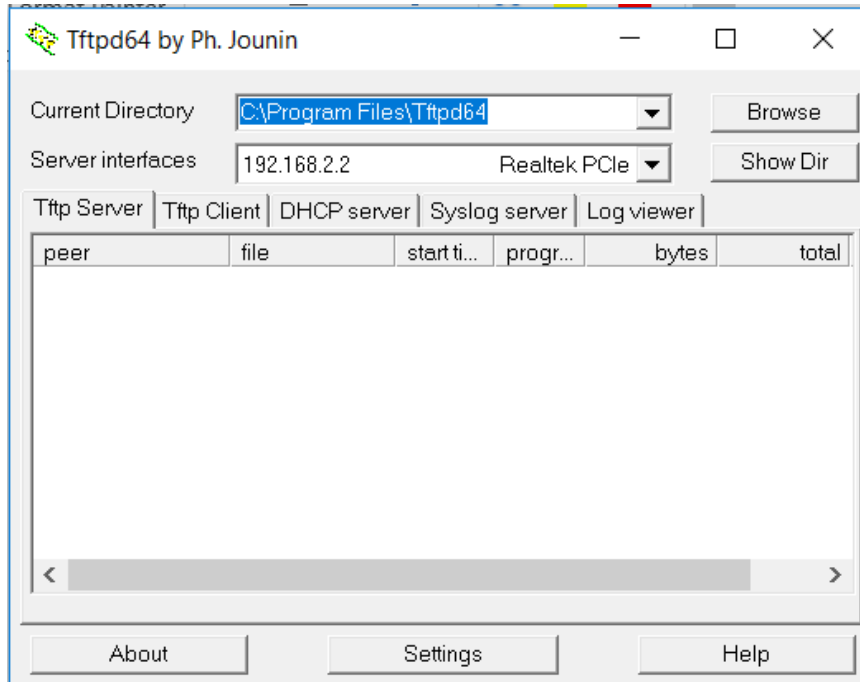


## ISHOD 4 – NADZOR MREŽE + BACKUP

Nadzor mreže nam je ključan u produkciji kako bi bili svjesni svega što se događa u našoj mreži, od ispada linka ili nekog servisa, do nadzora prometa, brzine,...te naravno sve moramo imati backupirano....za ove potrebe koristit ćemo dva alata....pa krenimo:

### 1. BACKUP + SYSLOG

Za ove potrebe koristit ćemo alat TFTPd64 (na ispitu će vas čekati instaliran)



Na routeru izvršimo par jednostavnih komandi da bi prebacili npr. Konfu iz NVRAM-a na tftp server koji je na našem Pcu:

```
Router#copy startup-config tftp:  
Address or name of remote host []? 192.168.2.2  
Destination filename [router-config]?  
!!  
2439 bytes copied in 0.060 secs (40650 bytes/sec)  
Router#
```

The screenshot shows the Tftpd64 application window. The main window title is "Tftpd64 by Ph. Jounin". The "Current Directory" is set to "C:\Program Files\Tftpd64". A "Tftpd64: directory" window is open, displaying a list of files and folders with their modification dates and sizes. The "router-config" file is highlighted in yellow, showing a size of 2439 bytes and a date of 7/11/2018. Other files listed include EUPL-EN.pdf, syslog.txt, tftpd32.chm, tftpd32.ini, tftpd64.exe, and uninstall.exe.

File Name	Modification Date	Size (bytes)
EUPL-EN.pdf	3/24/2009	34312
router-config	7/11/2018	2439
syslog.txt	7/11/2018	0
tftpd32.chm	5/5/2018	337332
tftpd32.ini	11/28/2013	1208
tftpd64.exe	5/5/2018	316928
uninstall.exe	7/11/2018	38386

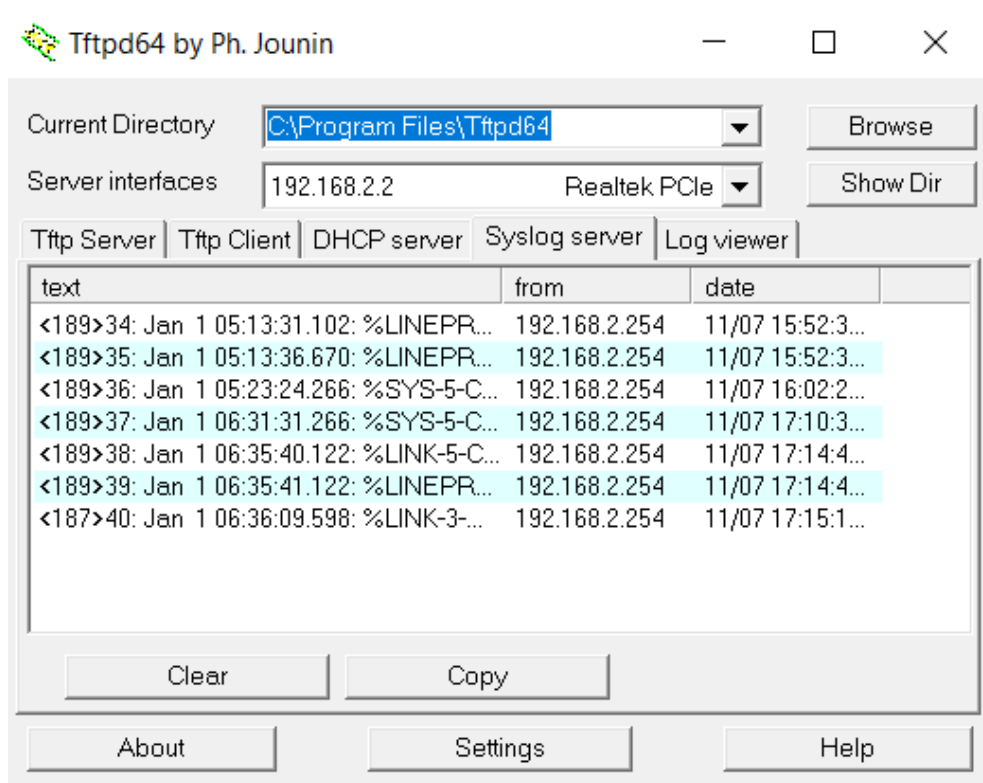
SYSLOG TRAP-ovi:

Level Keyword	Level	Description	Syslog Definition
<b>emergencies</b>	0	System unstable	LOG_EMERG
<b>alerts</b>	1	Immediate action needed	LOG_ALERT
<b>critical</b>	2	Critical conditions	LOG_CRIT
<b>errors</b>	3	Error conditions	LOG_ERR
<b>warnings</b>	4	Warning conditions	LOG_WARNING
<b>notifications</b>	5	Normal but significant condition	LOG_NOTICE
<b>informational</b>	6	Informational messages only	LOG_INFO
<b>debugging</b>	7	Debugging messages	LOG_DEBUG

Jednostavno ih konfiguriramo:

```
Router(config)#logging host 192.168.2.2
Router(config)#logg
Router(config)#logging tr
Router(config)#logging trap ?
  <0-7>          Logging severity level
  alerts         Immediate action needed          (severity=1)
  critical       Critical conditions              (severity=2)
  debugging      Debugging messages                (severity=7)
  emergencies    System is unusable                 (severity=0)
  errors         Error conditions                    (severity=3)
  informational  Informational messages                        (severity=6)
  notifications  Normal but significant conditions (severity=5)
  warnings       Warning conditions                            (severity=4)
  <cr>
Router(config)#logging trap █
```

Kada podesimo host (adresu našeg PC-a na kojem je server) i odaberemo severity level, možemo u syslog serveru vidjeti prve logove, npr. Ugasimo/uplaimo interfejs i vidmo te događaje:



## 2. NADZOR MREŽE I PROMETA PRTG ALAT

Za nadzor mrežnih uređaja i prometa (netflow) koristit ćemo besplatan i moćan alat PRTG koji je jako jednostavan za korištenje i daje nam uvid u našu mrežu, gdje možemo raditi fine tuning po svakom uređaju i interfejsu te dodavati brojne senzore koji nam pomažu u nadzoru....pa krenimo...

### 2.1. Nadzor WAN i LAN interfejsa na routeru

Postavit ćemo senzore za wan i lan interfejse koji će nam raditi stalni ping kako bi nam nadzirali dostupnost interfejsa i dodatno ćemo postaviti limite kako bi nam javljao poruke ukoliko je promet premali (npr. to nam ukazuje da nešto nije uredu s klijentima ili serverima u lan mreži jer ne proizvode promet) ili prevelik (npr. dolazi do zagušenja, netko generira prevelik promet).

Za potrebe nadzora koristimo SNMP protokol s kojim naš nadzorni alat PRTG (on je server) prikuplja podatke od klijenta (to je naš router).

Na routeru trebamo podesiti nekoliko bitinih stvari za SNMP:

## SNMP:

```
R1(config)#snmp-server community prtgRO RO
```

```
R1(config)# snmp-server community prtgRW RW
```

```
R1(config)# snmp-server trap-source FastEthernet0/0
```

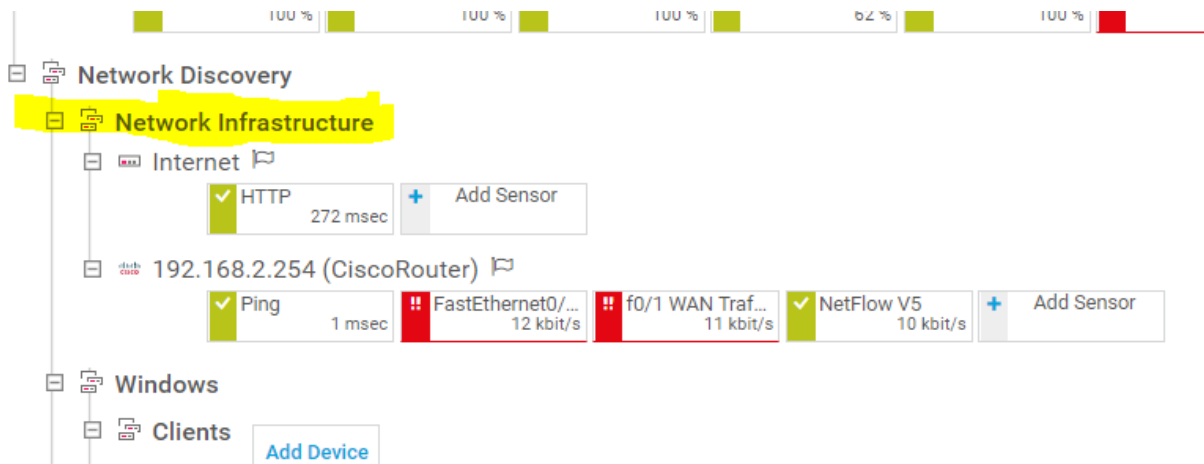
```
R1(config)#snmp-server enable traps
```

```
R1(config)# snmp-server host 192.168.1.10 version 2c prtgRO
```

Moramo postaviti community (to je naziv grupe npr prtgRO), RO znači read only, RW read write, podesimo source interface, enablamo trap-ove (trapovi su informacije koje će server tražiti od klijenta, kada upišemo enable otvaramo praktički sve) i na kraju podesimo ip adresu našeg PC-a i verziju zajedno s communityem jer ćemo te iste podatke podesiti na serveru.

A sad krenimo na server....

Desni klik na Network Infrastructure i odaberemo add device



Zatim podesimo naziv i ip adresu našeg rutera kako bi ga dodali u nadzor...

### Add Device to Group Network Discovery X

#### Device Name and Address

Device Name ⓘ  
CiscoRouter

IP Version ⓘ  
 Connect using IPv4  
 Connect using IPv6

IPv4 Address/DNS Name ⓘ  
192.168.2.254

Tags ⓘ  
+

Device Icon ⓘ


Cancel OK

Kad smo dodali router u nadzor možemo dodati senzore za WAN i LAN interfejsе kako bi nadzirali promet i kako bi dobivali poruke ukoliko se probiju limiti koje nadziremo!

192.168.2.254 (CiscoRouter)

Ping 0 msec	FastEthernet0/... 8.86 kbit/s	f0/1 WAN Traf... 8.09 kbit/s
----------------	----------------------------------	---------------------------------

Add Sensor to Device 192.168.2.254 (CiscoRouter) [192.168.2.254]

<b>Monitor What?</b> <ul style="list-style-type: none"><li><input type="radio"/> Availability/Uptime</li><li><input checked="" type="radio"/> Bandwidth/Traffic</li><li><input type="radio"/> Speed/Performance</li><li><input type="radio"/> CPU Usage</li><li><input type="radio"/> Disk Usage</li><li><input type="radio"/> Memory Usage</li><li><input type="radio"/> Hardware Parameters</li><li><input type="radio"/> Network Infrastructure</li><li><input type="radio"/> Custom Sensors</li></ul>	<b>Target System Type?</b> <ul style="list-style-type: none"><li><input type="radio"/> Windows</li><li><input type="radio"/> Linux/macOS</li><li><input type="radio"/> Virtualization OS</li><li><input type="radio"/> Storage and File Server</li><li><input type="radio"/> Email Server</li><li><input type="radio"/> Database</li><li><input type="radio"/> Cloud Services</li></ul>	<b>Technology Used?</b> <ul style="list-style-type: none"><li><input type="radio"/> Ping</li><li><input type="radio"/> SNMP</li><li><input type="radio"/> WMI</li><li><input type="radio"/> Performance Counters</li><li><input type="radio"/> HTTP</li><li><input type="radio"/> SSH</li><li><input type="radio"/> Packet Sniffing</li><li><input type="radio"/> NetFlow, sFlow, jFlow</li><li><input type="radio"/> PowerShell</li><li><input type="radio"/> Push Message Receiver</li><li><input type="radio"/> PRTG Cloud</li></ul>
---	---	---

< Cancel sensor creation

> Looking for more sensor types? See

Search  Type to search name or description

40 Matching Sensor Types

Most Used Sensor Types

<b>NetApp LIF BETA</b> Monitors logical interfaces of a NetApp cluster using SOAP <i>Needs .NET 4.5 installed on the computer</i>	<b>NetApp LUN BETA</b> Monitors the logical unit number (LUN) of a NetApp cDOT or ONTAP storage system using SOAP	<b>NetApp NIC BETA</b> Monitors the network interface controller (NIC) of a NetApp cDOT or ONTAP cluster using SOAP	<b>NetApp Volume BETA</b> Monitors volumes of a NetApp cDOT or ONTAP storage system using SOAP <i>Needs .NET 4.5 installed on the computer</i>	<b>SNMP Traffic</b> Monitors bandwidth and traffic on servers, PCs, switches, etc. using SNMP <i>Click question mark to open help</i>
---	--	--	--	---

Zatim editiramo senzore da bi postavili limite:

Group Group ★★★★★

Overview | 2 days | 30 days | 365 days | Alarms | Log | Management | **Settings** | Notifications

Status: OK | Sensors:  8  1 (of 9) | Search:

Group

192.168.1.20 (R1)	PING 4 msec	(001) FastEth... 2 kbit/s	(002) FastEth...	(003) FastEth...	(004) FastEth...	(005) Serial2/...	(006) Serial2/...	(007) Serial2/...
-------------------	-------------	---------------------------	------------------	------------------	------------------	-------------------	-------------------	-------------------

+ Add Remote Probe | + Add Group | + Add Auto-Discovery Group | + Add Device | + Add Sensor | + Add Mobile Android Probe

CREDENTIALS FOR SNMP DEVICES

inherit from  Network Infrastructure (SNMP Version: V2, SNMP Port: 161, SNMP Timeou...)

SNMP Version	<input type="radio"/> v1 <input checked="" type="radio"/> v2c <input type="radio"/> v3
Community String	<input type="text" value="prtgRO"/> <b>Default je public</b>
SNMP Port	<input type="text" value="161"/>
SNMP Timeout (Sec.)	<input type="text" value="5"/>

Settings

Channel Settings

### Select Channel

Channel

Downtime (ID -4)

Traffic Total (ID -1)

Traffic In (ID 0)

Traffic Out (ID 1)

### Edit Channel "Traffic Total"

Name ⓘ

Traffic Total

ID ⓘ

-1

Limit ⓘ

Cancel

OK



## Edit Object FastEthernet0/0 Traffic

X

### Limits

- Disable limits
- Enable alerting based on limits

### Upper Error Limit (kbit/s)

3000

### Upper Warning Limit (kbit/s)

2500

### Lower Warning Limit (kbit/s)

500

### Lower Error Limit (kbit/s)

100

### Error Limit Message

Link samo sto nije otkazao

### Warning Limit Message

Link je zagusen

### Graph Rendering

- Show in Graphs
- Hide from Graphs

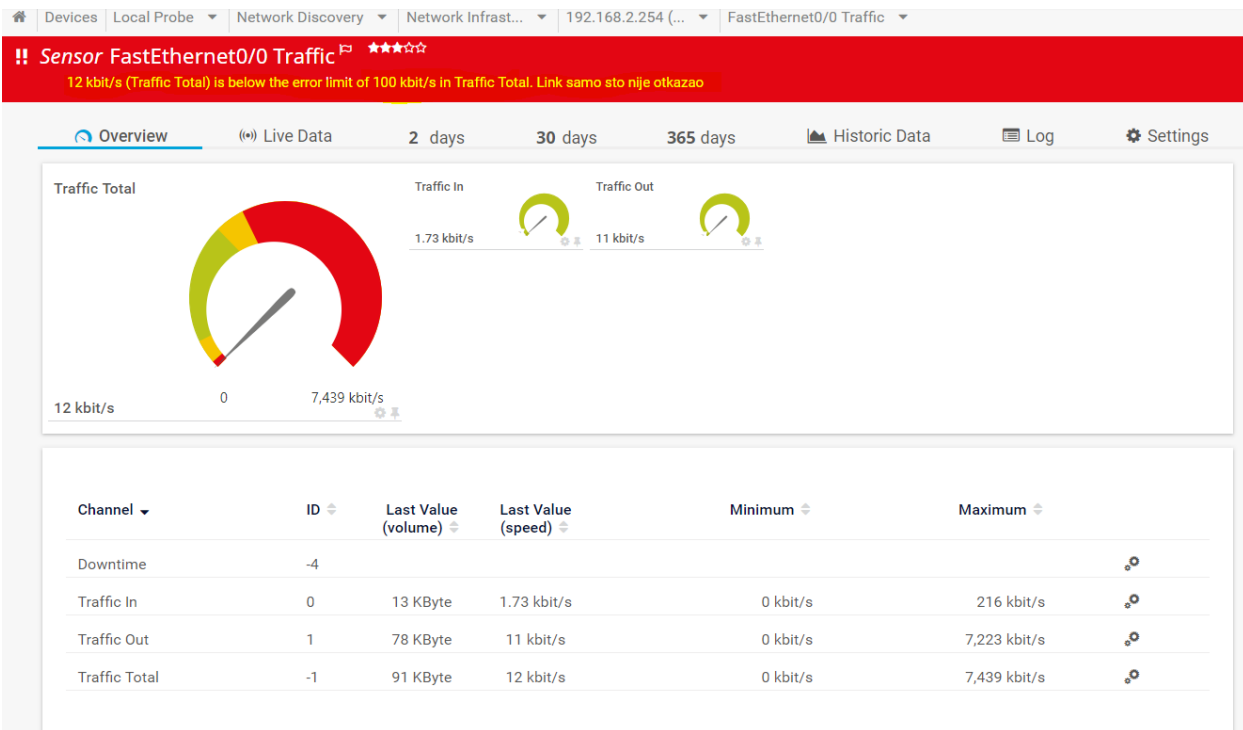
### Table Rendering

Cancel

OK

Postavite dovoljno male limite kako bi ih na ispitu lako mogli dokazati da rade!

Zatim generiramo neki promet ...ping, ili još bolje youtube kako bi generirali promet i dobili poruke od PRTG-a da smo probili limite...



Morate dobiti ovakvu poruku ako je promet premali ili ga nema!

## 2.2. NETFLOW

Također želimo imati uvid i grafove o korištenju linka, tko nam surfa, gdje i koliko...  
Za to koristimo senzor NETFLOW....pa idemo i to podesiti...

Prvo router konfamo:

```
R1(config)#int fa 0/0
R1(config-if)#ip flow ingress
R1(config-if)#ip flow egress
R1(config-if)#exi
R1(config)#ip flow-export source fa 0/0
R1(config)#ip flow-export ver 9
R1(config)#ip flow-export destination 192.168.0.22 9996
R1(config)#
```

Zatim u PRTG-u odaberemo add sensor:

The screenshot shows the PRTG Group Root interface. The left sidebar displays a tree view of the network structure. Under the '192.168.2.254 (CiscoRouter)' node, several sensors are listed, including 'Ping', 'FastEthernet0/...', 'f0/1 WAN Traf...', and 'NetFlow V5'. The 'NetFlow V5' sensor has a yellow box around its 'Add Sensor' button. The top navigation bar includes 'Overview', '2 days', '30 days', '365 days', 'Alarms', 'Log', 'Management', and 'Settings'. The bottom status bar shows the user 'PAESSLER' and the role 'PRTG System Administrator'.

U tražilicu upišete Netflow da vam nađe senzor (jer PRTG ima jako puno senzora pa je tražilica korisna) i odaberete ga te ga dalje editirate:

[Add Sensor to Device 192.168.2.254 \(CiscoRouter\) \[192.168.2.254\]](#)

The screenshot shows the 'Add Sensor to Device' dialog box in PRTG. The 'Monitor What?' section has 'Network Infrastructure' selected. The 'Target System Type?' section has 'Linux/MacOS' selected. The search bar contains 'Netflow'. The search results show 'NetFlow V5' as the selected sensor. The dialog box also includes a 'Cancel sensor creation' link and a 'Search' button.

Potrebno je podesiti ip adresu routera (LAN interfejs) i broj udp porta (stavimo bilo koji, ja sam stavio 9999, ali isti taj moramo podesiti i na routeru)

### Edit Object NetFlow V5

X

NetFlow V5

Parent Tags ⓘ

Tags ⓘ

bandwidthsensor X netflowsensor X +

Priority ⓘ

★★★★☆☆

### NetFlow V5 Specific Settings

Receive NetFlow Packets on UDP Port ⓘ

9999

Sender IP ⓘ

192.168.2.254

Receive NetFlow Packets on IP ⓘ

Cancel

OK

Overview

Live Data

2 days

30 days

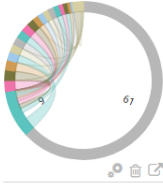
365 days

Historic Data

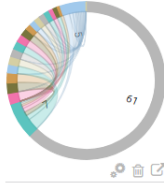
Log

Settings

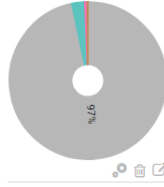
Top Talkers



Top Connections



Top Protocols



Add Toplist

Total



10 kbit/s

0

1,919 kbit/s

Infrastructure

0.26 kbit/s



0 kbit/s



NetBIOS

0 kbit/s



Other

0 kbit/s



Various

0.06 kbit/s



10 kbit/s

