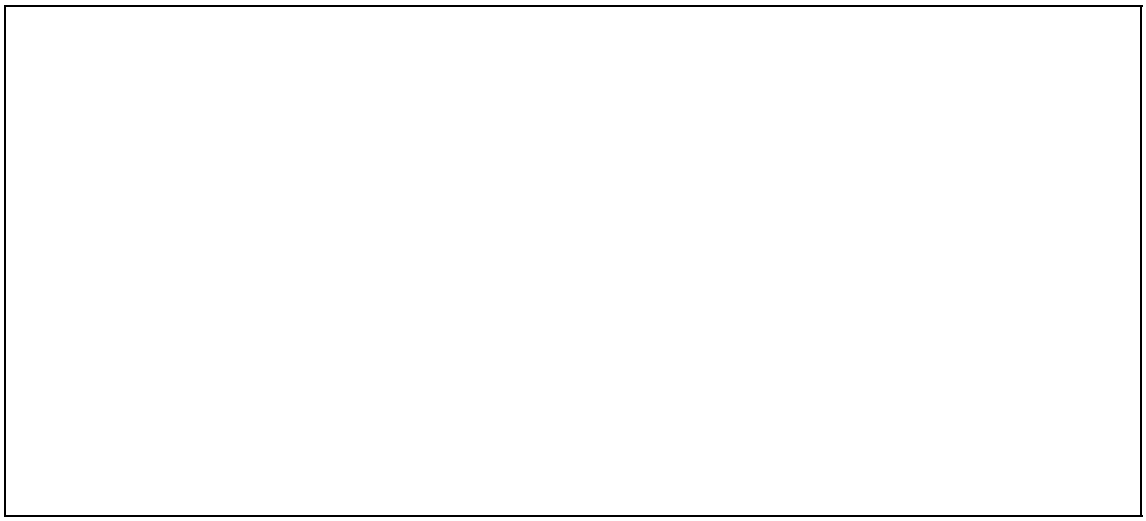
Contents

Introduction

DD-WRT include the capability of running rflow, a Cisco Netflow data exporter implementation. The netflow data is sent to a port of a computer (management server) on your LAN running a Netflow collector, in this case this is ntop.

Ntop is an open source network traffic monitoring tool that shows the network usage via a web browser. The web interface for monitoring, configuration and administration make ntop easy to use and suitable for monitoring various kind of networks.



Router Setup

My router is running the DD-WRT v24-sp2 firmware (you need a version with rflow support).
Rflow can monitor the available interfaces of the router, in my case these are br0 (Lan & Wlan), vlan0, eth1, Wlan0 and WAN.

Log into your router through your browser, than go to the *Services* | *Services* where you will find the *RFlow / MACupd section.*

RFlow: select "Enable"

Server IP: The IP address of your computer that wil run ntop.
This computer must have a static IP address, or using a DHCP static lease.

Port: The UDP port that will be used to send the netflow information.
Common default ports for Netflow are 2055 and 9996. In my first setup I used port 2055 but because this port was used by other applications I had to change to 9996 to make my installation stable.

Interface: LAN&WLAN

Then click *"Apply Settings"*

Setup ntop management server

Ntop will run on many operating systems. The ntop Web site offers multiple versions (sources and binaries) of the package for download. The free binary version for Windows is limited to capturing only the first 2000 packets. This limitation does not exist in the Linux versions and the paid Windows version. I use the free unlimited version **ntop for win32 v3.2 from OPENXTRA.** You can find the easy to install OPENXTRA version on several places on the Internet like here [1]

To run **ntop for win32** I use an old Windows XP laptop (320MB RAM) as terminal-, web-, file-, print- and scanner server in my network and this laptop proofs to have enough resources to do this additional job.

After the installation is finished, you should have a new icon in the system tray called OPENXTRA Commander. Double-click this icon to open the OPENXTRA Commander. If the NTop Service plug-in is not started, click Start in the Action column to start it. Once it is started, click the Launch action for the NTop plug-in, which will open your browser (http://localhost:3000). If all is well, you will already be collecting some impressive data. In the Windows *Control panel* | *Administrative Tools* | *Services* you can check if the ntop service is running. Optional you can configure the service to restart automatic after a failure.

Rfow configuration

You have to create a virtual rflow interface. Do this by selecting *Plugins* | *All* in the menu listing at the top of the webpage.

In the *Active* column click on *"NO"* next to NetFlow to enable the plugin.

Click on *"NetFlow"* in the *Configure* column.
Click on *"Add NetFlow Device".*

NetFlow Device Name: Any name you like, I choose DD-WRT.
Click on "Set Interface Name".

Local UDP Collector Port: Use the same port as configured in the router (I used 9996).
Click on "Set Port".

Virtual Netflow Interface Network Address: Your LAN network address and its netmask.
If your router is using 192.168.1.1, then this should be: 192.168.1.0/255.255.255.0. Ntop uses this address to recognize the local hosts from the remote hosts.
Click on "Set Interface".

Leave everything else now to defaults.

Now we have two interfaces ntop can monitor, the NIC of the local computer and the Netflow interface. We now can switch which interface we wish to monitor.
In the menu at the top select *Admin | Switch NIC.*
Under *Available Network Interface* select the NetFlow Device name you entered earlier (DD-WRT in my case).
Then click on *Switch to NIC.*

You will notice that some menu entries have a small padlock icon in them; these are the Web pages that require a password to access. The default credentials for the XTRA package is user = admin, password = admin.

You can take a first view of the web pages of ntop.

Rrd configuration

ntop stores all of its active data in RAM, so if the system is reset, you lose all your data. Archiving of this data to disk must be configured. Ntop is using rrd to prevent that your disk fills up. RRD uses a round robin database which stores time-series data in a very compact way so that it will not expand over time. You have to configure what data with what detail must be archived and with what retention time.

Do this by selecting *Plugins | All* in the menu listing at the top of the webpage.

In the *Active* column click on *"NO"* next to rrdPlugin to enable the plugin.

Then click on *"rrdPlugin"* in the *Configure* column to show the RRD Preferences.
I let the first 6 items (interval to delay) unchanged.

Data to dump: Hosts and Interfaces

Hosts Filter: I choose to only archive data of local hosts with my LAN address 192.168.1.0/255.255.255.0

RRD detail: I choose medium
RRD Files Path: This is the location where rrd stores his data: \NTopWin32\rrd.

Ports

ntop will tell you on different pages which ports are used. In the Windows version you will find the file "services" (without extension) in the directory C:\Program Files\OPENXTRA\NTopWin32.
The structure of the file is

```
port             port             alias            # description
name           number/tcp

like this:

pop2               109/tcp            pop-2             # Post Office Protocol - V2
pop3               110/tcp            pop-3             # Post Office Protocol - Version 3
sunrpc          111/udp       rpcbind


You can add portnames to this file if you want ntop to show a portname in stead of a port number.
I have added the follwing ports:

#
# Extra services
#
ssh                22/tcp
ms-sql-s       1433/tcp
ms-sql-s       1433/udp
ms-sql-m      1434/tcp
ms-sql-m      1434/udp
upnp               1780/tcp
upnp               1780/udp
ssdp               1900/udp
ntop               3000/tcp
rdp                3389/tcp
rdp                3389/udp
atq                3456/udp
nat-t              4500/udp
remotescan   6077/tcp
remotescan   6078/udp
netflow         9996/udp
dropbox       17500/tcp
dropbox       17500/udp
```

Stop and start the ntop service for the changes to take effect.

Protocols

There is a default list of protocols ntop will monitor for you, if you want you can define a smaller list of protocols or you can add protocols to the list. To do this you have to create a protocol.list in the directory C:\Program Files\OPENXTRA\NTopWin32. The ntop web page will display the protocols in the same order as they are defined in the list, you can change the order if you like.

The structure of the file is protocolname=port, where port is a portname that you can find in the file services or a portnumber.
Behind the = you can define multiple ports with port|port| or with 12-20.
In the following file I have first defined the default values and added some extra protocols.

```
## Default ntop protocollist ##
FTP=ftp|ftp-data|69
HTTP=http|www|https|3128
DNS=name|domain
Telnet=telnet|login
NBios-IP=netbios-ns|netbios-dgm|netbios-ssn
Mail=pop-2|pop-3|pop3|kpop|smtp|imap|imap2
DHCP-BOOTP=67-68
SNMP=snmp|snmp-trap
NNTP=nntp
NFS/AFS=mount|pcnfs|bwnfs|nfsd|nfs|nfsd-status|7000-7009
VoIP=5060|2000|54045
X11=6000-6010
SSH=22

## Default ntop Peer-to-Peer protocols ##
Gnutella=6346|6347|6348
Kazaa=1214
WinMX=6699|7730
DC++=-1
eDonkey=4661-4665
BitTorrent=6881-6999|6969

## Default ntop Messenger protocols ##
Messenger=1503|1863|5000|5001|5190-5193

## Extra ntop protocols ##
Comodo=1037-1045|1280|4447-4448
Avast=1281-1282
NetFlow=9996
UPnP=1780|1900
Dropbox=17500
Ntop=3000
Remotescan=6077|6078
RDP=3389
Streaming=554|1755|1935|3689|4070|5222|7070
Nat-t=4500
IIS=1025|3456
SQL=1433
LDAP=ldap|ldaps
RPC=111
SLP=427
LPR=515|631
```

After you have created the file you have to configure ntop to use this file. Select in the menu listing at the top of the webpage *Admin* | *Configure* | *Startup Options* and select the *IP Preferences* link. In the field *TCP/UDP Protocols To Monitor (-p)* specify C:\Program Files\OPENXTRA\NTopWin32\protocols.list (must be the full path). See ntop internal help for more information. Stop and start the ntop service for the changes to take effect.

Usage

In the Ntop Bandwidth Monitoring Guide you can find some interesting usage scenario's, like:

- Who are the top internet bandwidth users on my network?
- What websites do the top bandwidth users visit?
- What websites get the most traffic from within my organization?
- What websites' traffic consumes most of my bandwidth?
- What applications are being used?
- Which local hosts share the most data?
- At what time of the day is the network most Utilized?
- Performing a network inventory
- Exporting traffic data
- Detecting network security violations?

Suppose you identify a particular host as the major consumer of bandwidth, what if you want to find out just what exactly he is doing online that is consuming so much bandwidth? Here is how ntop can help:

1. Identify the host you are interested in [one way is to sort on the Data for Network Traffic stats for local hosts.
2. Click on that host to bring up the Info about xxxxx page where xxxx is the name or IP address of the host you are interested in.
3. Scroll down to the bottom of the page to the Active TCP/UDP Sessions table. A screen is shown which "lays it all out for you".

Host Fingerprints
You can switch the interface you want to monitor. You should remember when you use the NetFlow interface that NetFlow does not send you the actual packages like the local NIC interface. This is why ntop cannot report fingerprints when the Netflow interface is used. You can find Host Fingerprints in the menu *IP* | *Local* | *Host Fingerprints*.

Local Matrix
In the menu *IP* | *Local* | *Local Matrix* you will, when using the NetFlow interface, see no traffic between local hosts. This is caused by the default behaviour of a switch that is used to connect your local hosts to the router. Only the traffice between local hosts and remote hosts is captured.

Historical data
Historical data can be viewed with ntop (or other tools) by clicking on the icon  on webpages like Info about Host and Plugin | Round Robin Databases | Arbitrary Graphs.

Dumping Ntop Data
There are scripts to dump data in a MySQL database on sourceforge.net. However, within ntop, just click *Utils|Data Dump* to show a dialog box. You can dump data about different objects into different formats ? see the ntop guide for the formats. Some of these formats are importable into a spreedsheet and from there you can unleash the full power of Open Office Calc or Excel unto your traffic data.

Workarounds

In this version of ntop there are a few small annoyances to work around.

Hostname resolving
PC's in my network are not always on, I found when ntop starts he resolves the hostnames of al host in the network, but after some time when these PC's switch off and on ntop forget the hostname. For me it was no problem to restart the ntop service with a bat file every night with a scheduled task of Windows. The bat file look like this

```
@echo off
REM - File: Daily Restart ntop for win32.bat
REM - Description: Restart ntop for Win32 Service tbv name resolving
REM - Author: Jan S
echo Restarting ntop for Win32...
echo ====================================================
net stop "ntop for Win32"
net start "ntop for Win32"
echo ====================================================
echo ntop for Win32 Restarted
```

Broken links
On several pages links are used to services on the Internet for additional information. There are links to WHOIS information and there is a link voor ASN information.
There are several ways to solve this problem, because I use Firefox the easiest way for me was url rewriting in the browser, you can use the Firefox Add-On Redirector to do that.

WHOIS was `http://www.radb.net/cgi-bin/radb/whois.cgi?obj=*`
can be rewritten to `http://whois.domaintools.com/$1` or `http://www.lookip.net/$1` or any other you like.

ASN was `http://ws.arin.net/cgi-bin/whois.pl?queryinput=*`
ca be rewritten to `https://apps.db.ripe.net/search/query.htm?searchtext=$1`

FAQ, in the menu *About* there is a link to FAQ but the faq.html file is not local available. You can copy the file from `www.ntopsupport.com/faq.html` to C:\OPENXTRA\NTopWin32\html\faq.html.
There is a lot of important information available here.

Finally

The combination of a DD-WRT router running rflow and a PC running ntop provides a low cost solution for remote network traffic usage and activity (NetFlow monitoring). Rflow provides fast packet capture and also captures packets efficiently thus preserving CPU cycles. With ntop Luca Deri has created a brilliant tool for seeing what is happening on your network in realtime. This is only a basic tutorial to show what you can do with DD-WRT and rflow. ntop has many more possibilities, out of the box via configuration and via extra scripts which are available in the directory C:\OPENXTRA\NTopWin32\www and on the Internet.
There is a new version 5 available for Windows with many more possibilities, it's worth looking at it.

External Links

- Configuring Ntop to work with the DD-WRT firmware for the Linksys WRT54G(S) router
- Configuring ntop
- Ntop Netflow with a WRT54GS Firewall/Router and NST Probe
- RFlow Collector and MySQL
- Ntop, persistent data and rrd
- Ntop Bandwidth Monitoring Guide
- Ntop Users Guide
- Ntop Tutorial Slides