

Configuring Ntop to work with the DD-WRT firmware for the Linksys WRT54G(S) routers

Introduction

Ntop is an open-source network traffic monitoring tool. When used with a router that supports reporting traffic in Rflow format it allows you to get detailed information on what traffic goes through your router. The DD-WRT firmware supports Rflow.

Router setup

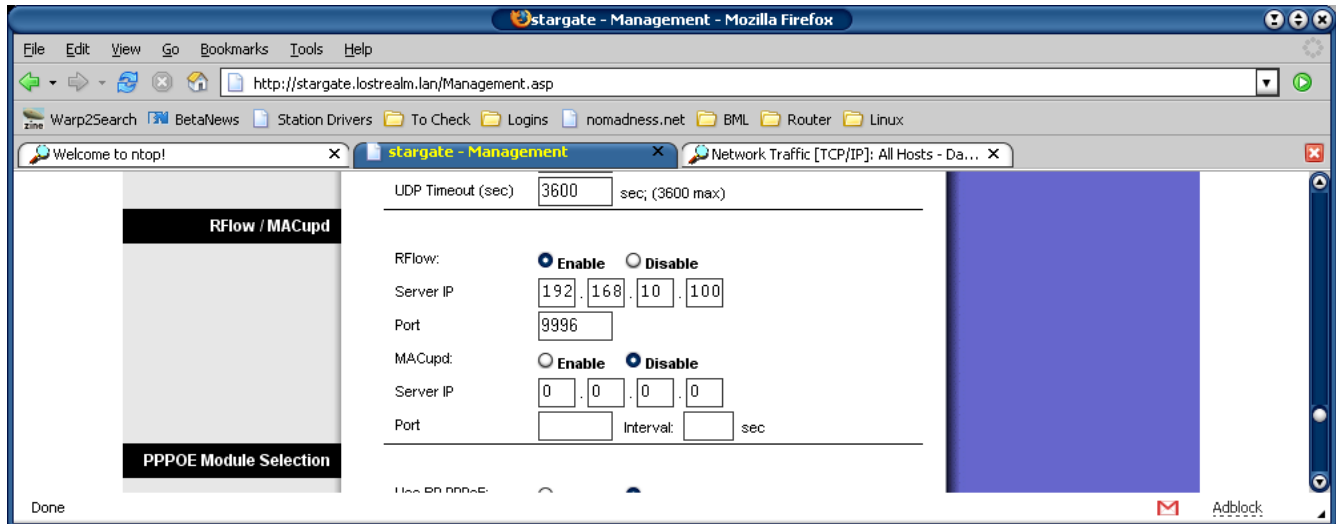
I assume you already have a router running the DD-WRT 22 Pre4 firmware (or any other with Rflow support).

Log into your router through your web browser, then go to the “*Administration*” page. Scroll down to the *Rflow / MACupd* paragraph.

Rflow: Select “Enable”

Server IP: The IP of the machine that will run Ntop. Best to make sure that machine is using a static IP, or using a DHCP Static Lease (can also be configured on that same page of the router configuration).

Port: The UDP port that will be used to send the traffic information. I used 9996 here (this was the same port used in the original example I based my setup on).



Then click on “*Save Settings*” at the bottom of the page.

Ntop

Get Ntop from this website and install it:

<http://www.openxtra.co.uk/products/ntop-xtra.php>

Once Ntop is installed, make sure the service is running (*Control Panel -> Administrative Tools -> Services*). If you can't see Ntop in the list of services, then open a command prompt, change directory to the folder containing Ntop (default is *C:\Program Files\OPENXTRA\NTopWin32*) and issue “ntop /i” to install the service.

To configure Ntop, open your web browser, and go to <http://localhost:3000>. If you get an error then it's probably because the Ntop service isn't running.

Rflow Plugin configuration:

You have to create a virtual Rflow interface. In Ntop go to “*Admin -> Plugins*”. In the active column click on “NO” next to NetFlow to enable that plugin.

Available Plugins

View	Configure	Description	Version	Author	Active [click to toggle]
	rrdPlugin	This plugin is used to setup, activate and deactivate ntop's rrd support. This plugin also produces the graphs of rrd data, available via a link from the various 'Info about host xxxxx' reports.	2.6	L.Deri	Yes
	NetFlow	This plugin is used to setup, activate and deactivate NetFlow support. ntop can both collect and receive NetFlow V1/V5/V7/V9 and IPFIX data. Received flow data is reported as a separate 'NIC' in the regular ntop reports. Remember to <i>switch</i> the reporting NIC.	3.99	L.Deri	Yes
	sFlow	This plugin is used to setup, activate and deactivate ntop's sFlow support. ntop can both collect and receive sFlow data. Note that ntop.org is a member of the sFlow consortium. Received flow data is reported as a separate 'NIC' in the regular ntop reports. Remember to <i>switch</i> the reporting NIC.	2.99	L.Deri	No
	icmpWatch	This plugin produces a report about the ICMP packets that ntop has seen. The report includes each host, byte and per-type counts (sent/received).	2.4	L.Deri	No

Report created on Fri Apr 22 23:15:24 2005 [ntop uptime: 13:01]
 Generated by ntop v.3.1 MT [WinNT/2K/XP]
 Build: Feb 2005. Version: the CURRENT stable version
 Listening on [ASUSTeK_Broadcom 440x 10_100 Integrated Controller_0,Stargate] without a kernel (libpcap) filtering expression
 Web report active on interface Stargate
 © 1998-2004 by Luca Deri

/showPlugins.html

Then, click on “Netflow” in the Configure column to setup the NetFlow plugin.

Click on “Add Netflow Device”. Here are the parameters that need to be set:

Netflow Device Name: Any name you want. LinksysRouter for example. Click on “Set Interface Name”.

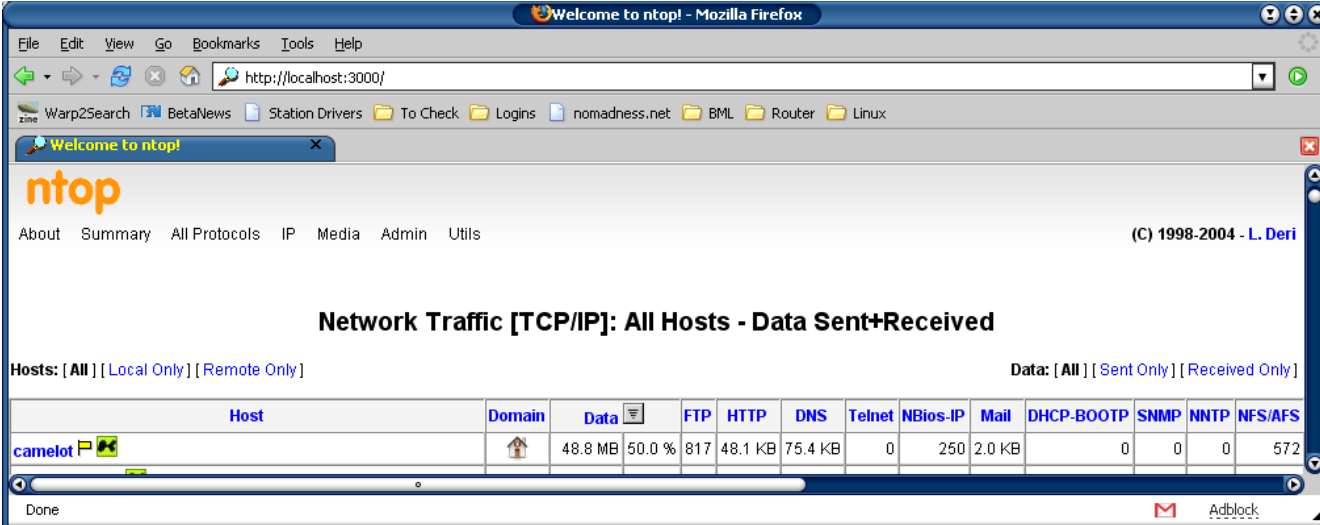
Local UDP Collector Port: Use the same port as configured in the router (I used 9996 here). Click on “Set Port”

Virtual NetFlow Interface Network Address: Your network address and its netmask. If your router is using IP 192.168.1.1, then this should be: *192.168.1.0/255.255.255.0*. Click on “Set Interface Address”.

Leave everything else to the defaults.

Now that we have defined our NetFlow interface, we need to tell Ntop this is the 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 (*LinksysRouter* in our example). Then click on **Switch to NIC**.

All done! After a minute or two select “IP -> Summary -> Traffic” in the menu. You should see a list of hosts that connected with you, as well as the amount and type of traffic that occurred between you and the hosts.



ntop

About Summary All Protocols IP Media Admin Utils (C) 1998-2004 - L. Deri

Network Traffic [TCP/IP]: All Hosts - Data Sent+Received

Hosts: [All] [Local Only] [Remote Only] Data: [All] [Sent Only] [Received Only]

Host	Domain	Data	FTP	HTTP	DNS	Telnet	NBios-IP	Mail	DHCP-BOOTP	SNMP	NNTP	NFS/AFS
camelot		48.8 MB 50.0 %	817	48.1 KB	75.4 KB	0	250	2.0 KB	0	0	0	572

Documentation written by Eric Sauvageau

Revision 0.1/23-April-2005