Netml-ns3-click: Modeling of Routers in Netml/ns3 by means of the Click Modular Router

R.G. Addie, Joshua Pravin Raj Natarajan
School of Agricultural, Computational and Environmental Studies
University of Southern Queensland
Email: ron.addie@usq.edu.au, JoshuaPravinRaj.Natarajan@usq.edu.au

***Abstract*—In this paper the design, development and use of a facility to run ns3 simulations, including Click routers, of networks constructed by the Netml system for analysis and design of networks in the cloud is described. The Netml system enables an XML description of a network to be converted into an ns3 program, and then runs this simulation, collecting and plotting the results, in a freely available public server at `netml.org`. A basic implementation of IPtables is also implemented. Users are able to specify any number of filtering rules within the forwarding chain of the filter table. This facility is implemented by generating a Click script from the rules.**

***Keywords*—Simulation, traffic, ns3, Click, IPtables.**

I. Introduction

The ns3 system [1] provides accurate and fast simulation of communication systems, with emphasis on the TCP/IP protocols. The ns3 system does not include its own native model of routers or router protocols, but instead has the capacity to model routers using the Click modular router system [2], [3], or to use other router implementations, including commercial software, by means of *emulation*, including interfacing with software running on virtual machines.

The Netml system was developed at the University of Southern Queensland for teaching and research of network protocols and technology [4]. Its objective is to enable students and users from industry to create networks easily, and to understand the full complexity of a multilayer network easily by means of highly configurable visualisation tools.

An example network, including a firewall, is shown in Figure 1. This example can be viewed and further investigated at http://netml.org. The circular nodes in this diagram are generic Netml/ns3 hosts; the rectangular node in the middle is a firewall modelled by means of IP Tables [5]; the thin lines with two directional arrow heads are point-to-point ethernet links the thick semi-transparent lines with one arrowhead are traffic, which in this instance is a mixture of on-off traffic,

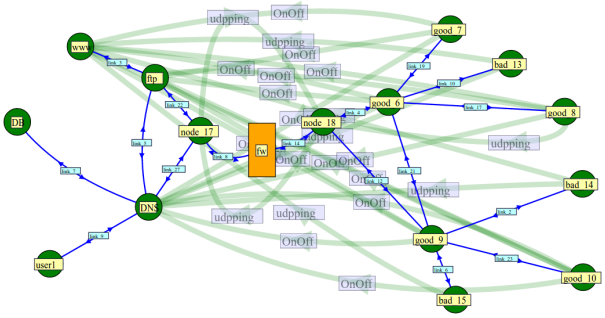

Fig. 1. An Example network with a firewall router

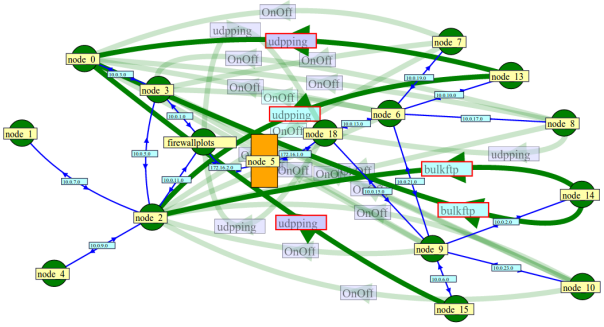

Fig. 2. The bad traffic (highlighted) to be blocked by the firewall

deterministically spaced UDP packets, and long-running ftp flows.

The firewall in this example is implemented by a subset of the IPTables system, implemented by means Click. There are five rules. The objective of these rules is to block the traffic which is shown hightlighted in Figure 2. When the firewall is turned off, traffic from all sources compete equally to gain access to the network on the other side of the firewall. A plot of selected traffic flows in this case is shown in Figure 3. A plot of the same traffic flows when the firewall is active is shown in Figure 4.

II. Features of Netml-ns3-Click

The Netml system enables users to easily create and edit complex networks through its graphical user interface which operates in a browser (not including Internet Explorer). It is not designed to create *pictures* of networks, but instead should be viewed as a visual editor of the network logic. For example, in Netml nodes do not have a characteristic icon which displays the identity and type of the device. Instead, the shape, colour, label, and title of each node, link, or traffic flow in the network can be configured, by the user, to display

SIMUTOOLS 2015, August 24-26, Athens, Greece

DOI 10.4108/eai.24-8-2015.2260965

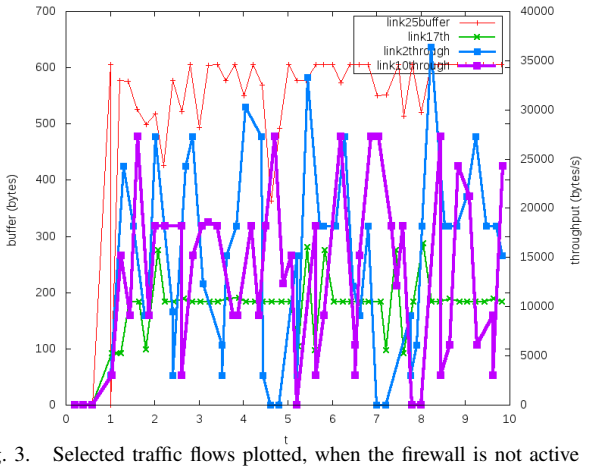

Fig. 3. Selected traffic flows plotted, when the firewall is not active

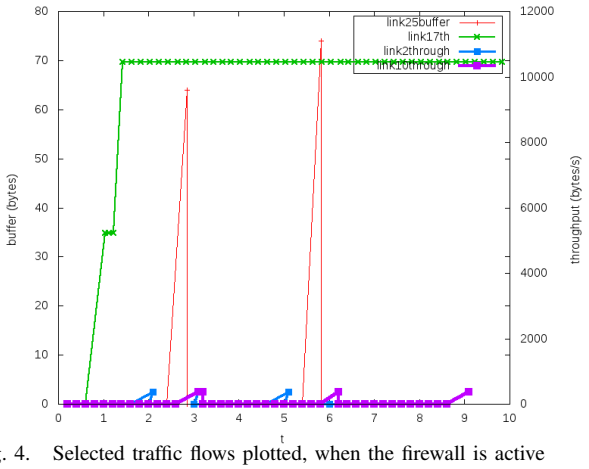

Fig. 4. Selected traffic flows plotted, when the firewall is active

any logical characteristic of that device. This is confusing for users who interpret the editor as a conventional editor of diagrams, but is very powerful for displaying and developing an understanding of the logic of networks.

IPTables [5] is a Linux system for configuring a Unix system as a firewall. It is widely used for implementation of network firewalls.

The functions of a router are a superset of those of a firewall. However, it is common practice in private networks to nominate a specific system with minimal routing role, at the interface between the private network and the Internet, as a firewall. The most characteristic feature of a firewall is packet filtering. However, it is common for a firewall to implement some packet transformations other than filtering.

IPTables is suitable for configuring a machine with this role. In IPTables, rules which match or manipulate individual packets may be specified, and these rules are then assembled in a sequence called a *chain*. Chains, in turn, are associated with tables.

The Netml user interface allows for an arbitrary number of rules, which are linked in sequence, to be placed in chains, which are in turn placed in tables. However, at present, the only table considered is the Filter table, and the only chain in this table which is considered is the forwarding chain. The rules in this chain are used to define an IPFilter element of a Click router, the other elemenets of which ensure that the

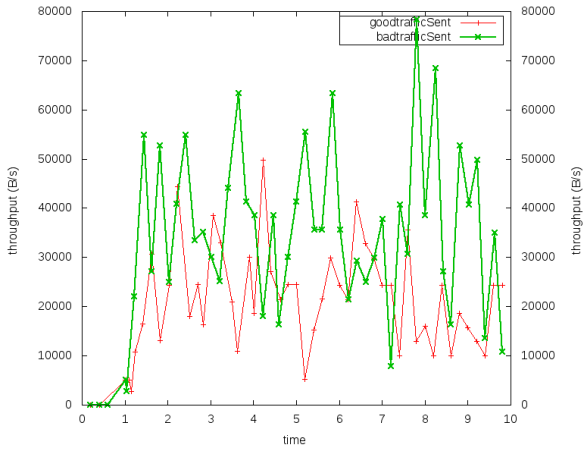

Fig. 5. Aggregate good traffic and aggregate bad traffic, as measured at the sources, when the firewall is not active

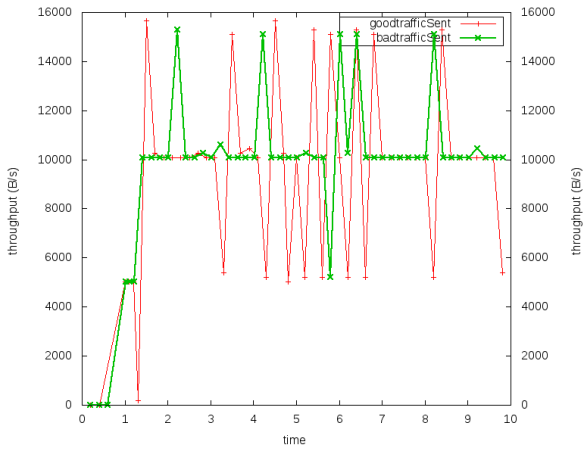

Fig. 6. Aggregate good traffic and aggregate bad traffic, as measured at the sources, when the firewall is active

basic functions of reeceiving, filtering, and forwarding packets are carried out.

As in the rest of the Netml system the graphical user interface is designed to enable users to specify and manage the plots they wish to produce as efficiently and expressibly as possible. This is achieved by subdividing the task into two parts: (i) definition of traced quantities; (ii) plotting of one or more traced quantities on a single plot. Trace dialogs and plot dialogs allow users to readily specify the details that they wish to gather and plot. The range of traceable quantities is very large, and traceable quantities can readily be combined together.

As well as enabling any ns3 traceable quantity to be easily plotted, the Netml-ns3-Click system allows multiple traces to be easily aggregated together, before plotting. For example, Figure 5 shows the aggregation of the traffic sent by the "good" nodes, in the example discussed above, when the firewall is not active, and Figure 6 shows the result when the firewall is in place. This provides a different test of the effectiveness of the firewall than the result shown previously. Note that since quite a bit of the traffic in this scenario is not TCP based, the firewall does not dramatically reduce the amount of traffic *sent* into the network.

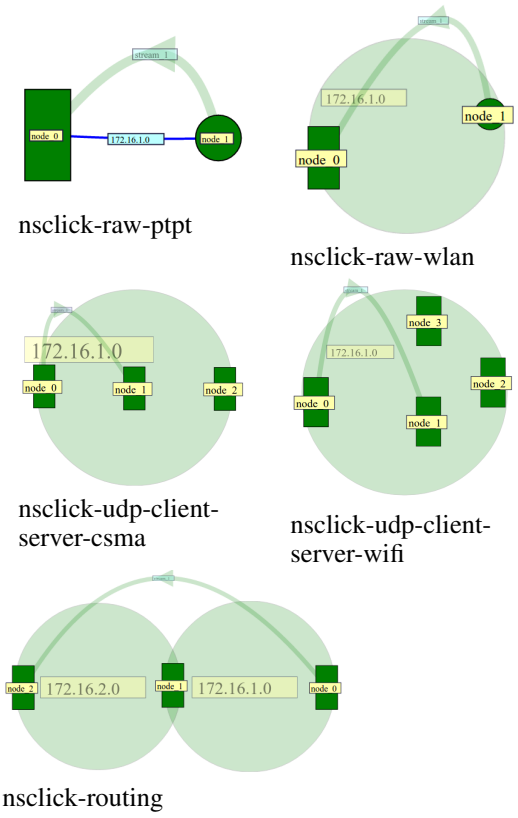

Fig. 7. The five Click Examples provided with the ns-click distribution.

The collection and aggregation of statistics from a collection of nodes, links, or traffic streams is achieved in Netml by defining an *abstract* node, link, or traffic stream. These are a little like *sets* of network elements. A variety of actions, when applied to an abstract network element, are passed on to the members rather than being applied to the abstract element. This is another example of how a graphical user interface can make the manipulation and analysis of networks easier and more effective. The network shown in Figures 1 and 2 include abstract links and nodes, which are not shown in these figures. This network can be viewed in full, in a browser (other than Internet Explorer) at http://netml.org/netml4_5/index.jsp?netname=fwtest16_4Filter&location=Demo or http://netml.org/netml4_5/index.jsp?netname=fwtest16_4NoFilter&location=Demo.

III. Design and Implementation

The ns-3 program and all the Click scripts used by any Click routers in the simulation are generated from the `Netml` by transformations written using the XSLT style sheet language [6]. Click scripts for routers may be included verbatim as an attribute of a router or, alternatively, by a graphical representation which is translated into The ns-click distribution includes 5 examples, as illustrated in Figure 7. These examples can be viewed and tried at http://netml.org/netml4_5/index.jsp?netname=nsclick-routing?location=Demo, etc. a click script.

A firewall in the Netml system is specified by constucting a special type of network which represents the rules of the firewall. This network is modeled on the `IPTables` system, and hence the nodes in a firewall representation are of three kinds: IPTables, IPChains, or IPRules. An example of such a firewall specification is shown in Figure 8. An example of an IPRule is shown in Figure 9.

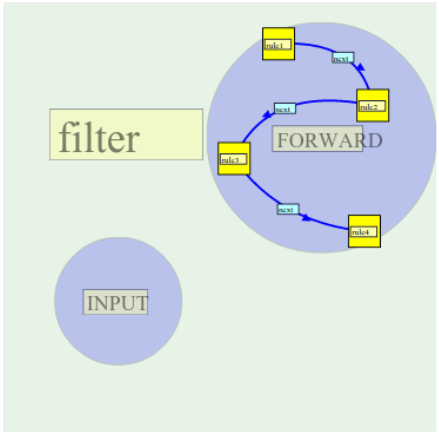

Fig. 8. An Example firewall router, graphically represented (the square represents an IP Table, the circles are IP Chains, and the linked rectangles are IP Rules)

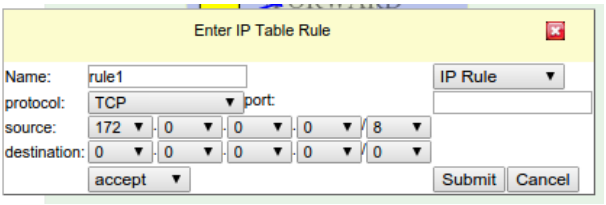

Fig. 9. An Example firewall rule, presented as a Netml form

IV. Conclusion

The simulator ns3 is a powerful tool for accurately modeling and developing an understanding of TCP/IP networks. The Netml systaem provides a graphical cloud-based tool for preparing networks, generating simulation programs, collecting data, and preparing graphical output. A graphical approach to specification of examples and visualisation of their analysis is ideal for networks because they are naturally represented as graphs, and the complex nature of networks and their operation creates a need for a tool which makes all the processes associated with network analysis and design as efficient and flexible as possible.

References

[1] GeorgeF. Riley and ThomasR. Henderson, "The ns-3 network simulator," in *Modeling and Tools for Network Simulation*, Klaus Wehrle, Mesut Gne, and James Gross, Eds., pp. 15–34. Springer Berlin Heidelberg, 2010.

[2] Eddie Kohler, *The Click Modular Router*, Ph.D. thesis, Massachusetts Institute of Technology, 2001.

[3] Lalith Suresh P. and Ruben Merz, "Ns-3-click: Click modular router integration for ns-3," in *Wns3*, 2011.

[4] Ronald G Addie, Yu Peng, and Moshe Zukerman, "Netml: networking networks," in *Dependable, Autonomic and Secure Computing (DASC), 2011 IEEE Ninth International Conference on*. IEEE, 2011, pp. 1055–1060.

[5] Oskar Andreasson, "Iptables Tutorial," *Available from World Wide Web: http://iptables-tutorial. frozentux. net/index. html*, 2002.

[6] James Clark et al., "Xsl transformations (xslt)," *World Wide Web Consortium (W3C). URL http://www. w3. org/TR/xslt*, 1999.