Computer Networks (ICT2223)
Lab Session 03 - Report

W.M.P.N. Jayaweera
TG/2018/392
Department of ICT
Faculty of Technology
University of Ruhuna

Table of Contents

Network Simulators

1. GNS3 – Graphical Network System 3

Graphical Network Simulator-3 (shortened to GNS3) is a network software emulator first released in 2008. It allows the combination of virtual and real devices, used to simulate complex networks. It uses Dynamips emulation software to simulate Cisco IOS.

GNS3 is used by many large companies including Exxon, Walmart, AT&T and NASA, and is also popular for preparation of network professional certification exams. As of 2015, the software has been downloaded 11 million times.

2. Cisco Packet Tracer

Cisco Packet Tracer is a cross-platform visual simulation tool designed by Cisco Systems that allows users to create network topologies and imitate modern computer networks. The software allows users to simulate the configuration of Cisco routers and switches using a simulated command line interface.

Cisco Packet Tracer makes use of a drag and drop user interface, allowing users to add and remove simulated network devices as they see fit. The software is mainly focused towards Certified Cisco Network Associate Academy students as an educational tool for helping them learn fundamental CCNA concepts. Previously students enrolled in a CCNA Academy program could freely download and use the tool free of charge for educational use.

3. EVE-Emulated Virtual Environment

VE is an excellent Network Virtual Environment Tool & Software created by EVE-NG Ltd. It is one of the favorite Emulated Virtual Environment For Network, Security and DevOps Professionals. Using EVE, you can emulate almost every kind of Network or Security Appliance and build, plan, configure, and test your complex network scenarios in a completely risk-free virtual environment.

4. Boson NetSim Network Simulator

NetSim is an excellent solution for preparing for CCNA, ENCOR, and ENARSI exams. Each subscription of NetSim covers 1 exam in its respective category as well, so you don’t need to dedicate money to it separately.

The core of NetSim is the Network Designer – a tool that allows you to create intuitive topologies with ease. Among the things that the Network Designer lets you do is aligning elements, annotating topologies, and easily identifying active or inactive connections.

NetSim allows you to share your own labs, lab packs, and network topologies with others as well. Likewise, you may view labs and topologies of other NetSim users, which may give you an edge in education.

5. Common Open Research Emulator (CORE)

Common Open Research Emulator, or CORE, has been originally developed by a Network Technology research group at Boeing Research and Technology. Now, the U.S. Naval Research Laboratory is supporting the further development of CORE.

As an open-source network simulation solution, CORE is highly customizable. Maintained by the U.S. Navy, it's reliable and frequently updated as well. CORE is efficient and scalable too, and it also allows you to run real-time connections to live networks.

6. Integrated Multiprotocol Network Emulator/Simulator (IMUNES)

IMUNES is based on the Linux and FreeBSD kernel. The kernel has been divided into smaller virtual nodes that can be connected with each other to form complex network topologies.

This tool may simulate or emulate IP networks at gigabit speeds in real time, with hundreds and thousands of nodes running on a single physical machine. INUMES is scalable as well, allowing you to perform large-scale experiments.

Completely open-source and free, IMUNES is remarkably customizable too. And what's also notable is that IMUNES is currently used for general-purpose network testing at Ericsson Nikola Tesla and learning at the University of Zagreb.

Packet Analyzers (Sniffers)

1. SolarWinds Deep Packet Inspection and Analysis Tool

SolarWinds Network Packet Sniffer provides the information of the application or the network whether it is affecting the end-user experience or not. It comes with the SolarWinds Network Performance Monitor (NPM). SolarWinds NPM will provide you an at-a-glance overview of real performance stats based on packet-level data through a dashboard.
This helps with pinpointing problematic traffic. It performs a deep packet inspection.

SolarWinds Network Packet Sniffer has a WiFi packet capture tool. It can differentiate normal traffic from abnormal traffic and provides detailed data and transaction volume according to the application. These insights will help you with spotting the problem and avoid the network security concern.

2. Paessler Packet Capture Tool

The Paessler Packet-Capture-Tool PRTG: All-In-One-Monitoring is a unified infrastructure monitoring tool. It helps you manage your network and your servers. The network monitoring segment of the utility covers two types of tasks. These are a network performance monitor, which examines the statuses of network devices and a network bandwidth analyzer, which covers the flow of traffic over links in the network.

3. ManageEngine NetFlow Analyzer

The ManageEngine NetFlow Analyzer takes traffic information from your network devices. You can choose to sample traffic, capture entire streams, or gather statistics on traffic patterns with this tool.
The makers of network devices don't all use the same protocol for communicating traffic data. Thus, the NetFlow Analyzer is capable of using different languages to gather information. These include Cisco NetFlow, Juniper Networks J-Flow, and Huawei Netstream. It is also capable of communicating with the sFlow, IPFIX, and AppFlow standards.

4. Wireshark

Wireshark can not only capture data, but also provides some advanced analysis tools. Adding to its appeal, Wireshark is open source, and has been ported over to almost every server operating system that exists. Named Ethereal, Wireshark now runs everywhere, including as a standalone portable app.
If you're analyzing traffic on a server with a desktop installed, Wireshark can do it all for you. The collected packets can then be analyzed all in one spot. However, desktops are not common on servers, so in many cases, you'll want to capture the network data packets remotely and then pull the resulting pcap file into Wireshark.

5. Tcpdump

The fundamental tool of almost all network traffic collection is tcpdump. It is an open-source application that comes installed on almost all Unix-like operating systems. Tcpdump is an excellent collection tool and comes complete with a very complex filtering language. It's essential to know how to filter the data at collection time to end up with a manageable chunk of data to analyze. Capturing all data from a network device on even a moderately busy network can create too much data to analyze efficiently.

6. WinDump

Most useful open source tools are eventually cloned to other operating systems. When this happens, the application is said to have been ported over. WinDump is a port of tcpdump and behaves in very similar ways.
One major difference between WinDump and tcpdump is that Windump needs the WinpCap library installed prior to being able to run WinDump. Despite both WinDump and WinpCap being provided by the same maintainer, they are separate downloads.

7. NetworkMiner

NetworkMiner is a fascinating tool that falls more into the category of a forensic tool rather than a straight-up network sniffer. The field of forensics typically deals with the investigation and collection of evidence and NetworkMiner does that job well for network traffic. Much like WireShark can follow a TCP stream to recover an entire TCP conversation, Network Miner can follow a stream to reconstruct files that were sent over the network.

8. OmniPeek

LiveAction Omnipeek, previously a product of Savvius, is a network protocol analyzer that can be used to capture packets as well as produce protocol analysis of network traffic. Omnipeek can be extended by plug-ins. The core Omnipeek system doesn't capture network packets. However, the addition of the Capture Engine plug-in gets the packet capture function. The Capture Engine system picks up packets on a wired network; another extension, called Wifi Adapter adds wireless capabilities and enables Wifi packets to be captured through Omnipeek.

The functions of the base Omnipeek Network Protocol Analyzer extend to network performance monitoring. As well as listing traffic by protocol, the software will measure the transfer speed and regularity of traffic, raising alerts if traffic slows down or trips passed boundary conditions set by the network administrator.

-END-