Defence Research and Development Canada
Recherche et développement pour la défense Canada

DRDC | RDDC
technologysciencetechnologie

RApid Network Generation and modElling tool (RANGE) quick start guide

Blair Campbell
Bret Schofield
Mike Gingell
General Dynamics Mission Systems, Canada Ltd.

Prepared by:
General Dynamics Mission Systems, Canada Ltd.
Land and Joint Solutions, 31 Millbrook Ave,
Dartmouth, Nova Scotia B2V 0A2
PSPC Contract Number: W7714-115274/001/SV
Technical Authority: Chris McKenzie, Scientific Programmer
Contractor's date of publication: February 2019

Defence Research and Development Canada

Contract Report
DRDC-RDDC-2019-C057
March 2019

Canada

IMPORTANT INFORMATIVE STATEMENTS

This document was reviewed for Controlled Goods by Defence Research and Development Canada using the Schedule to the *Defence Production Act*.

Disclaimer: This document is not published by the Editorial Office of Defence Research and Development Canada, an agency of the Department of National Defence of Canada but is to be catalogued in the Canadian Defence Information System (CANDIS), the national repository for Defence S&T documents. Her Majesty the Queen in Right of Canada (Department of National Defence) makes no representations or warranties, expressed or implied, of any kind whatsoever, and assumes no liability for the accuracy, reliability, completeness, currency or usefulness of any information, product, process or material included in this document. Nothing in this document should be interpreted as an endorsement for the specific use of any tool, technique or process examined in it. Any reliance on, or use of, any information, product, process or material included in this document is at the sole risk of the person so using it or relying on it. Canada does not assume any liability in respect of any damages or losses arising out of or in connection with the use of, or reliance on, any information, product, process or material included in this document.

RApid Network Generation and modElling tool (RANGE) quick start guide

Authors: Blair Campbell, Bret Schofield, Mike Gingell

Organisation: General Dynamics Mission Systems, Canada Ltd.

Address: Land and Joint Solutions, 31 Millbrook Ave, Dartmouth, Nova Scotia B2V 0A2

Technical Authority: Chris McKenzie

Contract Number: W7714-115274/001/SV

Date: **February 6, 2019**

Abstract

The RApid Network Generation and modElling tool (RANGE) is an application that was developed in order to meet a need for quickly generating realistic network models for the purpose of researching relevant cyber security applications. It provides interfaces that allow researchers to rapidly create and visualise models of networks of devices and hosts that include their corresponding interfaces, software inventory and vulnerabilities. Software and vulnerabilities can be added to selected nodes in the network. Supporting tools are available to rapidly create connections between nodes and to set realistic values, such as internet protocol (IP) addresses within subnets. RANGE uses a new cyber data exchange (CDE) schema to import and export networks that contain software and vulnerabilities. It is currently being used to support research on extending the functionality of the Automated Cyber Defence Project (ARMOUR) and to create test scenarios for ingestion into other cyber defence applications. The CDE model provides the fidelity required to exchange networks that include software and vulnerabilities. CDE has also been proven useful for the normalization of data exchanged between existing network scanning and inventory tools.

Résumé

L’outil RApid Network Generation and modElling (RANGE) est une application qui a été développée afin de répondre à un besoin lié à la génération rapide de modèles de réseaux réalistes aux fins de recherche d’applications de cybersécurité pertinentes. Il offre des interfaces permettant aux chercheurs de créer rapidement et de visualiser des modèles de réseaux d’appareils et d’hôtes qui comportent leurs interfaces, vulnérabilités et stocks de logiciels correspondants. Il est possible d’ajouter des logiciels et vulnérabilités à des nœuds choisis du réseau. Des outils à l’appui sont accessibles pour permettre de créer rapidement des connexions entre les nœuds et pour définir des valeurs réalistes, comme des adresses IP (Internet Protocol) dans des sous-réseaux. RANGE utilise un nouveau modèle d’échange de cyberdonnées (CDE) pour importer et exporter des réseaux comportant des logiciels et vulnérabilités. Il sert actuellement à appuyer la recherche visant à étendre la fonctionnalité du projet de cyberdéfense automatisée (ARMOUR) et à créer des scénarios d’essai aux fins d’intégration dans d’autres applications de cyberdéfense. Le modèle CDE offre la fidélité nécessaire à l’échange de réseaux comprenant les logiciels et vulnérabilités. CDE s’est avéré utile aussi pour normaliser les données échangées entre les outils existants utilisés pour le scannage et l’inventaire de réseaux.

RApid Network Generation and modElling tool (RANGE) quick start guide

v1.0.2

Contents

Figures

RANGE (RApid Network Generation and modElling) quick start guide

1 Introduction

RANGE is an application that was developed in order to meet a need for quickly generating realistic network models for the purpose of researching relevant cyber security applications. The tool provides a user intuitive interface that allows the modeller to rapidly create networks of devices and hosts that include their corresponding interfaces, software inventory and vulnerabilities. A visual representation of the nodes in the network make it easy to select single nodes, subnets or other collections of nodes and devices and to apply templates to each of the nodes in order to add software and vulnerabilities. In addition, tools exist to rapidly create connections between nodes and to set realistic values, such as IP addresses within subnets, on these nodes to create realizable subnets and topologies.

RANGE provides an intuitive interface that allows a network modeller or researcher to rapidly create networks of devices and hosts that include their corresponding interfaces, software inventory and vulnerabilities. A visual representation of the nodes in the network makes it easy to select single nodes, subnets or other collections of nodes and devices. A templating system is available in order to add software and vulnerabilities to selected nodes in the network, thus making it easy to apply patterns of software and vulnerabilities to relevant nodes. In addition, RANGE provides tools that are designed to rapidly create connections between nodes and to set realistic values, such as IP addresses within subnets, on these nodes to create realizable subnets and topologies.

In addition to the manual creation of networks, RANGE has the ability to import data from several external scanning tools, such as nmap[1], in their native formats to facilitate the creation and modelling of existing networks. These existing networks can be modified to add additional software and vulnerabilities in order to create models for further analysis. To facilitate the import and export of these network models, a cyber data exchange (CDE) schema was created. The CDE data model is a JavaScript Object Notation (JSON) object that contains all of the data for a network modelled in the RANGE tool. This object serialization into the CDE schema allows RANGE to export a comprehensive, realistic and realizable network for use in other tools and for further research.

RANGE has proven to be valuable tool for generating realistic networks including vulnerabilities. It is currently being used for research purposes related to automated computer network defence and has also been used extensively to create test scenarios for ingestion into other cyber defence applications. The existence of a comprehensive cyber data exchange (CDE) model has also proven to be useful. The CDE model provides the fidelity required to exchange networks that include software and vulnerabilities and has also been used to normalize the exchange of data between existing network scanning and inventory tools.

This document provides the user with a quick introduction to the features of the RANGE (RApid Network Generation and modElling) plugin for Cytoscape and contains the following information:

- Section 2, Prerequisites, describes requisite software required to support RANGE;
- Section 3, Installing the RANGE plugin for Cytoscape, describes the installation procedure for RANGE;

[1] Nmap: the Network Mapper – Free Security Scanner: https://nmap.org/

- Section 4, Importing Data into Cytoscape, describes mechanisms to add data to a RANGE network using data collected from various external sources;
- Section 5, Changing the Visual Layout in RANGE, describes the mechanism to change the network topology layout for visualization purposes;
- Section 6, Editing Attributes of a RANGE node, describes how a user can add, modify and delete attributes of a network node (or selected nodes);
- Section 7, RANGE Templates, describes the templating mechanism provided in RANGE that allows a modeller to quickly apply templates to add attributes to selected nodes;
- Section 8, Exporting or Saving a Network in RANGE, describes how a user can save or export a RANGE network model;
- Section 9, RANGE tools, presents several tools included with RANGE to facilitate the quick connection of nodes and generation of attributes that can realize a viable network; and
- Section 10, Cyber Data Exchange Format, describes an object model for the exchange of networks that include software and vulnerabilities.

2 Prerequisites

RANGE is an application that runs on the Cytoscape platform. This version of RANGE has been developed and tested on Cytoscape v3.6.1 for Windows or Linux and is available from https://cytoscape.org/. Cytoscape must be installed prior to installing the RANGE application.

Downloads are available at https://github.com/cytoscape/cytoscape/releases/3.6.1/.

For Windows and Mac users, if the Cytoscape installer doesn't find a suitable Java Virtual Machine (JVM) already on your workstation, it will download and install one for you. For Linux users, the Cytoscape installer won't download a JVM -- Java 8 (rev 151 or later) must be on the PATH (ahead of any other JVM) or referenced by the JAVA_HOME environment variable.

This version of RANGE has been tested against the following input sources:

Tool	Tested Version	File format
Nessus	8.0.1	Xml (default file format Nessus)
Nmap	7.12	Xml
Smarthawk	3.5.106	Xml

3 Installing the RANGE plugin for Cytoscape

RANGE is a plugin built for the Cytoscape application. This section will describe the process of installing the RANGE plugin using the Cytoscape App Manager tool.

3.1 Installation of RANGE application in Cytoscape

In the Cytoscape application toolbar there is a menu called “Apps” with a menu item called “App Manager”. Clicking this menu item will open the app manager screen as shown in Figure 1.

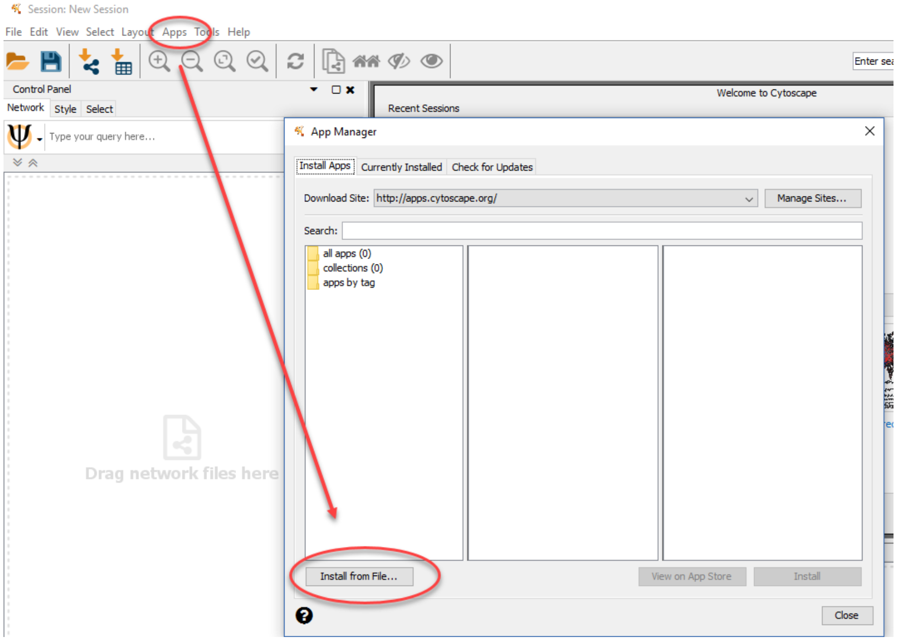


Figure 1 Installing the Range Plugin using the Cytoscape App Manager

To install the RANGE plugin, click the “Install from File…” button that will open a file chooser dialog and then navigate to the Range.jar file as shown in Figure 2.

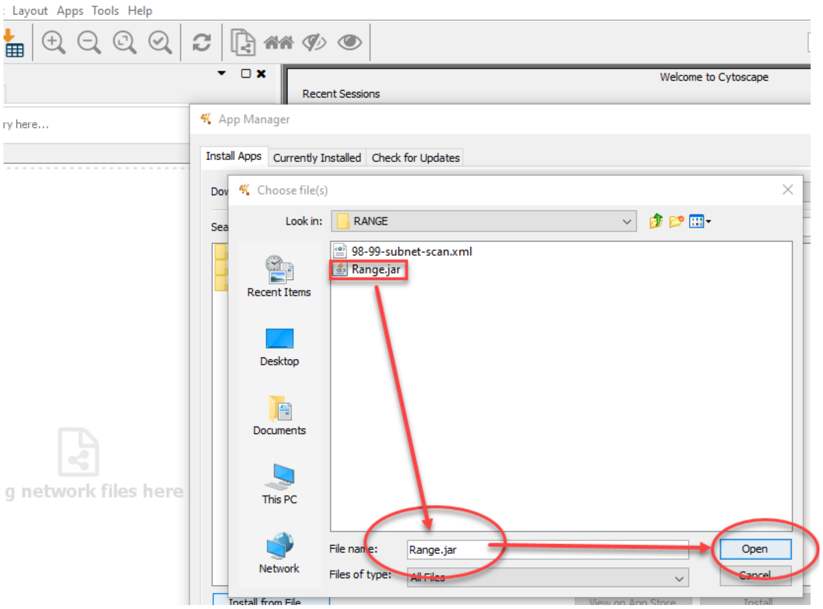
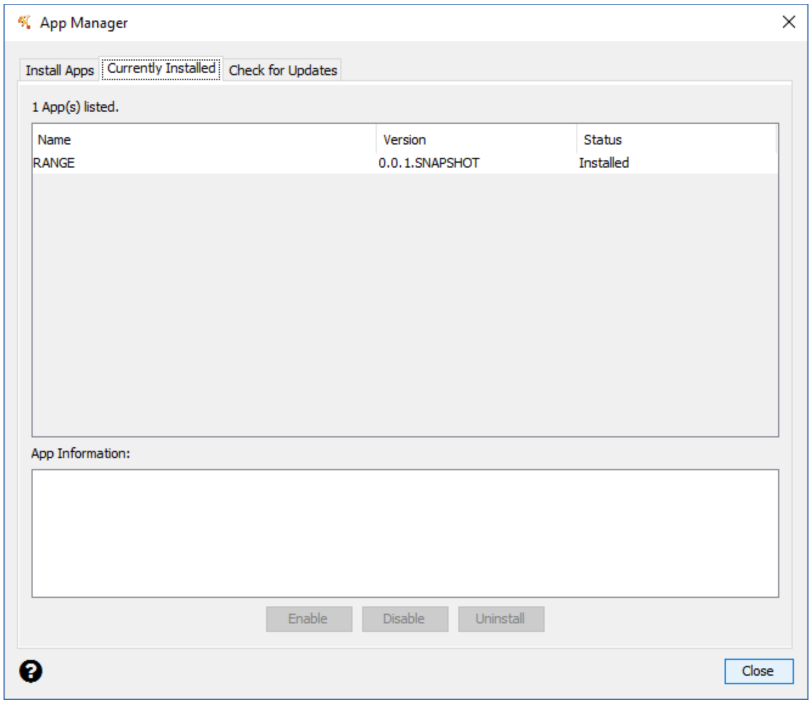


Figure 2 Selecting the RANGE jar file

The App Manager will show the installation status of the RANGE plugin in the “Currently Installed” tab. The RANGE plugin has been successfully installed if the Status column shows “Installed” as seen in Figure 3.



App Manager

Install Apps | Currently Installed | Check for Updates

1 App(s) listed.

Name	Version	Status
RANGE	0.0.1.SNAPSHOT	Installed

App Information:

Figure 3 Verifying the RANGE plugin has been installed.

4 Importing Data into Cytoscape

The Range plugin currently supports importing several different kinds of data such as NMAP, Nessus, Smarthawk and Cyber Data Exchange (CDE) (See section on Cyber Data Exchange Format for more details). This section will introduce to the user how to import these formats into Cytoscape.

Cytoscape requires that a network already exists before importing any data. It will create new nodes in the currently selected network. Figure 4 shows how to create a new network in Cytoscape by selecting File -> New -> Range Network.

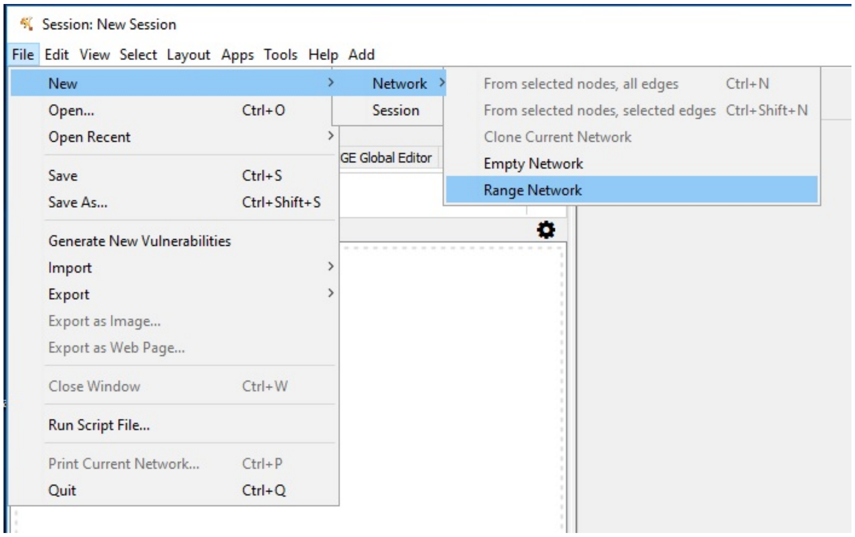


Figure 4 Creating a new empty network in Cytoscape

The different importers can be found in the Cytoscape toolbar as shown in figure 5, as well as in File -> Import.

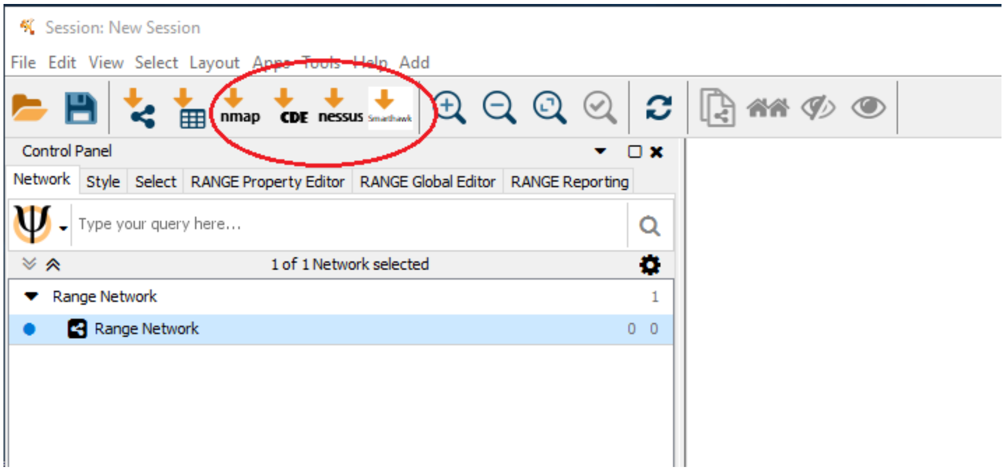
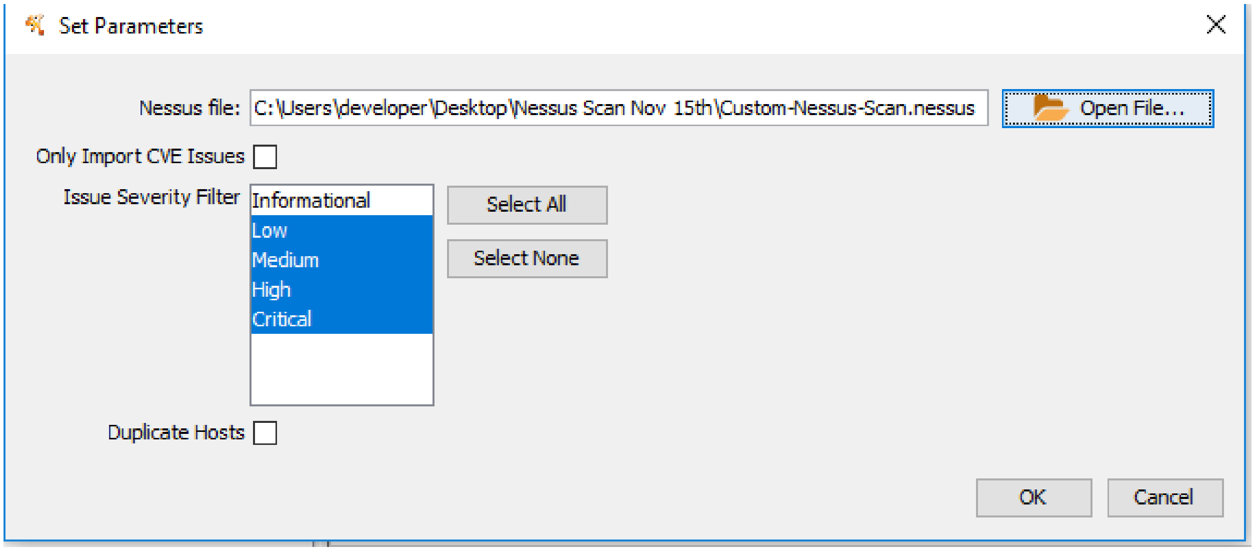


Figure 5 Import Data Functions in Cytoscape Toolbar

Clicking any of the toolbar buttons will bring up a File Chooser dialog where you can select a file for import. The File Chooser also contains a checkbox for duplication: When checked this will cause all hosts to be added, regardless of if they are already present on the network. If this is left unchecked then hosts with IP addresses or names already present on the graph will be overwritten.

4.1 Importing Nessus Data

All File Choosers for the different formats you can import are the same except for the Nessus import which contains one additional field. This field is for choosing the severity levels of vulnerabilities to be imported into Cytoscape from Nessus data. When importing a Nessus file no severities will be selected by default. A severity will be selected when it is highlighted as shown in Figure 6 below.



Nessus file: C:\Users\developer\Desktop\Nessus Scan Nov 15th\Custom-Nessus-Scan.nessus

Only Import CVE Issues □

Issue Severity Filter

- Informational
- Low
- Medium
- High
- Critical

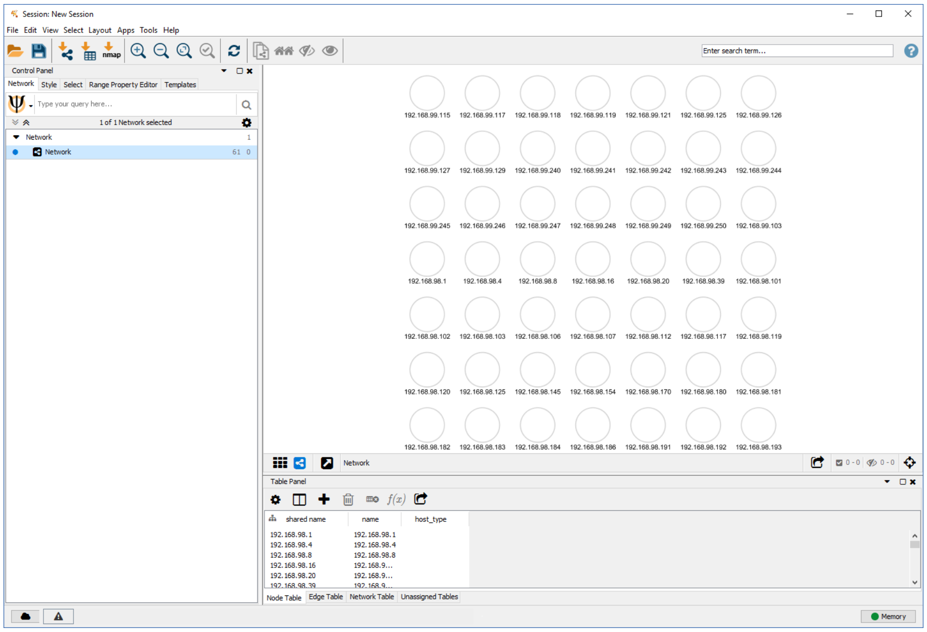
Duplicate Hosts □

Figure 6 Nessus import with several severities selected

Importing a Nessus file will create devices with network interfaces, software, and vulnerabilities. **Note that depending on the size of the network importing can take a long time.**

4.2 Importing Nmap Data

Figure 7 below contains an example of an imported NMAP file. The RANGE plugin will parse the NMAP file looking for hosts with an “up” status and will use the discovered IP address to name the newly created nodes.



shared name	name	host_type
192.168.98.1	192.168.98.1	
192.168.98.4	192.168.98.4	
192.168.98.8	192.168.98.8	
192.168.98.16	192.168.9...	
192.168.98.20	192.168.9...	
192.168.98.39	192.168.9...	

Figure 7 NMAP import successfully creating new nodes in Cytoscape

Note that importing Nmap data will create devices with network interfaces but there will be no ports as ports are associated with software.

5 Changing the Visual Layout in RANGE

When importing data into the RANGE plugin the layout of any already existing networks will be changed. However, Cytoscape comes with many existing layouts to quickly organize a network. Layouts can be found under the Layout header located in the top toolbar, as shown in Figure 8.

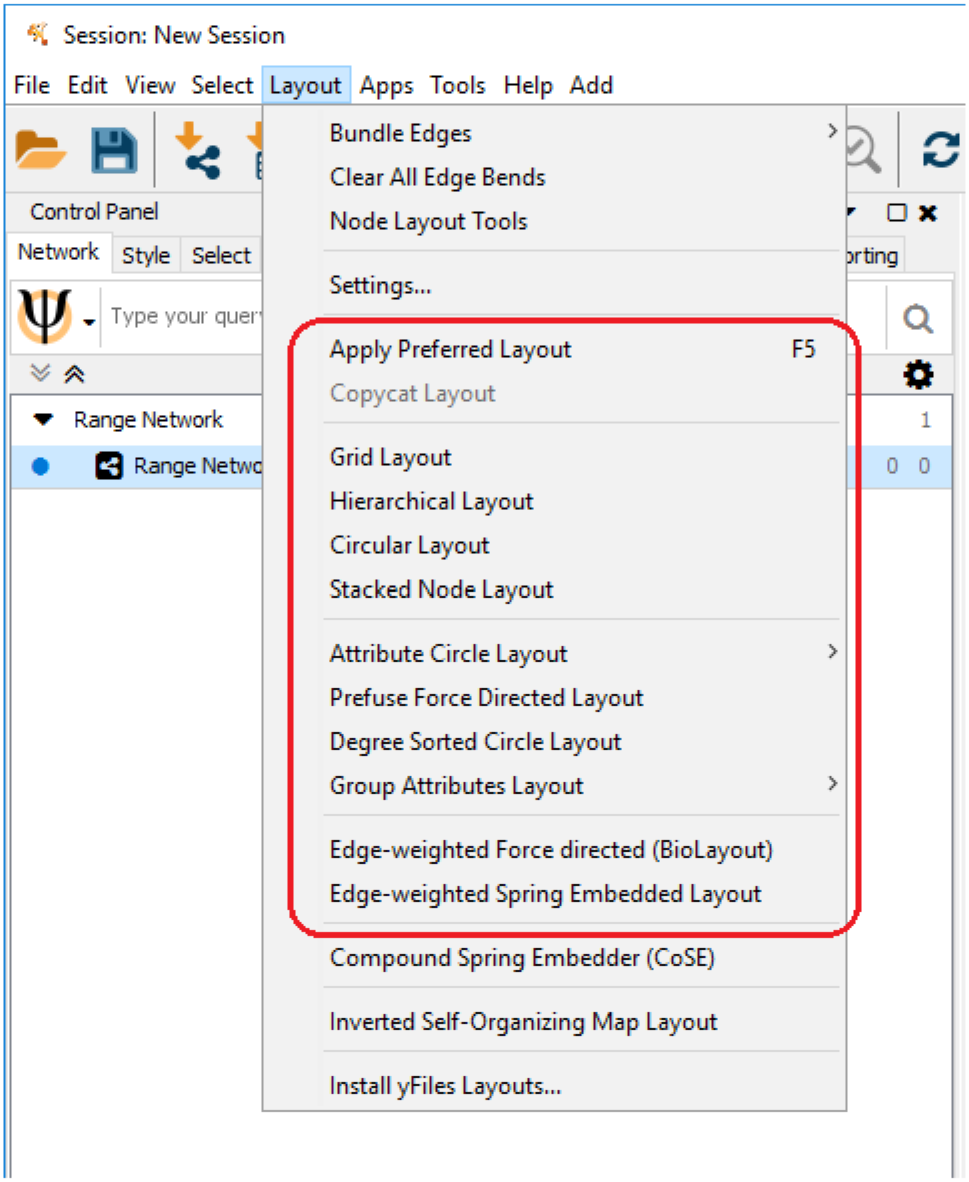
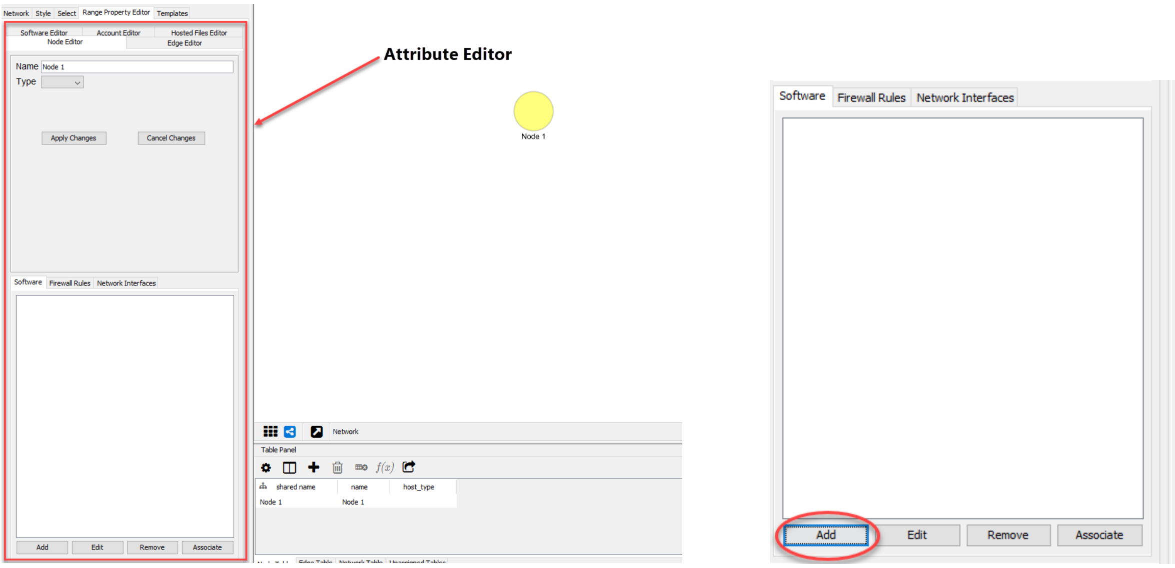

Session: New Session
File Edit View Select Layout Apps Tools Help Add
Control Panel
Network Style Select
Type your query
Range Network
Range Netwo
orting
1
0 0
Bundle Edges
Clear All Edge Bends
Node Layout Tools
Settings...
Apply Preferred Layout F5
Copycat Layout
Grid Layout
Hierarchical Layout
Circular Layout
Stacked Node Layout
Attribute Circle Layout
Prefuse Force Directed Layout
Degree Sorted Circle Layout
Group Attributes Layout
Edge-weighted Force directed (BioLayout)
Edge-weighted Spring Embedded Layout
Compound Spring Embedder (CoSE)
Inverted Self-Organizing Map Layout
Install yFiles Layouts...

Figure 8 Existing Layouts that can be applied to organize a network

6 Editing Attributes of a RANGE node

The RANGE plugin extends the existing table structure in Cytoscape to allow the user to edit RANGE specific attributes on both nodes and edges. The table structure will also allow the user to associate other, non-network data, such as software. This section will briefly introduce the attribute editor provided by the RANGE plugin, see figure 9.



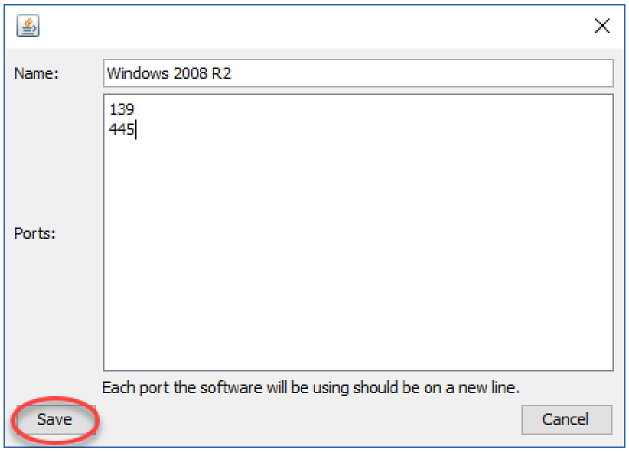
Name Node 1

shared name	name	host_type
Node 1	Node 1	

Figure 9 Attribute Editor in Cytoscape (left) and the Node Software Editor (right)

When a node is selected in the graph, the Node Editor will then be active for the selected node. This means the user can add, edit and remove attributes for that node in the "Node Editor" table in the "Range Property Editor". The node has two attributes, the node name and the node type. To apply any changes made to these attributes the user will click the "Apply Changes" button. If they wish to reset the property editor they can click the "Cancel Changes" button and the values will be populated to the original values found on the node.

The Node Editor also allows the user to edit associated node data. This data includes software, firewall rules and network interface information. In the above example, associated data can be added to a node by clicking the "add" button of the list control. A dialog will pop up and the user can fill in the data of the associated information, see figure 10.



Name: Windows 2008 R2

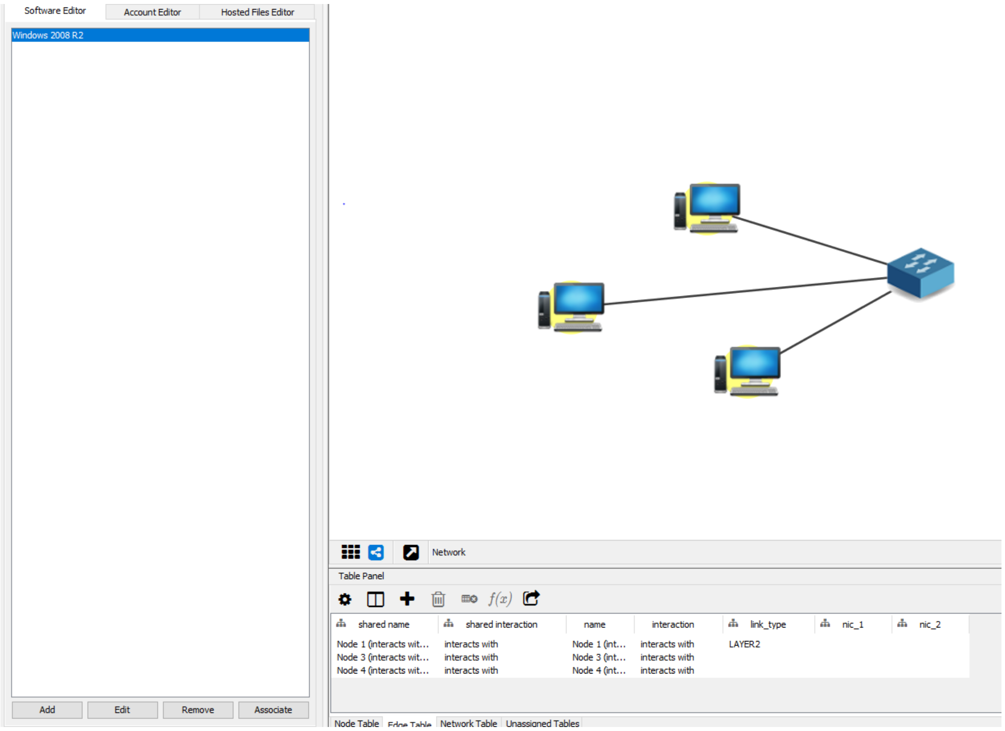
Ports:

139
445

Each port the software will be using should be on a new line.

Figure 10 Adding New Software Dialog

Firewall rules and network interfaces are associated to only one node; software can be associated to multiple nodes. The software editor tab allows users to create a global list of software and then associate that data to a group of selected nodes instead of going to each node individually to create and associate that software. To quickly associate software to a group of nodes, select that software in the Software Editor tab and then select the set of nodes in the graph. At the bottom of the software editor tab there is an "Associate…" button. This button will take the selected set of nodes in the graph and the selected software and create the linkage between each node and that software. A selected set of nodes, selected software and the associate button can be seen in Figure 11.



shared name	shared interaction	name	interaction	link_type	nic_1	nic_2
Node 1 (interacts wit…	interacts with	Node 1 (int…	interacts with	LAYER2		
Node 3 (interacts wit…	interacts with	Node 3 (int…	interacts with			
Node 4 (interacts wit…	interacts with	Node 4 (int…	interacts with			

Figure 11 Associating Software to Nodes

7 RANGE Templates

7.1 Creating Templates in RANGE

The RANGE plugin provides support to Cytoscape for creating templates of nodes. This facilitates the fast creation of nodes with pre-populated attributes, such as software and host types.

To add a node as a template to the template manager, right click the node and select “Range -> Add to template” action. Figure 12 shows the location of this menu item in the right click menu.   This will copy the node and any of its associated data into a template that will then be visible in the template manager. Figure 12 shows the newly created template in the template manager.

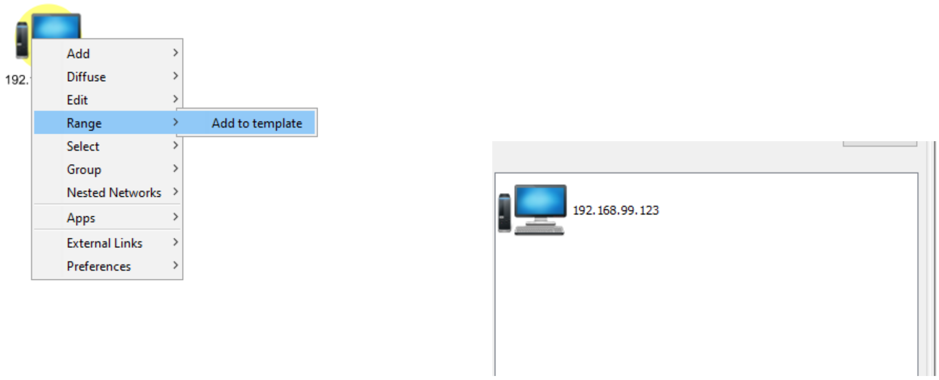
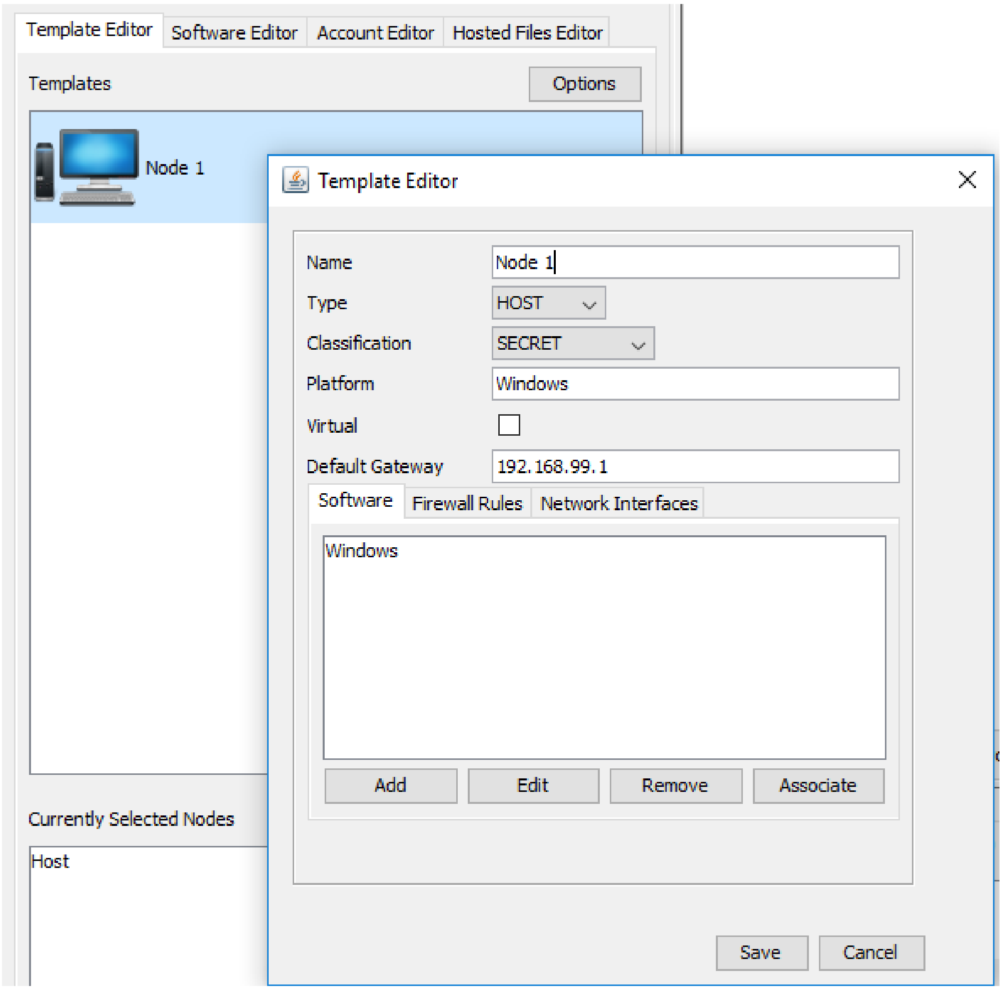


Figure 12 Creating a Template from a Node (left), Template now visible in the template manger (right)

7.2 Editing Templates data in RANGE

To edit a template in RANGE select the template you want to edit and then click “Edit Selected Template” from the template manager menu. This will open a device editor dialog containing all the attributes of the template. When you are done making any changes click the save button and the selected template will be saved with any modifications made. Figure 13 shows the template editor dialog for the template labeled Node 1.



Name: Node 1
Type: HOST
Classification: SECRET
Platform: Windows
Virtual: □
Default Gateway: 192.168.99.1

Figure 13 Editing a Template

7.3 Using Templates in RANGE

Using the template manager, templates can be applied to existing nodes or can be used to create new nodes.

For creating new nodes from a template, you select the template in the template manager and then you double click on the location in the Cytoscape graph that you want to create that new node. The new node will then be created from that template.

For applying templates to existing nodes, select the template from the template manager and then select a node or a group of nodes to which the template should be applied. A list of selected nodes will be shown and the button of the template manager. To apply the template, click the Apply Template button, see Figure 14.

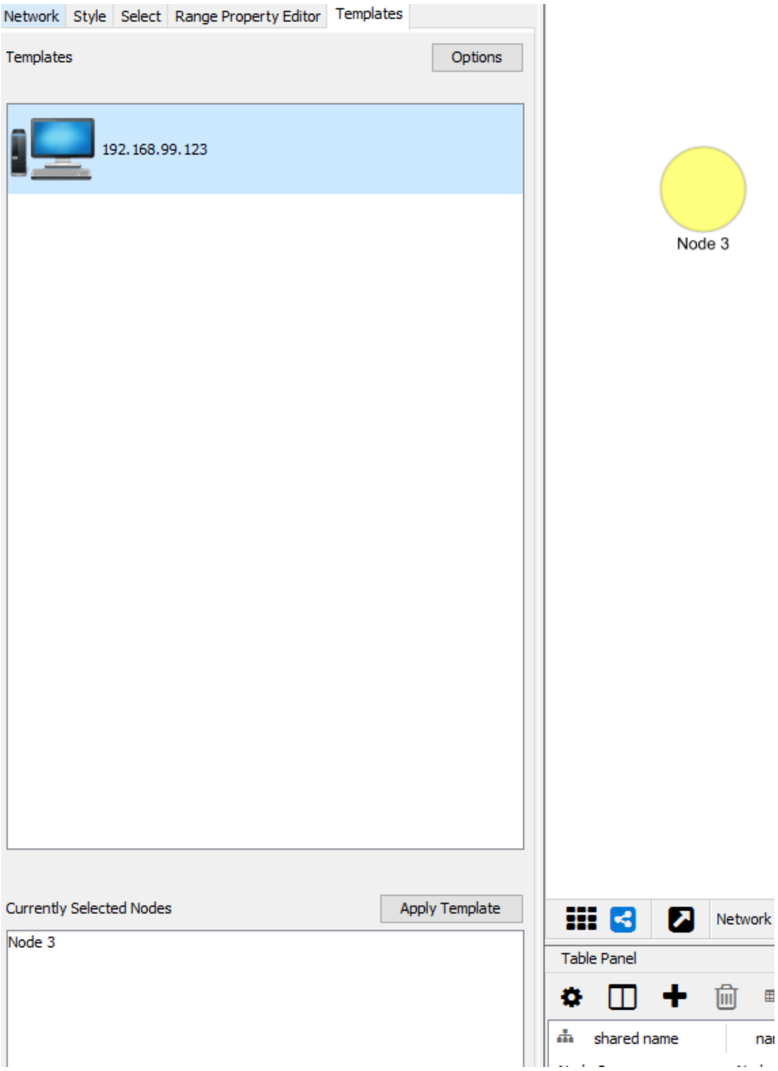


Figure 14 Applying template to existing node

7.4 Distributing Templates in RANGE

Templates can be randomly distributed to a selection of nodes giving the user the ability to create large meaningful networks quickly. To use this feature first select the nodes you wish to distribute the templates to. Next select the templates you want to apply from the template manager and select the "Distribute Templates" option from the template manager menu, see Figure 15.

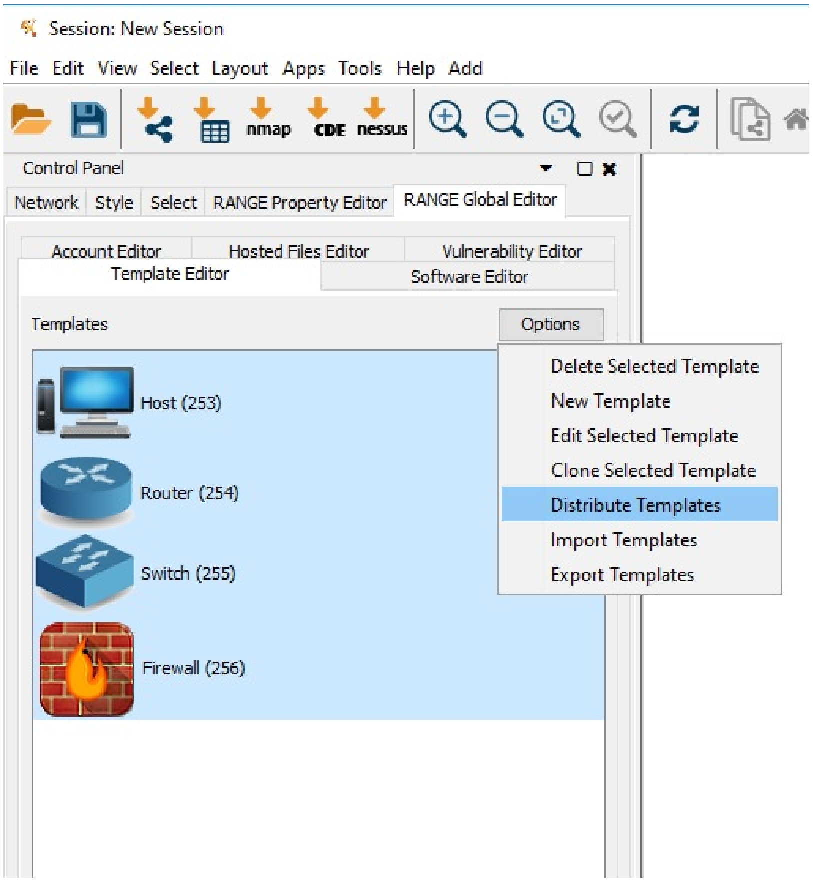
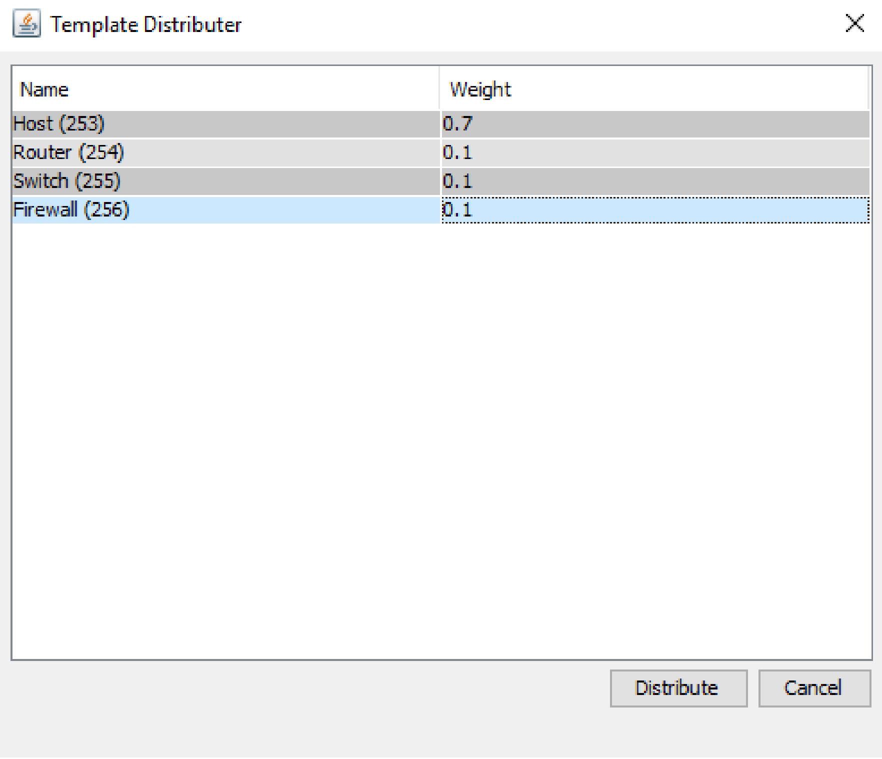


Figure 15 Menu option for distributing templates

This will open the Template Distributer dialog window containing all the selected templates and an associated weight which will have a default value of 0. The weight is a float value representing the percentage of selected nodes you want to apply the corresponding template to. For example, a value of 0.6 means the template will be applied to 60% of the selected nodes. The sum of all weights must be less than 1 and greater than 0. When all the desired values are entered for the weights click the "Distribute" button and the templates will be applied to the selected nodes, see Figure 16.



Name	Weight
Host (253)	0.7
Router (254)	0.1
Switch (255)	0.1
Firewall (256)	0.1

Figure 16 Template Distributer Dialog with template weights

When applying a template to a node all fields will be overwritten. If a field in the template is left empty, then the node it is being applied to will keep the value it already contained. This functionality also applies to all list items such as software, network interfaces, vulnerabilities, firewall rules, and properties.

7.5 Importing Templates in RANGE

Using the template manager you can import templates from CDE files. Each device in the CDE file will create a new template along with all its attributes. To import a template select “Options->Import Templates” from the template manager menu, shown in figure 17. This will open a File Chooser dialog and you can select the file you want to import.

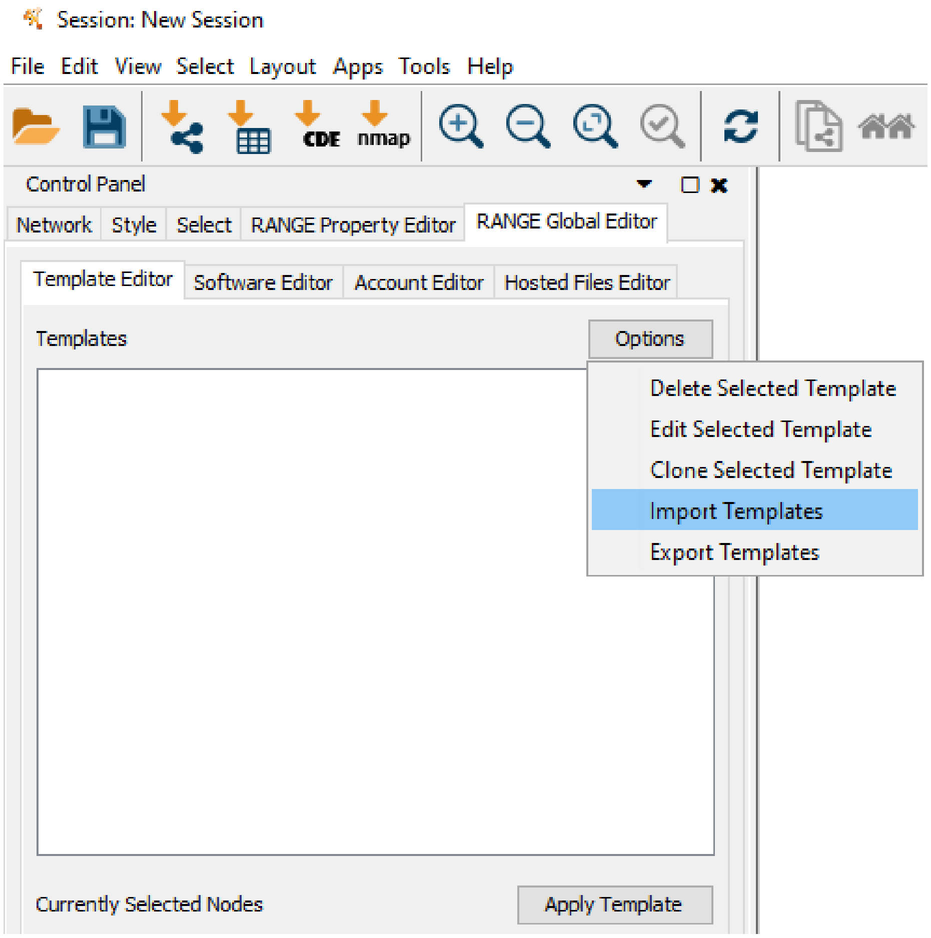


Figure 17 Menu option for importing a template

7.6 Exporting Templates in RANGE

Using the template manager you can export templates. To export, select the templates you want to export then select “Options->Export Templates” from the template manager menu, shown in Figure 18. This will open a File Chooser dialog so you can pick the destination and file name.

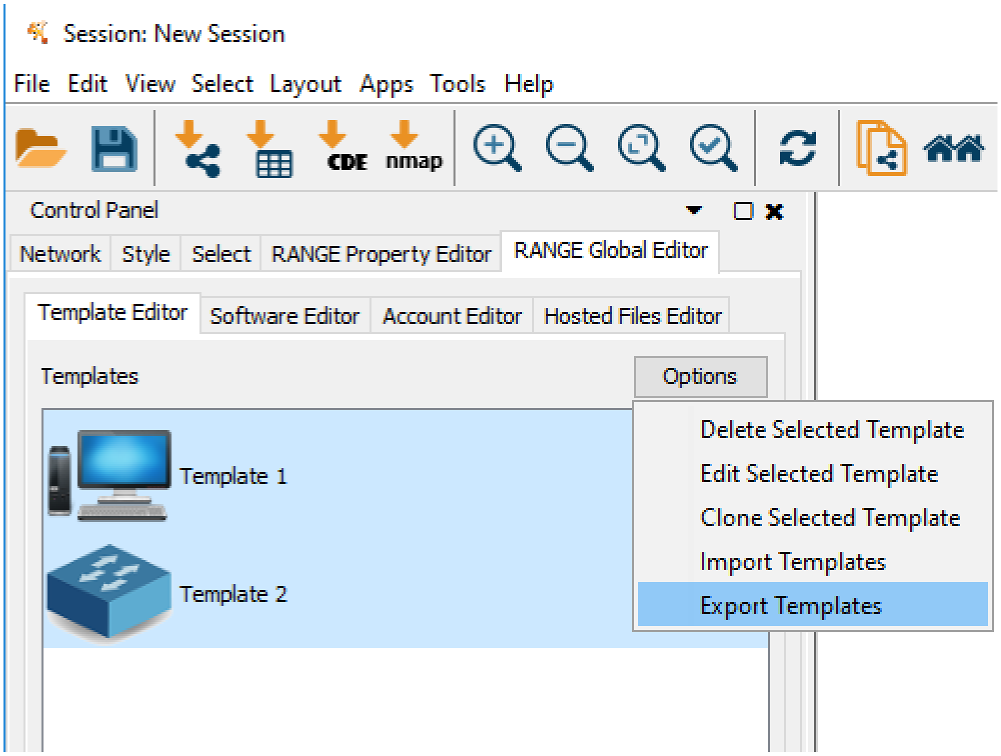


Figure 18 Menu option for exporting a template

8 Exporting or Saving a Network in RANGE

Due to irregularities in Cytoscape we currently cannot save networks in the .CYS format. The supported format for saving or exporting networks is CDE. To export a network to CDE, select File -> Export -> Network as shown in figure 19.

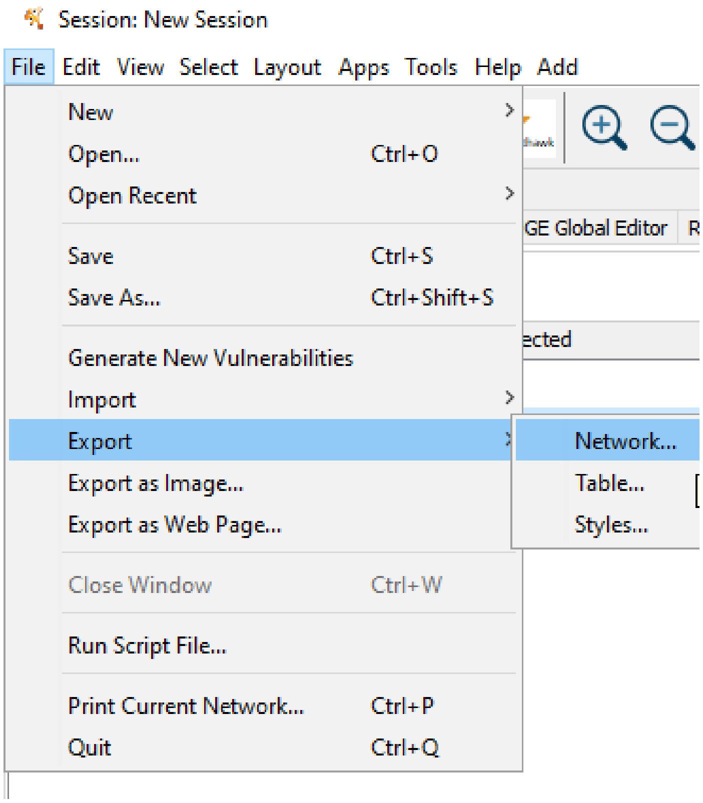
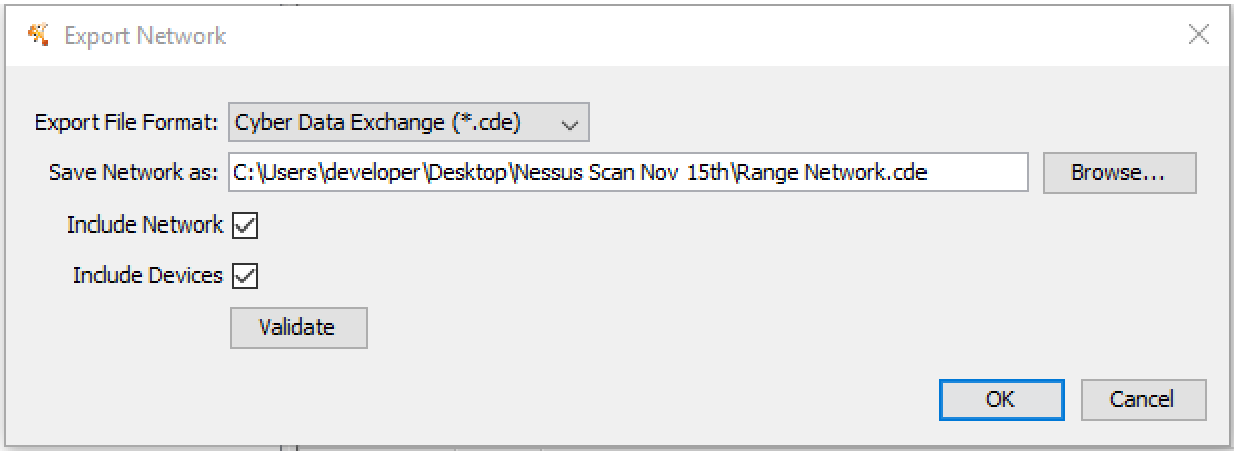


Figure 19 Exporting a network

Once selected, this will launch a file chooser dialog. Select "*Cyber Data Exchange (*.cde)*" from the drop down menu for the Export File Format, as seen below in figure 20.



Export File Format: Cyber Data Exchange (*.cde)

Save Network as: C:\Users\developer\Desktop\Nessus Scan Nov 15th\Range Network.cde

Include Network ☑

Include Devices ☑

Figure 20 File chooser dialog for exporting to CDE

Once you select CDE from the drop down menu you will be presented with more options that include two checkboxes and a validate button. *Include Network* and *Include Devices* will both be checked by default. Including the network will provide the topology and including the devices will provide all devices along with any associated data. Clicking the validate button will check your network for three things:

1) There are devices on a connected network
2) There are devices that contain ports
3) The network contains at least one vulnerable device

If the network being exported is missing any of the above a warning dialog will alert the user. If the network contains all of the pre-requisites no dialog will be shown.

9 RANGE tools

9.1 Quickly Connecting Nodes using the “Quick Connect” action

The RANGE plugin provides a feature called “Quick Connect” that enables the user to quickly connect a selected group of nodes to another node. This is handy when connecting hosts to switches or routers.

To use the “Quick Connect” feature, select the group of nodes that will be connecting to another node. Then right click the node that the set of nodes will be connecting to and navigate to the “Range -> Quick Connect” menu item as show in Figure 21. Figure 22 shows the result of the quick connect action.

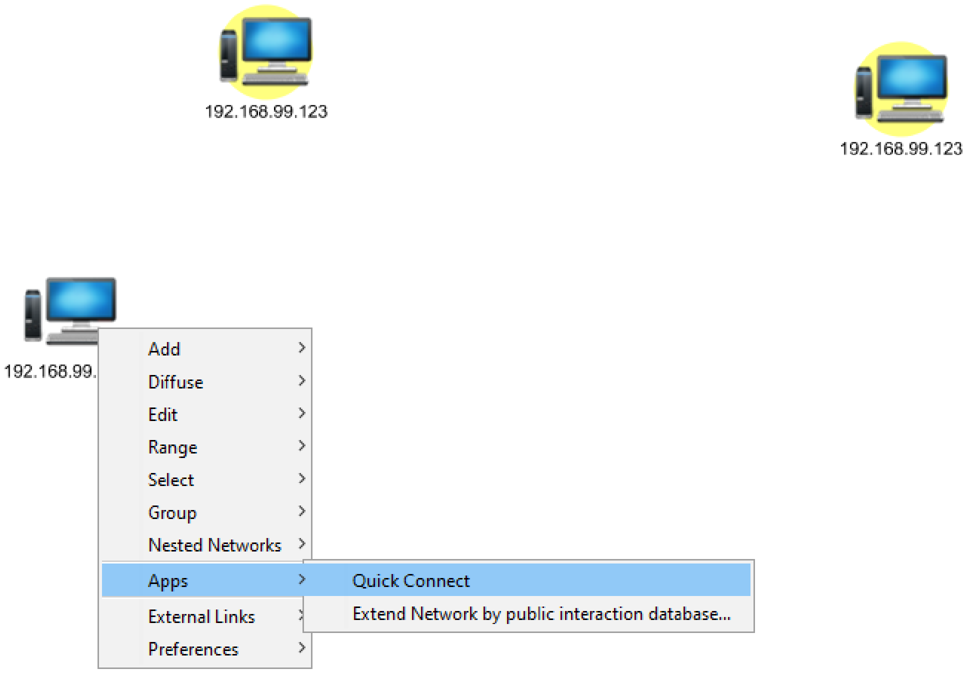


Figure 21 Quick Connect Action

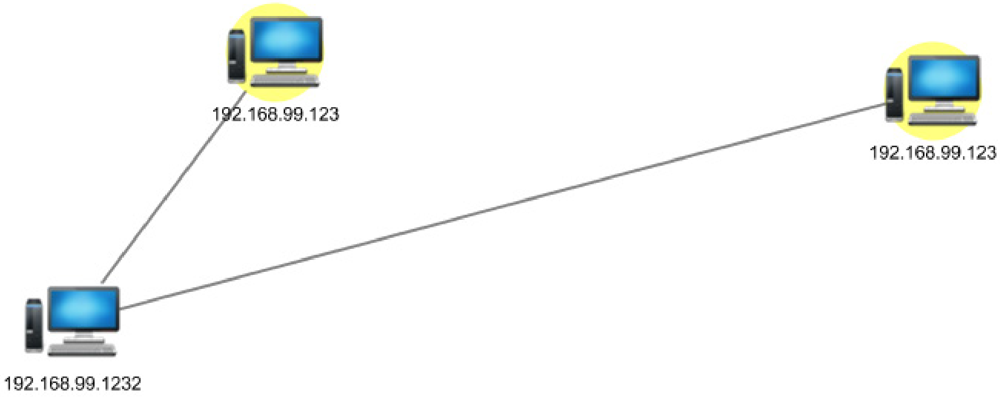
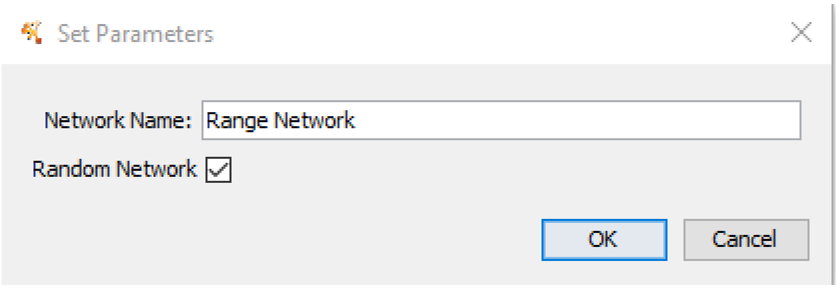


Figure 22 Quick Connect Result

9.2 Generating a Random Generated Network in RANGE

The RANGE plugin has the ability to generate a network of specified size when creating a new Range Network. To generate a random network create a new Range Network by clicking File -> New -> Network -> Range Network. This will launch a dialog to name your network and give you the option the make it a random network, see Figure 23.

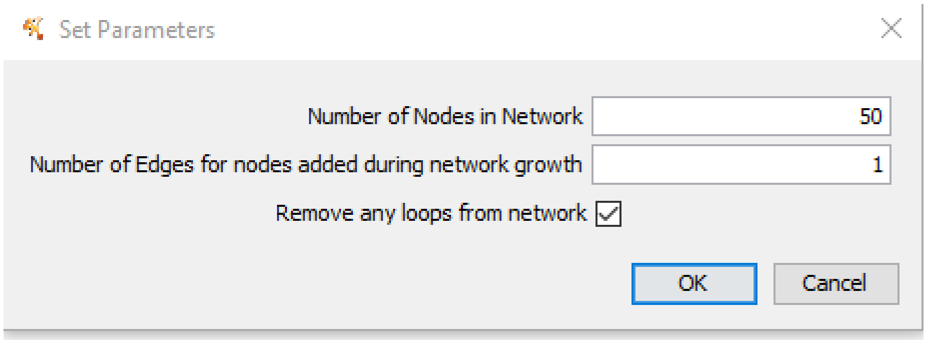

Set Parameters

Network Name: Range Network

Random Network ☑

Figure 23 Dialog to generate a random network

Select the checkbox to create a random network and click okay. This will launch a second dialog, shown in Figure 24, where you can specify the number of nodes you want in the network, number of edges for nodes added during network growth, and a checkbox to remove any loops from the network that is checked by default. It is recommended to keep this box checked.


Set Parameters

Number of Nodes in Network: 50

Number of Edges for nodes added during network growth: 1

Remove any loops from network ☑

Figure 24 Parameters Dialog for Random Generated Network

10 Cyber Data Exchange Format

RANGE has the ability to export and import data in a format called Cyber Data Exchange (CDE). This gives users the ability to easily save and share network information. This means custom defined devices or software templates that can be created or modified in the Range UI can also be exported or imported. If desired the whole network can be exported or imported as well. CDE files can also be imported into other tools such as the ARMOUR Project. Sample CDE files have been included in the RANGE source code. For example, the “minimum viable data set” contains all information needed to create a Course of Action when imported into the ARMOUR project.

It is important to note that the CDE format was designed to easily share data and does not require or enforce all data in a network to be populated. This means that if it’s being used for a specific case that requires all or part of the data to be present, it is up to the user to make sure that everything required is present. RANGE does however give the option to validate a network when exporting to CDE to ensure sufficient data is contained in the range network to be able to generate a Course of Action when imported into the ARMOUR Project.

For a schema representation of the CDE JSON file format please refer to Appendix A of this document.

Appendix A: Cyber Data Exchange Schema

```
{
  "$schema": "http://json-schema.org/draft-06/schema#",
  "title": "CyberDataExchange",
  "description": "Cyber Data Exchange Format",
  "type": "object",
  "additionalProperties": false,
  "required": [
    "source"
  ],
  "properties": {
    "source": {
      "description": "The source that was responsible for generating the CDE file",
      "type": "string"
    },
    "devices": {
      "description": "The collection of information that describes the configuration of devices",
      "type": "object",
      "required": [
        "device"
      ],
      "properties": {
        "device": {
          "description": "Device Configuration Information",
          "type": "array",
          "items": {
            "$ref": "#device"
          }
        },
        "software": {
          "description": "List of Software that is associated with entries in the device list",
          "type": "array",
          "items": {
            "$ref": "#software"
          }
        },
        "security": {
          "description": "A collection of vulnerabilities and weaknesses that affected devices with software
configurations",
          "type": "object",
          "properties": {
            "vulnerabilities": {
              "description": "List of Vulnerabilities and their associated list of affected device/software configuration
pairs",
              "type": "array",
              "items": {
                "$ref": "#vuln"
              }
            },
            "weaknesses": {
              "description": "List of Weaknesses and their associated list of affected device/software configuration
pairs",
              "type": "array",
              "items": {
                "$ref": "#weak"
              }
            }
          }
        }
      }
    },
    "network": {
      "$ref": "#topology"
    }
  },
  "definitions": {
    "affected_device": {
      "$id": "affected",
      "description": "Describes a list of devices with a software configuration that lead to the device being affected by
a vulnerability or weakness",
      "type": "object",
      "required": [
        "devices",
        "software"
      ],
      "properties": {
        "devices": {
          "description": "The list of device ids of the devices that are affected by a weakness or vulnerability",
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "software": {
          "description": "The list of software ids of the software that are involved in affecting a deviec with a weakness
or vulnerability.  The device will be associated each of these software ids.",
          "type": "array",
          "items": {
            "type": "string"
          }
        }
      }
    },
    "vulnerability": {
      "$id": "vuln",
      "description": "Represents a Vulnerability Configuration and how it affects devices",
      "type": "object",
      "required": [
        "id",
        "affected"
      ],
      "properties": {
        "id": {
          "description": "The unique identifier for the vulnerability",
          "type": "string"
        },
        "desc": {
          "description": "A description of the vulnerability",
          "type": "string"
        },
        "vector": {
          "description": "The access vector of the vulnerability",
          "type": "string"
        },
        "score": {
          "description": "The CVSS Score of the Vulnerability",
          "type": "string"
        },
        "affected": {
          "description": "List of Affected Configurations.  And affected configuration is a software list that is present
on a set of devices.  Many different configurations can be affected by a vulnerability",
          "type": "array",
          "items": {
            "$ref": "#affected"
          }
        }
      }
    },
    "weakness": {
      "$id": "weak",
      "description": "Represents a Weakness Configuration and how it affects devices",
      "type": "object",
      "required": [
        "id",
        "affected"
      ],
      "properties": {
        "id": {
          "description": "The unique identifier for the weakness",
          "type": "string"
        },
        "desc": {
          "description": "A description of the weakness",
          "type": "string"
        },
        "vector": {
          "description": "The access vector of the weakness",
          "type": "string"
        },
        "score": {
          "description": "The CWSS Score of the Weakness",
          "type": "string"
        },
        "affected": {
          "description": "List of Affected Configurations.  And affected configuration is a software list that is present
on a set of devices.  Many different configurations can be affected by a weakness.",
          "type": "array",
          "items": {
            "$ref": "#affected"
          }
        }
      }
    },
    "topology": {
      "$id": "#topology",
      "description": "Network Topology Description",
      "type": "object",
      "properties": {
        "direction": {
          "enum": [
            "directed",
            "undirected"
          ]
        },
        "devices": {
          "description": "Network Device Information",
          "type": "array",
          "items": {
            "$ref": "#net_device"
          }
        },
        "links": {
          "description": "Network Topology Adjaceny Matrix Information",
          "type": "array",
          "items": {
            "$ref": "#link"
          }
        }
      },
      "required": [
        "direction",
        "devices",
        "links"
      ]
    },
    "device": {
      "$id": "#device",
      "properties": {
        "id": {
          "description": "Unique Identifier for a device",
          "type": "string"
        },
        "hostname": {
          "description": "A label or name for this device",
          "type": "string"
        },
        "host_type": {
          "description": "The type of device",
          "enum": [
            "HOST",
            "SWITCH",
            "ROUTER",
            "PRINTER"
          ]
        },
        "classification": {
          "description": "The classification of the device",
          "enum": [
            "UNCLASSIFIED",
            "PROTECTED_A",
            "PROTECTED_B",
            "SECRET",
            "TOP_SECRET"
          ]
        },
        "virtual": {
          "description": "Is this device a virtualized device or a hardware device",
          "type": "boolean"
        },
        "platform": {
          "description": "The platform or operating system of the device",
          "type": "string"
        },
        "default_gateway": {
          "description": "The default gateway used by the device for network traffic",
          "type": "string"
        },
        "interfaces": {
          "description": "The list of network interfaces associated with the device",
          "type": "array",
          "items": {
            "$ref": "#interface"
          }
        },
        "firewall_rules": {
          "description": "The list of firewall rules associated with the device",
          "type": "array",
          "items": {
            "$ref": "#fw_rule"
          }
        },
        "software": {
          "description": "Software that is associated with this device.  The ID is the entry of the software item in the
software list of the CDE",
          "type": "array",
          "items": {
            "type": "string"
          }
        }
      }
    },
    "software": {
      "$id": "#software",
      "properties": {
        "name": {
          "description": "A friendly name for the software",
          "type": "string"
        },
        "vendor": {
          "description": "The vendor or manufacturer of the software",
          "type": "string"
        },
        "type": {
          "description": "The type of software",
          "enum": [
            "SERVICE",
            "OS",
            "APPLICATION",
            "LIBRARY"
          ]
        },
        "version": {
          "description": "The version of the software",
          "type": "string"
        },
        "assigned_ports": {
          "description": "The ports used by this software",
          "items": {
            "type": "string"
          }
        },
        "svc_pack": {
          "description": "The service pack version of the software",
          "type": "string"
        },
        "cpe": {
          "description": "The common platform enumeration used to identifier this software",
          "type": "string"
        },
        "account": {
          "description": "The account used to run the software",
          "type": "string"
        }
      }
    },
    "fw_rule": {
      "$id": "#fw_rule",
      "properties": {
        "name": {
          "description": "A Friendly Name of the Firewall Rule",
          "type": "string"
        },
        "source_object": {
          "description": "The source of the traffic that will match this rule.",
          "type": "string"
        },
        "source_ports": {
          "description": "The ports on the source object that are used to communicate traffic.",
          "type": "array",
          "items": {
            "type": "string"
          }
        },
        "source_mac_address": {
          "description": "The MAC address of the source traffic",
          "type": "string"
        },
        "destination_object": {
          "description": "The destination of the traffic that will match this rule",
          "type": "string"
        },
        "destination_ports": {
          "description": "The ports on the destination object that are used to communicate traffic",
          "items": {
            "type": "string"
          }
        },
        "destination_mac_address": {
          "description": "The MAC address of the destination traffic",
          "type": "string"
        },
        "rule_index": {
          "description": "Used to sort the firewall rules by order of matchin",
          "type": "string"
        },
        "action": {
          "description": "Should the network traffic that matched this rule be allowed or denied",
          "enum": [
            "ALLOW",
            "DENY"
          ]
        },
        "protocol": {
          "description": "The protocol of network traffic that this rule should match",
          "enum": [
            "TCP",
            "UDP",
            "IP"
          ]
        }
      },
      "required": [
        "rule_index"
      ]
    },
    "network_interface": {
      "$id": "#interface",
      "properties": {
        "mac": {
          "description": "The MAC Address of the interface",
          "type": "string"
        },
        "ip_address": {
          "description": "The IP Address of the interface",
          "type": "string"
        },
        "mask": {
          "description": "The netmask of the interface",
          "type": "string"
        },
        "family": {
          "enum": [
            "ipv4"
          ]
        }
      }
    },
    "network_device": {
      "$id": "#net_device",
      "properties": {
        "id": {
          "description": "A Unique Identifier for the device on the network",
          "type": "string"
        },
        "label": {
          "description": "A Friendly Name for this device on the network",
          "type": "string"
        },
        "ip_addresses": {
          "description": "A List of the IP Addresses associated with this network device",
          "type": "array",
          "items": {
            "type": "string"
          }
        }
      }
    },
    "link": {
      "$id": "#link",
      "properties": {
        "adjacency_1": {
          "description": "",
          "type": "array",
          "items": {
            "type": "string"
          },
          "minItems": 1,
          "uniqueItems": true
        },
        "adjacency_2": {
          "description": "",
          "type": "array",
          "items": {
            "type": "string"
          },
          "minItems": 1,
          "uniqueItems": true
        },
        "attributes": {
          "$ref": "#link_attributes"
        }
      },
      "required": [
        "adjacency_1",
        "adjacency_2"
      ]
    },
    "link_attributes": {
      "$id": "#link_attributes",
      "properties": {
        "nic_source": {
          "description": "",
          "type": "string"
        },
        "nic_target": {
          "description": "",
          "type": "string"
        },
        "is_ap_wireless": {
          "description": "",
          "type": "boolean"
        },
        "is_manet_wireless": {
          "description": "",
          "type": "boolean"
        }
      }
    }
  }
}
```

DOCUMENT CONTROL DATA

*Security markings for the title, authors, abstract and keywords must be entered when the document is sensitive

1. ORIGINATOR (Name and address of the organization preparing the document. A DRDC Centre sponsoring a contractor's report, or tasking agency, is entered in Section 8.)

General Dynamics Mission Systems, Canada Ltd.
Land and Joint Solutions, 31 Millbrook Ave,
Dartmouth, Nova Scotia B2V 0A2

2a. SECURITY MARKING
(Overall security marking of the document including special supplemental markings if applicable.)

CAN UNCLASSIFIED

2b. CONTROLLED GOODS

NON-CONTROLLED GOODS
DMC A

3. TITLE (The document title and sub-title as indicated on the title page.)

RApid Network Generation and modElling tool (RANGE) quick start guide

4. AUTHORS (Last name, followed by initials – ranks, titles, etc., not to be used)

Campbell, B.; Schofield, B.; Gingell, M.

5. DATE OF PUBLICATION
(Month and year of publication of document.)

February 2019

6a. NO. OF PAGES
(Total pages, including Annexes, excluding DCD, covering and verso pages.)

33

6b. NO. OF REFS
(Total references cited.)

0

7. DOCUMENT CATEGORY (e.g., Scientific Report, Contract Report, Scientific Letter.)

Contract Report

8. SPONSORING CENTRE (The name and address of the department project office or laboratory sponsoring the research and development.)

DRDC – Ottawa Research Centre
Defence Research and Development Canada, Shirley's Bay
3701 Carling Avenue
Ottawa, Ontario K1A 0Z4
Canada

9a. PROJECT OR GRANT NO. (If appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant.)

05ac - Cyber Decision Making and Response (CDMR)

9b. CONTRACT NO. (If appropriate, the applicable number under which the document was written.)

W7714-115274/001/SV

10a. DRDC PUBLICATION NUMBER (The official document number by which the document is identified by the originating activity. This number must be unique to this document.)

DRDC-RDDC-2019-C057

10b. OTHER DOCUMENT NO(s). (Any other numbers which may be assigned this document either by the originator or by the sponsor.)

11a. FUTURE DISTRIBUTION WITHIN CANADA (Approval for further dissemination of the document. Security classification must also be considered.)

Public release

11b. FUTURE DISTRIBUTION OUTSIDE CANADA (Approval for further dissemination of the document. Security classification must also be considered.)

12. KEYWORDS, DESCRIPTORS or IDENTIFIERS (Use semi-colon as a delimiter.)

Cyber Security; Cyber Decision Making

13. ABSTRACT/RÉSUMÉ (When available in the document, the French version of the abstract must be included here.)

The RApid Network Generation and modElling tool (RANGE) is an application that was developed in order to meet a need for quickly generating realistic network models for the purpose of researching relevant cyber security applications. It provides interfaces that allow researchers to rapidly create and visualise models of networks of devices and hosts that include their corresponding interfaces, software inventory and vulnerabilities. Software and vulnerabilities can be added to selected nodes in the network. Supporting tools are available to rapidly create connections between nodes and to set realistic values, such as internet protocol (IP) addresses within subnets. RANGE uses a new cyber data exchange (CDE) schema to import and export networks that contain software and vulnerabilities. It is currently being used to support research on extending the functionality of the Automated Cyber Defence Project (ARMOUR) and to create test scenarios for ingestion into other cyber defence applications. The CDE model provides the fidelity required to exchange networks that include software and vulnerabilities. CDE has also been proven useful for the normalization of data exchanged between existing network scanning and inventory tools.

L'outil RApid Network Generation and modElling (RANGE) est une application qui a été développée afin de répondre à un besoin lié à la génération rapide de modèles de réseaux réalistes aux fins de recherche d'applications de cybersécurité pertinentes. Il offre des interfaces permettant aux chercheurs de créer rapidement et de visualiser des modèles de réseaux d'appareils et d'hôtes qui comportent leurs interfaces, vulnérabilités et stocks de logiciels correspondants. Il est possible d'ajouter des logiciels et vulnérabilités à des noeuds choisis du réseau. Des outils à l'appui sont accessibles pour permettre de créer rapidement des connexions entre les noeuds et pour définir des valeurs réalistes, comme des adresses IP (Internet Protocol) dans des sous-réseaux. RANGE utilise un nouveau modèle d'échange de cyberdonnées (CDE) pour importer et exporter des réseaux comportant des logiciels et vulnérabilités. Il sert actuellement à appuyer la recherche visant à étendre la fonctionnalité du projet de cyberdéfense automatisée (ARMOUR) et à créer des scénarios d'essai aux fins d'intégration dans d'autres applications de cyberdéfense. Le modèle CDE offre la fidélité nécessaire à l'échange de réseaux comprenant les logiciels et vulnérabilités. CDE s'est avéré utile aussi pour normaliser les données échangées entre les outils existants utilisés pour le scannage et l'inventaire de réseaux.