

Network Deployment Automation Maintenance Tool

Contents

1. Introduction
 1. Platform functionality
 2. Prerequisite knowledge
2. System requirements
3. Installation (client side)
4. Setting up the Local Area Network
 1. FTP server
 2. Console server
 3. Database server
5. Configuring initial application settings
6. Deploying devices
7. Keeping track of the configuration files
8. Scanning a Local Area Network
9. Troubleshooting problems

1.Introduction

This program is a lightweight network automation tool, intended to increase efficiency and productivity of network engineers, by automating repetitive tasks.

1. Platform functionality

This program is aimed at network engineers and is intended to automate the deployment of high-end networking devices manufactured by Juniper Networks, allow for version control of device configurations as well as enabling the user to easily map out a local area network.

2. Prerequisite knowledge

A basic level of networking knowledge is required to use this program to its full potential. However, a medium level is required to set up the local area network necessary for the deployment module to be utilised.

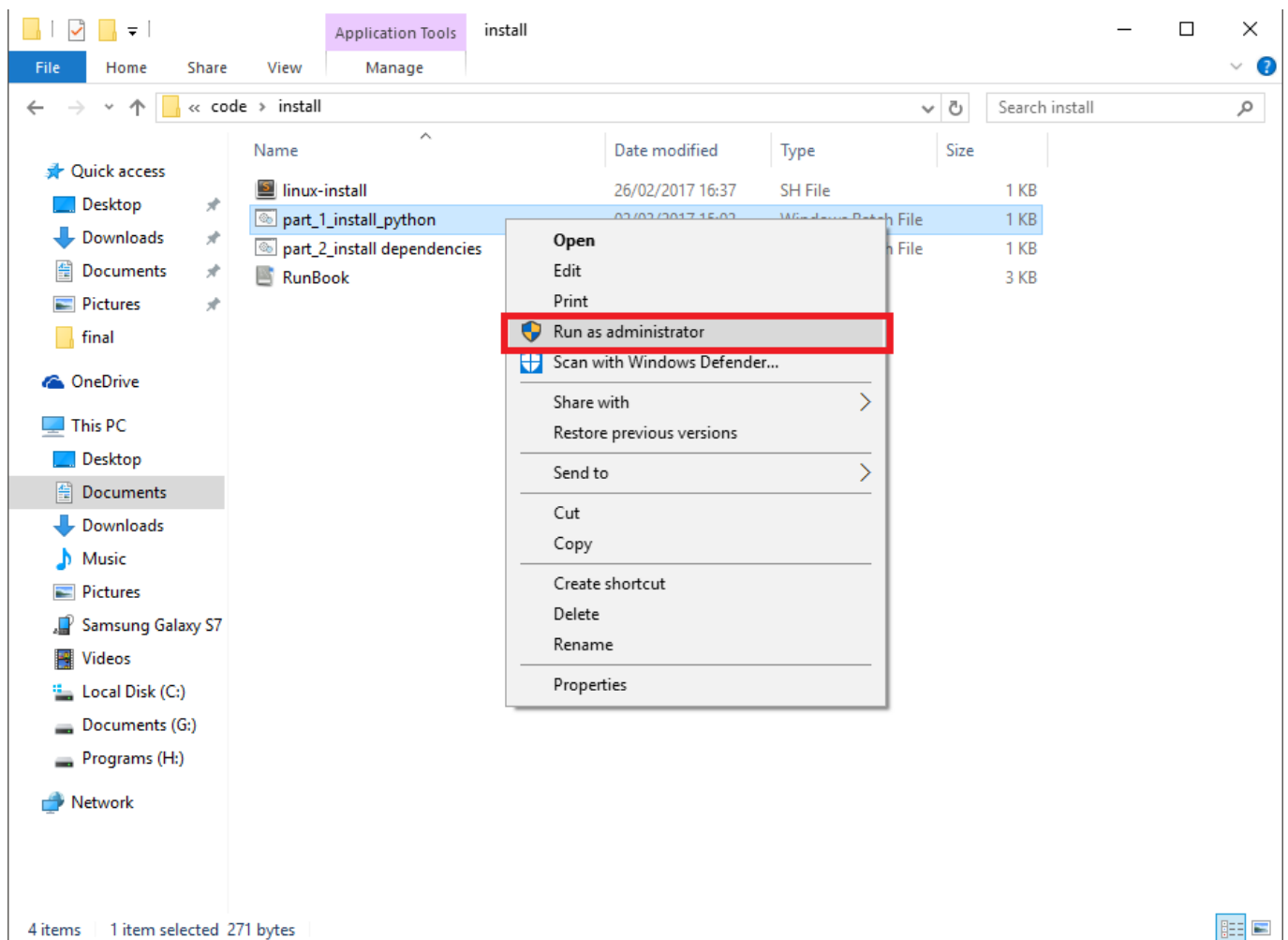
2.System requirements

The operating systems supported by this software are: - Windows 7/8/10 - Linux Distributions (Ubuntu, Elementary OS, etc) - macOS (Limited support)

Minimum system configuration: - Single core 1GHz Intel or equivalent AMD processor - 1GB of RAM - Screen resolution of 1280×720 - 55MB free disk space

3.Installation (client side)

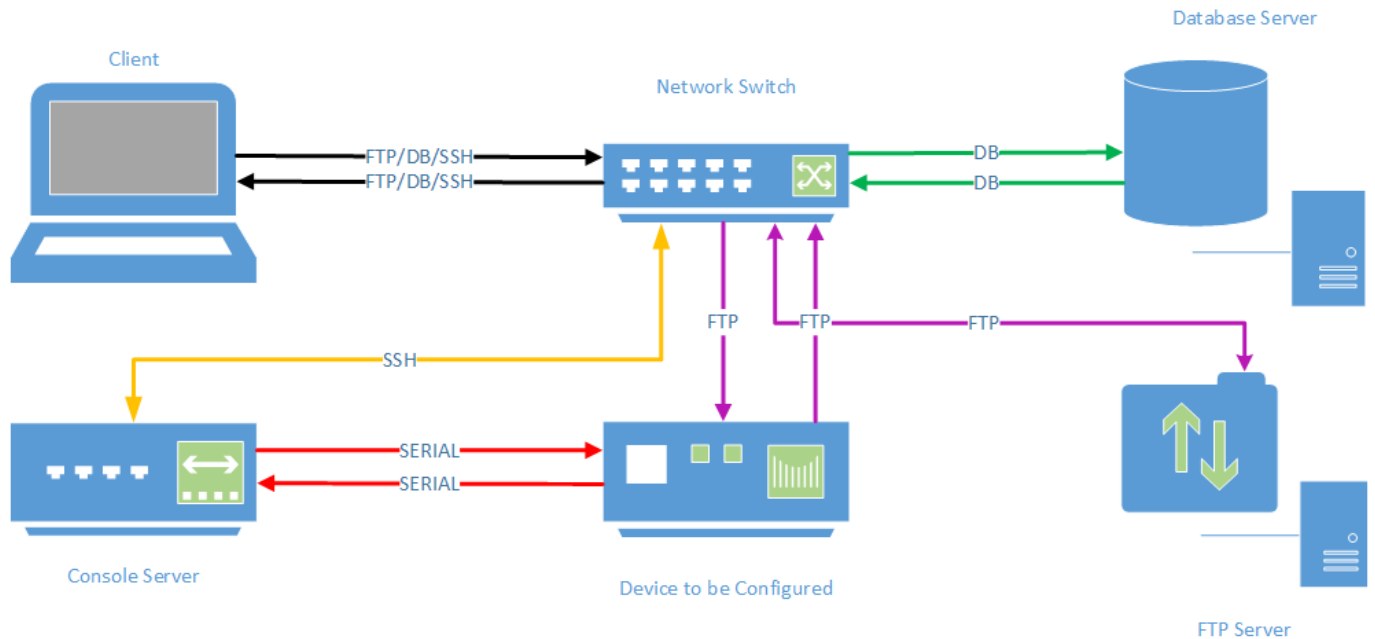
- 1.Open the `*/code/install*` directory
- 2.Run the `*part_1_install_python*` file ****as Administrator****
- 3.Wait for the program to execute
- 4.Run the `*part_2_install_dependencies*` file ****as Administrator****
- 5.Wait for the program to execute



- On Linux/Unix devices only run the `linux-install.sh` file with **sudo** privileges

4.Setting up the Local Area Network

To automate the deployment of networking devices the following network setup is necessary.



1.FTP server

An FTP server is made up of hardware/software using the File Transfer Protocol to store, receive and share files over a network. By using this, our application is able to store and access configuration files for each device deployed. We can also add to it as time goes on so we can store any changes made to files.

Due to a vast majority of FTP server solutions, this manual will not cover the topic of installation and setup of an FTP server.

However, two main requirements of the system include:

1. Having password protected access to the configuration and operating system files.
2. A user account with the capability of reading and writing to three directories used by the program. They are the operating system directory (containing desired Juniper OS images), initial configuration directory (containing configuration files to be applied to devices during the deployment process) and finally a configuration directory (used for configuration version control).

*Two most popular solutions include FileZilla for Windows based systems and *vsftpd* for Linux based systems.

2.Console server

A Console server is a device containing one or multiple serial ports, allowing it to interface with other devices using various networking technologies. They're mainly deployed as a management device, as it enables the user to monitor and control devices plugged in from a local or remote network. Our application uses this to interface with one or many devices and deploy them all at the

same time. This approach is extremely efficient and can save an engineer hours.

Due to the large number of console server manufacturers, this manual will not cover how to install and configure a console server.

However, there are three main pre-conditions needed to be satisfied for efficient operation:

1. There is a password protected user account set up, with administrative privileges.
2. The console ports can be accessed directly via an IP address, for example, `**username:port_number\@console_ip_address**`.
3. There is a sufficient number of console ports proportional to the number of devices to be configured.

3.Database server

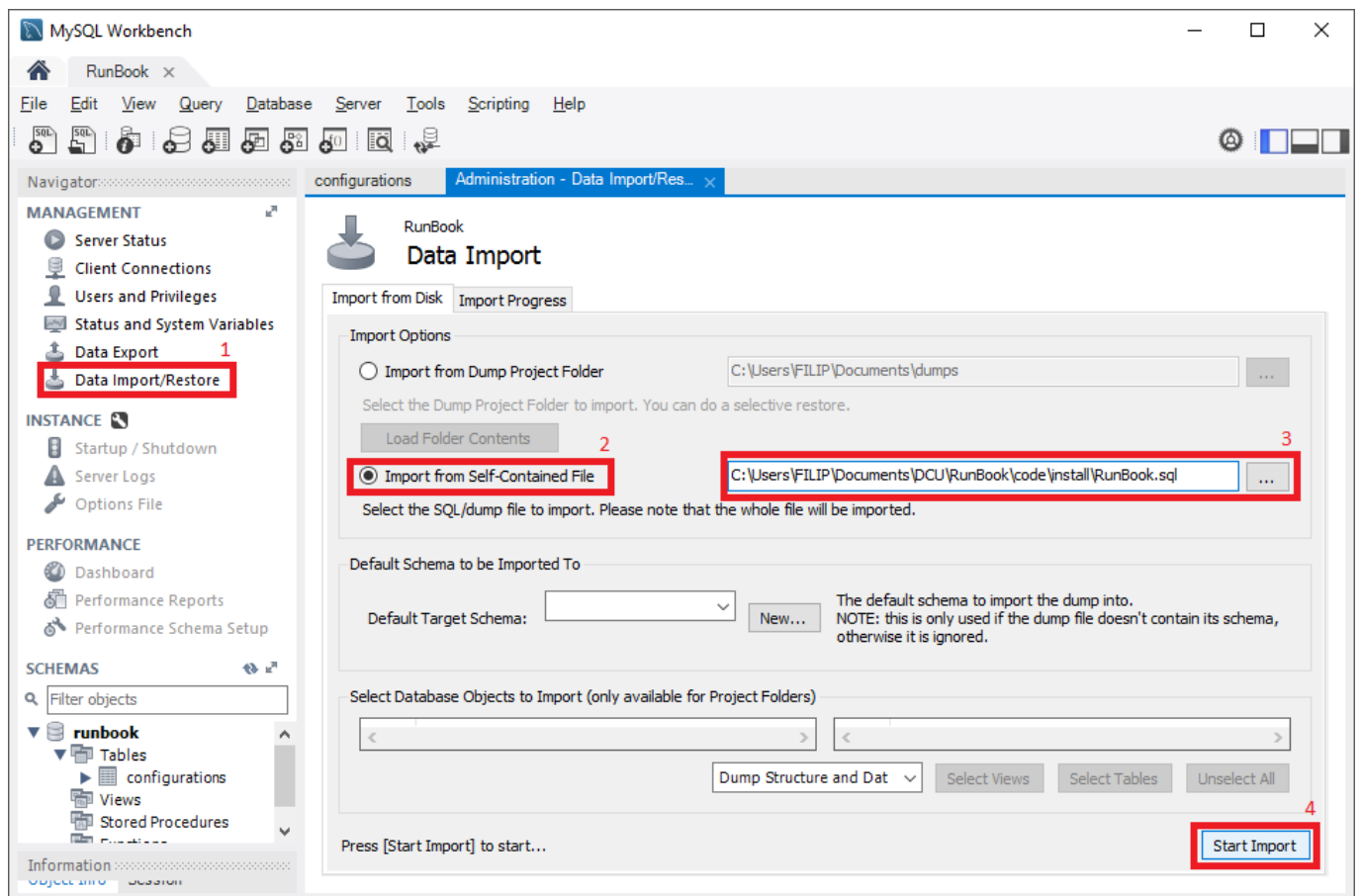
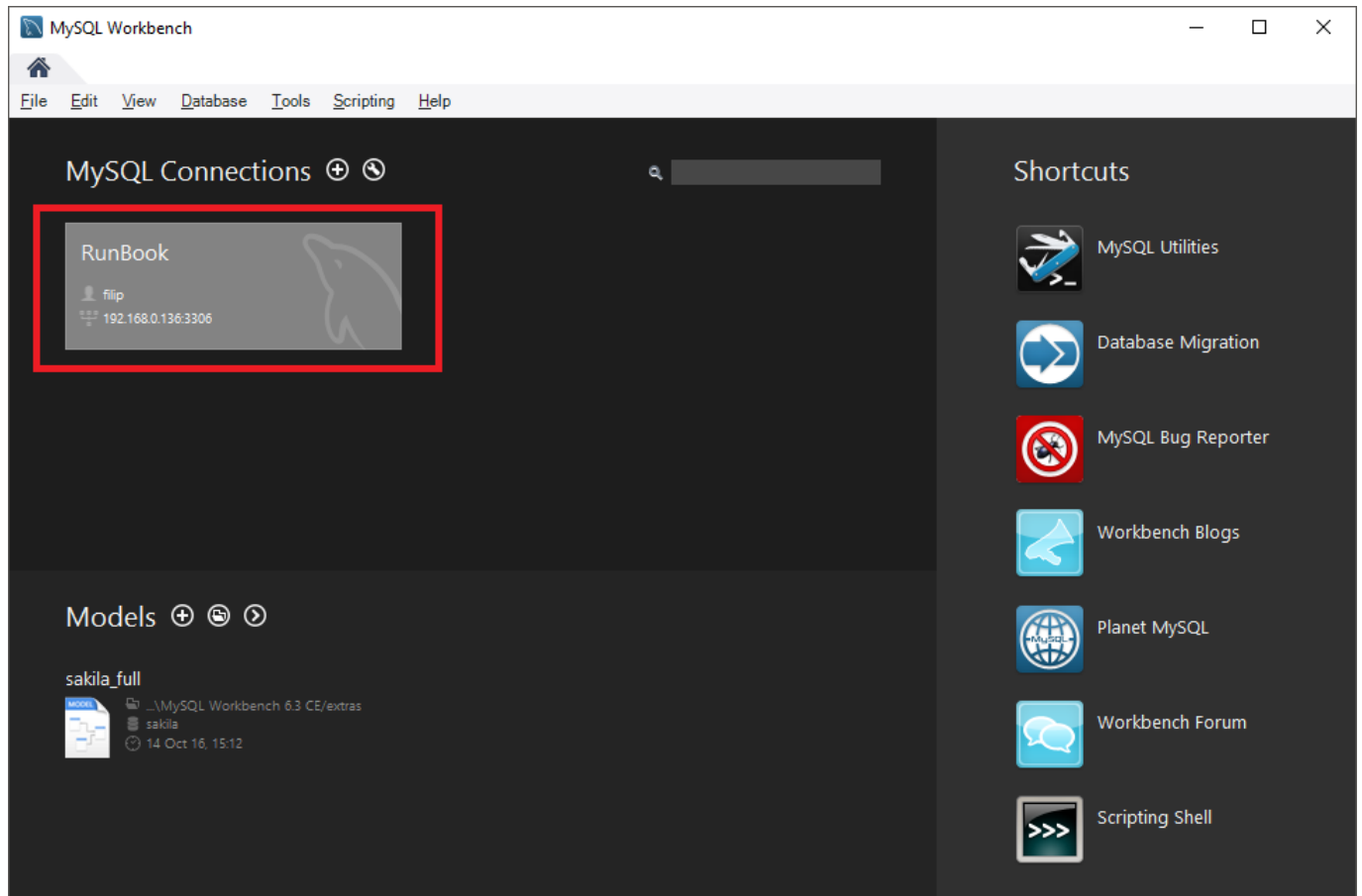
A database is made up of hardware/software using languages such as MySQL to store and access data from a local/remote location for tasks such as analysis, storage, manipulation and archiving. To allow us to use the core features of our application we require a database to store information about deployed devices along with additions to their configurations.

The database server setup is the responsibility of the network administrator and is required to be an SQL database.

*Two most popular server side solutions include MySQL Community Server for Windows based systems and mysql-server for Linux based systems.

In this demonstration, MySQLWorkbench client application will be used:

1. Connect to the SQL Server using a username/password
2. Import the provided SQL file from the `/code/install/RunBook.sql` file as outlined in the diagram below:



This completes the database set-up

5.Configuring initial application settings

1. FTP Configuration

1. Server Address - input the IPv4 address of the FTP server accessible to the application via your Local Area Connection.
2. FTP Username - enter the username of an account set up on the FTP server with file read, write and execute privileges.
3. OS Directory Path - used to store the Juniper Operating system (JUNOS) images. *Files are uploaded by the user used as input.
4. Configuration Path - used to store the configuration files and version control. *Files uploaded by the application.
5. Initial Configuration Path - used to store the configuration files and version control. *Files uploaded by the user used as input.

2. Console Server Configuration

1. Console Server Address - input the IPv4 address of the console server accessible to the application via your Local Area Connection.
2. Console username - enter the username of an account set up on the console server with the ability to access each console port individually.

3. Database Configuration

1. Database Address - input the IPv4 address of the database server accessible to the application via your Local Area Connection.
2. Database username - enter the username of an account with the ability to access the provided RunBook SQL database schema.

Network Deployment Automation Maintenance Tool

<

FTP Configuration

Server Address

FTP Username

OS Directory Path

Configuration Path

Initial Config Path

*This will be used to push and pull config files for your device as you work

Console Server Configuration

Full Console Address

Username

*To allow for bulk updates your console server's info will be required here

Database Configuration

Full Database Address

Username

*This database will be used to track updated devices and their config files as you work

Apply Settings

*Enter the DB and FTP server passwords which correlate to the provided accounts.

*You can also enter the settings screen by using the "Edit Settings" button.

Login Details

✓ Login Credentials

Database Password

FTP Password

Login

Edit Settings

6. Deploying devices

When networking devices are being set up they require the latest version of whatever operating system they're using along with the rules that the device will follow (it's network configuration). This needs to be done for every device that is being deployed and can be extremely tedious and time consuming. When deploying a device the only thing that changes is what operating system you're going to use and what configuration it's going to have, the commands to do all this stay the exact same. What our application does is remove the time consuming tediousness of these tasks and allows you to perform them on as many devices as your hardware allows with only minimal input from the user. Once you've selected what you want on each device we can run these commands along with the selected operating system and configuration.

- This module allows you to update the OS and configuration of desired Juniper devices, to streamline and automate this repetitive process.
- The two buttons carried across the application modules are *back* & *refresh*:



1. The first field is populated by the JUNOS file, automatically selected from the FTP server's *os* directory. Select the desired OS for the device via this drop-down.

1. *From Port No* - Input the first console port connected to the device to be configured.
2. *To Port No* - Input the last console port connected to the last device to be configured.

*If you are configuring only one device, enter the same value into the *To Port No* field.

*Ensure that the console ports chosen are sequential, for example port 23 to port 26 (three devices to be configured).

1. *Console Server Password* - this password correlates with the username provided in the settings menu under *Console Server Configuration*.
2. *Clone to Backup Partition* - most Juniper devices have a primary and backup drive partition, if you select this option, the operating system chosen earlier will be installed on the backup partition of the device, as well as the primary.
3. *Initial Configuration Range* - these two drop-down menus will contain configuration files from the FTP server's *Initial Configuration* directory.
 - Select the first configuration file to be applied to the device plugged into the first port of the console server, as selected above.
 - Select the last configuration file to be applied to the device plugged into the last port of the console server, as selected above.

*If you are deploying a single device, these two fields will contain the same configuration file.

*Ensure that the configuration files to be applied are in sequential order on the FTP server, as they will be applied to the devices in order.

4. Finally click *Begin Deployment* – the progress bar on the right will be updated, as the devices are being deployed.

Network Deployment Automation Maintenance Tool

< [Refresh]

Device Deployment Information

▶ From Port No. TO ▶▶ To Port No.

☐ Clone to Backup Partition

Initial Configuration Range (Optional)

▶

▶▶

Begin Deployment

Display Database

✓Deployment Progress

- Connect to the device
- Log in
- Downloading OS
- Installing OS
- Rebooting the device
- Logging into the device
- Applying the configuration file
- Rebooting the device
- Deployment Successful

By clicking the **Display Database** button, you will be able to view database entries, containing various information about devices deployed by the application.

Database Results

Name	Serial Number	User	Timestamp	Config Path	Entry Title	Description	Is Current Configuration
School	123456	filip	02-03-2017 09:43:29.15	/iniconfig/12007G-41221-srx300.conf	Initial Configuration	School Location	0
School	123456	filip	02-03-2017 09:45:44.33	/config/02-03-2017_09-45-44.conf	Small changes	Changed 2 lines	1

Export to CSV

7.Keeping track of the configuration files

Devices that are currently in the field are constantly changing in response to the ever evolving world of networking. This can be due to security reasons or an upgrade to a preexisting network. Devices will require a new configuration file and it would be in the owners best interest to keep track of the changes made to each device and by who. Our application allows you to do just that. You can keep track of and compare changes to files being uploaded and any user that does is

tracked.

- This module has GitHub like functionality, providing version control of configuration files applied to Juniper devices which have been deployed.

1. Select a local configuration file to be uploaded.
2. Enter the title of the commit.
3. Enter a detailed description, usually containing reasons for changes being made.
4. Choose the target device to commit to.
5. Select a commit to compare the local file to.
6. The green text shows what settings have been added into the new configuration file compared to the old one.
7. The red text shows what settings have been deleted.
8. Finally click the *Add to Repository* button.

*You will see the new configuration added under the *Commits* heading.

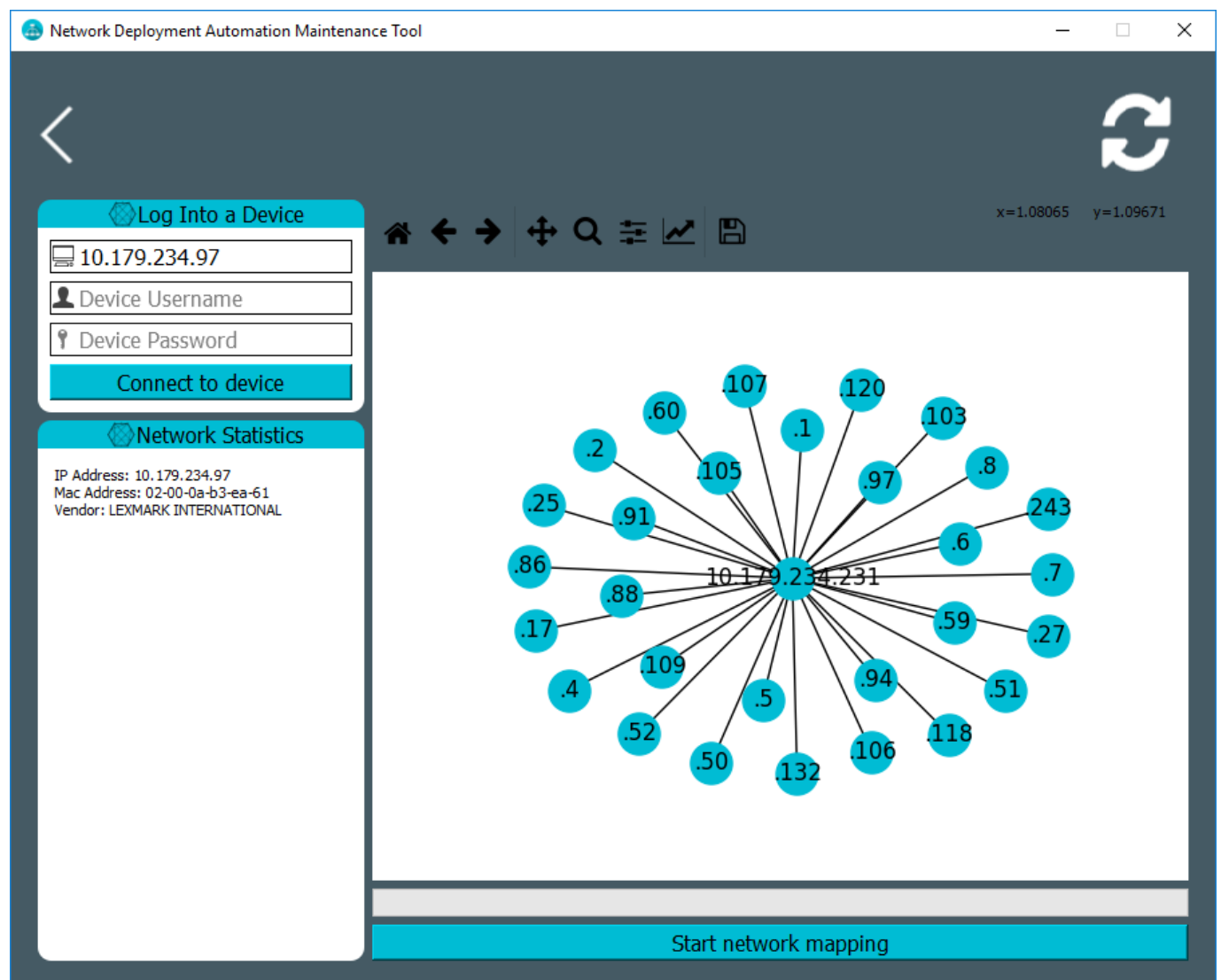
The screenshot displays the 'Network Deployment Automation Maintenance Tool' interface. At the top, three red callout boxes with arrows point to specific UI elements: 'Select a local configuration file' points to a text input containing '2007G-41221-srx300.cor'; 'Choose the target device' points to a dropdown menu showing 'School'; and 'Select a commit to compare to the local file' points to a list of commits under the 'Commits' heading. The main interface is divided into three sections. The left section contains a 'Commit Title' field and a 'Commit Description...' text area, with an 'Add to Repository' button at the bottom. The middle section shows a comparison of configuration files, with green text indicating additions (e.g., '+ @8: set system radius-server 87.32.12.15 source-address 87.37.152.89') and red text indicating deletions (e.g., '- @1: set system host-name s41221-cr'). The right section, titled 'Commits', lists two commits with timestamps: '02-03-2017 09:45:44.33' and '02-03-2017 09:43:29.15'.

8. Scanning a Local Area Network

One of the main tasks of a network engineer in day to day operations is troubleshooting a network.

This may have to be done in a variety of ways such as checking the status of the entire network or just a singular device. Our application removes some of the timeconsuming tasks surrounding this. By allowing you to scan your network you can see what devices are live, what device it is and what it's current status is if needs be.

1. Click the *Start network mapping* button.
2. A network map will be displayed, with the final byte of the IPv4 address marking each node. Your computer will be in the middle.
3. You can manipulate the diagram using the buttons located above.
4. The network statistics screen contains the device IPv4 address, MAC address as well as device manufacturer (*Vendor*).
5. If the device vendor is Juniper Networks and you have the correct login access, additional information will be displayed under existing network settings, such as:
 1. *Device Uptime*
 2. *CPU Utilisation*
 3. *RAM Usage*
 4. *Device Alarms*



9. Troubleshooting problems

- Cannot connect to the Database/Console/FTP Server □ use tools such as ping to determine whether you have a stable connection to these devices.
- Cannot see all devices on the network □ this may occur, as some devices might have *icmp* disabled.
- Running on VM □ as most VMs run behind a NAT connection, the network scanner functionality will not be available.

*Additional information available in the [Video Walkthrough](#) of the application.