COMP3000

Computing Project

2020/2021

Project Title:
NetManager: Network Configuration & Management Tool with Enhanced Security

Links:
Source Code: https://github.com/jwhite96/COMP3000

Backlog: https://tasks.office.com/live.plymouth.ac.uk/en-US/Home/Planner/#/plantaskboard?groupId=434e3152-1419-4e0c-b2c3-c4e0d0d4a459&planId=JwVQaMjgi06AWHtSP1mLf5YABBy3

Project Vision:
The continued growth in IT and the increase in users has led to larger and more complex networks making the management of these systems a challenge for networking professionals. Traditionally configuring a network requires direct access to the network hardware and configuring each device manually. This is both time consuming and prone to human error. A possible solution to this problem is Software-Defined Networking (SDN) which separates the data and control plane creating one centralised controller for the network. This allows for programmatically efficient configuration and easier management of the network. SDN can be used to build software applications that automatically configure networks, monitor network status and manage networks dynamically.

NetManager is a network configuration and management tool (NCM) for automatic configuration of a network and dynamic management of a network topology. This application will assist networking professionals in monitoring and controlling their networks as well as enforcing security policies by automatically implementing network security features (e.g. access lists, port security etc.). NetManager will include an easy to use graphical interface that utilises a Python programmed API that will gather information and pass commands to and from the network hardware. From the GUI, users will be able to view the network topology, monitor network performance, manually and automatically make configuration changes and implement network security features. This application will also feature an auditing system for logging recent activities such as device updates, configuration and/or topology changes and known security threats allowing system administrators to maintain greater control over their networks.

Applications using the software defined networking architecture are becoming more widely used in modern networks today. They greatly improve the speed and efficiency of network configuration, monitoring and management. Using programming to automate many networking processes and features allows one centralised controller to oversee and control the entire network providing increased network performance and improved scalability.

Risk Plan:

Risk ID	Risk Category	Risk Description	Impact Score (1-5)	Likelihood %	Risk Rating	Risk Response	Contingency Plan
Project Execution							
R1	Project Execution	Project too complicated/difficult to complete	5	25%	1.25	Risk Avoidance	Thorough technical analysis and prototyping
R2	Project Execution	Run time performance issues	3	25%	0.75	Mitigation	Code optimization and software changes to improve performance.
R3	Project Execution	MVC compatibility issues	3	40%	1.2	Mitigation	Adequate testing during each development stage to check each component is compatible
R4	Project Execution	Project not within scope	3	25%	0.75	Risk Avoidance	Ensure project is still within scope during supervisor meetings
R5	Project Execution	Changes to different technologies during development	2	35%	0.7	Mitigation	Integrate new technology where possible into existing project
Personnel Risk							
R6	Personnel	Insufficient knowledge to complete system requirements	4	25%	1	Risk Avoidance	Ensure enough research is carried out before development begins (mostly during sprint zero)
R7	Personnel	Unexpected illness or personal issues	2	30%	0.6	Mitigation	Alter current schedule and pushback tasks into next sprints if required
Schedule Risk							
R8	Schedule	Unexpected server downtime/maintenance	1	50%	0.5	Acceptance	*None*
R9	Schedule	Time constraints due to other commitments	3	30%	0.9	Mitigation	Improved planning and alteration to current schedule
R10	Schedule	Issues related to the COVID-19 Pandemic	2	60%	1.2	Mitigation	*Dependant on restrictions and changes*
Compliance Risk							
R11	Compliance	Potential copyright infringement with similar products	1	25%	0.25	Acceptance	As this is project is for educational purposes this risk can be accepted but will still need to be taken into consideration during development and/or before any real-world deployment

R12	Compliance	Unintentional regulatory noncompliance's	1	10%	0.1	Acceptance	*Same as above*
Loss							
R13	Loss	Accidental loss of work	3	20%	0.6	Mitigation	Create multiple backups to keep loss to a minimum
R14	Loss	Theft/Fraud	4	10%	0.4	Acceptance	*Same as above*

Risk Plan Key:

Risk Category	Definition
Project Execution	Risks affecting the development of the project e.g. systems, technologies, code etc.
Personnel	Risks affecting the human aspect of the project
Schedule	Risks that could affect the schedule and cause time delays during development
Compliance	Risks associated with failure to meet regulatory/industry standards and/or legal requirements
Loss	Risks related to the loss of work, hardware or data

Risk Response	Definition
Risk Avoidance	Eliminating the risk before it occurs
Mitigation	Reducing the damage caused if this risk occurs
Acceptance	Accepting the risk if it occurs

Probability Level	Range
High	Greater than 50%
Significant	30-50% chance
Moderate	10-29% chance
Low	Less than 10% chance

Keywords:

Network, Networking, Network Management, Network Configuration, Network Monitoring, Python, Software Defined Networking, Network Security, Routing, Switching, IP Addressing, GNS3, Cisco, Wireshark