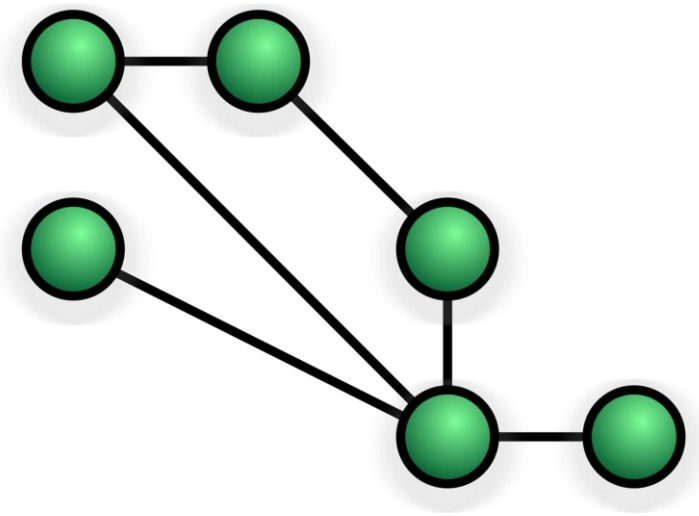
Network Scripting Management

Final Project – Technical Report



Written by: Areeb Abubaker

Date: March 15 2023

Blank Left Intentionally

Executive Summary

I'm happy to offer this report outlining the needs and strategy for developing a web-based network management system because I'm a voracious learner and devotee of network scripting and management. Fault, Configuration, Accounting, Performance, and Security Management elements are all included in this project demonstration, and each feature has been meticulously created to seem appealing to the end user. On the fault management page, link up and link down events are automatically identified using Python scripts in a user-friendly way with red and green color indicators. Network interfaces may be easily provisioned and modified thanks to the Configuration Management page, which also shows device configuration information and system updates.

The Performance Management page comprises Throughput, System Load Report, and RTT Report, all of which make use of the capability of Simple Network Management Protocol (SNMP) for effective data gathering and analysis. The Accounting Management page offers detailed usage reports.

The showcase also demonstrates the use of Python, automation, SNMP, and scripting. This project is a testament to my dedication to mastering network scripting and management. With a well-designed webpage that is both easy to use and navigate, this showcase demonstrates my proficiency in developing innovative solutions for complex network management challenges.

Introduction

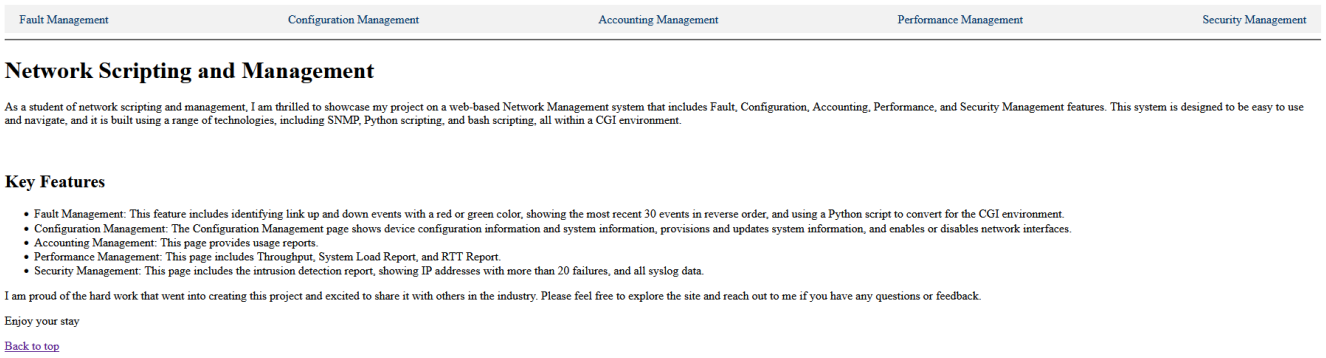
My first steps within the field of network engineering and security are represented in this report. I've been requested to write a report about my experience learning HTML, CSS, and scripting in the context of networking because I want to be a network engineer. This project gives me the chance to explore and understand the fundamentals of network automation and web design since it is my first experience working with these technologies.

This project will only be the beginning for me and that, as my expertise and understanding increase, so will the breadth of my work. But, I'm eager to take on this task, and I think the knowledge I'll gain from it will be useful as I advance in the field of network engineering and security.

Navigation Tree

- *Fault Management*
- *Configuration Management*
    - *IP Routing Table*
    - *ARP Table*
    - *MAC Address Table*
    - *Interface Table*
    - *Cisco Discovery Protocol*
    - *Update Network Device Information*
    - *Network Interface Configuration*
- *Account Management*
- *Performance Management*
    - *Network Throughput Report*
        - *Switch-01*
        - *Switch-02*
        - *Switch-03*
    - *Linux 05 System Load Report*
    - *Network Research Lab RTT Report*
- *Security Management*
    - *Security Report*

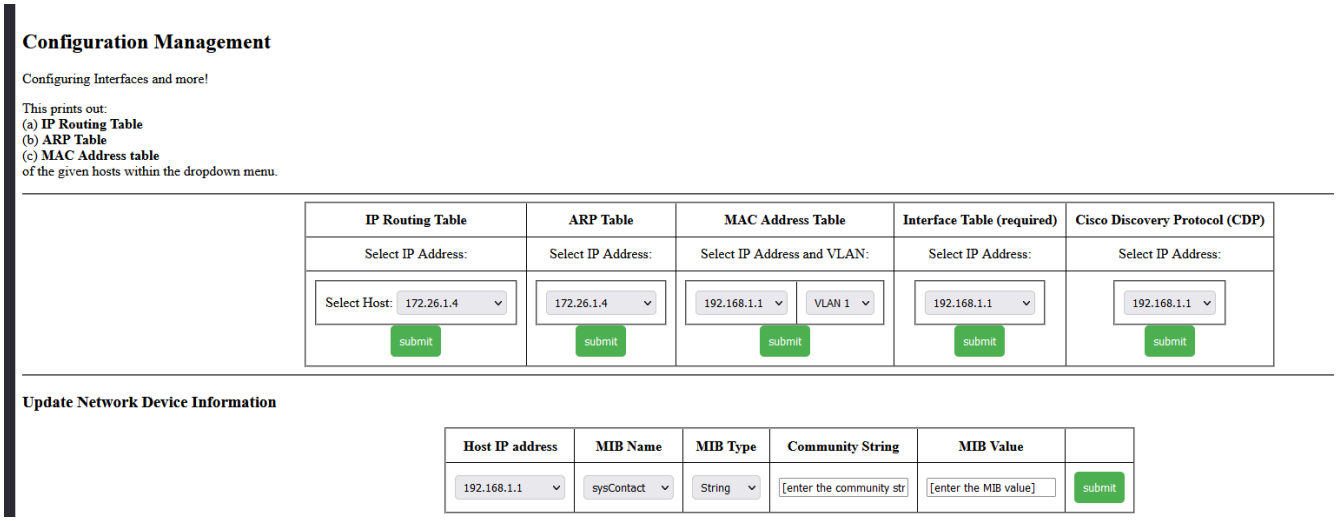
Demonstration



This is the Homepage upon visiting the stie.

Date	Time	Device	Interface	Status
2023-03-15	22:24:16	192.168.1.1	FastEthernet0/22	Link Up
2023-03-15	20:31:24	192.168.1.1	FastEthernet0/22	Link Down
2023-03-15	19:54:48	192.168.1.1	FastEthernet0/22	Link Up
2023-03-15	19:54:38	192.168.1.1	FastEthernet0/22	Link Down
2023-03-15	18:31:35	192.168.1.1	FastEthernet0/22	Link Up
2023-03-15	18:31:11	192.168.1.1	FastEthernet0/22	Link Down
2023-03-15	18:22:46	192.168.1.1	FastEthernet0/22	Link Up
2023-03-15	18:22:19	192.168.1.1	FastEthernet0/22	Link Down
2023-03-15	18:19:35	192.168.1.1	FastEthernet0/22	Link Up
2023-03-15	18:19:25	192.168.1.1	FastEthernet0/22	Link Down
2023-03-15	18:18:30	192.168.1.1	FastEthernet0/22	Link Up
2023-03-15	18:14:35	192.168.1.1	FastEthernet0/22	Link Down

This is the configuration information in the Fault Management using SNMP Traps



This is the Configuration Management section in which you can view various device information given IP addresses or VLANS. The section below of updating network device information has yet to be implemented but ensures there are no crashes when the selection is chosen.

Account Management

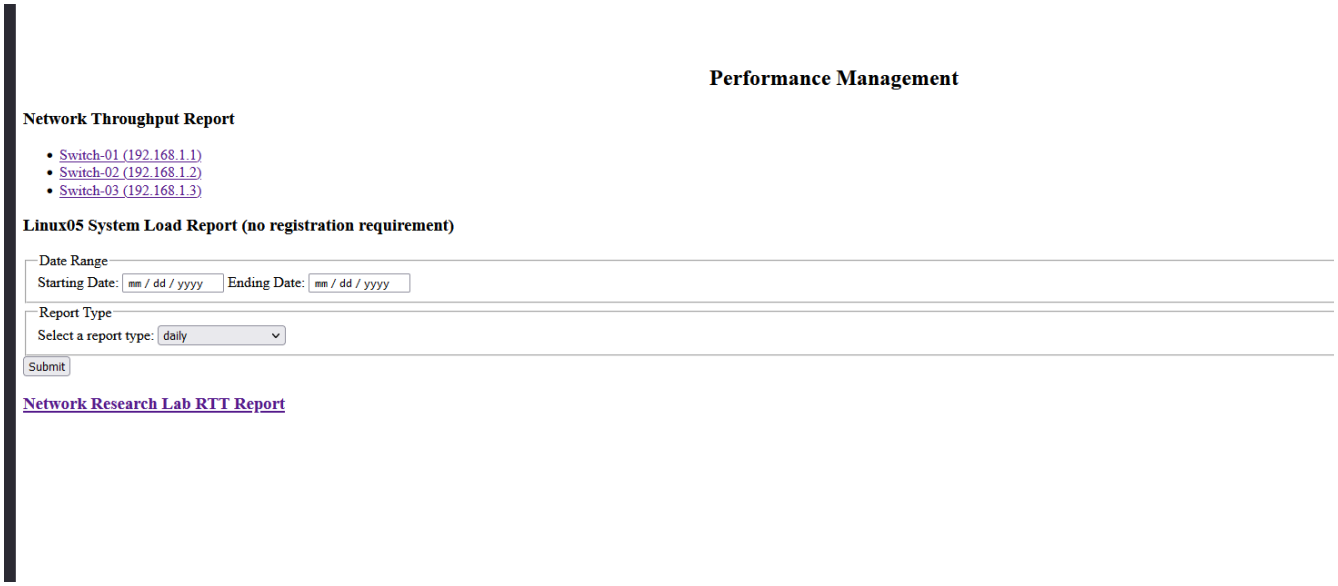
- Fault Management
- Configuration Management
- Accounting Management
- Performance Management
- Security Management

Account Usage Report

Session Information

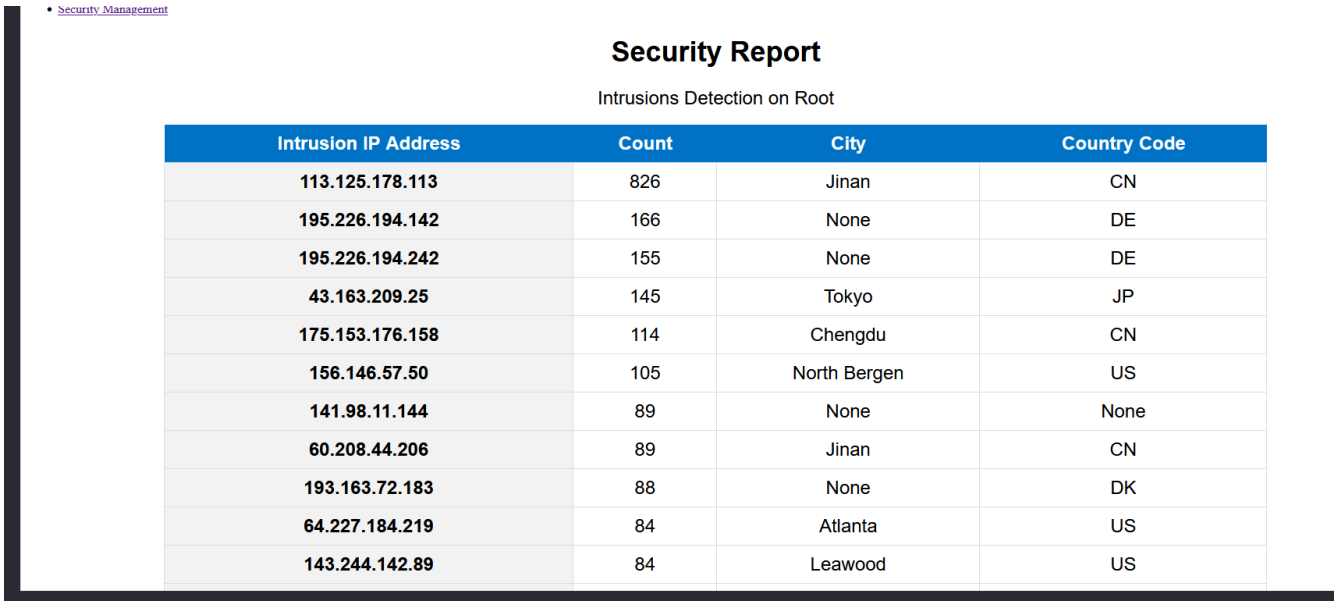
Account	Count	Total Time	Average
achung	3152	10085.00 seconds	3.00 seconds
net484s01	1085	217985.00 seconds	200.00 seconds
net484s02	3167	300447.00 seconds	94.00 seconds
net484s03	1124	436650.00 seconds	388.00 seconds
net484s04	1061	165596.00 seconds	156.00 seconds
net484s06	1060	279476.00 seconds	263.00 seconds
net484s08	1059	68028.00 seconds	64.00 seconds
net484s11	1136	132575.00 seconds	116.00 seconds
root	5035	28.00 seconds	0.00 seconds

This is the usage report of each user, given how many times they have logged on in the week and their average time per session.



This is the Performance Management section in which you can the Network Throughput reports, and system load reports given a certain date range.

At the end, you can see if the Round Trip Time (RTT) formatted in a simple manner to ensure devices are up and now slowed down within the subnet.



- Security Management

Security Report

Intrusions Detection on Root

Intrusion IP Address	Count	City	Country Code
113.125.178.113	826	Jinan	CN
195.226.194.142	166	None	DE
195.226.194.242	155	None	DE
43.163.209.25	145	Tokyo	JP
175.153.176.158	114	Chengdu	CN
156.146.57.50	105	North Bergen	US
141.98.11.144	89	None	None
60.208.44.206	89	Jinan	CN
193.163.72.183	88	None	DK
64.227.184.219	84	Atlanta	US
143.244.142.89	84	Leawood	US

Finally, this is the security report part of the showcase as it shows how many times an attempt was made to login to the root user on this device. It has been sorted to only give amounts greater than 20 and give a country and city of origin.

Conclusion

As I develop more expertise and understanding in networking and security, I anticipate continuing to hone and improve the report, webpage, and scripts. I can automate repetitive and time-consuming tasks by using scripting, freeing up my time to focus on more complex and critical security and network management issues. As a security and network engineer, this will improve my efficiency and productivity and enable me to better defend my network against online threats.

I will also be able to design increasingly complex scripts and tools as I continue to hone my abilities, like automated vulnerability scanners, intrusion detection systems, and incident response playbooks. These technologies will enable me to identify and mitigate security issues more quickly and effectively.

This course in my DePaul journey has shown me how to become more proficient in scripting and network management. By consistently enhancing my knowledge and skills, I can contribute to the larger objective of making the internet a safer and more secure place for everyone while also assisting in maintaining the security and stability of my network.