

plagiarism report

by Plagiarism Report Plagiarism Report

Submission date: 25-May-2019 08:14 AM (UTC-0500)

Submission ID: 1135784414

File name: IT_345_Milestone_One.edited.docx (14.51K)

Word count: 1308

Character count: 7057

Title: IT 345 Milestone One

Name:

University:

Course:

Tutor:

Date:

¹
IT 345 Milestone One

Executive Summary

Network Performance Analysis: FreshSource Distribution Inc. has been a medium-sized company but has recently been quickly expanding and growing each year. Due to this quick expansion, the original network which supported the firm is not able to keep pace with the dramatic growth. The existing network environment and infrastructure is utilizing legacy equipment which is slow as well as outdated. This is likely to cause degradation within the network quality of the company. If the current trend continues, the network will be unable to effectively support the level and kinds of network traffic which the users will be generating.

To address this issue, FreshSource Distribution Inc. is planning for network upgrades. ¹The company currently has a wide area network (WAN) connectivity in its three warehouses, utilizing linked ¹128 Kbps ISDN lines. Each warehouse also has a local area network (LAN) which is linked to the external-facing router. The data center of the company is in Florida, which is the central warehouse. The other two warehouses are supposed to synchronize their activities and ¹inventories with the major inventory control servers located at the central warehouse. Since these files are continuously becoming bigger in size as well as taking too much time to synchronize, the company has realized that there is a need for network upgrades.

¹**Root Causes:** the root causes of problems the firm is facing include the consistent expansion and growth of the company. Despite the company seeing vibrant business growth as well as expanding hiring by about 10% to 15% every year, the company is still utilizing legacy equipment which is outdated and slow. This expansion in business and employees has also resulted in more users, who are generating more traffic in the company's network. Furthermore,

the inventory files from the two warehouses which need to be synchronized with inventory control server in the central warehouse are also becoming large in size as well as taking too long to synchronize for the company's WAN.

The other notable root cause of the problem is the fact that all sites or warehouses have to ¹access the internet via the central location or the ¹datacenter of the company. The internet connection encompasses a single 128 Kbps line. This is causing degradation in network performance as well as causing more traffic in the network of the company. Moreover, the network administration employees have noted numerous unwanted devices trying to access their and connect to the internal network by continuously trace routing and pinging the external router. That issue has raised a security issue with the company's management as well as caused degradation in ¹network performance.

Continued Impact on the Business: the continued impact which FreshSource Distribution Inc. may experience includes network slowdown. The network will continue to report an increase in latency and users from different network locations will also report various network slowdown. The other notable impact on the company will be disconnections since some users will often experience disconnections from the network, although they might be able to reconnect afterward (Kino, 2011). The other problem will be outage since the network services will be becoming unavailable to certain users or sites at a specific point in time. Another problem will be end-user complaints. The company network administration staff will be getting reports that some users or even sites are complaining about various slow response times, although they might be not giving sufficient details that can help in identifying the slowdown scope.

Furthermore, the network might cause propagation delays in the IT infrastructure as well as problems with network routing. The IT system will continue causing different types of delays and end-point problems. This will be partly due to the fact that data destinations will be experiencing delays as a result of lack of enough processing capacity or memory of the network. But although hardware device problems may not depress functionality in the entire network, some problems can depress functionality of the entire network. For example, data packets fragmentation problems can have an impact on entire network performance (Kino, 2011).

¹
Business Needs and Initiatives: the **business needs** which should **be met by the network architecture** include improving the reliability, performance as well as security of the network. The effective way of getting more performance from the network will be by improving the performance of both WAN and LAN. This will be addressed by ensuring good architecture encompassing things such as 100-Megabit or even various Gigabit Ethernet switches that have VLAN capabilities (Cheminod et al., 2012). These network devices are vital for various surfacing network technologies which place more emphasis and demand on various networks. Since switching and latency are vital, there is a need to have a network core and switches which can effectively support them.

The other important business need for the network upgrade is reliability. It is important to ensure the company has a reliable network as well as a high-functioning router. For example, it may be important to ensure the company has something which is Cisco quality and to have more control and granularity to go into its warehouses' routers in order to control its traffic more effectively (Kino, 2011). Furthermore, the next important business need involves security. It is necessary to ensure everything moves via the same pipe and is unified, as well as ensures the business has a dedicated firewall. There is a need to get a purpose-built firewall that can be deployed as a

separate tool to support firewall processing. This will ensure that the firewall is focusing on various types of traffic as well as ever-increasing threats which come via the network (Cruz et al., 2015).

Security Standards and Best Practices: a vital security standard would be ensuring device security. As a best practice, it is important for the company to ensure device security as a means of helping to block or prevent potential intruders from accessing crucial data of the company. Companies need to protect certain known vulnerabilities including open UDP and TCP ports and open serial ports as well as places to put or inject various code including web servers and unencrypted communications. The other best practice to ensure device security is by upgrading them or even deploying security patches as required. It is important to determine the security capabilities of various devices before investing in them (Cheminod et al., 2012).

The next important thing is ensuring network security. The company, as well as other firms, should ensure the networks which they utilize for ICT are secure. This may entail the utilization of strong access control and authentication mechanism to ensure only authorized users are the ones who can gain access to data and network of the company (Kino, 2011). The other important security standard is protecting data of the company. The company including other companies should secure their ICT data themselves. Numerous connected devices and tools will be transmitting and storing sensitive and personally identifiable data, and this data should be strongly protected. By failing to protect this data, a company cannot only face negative business effect but also various regulatory penalties. Furthermore, good security as well means companies should have strong security operation policies put in place (Cruz et al., 2015). This security standards as well as best practices are not specific to this company but can also be applied by any other company in any other industry.

References

- Cheminod, M., Durante, L., & Valenzano, A. (2012). Review of security issues in industrial networks. *IEEE transactions on industrial informatics*, 9(1), 277-293.
- Cruz, T., Barrigas, J., Proença, J., Graziano, A., Panzieri, S., Lev, L., & Simões, P. (2015, May). Improving network security monitoring for industrial control systems. In *2015 IFIP/IEEE International Symposium on Integrated Network Management (IM)* (pp. 878-881). IEEE.
- Kino, T. (2011). Infrastructure Technology for Cloud Services. *Fujitsu Sci. Tech. J*, 47(4), 434-442.

plagiarism report

ORIGINALITY REPORT

11%	0%	0%	11%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Southern New Hampshire University - Continuing Education	11%
	Student Paper	

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	On		