Strategic Planning and Monitoring of Network Design

Yiqiao Yin
Ph.D. Student

Abstract

This paper discusses and explores the model architecture of network types. The premise assumes that the role is to create a training document to explore some network types and topology with the interns at a large company. To achieve this task, this paper investigates and provides in-depth overview of the different network types and topologies.

1 Background

This final paper provides thorough investigative work of the network operations strategy to develop proactive plan to monitor the network performance. The content of this paper is to provide design and to build the strategic planning. In addition, the paper provides monitoring system of the proposed network design. It is designed and built upon the foundation of all the previous assignments. The work builds on a variety of understanding including network design, network topology, and network reliability. The plan is to design a real-time monitoring system to measure the network performance and availability. The security of the network is part of the equation as well and will be proactively monitored.

1.1 Summary of the Organization Business Demands

This paper investigates the requirements of the network system that is to be implemented in the company (throughout the rest of the paper, we refer the "company" to be the target company with simulated assumptions in the assignment). The company has an existing WAN that provides internet services with the entire Northeastern region. The region currently covers 12 branches. After the acquisition, the projection is to expand the network services with 30 additional locations and these are sites that cross multiple different states under the same region.

The goal for this investigation is to provide the basic understanding and the premises required for this expansion. A complex and adaptive system is to be designed for this implementation. A research done in 1979 first recognized the importance of the characteristics of such expansion [8]. It states the phenomenon that though the system can be easily understood at a local level the whole system may work in a surprising way globally due to local interactions amongst different units.

1.2 Network Performance Monitoring Tools and Probes

In the beginning stage of development, the network monitoring is extremely delicate and challenging. Considering that the premises states that we are a company operating 150 branches across multiple states in the northeastern region of the United States. The environment is the first thing to discuss and all applications distributed need to be delivered to each station and branch with timely manner. The overall goal is to measure the performance issue as well as a set of other different metrics by supervising the capabilities of network probes. Many scholars have been investigating the systems that adapt large-scale network mapping and the capacity to handle different variety of resources [11, 14, 20].

It is proposed a novel solution to measure the network performance by capturing its traffic [23]. When the network probes are available and there is no online traffic required to be measured, the active probes are then recommended to provide a variety of different measures [12, 23]. In our case, this solution is recommended to be put to test case. This is because the solution can be an ideal candidate for the scalability of network that is desired to be measured. With over 150 sites traveling all at once, the information hub can really deliver some surprising impact and hence affect the network performance issues. A solid monitoring system needs to be put to place and proposed a solution especially for this case, because their work targets on the flexibility of the network architecture [12]. The network needs to modify the strategy to adapt to different runtime issues and the potential roadblocks of unavailable bandwidth. Second, the reporting cannot be neglected either, because it is an important step leading to critical performance issues.

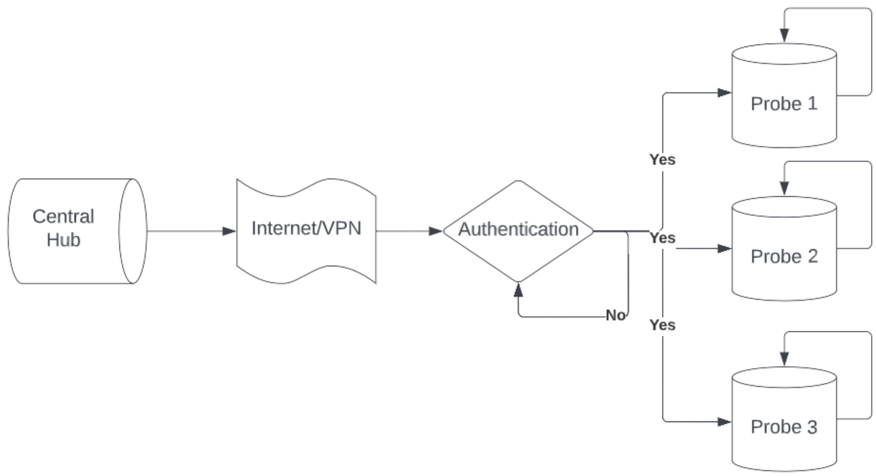
One additional concept to discuss in regarding to network performance monitoring tools and probes is the user-level information. This is referring to the specific bandwidth and data transferring efficiency at a level that is benchmark to each user. This can be an important benchmark and metrics to evaluate when it comes measuring large-scale performance issues. Not only do we want to ensure the WAN operates globally without interruption we also want to ensure at a user level contingency plans are at place when any malfunction occurs. MAGNeT allows the network signal to passes through the web traffic and then it measures and categorize the signal. Hence, it is pruned to understand the issues between each layer of stacked internet protocols. LTT, alternatively, is widely used for debugging purposes and it is popular for collecting information on a global level instead of trivial information from each connection. Hence, a network operating system (NOS) is setup using a prototype that is presented in Figure 1.

Many other tools [13, 12, 6, 21, 3] that are available for us are the following. The Web100 tool provides a variety of different instruments to measure network connectivity issues [13]. For kernel based tools, MAGNeT and the Linux Trace Toolkit (LTT) can be potential contenders [12, 6].

1.3 Connection to the Northeastern Region

The first premise is regarding to Wide Area Network or WAN. Many scholars have discussed different approaches of management system [17, 9, 18]. The target expansion that the executive team is planning on is a direct application of Wide Area Network (WAN) covering the entire Northeastern region. The network is capable of spanning a large amount of geographical area such as different cities, states, and other locations even nations. WAN is the optimal choice for corporations, multi-location companies, large organizations co-operating amongst different locations to execute data exchange.

Figure 1: **Network Operating System (NOS)**. The central hub initiates the signals. The signals goes through the cloud for authentication. When successfully approved, the information is then released to each probe.



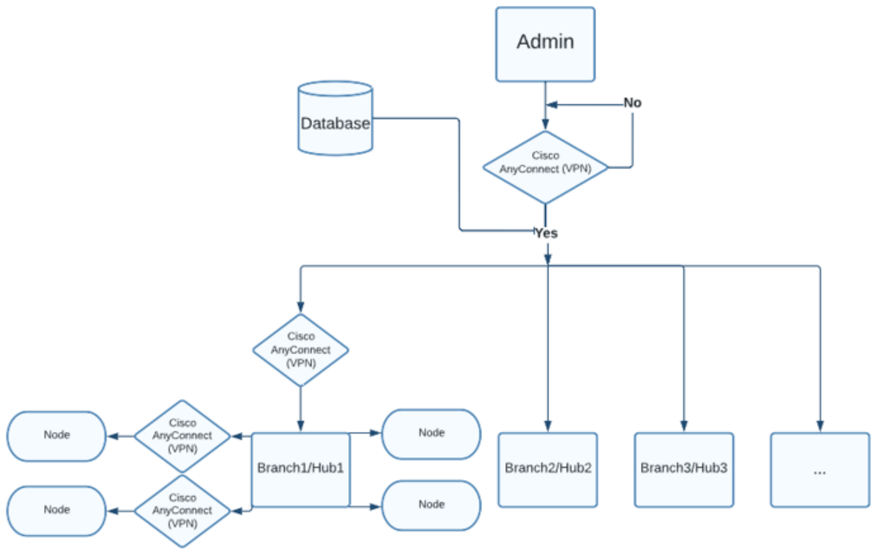
Comparing with the other types of networks, WANs serve similar purpose to that of LANS. However, WANs fundamentally has a different structure and the operating procedure is different as well. The branches of a WAN does not take ownership of the connections or the remote computer systems. Instead they are acting as subscribers. A service is provided to the these subscribers (branches). The data transfer speed is mostly about 1.5 megabits per second (Mbps) or less.

The profiling for WAN is point-to-point. This is based on a procedure that is able to divide digital service. It can split a digital service wire with a rate of 1.544 Mbps into many channels. These channels are technological profile with 64 Kbps each assuming it is split into 24 channels. In addition, cost is another contributing factor. For faster wire connection, the cost is higher. The setup can be quite substantial for a company with this size. A report has projected a 30% growth on the WANs implementation nationwide [7] and due to the amount of branches the executive team is planning to operate WAN is the appropriate choice for the expansion.

1.4 Summary of the Recommendations to Address Business Needs

First, the proposed network topology (see Figure 2) organically integrate the administrator and company officials with the internet providers in a secure environment. In addition, the data transfer and distribution has been safely provided to each branch and distributed to each node branch. A network service provider workflow is also provided to address the source of the internet provider (see Figure 3). In addition, to feed the company secure internet connectivity services, an executive diagram of the internet path is provided to address this issue (see Figure 4). The web service road-map is also provided with a workflow chart (see Figure 5). To allow successful data storage and optimal bandwidth control, executive diagrams of data storage and bandwidth are provided with or without the virtual machine in place. Due to the complexity of data security using scientific computing and data transfer, additional private network system such as VPN are provided to justify the difference (see Figure 6 and Figure 7).

Figure 2: **Executive Diagram of the Proposed Network Topology**. This figure presents the proposed network topology.



2 Comprehensive Network Design Architecture

The proposed network topology is presented in Figure 2. The topology suggests a hierarchical design branched out with a star design. The hierarchical design is appropriate for the hierarchy of the company organization. The company has more than 150 branch sites and each sites would need to have their own internet probes. It is important to ensure a failure of a site does not automatically affect the rest of the sites to ensure the secure data transfer and distribution protocols. Hence, the the hierarchical design is in place to achieve this goal. In addition, at each site (represented by the center or main hub of each branch), there is a start design. This proposed architecture is set in place because of each node carries important weight in the branch. This could be a desk or an office where a customer manager is making deals with a client. To ensure the most optimal service is provided to our clients, a node (which can be a desktop for a customer manager) should have its own independent connections with the hub and a failed connection should not affect the rest of the workflow.

2.1 Suggested Management and Monitoring Tools

First, the proposed management team is required to start an official business contract with a third party network provider such as Verizon and AT&T. A pricing and availability platform is strongly recommended to be set in place to allow continuous monitoring of the service plan. The subject matter experts and IT professionals need to be employed and to be put in place at service to ensure continuous internet provider. The optimal internet connection down to branch level is designed strategically to allow the company to work with the internet provider and its employees. The optimization is key in this scenario due to the highly customized nature to accommodate the personalized system of over 150 branches. This workflow is proposed in Figure 3.

Figure 3: **Executive Diagram of Internet Source**. The figure suggests the potential road-map required to hire a third-party to provide internet services.

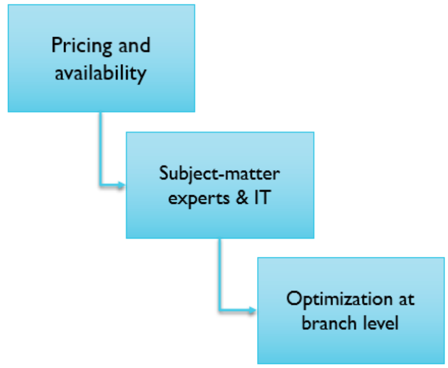
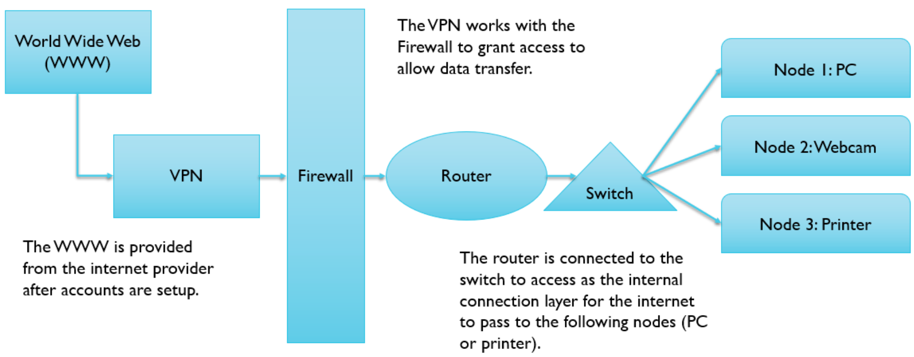


Figure 4: **Executive Diagram of Internet Path**. The figure suggests the core path of how the internet plugs into the company and distribute the data.

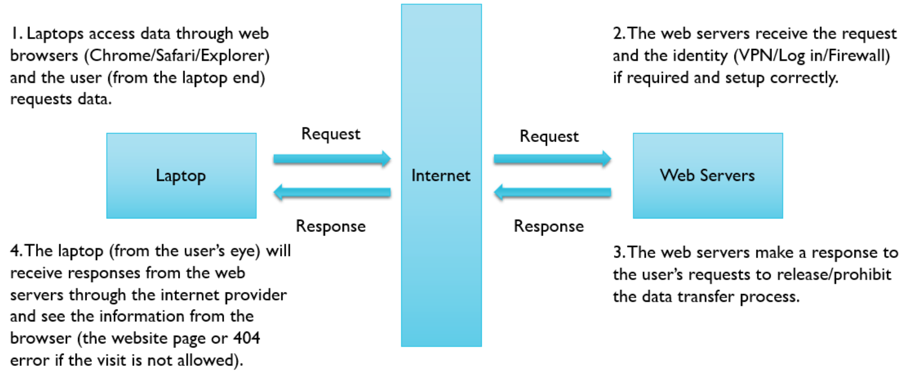


Next, the core internet path is addressed. This paper provides an executive diagram for this strategic plan and the figure is presented in Figure 4. External to the company, the World Wide Web or WWW is the source where we upload and/or download data and other information. A Virtual Private Network or VPN is required to be set in place. For example, a third party provider such as Sysco AnyConnect can help achieve this goal. The Firewall is set up with the VPN to filter and allow approved information to pass through. The connection is then linked with a Router where the Router can send the information through a Switch to different nodes. A node can be a machine such as a desktop/laptop, printer, or webcam.

2.2 Identification of Security Risks, Implications, and Risk Mitigation

To identify the security risks, implications, and to develop a risk mitigation strategy, it is important to understand the relationship between each machine such as a laptop and the web servers. This relationship is described in Figure 5. This is a 4-step process. First, the machine (such as a personal laptop) needs to access data through the web browsers. This can be a browser such as Chrome, Safari, or Internet Explorer. The user requests data from the end of the laptop. The signal gets sent through the Internet of which it requests the data from the server. This leads to the second step. The web servers receive the request signal that needs to be processed. Upon approval of the requests, a VPN or

Figure 5: **Executive Diagram of Web Servers**. The figure suggests the potential relationship and procedural steps required to establish web servers.



log-in information is verified for the particular data request. Then the web server will make a response which is the third step. The action is either to release the information or to prohibit the data transfer process. Last, the laptop from the user side will receive the information and the browser will present the information in front of the user. In case of failed approval or rejection of password, a 404 error can occur to indicate to the user that the web browser is not allowed.

2.3 Storage Capacity, Bandwidth, and Latency Considerations

This subsection discusses the contents of the storage capacity, bandwidth, and the latency considerations. One important caveat is the inclusion of a virtual machine or scientific computation in the system. To cover all basis, this paper provides both workflow. The diagrams are presented in Figure 6 and Figure 7. First, the diagram without the scientific computing virtual machine is provided. The users and the bank employees from the branch request data upload or download. This request is verified through a VPN and the signal is transferred to the cloud storage platform requesting release of the data. The cloud storage is connected many buckets where each bucket is a virtual folder for data storage. Next, the upgraded diagram with the scientific computing virtual machine is also provided. Every other building block is exactly the same with before. The additional piece is the introduction of a virtual machine. The communication between a virtual machine and the data storage is required to be verified with a VPN in the middle.

Researchers analyzing credit card defaults use machine learning techniques to understand the important features affect the probability of the credit card default level [16, 5]. To conduct this part of the research internally using internal data, the cloud storage platform with bucket locations is not sufficient for this type of scientific computing. Virtual machines are required to be set in place to allow large-scale data processing. This requires updated workflow diagram which can be seen in Figure 7.

In addition, the internet connection should be able to allow online conference. This was especially a changing point and a shift of culture during the pandemic of COVID-19 for many companies. Due to the pandemic, the policy of working from home or WFM is implemented so that people can create a somewhat distant environment to stop the spread of the disease. This requires the online platform to have strong, robust, and consistent internet connection to establish this platform as a response to the implemented policy. The diagram, in Figure 8, presents the workflow of a proposed online conference

Figure 6: **Executive Diagram of Data Storage and Bandwidth**. The figure illustrates the proposed relationship between users and online data storage platforms without cloud computing.

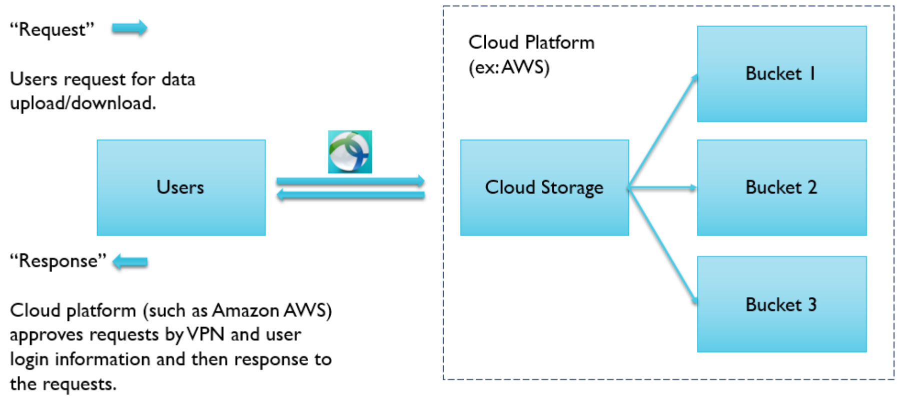


Figure 7: **Executive Diagram of Data Storage and Bandwidth (with computing)**. The figure illustrates the proposed relationship between users and online data storage platforms with cloud computing. A virtual machine is needed to establish a secured platform for scientific computing.

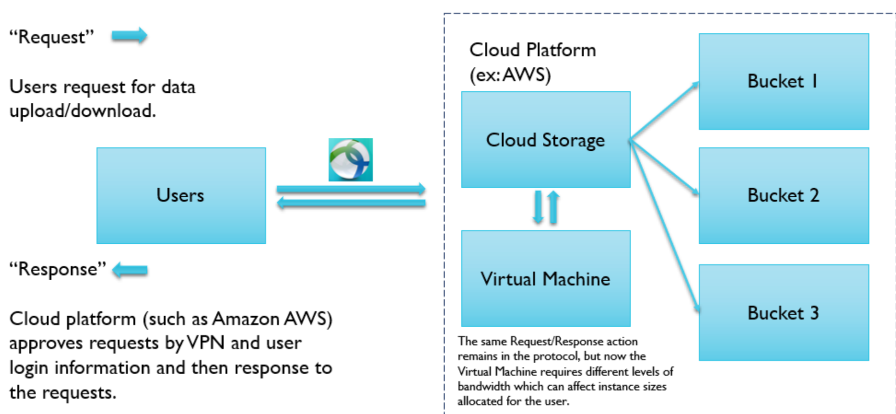


Figure 8: **Executive Diagram of Remote Conference and WFM**. The figure demonstrates the procedure and workflow for user-to-user online/remote conferences and work-from-home scenario setup.

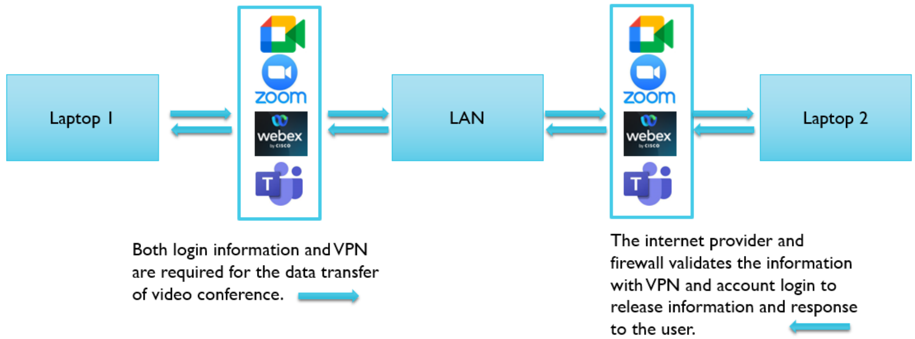
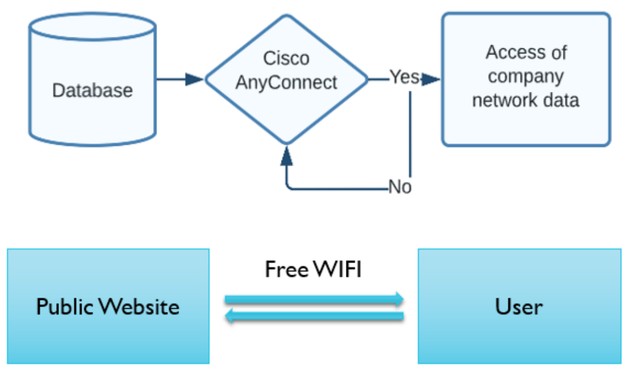


Figure 9: **Executive Diagram of WIFI Connection**. The figure illustrates the potential workflow for internet connection process using WIFI connections with and without VPN.



flowchart. A laptop is using online meeting platforms (Google Meet, Zoom, WebEx, and Microsoft Meet) to establish connections. The system, upon approval of the valid login and VPN credentials, communicates with LAN which is the next tier of internet services after WAN. The information transfers from LAN goes into another online conference platform to communicate with a second laptop where the second laptop is not required to be in the same place as the first one.

Upon the visits of a customer, it is recommended to have on-site wifi and internet connection at a local branches to provide over-the-counter services to the clients. The on-site internet connection is separated into two types of connections, one with VPN in place and the other without. The difference of this two types of internet connections are provided in Figure 9. The secured wifi connections for the in-store employees are required to use a third-party encryption system that is approved with a login credential. For example, a platform such as Cisco AnyConnect can be set in place to encrypt the data transferred and distributed from the branch hub to each machine (laptop/desktop). For customers who need the internet connections, free wifi without password can be provided.

Table 1: **Summary Table of List of Events**.

Type	Cite
Jamming	[10]
DoS	[2]
Intrusion Detection System (IDS)	[1]
Internal	[19]
Access control	[22]
Wormhole	[4]

3 Network Operations Center

A strategic network monitoring system is also required to complete the internet setup. This section of the work is proposed and built upon the foundation of the previous assignment. The work builds on a variety of understanding including network design, network topology, and network reliability. The plan is to design a real-time monitoring system to measure the network performance and availability. The security of the network is part of the equation as well and will be proactively monitored. In the his assignment, we list out comprehensive plans for how to shift strategic plan to focus on Network Operations Center (NOC for short).

3.1 Events to Monitor and Detect Security Issues

It is provided a list of potential threats and events that are worth monitoring and these events posed danger to security safety [15]. Hence, it is important to include a list of attacks in this document as well (may have some overlap with previous assignments).

Jamming attack is the first type of event on the list and it is originally introduced by [10]. It is a type of DoS attacks where the strategy of such attack focus on sending a large volume of signals to affect the reliability of the communication channel. DoS attack, as the most common attack in Internet of Things, is another type of event because it often attacks user at low-end device which usually can be neglected by users [2]. One interesting attack that arise is called Intrusion Detection System (IDS) [1]. In regarding to this type of attacks, machine learning tools such as anomaly detection can be used to tackle this type of problems. This problem is magnified at today's world because modern day computing technology including networking, data storage, management, and so [1] proposed a sequential model to investigate and evaluate the data security. Their work showed improved stability and robustness in regards of performance measure metrics of the dataset on the end-users IoT devices [1]. Malicious node can be another form of attacks and this type of events focus on the heterogeneous nature of the smart phone or other similar devices that users use. This can be crucial when employees of the companies have their accounts logged into using their remote devices such as iPhone or iPad and they are accessing the internet using public Wifi and so on. Events like this can be an area where malicious attack can take place. Hence, this report proposes to have monitoring system in place. Internal and access attack are orchestrated together simultaneously which then could potentially create this parallel process called a Wormhole attack [19, 22, 4]. Wormhole attack can cause severe damage to the IoT routing [4]. It constructs a tunnel between two users or two machines in the internet topology to design an information passage. The wormhole attack relies on this type of passage to transfer malware across different locations of the system. The diagram of this type of attack is drawn in Figure 10 which is cited from Figure 2 of [4].

Figure 10: **Generalized diagram for wormhole attack**. [4]

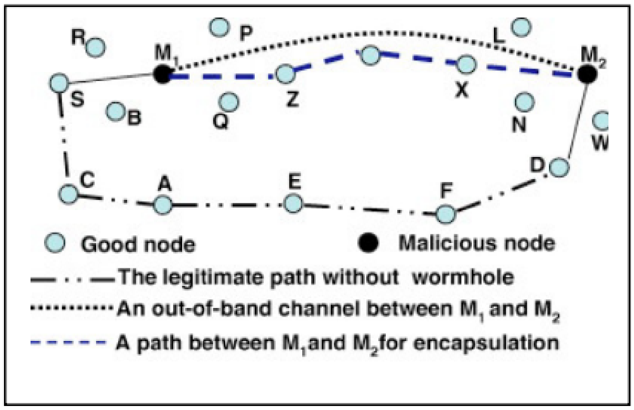


Table 2: **Confusion matrix of alert system correctness**.

		Notified	
		Yes	No
Malfunction	Yes	True Pos.	False Neg.
	No	False Pos.	True Neg.

3.2 Alerts and Notification Responses

In emergency situation where there is a shut down or some malfunction in the network system, the responsive personnel will be notified. This calls for a contingent plan in place. Disregard the channel, some form of notification is needed and the role responsible needs to be checked and put in place. As naive as this may sound, the entire alert and notification responses system essentially refer to the system where a message, an email, or call will be triggered to send to the employee who is in charge of a malfunction situation. Hence, the system is required to be precise and on-time. This is to avoid the scenarios where the person is notified but there is not a malfunction or the person is not notified when there is one. To describe the scenarios thoroughly, denote the scenarios for the signal to be either malfunction or normal and assume the person is either notified or not. Hence, we have a two-way table and this gives us $2^2 = 4$ scenarios. This is shown in Table 2. The notification can be passed or not, and hence the situation can either be “yes” or “no”. The malfunction can also be positive or negative because there is either an alert or not. This gives 4 unique scenarios. They are true positive, true negative, false negative, and false positive. The two true scenarios are easy to interpret. They refer to the situations where the notification is correct. The incorrect situations can be false negative and false positive. The false negative is when there is not a notification when there is a malfunction. The false positive is when there is a notification but there is no malfunction. The false positive is the classic “crying wolf” situation and the high occurrences of false positives can lead to a potential unvisit when there is a “yes” for notification.

Hence, based on the above reasoning, there also needs to be a learning procedure in place to improve the notification and alert accuracy when responses are triggered. The end of the channel is the human response. Since it is a human response, psychology and behavioral instinct plays into the equation so that we the designer of this entire strategic monitoring system needs to take this into consideration. This is because it is not just our responsibility to design a complete system. We also need to think in the positions of our employees who are waking up 2AM in the morning to check the system if there is ever a malfunction. They better not be waking up at 2AM and arrive to the factory at 3AM only realizing it is a false positive. This event creates discouragement for these employees to do their job correctly.

The alert and notification system can be quite substantial when we are at the beginning stage designing the network system for a company that has 150 branches operating in the northeastern region of the United States. By setting quick and efficient notification system, the first responders are able to arrive at the scene to tackle the malfunction and any other internet connectivity issues. In addition, a learning system is also recommended to be set up so that the precision and accuracy of the notification/alert can improve.

4 Key Performance Indicators (KPIs)

A Key Performance Indicators (KPIs) is a performance measure metric that evaluates the network management. There are several perspectives to be aware of. Here we list them in the following.

First, the KPI needs to efficiently conform the definition of the performance measure. IF there is not a direct link between KPI and the network connectivity status, then the KPI would be not be meaningful. Second, the KPI needs to be understood easily. The description needs to state the issues inside out and every building block needs to be well understood by not just technicians but also management team. The KPI also requires a protocol for action. For various reasons, it is important that the document and the evaluation metrics calls for action. This avoids unnecessary costs in the operation process and the negligible behavior in the corporate management workflow.

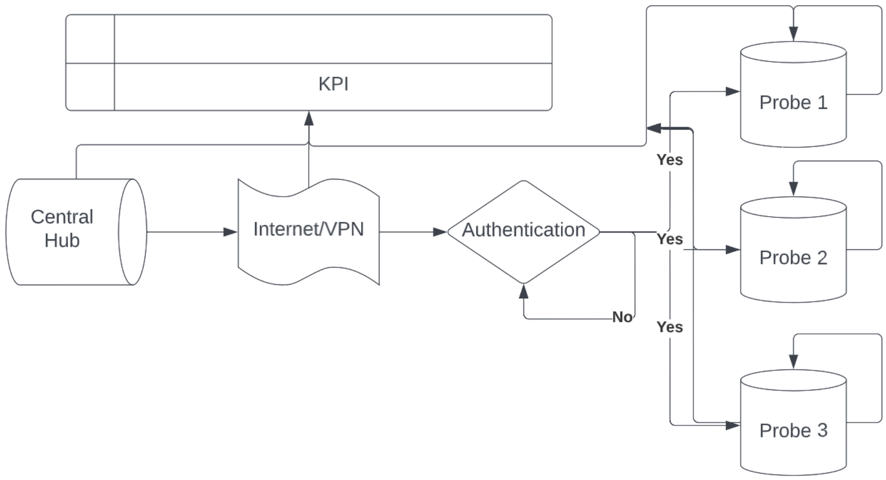
4.1 Visualization and Reporting

The visualization of the proposed reporting system is drawn in Figure 11. The central hub starts with the initiation of the data transfer on a secure network system. The internet and VPN remains in tact and will be required to transfer the data towards each probe. The authentication is set in place to verify the access or request from each probe. The probes serve as branches to ask for data from the central hub upon approval of the internet access.

5 Conclusion

As a summary, this document summarizes the entire network design that is the culmination of all the work and foundation for the previous assignments. The document provides quality report to assist the business leaders (CIO and CEO of the company) to develop the viable plan of hiring the correct teams to setup the internet connection platform and hence to be able to explore and design the most optimal IoT platform for the applications required for the company expansion. The document starts with the background of the organization expansion and address the business needs. Then the document provides a comprehensive network design with designated workflow chart or diagrams to reflect the proposed strategy, platforms, or other IoT devices. In addition, the document provides suggested management and monitoring platform to allow special situations to arise. The document also provides ample amount of information in regarding to identification of security risks, implications, and risk mitigation strategies for IoT platforms and devices.

Figure 11: **Diagram of KPI Reporting System**.



The document also spans the data storage and cloud platforms to allow the company to enrich its network operations center and to develop minoring and detection issues.

References

[1] M. Almiani, A. AbuGhazleh, A. Al-Rahayfeh, S. Atiewi, and A. Razaque. Deep recurrent neural network for iot intrusion detection system. *Simulation Modelling Practice and Theory*, 101:102031, 2020.

[2] Z. A. Baig, S. Sanguanpong, S. N. Firdous, T. G. Nguyen, C. So-In, et al. Averaged dependence estimators for dos attack detection in iot networks. *Future Generation Computer Systems*, 102:198–209, 2020.

[3] B. P. M. M. D. Callaghan, J. M. C. J. K. Hollingsworth, R. B. I. K. L. Karavanic, and K. K. T. Newhall. The paradyn parallel performance measurement tools. ., 1994.

[4] S. Deshmukh-Bhosale and S. S. Sonavane. A real-time intrusion detection system for wormhole attack in the rpl based internet of things. *Procedia Manufacturing*, 32:840–847, 2019. 12th International Conference Interdisciplinarity in Engineering, INTER-ENG 2018, 4–5 October 2018, Tirgu Mures, Romania.

[5] T. Ekici and L. Dunn. Credit card debt and consumption: evidence from household-level data. *Applied Economics*, 42(4):455–462, 2010.

[6] M. K. Gardner, W.-c. Feng, and J. R. Hay. Monitoring protocol traffic with a magnet. In *Passive & Active Measurement Workshop*, 2002.

[7] G. Held. *Internetworking LANs and WANs: concepts, techniques, and methods*. John Wiley & Sons, Inc., 1998.

[8] D. R. Hofstadter. *Gödel, escher, bach*. Basic books New York, 1979.

[9] N. Kumbakara. Managed it services: the role of it standards. *Information Management & Computer Security*, 2008.

[10] M. López, A. Peinado, and A. Ortiz. An extensive validation of a sir epidemic model to study the propagation of jamming attacks against iot wireless networks. *Computer Networks*, 165:106945, 2019.

[11] B. Lowekamp, N. Miller, R. Karrer, T. Gross, and P. Steenkiste. Design, implementation, and evaluation of the remos network monitoring system. *Journal of Grid Computing*, 1(1):75–93, 2003.

[12] B. B. Lowekamp. Combining active and passive network measurements to build scalable monitoring systems on the grid. *ACM SIGMETRICS Performance Evaluation Review*, 30(4):19–26, 2003.

[13] M. Mathis, J. Heffner, and R. Reddy. Web100: extended tcp instrumentation for research, education and diagnosis. *ACM SIGCOMM Computer Communication Review*, 33(3):69–79, 2003.

[14] W. Matthews and L. Cottrell. The pinger project: active internet performance monitoring for the henp community. *IEEE Communications Magazine*, 38(5):130–136, 2000.

[15] B. K. Mohanta, D. Jena, U. Satapathy, and S. Patnaik. Survey on iot security: Challenges and solution using machine learning, artificial intelligence and blockchain technology. *Internet of Things*, 11:100227, 2020.

[16] M. C. Nelson, K. Lust, M. Story, and E. Ehlinger. Credit card debt, stress and key health risk behaviors among college students. *American journal of health promotion*, 22(6):400–406, 2008.

[17] C. Scarpitta, P. L. Ventre, F. Lombardo, S. Salsano, and N. Blefari-Melazzi. Everywan-an open source sd-wan solution. In *2021 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME)*, pages 1–7. IEEE, 2021.

[18] P. Segeč, M. Moravčik, J. Uratmová, J. Papán, and O. Yeremenko. Sd-wan-architecture, functions and benefits. In *2020 18th International Conference on Emerging eLearning Technologies and Applications (ICETA)*, pages 593–599. IEEE, 2020.

[19] N. Tariq, M. Asim, Z. Maamar, M. Z. Farooqi, N. Faci, and T. Baker. A mobile code-driven trust mechanism for detecting internal attacks in sensor node-powered iot. *Journal of Parallel and Distributed Computing*, 134:198–206, 2019.

[20] R. Wolski. Forecasting network performance to support dynamic scheduling using the network weather service. In *Proceedings. The Sixth IEEE International Symposium on High Performance Distributed Computing (Cat. No. 97TB100183)*, pages 316–325. IEEE, 1997.

[21] K. Yaghmour and M. R. Dagenais. Measuring and characterizing system behavior using {Kernel-Level} event logging. In *2000 USENIX Annual Technical Conference (USENIX ATC 00)*, 2000.

[22] H. Yan, Y. Wang, C. Jia, J. Li, Y. Xiang, and W. Pedrycz. Iot-fbac: Function-based access control scheme using identity-based encryption in iot. *Future Generation Computer Systems*, 95:344–353, 2019.

[23] M. Zangrilli and B. B. Lowekamp. Comparing passive network monitoring of grid application traffic with active probes. In *Proceedings. First Latin American Web Congress*, pages 84–91. IEEE, 2003.