2024

VRQ GAMING REPORT

CSEC 394/395

GROUP 12: BOYAN DJUROVIC, JADEN DORF, ESTEBAN MIRANDA, RUMESA RAZI, MAX THEODOSAKIS

Contents

Introduction:

Virtual Reality – Experience the impossible. Go places you've never been and do things you never could. Here at Virtual Reality Quidditch (or VRQ for short), we want our players to experience the thrills, teamwork, and victories of quidditch – all from a danger-free zone in one of our three facilities. In this report, we will outline the design and implementation of the optimal network infrastructure for our VRQ facilities.

Our startup company is leading the way in competitive VR gaming. The goal is to provide players a safe space where they can easily compete in leagues against other teams in different locations in a Virtual Reality environment using Fulbodus Slide. VRQ endeavors to establish a dynamic playing environment across three Midwest locations. This report outlines a comprehensive plan to integrate the 3 locations into a unified network infrastructure as well as explores the intricacies of designing and building a strong network infrastructure that supports real-time gaming, administrative operations, and spectator access.

Objectives:

The network infrastructure's main goal is to give VRQ a secure, scalable, and dependable platform that can not only handle the company's present needs but also set the company up for future anticipated growth. We will fulfill VRQ's needs by building a technological foundation that provides redundant internet access for live spectatorship, maximizes gaming experiences, and enables real-time synchronization across different locations by leveraging cutting-edge technologies. The network design is crafted to not only support the current scale of operations but also to facilitate future expansions, accommodating a projected 10% staff growth over the next six months.

At the core of VRQ's mission is the commitment to provide an unmatched gaming experience for both players and spectators. Our network infrastructure, as outlined in the report, focuses on optimizing connectivity, both internally among the VRQ staff and among players and spectators. In alignment with VRQ's goals, our focus is to elevate user interaction quality and create an environment that fosters innovation, security, and operational efficiency.

Summary:

This report details the design and implementation of the VRQ facilities across three Midwest locations. We will detail a plan to integrate a network infrastructure that will support virtual reality gaming, administrative operations, spectator access, and security all within a $20,000 budget. The network infrastructure is also designed with a possible 10% staff increase in mind. The main HQ is in Lincoln Park, and remote offices are in St. Louis and Milwaukee. The network must accommodate a data traffic load of 100 Kbps per player to each server to ensure smooth gameplay and communication. We will prioritize point-to-point links to minimize latency and include a backup infrastructure in the event of communication failure.

The design for the main headquarters will include dual active/passive firewalls for continous protection. One inside switch connects a staff wireless access point, an application server, and two mail and web servers. The second switch on the outside of the firewalls will connect three wireless access points for the Lincoln Park VR headset to connect to. Also, the external switch manages the connection to the ISP router, the point-to-point St. Louis router, and the point-to-point Milwaukee router. Each remote office will house a single switch connected to a dedicated firewall. The switch will be on the outside of the firewall and extended connectivity through point-to-point links to both the headquarters and the other branch offices, establishing a secure and direct communication channel. For added security, devices behind the firewalls will have

MFA, and USB ports will be disabled. We also detail deployment of the network; our pre-deployment evaluation and survey and our physical deployment.

Requirements:

In order to create a network architecture that combines virtual reality gaming with operational efficiency, it is essential to comprehend the unique characteristics of VRQ's operations. This section offers an overview for establishing a network infrastructure that is specifically customized to meet VRQ's needs.

VRQ’s unique team-based Virtual Reality competition unfolds across three different locations in the Midwest: Lincoln Park (Chicago), St. Louis, and Milwaukee. Each location has a dedicated VRQ gameplay field, with the main headquarters situated at our Lincoln Park location.

Technical Requirements:

The network must accommodate a data traffic load of 100 Kbps per player to each server to ensure low-latency effortless communication between locations. The network design should prioritize point-to-point links to minimize latency and include a backup infrastructure in the event of communication failure.

Virtual Reality Quidditch will engage viewers from all around the world in addition to the players, hence, it is crucial to have redundant internet access for fans to watch the games live. Each of the three locations must have redundant internet connectivity using 2 ISPs from JP and KQ TELCO. This will not only ensure uninterrupted spectator access but also fortify the network against potential disruptions.

As VRQ is leading the way in competitive virtual reality, the company is expected to grow exponentially in the future. Over the following six months, a 10% increase in staff is anticipated.

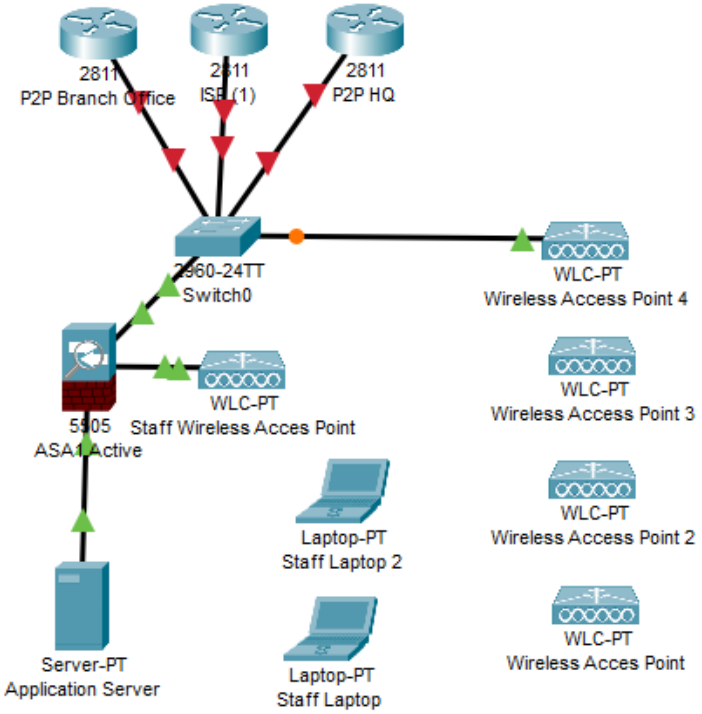
The proposed network infrastructure must be scalable to seamlessly handle this expansion. Furthermore, cost minimization is a crucial factor even if the application's efficiency and functionality are of utmost importance. Within the limitations of the budget, maintaining the network infrastructure's longevity requires striking a compromise between cost-effectiveness and performance.

The overall project is funded by a significant kickstart initiative that generated $20,000.00 for one year of operation. The management's goal is to not only cover the costs of equipment (LAN equipment such as routers, servers, switches, workstations, etc.) and software licenses but also incorporate one year's worth of telecommunication and operation costs. Beyond the implementation phase, management hopes to have enough funds for marketing and advertising to boost VRQ's visibility and market presence.

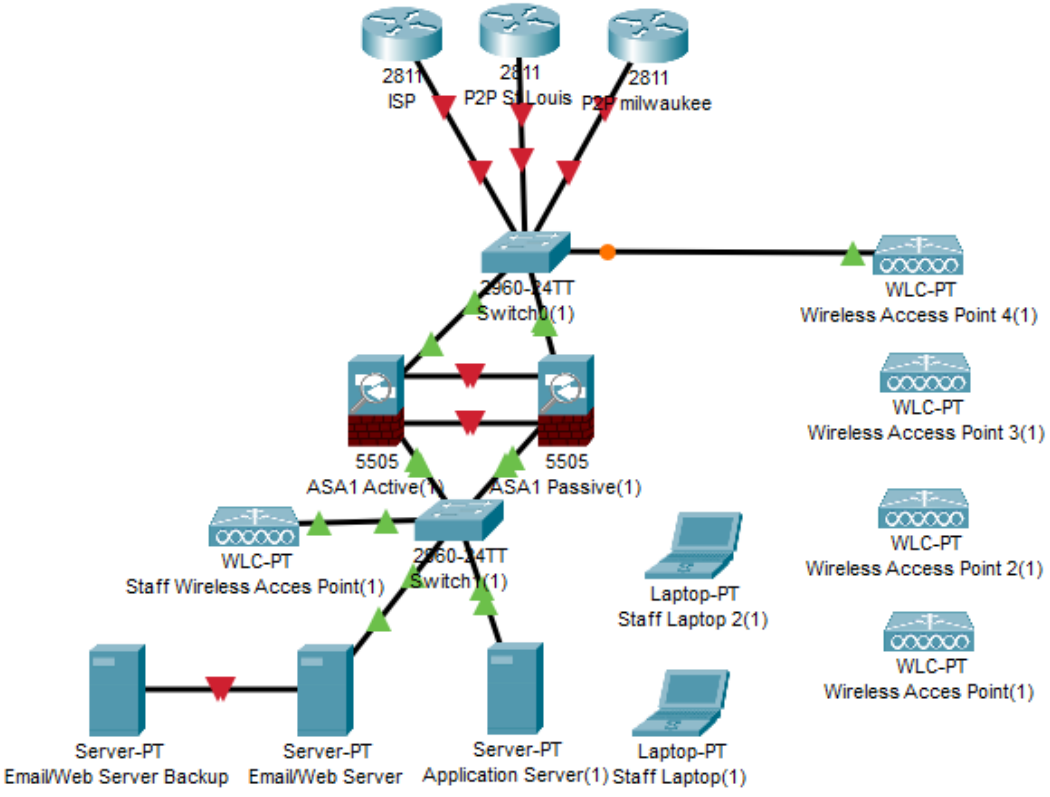
By carefully analyzing VRQ's needs, we lay the groundwork for a customized network infrastructure that not only satisfies the present operational needs but also anticipates and accommodates future growth and innovation. The following sections go into greater detail on the proposed design and provide an outline for implementing a resilient and cutting-edge network for VRQ.

Network Topology:

Remote Office



Main HQ



Network Design:

We've designed the optimal network for VRQ according to the specific requirements. At the main headquarters, we've implemented a robust security setup with dual firewalls– one active and another serving as a failover backup. This ensures continuous network protection, with seamless transitions in the event that the main firewall goes down as the backup will kick in. There will be two switches, one switch will be on the inside of the firewalls. The switch on the inside interconnects a staff wireless access point, an application server, and two mail and web servers, forming a secure and efficient internal network. The second switch, situated on the outside of the firewalls, will connect three wireless access points for the Lincoln Park VR headsets to connect to. Additionally, this external switch manages connections to the ISP router, the point-to-point St. Louis router, and the point-to-point Milwaukee router.

For the remote offices, the network equipment will be less. Each remote office houses a single switch connected to a dedicated firewall. The inside of the firewall connects the application server and a staff wireless access point. The switch extends connectivity through point-to-point links to both the headquarters and the other branch offices, establishing a secure and direct communication channel. Furthermore, this remote office setup facilitates direct internet access, ensuring seamless internet connectivity for on-site operations and field activities through four strategically placed wireless access points. This comprehensive design not only meets the specific requirements but also provides flexibility and scalability for future expansions.

Security:

Devices behind the firewall(s) will have multi-factor authentication using Auth0. This software requires our users to authenticate their login with an additional passcode or biometric to validate

their identity. Auth0 adds an extra layer of security so that non-employees cannot log in to the servers illegally. Auth0 is $23 a month, so for a year of operations, it will cost $276 in total.

For added security, we also disabled USB ports to ensure that there is no physical security risk. If an attacker brings in an infected USB, they will have nowhere to plug it in. This measure mitigates physical security risks, preventing potential attackers from introducing threats through infected USB devices. By eliminating the use of USB ports, we reinforce the overall security posture of VRQ's network, safeguarding against potential vectors of attack.

Benefits of our Network Design

Our network design boasts several notable features. Firstly, our network is very scalable. It will be easy to add devices and expand/increase the network size due to the flexible, symmetrical network topology. Adding more computers, firewalls, or servers will be easy to accomplish if they are needed in the future.

Our network also has redundancy built in. We designed it with two firewalls. Both firewalls in the main headquarters will not be active at the same time. The active firewall will be in charge of all of the packet filtering. If anything goes wrong with that router – a DDoS attack, for example – the backup firewall will immediately spring into action and pick up where the active firewall left off. This means that even if an attack occurs, and *even if* the first firewall falls, there will be a backup ready to go. In this scenario, VRQ can continue to function seamlessly regardless of the attack on the firewall. Employees will be able to reach vital backend data servers through a VPN tunnel configured at every site, which will allow for a secure connection to the internal network of our HQ. Finally, there’s one more benefit of our network – it's secure. We have installed two-

factor authentication on every device behind the firewall. This means you cannot access those devices unless you are authorized, so hackers will not be able to breach the VRQ network.

IP Addressing:

Lincoln Park HQ				
Device	Int	IP Address	Mask	Notes/Remarks - Connection
R1-ISP-JP	G0/1	8.8.8.8		Route to internet
R1-ISP-KQ	G0/0	4.4.4.4		Redundant route to internet
R2-MKE	G0/0	10.1.1.1	/24	Inside to switch
R2-MKE	G0/1	100.1.1.1		Link to MKE branch site
R2	L0	11.1.1.1		
R2	L1	12.2.2.2		
R3-ST LOUIS	G0/0	10.1.1.2	/24	Inside to switch
R3-ST LOUIS	G0/1	100.1.2.1		Link to STL branch site
R3	L0	13.3.3.3		
R3	L1	14.4.4.4		
FW1	Inside	10.0.1.1		Active firewall
FW1	Outside	10.1.1.5		
FW2	Inside	10.0.1.1		Virtually configured as a
FW2	Outside	10.1.1.5		passive firewall
SERVER1		10.0.1.5		Email/Web Backup
SERVER2		10.0.1.3		Email/Web
SERVER3		10.0.1.4		Application

LAPTOP1		10.0.1.8	/24	DHCP
LAPTOP2		10.0.1.x	/24	DHCP
Access Point 1	G0/0	10.0.1.10		Staff Wireless AP
Access Point 2	G0/0	10.1.1.10		All mesh networks will be on
Access Point 3	G0/0	10.1.1.20		WiFi 6 running a 5Ghz
Access Point 4	G0/0	10.1.1.30		connection for maximum
Access Point 5	G0/0	10.1.1.40		security

Milwaukee Branch				
Device	Int	IP Address	Mask	Notes/Remarks - Connection
R1	G0/0	10.2.1.1	/24	Inside to switch
R1	G0/1	100.1.1.2		P2P to HQ
R1	L0	15.5.5.5		
	L1	16.6.6.6		
R2-REMOTE	G0/0	10.2.1.2		Branch Office
R2-REMOTE	G0/1	100.1.3.1		P2P to MKE branch office
R2	L0	17.7.7.7		
R2	L1	18.8.8.8		
FW3	Inside	10.0.2.1		ACLs will allow 10.0.2.x
FW3	Outside	10.2.1.3		
SERVER	G0/0	10.0.2.2		Application
Access Point 1	G0/0	10.0.2.10		Staff wireless AP

Access Point 2	G0/0	10.2.1.10		All mesh networks will be on
Access Point 3	G0/0	10.2.1.20		WiFi 6 running a 5Ghz
Access Point 4	G0/0	10.2.1.30		connection for maximum
Access Point 5	G0/0	10.2.1.40		security
LAPTOP1		10.0.2.x	/24	DHCP
LAPTOP2		10.0.2.x	/24	DHCP

St. Louis Branch				
Device	Int	IP Address	Mask	Notes/Remarks - Connection
R1	G0/0	10.3.1.1		Inside to Switch
R1	G0/1	100.1.2.2		P2P for HQ
R1	L0	19.9.9.9		
	L1	20.0.0.0		
R2-REMOTE	G0/0	10.3.1.2		Inside to switch
R2-REMOTE	G0/1	100.1.3.2		P2P for MKE branch
R2	L0	21.1.1.1		
R2	L1	22.2.2.2		
FW4	Inside	10.0.3.1		Inside ACLs for internal
FW4	Outside	10.3.1.3		Outside
SERVER	G0/0	10.0.3.2		Application
Access Point 1	G0/0	10.0.3.10		Staff wireless AP
Access Point 2	G0/0	10.3.1.10		All mesh networks will be on
Access Point 3	G0/0	10.3.1.20		WiFi 6 running a 5Ghz
Access Point 4	G0/0	10.3.1.30		connection for maximum

Access Point 5	G0/0	10.3.1.40		security
LAPTOP1		10.0.3.x	/24	DHCP
LAPTOP2		10.0.3.x	/24	DHCP

The focus is to create a redundant strategy across three locations the St. Louis Branch, Lincoln Park HQ, and Milwaukee Branch. The organization network spans three various sites each in a different major city, equipped with firewalls, servers, and wireless access points, which are configured for both internal and customer use. The IP addressing strategy uses subnetting to optimize the overall network performance and security posture. DHCP is utilized to efficiently manage IP addresses for all client device needs.

Detailed Branch Configurations:

St. Louis Branch:

Internet Redundancy: This site will have 2 P2P connections/routes it can take if one of the two were to go down. One to HQ and the other to the Milwaukee branch.

Firewall FW4: Separates our internal and external traffic with dedicated interfaces, completed by strict ACLs to enforce security. As well as having a direct tunnel into the HQ site for backend data.

Wireless Infrastructure: Allows for multiple APs using advanced Wi-Fi 6 protocols for secure and reliable wireless communication within the office premises. We will have two networks, internal and external, both encrypted with WPA2, only the external password will be provided to customers if they request it.

Client Devices: Laptops and other mobile devices leverage DHCP for IP allocation, allowing for network flexibility and efficient address management.

Lincoln Park HQ:

Internet Redundancy: Two separate direct connections with JP & KQ Telco. ISPs to ensure redundancy and maintain a stable connection.

Routing Redundancy: Additional routes maintain internal communication integrity and include two P2P links, one as a fail-safe for branch-to-branch communication.

Firewall Configuration: FW1 and FW2 provide an active/passive HA setup, ensuring zero downtime for firewall services as well as configured tunneling to allow both branches access to internal servers through secure remote access.

Server Placement: Servers are assigned static IPs within the network range, including email/web hosting and core applications, set up for load balancing and optimal performance.

Milwaukee Branch:

Internet Redundancy: This site will have 2 P2P connections/routes it can take if one of the two were to go down. One to HQ and the other to the St. Louis branch.

Firewall FW3: Separates our internal and external traffic with dedicated interfaces, completed by strict ACLs to enforce security. As well as having a direct tunnel to get into the HQ site for backend data.

Wireless Infrastructure: Allows for multiple APs using advanced Wi-Fi 6 protocols for secure and reliable wireless communication within the office premises. We will have two networks, internal and external both encrypted with WPA2, only the external password will be provided to customers if they request it.

Client Devices: Laptops and other mobile devices leverage DHCP for IP allocation, allowing for network flexibility and efficient address management.

The design demonstrates a descriptive approach to creating a highly resilient and redundant network, each layer of the network has carefully considered a failsafe to ensure a constant secure connection to the internet. Moving forward, it is recommended to conduct periodic simulations of failover to ensure that failover system systems are functioning properly. Additionally, continuous monitoring of network traffic and performance can identify issues even before they occur. Finally, creating a disaster recovery and business continuity plan to have a system in place in case of an emergency.

Equipment Overview:

Our design is based on a careful selection of state-of-the-art equipment to strengthen VRQ's network infrastructure. Most of the hardware was purposefully purchased through low-cost channels like eBay and other internet marketplaces. By using this strategy, we were able to stay within the $20,000 budget and provide the best possible speed, security, and scalability for VRQ's network infrastructure. The following section provides a comprehensive overview of the essential components of our network infrastructure, including switches, firewalls, routers, servers and other critical hardware that were chosen to ensure optimal performance, security, and scalability.

Equipment:

Switches:

For our network infrastructure, we chose Cisco WS-C2950G-12-EI switches. We were able to find a pack of 6 switches, each priced at $20. These switches, equipped with 12 10/100 ports and two fixed GBIC-based 1000BASE-X uplink ports, offer a cost-effective solution while providing reliable and efficient performance. These Cisco switches are in good condition, have been tested,

and come with a 30-day guarantee. They fit our budget constraints without compromising on functionality, which helps us build a robust network for VRQ.

Firewalls:

To strengthen the security of VRQ's network, we've selected four Cisco ASA5505-BUN-K9 Security Firewalls. These used firewalls come with power adapters, ensuring ease of setup. These Cisco firewalls, which are well-known for their effectiveness in network security, fit our financial limits without compromising on performance. Their integration into the network infrastructure contributes to our main objective of creating a reliable and cost-effective solution for VRQ's security needs.

Mesh Wi-Fi Routers:

To ensure seamless and expansive Wi-Fi coverage, we've opted for four of the TP-Link Deco M4 3-Pack Mesh Wi-Fi System. This is a certified refurbished product and includes the mesh routers and power adapters. The 3-pack system is designed to cover an area up to 5,500 square feet and allows for smooth roaming with a single Wi-Fi identity. As users move though the field locations or the HQ, their devices automatically connect to the fastest Deco unit, providing an uninterrupted Wi-Fi experience. By utilizing 802.11ac wireless technology, the Deco M4 provides three times faster network speeds than routers from earlier generations, guaranteeing a seamless connection for up to 100 device at once. This TP-Link mesh router helps us achieve our objective of providing dependable and high-performance Wi-Fi coverage by meeting the diverse connectivity needs inside VRQ's network.

Wireless Access Points:

To enhance VRQ's wireless connectivity, we are purchasing three Cisco Meraki MR42 Dual-Band Cloud Managed Wireless Access Points. The access points are used but fully functional. With a 1.90 Gbit/s maximum wireless data bandwidth, the MR42 guarantees fast

communication. These APS provide offer versatile and reliable network access with their dual-band capabilities and compatibility with both Wireless Wi-Fi 802.11ac and Wired Ethernet (RJ-45) connections. Their unclaimed status indicates that these devices are ready for seamless integration into our cloud-managed system. For deployment, these APs will be carefully linked to the TP-Link Deco M4 mesh routers. The setup ensures comprehensive Wi-Fi coverage, particularly n the designated game playing fields, enhancing the overall gaming experience for VRQ participants.

Ethernet Cables:

To satisfy VRQ's Ethernet connectivity needs, we sourced a set of 50 Monoprice Cat6 10ft cables as an affordable solution. Although the network infrastructure needs around 40 cables, this larger bundle fits our budgetary limits and adds more cables for future growth. The cables have a 550 MHz bandwidth and provide strong performance. The snagless cable boot enhances durability by protecting the plug retaining clip and the 50µm gold-plated contacts ensure reliable and high-quality connections. The extra cables not only prepare VRQ for future expansion but also allows for direct connections where needed, optimizing internet connectivity across VRQ's locations.

Servers:

Application Servers:

For VRQ's application servers, we opted for three Living as One Gaming + Live Streaming Rackmount Servers. Theses servers have a Core i7-6700l processor, GTX 1050 graphics card, Z270M Exterme4 P2.10 motherboard, 8GB RAM (2x4GB) running at 2133 MHz, and a reliable Samsung 850 PRO SSD. The servers come without an operating system, which allows flexibility in software installation. This robust configuration ensures efficient processing for VRQ's

applications, providing the computational power needed for various tasks contributing to the overall operational efficiency of the organization.

Web/Email Servers:

To strengthen VRQ's email and web hosting capabilities, we've chosen two HP Desktops, each with a quad-core Intel Core i7 7700 processor, a 32GB RAM, and a well-balanced storage solution that includes a 500GB SSD paired with a 3TB HDD. These desktops come pre-installed with Windows Server 2022 Standard, providing a robust and feature-rich operating system for efficient email and web server functionalities. This configuration ensures that VRQ's online presence and communication are backed by reliable and high-performance servers, which contributes to a seamless experience for both players and spectators.

Server Keys:

To activate the application servers, we're buying three Windows Server 2022 Standard keys. With these keys, we can ensure that the servers have the most recent security updates and Windows Server capabilities.

Devices:

Lenovo IdeaPad:

To meet the operational needs at each VRQ location, we're acquiring six Lenovo IdeaPad 1 Student Laptops, ensuring two laptops per site. These laptops feature an Intel Dual-Core Processor, 20GB RAM, and a 1TB SSD + 128GB eMMC storage combo for efficient multitasking and data storage. These devices come with a user-friendly operating system, versatile connectivity, and a clear, immersive experience. This device selection aligns with the essential requirement of having laptops available at each location to facilitate various on-site tasks for VRQ.

Budget Allocation:

VRQ BUDGET ALLOCATION

Equipment	Quantity	Cost/unit	Subtotals
ISP: JP & KQ TELCO			$14,400
128 Kbps p2p	3	$200	$600
128 Kbps to Internet	3	$200	$600
Lenovo ThinkPads	6	$372	$2,232
Servers:			$1,842
Application	3	$400	
Email/Web	2	$321	
Networking Equipment:			$954
Switches	6	$20	$120
Firewalls	4	$45	$180
Mesh Router	4	$110	$440
Wireless Access Points	3	$18	$54
Ethernet Cables	50	$3	$160
MFA-Auth0			$276
Windows Server Keys	3	$21	$61

Total

Internet	$14,400
Devices	$4,074
Networking Equipment	$954
MFA	$276
Licensing	$61
TOTAL	$19,765
Left	$235

Budget Overview:

Our network design is easily the best option within the confines of the $20,000 budget. Internet service will be provided through JP & KQ TELCO, employing 128 Kbps dedicated point-to-point links and redundant links. The three 128 Kbps point-to-point connections, allocated to the three branch offices, will incur a monthly cost of $200 each, totaling $600. Additionally, three 128 Kbps redundant links, also distributed among the branches, will total another $600 per month. Thus, the monthly internet costs will be $1,200 and the yearly will be $14,400.

One significant cost-saving strategy is the acquisition of used equipment which ensures us from going over budget. Staff members at each location will share two Lenovo IdeaPad Laptops, with a total of six laptops priced at $372 each, resulting in a cost of $2,232. Three application servers, each priced at $400, will sum up to $1,200. Additionally, two email/web servers, each costing $321, will have a combined total of $642. The total expenditure on servers will amount to $1,842.

For networking equipment, we calculated the most cost-effective way to achieve a well-balanced and efficient network infrastructure. We invested in a pack of six switches, each priced at $20, summing up to a total cost of $120. Since security is paramount in our design, we've incorporated four firewalls, each priced at $45. This allocation resulted in a total expenditure of $180.

For wireless capabilities, we found a 3-pack mesh router priced at $110 and got four of those, which amounted to $440. Mesh routers enhance the coverage and provide a seamless and robust wireless experience for staff and players. However, we decided to add three Cisco Meraki Wireless Access Points to extend wireless connectivity. The access points cost $54, with each piece at $18.

In addition to the hardware, we included a pack of 50 ethernet cat6 10ft cables from Monoprice. Each cable was priced at $3, and the 50-pack totaled $160. The collective expenditure for networking equipment amounted to $954.

We subscribed to Auth0 for Multi-Factor Authentication to enhance security which incurred a cost of $23 per month and $276 yearly. Lastly, our application servers did not come with a pre-installed operating system, so we decided to get three Windows Server 2022 Standard keys at $21 each, summing up to $61.

In summary, our network design for VRQ comes out to a total of $19,765, which leaves $235 within the allocated $20,000 budget. Internet service turned out to be the major expense at $14,400, while networking equipment, device procurement, and security measures sum up to $4,074.

With $235 left, there's room for other projects, potentially using those funds towards marketing and advertising initiatives, in line with the management's hopes. This financial flexibility ensures not only a robust network infrastructure but also the potential for future growth and promotional activities.

Deployment/Migration:

In the initial phase of the deployment and migration plan, a pre-deployment strategy will be implemented. This includes conducting a thorough site survey at the locations, evaluating the existing infrastructure, and creating a detailed plan for the upcoming deployment. To ensure an understanding of the resources at hand, an inventory of all hardware and network components will be conducted. Employees will also be involved in communication initiatives to foster awareness and collaboration during the deployment process.

The next stage is the installation and configuration of network hardware such as switches, routers, and firewalls at each location. Point-to-point links will be established between the headquarters and remote offices to ensure secure and reliable connectivity. At the main headquarters, web/email servers and application servers will be deployed simultaneously. After that comes the configuration of all the software, including the game management VR application, operating systems, and security applications. This will ensure a smooth integration and synchronization across all three locations. Security measures, such as the activation of multi-factor authentication through Auth0, will be activated on servers and devices behind firewalls. Similarly, USB port disablement and establishment of VPN tunnels between firewalls will take place to further strengthen the security of the network infrastructure.

As part of the deployment process, the network infrastructure will be thoroughly tested to find and resolve any potential issues. This will include a thorough analysis of the game management VR application to ensure real-time synchronization between servers. Before connecting to the internet, thorough testing will be done to verify the firewall configuration and ensure the network is robust. This testing phase will be the longest part of the deployment process as it will cover security validations, performance benchmarks, and other issues. After testing is completed successfully, users will be gradually moved to the new network, and staff members will receive special training to familiarize them with the updated infrastructure. The last step is to create extensive documentation that outlines the network configurations, IP addressing schemes, and security protocols to be used as a reference for ongoing management.

Assumptions:

2 employees doing troubleshooting for the games at each time. One laptop will be for each dedicated person and manager access for each location. Each will have access to each laptop via

Auth0 2FA. This assumes that 9 employees total will have access to the troubleshooting laptops; 3 per location.

While we did not have a backup isp at each branch since we mapped the network via point to point as well, we have our backup ISP as each internet connection on each separate branch. This way if an internet connection fails at one of the three branches, they can still connect directly to one of the other branches and access the internet through their connection.

In order to maximize streaming bandwidth and player communication with the application server, we elected to have each branch with its own application server. This way streamers within the stadium and games played within the stadium will be at maximum performance and can fall back on the isp to connect to another branch. This assumes the staff at each branch will be able to maintain each server and keep the game updated across 3 different branches.

When choosing the method of covering each field for internet, we chose a method that will require 2 different routers connected to our switch at each location. This means that each building will have to have ethernet ports throughout the building.

Over budget proposal:

As profits scale with time, VRQ might want to consider some upgrades to the existing framework laid by our firm. When the time comes to expand, you can upgrade the existing internet connections and point to point from 128kbps to 1mbps. This should allow for seamless streaming across fields as well as viewers to tune in from external locations or view games in other stadiums.

Conclusion:

Our network for VRQ is the best for several reasons. We designed a secure, reliable network with built-in redundancies and scalability that manages to be under the budget of $20,000 dollars without significant compromise to its performance. Each player can play VRQ smoothly at 100 kbps with others at their location and at the 2 other locations. With an active and passive firewall at the Main Headquarters, our network is as secure as it gets – if the active firewall collapses, the passive will boot up and pick up where its fallen brethren left off. We've accurately determined costs based on a potential 10% growth of staff at the company, and provided an over-budget option if more performance is preferred over minimizing costs. We have provided links to all the equipment that is necessary to our network design – and finally, we included a deployment plan which details how to set up and start our network.

We hope you will make the right choice for Virtual Reality Quidditch. Once you do, please don't hesitate to reach out to us so we can deploy the VRQ network.