***Technology assessment for FGS Foods Ltd.***

Proposal, Technical Project

Plan X

***Aviraj Sinha***

***[FGS Food Ltd]***

***[8823 Sachin Industrial Area]***

***Surat, India***

***fgsfood@email.com***

Version:001

This proposal is submitted to the Computer and Information Science faculty in partial fulfillment for the degree

Master of Science in Computer and Information Science.

**TABLE OF CONTENTS**

1. Introduction 1

1.1 Problem Statement 1

1.2 Background 1

1.3 Needs STATEMENT 1

1.4 OBJECTIVE 1

2. Proposed TECHNICAL APPROACH 1

2.1 Requirements 1

2.2 Architecture Design 1

2.3 Implementation DESIGN 1

2.4 Quality Assurance Plan 1

3. Expected Project Results 1

3.1 MEASURES of SUCCESS 1

4. Schedule 1

# Introduction

This plan contains details pertaining to the core requirements of the FGS foods company. These technologies are incorporated into our plan as they become beneficial to the company.

## Needs STATEMENT

No current network for small business requirements.

## OBJECTIVE

*[Identify changes desired to be seen upon completion of effort.]*

Providing reliable and predictable service.

Providing more and/or better service where there is already high network usage.

Providing service where there is anticipated growth in the future:

- bandwidth

- security

- scalability

- internet

Using existing network infrastructure as efficiently as possible

Improving the way people connect so they can reach more resources in less time

# Proposed TECHNICAL APPROACH

*[Define clearly a well thought-out and solid technical plan for applying information technology to the proposed project. This section should include a description of the methodology to be used to complete the project, a specific plan for gathering requirements, an architecture design, best practice for implementation, and quality assurance.]*

*We used a traditional 6 step approach:*

* *Collect requirement*
* *Assess requirement*
* *Define an Architectural Framework*
  + *Networks – Wired vs. Wireless*
  + *Network Set-up – Peer-to-Peer Vs. Client Server*
  + *Equipment required*
  + *Security requirement*
* *Cost estimation*
* *Implementation*
* *Maintenance*

## Requirements

*[Present the requirements as understood at this time through contacts with the stakeholder. Include a high-level diagram such as a use case system diagram or block diagram to capture the situation being addressed.]*

The following requirements were collected after interview process

Category Information :

1. Number of users and How many network users, printers, and servers will the network types of equipment support?

To determine the number of network users the network must support, be sure to consider how many users will be added over the next 12 months, and how many network printers and network servers the network has to accommodate.

1. Projected growth What is the expected growth in the company or organization? Will the company be hiring new employees who must be provided with access to network resources? Will a new branch office be opened that will require connectivity?
2. Current Internet connectivity How does your business connect to the Internet? Does the ISP provide the equipment, or do you own it? Often with a high-speed Internet connection such as DSL or cable, the service provider owns the equipment needed to connect to the Internet (for example, a DSL router or cable modem). If the connectivity is upgraded, the equipment that provides the connectivity may also need to be upgraded or replaced.
3. Application requirements What applications does the network need to support? Do you require services for applications such as IP telephony or videoconferencing? It is important to identify the needs of particular applications, especially voice and video. These applications may require additional network device configuration and new ISP services to support the necessary quality.
4. Existing network infrastructure How many networking devices are installed in your network? What and physical layout functions do they perform? Understanding the existing number and types of networking equipment that are currently installed is critical to being able to plan for the upgrade. It is also necessary to document any configurations that are loaded on the existing devices.
5. New services required Will any new services be required either now or in the future? Will the company be implementing VoIP or videoconferencing technology? Many services require special equipment or configurations to optimize their performance. Equipment and configurations must take into account the possibility of new services to protect the investment and optimize performance.
6. Security and privacy Do you currently have a firewall in place to protect your network? considerations When a private network connects to the Internet, it opens physical links to more than 50,000 unknown networks and all their unknown users. Although this connectivity offers exciting opportunities for information sharing, it also creates threats to information not meant for sharing. Integrated Services Routers (ISR) incorporate firewall features along with other functionality.
7. Wireless requirements Would you like a wired, wireless, or wired plus wireless local-area network (LAN)? How big is the area that the wireless LAN (WLAN) must cover? It is possible to connect computers, printers, and other devices to the network using a traditional wired network (10/100 switched Ethernet), a wireless-only network (802.11x), or a combination of wired and wireless networking. Each wireless access point that connects the wireless desktop and wireless laptop computers to the network has a given range. To estimate the number of access points that are required, you must know the required coverage area and the physical characteristics of the location that the wireless network must cover.
8. Reliability and uptime What is the real cost of downtime in the company or organization? expectations How long an outage can the company tolerate before suffering serious financial or customer losses? Maintaining nearly 100% uptime requires complete redundancy in all equipment and services and is extremely expensive to implement. Networks must be designed to reflect the real need for uptime and system reliability. This level can be determined only through intensive investigation and discussions with all the business stakeholders.
9. Budget constraints What is the budget for the network installation or upgrade? System performance, reliability, and scalability are all expensive to achieve. The project budget normally is the deciding factor as to what can and cannot be done. A complete cost-benefit analysis must be completed to determine which features and services are the most critical

## Architecture Design

*[Explain the technology to be used in the project. Describe hardware, software, or network components as relevant and as understood at this time. Draw a high-level architecture diagram to illustrate the proposed system components and the relationships between them. ]*

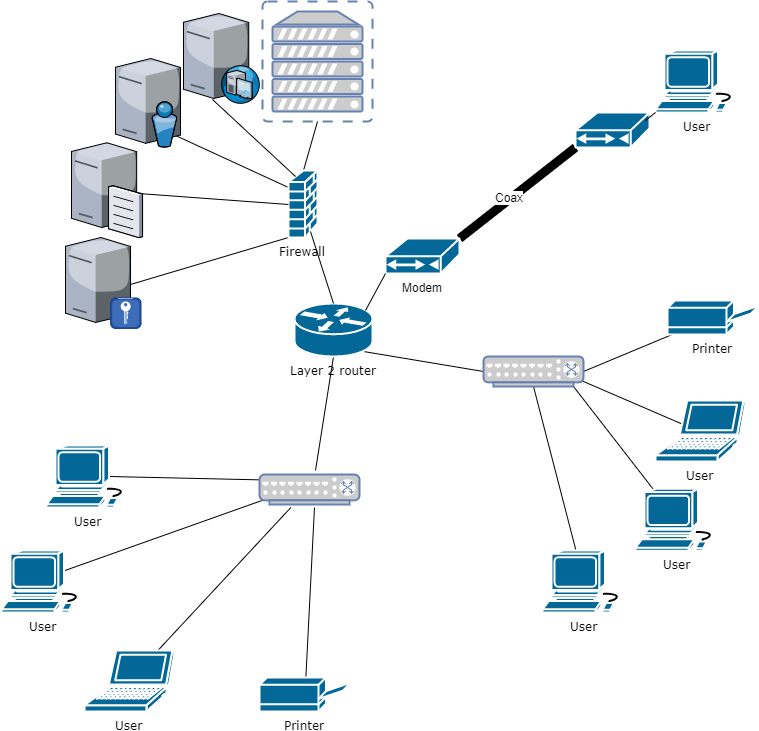
*Design Consideration:*

*[OPTIONAL CONTENT: Include a best-practice approach to be followed.]*

Cabling Considerations: When planning the installation of network cabling, the following were considered

1. physical areas,
2. User work areas
3. Telecommunications rooms
4. Network Cables Cable Type
5. Characteristics Shielded twisted-pair (STP) Usually Category 5, 5e, or 6 cable that has a foil shielding to protect from outside electromagnetic interference (EMI). The distance limitation is approximately 328 feet (100 meters).
6. Unshielded twisted-pair (UTP) Usually Category 5, 5e, or 6 cable. It does not provide extra shielding from EMI, but it is inexpensive. Cable runs should avoid electrically noisy areas. The distance limitation is approximately 328 feet (100 meters).
7. Fiber-optic cable A medium that is not susceptible to EMI and that can transmit data faster and farther than copper. Depending on the type of fiber
8. Network Devices: After considering the customer requirements we analyzed, and recommended the appropriate network devices to connect and support the new network functionality. A general rule is that the higher the device is in the OSI model, the more intelligent it is. This means that a higher-level device can better analyze the data traffic and forward it based on information not available at lower layers. For example, a Layer 1 hub can only forward data out all ports, a Layer 2 switch can filter the data and only send it out the port connected to the destination based on MAC address, and a Layer 3 router can decide which traffic to forward or block based on the logical address. As switches and routers evolve, the distinction between them becomes blurred.
9. LAN Devices Although both a hub and a switch can provide connectivity at the access layer of a network, switches should be chosen for connecting devices to a LAN. Switches generally are more expensive than hubs, but the enhanced performance makes them cost-effective. A hub generally is chosen as a networking device within a very small LAN, within a LAN that requires low throughput requirements, or when finances are limited. A hub may also be installed in a network when all network traffic is to be monitored. Hubs forward all traffic out all ports, whereas switches microsegment the network. Connecting a network monitoring device to a hub allows the monitoring device to see all network traffic on that segment.
10. Internetworking Devices After the LAN switches have been selected, we determined which router is appropriate for the customer. A router is a Layer 3 device. It performs all tasks of devices in lower layers and selects the best route to the destination network based on Layer 3 information. Routers are the primary devices used to interconnect networks. Each port on a router connects to a different network and routes packets between the networks. Routers can break up broadcast domains and collision domains
11. Connectivity Routers are used to interconnect networks that use different technologies. They can have both LAN and WAN interfaces. The router’s LAN interfaces connect to the LAN medium. This medium typically is UTP cabling, but modules can be added to the router to allow the use of fiber-optic cable and other types of media. Depending on the series or model of router, there can be multiple interface types for connecting LAN and WAN cabling. We considered organization’s future connectivity requirements considering the following features such as the following: ■ Security ■ Quality of service (QoS) ■ Voice over IP (VoIP) ■ Network Address Translation (NAT) ■ Dynamic Host Configuration Protocol (DHCP)
12. Security : Security

Security is a feature that must be designed into the network, not added on after the network is complete. Planning the location of security devices, filters, and firewall features is critical to safeguarding network resources. Infrastructure and Architecture overview



## Implementation DESIGN

*[Describe your methodology for implementation.]*

Benefits

In networking, a hierarchical design is used to group devices into multiple networks. The hierarchical design model has three basic layers: Core layer: Connects distribution layer devices. Distribution layer: Interconnects the smaller local networks. Access layer: Provides connectivity for network hosts and end devices

The benefits of this **hierarchal network design** using router allows multiple separate networks to be created. By organizing in a layered approach a core layer connects smaller local networks. Access layer’s intermediary frame: provides connectivity for network hosts and end devices.

In a **Client-server network**, all computers are connected to a central server that acts as the hub of you business’ data. Applications and files are a available on the server and everyone can use these resources at anytime, provided they are authorized to access the information.

The main difference between the two is that P2P network relies on information provided by the clients (users) and it could have other issues such as limited performance and security, and can only carry a small number of users.

Although client-server networks are a little bit pricier, it allows for faster processes, more RAM and storage space, all which plays an important part in ensuring the efficiency of your organization.

Enterprise Physical Facility

The main distribution frame should contain the main router, security system and servers. Management of cables include proper connections and labeling, decreased airflow, controlled temperature, and cable management equipment.

Hardware Details and Configuration

All hardware needed

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Network hardware** | **quantity** | **Cost($)** |  | **Reason** |
| Cisco 880 Series Integrated Services Routers | 1 | 400 | 400 | capabable of wan lan wlan and various security settings |
| Cisco 250 Series Smart Switches SG250-26 | 2 | 250 | 500 | business-class switch |
| ASA 5506-X with FirePOWER Services | 1 | 600 | 600 | optional extra protection allows finer control of access control lists and more security incase of internet operablility |
| Synology DiskStation 4-Bay (Diskless) Network Attached Storage DS412+ | 1 | 500 | 500 | file storage server |
| HP ProLiant MicroServer Gen8 Ultra Micro Tower Server (783958S01) | 1 | 700 | 700 | application server |
| D-Link DCM 301 - Cable modem - Gigabit Ethernet - 340 Mbps | 1 | 50 | 50 | change coax back to ethernet for long distance |
| TPA-311 (Version v1.0R) Mid-Band | 1 | 50 | 50 | ethernet to coax |
| HP Officejet Pro 8600 Plus | 2 | 200 | 400 | office printing |
| Wyse Technology 902175-05L-ES | 20 | 70 | 1400 | thin clients which have just enough computing to access servers |

IP configuration (DHCP)

Manually assigning IP addresses to a network is time consuming as you need to record which address you have used and which computer that you have assigned it to. This is suitable for a one-room computer room as you can quickly check which addresses are available. For a large or widespread network, you should automatically assign IP addresses using DHCP. This assigns dynamic IP addresses to each computer when they ask for one when starting up from a set range allocated by the administrator. DHCP should be enabled on router

Virtualization

Virtualization Many separate logical servers can be located on one physical server. The physical server uses an operating system specifically designed to support multiple virtual images. This feature is known as virtualization. This technology reduces the cost of providing redundant services, load balancing, and failover for critical network services

Wiring

Wired LANs use Ethernet cables and network adapters. Ethernet cables must be run from each computer to another computer or to the central device. It can be time-consuming and difficult to run cables under the floor or through walls, especially when computers sit in different rooms.

Wired LANs need ethernet cables and network adapters. When connecting devices of the same type (ie computer to computer) a cross over cable is needed however for the current design only straight through cables are needed. It can be time-consuming and difficult to run cables under the floor or through walls, especially when computers sit in different rooms but it would be much for faster than ethernet over power line.

Some newer buildings are pre-wired with CAT5 cable, greatly simplifying the cabling process and minimizing unsightly cable runs.

The correct cabling configuration for a wired LAN varies depending on the mix of devices, However, none of these options pose any more difficulty than, for example, wiring a home theater system.

Wired LANs offer superior performance. Traditional Ethernet connections offer only 10 Mbps bandwidth, but 100 Mbps Fast Ethernet technology costs little more and is readily available. Although 100 Mbps represents a theoretical maximum performance never really achieved in practice.

Wired LANs utilizing hubs can suffer performance slowdown if computers heavily utilize the network simultaneously. Use Ethernet switches instead of hubs to avoid this problem; a switch costs little more than a hub.

Servers

Creating a server farm results in the following benefits: Network traffic enters and leaves the server farm at a defined point. This arrangement makes it easier to secure, filter, and prioritize traffic. Redundant, high-capacity links can be installed to the servers and between the server farm network and the main LAN. This configuration is more cost-effective than attempting to provide a similar level of connectivity to servers distributed throughout the network. Load balancing and failover can be provided between servers and between networking devices. The number of high-capacity switches and security devices is reduced, helping to lower the cost of providing services.

**File server** - Stores network users' data files

**Print server** - Manages the printers that are connected to the network and the printing of user documents on the network printers

**Application server** - Shares network-enabled versions of common application software and eliminates the need for software to be installed on each workstation

**Database server** - Manages common databases for the network, handling all data storage, database management and requests for data

**Domain server** - Authenticates and authorises computers and users to access resources within the logical domain

Security

This should also be factored in to your small business networking service, and it all boils down to how secure you need your network to be. As mentioned before, a client-server network would be a better business IT solution because it provides a high level of security. A client-server set-up also allows you to limit access level to certain users only such as top level management.

Identify risk areas and mitigation strategies

Business continuity

Preventing Failures The network designer must strive to provide a network that is resistant to failures and that can recover quickly in the event of a failure. Core routers and switches can contain the following:

UPS

Larger enterprises often install generators and large uninterruptible power supply (UPS) devices. These devices prevent minor power outages from causing large-scale network failures.

Firewalls

Hardware-based firewalls protect all the computers on your network. A hardware-based firewall is easier to maintain and administer than individual software firewalls.

The ideal solution for small businesses is a hardware firewall integrated into a comprehensive security solution. In addition to a firewall, the solution should include virtual private network (VPN) support, antivirus, antispam, antispyware, content filtering, and other security technologies.

Maintenance

Document updating infrastructure and change management procedures. Many network failures are the result of poorly planned, untested updates or additions of new equipment. Never make a configuration change on a production network without first testing it in a lab environment.

Manageability: No matter how good the initial network design is, the available network staff must be able to manage and support the network. A network that is too complex or difficult to maintain cannot function effectively and efficiently.

## Quality Assurance Plan

*[Describe the potential risks related to the software quality. Provide the project management plan to enable quality. Describe the salient, planned testing considerations.]*

*[OPTIONAL CONTENT: Include any analysis plan for usability and acceptance testing.]*

# Conclusion & recommendation

If the plan is followed the star topology and server client design will result in ease of resource distribution, scalability, and ease of use.