**Assignment 2 – Help Document**

**Part 1 Design efficient networked systems**

1. **Prepare a written step-by-step plan of how you are going to design a Local Area Network including a blueprint of your LAN.**

**Installation/Selection of components:**

* Read through the scenario carefully identifying current hardware available to you.
* Consider if the hardware specified is suitable for use in this new network
* If upgrading or suggesting new hardware remember it is a small business (consider value and need) and you must justify your selection.
* Outline and select all hardware, software (Could also include cabling) for the network. Reflect back to assignment 1. Topology, infrastructure? Storage requirements? Which NOS will you use?
* Include minimum specs of software needed and extra costs involved.
* Hardware specs and recommendations for upgrades including costs.
* Include existing hardware and software here along with items to be bought.

**Create a Network Layout/blueprint diagram – See end of document for example – MS Visio/www.draw.io could be used**

**Bandwidth**

* Consider local bandwidth (Switch/cabling/router) and internet speed (fine as it is or needs an upgrade?)
* Cost constraints
* Expected average load; anticipated peak load. Research and estimate bandwidth usage for local and internet needs.
* Use LAN Speed Test software(<https://totusoft.com/lanspeed>) on the network for testing.

***Formula for identifying bandwidth requirements:***

***N x T = BN******N****umbers of users (x)****T****raffic estimate based on usage weight =****Bandwidth Needed***

**Service**

* What services need to be configured - DNS, DHCP, Active Directory, Printer services etc. Why?

**Naming system**

* Domain name and local server name.
* User name and passwords for users. Use a table.

**Addressing: method eg allocation of addresses for NOS services**

* IP Address list for each hardware.
* Use of DHCP?
* Static vs dynamic IP addressing, reservations, scopes, leases

**Security**

* Policy eg patch management, anti-viral management, access requirement/rights, administrative rights, authentication, password policy.
* Explain your intruder detection system e.g firewall with filers and rules, email monitoring, application and packet monitoring
* Physical security(Server room access)
* Explain the router setup(Firewall, encrypted WI-FI)
* Anti-Virus

**Security Policies & Procedures to consider**

* Password (timeout, requirements, history)
* Security (Group policy, CCTV, guards, check points)
* Vetting (DBS, CRB, references)
* Physical protection (Doors & locks)
* Encryption (Bitlocker etc)
* Timeout (Session, PC, User account)
* User roles (Admin, non-admin, restricted admin, guest)
* Backup & Data evacuation
* Data protection act, GDPR
* Two factor Authentication (Software, hardware, physical)
1. **Justify your choice of devices for your network design.**

Justify the components you have selected to support the required infrastructure either in its own section or as you list each item.

1. **Produce a test plan to evaluate this design for the requirements of bandwidth and cost constraints as per user specifications.**
* Create a test plan. It should define the objective of testing and should include the following types of testing:
* Hardware compatibility testing.
* Operating system compatibility testing
* Application compatibility testing.
* Security testing.
* Hardware and software assessment.
* Performance baseline determination.

You should also document all installation, configuration and administrative processes which you are going to utilize.

Use a table like below. Include everything you have installed or configured on Windows Server. Include tests at the client end to check services and features have been set up correctly. Check that hardware can communicate with each other. Check bandwidth and transfer speed (Use LAN Speed Test software). Test whether and how the new network design works with the existing network infrastructure. Screenshot’s ideally should be used as evidence. Screenshot any issues and how you fixed them.

Have tests that conduct verification with Ping, extended ping, trace route, telnet, etc.

|  |  |  |  |
| --- | --- | --- | --- |
| **Test** | **Expected Result** | **Actual Result** | **Problems** |
| Installation of Windows 2012 | Successful installation of NOS | Successful but had issues creating a new partition. | List issues and how you overcame them. |
| Domain created/set up | Successful domain creation of ABCMarketing.net domain |  |  |
| PC 1. IP Address 192.168.1.10.Ping router, server, printer and other machines/hardware |  |  |  |

The following commands in the CMD Line can be used when testing the network:

Use “**ping”** to test network connections between current used device and other devices.

Use “**extended ping**” command is used, the source IP address can be changed to any IP address on the router.

Use “**trace route”** to determine the route packets take on the network. Example:

* *tracert 192.168.0.10*

Use “**telnet**” to determine open ports on the network. For example, to verify connection to 192.168.0.10 on port 25, issue the command:

* *telnet 192.168.0.10 25*
1. **Justify the security requirements and quality of services needed for selection of accessories.**

**Consider:**

**Users/scenario:** Quality expectations, concept of system growth.

**Communications**: Suited to devices, suited to users, supportive of lifestyle desires, supportive of commercial requirements, security requirements, quality of service needs.

**Quality of service considerations:**

| **System Quality** | **Description** |
| --- | --- |
| Performance  | The measurement of response time and throughput with respect to user load conditions.  |
| Availability  | A measure of how often a system’s resources and services are accessible to end users, often expressed as the **uptime** of a system. |
| Scalability  | The ability to add capacity (and users) to a deployed system over time. Scalability typically involves adding resources to the system but should not require changes to the deployment architecture.  |
| Security  | A complex combination of factors that describe the integrity of a system and its users. Security includes authentication and authorization of users, security of data, and secure access to a deployed system.  |
| Latent capacity  | The ability of a system to handle unusual peak loads without additional resources. Latent capacity is a factor in availability, performance, and scalability qualities.  |
| Serviceability  | The ease by which a deployed system can be maintained, including monitoring the system, repairing problems that arise, and upgrading hardware and software components.  |

(Oracle, 2019)

Further reading: <https://docs.oracle.com/cd/E19636-01/819-2326/gaxqg/index.html>

**Scalable**: Able to support device growth, able to support addition of communication devices, able to cope with bandwidth use and trend changes, protocol utilisation, addressing.

**Networking services and applications**: DHCP; static vs dynamic IP addressing, reservations, scopes, leases, options (DNS servers, Suffixes), IP helper, DHCP relay, DNS records, Dynamic DNS.

1. **Suggest a maintenance schedule to support the networked system.**

**Maintenance schedule/Disaster recovery**

* Disaster recovery setup - Devise a regular backup plan/methodology – where will this data be stored? How? Backup-power supply? Off site management? How will you ensure high availability and fault tolerance?
* Backup Software? (e.g Windows Server Backup, Acronis. Which and why.)

**Network Blueprint Example**

The IP addresses for each device would be useful to add to the above example