FASTPACE NETWORK DIAGRAM DETAILED EXPLANATION

Presented by:
Ephraim M. Adehenu.
Systems Administrator.
20200808.

Software used - **LibreOffice** on Windows 10
Version: **6.4.6.2 (x64)**
CPU threads: 4; OS: Windows 10.0 Build 18362; UI render: default; VCL: win;
Locale: en-US (en_US); UI-Language: en-US
Extension - **VRT-NETWORK-EQUIPMENT**

Procedure

Visit https://www.libreoffice.org/download/download/ and download any LibreOffice version of your choice (v6.4.6.2) in my case, install software
Visit https://extensions.libreoffice.org/en/extensions/show/vrt-network-equipment and download the latest build of the extension
Open **LibreOffice Draw**, go to **tools** tab, click **extension manager**, click the **add** button
A file explorer opens, browse to the location of the downloaded file (**.oxt** file) and select and **open**, install extension and restart LibreOffice Draw, go to **view** tab, select **gallery**, select **vrt extensions** from the list of themes depending on the device you wish to add to the diagram, edit your drawing.

Network design

ISP – **197.159.129.129/26** – for a few connections between ISP and company alone – for security purposes.
LAN – **192.168.1.0/24 – 254** hosts can be generated – can be further broken down if need be with private IP addresses and NAT protocols.
SERVERS – **192.168.1.2 – 20/24 and 192.168.1.201 – 254/24** ample space for more additional services in the future.
Departments have IP address allocation of 10 addresses each in this format:
Technology - 192.168.1.21 -30/24,
Marketing – 192.168.1.31-40/24,
Accounting – 192.168.1.41-50/24,
Ops – 192.168.1.51-60/24.

From which the IP addresses of the printers can be:
192.168.1.21 - Technology
192.168.1.31 - Marketing
192.168.1.41 - Accounting
192.168.1.51 – Operations

We have an extra 100 IP addresses still in the system unused after sharing IPs to available devices. We can reserve these for future testing, use and unforeseen circumstances **(192.168.1.101 – 200/24).**

Virtualization Server

This server can be used to reduce expenses on server infrastructure if possible.
It can be virtualized to host other less demanding servers like print, PBX, inventory, intranet, camera, and also testing new services for later deployment
In our case we have
Virtualization server - 192.168.1.11/24
Print server -192.168.1.10/24
Intranet-129.168.1.6/24
Intercom – 192.168.1.7/24
Antivirus – 192.168.1.8/24
Mail – 192.168.1.9/24
If the mail is hosted locally we can place it on here or on a dedicated server. Microsoft exchange can be set up on this server as the network mail service.

Firewall
All routers are connected to the firewall
Main server can also be connected to the firewall for security
Firewall handles one part of the user access and permissions service by filtering what the user can access outside the network and also monitoring what goes on locally to prepare for possible threats both within and without.
Our firewall uses the IP **192.168.1.2/24**

LAN Router
It grants us access to the ISP router and then the internet as a whole
Its **IP - 192.164.1.1/24**

Switches
Both the main switch and the departmental switches are not managed.
They only supply data traffic to all other network devices on the network.
This way it is easier to maintain and work with and managed switches can come at a later date.

WI-FI – **192.168.1.71 – 100/24**

WI-FI router has a DHCP address range of **192.168.1.71 – 100/24** for use by wireless devices – allowed for external business partners and meetings, also visitors come in each day and might need internet to do their work.
Server addresses range from **192.168.1.2 – 20/24** – and **192.168.1.201 - 254/24** for any additional servers.

NAS
This is the file storage server of choice for the network – folders are created on the file server for each department and access to each folder given only to the specific department members the folder is created for.
Heads of department are given their own folder on the server to share confidential files and reports – no outside access.
Users can create their own private folders in the department folder where they can save their own work – also an automatic mapped drive can be created on their local computers once their user access is created on the active directory domain controller where they can save their files locally and privately.
All NAS devises have event logging features and this feature can be enabled to log all file server access and files opened and read, added, removed and modified.

Office 365 can be used to collaborate and work on company documents – this software package has a history modification feature where a user of a particular file can see all the updates made to that file and be able to revert file to an earlier date on a file and save differently

Authentication Server

User access and passwords controlled on the **authentication server**, active directory is setup on this server and domain controller. private user folders are automatically mapped to this computer once user is created on the Active Directory.
The Domain Name Server, where the domain is created and named is also placed on the authentication server since they are similar services. **DHCP** server which shares IP addresses can also be set up there. Strict rules will be followed when creating ranges of IP address for departments, devices and services.

The **Web server** is placed outside our firewall for outside IP addresses to be able to reach us either using a dedicated IP address for mobile access to our platform service online - **(http(s)://197.159.129.129:7070)** and our website (www.fastpacer.gh) address for information and other purposes – we are hosting both these services.

Authentication server hosts the domain controller in this case and handles all user, password and access rights or permissions on the network
Authentication server can also be configured with Microsoft authentication service for multi-factor authentication on the network

User Migration

Create a new computer naming convention in the new active directory domain at the new office
Rename all computers using this format
Connect the computers to the new network
Join each computer to the new network
Create each staff in the new active directory domain
Check all security measures for access to resources on the new network
Let the local user login to the new system with their new credentials and unique passwords.
Since it is a new system or network, we only need to join the old local users to the new system using their own private and secure logins instead of the old universal login.