Patton-fuller network design project

Design

Each department also has its own uninterruptible power supply. The topographical network design shows that of a centralized design. This system has benefits with no need for an operating system stored locally. Thus improving the performance because the SO and user applications are already running on the servers, however it also increases the risk if the mainframe suddenly lost power it will affect all terminals. Distributed networks have much less risk of power outages because if one component in the network fails the others will still have functionality.

On the other hand they require SO and software installed on individual computers which require additional hardware to store it, which can take more time to maintain and update. The network bridge is a critical component in this network that passes information locally throughout the network. Doctors can be authorized in a virtual private network (VPN) from a router linked to the remote access server (RASA) that permits them access to the servers from their home. For email functions the network has a Windows Exchange server running on an IBM xi series. Workstations in doctor's offices and nurses have Imax clients on fiber cables.

The senior managers in unman resources, operations, and finance have virtual operating systems with both Mac SOX (Leopard) and Windows XP. The hospitals current network architecture comprises of a network bridge Joining the administrative and clinical areas. All administrative functions have lines contained in a trunk using Cat 6. The executive departments have Apple desktop systems with Wi-If cards installed. The hospital central mainframe is an IBM series CZECH featuring a database storing patient records and with a fiber connection to a 10 terabyte NAS.

Clinical departments have another run line on a single mode fiber optic line. (Virtual Organizations Portal, 2011) As part of HAIFA, which is meant to protect patient information in attempts of data breaches. This information is stored in encrypted data files using AES (advanced encryption standard). Access is permitted through identification and authentication of any user the requests this information. Standards are important in networking because all networking devices must have the same rules for communication to prevent a loss of data.