Networking Case Study: Recommendations

Student’s Name

Professor’s Name

Course

Date

Networking Case Study: Recommendations

**Beneficiaries**

The Bring-Your-Own-Device (BYOD) global market is approximately 181 billion dollars, and this statistic was taken in 2017. BYOD policies are a great approach to increasing worker convenience and satisfaction. Allowing employees to tag along their devices to work creates an open, relaxed, and more efficient working environment, benefitting both the employer and the employee. For the employer, expenditure is reduced to an average of 350 dollars per worker because the need to get each employee specific equipment or device is eliminated (Bouk, 2018). Costs reduced are not only for purchasing but also for upgrades and in case of tear and wear as they are transferred to the employees. Office space, which correlates with increased rental costs, may be eliminated.

 For the employees, they get the most benefits starting from the ease, satisfaction, happiness, comfortability, and familiarity that help in boosting productivity. In addition, employees get to use technology that is up-to-date while working. According to Suvillan and Frost's Study sponsored by Samsung, BYOD saves each employee approximately 58 minutes in a day (Bouk, 2018). BYOD also decreases the application learning curve because of end-user familiarity. With greater flexibility and enhanced convenience, individuals can work at anytime and anywhere; hence, more hours could be put into working.

**Deliverables**

**Network Interface Card (NIC)**

NIC provides the capabilities of networking. It may either be an Ethernet (a wired connection) or Wi-Fi (a wireless connection). However, for this new location with a policy of BYOD and 40 users, a wireless NIC would be best. While the wired network may be faster than wireless, the current craze is with tablet PCs, but iPads do not have a data port; hence, a Wi-Fi connection would be best (Wegner, 2016). There must be planning for BYOD capacity, and since this organization is not a college or a campus where kids own three to five devices, this environment would be best suited for 2.5 devices per employee (Wegner, 2016).

**Routers or Wireless Access Points or Both,**

A wireless router is often referred to as a router. I would recommend this to be used in the new location because it helps users connect to the network without any cables at home or in a small organization (40 users is a small business). A wireless router has an inbuilt point of access; therefore, adding a wireless access point for the purpose of extending the range of the network is only confusing. The router allows wireless communication and data sharing among computers and devices connected to a certain network, and this is achieved through the allocation of an IP address to the devices and computers. This will also help in sharing scanners and the two HP 4230 LaserJet printers.

**Cables And Connectors To Implement A Physical Network,**

Wireless network adapters, also known as wireless NICs, are vital for each of the devices connected to a wireless network, especially for older laptop PCs or those that do not have it as a built-in feature. Wireless routers and especially AC routers, handle multiple devices well. Wireless antennae may be added to increase the communication range significantly. A wireless repeater can also serve to extend the network’s reach and is mostly called the signal booster. If the office is a large room with many rooms, this will be important to ensure a strong Wi-Fi signal is maintained.

**Any Other Needed Network Hardware,**

Because there is a need to connect the two HP 4230 LaserJet printers to the wireless network, the method used will be the Wi-Fi Protected Setup (WPS). This method requires the HP laserjet printers to support the WPS method, a router with a WPS button, and a wireless network that utilizes the WPA or WPA2 password.

**Physical and Logical Network Topologies,**

The physical and logic network most suitable for the wireless network is the physical star and logical ring topology (Viswanathan, 2017). This is where individual devices are connected to a central hub, just like in a typical star topology. However, the physical connectors within each hub form a ring. If the physical ring is disabled, the devices can cut their physical connection at any position in the internal ring to restore the ring. This is also preferred because of the ease of adding users.

**Internet Protocol (IP) Version (Ipv4 Or Ipv6) And The Reason It Was Selected,**

While IPv4 is more familiar to network operators, it only allows classes A to E of IP addresses. The use of IP in IPv4 is also optional. In this case, the organization needs to implement the mandatory use of IP addresses because of the data sharing influenced by the router. IPv6 has an unlimited number of IP address storage unique for each employee. IPv6 devices can be publicly accessed without more configurations hence saving on resources (Islam, McFarlane & Williams, 2015).

**IP Address Pool for the network,**

The router, by default, acts as the Dynamic Host Configuration Protocol (DHCP) server. The router is what assigns IP addresses to all the connected devices, and the default address of the gateway is the router’s LAN address. Therefore, the IP pool addresses ought to be part of the subnet of the similar IP address as the router’s LAN IP. The default addressing scheme will take one to define a pool ranging between 192.168.1.254 and 192.168.1.2. Part of the range can be saved for fixed devices.

**Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHCP)**

DNS will be used to translate the names of the host into IP addresses. This is more user friendly than typing a whole numerical IP address. Therefore, there is a need for a DNS server configuration. As mentioned above, the IPv6 will be used with a specific range of pool address. DHCP will be used to assign the IP addresses to devices automatically. It may also provide the gateway default, DNS server, and the domain name.

**Any Other Network Software Component.**

One important aspect to consider is the security of the BYOD device. Therefore, there is a need to implement a Mobile Device Management (MDM) software to manage, monitor, and configure all the devices from a central point or location. Scans for vulnerability, as well as antimalware updates, are made possible through MDM.

References

Bouk, J. (19 April 2018). What are the benefits of BYOD? Retrieved from https://www.cassinfo.com/telecom-expense-management-blog/what-are-the-benefits-of-byod

Islam, J., McFarlane, J. S., & Williams, C. (2015). *U.S. Patent No. 8,976,963*. Washington, DC: U.S. Patent and Trademark Office.

Viswanathan, T. (2017). Unit-8 Network Topology. IGNOU.

Wegner, P. (26 March 2012). Want to allow BYOD? Consider these 3 BYOD Wireless Network issues first. *Secureedge*. Retrieved from https://www.securedgenetworks.com/blog/want-to-allow-byod-consider-these-3-byod-wireless-network-issues-first