1. Carrier Sense Multiple Access with Collision Detection (CSMA/CD) is a protocol used in local area networks. This protocol was developed for earlier networks as a method of data communication to minimize data collisions. Using this technology, computers on a system would wait and listen to a network to determine when a viable time to send data is. Once the line is idle, a computer will begin to transmit. The computers on the network will then listen for a data collision. Should a data collision occur, all computers will cease data transmission. The computers involved in the data collision will then set a random timer per machine to retry data sending until the transmission is received in full (Snoeren, n.d.). Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) is a similar protocol used in wireless communications. CSMA/CD cannot be used in a wireless system for two main reasons. Firstly, A wireless transmitter cannot both transmit, and detect data collisions at the same time. It would also be unreasonable to assume that data communications happening simultaneously would be an indicator of a data collision (Souvik Sen, 2011). In CSMA/CA, data collisions need to be avoided altogether due to the absence of a cable connecting all devices for the aforementioned reasons. To this end, computers on the network will wait until they sense no alternate signals being sent to the access point and will then begin to transmit its data. The access point will send an acknowledgement to the sending device to act as a confirmation. Should this confirmation not be received by the sending device, it will attempt to re-send the delivery package.

2. a.

|  |  |
| --- | --- |
| Speed | Projected Cost |
| 100 Mbps | $314 ($40 Modem + $174 Network Switch + $100 Ethernet Cables) before ISP subscription |
| 1000 Mbps | $559.94 ($100 Modem + $359.94 Network Switch + $100 Ethernet Cables) before ISP subscription |

b. As I understand cost may be an issue for this company, I understand the appeal behind the 100 Mbps setup. Not only is it over $200 cheaper to set up, but it’s also less expensive in terms of monthly cost from the ISP. However, in an office of 100 individuals all demanding file sharing and online activities, 100 Mbps is not much to go on. Primarily due to the high demand of file sharing, I would recommend the gigabit option for this company.

c. The choice outlined in section 2.b will likely lead to enhanced internet speeds of even simple casual users on this network. Particularly during times of collaboration, 100 Mbps will be congested much more easily than 1000 Mbps, which will lead to much more waiting for all users online. Upgrading this setup will relieve the congestion on the network, and by virtue decrease the wait times and responsiveness of this network while using it.

d. As described in the ITIL six value chain activities; I believe this setup will help drive more value to this company. I believe that the demand in our company as caused by heavy internet uses such as file sharing will lead to an easily congested network. Upgrading our network to counter this threat will co-opt the Engage and deliver tiers of the ITIL value chain (Rance, July), which will in turn help the company drive more productivity through less wait time. This productivity will help drive value to the company, and keep our business running effectively.

3. Physical and virtual networks have many different important factors to consider. They are similar in that they allow a user access to your network, and the files therewithin. It may be very easy to work while connected to the network, as file management is as simple as sending it over the LAN. Another similarity is that they allow for simple device connectivity. It may be easy to download a PDF on your phone, read through it, and then transfer the file to your computer in order to work on it as long as you are connected to this network. Main differences, however, are many. Firstly, a virtual network will allow the user a degree of freedom that a physical network may not. In a virtual network, a user is able to connect remotely using their own device and still access all the information needed to get work done. With a physical network, the worker must be present at the location of the network in order to connect (Massachusetts Institute of Technology, 2002). Another difference derived from the above statement would be security. A physical network is much harder to break into with malicious intent, as it requires proximity in order to access. This is not true with a virtual network (Massachusetts Institute of Technology, 2002), as anyone with the right software and credentials will be able to intrude into your network and steal any information that they so desire.

4. Switches are an essential part of any large-scale network. Although rather cheap in pricing, they provide an immense value to your network. As a company with 100+ individuals working simultaneously, online bandwidth will become a commodity in the office. Due to this, it is highly recommended to offload some of this stress into a physical connection to help alleviate bandwidth concerns. Using a switch, it is possible to hardwire more devices than your router or modem has ports for (Freedman, n.d.). This is distinctly different from a hub, that would be unable to function to bridge your various computers with your router(s) due to signal duplication and bandwidth issues (Freedman, n.d.). Hubs are typically used to connect multiple computers together, rather than connecting computers to network devices.

# **References**

Freedman, M. (n.d.). *Hubs, Switches, and Routers, Oh My!* Retrieved from COS 461: Computer Networks: https://www.cs.princeton.edu/courses/archive/spr20/cos461/docs/lec04-routers.pdf

Massachusetts Institute of Technology. (2002). *Components of a Virtual Network*. Retrieved from MIT.edu: https://stuff.mit.edu/afs/sipb/project/vmdialup/archive/i386\_linux24.old/lib/vmware-console/help/esx/networking-components.htm

Rance, S. (July, 2012). *Key Element Guide ITIL Service Transition*. Retrieved from Stuart Rance: https://archivebooks.online/download/4715293-key-element-guide-itil-service-transition-key-elem

Snoeren, A. C. (n.d.). *Carrier Sense Multiple Access*. Retrieved from UC San Diego: https://cseweb.ucsd.edu/classes/fa13/cse123-a/lectures/123-fa13-l8.pdf

Souvik Sen, R. R. (2011). *CSMA/CN: Carrier Sense Multiple Access with Collision Notification*. Retrieved from University of South Carolina: https://www.cse.sc.edu/~srihari/pubs/CSMA\_CN\_ToN12.pdf