WEP is not secure because of multiple reasons. Its sufferers from key management problems, its encryption mechanism contains weaknesses, and WEP also had implementation errors. It is said to provide no real security, because it is so easy to get through and hack.

There are three different types of Wi-Fi encryption methods. They are Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), and Wi-Fi Protected Access Version 2 (WPA2). All the Wi-Fi encryption methods protect data on networks. WEP was the first of the three to be made. It contained a lot of deficiencies in its security and is easy to hack, and is now replaced with other methods. WPA was born to take the place of WEP because of the weaknesses it had . There are two types of WPA, WPA-TKIP and WPA-PSK. WPA-PSK is more secure. WPA2 is a more advanced WPA and has a higher level of security. It uses AES, which is used by the government.

Hello Zach, I like your discussion post, it is very informative a about Wi-Fi encryption methods. It is a good thing that they saw that WEP wasn’t meeting the requirements and was lacking in security. It seems like they had to keep trying to make up a new method because of the lack in others, which is a great thing because technology is always improving, which mean so are viruses.

How to Choose Wifi Encryption Settings | Wifi Guide from Cox. (2022). Retrieved 3 September 2022, from <https://www.cox.com/residential/internet/guides/securing-wifi/wep-vs-wpa-vs-wpa2.html#:~:text=There%20are%20three%20types%20of,how%20well%20they%20do%20so>.

Live migration and storage migration are both features of Hyper-V in Windows Server. Live migration allows you to move running VMs from a Hyper-V host to another. Another benefit is that it is flexible, while running Virtual Machines they aren’t tied to a single host. Storage migration can help move VMs to another location without compatibility issues, and can perform on VMs avoiding downtime and continue business operations as usual. Hyper-V migrations often used when a storage device is running low on space, or maintenance or an upgrade is required, or when it starts experiencing problems with eh operations, or when traffic is too high and need to be redistributed among other storages.

Live Migration Overview. (2022). Retrieved 3 September 2022, from https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/manage/live-migration-overview

Reed, J. (2022). How to Perform Hyper-V Storage Migration - Complete Guide. Retrieved 3 September 2022, from <https://www.nakivo.com/blog/hyper-v-storage-migration-guide/>

Hello class, Network Load Balancing also known as NLB, distributes traffic across multiple servers, it can do so by using TCP/IP networking protocol. With it being on multiple computers at once the applications turn into a single virtual cluster. NLB helps with reliability and performance for the network and other servers. NLB have benefits like, Protecting applications from oncoming threats, You must have authenticated user access, it protects against DDoS attacks, and you can easily add on additional servers. You can also simplify business continuity like, for disaster recovery NLB can detect outages and send unknown users to an alternate site.

Network Load Balancing. (2022). Retrieved 3 September 2022, from <https://docs.microsoft.com/en-us/windows-server/networking/technologies/network-load-balancing>

Rhine, J. (2019). What does a load balancer do? | Lume | Benefits of a Load Balancer. Retrieved 3 September 2022, from <https://lumecloud.com/what-does-a-load-balancer-do/>

Hello Class, key Exchange is a protocol, and it shares data with two parties. Starts off as Diffie-Hellman (DHKE) and Elliptic-Curve Diffie-Hellman (ECDH), both parties negotiate with the data secrets. While one party shares the secret the other party obtains the secret from them. Transport schemes goes through public-key cryptography. Then key exchange schemes exchange cryptographic keys between them, so that no one knows the keys for the data. Then an authenticated key exchange is done by the exchanging protocol that authenticates the identities of the parties

(2022). Retrieved 3 September 2022, from <https://www.youtube.com/watch?v=tUY9D4CxmuU>

Hello Jamie, I like your discussion post and your example. The way you explain it makes it simple to understand. By using Biggie and Tupac being informative you also made it fun and also understanding. The video I watched also included the Diffie-Hellman key exchanged.

-Desmond Hughes