

Synthesize a solution to a potential real-life scenario

Author: Jake Russell

Student ID: 1602835

Lecturer: Dr Carlene Campbell

1 CONTENTS

2	Introduction	3
3	Related work	3
4	Problem Formulation	4
5	Implementation	4
5.1	Policies	4
5.2	Mobile Device Management Software	5
5.3	Network	6
6	Results/Findings & Discussions	6
6.1	Advantages and Disadvantages of BYOD	6
6.1.1	Advantages	6
6.1.2	Disadvantages	7
7	Conclusions & Recommendations	7
8	Bibliography	7

2 INTRODUCTION

The aim of this report is to develop a BYOT framework for a hypothetical real-life scenario involving a company called Hyper-Fort. Hyper-Fort is a company that uses cloud services to send IT services to its staff and clients. 95% of the company's network is wireless and they have a large social media and online presence. The staff and customer base now wish to use their own devices to access the company's network and resources.

3 RELATED WORK

To prepare for this report, an investigation into appropriate network structures was done. A key one found was Cisco's 3-tier hierarchal network model. According to Cisco (1) "A hierarchical network design model breaks the complex problem of network design into smaller, more manageable problems. Each level, or tier in the hierarchy addresses a different set of problems. This helps the designer optimize network hardware and software to perform specific roles. For example, devices at the lowest tier are optimized to accept traffic into a network and pass that traffic to the higher layers. Cisco offers a three-tiered hierarchy as the preferred approach to network design."

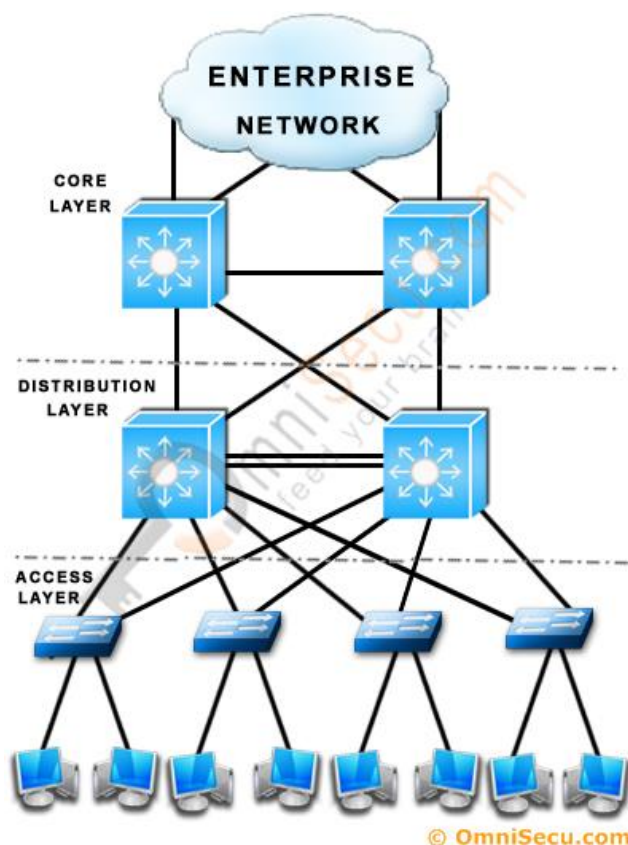


Figure 1: Example of 3-tier hierarchal model (2)

As shown by figure 1, the model consists of three layers, the core layer, the distribution layer, and the access layer. According to OmniSecu (2) the "Core layer consists of biggest, fastest, and most expensive routers with the highest model numbers and Core Layer is considered as

the back bone of networks. Core Layer routers are used to merge geographically separated networks. The Core Layer routers move information on the network as fast as possible. The switches operating at core layer switches packets as fast as possible.” The “Distribution Layer is located between the access and core layers. The purpose of this layer is to provide boundary definition by implementing access lists and other filters. Therefore the Distribution Layer defines policy for the network. Distribution Layer include high-end layer 3 switches. Distribution Layer ensures that packets are properly routed between subnets and VLANs in your enterprise.” (2), and the “Access layer includes access switches which are connected to the end devices (Computers, Printers, Servers etc). Access layer switches ensures that packets are delivered to the end devices.” (2)

4 PROBLEM FORMULATION

The problems this report will be focusing on will be to do with managing security risks, managing users, and managing devices. It is assumed that the company already has policies in place to deal with any issue that was not specified above. The main problems faced are: If data is moved around a lot among many devices, it can be difficult to manage and protect, therefore a way to keep employee and client data secure through this travel of devices must be implemented. If an employee loses their device with important company data, there must be a way to prevent unwanted access to said data. If an employee is using their own device in the work place, policies must be in place to prevent them doing non-work-related activities. Employee’s private data must be kept safe from the company. If an employee leaves the company there is a risk of theft, therefore there should be a policy which prevents this. Employee’s may bring multiple kinds of different brands of hardware as their devices, there could be hardware which is unsupported.

5 IMPLEMENTATION

5.1 POLICIES

The following are policies to be implemented to negate the issues presented above:

- Only personal devices that have been authorised by Hyper-Fort’s IT department will be granted access into the BYOD framework
- All users using BYOD must adhere to an acceptable use policy, this policy entails users only allowed access to apps, programs, or web pages green-lit by Hyper-Fort’s IT department
- All users must agree to have their devices monitored when using Hyper-Fort’s network. Hyper-Fort will not monitor specific details or data, only the names of apps, programs and web pages to check whether the user is adhering to the acceptable use policy, this way hyper-fort will not access any private data of the user.
- To access company data on the user’s device, they must complete an authorisation process, typically a passcode

- If a specific number of failed access attempts selected by Hyper-Fort occur, a remote wipe of the company data will occur on the device
- Cloud storage of company data shall only be enabled if it is monitored and controlled by Hyper-Fort themselves
- The user will be required to keep devices updated at the upmost possibility
- Only devices that are still supported by their respective brand will be authorised for use with Hyper-Fort
- Hyper-Fort will provide and update a list of authorised devices users could use as their BYOD
- If a user leaves Hyper-Fort and remote wipe of company data will occur

5.2 MOBILE DEVICE MANAGEMENT SOFTWARE

For a BYOD system to succeed a form of Mobile Device Management Software is required. There is a plethora of choices to go for however for this system the choice is Microsoft Intune. There are multiple reasons for this choice, and they are as follows: Hyper-Fort's IT department won't have to monitor every single device to maintain its security, this is because Intune grants the ability to create app protection policies to protect company data with no need for the device's to be completely managed by Hyper-Fort. Intune is compatible with almost all operating systems, including ones such as Android, IOS and Mac OS X. Intune can give employee's access to internal apps made by Hyper-Fort across as many devices as they would use for work. Intune allows admins to perform security procedures such as remotely wiping data, resetting passcodes, encrypt data, lock devices and even stop devices cameras and their capability of network roaming. Intune will allow Hyper-Fort to black-list specific apps or URLs to deny access. Intune can deploy updates and software across all devices, allowing Hyper-Fort to make sure everybody is up-to-date. Intune has malware protection built in, using the Microsoft Malware Protection Engine.

5.3 NETWORK

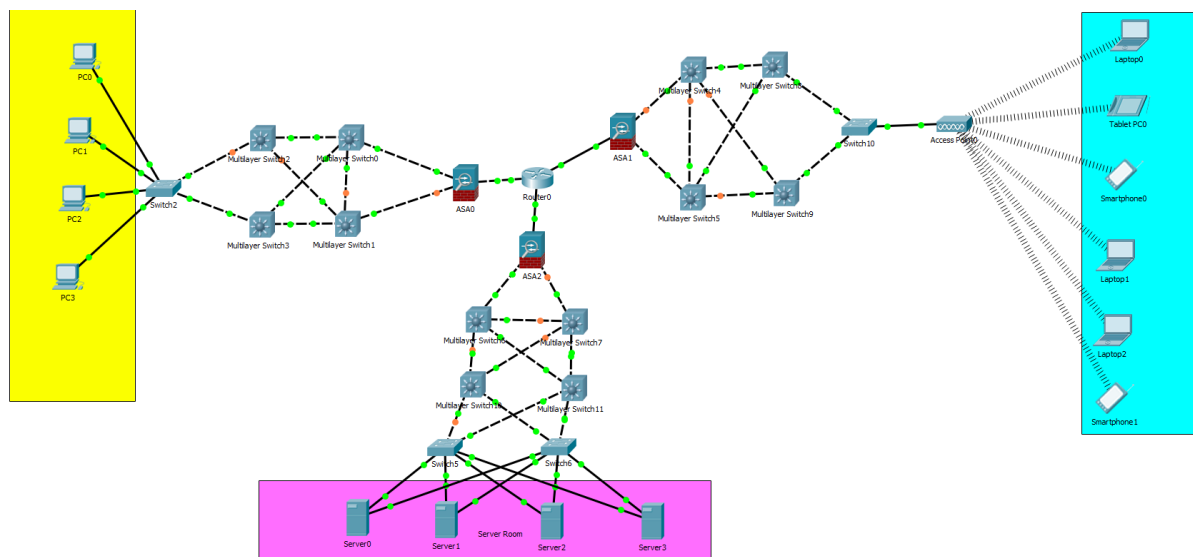


Figure 2 Network built in packet tracer

Here is the network built for Hyper-Fort using Packet Tracer. It follows the principles of Cisco's 3 tier hierarchal network model, for the sake of testing purposes all SSIDs are "Cisco", wpa2 passcodes are "ciscocisco", and passwords for the routers are "cisco". The network has Hyper-Forts Network router with 6 multilayer switches separated by 3 firewalls acting as the "Core layer", then followed by 6 more multilayer switches acting as the "distribution layer", and lastly 4 switches along with pc's, servers and an access point to act as the "access layer". This architecture was chosen due to its better redundancy, packets have many different routes they can travel down, meaning if a switch or two are compromised, then the network will still function. To make the redundancy even better you could add more switches to the access layer. The access point is protected by wpa2 security and the routers should be password protected to access directly.

6 RESULTS/FINDINGS & DISCUSSIONS

6.1 ADVANTAGES AND DISADVANTAGES OF BYOD

6.1.1 Advantages

- Reduces companies costs as there is no need to provide employees with work devices or upkeep current ones
- Increases Employee engagement in the workplace and outside of work
- Hardware is more likely to be the latest technology as it is the employee's personal hardware
- Employee's don't require training to learn company devices
- Supports flexible work times and encourages work on the go
- Employee's will have personalised user interfaces to which they are most comfortable with, increasing productivity

- Employee's are more likely to take good care of their personal devices
- Giving employee's the freedom of device and software can increase employee satisfaction

6.1.2 Disadvantages

- Personal devices are more at risk of malware and scams as they are used in employee's everyday life outside work
- Personal devices are more at risk of getting stolen or lost, this could lead to unauthorised access
- Personal devices are more capable of hacking into the company's private data
- Employee's no longer within the company could still have access to important company data. This presents a large risk of a data breach, especially if the employee has a vendetta against the company
- Employee's may use their devices for non-work-related activities during work hours
- An employee's device may not be supported in the company's BYOD framework
- If employee's have multiple devices, it could be stressful on the network to handle all the traffic
- Employee's may be unhappy to have to pay for their own devices

7 CONCLUSIONS & RECOMMENDATIONS

In conclusion, BYOD systems still need refining in order to be viably integrated into all Organisations. However, from the findings gained, they have large potential for organisations if they find ways to round out its edges. It is recommended that all organisations investigate BYOD and put it into strong consideration as currently there are ways to mitigate the risks (mainly that of security). These being the MDMs available, MDMs such as Intune are already very adept in minimising these Risks, and they can only get better from here. If you are a small organisation who maybe cannot afford an MDM it is reasonable to dismiss BYOD for now, unless a lot of finances are having to go into providing devices to the employees, then it is possible that switching to BYOD with an MDM would save money.

8 BIBLIOGRAPHY

1. *Cisco*. [Online] [Cited: 7 January 2019.] https://www.cisco.com/web/learning/netacad/demos/CCNP1v30/ch1/1_1_1/index.html.
2. *OmniSecu*. [Online] [Cited: 7 January 2019.] <http://www.omnisecu.com/cisco-certified-network-associate-ccna/three-tier-hierarchical-network-model.php>.