Bradley De’Ath

DEA18001355 | SCDT43 – Assignment 1

Network Architectures, Protocols and Cyber Vulnerabilities

Table of Contents

[The Network Model 2](#_Toc31661310)

[Network Model Justification 2](#_Toc31661311)

[The Network Architecture 2](#_Toc31661312)

[The Network Topology 3](#_Toc31661313)

[Limiting Internet Access 3](#_Toc31661314)

[Managing Communication within the Network 4](#_Toc31661315)

[Shared File Systems 4](#_Toc31661316)

[Cyber Threats and Security Analysis 4](#_Toc31661317)

[Injection Attacks 5](#_Toc31661318)

[Broken Authentication 5](#_Toc31661319)

[Broken Access Control 5](#_Toc31661320)

[Evaluating Cyber Security 5](#_Toc31661321)

[Use of the Protocols 6](#_Toc31661322)

[The TCP/IP Stack 6](#_Toc31661323)

[The Transmission Control Protocol 6](#_Toc31661324)

[The Internet Protocol 6](#_Toc31661325)

[The Internet Control Message Protocol 7](#_Toc31661326)

[Bibliography 7](#_Toc31661327)

# The Network Model

# Network Model Justification

## The Network Architecture

When designing the Popleopolis network layout, ensuring that the proper designs and systems have been chosen is important for making sure that the system runs efficiently and properly. For the architecture of the network, I chose to use a Local Area Network Topology. This is because the communication between devices is only required within the building itself and doesn’t need to be accessible remotely. “*A local area network (LAN) is a collection of devices connected together in one physical location*” **(Cisco, n.d.),** which means that the Popleopolis network needs to be fitted for use within the building and nowhere else. This makes this architecture more suitable for this building than another commonly used architecture, WAN. A WAN (or Wide Area Network) is used when the network needs to reach several locations over a larger area, with the ability to connect devices that are otherwise separated by physical location **(Cisco, n.d.)**. This would be highly unnecessary for the Popleopolis building, as the building’s network doesn’t require a single network connection over several location, with all communications being managed within the building itself.

## The Network Topology

The network topology is an important factor in the cost and performance of the network, as the incorrect choices can lead to choke point and slowdowns within the network **(Mudrakola, n.d.)**. For this scenario, I chose the Star network topology, due to its benefits with fault management and speed. The key design principle for the star topology is that the end devices have their own separate connection. Similar to the shape of a star with protruding connections from the devices in the “centre” of the network. The switch(es) in the central point of the network acts as the connecting point between the devices and is used to funnel all communications and data being shared on the network **(Faircloth, 2013)**.

Having all communications run through central switches means that the devices do not rely on each other to pass data. Unlike other topologies, the star layout doesn’t require other devices on the network to be operational in order for communications to be passed through, this is because the switch acts as a central directing hub, and is the only system needed to connect two devices and share data between them. **(BBC Bitesize, n.d.)**.

Moreover, the use of the star topology means that the network is more adaptable to changes to device connections. Due to the direct connections to the switch, each end device never directly interacts or connects with another. This means that in the event that devices are added or removed, the routing for the communications doesn’t need to directly change **(Fcit.usf.edu, n.d.)**. Since the routing is done through the switch, the data routes do not need to be directly re-calculated as the path from the device to the switch never changes.

In contrast, the ring topology would not have been a suitable choice for this network scenario. If I had used the ring topology, the benefit of adaptability would not have been anywhere near as prevalent. Due to the design of the ring topology, if the layout of the network is changed, or one of the end devices fail – then the entire network suffers. Communications are passed through the network by passing through each device until it reaches the intended recipient, this means that of one of the devices in the path between the communicating devices fails, then the traffic will stop as it cannot pass **(Orava and Ramfelt, 2008)**. Due to the size of the Popleopolis network and the amount of traffic that would be active within it, using this topology would be inefficient and slow.

## Limiting Internet Access

One of the requirements for the network was that the Private Meeting Suites had their internet access restricted and so online capabilities are disabled. This means that no communications or packets can go between the devices in these rooms and the outside networks. To meet this requirement, I chose to use a firewall on the computers within the suites.

A firewall is a device used to monitor and manage incoming/outgoing traffic on a network **(Cisco, n.d.)**,this means that it can be used to block certain IP addresses from sending their packets through. While there is no way for a firewall to know every single possible IP address of a host that may try to send packets from the internet, only a single IP address is needed to block external traffic. The port of the router that is connected to the wider internet has its own IP address, and so any traffic that comes from outside of the network will be associated with said IP address. This means that setting a firewall to filter out packets related to the IP address of that port will stop communications between the PCs in the suites and the devices that are outside of the Popleopolis network.

## Managing Communication within the Network

Another of the requirements for the Private Meeting Suites in the Popleopolis building, was for these rooms to have an internal connection only – meaning that they are separate from the other PCs in the building. To meet this requirement, I used an IP access list to manage the IPs that are allowed to pass through. I chose to use these lists over a firewall as the specificity of IP addresses goes into more detail **(Burton et al., 2003)**.

As stated in another requirement for the network, the printers in the East and West wing rooms need to be accessible by any PC in the building, this means that if all IPs from the building were blocked for the Suites, then the PCs within wouldn’t be able to communicate with any of the printers. Using an IP Access List means that packets from the IP addresses belonging to only the printers will be accepted, while any other devices from the same room would be denied **(Cisco, n.d.)**.

## Shared File Systems

As per the requirements, each room in the building needs to have access to their own shared file system. In my design for the network layout, each of the file systems are stored within the Hardware Cupboards, but the content stored within them can only be accessed by PCs in the buildings. This is important for the security of the content in the files, as otherwise anyone could access potentially sensitive information. I provided security for these file systems by including a firewall to the severs the information is stored on. As mentioned previously, the firewalls can be used to block communications from outside the internal network, and so stopping anyone who isn’t logged onto a computer in the building from accessing the content.

# Cyber Threats and Security Analysis

As more aspects of organisations’ systems become digitalised, the opportunities for cyber-attacks and vulnerabilities also increase. When implementing this new network model, there are a range of threats that must be considered by the system administrators. Without the use of proper cyber-security, those who use the network and the data stored on it, can be susceptible to a range of risks. According to the OWASP Top 10, one of the top cyber security risks is Injection. The OWASP is a trusted non-profit organisation that focuses on web application security, their top 10 list is designed to highlight the biggest risks to cyber security as of current **(Owasp.org, 2017)**.

## Injection Attacks

Injection attacks are a common attack type that rely on breaking the inputs in applications to inject malicious code into the system **(Running an SQL Injection Attack - Computerphile, 2016)**. Through breaking the system for reading user inputs, the attacker’s own commands can be run through the inputs and can allow the user to gain access to data and systems that would otherwise be inaccessible. If the data and information stored within a system is banked in the same area as the user inputs, then it becomes vulnerable to injection attacks.

If characters are entered into an input that break the system’s ability to differentiate between input text and commands, then text that is entered (that may contain commands readable by the system) can be run as if it was a command **(Alvarez, 2017)**. Through this type of attack, the vulnerable data can include user logins and private information on users that could be dangerous if leaked out to the public, such as addresses and passwords **(Owasp.org, n.d.)**.

## Broken Authentication

Another cyber threat that could be a risk to those in the Popleopolis building is that of Broken Authentication. Ensuring that only users that are supposed to have access to a system are able to get in, as otherwise anyone could gain entrance to the private data relating to the organisation and the users of the system. If the proper authentication is not checked on those attempting to login to the system, any password or login combination could be used to break into a recognised user’s account **(Owasp.org, n.d.)**.

Broken authentication doesn’t just include the incorrect management of entered logins, as session tokens can lead to unauthorised access. Upon authenticating a user’s identity into the system, that user’s login session is given a unique ID to prove that the login is genuine; upon logging out: the session is listed as terminated and so the ID is no longer valid. If the tokens are not properly managed, then it can lead to multiple users logging in under the same session token **(Hassan et al., 2018)**. This means that people can impersonate recognised users and gain access to files and information that would otherwise be off limits.

## Broken Access Control

Properly ensuring that data is only accessible by those who are authorised to view it helps prevent the prevalent cyber threat of Broken Access Control. Poor detection and authorisation of those who are using a system can lead to people having the ability to manage content above their access level **(Owasp.org, n.d.)**. Through managing the content on the Popleopolis network, users with unauthorised access could obtain and edit user data and logins; potentially crippling the security and business processes of the different industries using the building’s facilities.

## Evaluating Cyber Security

These above cyber-attacks help highlight how important Cyber Security is to a network, and how not putting the proper safeguards in place can be detrimental for the businesses as well as the Popleopolis building itself.

In the case that a business that is renting out an office space is the victim of a cyber-attack due to poor cyber security on the network, they may attempt to claim compensation from the Popleopolis building. Network providers are often seen at blame for cyber-attacks on their networks, and so would suffer reciprocation from the business using it **(Shackelford, 2012)**.

# Use of the Protocols

## The TCP/IP Stack

The TCP/IP stack is an important part of any network. It is a collection of network protocols; these protocols are an umbrella term used to describe systems that manage how packets and data are used **(Kozierok, 2005)**. This stack is sorted into several layers, which are used to identify what functionality to the network the protocols on that layer have. The four layers of the TCP/IP stack are:

* The Application Layer
* The Transport Layer
* The Internetwork Layer
* The Link Layer

## The Transmission Control Protocol

One of the most important of these protocols that I used when designing the network is the Transmission Control Protocol, which is a part of the Transport Layer. This is one of the most important of these protocols, due to its importance in communication between devices. When two devices are communicating, the information is sent through packets across the network and its components, until the intended recipient is reached. In the case of the Popleopolis network, with the large number of devices that each need to communicate with each other, the traffic that would be simultaneously passing through the network would be large and could potentially be overwhelming. This is the prime example of why the TCP (Transmission Control Protocol) is important, as it manages the flow for the packets to help ensure that there is no overflow or congestion **(Obaidat, Nicopolitidis and Zarai, 2015)**.

## The Internet Protocol

Another of the protocols in this stack that are very important to the design of the Popleopolis network is the Internet Protocol, which is a part of the Internetwork Layer. In many ways this protocol is the backbone for the entirety of the network and its features, as without it the transmission of data on the network would not be possible. The use of IP addresses on the packets of data passing through the network are used to identify where information is destined along with where it has come from. Without the identifiers made available from this protocol, then the packets would be unable to reach its intended location. This is because the protocol allows for the packets to be sent through each device until one matching the intended location is reached, otherwise without the IP the devices would not know where to send the packets to next, and so would be dropped by the network **(Postel, Sunshine and Cohen, 1981)**.

## The Internet Control Message Protocol

As well as these, the Internet Control Message Protocol (ICMP) is another of the Internetwork protocols that is used in the Popleopolis Network. The purpose of this protocol is to send and manage messages sent to devices relating to the success status of the sent packets. The ICMP runs in unison with the Internet Protocol, with the potential error messages being sent to the device that sent out the packets using IP **(Ziegler, 2008)**. Without the use of this protocol in the network, devices sending out packets of data would be unaware of any issues that prevent the data from reaching its intended recipient, as there would be no message displayed to them.

# Bibliography

Alvarez, M. (2017). *Injection Attacks: The Least Glamorous Attack Is One of the Most Threatening*. [online] Security Intelligence. Available at: https://securityintelligence.com/injection-attacks-the-least-glamorous-attack-is-one-of-the-most-threatening/ [Accessed 27 Jan. 2020].

BBC Bitesize. (n.d.). *Network topologies, protocols and layers - OCR - Revision 1 - GCSE Computer Science - BBC Bitesize*. [online] Available at: https://www.bbc.co.uk/bitesize/guides/zr3yb82/revision/1 [Accessed 25 Jan. 2020].

Burton, J., Dubrawsky, I., Osipov, V., Baumrucker, C. and Sweeney, M. (2003). *Cisco security professional's guide to secure intrusion detection systems*. Rockland, Mass.: Syngress.

Cisco. (n.d.). *What Is a Firewall?*. [online] Cisco. Available at: https://www.cisco.com/c/en\_uk/products/security/firewalls/what-is-a-firewall.html [Accessed 1 Feb. 2020].

Cisco. (n.d.). *Configuring IP Access Lists*. [online] Available at: https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/23602-confaccesslists.html [Accessed 1 Feb. 2020].

Cisco. (n.d.). *Cisco Global Learning Network*. [online] Available at: https://www.cisco.com/web/learning/netacad/demos/CCNA2v3Demo/ch1/1\_1\_1/index.html [Accessed 1 Feb. 2020].

Cisco. (n.d.). *What is a LAN? Local Area Network*. [online] Available at: https://www.cisco.com/c/en/us/products/switches/what-is-a-lan-local-area-network.html [Accessed 1 Feb. 2020].

*Running an SQL Injection Attack - Computerphile*. (2016). [video] England: Computerphile.

Faircloth, J. (2013). *Enterprise Applications Administration*. Elsevier Science.

Hassan, M., Nipa, S., Akter, M., Haque, R., Deepa, F., Rahman, M., Siddiqui, M. and Sharif, M. (2018). Broken Authentication and Session Management Vulnerability: A Case Study of Web Application. *International journal of simulation: systems, science & technology*. [online] Available at: https://pdfs.semanticscholar.org/d9e1/35b38ba641e78bd60c2fc1de97d73ea019ff.pdf.

Kozierok, C. (2005). *The TCP/IP guide*. San Francisco: No Starch Press, pp.11-12.

Mudrakola, S. (n.d.). *Network topology guide: Why it’s crucial you build the right structure*. [online] TechGenix. Available at: http://techgenix.com/network-topology/ [Accessed 25 Jan. 2020].

Obaidat, M., Nicopolitidis, P. and Zarai, F. (2015). *Modeling and simulation of computer networks and systems*.

Orava, F. and Ramfelt, L. (2008). *Method of sending information through a tree and ring topology of a network system*. US7391771B2.

Owasp.org. (2017). *OWASP Top Ten*. [online] Available at: https://owasp.org/www-project-top-ten/ [Accessed 24 Jan. 2020].

Owasp.org. (n.d.). *A1-Injection | OWASP*. [online] Available at: https://owasp.org/www-project-top-ten/OWASP\_Top\_Ten\_2017/Top\_10-2017\_A1-Injection [Accessed 27 Jan. 2020].

Owasp.org. (n.d.). *A2-Broken Authentication | OWASP*. [online] Available at: https://owasp.org/www-project-top-ten/OWASP\_Top\_Ten\_2017/Top\_10-2017\_A2-Broken\_Authentication [Accessed 27 Jan. 2020].

Owasp.org. (n.d.). *A5-Broken Access Control | OWASP*. [online] Available at: https://owasp.org/www-project-top-ten/OWASP\_Top\_Ten\_2017/Top\_10-2017\_A5-Broken\_Access\_Control [Accessed 29 Jan. 2020].

Postel, J., Sunshine, C. and Cohen, D. (1981). The ARPA internet protocol. *Computer Networks (1976)*, 5(4), pp.7-9.

Shackelford, S. (2012). Should your firm invest in cyber risk insurance?. *Business Horizons*, 55(4), pp.349-356.

Ziegler, M. (2008). Internet control message protocol. p.3.