BLU16274423

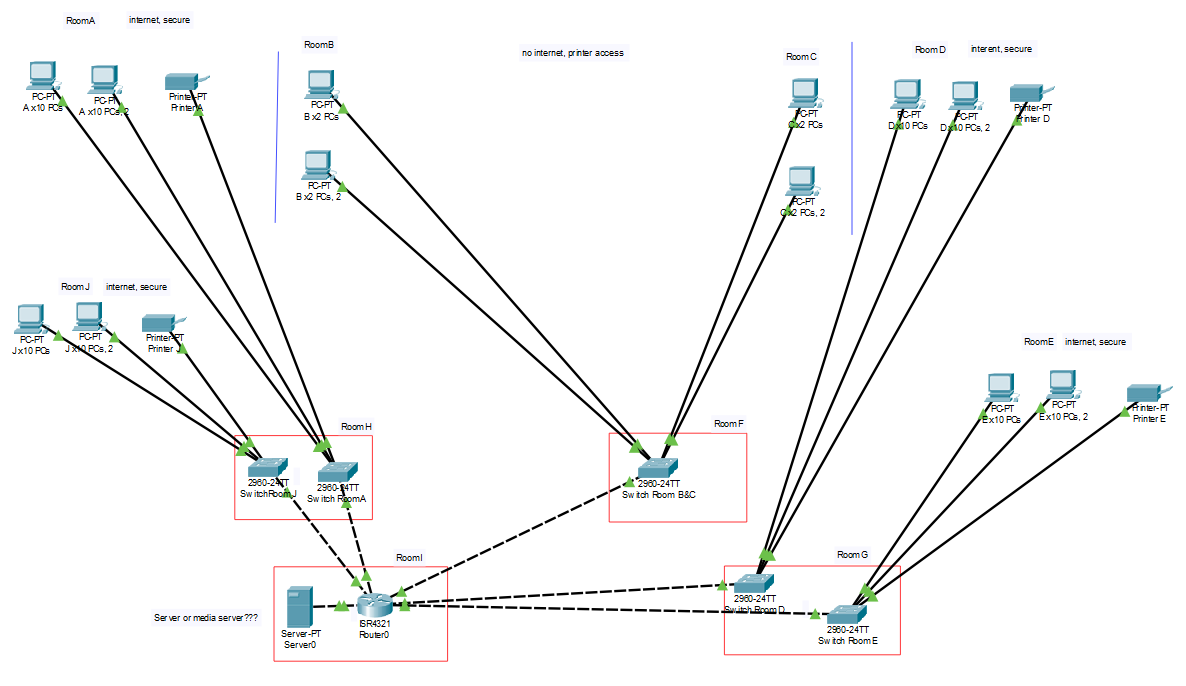
Toby bluck  Word count: 1977

SCDT43 CW1

Network Architectures, Protocols and Cyber Vulnerabilities

# PT1 -

## Justification of PacketTracer Model

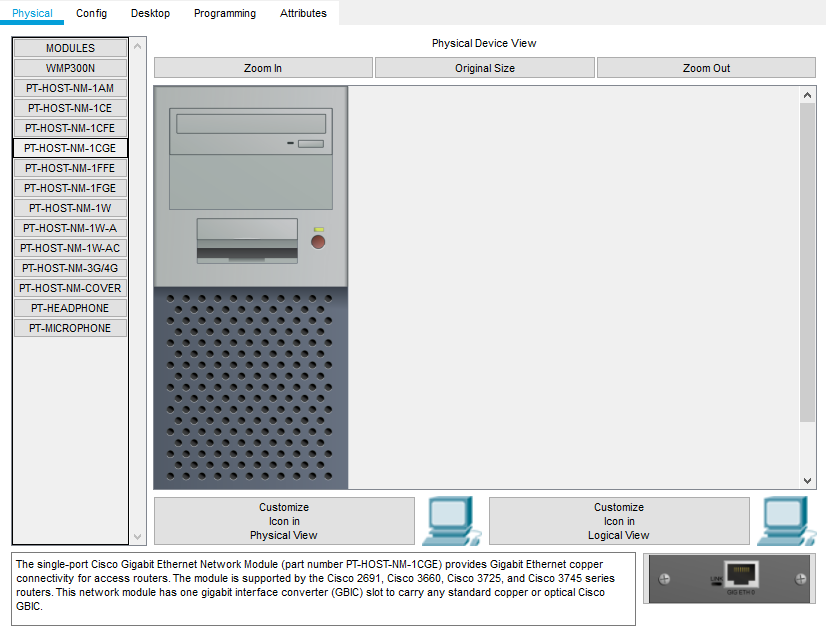


This network model is for the Popleoplis building, each section has been broken up into the designated rooms from room A – J, room A, D, E and J are rooms which used for internet access, rooms B and C have no internet access though the denying of IP address with an access list on the router. Rooms F, G, H and I are used as storage to store the switches, router and sever. All PCs are connected to a switch designated for that room using a gigabit connection from PC to Switch. From the switch to the router it uses a Copper cross over cable to gigabit ports. This allows for communication to all system by going through the router to be directed to the correct end point.

## Network architecture

Resources accessible within the network, printer are accessible throughout the building through routing, within the meeting rooms they are able to access the printers within the other rooms, file transferring is supported and can be used to store files on the server. Emails are accessible on all computers except the meeting room computers as they have local connection. Web browsing is accessible.

Cabling used: there is copper straight through on all PCs and printers which would be classed as Cat6 Ethernet using a RJ-45 connector, this would allow for gigabit transfer on the network for up to 100 meters. Copper cross over is used to connect anything to the router, this would still use Cat6 Ethernet as this would allow for gigabit speeds to persist over the network to have a full gigabit network meaning there is no bottle necks. (Gigabit Ethernet, 2020), (What is a Category 6 Cable (Cat 6 Cable)? - Definition from Techopedia, 2020)

Connections: all PCs are equipped with the PT-HOST-NM-1CGE, module which is a single port connection for the PC which had gigabit connectivity which uses a RG45 connection. Connections from the switches and server to the router all function off gigabit connections allowing for the fastest data transfer speeds. 

Protocols used: DHCP is used for the simplified task of network management with auto assigned IP addresses (Advantages of Using DHCP - Oracle Solaris Administration: IP Services, 2020), FTP is used to allow for the transferring of file from PCs to the server for central file storage, HTTP this protocol is used for the access to websites from the web browsers, SMTP & POP3 are used for the incoming and out going emails from the server. (POP and SMTP - smtp mail server - professional SMTP service provider, 2020)

Future plans: this network can be expanded in the future to support more systems, potentially a wireless network to create a mesh topology wirelessly with heightened security and more routers to enable RIPv2. (DCN - Computer Network Topologies - Tutorialspoint, 2020).

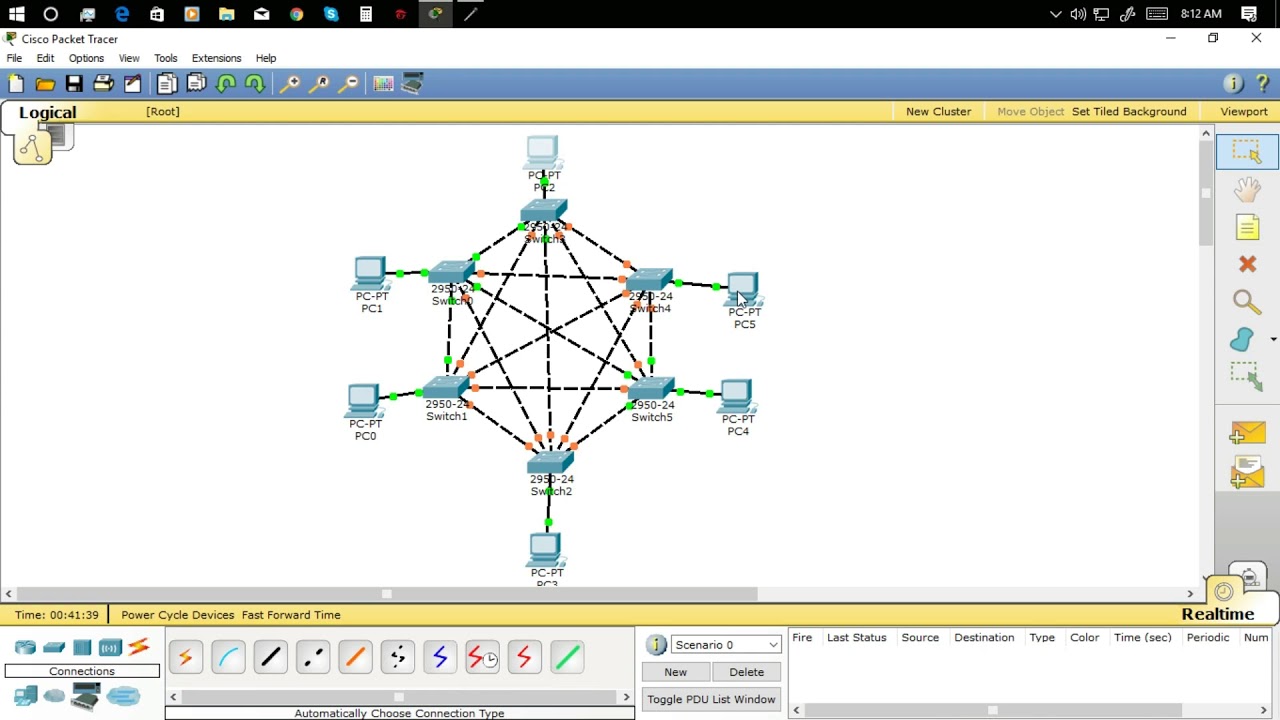
## Topology and routing protocol

The network that has been made for the Popleopolis building uses a standard star topology, this has been used as the router is used as a central device for the network. Where switches are connected to the router, they are used as a repeater for the systems which are connected to the switch. This topology is relatively cheap to do which simple cabling and can allow systems to go down without affecting the whole network. RIP/RIPv2 is not used within this network as there is only one router to make routing tables etc. and does not need another router to routing information throughout the network. (IP Routing: RIP Configuration Guide, Cisco IOS Release 15M&T - Configuring Routing Information Protocol [Cisco IOS 15.4M&T], 2020), (RIP Configuration in Packet Tracer | Step By Step Guide, 2020), (DCN - Computer Network Topologies - Tutorialspoint, 2020).

## Other options being discounted.

A better different topology could be used such as mesh or a hybrid topology could be used such as star and ring, this would add an extra level of complexity to the network and make configuration and cost exponentially more. For a full mesh network, it would be classified as the most reliable but will be exponentially more complexed and will incur greater costs due to more cable being used. This is unneeded for a small-scale network like this. (DCN - Computer Network Topologies - Tutorialspoint, 2020).

### An example of a mesh network in PacketTracer: figure 1



(Bayani, 2017)

# PT 2-

## Vulnerabilities

Software vulnerabilities are sometimes a problem, which can be made apparent through attacks or researchers, recently a large vulnerability that has affected the Windows 10 & Server 2016, 2019 was unearthed by the NSA (National Security Agency). The vulnerability was called CryptoAPI spoofing vulnerability, this allowed for EEC certificate validation to be bypassed by a malicious software which could be made out to look like a trusted source, which allows for antivirus and users to be tricked into installing the malicious software, this is detrimental to organisations as it would allow for attackers to read/write, modify and delete data. Overall, vulnerabilities are patched very quickly if they have a large security flaw but should always be kept in mind that software updates should be performed routinely. Most attacked that are carried out exploit vulnerabilities, this can lead to a varying amount of damage such as loss of customer data, which would violate GDPR 2018 Laws and also cost the organisation depending on size anywhere between £3.9m to £1.4bn. (Critical Vulnerabilities in Microsoft Windows Operating Systems | CISA, 2020), (Weekly Threat Report 17th January 2020, 2020), (NCA, 2018), (The Cost of Cyber Crime), (Understanding vulnerabilities, 2015)

## Malicious Emails

Within organisations, malicious emails are prevalent with approximately 1 in 412 sent in 2018 being malicious, these emails are used to spread malware to gain access to information or destroy data within an organisation, phishing is used to deceive the user and either buy or give money to a sender, or give sensitive information about them or an organisation, spam emails sometimes are spoofed allowing for the identity of the sender to disguise itself as something more legitimate. From these emails they normally use scripts (48%) and/or file to be executes such as. exe’s (26%) other forms (24%). These will when downloaded or ran, will activate and start to spread malware or malicious software or direct them to a malicious website. Within the software and computer services, its predicted that malicious software that has been distributed and/or attack cost a total of £1.6Bn in the UK. in the last few years this method has continued to grow as a steady pace with all emails sent in 2018 55% of them were to be classified as spam which is directly linked to phishing and malicious intentions within emails. Malware is used in many forms to attack a user, the one which has drastically increased (approx. 100ish% in 2018) is PowerShell scripts, which is normally triggered when an office document is open from an email. JS/VBS.Downloaders are still common but on the decline due to being easily picked up by anti-virus. This can do any number of things, such as creating files to slow the system, backdoors and error messages but unknown word documents should be scanned and not opened if from an unknown source. (Stine & Scholl, 2020), (ISTR, 2019), (Get Safe Online, 2020), (The Cost of Cyber Crime)

## What is cyber security?

Cyber security is the way of securing systems and networks from attacks or any unauthorised access to them. This allows for the confidentiality and integrity of data being transported or stored, there are risks of having poor cyber security and ways how it can be improved. Poor cyber security will allow for attackers to easily gain access and cause damages and/or steal data. The best way to maintain a decent level of cyber security is implement well configured firewalls, multi-factor authorisation on systems complexed passwords and up to date software and antivirus. (What is Cybersecurity? | CISA, 2019), (What is cyber security?, 2020)

## Advantages & disadvantages

Due to cybersecurity playing a large role within organisations, usable cyber security is a key consideration. Planning in the early stages for usability with cyber security and the implementation of its methods, the security should allow for all users to be fully accommodated when using systems or networks, a good amount of documentation of security and advice when using its functionality, designing the security so that all layers of system are covered, security should not compromise performance. Problems occur in cyber security when inadequate configuration of tools are made mainly firewalls, but other tools as well. In 2018 there was roughly 348 million web attacks, this takes into account targeted attacks on organisations, poorly configured firewalls could allow these attacks to get through and cause hefty amounts of damage. (ISTR, 2019), (Nurse et al., 2011), (Uma et al., 2013)

# PT 3-

## TCP/IP

TCP/IP is a collection of protocols used for communication with a network this is used in both internal and external networks. This set of protocols are used to create the foundation and rules of the exchanging of data, this states the break down of information into packets, how they are addressed, the transmission and routing of packets until they are received by the end point. TCP is used to define how to communicate throughout a network and the breaking down of data into packets, and the transmission of them, to the end point where they would be order and assembled again. IP in the stack is used to define the address of the devices and route the packets in the correct direction to the end point. (Rouse, 2020)

TCP/IP model can be broken down into 4 layers:

Application: this allows applications to exchange data, the protocols which utilise this layer are FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol) & HTTP (Hyper Text Transfer Protocol) etc.

Transport: this is used for the communication from point to point, TCP is used for the handling of communication between host and end point with a control over the data flow. UDP (User Datagram Protocol) is used in special situations, where a constant stream of data without error correction is needed.

Network/Internet: this layer handles the packets of data, and the connection between networks for the transportation by using the IP.

Physical/Link: this layer is used for the data transmission within the network physically between nodes and end point i.e Ethernet (most common). (Wilkins, 2011), (Rouse, 2020)

## Application Layer protocols:

FTP: is used in the TCP/IP which is classed as a client server protocol, establishes 2 connections, port 20 is used for the data connection, port 21 is used for the control connection, the data connection is only used while there is data transfer occurring. The control connection sends commands to establish a data connection and will be open for the duration of a session. Authentication is needed when sending or requesting data and once established port 20 will be open for connection on both systems. (Shimonski et al., 2002), (Internet Protocols - Tutorialspoint, 2020)

HTTP: is used in TCP/IP to transfer data from the internet, this is used to establish a connection between a client and server, the client requests data and the server sends it, this is done on port 80 on the server. The request sent by the client has a URI (Universal Resource Identifier) which allows the server to locate the data needed to transfer. (Insam, 2003)

SMTP, POP3: SMTP is used to send, POP3 is used to receive, delete and managing mail. SMTP operates on port 25 as a default unless it is secure which would be port 465. POP3 uses port 110 and port 995 if it is needed to be secure. (Insam, 2003), (Email Protocols - POP3, SMTP and IMAP Tutorial, 2020)

DHCP: this is used within TCP/IP to automatically assign the addresses of devices, typically they automatically configure the IP address, gateway and subnet mask. A DCHP server can manage the IP address available in a pool, however the lease time will cause them to change unless specified. (Liu, et al., 2009)

## Routing & relationships

The application layer in the TCP/IP stack is used for the application protocols to provide the services on a running application within the system. The relationship between the application layer and the application protocols is that the layer is used to specify the services needed for an application. This allows for the application layer to integrate the application on the system to the network itself.

### Application layer > transport layer

The transport layer is at a higher level in the stack then the application layer but can be used to provide error recovery in TCP for the application layer. This allows for the checking of the delivery of data over a network, application layers protocols such as FTP would need to ensure that packets have successfully been delivered without loss as this would render the data corrupt. Within the TCP, the TCP header is given a sequence number for each packet, when transported the receiver then checks the sequence number i.e. 1-5 and if 3 is not received, then it is requested again until it is received where it can be compiled by the receiver. This is used for all application protocol unless UDP is used. Error recovery is very beneficial for HTTP, FTP, SMTP, POP3 protocols.

(The Transport Layer in TCP/IP Model, 2020), (Wilkins, 2011), (Odom, 2011), (Hunt, 2002)

References

|  |
| --- |
| References |
| Advantages of Using DHCP - Oracle Solaris Administration: IP Services (2020) Docs.Oracle.Com, [Online]. Available at https://docs.oracle.com/cd/E23824\_01/html/821-1453/dhcp-overview-12a.html (Accessed 2020). |
| Bayani, J. (2017) Cisco Packet Tracer (Mesh Topology Tutorial), [Online]. Available at https://i.ytimg.com/vi/oKwLEdIdKGo/maxresdefault.jpg (Accessed 2020). |
| Critical Vulnerabilities in Microsoft Windows Operating Systems | CISA (2020) Us-Cert.Gov, [Online]. Available at https://www.us-cert.gov/ncas/alerts/aa20-014a (Accessed 2020). |
| DCN - Computer Network Topologies - Tutorialspoint (2020) Tutorialspoint.Com, [Online]. Available at https://www.tutorialspoint.com/data\_communication\_computer\_network/computer\_network\_topologies.htm (Accessed 2020). |
| Email Protocols - POP3, SMTP and IMAP Tutorial (2020) Siteground, [Online]. Available at https://www.siteground.com/tutorials/email/protocols-pop3-smtp-imap/ (Accessed 2020). |
| Get Safe Online (2020) Getsafeonline.Org, [Online]. Available at https://www.getsafeonline.org/protecting-your-computer/spam-and-scam-email/ (Accessed 2020). |
| Gigabit Ethernet (2020) Tutorialspoint.Com, [Online]. Available at https://www.tutorialspoint.com/gigabit-ethernet (Accessed 2020). |
| Hunt, C. (2002) TCP/IP Network Administration, 3rd Edition, O’Reilly Online Learning, [Online]. Available at https://www.oreilly.com/library/view/tcpip-network-administration/0596002971/ch01.html (Accessed 2020). |
| Insam, E. (2003) Application Layer Protocol - an overview | ScienceDirect Topics, Sciencedirect.Com, [Online]. Available at https://www.sciencedirect.com/topics/computer-science/application-layer-protocol (Accessed 2020). |
| Internet Protocols - Tutorialspoint (2020) Tutorialspoint.Com, [Online]. Available at https://www.tutorialspoint.com/internet\_technologies/internet\_protocols.htm (Accessed 2020). |
| IP Routing: RIP Configuration Guide, Cisco IOS Release 15M&T - Configuring Routing Information Protocol [Cisco IOS 15.4M&T] (2020) Cisco, [Online]. Available at https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute\_rip/configuration/15-mt/irr-15-mt-book/irr-cfg-info-prot.html#GUID-3BDFB323-19CF-4D86-BC69-A398128A83D2 (Accessed 2020). |
| ISTR (2019) Internet Security Threat Report, Symantec [Online]. Available at https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf (Accessed 2020). |
| NCA, (2018) The Cyber Threat To UK Businesses, National Cyber Security Centre [Online]. Available at https://www.nationalcrimeagency.gov.uk/who-we-are/publications/178-the-cyber-threat-to-uk-business-2017-18/file (Accessed 2020). |
| Nurse, J., Creese, S., Goldsmith, M. and Lamberts, K. (2011) Guidelines for usable cybersecurity: Past and present, 2011 Third International Workshop On Cyberspace Safety And Security (CSS), . |
| Odom, W. (2011) Foundation Topics > The TCP/IP and OSI Networking Models, Ciscopress.Com, [Online]. Available at http://www.ciscopress.com/articles/article.asp?p=1757634&seqNum=2 (Accessed 2020). |
| POP and SMTP - smtp mail server - professional SMTP service provider (2020) Smtp Mail Server - Professional SMTP Service Provider, [Online]. Available at https://serversmtp.com/pop-and-smtp/ (Accessed 2020). |
| RIP Configuration in Packet Tracer | Step By Step Guide (2020) Protechgurus, [Online]. Available at https://protechgurus.com/configure-rip-routing-cisco-packet-tracer-ripv2/ (Accessed 2020). |
| Rouse, M. (2020) What is TCP/IP and How Does It Work?, Searchnetworking, [Online]. Available at https://searchnetworking.techtarget.com/definition/TCP-IP (Accessed 2020). |
| Shimonski, R. and Gordienko, Y. (2002) file transfer protocol - an overview, Sciencedirect.Com, [Online]. Available at https://www.sciencedirect.com/topics/computer-science/file-transfer-protocol (Accessed 2020). |
| Stine, K. and Scholl, M. (2020) E-mail Security: An Overview of Threats and Safeguards, Library.Ahima.Org, [Online]. Available at http://library.ahima.org/doc?oid=99319 (Accessed 2020). |
| The Cost of Cyber Crime, Assets.Publishing.Service.Gov.Uk, [Online]. Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\_data/file/60943/the-cost-of-cyber-crime-full-report.pdf (Accessed 2020). |
| Uma, M. and Padmavathi, G. (2013) A Survey on Various Cyber Attacks and Their Classification, International Journal Of Network Security, vol. 15, no. 5, pp. 390 - 396 [Online]. Available at https://pdfs.semanticscholar.org/ba7b/234738e80b027240e9bfd837bfba61c13e17.pdf (Accessed 2020). |
| Understanding vulnerabilities (2015) Ncsc.Gov.Uk, [Online]. Available at https://www.ncsc.gov.uk/information/understanding-vulnerabilities (Accessed 2020). |
| Weekly Threat Report 17th January 2020 (2020) Ncsc.Gov.Uk, [Online]. Available at https://www.ncsc.gov.uk/report/weekly-threat-report-17th-january-2020 (Accessed 2020). |
| What is a Category 6 Cable (Cat 6 Cable)? - Definition from Techopedia (2020) Techopedia.Com, [Online]. Available at https://www.techopedia.com/definition/17070/category-6-cable-cat-6-cable (Accessed 2020). |
| What is cyber security? (2020) Ncsc.Gov.Uk, [Online]. Available at https://www.ncsc.gov.uk/section/about-ncsc/what-is-cyber-security (Accessed 2020). |
| Wilkins, S. (2011) OSI and TCP/IP Model Layers | OSI and TCP/IP Model Layers | Pearson IT Certification, Pearsonitcertification.Com, [Online]. Available at http://www.pearsonitcertification.com/articles/article.aspx?p=1804869 (Accessed 2020). |