

1809809

by Rhys Davies

Submission date: 29-May-2022 10:32PM (UTC+0100)

Submission ID: 181970034

File name: 16479_Rhys_Davies_1809809_169044_1780376205.pdf (3.52M)

Word count: 12313

Character count: 59080

HND Electrical And Electronic Engineering
PSDE5034 - Networking Systems For Engineers
Assignment - Network Design for
Industry using CIDR
Subnetting

Author: Rhys Davies (1809809)

29th May 2022

Word Count: 10,632

Table Of Contents:

	Page:
List Of Figures:	3
Element 1	5
1. Introduction	5
2. Research	6
3. Design Requirements	14
4. Implementation	16
5. Test & Analysis	26
6. Evaluation	30
Element 2	31
1. Introduction	31
2. System Configuration Requirements	32
3. Implementation	38
4. Test & Analysis	47
5. Evaluation	50
Element 3	51
1. Introduction	51
2. System Configuration Requirements	52
3. Implementation	53
4. Test & Analysis	61
5. Conclusions & Recommendations	64
Citation List	65
Appendix	66

List Of Figures:

	<u>Page:</u>
Figure 1 - Typical Layering Model (Imperva - 2022)	6
Figure 2 - 7 Layer Vs 4 Layer OSI Model (Comer, D.E. - 2015)	8
Figure 3 - 4 Layer 4 vs. 7 Layer Load Balancing Comparison Table (Medium, 2022)	9
Figure 4 - Encapsulation Vs Decapsulation (ComputerNetworkingNotes, 2022)	10
Figure 5 - Element 1 Network Overview	14
Figure 6 - Class 'A' Network Subnet Configuration	14
Figure 7 - Class 'B' Network Subnet Configuration	15
Figure 8 - Class 'C' Network Subnet Configuration	15
Figure 9 - Network Overview - Static Routing	16
Figure 10 - Router 1 (Left) Static Routing	17
Figure 11 - Router 3 (Centre) Static Routing	17
Figure 12 - Router 2 (Right) Static Routing	18
Figure 13 - Router 1 (Left) Routing Table	18
Figure 14 - Router 3 (Centre) Routing Table	18
Figure 15 - Router 2 (Right) Routing Table	19
Figure 16 - Router 1 (Left) Dynamic Routing Commands	20
Figure 17 - Router 1 (Left) Dynamic Routing Table	20
Figure 18 - Router 3 (Centre) Dynamic Routing Commands	20
Figure 19 - Router 3 (Centre) Dynamic Routing Table	20
Figure 20 - Router 2 (Right) Dynamic Routing Commands	21
Figure 21 - Router 2 (Right) Dynamic Routing Table	21
Figure 22 - Network Overview - DHCP Address Routing	22
Figure 23 - Router 3 (Left) DHCP Allocation - Router Programming	23
Figure 24 - Router 1 (Middle) DHCP Allocation - Helper Address Programming	23
Figure 25 - Router 2 (Right) DHCP Allocation - Helper Address Programming	24
Figure 26 - Router 3 (Left) DHCP Allocation - Address Exclusions	25
Figure 27 - Static Routing - Packet Test Results	26
Figure 28 - Dynamic Routing - Packet Test Results	26
Figure 29 - PC1 (Left) DHCP Test without Helper Address	27
Figure 30 - PC2 (Middle) DHCP Test without Helper Address	27
Figure 31 - PC3 (Right) DHCP Test without Helper Address	27
Figure 32 - PC2 (Middle) DHCP Test with Helper Address	28
Figure 33 - PC3 (Right) DHCP Test with Helper Address	28
Figure 34 - PC1 (Left) DHCP Address - Post Exclusions	29
Figure 35 - PC2 (Middle) DHCP Address - Post Exclusions	29
Figure 36 - PC3 (Right) DHCP Address - Post Exclusions	29
Figure 37 - 3 Router WAN - Network Overview	32
Figure 38 - CIDR/28 Subnet Configuration Overview	32
Figure 39 - Rome Network - Network IP Configuration	33
Figure 40 - Paris Network - Network IP Configuration	33
Figure 41 - London Network - Network IP Configuration	33
Figure 42 - London - Rome Network - Serial IP Configuration	34
Figure 43 - Rome - Paris Network - Serial IP Configuration	34
Figure 44 - Paris - London Network - Serial IP Configuration	34
Figure 45 - CIDR27 & 30 Network Subnet Configuration	35
Figure 46 - Rome Network - CIDR28 > CIDR27 IP Configuration Changes	35

Figure 47 - Paris Network - CIDR28 > CIDR27 IP Configuration Changes	36
Figure 48 - London Network - CIDR28 > CIDR27 IP Configuration Changes	36
Figure 49 - London - Rome Network - CIDR28 > CIDR30 Serial IP Configuration Changes	37
Figure 50 - Rome - Paris Network - CIDR28 > CIDR30 Serial IP Configuration Changes	37
Figure 51 - Paris - London Network - CIDR28 > CIDR30 Serial IP Configuration Changes	37
Figure 52 - Rome Router - CIDR/28 Programming	38
Figure 53 - Paris Router - CIDR/28 Programming	38
Figure 54 - London Router - CIDR/28 Programming	38
Figure 55 - Rome Router - CIDR/27&30 Programming	40
Figure 56 - Paris Router - CIDR/27&30 Programming	40
Figure 57 - London Router - CIDR/27&30 Programming	40
Figure 58 - Rome Router - CIDR/27&30 Show IP Route	41
Figure 59 - Paris Router - CIDR/27&30 Show IP Route	41
Figure 60 - London Router - CIDR/27&30 Show IP Route	42
Figure 61 - 3 Router Network - VLAN Representation	43
Figure 62 - London Router - VLAN Show IP Results	44
Figure 63 - Paris Router - IP Address Deny Configuration	45
Figure 64 - Paris Router - IP Address Deny 'Show Run'	46
Figure 65 - CIDR28 Routing - Packet Test Results	47
Figure 66 - CIDR27&30 Routing - Packet Test Results	47
Figure 67 - VLAN Network - Packet Test Results	48
Figure 69 - London PC2 > PC1 - Ping Results	48
Figure 70 - London PC2 > PC1 - Ping Results	49
Figure 71 - Element 3 Network Overview	52
Figure 72 - Element 3 Finalised Network Map	53
Figure 73 - Element 3 Switch VLAN Creation	53
Figure 74 - Element 3 Switch VLAN Port Assigning	54
Figure 75 - Element 3 Router VLAN Programming	55
Figure 76 - Element 3 Router - 'Show IP Brie' Result	55
Figure 77 - Siemens S7-1200 PLC - Set IP Address	56
Figure 78 - Siemens S7-1200 - Web Server Activation	56
Figure 79 - Siemens S7-1200 - User Defined Pages	57
Figure 80 - Siemens S7-1200 PLC - Web Server Function Call Block	57
Figure 81 - Siemens S7-1200 PLC - Web Server Function Call Block	58
Figure 82 - Siemens S7-1200 PLC - IO Tag List	58
Figure 83 - Siemens S7-1200 PLC - User Files	59
Figure 84 - Siemens S7-1200 PLC - Web Server Default Page	59
Figure 85 - Siemens S7-1200 PLC - Motor PWM Flow Diagram	60
Figure 86 - Siemens S7-1200 PLC - Motor Run Status Flow Diagram	60
Figure 87 - Network Terminal - Ping Test to PLC & PLC Terminal	61
Figure 88 - PLC Terminal - Ping Test to PLC & Network Terminal	61
Figure 89 - S7-1200 Web Server Motor Test - 60% PWM Output	62
Figure 90 - S7-1200 IO Tag List Monitoring - 60% PWM Output	62
Figure 91 - S7-1200 Web Server Motor Test - 90% PWM Output	63
Figure 92 - S7-1200 IO Tag List Monitoring - 90% PWM Output	63
Figure 93 - VLAN London Switch - VLAN Naming	66
Figure 94 - VLAN London Switch - VLAN Port Assigning	67
Figure 95 - VLAN London Switch - VLAN Trunk Assigning	68

Element 1

1. Introduction

This assignment will research and investigate how different types of networks such as LAN and Wan networks are constructed and configured, specifically focussing on how the 3 different Classes available are configured and how they can be interconnected so that successful comms can be established.

With communications established, we will investigate how address pools can be assigned, together with exclusion addresses for static IP reservations.

Finally, the network will be developed to a ring style network so that communication can take various routes to reach the intended destination.

With numerous LAN clients, the use of VLANs will allow a LAN network to be segregated so that client isolation and presentation can be achieved.

Good outline of task that indicated a good understanding of the requirements (this proves that the brief has been studied).

2. Research

OSI 7 Layer and 4 Layer Models with reference to the network design

Communication within a network context must involve at least two separate network entities, whether situated in the same local network or part of separate networks, conjoined by other networks. This communication is the sending and receiving of various forms of data. Network communication also include system entities that merely intend to forward on data that is passed to them, for retransmission across vast distances. What we must highlight is that for communication to be effective and success, all entities on the network must come to a mutual agreement on the format, speed and method that it is sent and interpreted for communication to work. (Comer, D.E. - 2015) [The essence of a network link](#)

The data sent across a network must be ensured that it has been constructed in such a way that it is complete and without any form of error. The overall communication protocol used within a network relies on different protocols. This means that each protocol is handled at different stages and constructed as it is being built. But instead of each protocol made separately and collaborated at the end of the process, each protocol is constructed in its entirety before being incorporated in the next protocol as it builds before being sent.

7	Application Layer	Human-computer interaction layer, where applications can access the network services
6	Presentation Layer	Ensures that data is in a usable format and is where data encryption occurs
5	Session Layer	Maintains connections and is responsible for controlling ports and sessions
4	Transport Layer	Transmits data using transmission protocols including TCP and UDP
3	Network Layer	Decides which physical path the data will take
2	Data Link Layer	Defines the format of data on the network
1	Physical Layer	Transmits raw bit stream over the physical medium

A very good interpretation of the construction of data packets. Good supporting image with ref source.

Figure 1 - Typical Layering Model (Imperva - 2022)

Network layer model show is not a concept but relies on the process that an upper layers data is passed down through the layer chain where it is encompassed and added to by the next layer. To improve efficiency in this process, the entire packet is not copied but a protocol pair in the adjacent payers transfer a pointer to the packet. (Comer, D.E. - 2015)

7 Layers of the OSI Model:

1. Application Layer:

The application layer is used by end-user 'Human Interface' software in network clients. It houses protocols that allow the interface software to send and receive certain type of information and convert it to a format suitable for users. A few examples are: **HTTP, FTP, IRC, SSH, DNS are used**

2. Presentation Layer:

The presentation layer defines how two devices in the communication protocol should encode, encrypt, and compress data so it is received correctly. The presentation layer is merely converted any data passed on from the application layer, despite its contents or length and does not add any data.

Protocols such as SSL, SSH, IMAP, FTP, MPEG, JPEG are used

3. Session Layer:

The session layer creates a comms channels between the appropriate devices, which is called a 'session'. It is responsible for opening and closing sessions, ensuring they remain open and functional during data transferral. During a data transfer, checkpoints are created to verify if the session is not being interrupted and whether devices can resume data transfer between checkpoints.

Protocols such as API's, Sockets, Winsock are used

4. Transport Layer:

The transport layer is responsible in breaking up the takes data transferred into "segments" on the so it can be transmitted during checkpoints in the session. It is responsible for reassembling the segments on the receiving end, turning it back into data that can be used by the session layer. It also controls the speed of data being sent and making sure that the recipient is ready to receive it at the same rate. Throughout this process, error checking is also carried out and requesting retransmission if errors are detected.

Protocols such as TCP & UDP are used

5. Network layer:

The network layer functions to break up the segments made by the transport layer, into network packets, and reassembling the packets on the receiving end. It also uses packet discovery by analysing the packet and deciding which method is should be sent to reach the destination node.

Protocols such as IP, ICMP, IPSec and IGMP are used

6. Data Link Layer:

The data link layer establishes and terminates a connection between two networked devices. Further work into breaking up the completed formed packets and segregates into network 'frames'. This layer is also responsible for sending them across the next physical layer. The use of LLC (Logical Link control) and MAC addresses are crucial to this layer to make sure that these devices are able to receive and interpret the data that is being sent.

Components such as Ethernet, PPP, 'Switches' and 'Bridges' are used

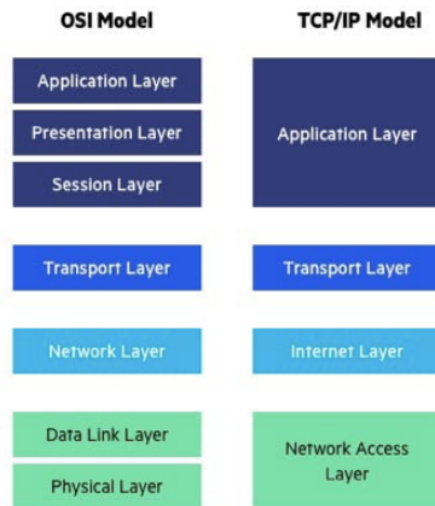
7. Physical Layer:

This layer is the actual physical layer that physically joins the network nodes together via various forms. This layer specifies the type of connections to be used and resultant protocol.

Connection Mediums such as Coax, Fiber, Wireless, Hubs and Repeaters are used

(Imperva, 2022) (BMC, 2022)

The older '4 layer network layer' was further expanded as 7 layer is more defined to use as all network traffic where as 4 layer is used for TCP/IP communication, typically found in Internet based comms.



The image supports the explanation

Figure 2 - 7 Layer Vs 4 Layer OSI Model (Comer, D.E. - 2015)

Layer 4 load balancing takes place at the transport layer of the OSI model, which is in charge of delivering messages regardless of their content.

This is a significant point

Layer 4 vs. Layer 7 Load Balancing Comparison			
Layer 4		Layer 7	
Advantages	Disadvantages	Advantages	Disadvantages
Suitable for packet-level balancing of loads	Based on the content, smart load balancing is not possible.	Based on the URL, it provides smart routing.	It is expensive.
It is quick and efficient because it does not take data into account.	Cannot perform true microservices.	It offers caching.	Decryption is required.
Because packets are not examined, they are more secure. If it is compromised, no one will be able to access the data.	Because it is a stateful protocol, it must be sticky. When a connection is established, it is routed to a single server in the backend. All packets sent through this connection are routed to a single server. Based on the algorithm, the next connection will select another server.		In terms of security, your certificate must be shared with the load balancers. If an attacker gains control to the load balancer, they will have total access to all of your data.
It just forwards the packets. It does not need to decrypt the content before forwarding.			Its proxy establishes several connections — client to proxy/proxy to server — so you are limited by the load balancer's maximum TCP connection.
NAT is used.			
Maintains only one NATed connection between the client and the server, allowing your load balancer to serve a maximum number of TCP connections.			

Figure 3 - 4 Layer 4 vs. 7 Layer Load Balancing Comparison Table (Medium, 2022)

Good comparison between models

Encapsulation:

Encapsulation is a process where a protocol of a lower layer receives data from the directly higher layer and places the complete layer data into the data portion of the layer frame.

The encapsulation process is where the completed data of the frame is fully encompassed into the layer below, and added to by the layers specific function and creates a larger packet.

As the encapsulation process continues down the OSI network model, the lowest levels are sometimes referred to as 'framing'.

(Network Encyclopedia, 2022)

A very good image that supports the very clear explanation

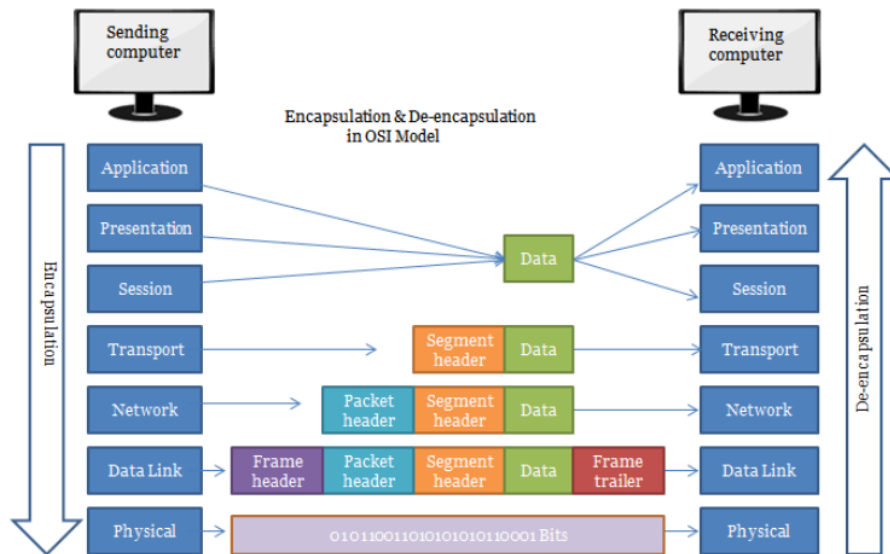


Figure 4 - Encapsulation Vs Decapsulation (ComputerNetworkingNotes, 2022)

The encapsulation process happens on the sender side of the OSI network model where the initial application data created by the user program needs additional 'information' for it to be encrypted, segregated into sizeable data chunks for it to be sent, addressed to a correct destination as well as functions to check if errors have been introduced during the transmission and decapsulation process.

The encapsulation process is commenced from the 'transport layer' downwards, is listed in the following steps:

Step 1: The Application, Presentation, and Session layer of the OSI model, or the Application layer in the TCP/IP model takes the complete data and forwards it onto the transport layer. The data packet does not add any layer header or layer footer but a header may be added, if required.

Step 2: The transport layer analyses the data for length and divides it into consistent sized chunks. The layer adds a suitable header and footer to each chunk of data and now forms 'segments'. The header of each segment contains information on how the segments are required to be re-assembled on the receiving end.

Step 3: The network or internet layer receives the segments created in the transport layer and adds further header and footers to the packet segments which have information on routing, how the data segments are to be sent to its intended destination. From here on, the completed encapsulated data is referred to as a 'data packet'.

Step 4: This layer receives the complete data packet, adds yet more header and footer which contains information about what hardware components are required to be used to send the data to its intended destination as well error detection and control during transmission and the request to re-transmit if errors are detected. From here on, the completed encapsulated data is referred to as a 'data frame'.

Step 5: The physical layer uses the 'data frame' and encapsulates it into the final steps where it is converted into a complete data packet into a signal that can be transmitted. Here, the data and all associated layers are transmitted via the same communication data speed ready for it to be read and decapsulated at the receiving end.

Good explanation that is consistent with the diagram illustrated

(Afteracademy, 2022)

Broadcasting:

In terms of sending packets of data, there are multiple methods in specifying the intended destination of the data packet. **Unicast, multicast and broadcast.**

Unicast: Sent to one specific device only, all other devices received are to discard

Multicast: Sent to a group of devices designated as a defined network

Broadcast: Sent to all devices on a specific subnet of a network

Every type of network or subnet has a specific 'broadcast' address, usually allocated to the last IP address of each subnet, used to broadcast information. This address can be used to broadcast information to all devices in the subnet without prior knowledge of what IP addresses are situated on the network. (IONOS, 2022)

Good point identified

Here are two examples for when a broadcast can be used on a computer network:

- A computer has been connected to a network and requires a correct IP address so it can communicate with the rest of the network. The broadcast command from the computer broadcasts a message asking if there any DHCP servers available and to request an address to be allocated to it. The computer is unaware if and where the DHCP router is stated so a broadcast transmission is used and although every other LAN network device receives the broadcast, only the router will respond.
- A computer wants to know what other devices are connected to the same Lan network as itself, to it knows if the other clients are visible and what services are available (file sharing or printer services) so a broadcast message is sent for request to be received by any clients that can respond with the initial request.

*Broadcast purpose is explained
Large networks are generally split up into smaller domains to reduce broadcast operations. This makes the network more reliable and faster.* (Homenethowto, 2022)

Of the 65,535 available port numbers, some are designated and reserved by the industry where as others are classified as temporary during the connection and data transfer.

0-1023 are reserved for high end company protocols

1024-49151 are available for registration and reservation by other businesses and services

49152-65535 are allocated for temporary use during a transmission.

Ports are identified

Port Allocation:

Port numbers are used to inform the recipient of data, which type of data is being sent. This is used to identify which protocol has being used.

An IP address is used to specify the physical client destination where as there added port number then determines the application to be used on that client or destination.

i.e 192.168.0.20:8080 where '192.168.0.20' is the IP address of the destination and '8080' is the port number to specify the application to read and use the data being sent.

Port numbers usually are made up of 16 bit numbers.

Here are some commonly used ports and their associated networking protocols:

- **Ports 20 and 21.** 'FTP' - used to transfer physical files between a client and a server.
- **Port 22.** [Secure Shell](#) is one of several tunneling protocols used to build secure network connections.
- **Port 25.** Simple Mail Transfer Protocol or ([SMTP](#)) is commonly used for email applications to read and convert emails.
- **Port 53.** Domain name system ([DNS](#)) is a very important process that matches written URLs (web addresses) into server destination IP addresses. The use of DNS ensures that names instead of numbers are used, for easy recollection.
- **Port 80.** HTTP is the protocol that converts general world wide webdata into browser format for reading and graphical imagery.
- **Port 123.** [Network Time Protocol](#) used by servers and clients to synchronise time data to ensure that time stamps are accurate, used for error checking and encryption.
- **Port 179.** Border Gateway Protocol ([BGP](#)) is a protocol which helps establishing the most efficient route between networks which make up the whole internet. The BGP is used by network gateways to broadcast information about what network they contain so that information is addressed to the specific gateway efficiently.

Good work here with good supporting ref sources (Techtarget, 2022)

Research section is covered in good detail and supported with good relevant images and ref sources

3. Design Requirements

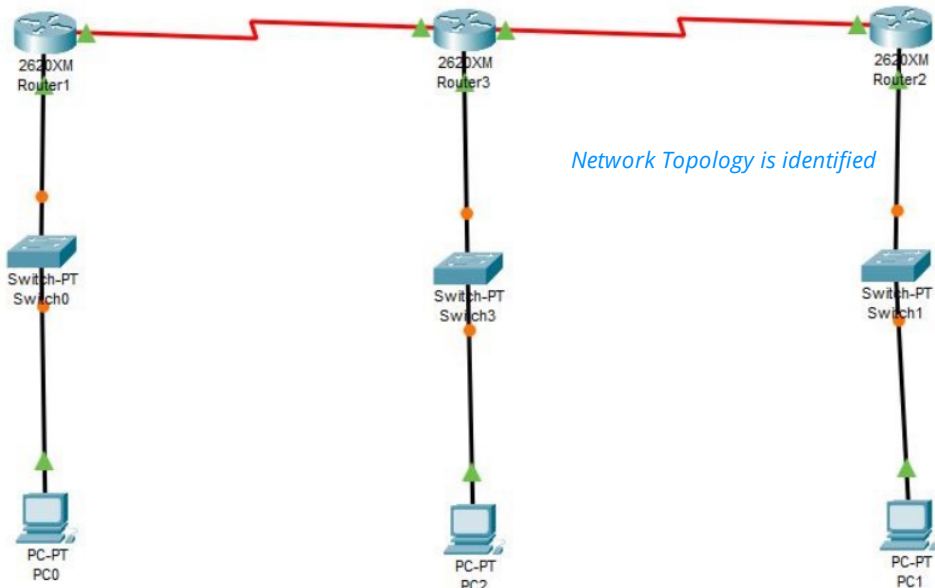


Figure 5 - Element 1 Network Overview

The network shown above, which comprises of 3 LAN networks (1 Router, 1 switch and 1 PC Client) shown in black) is interconnected via 2 WAN Serial networks (showing connected in red) via the 3 routers.

To demonstrate the possible use of IP addressing using the different Class addressing, the above network was constructed using a virtual network software to show the relationship and possible connection between three different types of Class networks using different subnets.

Note how the network is in a radial configuration and relies upon 'Router 2' to be able to route traffic across its 2 WAN connections as well as being able to send communication to the right serial WAN port to reach the intended LAN network downstream to the other routers.

The three Class networks used and chosen IP address are:

Class 'A' Network Subnet Configuration				
Binary Number	11111111	00000000	00000000	00000000
Boolean Number	255	0	0	0

Figure 6 - Class 'A' Network Subnet Configuration

Number of available clients: $2^n - 2$

$= 2^{24} - 2 = 16,777,214$

Where n = number of available octets

Class 'A' IP Address Chosen: **55.0.0.0** Subnet: **255.0.0.0/8**

Class 'B' Network Subnet Configuration				
Binary Number	11111111	11111111	00000000	00000000
Boolean Number	255	255	0	0

Figure 7 - Class 'B' Network Subnet Configuration

Number of available clients: $2^n - 2$

$$= 2^{16} - 2 = 65,534$$

Where n = number of available octets

Class 'B' IP Address Chosen: **170.5.0.0** Subnet: **255.255.0.0/16**

Class 'C' Network Subnet Configuration				
Binary Number	11111111	11111111	11111111	00000000
Boolean Number	255	255	255	0

Figure 8 - Class 'C' Network Subnet Configuration

Number of available clients: $2^n - 2$

$$= 2^8 - 2 = 254$$

Where n = number of available octets

Class 'C' IP Address Chosen: **192.168.5.0** Subnet: **255.255.255.0/24**

Very good address scheme method that clearly defines the understanding

The 3 address classes are established with the appropriate subnet masking

4. Implementation

Static Routing:

Using Cisco packet Tracer, each router was programmed using 'Static routing' function.

Router 1 > Router 3: Router 1 has a WAN connection between itself and the next Router (Router 3). This was designated as 10.10.10.1

Router 3 > Router 2: Router 2 has a WAN connection between itself and the next Router (Router 3). This was designated as 10.10.10.2

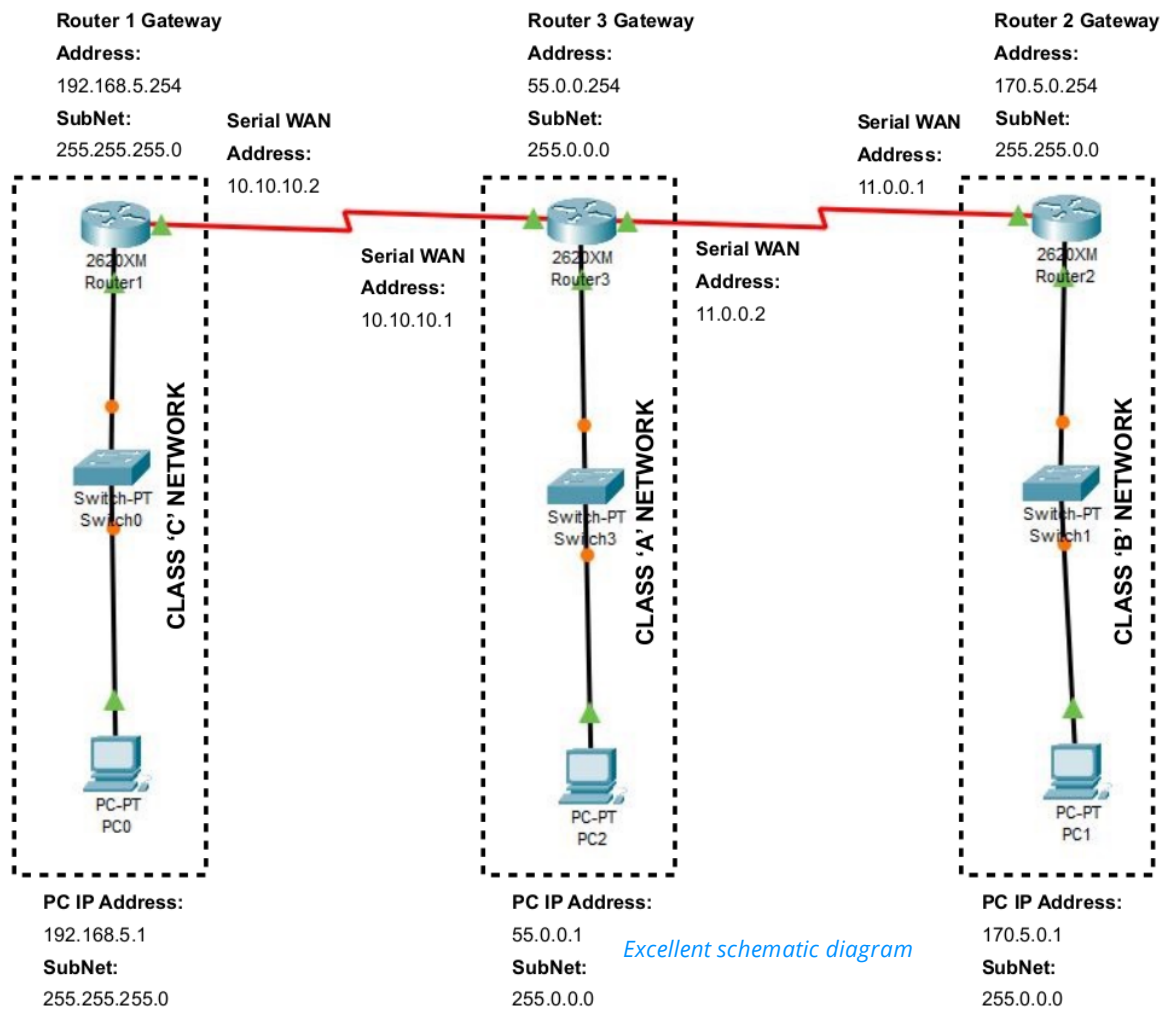


Figure 9 - Network Overview - Static Routing

With the network and appropriate addressing now planned out, the Routers were programmed using the Packet tracer program, using the menus to type and confirm that the LAN networks were successfully tied to the correct WAN networks.

This static routing programming states that all external LAN networks need to be accessed through the WAN IP addressed connection of the router.

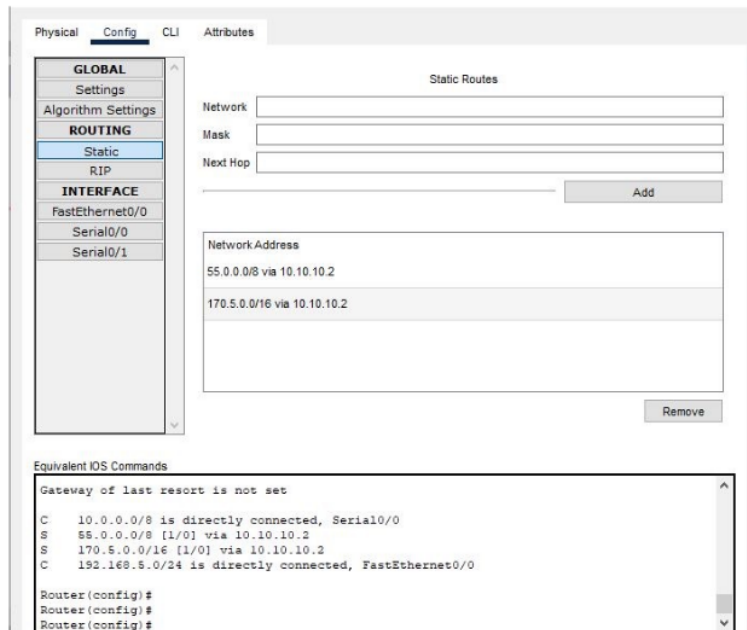


Figure 10 - Router 1 (Left) Static Routing

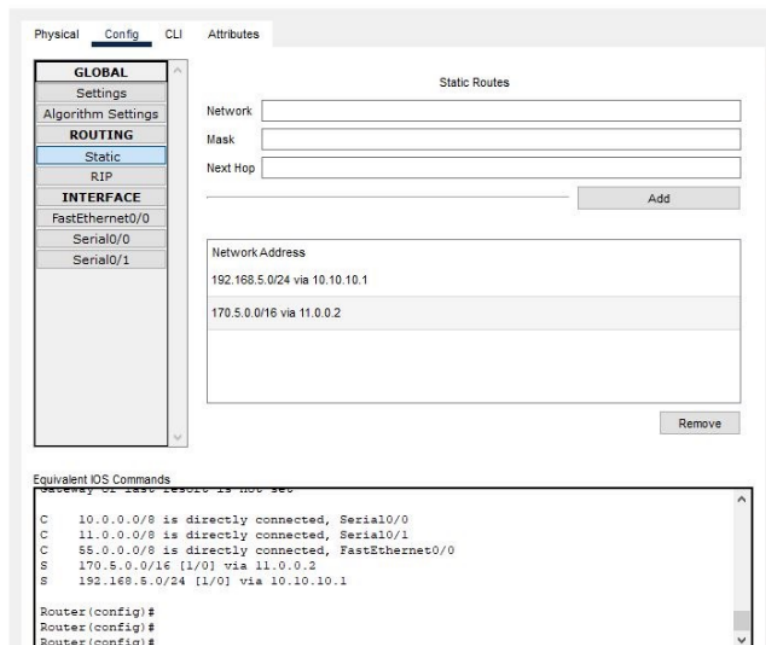


Figure 11 - Router 3 (Centre) Static Routing

Physical Config CLI Attributes

GLOBAL Settings Algorithm Settings ROUTING Static RIP INTERFACE FastEthernet0/0 Serial0/0 Serial0/1

Static Routes

Network

Mask

Next Hop

Add

Network Address
55.0.0.0/8 via 11.0.0.1
192.168.5.0/24 via 11.0.0.1

Remove

Equivalent IOS Commands

```

170.5.0.0/16 is directly connected, FastEthernet0/0
S    192.168.5.0/24 [1/0] via 11.0.0.1
Router(config)#
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
Router(config)#
  
```

Static routing tables are configured

Figure 12 - Router 2 (Right) Static Routing

With the routing now programmed, all PCs (network clients) were programmed with static IPs which coincided with the type of Class networks they were connected with. Figure 9 above shows the IP addresses chosen.

Using the 'Routing Table' function, this shows that the routing was corrected setup, with the centre router (Router 3) having additional routing results due to having to route between the 2 WAN networks either side.

```

C    10.0.0.0/8 is directly connected, Serial0/0
S    55.0.0.0/8 [1/0] via 10.10.10.2
S    170.5.0.0/16 [1/0] via 10.10.10.2
C    192.168.5.0/24 is directly connected, FastEthernet0/0
Router(config)#
  
```

Figure 13 - Router 1 (Left) Routing Table

```

C    10.0.0.0/8 is directly connected, Serial0/0
C    11.0.0.0/8 is directly connected, Serial0/1
C    55.0.0.0/8 is directly connected, FastEthernet0/0
S    170.5.0.0/16 [1/0] via 11.0.0.2
S    192.168.5.0/24 [1/0] via 10.10.10.1
Router(config)#
  
```

Figure 14 - Router 3 (Centre) Routing Table

```
C    11.0.0.0/8 is directly connected, Serial0/0
S    55.0.0.0/8 [1/0] via 11.0.0.1
C    170.5.0.0/16 is directly connected, FastEthernet0/0
S    192.168.5.0/24 [1/0] via 11.0.0.1
Router(config)#
```

*Router report tables indicate
correct configuration*

Figure 15 - Router 2 (Right) Routing Table

Static routing is configured

Dynamic Routing:

With the static routing implemented and Routing table now showing successful LAN <> WAN connections, We can now remove the static routes specified in the last step, and implement dynamic routing.

```
Router(config-router)#net 192.168.5.0
Router(config-router)#net 11.0.0.0
Router(config-router)#net 55.0.0.0
Router(config-router)#^Z
Router#
```

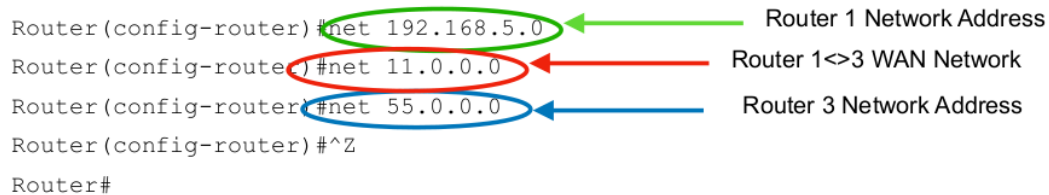


Figure 16 - Router 1 (Left) Dynamic Routing Commands

```
Router(config-router)#do show ip route
C    10.0.0.0/8 is directly connected, Serial0/0
R    11.0.0.0/8 [120/1] via 10.10.10.2, 00:00:17, Serial0/0
R    55.0.0.0/8 [120/1] via 10.10.10.2, 00:00:17, Serial0/0
R    170.5.0.0/16 [120/2] via 10.10.10.2, 00:00:17, Serial0/0
C    192.168.5.0/24 is directly connected, FastEthernet0/0
```

Figure 17 - Router 1 (Left) Dynamic Routing Table

```
Router(config-router)#net 10.0.0.0
Router(config-router)#net 55.0.0.0
Router(config-router)#net 11.0.0.0
Router(config-router)#net 170.5.0.0
Router(config-router)#^Z
Router#
```

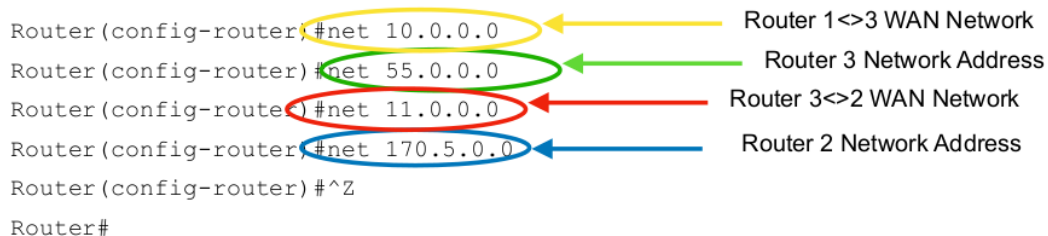


Figure 18 - Router 3 (Centre) Dynamic Routing Commands

```
Router(config-router)#do show ip route
C    10.0.0.0/8 is directly connected, Serial0/0
R    11.0.0.0/8 [120/1] via 10.10.10.2, 00:00:17, Serial0/0
R    55.0.0.0/8 [120/1] via 10.10.10.2, 00:00:17, Serial0/0
R    170.5.0.0/16 [120/2] via 10.10.10.2, 00:00:17, Serial0/0
C    192.168.5.0/24 is directly connected, FastEthernet0/0
```

Figure 19 - Router 3 (Centre) Dynamic Routing Table

```
Router(config)#router rip
Router(config-router)#ver 2
Router(config-router)#net 170.5.0.0
Router(config-router)#net 11.0.0.0
Router(config-router)#net 55.0.0.0
Router(config-router)#^Z
Router#
```



Figure 20 - Router 2 (Right) Dynamic Routing Commands

```
Router(config-router)#do show ip route
R   10.0.0.0/8 [120/1] via 11.0.0.1, 00:00:13, Serial0/0
C   11.0.0.0/8 is directly connected, Serial0/0
R   55.0.0.0/8 [120/1] via 11.0.0.1, 00:00:13, Serial0/0
C   170.5.0.0/16 is directly connected, FastEthernet0/0
R   192.168.5.0/24 [120/2] via 11.0.0.1, 00:00:13, Serial0/0
```

Figure 21 - Router 2 (Right) Dynamic Routing Table

Dynamic routing is configured

DHCP Routing:

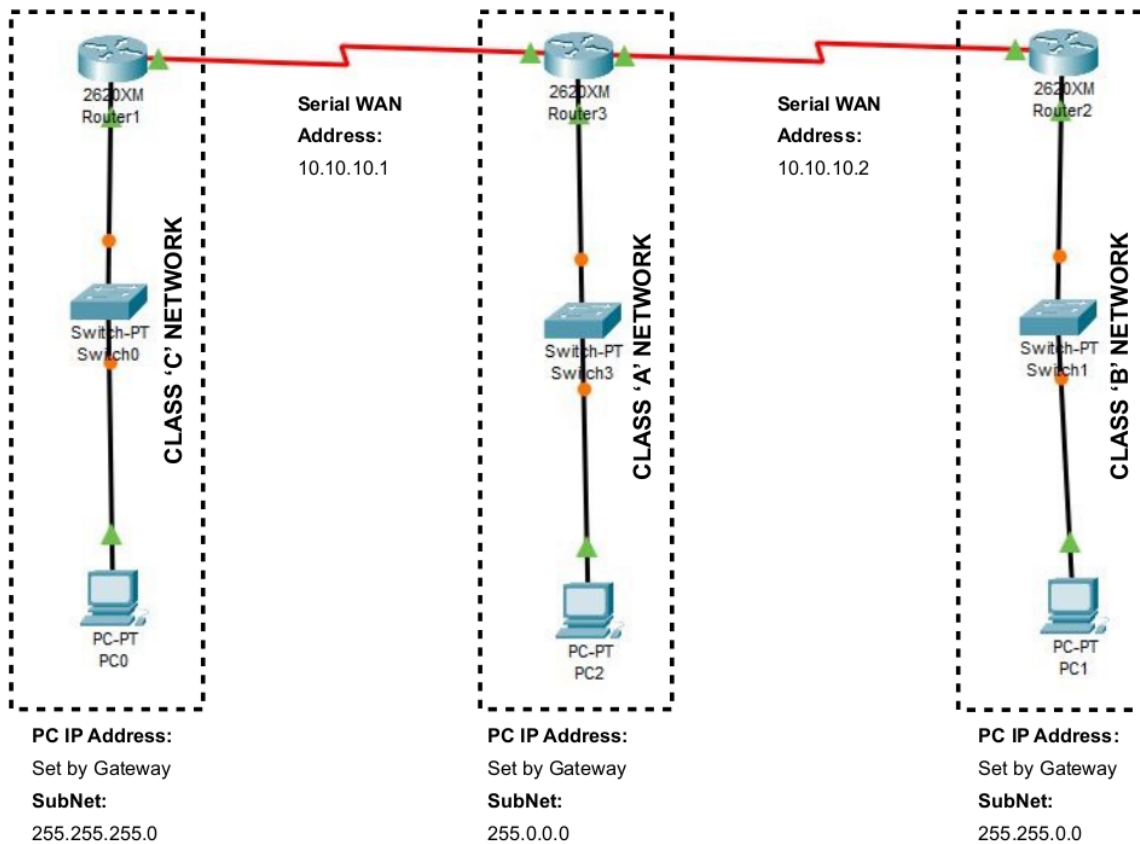
Now that the static LAN <> WAN routing as well as Dynamic Routing between WAN networks has been programmed and tested, we can now proceed with DHCP routing, where the gateways are programmed to provide the PC (Network clients) with the appropriate I.P address that show fall in the correct subnet.

This demonstrates that the Class A,B or C subnets are creating DHCP pools to show that small or large networks can be produced.

Router 1 Gateway
Address: 192.168.5.254
SubNet: 255.255.255.0
DHCP: 192.168.5.0-254

Router 3 Gateway
Address: 55.0.0.254
SubNet: 255.0.0.0
DHCP: 55.0.0.0-254

Router 2 Gateway
Address: 170.5.0.254
SubNet: 255.255.0.0
DHCP: 170.5.0.0-254



Good diagram indicating function of DHCP

Figure 22 - Network Overview - DHCP Address Routing

```

Router(config)#ip dhcp pool net1
Router(dhcp-config)#net 192.168.5.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.5.254
Router(dhcp-config)#dns-server 192.168.5.254
Router(dhcp-config)#exit
Router(config)#ip dhcp pool net2
Router(dhcp-config)#net 170.5.0.0 255.0.0.0
Router(dhcp-config)#default-router 170.5.0.254
Router(dhcp-config)#dns-server 170.0.0.254
Router(dhcp-config)#exit
Router(config)#ip dhcp pool net3
Router(dhcp-config)#exit

```

```

Router(config)#ip dhcp pool net2
Router(dhcp-config)#net 55.0.0.0 255.0.0.0
Router(dhcp-config)#default-router 55.0.0.254
Router(dhcp-config)#dns-server 55.0.0.254
Router(dhcp-config)#exit
Router(config)#ip dhcp pool net3
Router(dhcp-config)#net 170.5.0.0 255.255.0.0
Router(dhcp-config)#default-router 170.5.0.254
Router(dhcp-config)#dns-server 170.5.0.254
Router(dhcp-config)#exit
Router(config)#
Router#

```

Figure 23 - Router 3 (Left) DHCP Allocation - Router Programming

```

Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int f0/0
Router(config-if)#ip helper-address 10.10.10.1
Router(config-if)#exit
Router(config)#

```

Figure 24 - Router 1 (Middle) DHCP Allocation - Helper Address Programming

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int f0/0
Router(config-if)#ip helper-address 10.10.10.1
Router(config-if)#exit
Router(config)#
```

Figure 25 - Router 2 (Right) DHCP Allocation - Helper Address Programming

DHCP configuration is set along with helper addresses to cross boundaries

DHCP Address Exclusion:

To implement a range of addresses to be excluded from a DHCP pool (so that the addresses can be 'assigned' to network devices i.e switches or other gateways, then we can also perform commands to instruct the gateway to start the DHCP Pool at a certain address rather than x.1

```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip dhcp excluded-address 192.168.5.10
Router(config)#ip dhcp excluded-address 55.0.0.1 55.0.0.10
Router(config)#ip dhcp excluded-address 192.168.5.1 192.168.5.10
Router(config)#ip dhcp excluded-address 170.5.0.1 170.5.0.10
Router(config)#exit
Router#
```

The diagram illustrates the configuration of DHCP address exclusions. It shows four lines of configuration commands. The first line, `ip dhcp excluded-address 192.168.5.10`, is annotated with a green oval and an arrow pointing to the text `55.0.0.1 > .10 Excluded`. The second line, `ip dhcp excluded-address 55.0.0.1 55.0.0.10`, is annotated with a blue oval and an arrow pointing to the text `192.168.5.1 > .10 Excluded`. The third line, `ip dhcp excluded-address 192.168.5.1 192.168.5.10`, is annotated with a red oval and an arrow pointing to the text `170.5.0.1 > .10 Excluded`. The fourth line, `ip dhcp excluded-address 170.5.0.1 170.5.0.10`, is annotated with a blue oval and an arrow pointing to the text `192.168.5.1 > .10 Excluded`.

Figure 26 - Router 3 (Left) DHCP Allocation - Address Exclusions

These commands now mean the 10 addresses situated between:

192.168.5.1 to 192.168.5.10

55.0.0.1 to 55.0.0.10

170.5.0.1 to 170.5.0.10

are now excluded from the DHCP address pools.

Exclusion addresses are configured

5. Test & Analysis

Static Routing Packet Testing:

Packets were set between all Client PCs across the 3 switches and routers to demonstrate successful routing and communications across all routers and switches, including the WAN connections.

Fire	Last Status	Source	Destination	Type	Color
	Successful	PC0	PC2	ICMP	
	Successful	PC0	PC1	ICMP	
	Successful	PC2	PC0	ICMP	
	Successful	PC2	PC1	ICMP	
	Successful	PC1	PC0	ICMP	
	Successful	PC1	PC2	ICMP	

Test results support static routing protocol function

Figure 27 - Static Routing - Packet Test Results

Dynamic Routing Packet Testing:

Packets were set between all Client PCs to demonstrate successful routing and communications across the WAN connections of the 3 routers.

PDU List Window										
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	De
	Successful	PC0	PC2	ICMP		0.000	N	0	(edit)	
	Successful	PC0	PC1	ICMP		0.000	N	1	(edit)	
	Successful	PC2	PC0	ICMP		0.000	N	2	(edit)	
	Successful	PC2	PC1	ICMP		0.000	N	3	(edit)	
	Successful	PC1	PC0	ICMP		0.000	N	4	(edit)	
	Successful	PC1	PC2	ICMP		0.000	N	5	(edit)	

Figure 28 - Dynamic Routing - Packet Test Results

Test results support the dynamic routing protocol

DHCP Address Allocation:

As only one router/gateway was programmed, initial checks to see if the 3 client PCs reviewed the correct IP address allocated by the gateway.

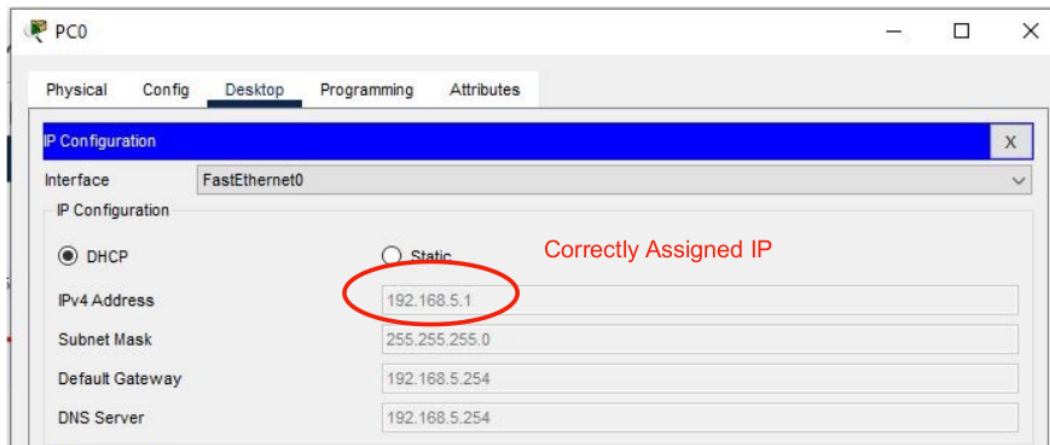


Figure 29 - PC1 (Left) DHCP Test without Helper Address

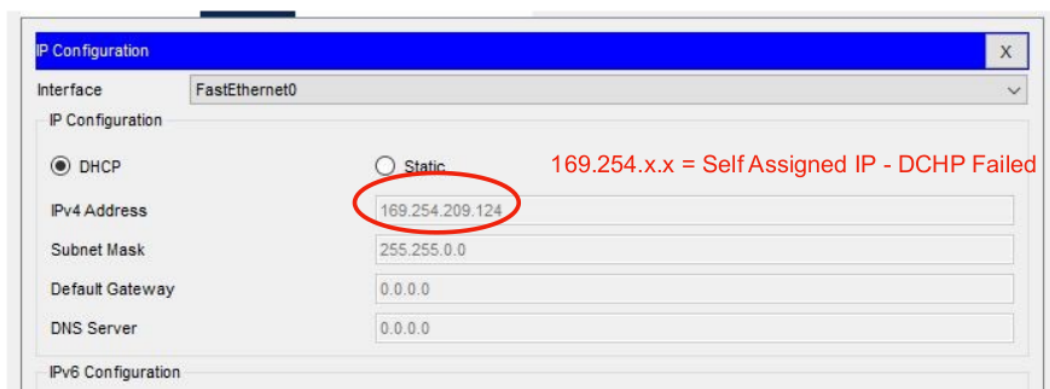


Figure 30 - PC2 (Middle) DHCP Test without Helper Address

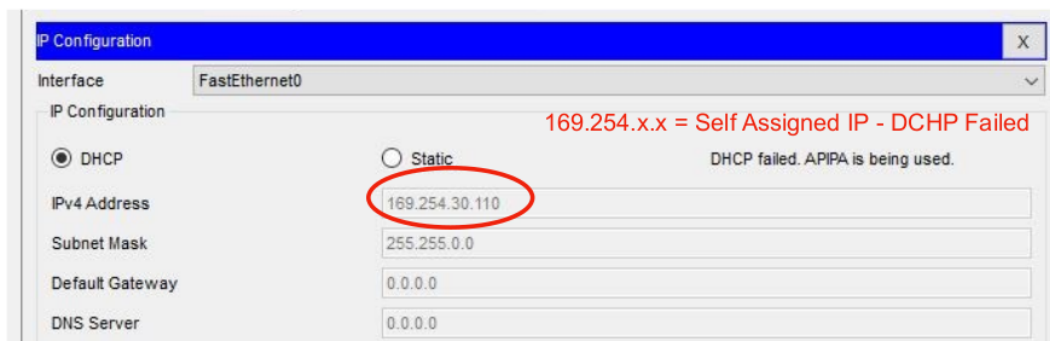


Figure 31 - PC3 (Right) DHCP Test without Helper Address

Good test showing errors due to no helper addresses
configured

Result: PC2 and PC3 (Client PCs) could not pick up a correct IP address in the correct subnet to allow a successful connection, and therefore was assigned a non Network IP address. (169.254.x.x)

To correct this, 'Helper Address' Config added to the router and the test was repeated to prove that the added config works:

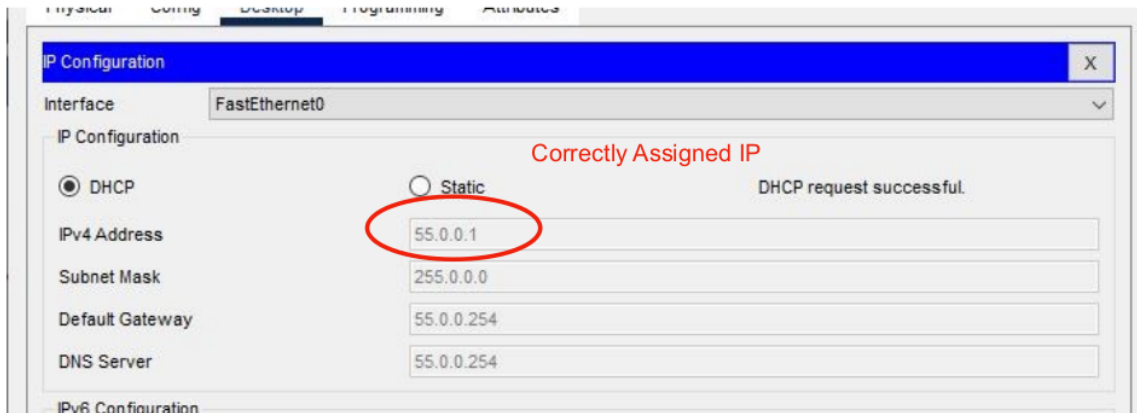


Figure 32 - PC2 (Middle) DHCP Test with Helper Address

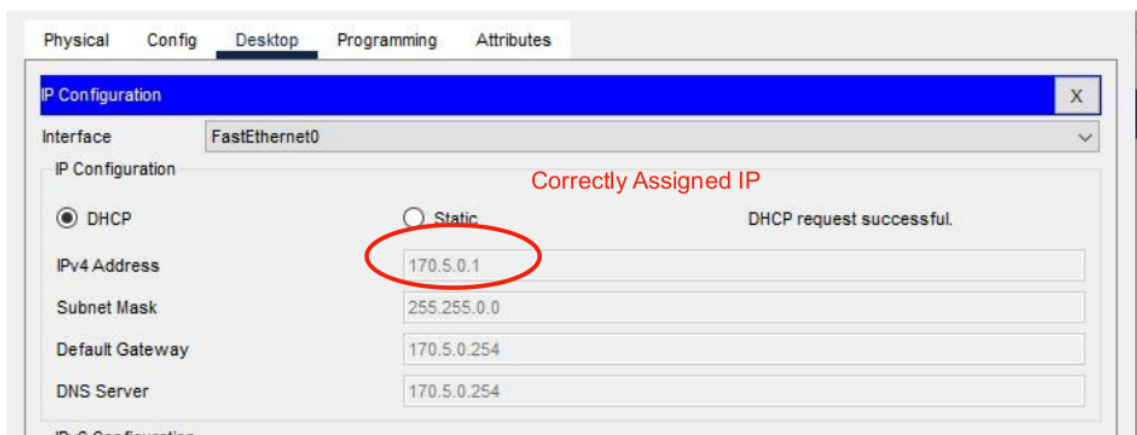


Figure 33 - PC3 (Right) DHCP Test with Helper Address

DHCP Address Exclusions:

Checking the Client PC IP address for what address was automatically allocated to it by the appropriate gateways DHCP Server, proving that the exclusion address ranges was working as intended.

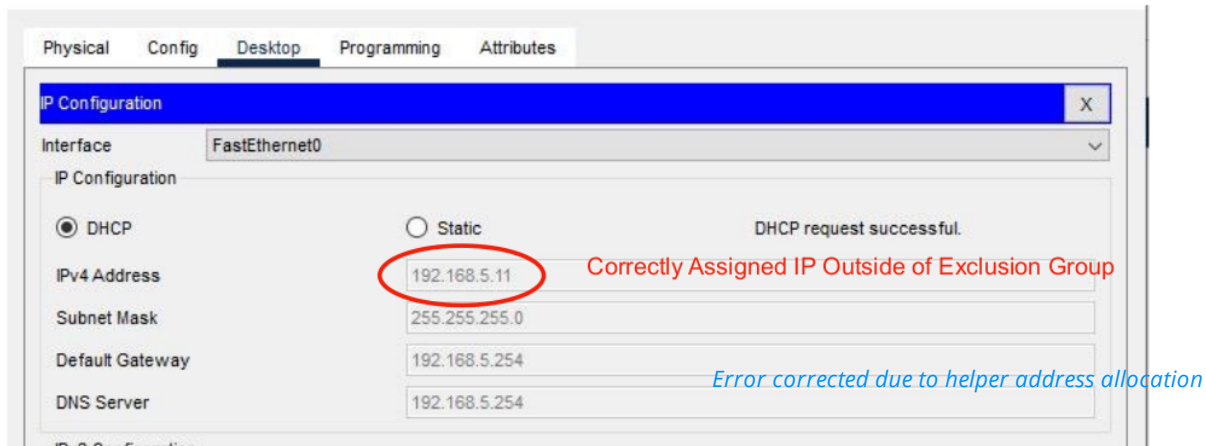


Figure 34 - PC1 (Left) DHCP Address - Post Exclusions

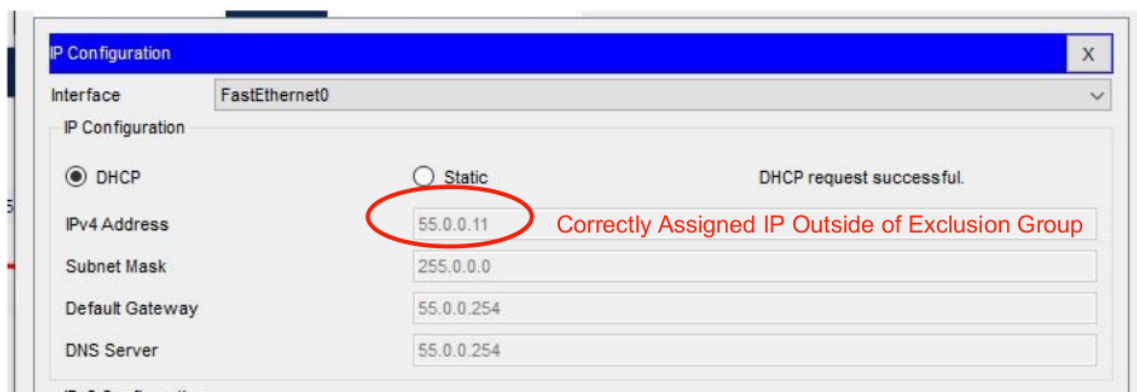


Figure 35 - PC2 (Middle) DHCP Address - Post Exclusions

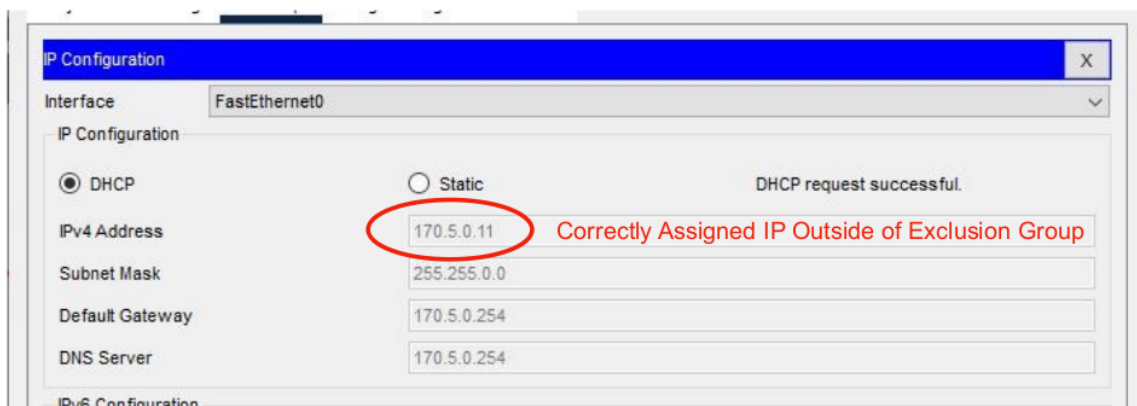


Figure 36 - PC3 (Right) DHCP Address - Post Exclusions

6. Evaluation

The use of programming the 3 routers allows the three different types of Class of networks to be easily setup that communication can be established. Although the routers effectively 'segregate' the LAN connections, this minimises the chance of possible security issues through the use of hacking via direct IP attacks as routers block broadcast requests for the clients available on a specific network.

The only issue that is because the WAN serial ports were not of a 'web' or ring layout, the data relies upon the successful and correct operation of the intermediate router in between the two outer LAN networks.

The middle router relies upon the knowledge of the two networks that lie either side and rely on some more configuration than the other two as its is effectively routing data 'across' the 2 WAN connections as well as down to the LAN network it is overseeing.

The configuration of the middle router relies on knowing what router and network is situated on what specific WAN port, otherwise the data is sent down the wrong WAN port and communication is not established.

The ability to create exclusion addresses during DHCP addressing allows networks to effectively operate in 2 modes, where the excluded address fields are most likely used for dedicated static IP address clients that need to be kept as much s possible i.e server devices.

The use of exclusion addresses allow static IP reservation, so that a device, although receives a fixed MAC address from the manufacturer, it can now receive a static IP address at the choosing of the network operator.

With IP reservation as well as DHCP, it allows some devices to have a leased IP address as its numerical address doesn't need to be fixed and known for it to correctly operate, as it is effectively a client.

Good informative evaluation that sets up a knowledge base for the next element

Element 2

1. Introduction

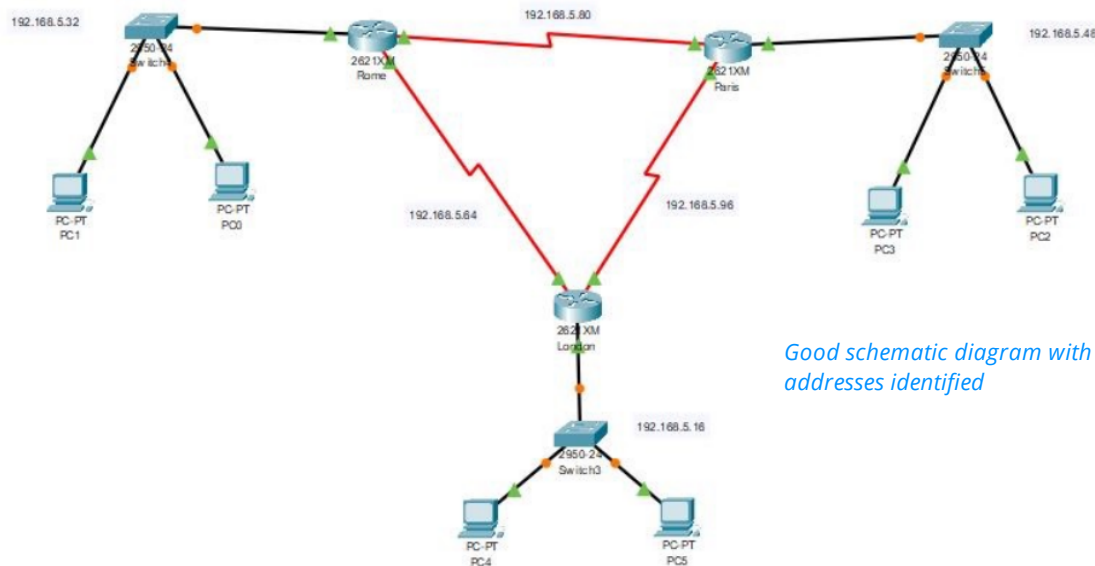
With Element 1 network now completed, the learnings about how to configure the routers can now be further expanded with Classless addressing. Classless addressing allows us to configure the subnet to mask out the number of available addresses instead of relying on the popular Class A, B or C framework. Using CIDR/28 (Classless Inter-domain Routing), we can address all network components according to the CIDR/28 address layout.

With the CIDR/28 tested, we can then reconfigure the network so LAN networks are CIDR/30 and WAN networks are CIDR/27.

We will also investigate the method of creating 2 VLANs from 1 physical LAN network, and the benefits and features that this could bring as we progress into the final element.

Good introduction to the scope of the element

2. System Configuration Requirements



Good schematic diagram with network addresses identified

Figure 37 - 3 Router WAN - Network Overview

A CIDR/28 network does not fall under a Class A, B or C network but is classified as a 'classless network'. The number 28 means that the first 28 bits are effectively 'masked out', 8 in the first octet, 8 in the 2nd, 8 in the 3rd and only 4 in the last octet.

Good effective explanation

CIDR/28 Network Configuration				
Binary Number	11111111	11111111	11111111	11110000
Boolean Number	255	255	255	240

Figure 38 - CIDR/28 Subnet Configuration Overview

Subnet mask is identified

Therefore, a CIDR/28 network results in a 255.255.255.240/28 subnet.

With a '240' mask in the final octet, this leaves the final 4 bits available for addressing, resulting in 16 available addresses left in the subnet. This means that each LAN network should be spaced 16 bits apart.

Using the network layout shown above, the IP addresses of the routers are as follows:

London Router Network Groups: 192.168.5.1 > 192.168.5.16

Rome Router Network Groups: 192.168.5.17 > 192.168.5.32

Paris Router Network Groups: 192.168.5.33 > 192.168.5.48

This should start at .16 instead of .1, However the spacing is correct

Using the assigned network groups, we can plan out the networks so it can be programmed without any overlap or gaps.

CIDR/28	Rome Network 1				LAN Address 32				
Subnet Mask	1	1	1	1	0	0	0	0	255.255.255.240/28
	0	0	0	0	0	0	0	0	Not Used
Network Address 32	0	0	1	0	0	0	0	1	Lowest host address 33
Network Address 32	0	0	1	0	0	0	1	0	Next host address 34
Default Gateway	0	0	1	0	1	1	1	0	Fastethernet 0/0 address 46
	0	0	1	0	1	1	1	1	Broadcast 47

Figure 39 - Rome Network - Network IP Configuration

CIDR/28	Paris Network 2				LAN Address 48				
Subnet Mask	1	1	1	1	0	0	0	0	255.255.255.240/28
	0	0	0	0	0	0	0	0	Not Used
Network Address 48	0	0	1	1	0	0	0	1	Lowest host address 49
Network Address 48	0	0	1	1	0	0	1	0	Next host address 50
Default Gateway	0	0	1	1	1	1	1	0	Fastethernet 0/0 address 62
	0	0	1	1	1	1	1	1	Broadcast 63

Figure 40 - Paris Network - Network IP Configuration

CIDR/28	London Network 3				LAN Address 16				
Subnet Mask	1	1	1	1	0	0	0	0	255.255.255.240/28
	0	0	0	0	0	0	0	0	Not Used
Network Address 16	0	0	0	1	0	0	0	1	Lowest host address 17
Network Address 16	0	0	0	1	0	0	1	0	Next host address 18
Default Gateway	0	0	0	1	1	1	1	0	Fastethernet 0/0 address 30
	0	0	0	1	1	1	1	1	Broadcast 31

Figure 41 - London Network - Network IP Configuration

Address scheme is established for LAN networks

Serial Link Addresses:

The WAN connections between the 3 routers also require IP addresses, but because the CIDR/28 subnet is used on this also, these addresses also need to be 16 addresses apart from the next WAN network range.

London Router: LAN Address: 192.168.5.64 WAN Addresses: 192.168.5.77&78
Rome Router: LAN Address: 192.168.5.80 WAN Addresses: 192.168.5.93&94
Paris Router: LAN Address: 192.168.5.96 WAN Addresses: 192.168.5.109&110

*Serial link
spacing is
correct*

London - Rome Network 1 LAN Address 64										
London Router	0	1	0	0	1	1	0	1	Serial 0/0 Add 77	192.168.5.77
Rome Router	0	1	0	0	1	1	1	0	Serial 0/1 Add 78	192.168.5.78

Figure 42 - London - Rome Network - Serial IP Configuration

Rome - Paris Network 1 LAN Address 80										
Paris Router	0	1	0	0	1	1	0	1	Serial 0/0 Add 93	192.168.5.93
Rome Router	0	1	0	0	1	1	1	0	Serial 0/0 Add 94	192.168.5.94

Figure 43 - Rome - Paris Network - Serial IP Configuration

Paris - London Network 1 LAN Address 96										
Paris Router	0	1	1	0	1	1	0	1	Serial 0/1 Add 109	192.168.5.109
London Router	0	1	1	0	1	1	1	0	Serial 0/1 Add 110	192.168.5.110

Figure 44 - Paris - London Network - Serial IP Configuration

Serial addresses are identified

CIDR/28 to CIDR27/30 Conversion:

With all network components addressed under a CIDR/28 configuration (allowing for 16 addresses per network), the network can be further refined and improved by changing the subnet and resultant network IP address pool size.

This also gives us the opportunity to change the WAN network size as there are only 2 WAN connections per router.

CIDR/27 Network Configuration				
Binary Number	11111111	11111111	11111111	11100000
Boolean Number	255	255	255	224
This results in a 255.255.255.224 Subnet Mask				
CIDR/30 Network Configuration				
Binary Number	11111111	11111111	11111111	11111100
Boolean Number	255	255	255	252
This results in a 255.255.255.252 Subnet Mask				

Subnets are identified for both network schemes

Figure 45 - CIDR27 & 30 Network Subnet Configuration

The following tables show the LAN address changes required to convert from a CIDR/28 to a CIDR/27 network for each of the 3 routers in the overall network.

CIDR/28	Rome Network 1		LAN Address 32						
Subnet Mask	1	1	1	1	0	0	0	0	255.255.255.240/28
	0	0	0	0	0	0	0	0	Not Used
Network Address 32	0	0	1	0	0	0	0	1	Lowest host address 33
Network Address 32	0	0	1	0	0	0	1	0	Next host address 34
Default Gateway	0	0	1	0	1	1	1	0	Fastethernet 0/0 address 46
	0	0	1	0	1	1	1	1	Broadcast 47
CIDR/27	Rome Network 1		LAN Address 32						
Subnet Mask	1	1	1	0	0	0	0	0	255.255.255.224/27
	0	0	0	0	0	0	0	0	Not Used
Network Address 32	0	1	0	0	0	0	0	1	Lowest host address 33
Network Address 32	0	1	0	0	0	0	1	0	Next host address 34
Default Gateway	0	1	0	0	1	1	1	0	Fastethernet 0/0 address 62
	0	1	0	0	1	1	1	1	Broadcast 63

The '1' here should be one place to the right

Figure 46 - Rome Network - CIDR28 > CIDR27 IP Configuration Changes

First 4 digits from the right should be 0010

The address for 62 should be 00111110 and 63 would be 00111111

CIDR/28	Paris Network 2				LAN Address 48				
	0	0	0	0	0	0	0	0	Not Used
Network Address 48	0	0	1	1	0	0	0	1	Lowest host address 49
Network Address 48	0	0	1	1	0	0	1	0	Next host address 50
Default Gateway	0	0	1	1	1	1	1	0	Fastethernet 0/0 address 62
	0	0	1	1	1	1	1	1	Broadcast 63
CIDR/27	Paris Network 2				LAN Address 96				
Subnet Mask	1	1	1	1	0	0	0	0	255.255.255.224/27
	0	0	0	0	0	0	0	0	Not Used
Network Address 96	0	1	1	0	0	0	0	1	Lowest host address 97
Network Address 96	0	1	1	0	0	0	1	0	Next host address 98
Default Gateway	1	1	1	1	1	1	1	0	Fastethernet 0/0 address 126
Error herewith last 2 lines	1	1	1	1	1	1	1	1	Broadcast 127

Figure 47 - Paris Network - CIDR28 > CIDR27 IP Configuration Changes

CIDR/28	London Network 3				LAN Address 16				
Subnet Mask	1	1	1	1	0	0	0	0	255.255.255.240/28
	0	0	0	0	0	0	0	0	Not Used
Network Address 16	0	0	0	1	0	0	0	1	Lowest host address 17
Network Address 16	0	0	0	1	0	0	1	0	Next host address 18
Default Gateway	0	0	0	1	1	1	1	0	Fastethernet 0/0 address 30
	0	0	0	1	1	1	1	1	Broadcast 31
CIDR/27	London Network 3				LAN Address 64				
Subnet Mask	1	1	1	0	0	0	0	0	255.255.255.224/27
	0	0	0	0	0	0	0	0	Not Used
Network Address 64	0	1	0	0	0	0	0	1	Lowest host address 65
Network Address 64	0	1	0	0	0	0	1	0	Next host address 66
Default Gateway	0	1	0	1	1	1	1	0	Fastethernet 0/0 address 94
	0	1	0	1	1	1	1	1	Broadcast 95

Figure 48 - London Network - CIDR28 > CIDR27 IP Configuration Changes

[Correct here](#)

The following tables show the WAN address changes required to convert from a CIDR/28 to a CIDR/30 Wan serial network for each of the 3 routers.

CIDR/28 London - Rome Network 1 LAN Address .64										
London Router	0	1	0	0	1	1	0	1	Serial 0/0 Add 77	192.168.5.77
Rome Router	0	1	0	0	1	1	1	0	Serial 0/1 Add 78	192.168.5.78
CIDR/30 London - Rome Network 1 WAN Address .8										
London Router	0	0	0	0	1	1	0	0	Serial 0/0 Add .10	192.168.5.10 <i>Error here</i>
Rome Router	0	0	0	0	1	0	0	1	Serial 0/1 Add 9	192.168.5.9 <i>Correct</i>

Figure 49 - London - Rome Network - CIDR28 > CIDR30 Serial IP Configuration Changes

CIDR/28 Rome - Paris Network 1 LAN Address .80										
Paris Router	0	1	0	0	1	1	0	1	Serial 0/0 Add 93	192.168.5.93
Rome Router	0	1	0	0	1	1	1	0	Serial 0/0 Add 94	192.168.5.94
CIDR/30 Rome - Paris Network 1 WAN Address .4										
Paris Router	0	0	0	0	0	1	0	1	Serial 0/0 Add 5	192.168.5.5
Rome Router	0	0	0	0	0	1	1	0	Serial 0/0 Add 6	192.168.5.6 <i>Correct</i>

Figure 50 - Rome - Paris Network - CIDR28 > CIDR30 Serial IP Configuration Changes

CIDR/28 Paris - London Network 1 LAN Address .96										
Paris Router	0	1	1	0	1	1	0	1	Serial 0/1 Add 109	192.168.5.109
London Router	0	1	1	0	1	1	1	0	Serial 0/1 Add 110	192.168.5.110
CIDR/30 Paris - London Network 1 WAN Address .12										
Paris Router	0	0	0	0	1	1	0	1	Serial 0/1 Add 13	192.168.5.13 <i>Correct</i>
London Router	0	0	0	0	1	1	1	0	Serial 0/1 Add 14	192.168.5.14

Figure 51 - Paris - London Network - CIDR28 > CIDR30 Serial IP Configuration Changes

3. Implementation

CIDR/28 Router Programming:

Each router received the appropriate programming commands, detailing the local LAN address first, and then each of the neighbouring WAN IP addresses as listed in the CIDR/28 tables above.

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router rip
Router(config-router)#ver 2
Router(config-router)#net 192.168.5.32
Router(config-router)#net 192.168.5.64
Router(config-router)#net 192.168.5.80
Router(config-router)#exit
Router(config)#
```

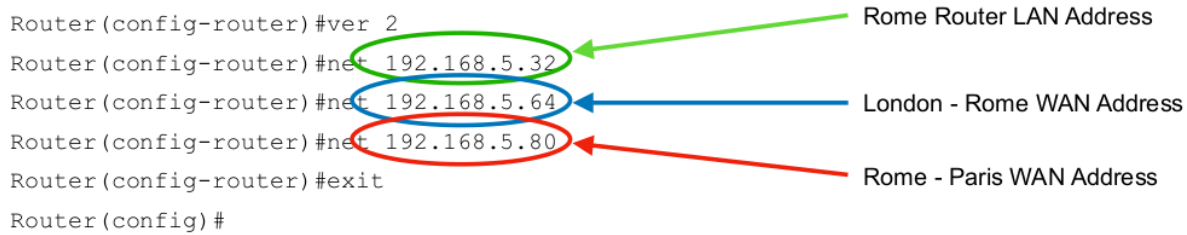


Figure 52 - Rome Router - CIDR/28 Programming

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router rip
Router(config-router)#ver 2
Router(config-router)#net 192.168.5.48
Router(config-router)#net 192.168.5.96
Router(config-router)#net 192.168.5.80
Router(config-router)#exit
Router(config)#
```

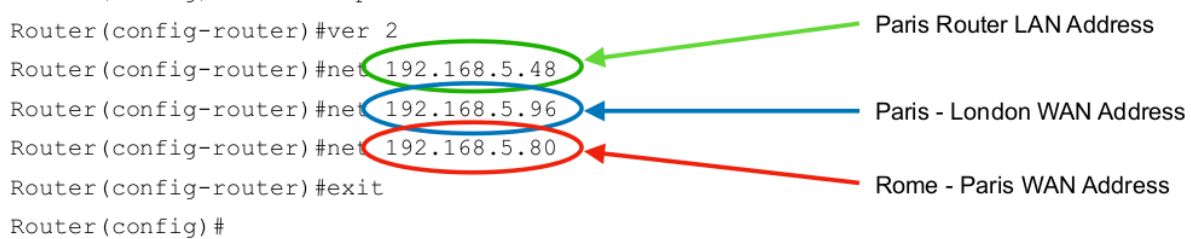


Figure 53 - Paris Router - CIDR/28 Programming

```
Router#en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router rip
Router(config-router)#ver 2
Router(config-router)#net 192.168.5.16
Router(config-router)#net 192.168.5.64
Router(config-router)#net 192.168.5.96
Router(config-router)#exit
Router(config)#
Router#
```

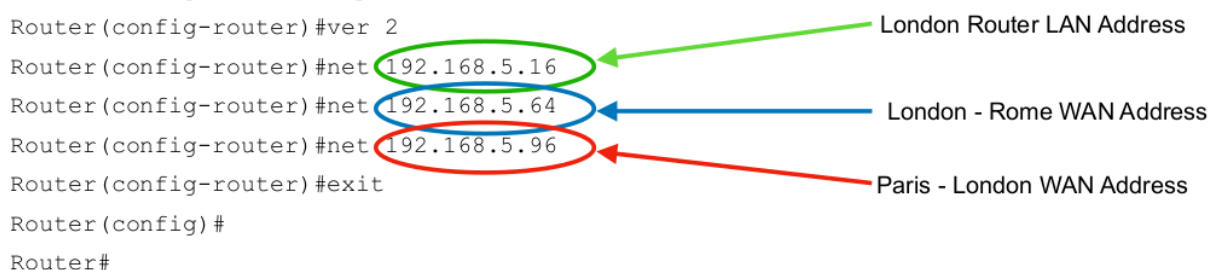


Figure 54 - London Router - CIDR/28 Programming

Despite the minor errors in the schematic tables with binary 1ns in wrong places in 3 instances, the configuration is correct

With the router configurations completed, checking the routing table for each router shows successful routing across the router from the client PCs to the other routers via the 2 serial WAN connections.

CIDR/27&30 Router Programming:

Each router received the appropriate programming commands, detailing the local LAN address first, and then each of the neighbouring WAN IP addresses as listed in the CIDR/28 tables above.

```
Router#en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router rip
Router(config-router)#ver 2
Router(config-router)#net 192.168.5.32
Router(config-router)#net 192.168.5.4
Router(config-router)#net 192.168.5.8
Router(config-router)#exit
Router(config)#
```

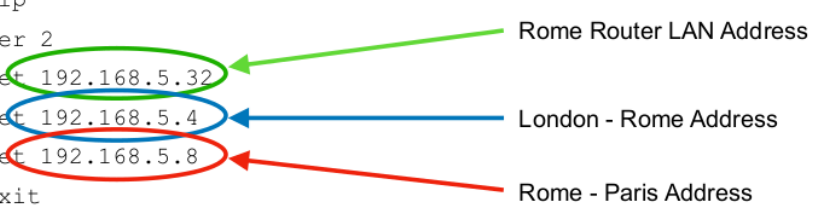


Figure 55 - Rome Router - CIDR/27&30 Programming

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router rip
Router(config-router)#ver 2
Router(config-router)#net 192.168.5.96
Router(config-router)#net 192.168.5.5
Router(config-router)#net 192.168.5.13
Router(config-router)#exit
Router(config)#
```

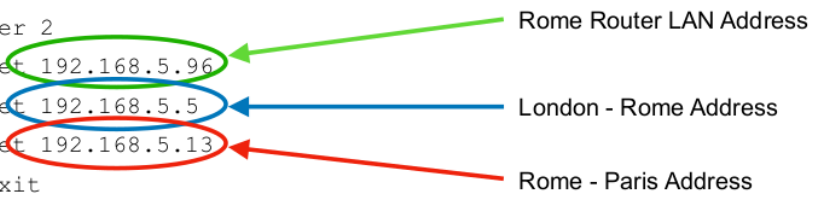
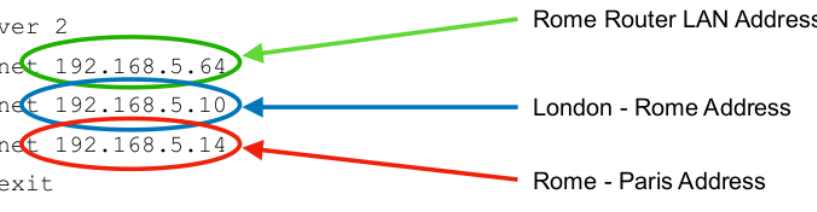


Figure 56 - Paris Router - CIDR/27&30 Programming

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router rip
Router(config-router)#ver 2
Router(config-router)#net 192.168.5.64
Router(config-router)#net 192.168.5.10
Router(config-router)#net 192.168.5.14
Router(config-router)#exit
Router(config)#
```



Configuration is good

Figure 57 - London Router - CIDR/27&30 Programming

With the subnets across all routers now changed to reflect the CIDR27&30 framework, a 'show ip route' command displays that the routing has been established with the appropriate commands listed:

```
Router>en
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

    192.168.5.0/24 is variably subnetted, 6 subnets, 2 masks
C       192.168.5.4/30 is directly connected, Serial0/0
C       192.168.5.8/30 is directly connected, Serial0/1
R       192.168.5.12/30 [120/1] via 192.168.5.10, 00:00:09, Serial0/1
           [120/1] via 192.168.5.5, 00:00:09, Serial0/0
C       192.168.5.32/27 is directly connected, FastEthernet0/0
R       192.168.5.64/27 [120/1] via 192.168.5.10, 00:00:09, Serial0/1
R       192.168.5.96/27 [120/1] via 192.168.5.5, 00:00:09, Serial0/0

Router#
```

Figure 58 - Rome Router - CIDR/27&30 Show IP Route

```
Router>en
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

    192.168.5.0/24 is variably subnetted, 6 subnets, 2 masks
C       192.168.5.4/30 is directly connected, Serial0/0
R       192.168.5.8/30 [120/1] via 192.168.5.14, 00:00:24, Serial0/1
           [120/1] via 192.168.5.6, 00:00:26, Serial0/0
C       192.168.5.12/30 is directly connected, Serial0/1
R       192.168.5.32/27 [120/1] via 192.168.5.6, 00:00:26, Serial0/0
R       192.168.5.64/27 [120/1] via 192.168.5.14, 00:00:24, Serial0/1
C       192.168.5.96/27 is directly connected, FastEthernet0/0

Router#
```

Figure 59 - Paris Router - CIDR/27&30 Show IP Route

```

Router>en
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

    192.168.5.0/24 is variably subnetted, 6 subnets, 2 masks
R       192.168.5.4/30 [120/1] via 192.168.5.9, 00:00:11, Serial0/0
        [120/1] via 192.168.5.13, 00:00:12, Serial0/1
C       192.168.5.8/30 is directly connected, Serial0/0
C       192.168.5.12/30 is directly connected, Serial0/1
R       192.168.5.32/27 [120/1] via 192.168.5.9, 00:00:11, Serial0/0
C       192.168.5.64/27 is directly connected, FastEthernet0/0
R       192.168.5.96/27 [120/1] via 192.168.5.13, 00:00:12, Serial0/1

Router#

```

Figure 60 - London Router - CIDR/27&30 Show IP Route

Reports indicate configuration is correct and show what is directly connected and routed.

VLAN Integration:

To demonstrate the facility of 'trunking', 2 VLANs are required to be setup so that the firewall rules between the 2 VLANs and the outward bound rules from the VLANs onto the wider network, can be controlled.

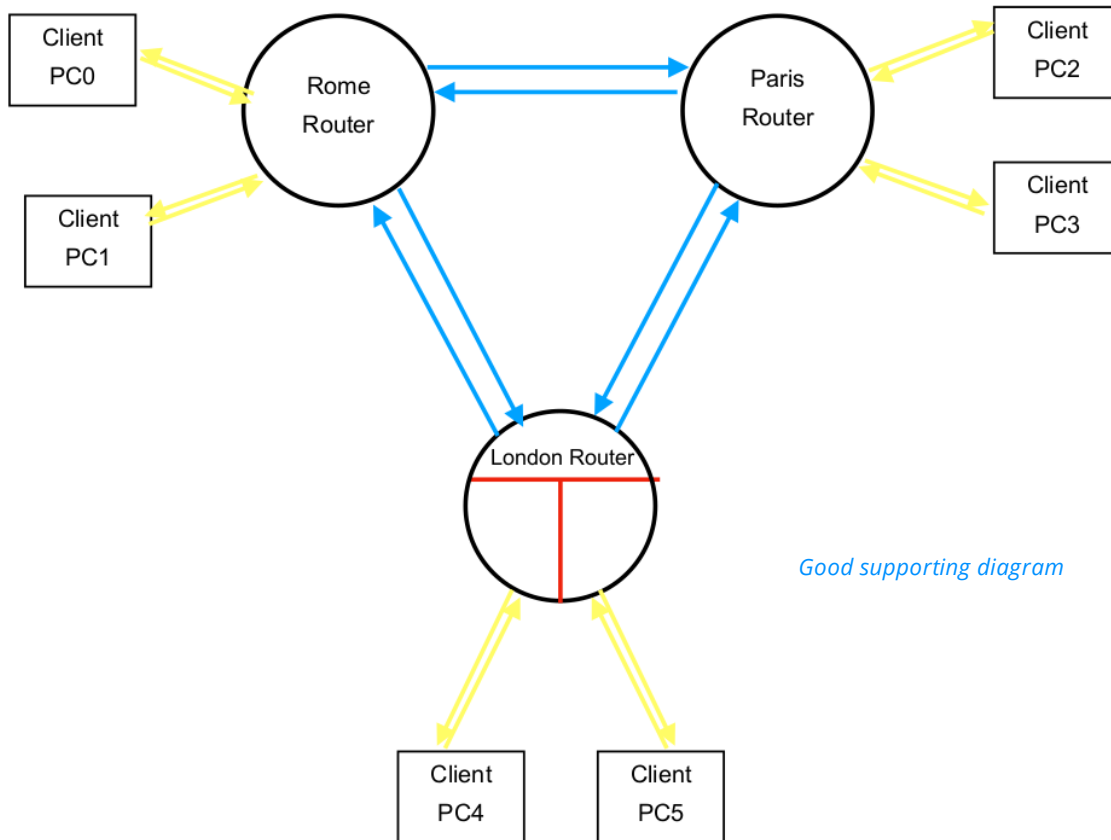


Figure 61 - 3 Router Network - VLAN Representation

The above figure shows the typical configuration of the VLAN network where the London Router/Gateway will be configured to separate the Router into 2 individual 'virtual' networks. The **red lines** represent VLAN separation where firewall rules govern the data that can or cannot pass over these divisions.

This allows rules to be implemented to prevent/authorise access between the 2 newly created Virtual networks (or VLANs) and even prevention/permission to access the wider network to the other 2 routers and subsequent client PCs (if required)

VLAN Implementation:

Note: See Appendix for full London switch VLAN naming, VLAN assignment and trunking configurations used

With the London switch now programmed, a 'show ip int brie' command on the London Router shows how the VLANs and associated clients are assigned to which port, with Ports now assigned to 1 of the 2 VLANs we have now created.

```
Router#show ip int brie
Interface                IP-Address      OK? Method Status
Protocol
FastEthernet0/0          unassigned      YES manual up
FastEthernet0/0.2        192.168.5.94    YES manual up
FastEthernet0/0.3        192.168.5.158   YES manual up
FastEthernet0/1          unassigned      YES unset  administratively down down
Serial0/0                192.168.5.10    YES manual up
Serial0/1                192.168.5.14    YES manual up
Router#
```

Figure 62 - London Router - VLAN Show IP Results

*Report shows Vlans subnetted with trunk protocol configured.
The 0/0.2 and 0/0.3 indicate the trunk is setup and the two gateways now exist on the one link.*

ACL Implementation:

Using the Paris Router, it was programmed to deny access to a specific IP address, a London PC with IP: 192.168.5.129 and permit all other traffic.

```
Router>en
Router#conf t
Router(config)#hostname Router
Router(config)#access-list 1 deny 192.168.5.129 0.0.0.0
Router(config)#access-list 1 permit any
Router(config)#exit
Router#conf t
Router(config)#int f0/0
Router(config-if)#ip access-group 1 out
Router(config-if)#exit
```

IP address to be denied
'access' into Paris LAN
network

All other IP addresses
given access 'access'
into Paris LAN network

ACL is configured

Figure 63 - Paris Router - IP Address Deny Configuration

```
Paris#show run
Building configuration...
Current configuration : 778 bytes
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname Paris
```

```
interface FastEthernet0/0
ip address 192.168.5.126 255.255.255.224
duplex auto speed auto
```

```
interface FastEthernet0/1
no ip address
duplex auto
speed auto
shutdown
```

```
interface Serial0/0
ip address 192.168.5.5 255.255.255.252
clock rate 2000000
```

```
interface Serial0/1
ip address 192.168.5.13 255.255.255.252
clock rate 2000000
```

```
router rip
version 2
network 192.168.5.0
```

```
ip classless
ip flow-export version 9
access-list 1 deny host 192.168.5.129
```

```
access-list 1 permit any
```

```
line con 0
line aux 0
line vty 0 4
login
end
```

WAN connection showing
correct IP address and
CIDR/30 subnet

Denial of IP address
confirmed

Good annotation of report

Access for all other IP
addresses confirmed

Figure 64 - Paris Router - IP Address Deny 'Show Run'

4. Test & Analysis

CIDR28 Network Testing:

With the routing table previously confirmed that the LAN and WAN network IP address tables have worked, packet send results show that the PC0 to PC5 spanning across the 3 different LAN networks can communicate with each other successfully.

Test supports the implementation

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num
	Successful	PC1	PC3	ICMP		0.000	N	0
	Successful	PC0	PC4	ICMP		0.000	N	1
	Successful	PC2	PC0	ICMP		0.000	N	2
	Successful	PC3	PC5	ICMP		0.000	N	3
	Successful	PC4	PC2	ICMP		0.000	N	4
	Successful	PC5	PC1	ICMP		0.000	N	5

Figure 65 - CIDR28 Routing - Packet Test Results

CIDR27/30 Network Testing:

After the LAN and Wan network subnets were changed to suit the CIDR27 and CIDR30 frame work respectively. Further packet tests confirm successful communication across the routers and WAN serial connections.

Test shows the errors in the address tables are typo errors rather than planned.

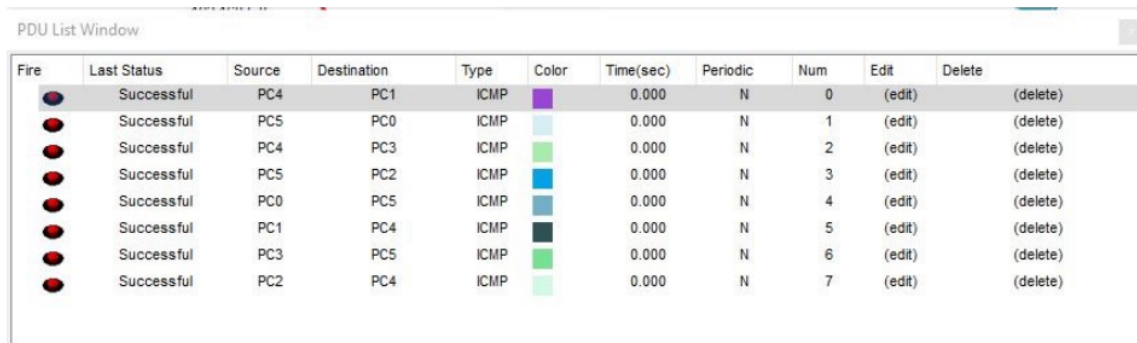
PDU List Window								
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num
	Successful	PC1	PC4	ICMP		0.000	N	0
	Successful	PC0	PC3	ICMP		0.000	N	1
	Successful	PC2	PC5	ICMP		0.000	N	2
	Successful	PC3	PC1	ICMP		0.000	N	3
	Successful	PC4	PC0	ICMP		0.000	N	4
	Successful	PC4	PC2	ICMP		0.000	N	5

Figure 66 - CIDR27&30 Routing - Packet Test Results

VLAN Network Testing:

Note: See Appendix for full London switch VLAN naming, VLAN assignment and trunking configurations used

With the London router now modified to create 2 VLANs instead of 1 LAN, packet tests confirm that the VLANs are still connected to each other and that the config has not defaulted to keep them separate despite separate gateway addresses. Packet send results show that both VLANs are exposed to each other and the rest of the wider network.



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC4	PC1	ICMP		0.000	N	0	(edit)	(delete)
	Successful	PC5	PC0	ICMP		0.000	N	1	(edit)	(delete)
	Successful	PC4	PC3	ICMP		0.000	N	2	(edit)	(delete)
	Successful	PC5	PC2	ICMP		0.000	N	3	(edit)	(delete)
	Successful	PC0	PC5	ICMP		0.000	N	4	(edit)	(delete)
	Successful	PC1	PC4	ICMP		0.000	N	5	(edit)	(delete)
	Successful	PC3	PC5	ICMP		0.000	N	6	(edit)	(delete)
	Successful	PC2	PC4	ICMP		0.000	N	7	(edit)	(delete)

Figure 67 - VLAN Network - Packet Test Results

Vlan test is successful

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.5.65

Pinging 192.168.5.65 with 32 bytes of data:

Reply from 192.168.5.65: bytes=32 time<1ms TTL=127
Reply from 192.168.5.65: bytes=32 time<1ms TTL=127
Reply from 192.168.5.65: bytes=32 time<1ms TTL=127
Reply from 192.168.5.65: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.5.65:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Figure 69 - London PC2 > PC1 - Ping Results

ACL Testing:

The London PC1 (IP: 192.168.5.65) and PC2 (IP: 192.168.5.129) was pinged from the Paris client PC with the ping results showing successful Access Control List protocols implemented:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.5.129

Pinging 192.168.5.129 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.5.129:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.5.65

Pinging 192.168.5.65 with 32 bytes of data:

Reply from 192.168.5.65: bytes=32 time=1ms TTL=126
Reply from 192.168.5.65: bytes=32 time=10ms TTL=126
Reply from 192.168.5.65: bytes=32 time=11ms TTL=126
Reply from 192.168.5.65: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.5.65:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 11ms, Average = 5ms

C:\>|
```

*Denial of service is
identified for the
address blocked by in
the ACL config*

Figure 70 - London PC2 > PC1 - Ping Results

5. Evaluation

The test results show that the packet test feature within the Cisco packet tracer program shows that the data was passing across all configured networks without issue, showing that the planned network IP address tables were correctly spaced and chosen to ensure no overlap or incorrect spacing according to the subnet.

The use of classless subnets allow for the size of the networks (the amount of clients allowed in the subnet before it is full) to be configured to the exact amount required.

This gives the benefit of creating a network that physically prevents further clients from connecting to the network and improves security and integrity of the network considerably.

The less possible clients that can live on a network at any one time also improves the speed and robustness of a network.

As the CIDR/28 allowed 16 IP addresses per network, the final network layout identified that the WAN connections did not be required to stay on a CIDR/28 and could be reduced down using a CIDR/30, only allowing 2 connections, which was sufficient as the router layout that 2 Wan connections were required.

Good significant point

The Cisco packet tracer programs features, particularly the router tables and 'Show IP route' gateway result was an effective visual representation of how the network was configured without the use of ping testing and physical connection and real world testing of the network.

As with any ACL (Access Control List) rule, the ability to command specific 'block requests' for 1 individual IP address was effective as long as another rules can also be implemented. In this example, the ability to specify that all other traffic be granted ensured that ONLY the IP address was being denied and not the associated VLAN etc.

Good informative evaluation which identified the effective methods used in the tasks

Element 3

1. Introduction

Using the programming and learning so far, with the ability to configure different LAN networks connected via WAN serial connections, with the ability to configure Class A, B, C or classless CIDR/27,28 or even CIDR/30 subnets.

This element will focus on the ability to transfer the theoretical programming using software to create 2 physical VLANs on the same gateway using specific switch port numbers.

These 2 VLANs will be used to then testing the ability to prove that real world data (PLC data) can pass across these 2 VLANs to show that data on one VLAN can be transferred to another VLAN where it can be received and interacted with, for retransmission back to the PLC.

Good informative introduction that identifies requirements

2. System Configuration Requirements

Using the London network as a base, the network will comprise of 3 wired network clients, with 2 being user Laptops and 1 being a Siemens S7-1200 PLC.

Each client will connect to a Cisco 2950 switch and an upstream 2600 Gateway/Router.

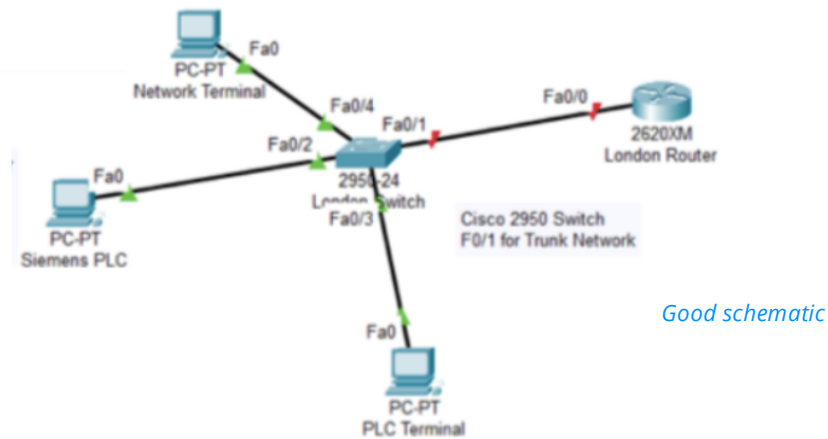


Figure 71 - Element 3 Network Overview

3. Implementation

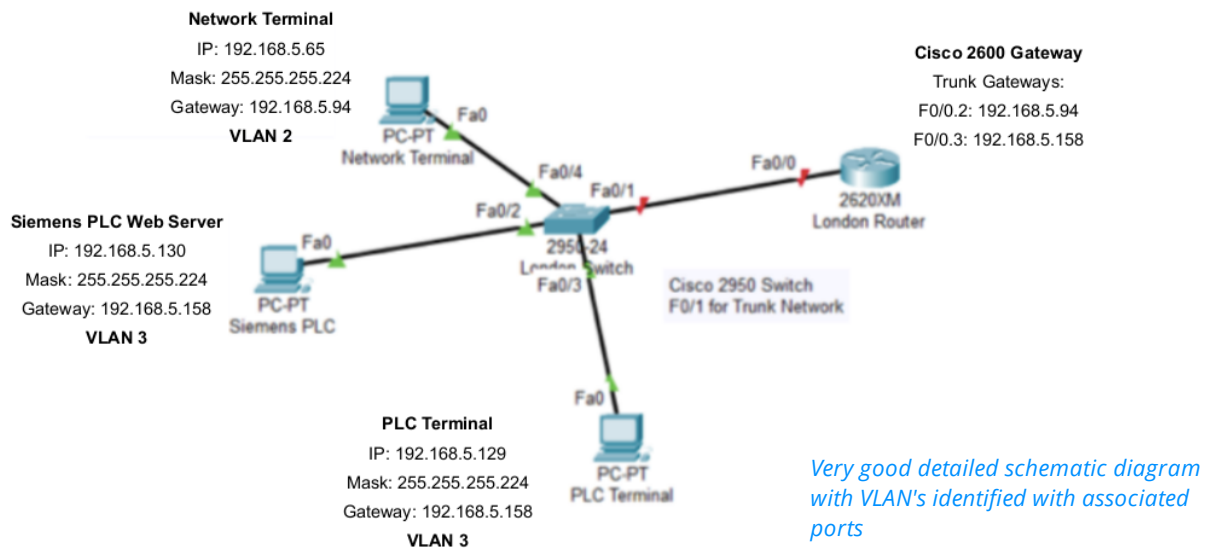


Figure 72 - Element 3 Finalised Network Map

Using the Cisco 2600 gateway, 2 trunks or VLANs will be created. Using specific configuration, and because we know the physical ports that all 3 clients are connected to, we can specify what ports are assigned to what VLANs, effectively segregated them by their physical port selection on the switch.

Cisco Switch VLAN Name Config:

```
Switch>en
Switch#conf t
Switch(config)#vlan 2
Switch(config-vlan)#name vlan2
Switch(config-vlan)#exit
Switch(config)#vlan 3
Switch(config-vlan)#name vlan3
Switch(config-vlan)#exit
Switch(config)#^Z
```

VLAN's are set and named

Figure 73 - Element 3 Switch VLAN Creation

Assigning Cisco Switch Ports to their respective VLAN:

```
Switch#conf t
Switch(config)#int f0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 3
Switch(config-if)#exit

Switch(config)#int f0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 3
Switch(config-if)#exit

Switch(config)#int f0/4
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 2
Switch(config-if)#exit
Switch(config)#^Z
```

Ports are allocated

Figure 74 - Element 3 Switch VLAN Port Assigning

Cisco Router Config:

```
Router>en
Router#conf t
Router(config)#int f0/0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#int f0/0
Router(config-if)#no ip address
Router(config-if)#exit

Router(config)#int f0/0.2
Router(config-subif)#encapsulation dot1Q 2
Router(config-subif)#ip address 192.168.5.94 255.255.255.224
Router(config-subif)#no shutdown
Router(config-subif)#exit

Router(config)#int f0/0.3
Router(config-subif)#encapsulation dot1Q 3
Router(config-subif)#ip address 192.168.5.158 255.255.255.224
Router(config-subif)#no shutdown
Router(config-subif)#exit
```

Gateway port is disabled

Two new gateway addresses are assigned. One for each VLAN

Figure 75 - Element 3 Router VLAN Programming

```
Router#show ip int brie
```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	unassigned	YES	manual	up	up
FastEthernet0/0.2	192.168.5.94	YES	manual	up	up
FastEthernet0/0.3	192.168.5.158	YES	manual	up	up
FastEthernet0/1	unassigned	YES	unset	administratively down	down
Serial0/0	unassigned	YES	unset	administratively down	down
Serial0/1	unassigned	YES	unset	administratively down	down

```
Router#
```

Report shows the two gateways are configured and active

Figure 76 - Element 3 Router - 'Show IP Brie' Result

With the correct switch ports now assigned to their intended VLANs, any clients connected to those ports will be forced into either a 192.168.5.94 gateway or 192.168.5.158 gateway addresses. *Correct*

With all 3 clients now physically connected to the associated switch ports, the PLC required a manual IP assignment via the TIA portal program.

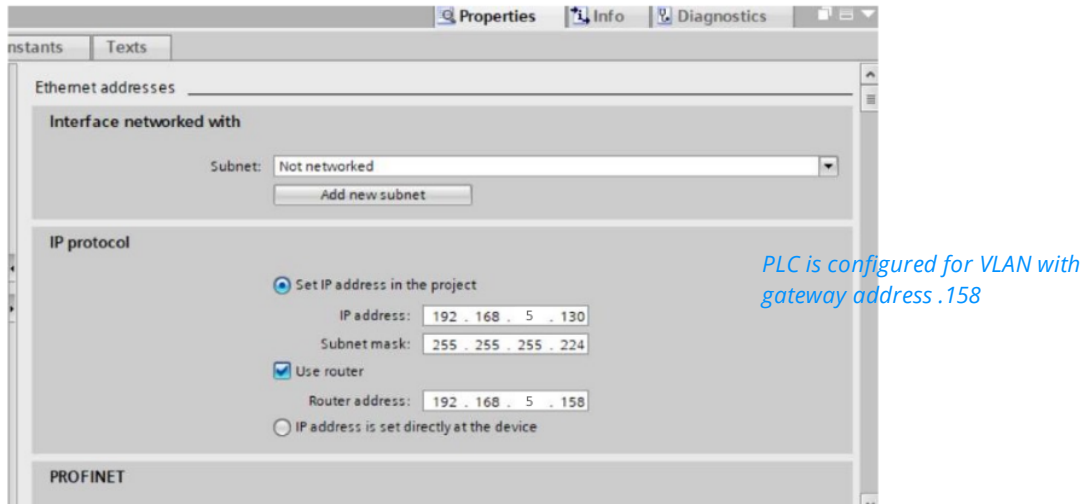


Figure 77 - Siemens S7-1200 PLC - Set IP Address

Now the PLC is required to be setup as a web server so that the 2 Laptop clients can access and read data via a browser using the HTTP protocol.

The PLC Terminal was used to access the Siemens S7-1200 PLC via the TIA Portal program to activate the inbuilt Siemens web server.

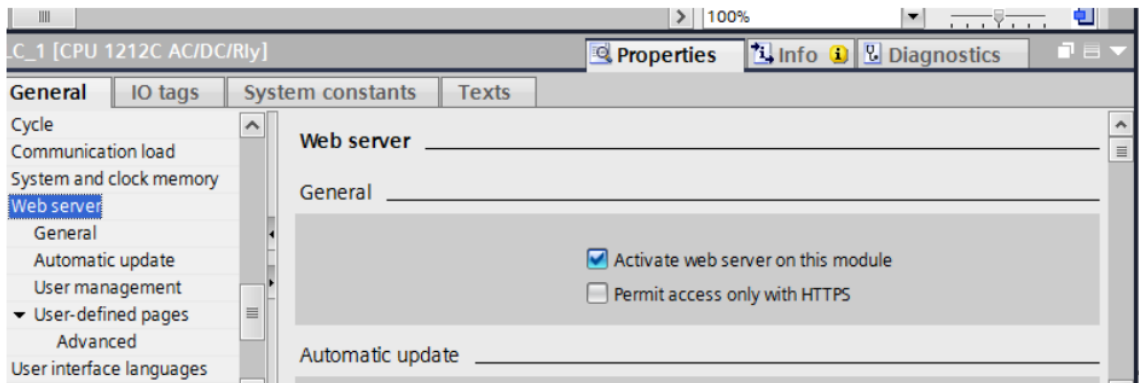


Figure 78 - Siemens S7-1200 - Web Server Activation

TIA Portal is also used to specify the types of files used in the web server. These file types will be used to create inside the web server pages to create dynamic content needed to display the dynamically changing data coming from or going to the PLC.

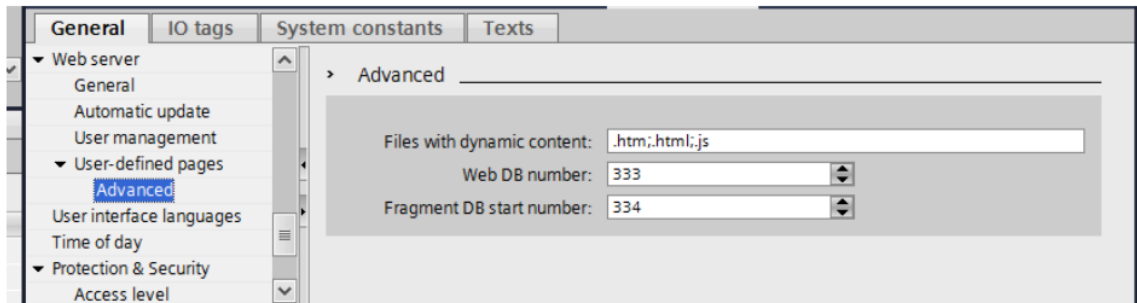


Figure 79 - Siemens S7-1200 - User Defined Pages

The file types used are:

.htm - Hypertext Markup

.html - Hypertext Markup Language

.js - javascript

Web server is configured and program is downloaded over the VLAN network

Note: Because .js is not natively compatible on S7-PLC models lower than '1500 series', the .js program will be embedded in the HTML code using .json library functions.

Good point identified

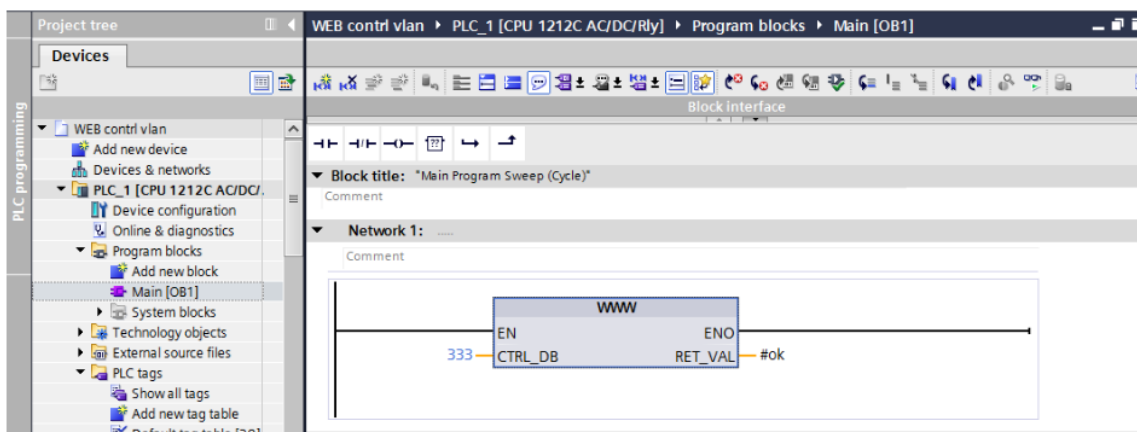


Figure 80 - Siemens S7-1200 PLC - Web Server Function Call Block

To enable the web server to read the DB333, the 'WWW' block was added to the main Organisation Block 'OB1' so it will be called to run when the PLC is in 'RUN' Mode.

This means that the web server read and writes to DB333, which must exist in the PLC code for it to work.

Motor Control PLC Code:

To control an external DC motor via PWM signals, some Function blocks were added to OB1.

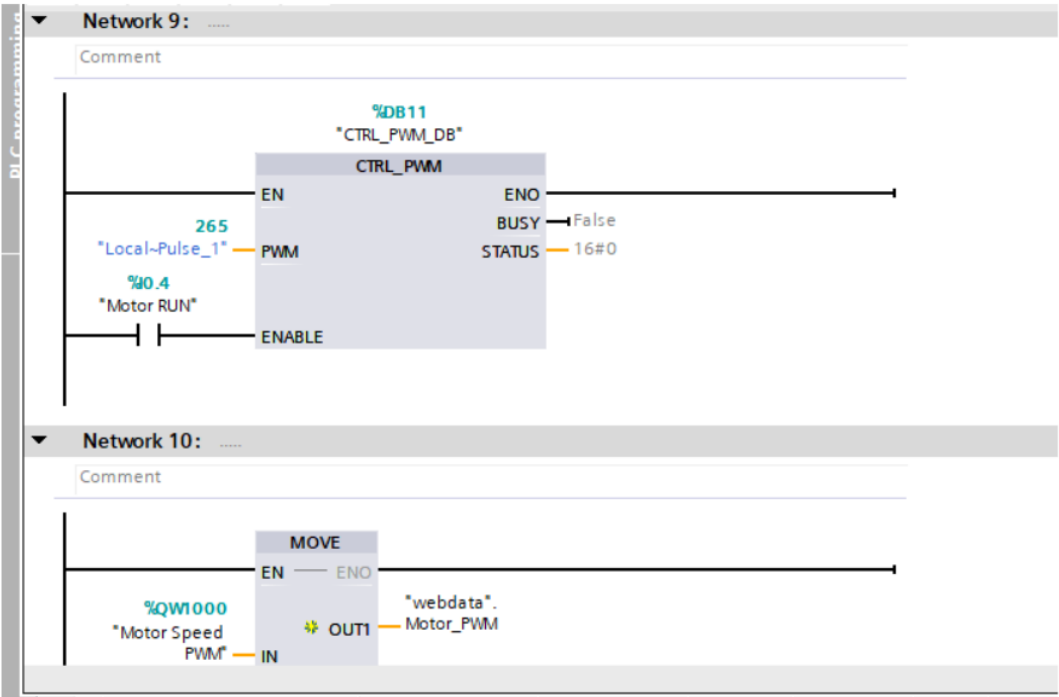


Figure 81 - Siemens S7-1200 PLC - Web Server Function Call Block

IO Addresses were specified for the physical PLC inputs for the PWM output, switch input and PWM speed.

Default tag table			
	Name	Data type	Address
	Motor Speed PWM	Word	%QW1000
	Motor RUN	Bool	%I0.4
	Motor PWM output	Bool	%Q1.1

Figure 82 - Siemens S7-1200 PLC - IO Tag List

PLC program to run DC motor

A series of files were required to be downloaded into the S7-1200 PLC folder structure so they could be referenced and called by the web server.

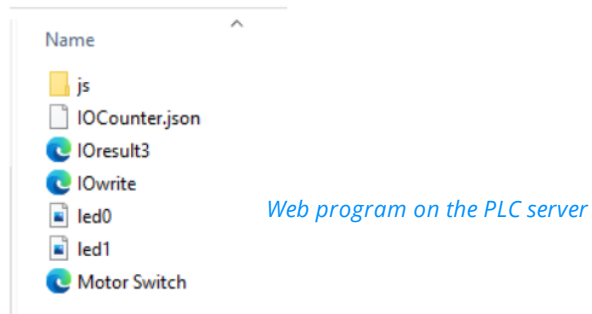


Figure 83 - Siemens S7-1200 PLC - User Files

TIA portal also has the functionality to specify the html file that is called by default, which gives a nicer solution to the end user.

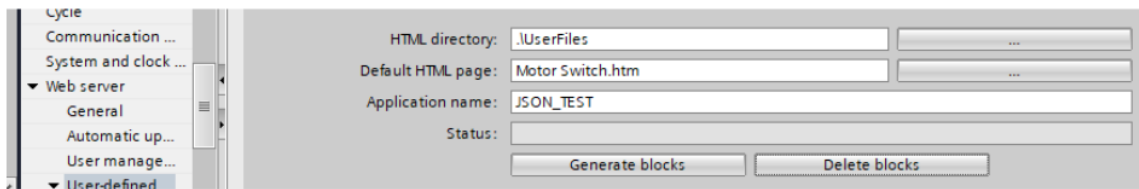


Figure 84 - Siemens S7-1200 PLC - Web Server Default Page

The Motor switch.htm file references the the rest of the files contained within the 'User Files' downloaded to the PLC.

The following flow diagrams show how the Motor Switch.HTM file sends and receives data to/from the PLC and refreshes it with a 1000mS refresh rate, set by the javascript.

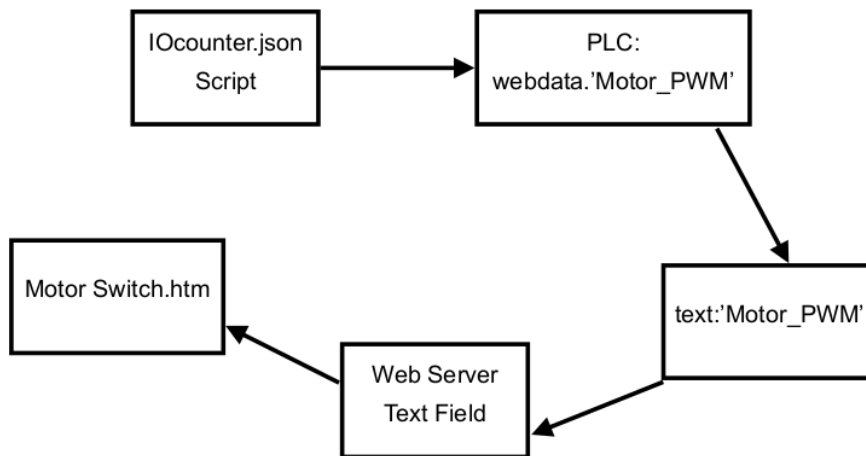


Figure 85 - Siemens S7-1200 PLC - Motor PWM Flow Diagram

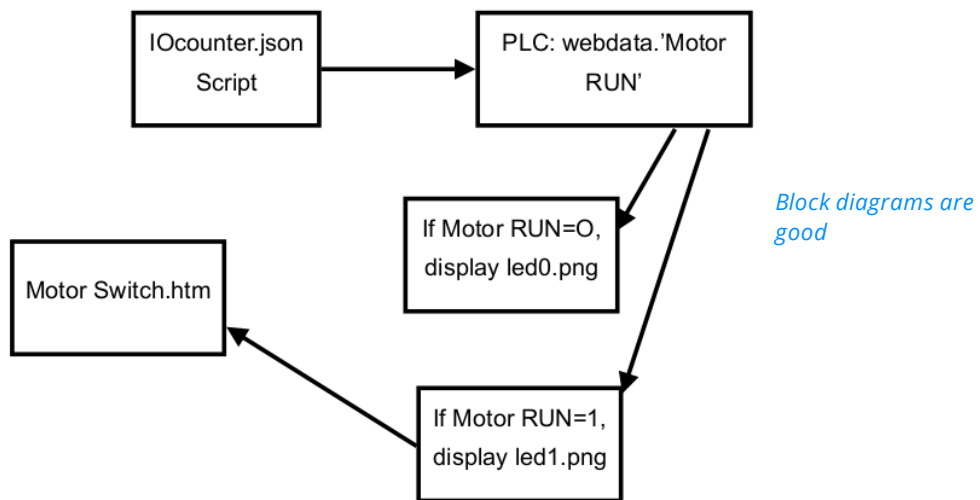
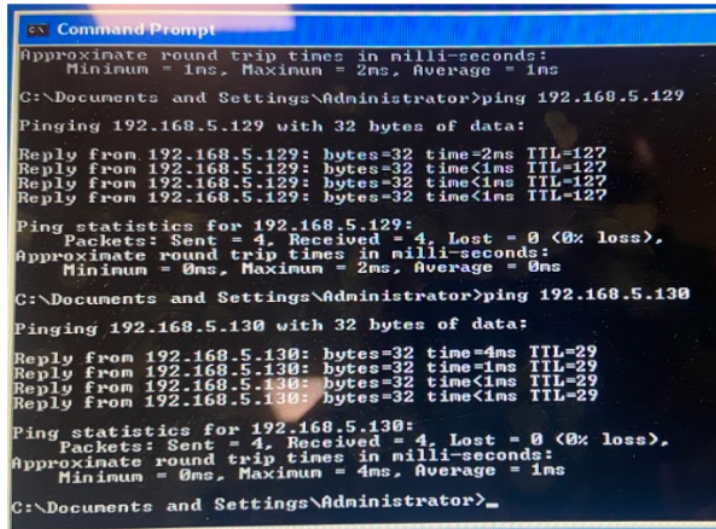


Figure 86 - Siemens S7-1200 PLC - Motor Run Status Flow Diagram

4. Test & Analysis

VLAN

With the Network Laptop terminal situated on one VLAN and the PLC & PLC Terminal on the other VLAN, we initiated a 'ping test' using Windows Command Prompt to check communication across the 2 VLANs (between the PLC terminal/PLC and the network terminal) was possible.



```
Command Prompt
Approximate round trip times in milli-seconds:
  Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\Documents and Settings\Administrator>ping 192.168.5.129

Pinging 192.168.5.129 with 32 bytes of data:

Reply from 192.168.5.129: bytes=32 time=2ms TTL=127
Reply from 192.168.5.129: bytes=32 time<1ms TTL=127
Reply from 192.168.5.129: bytes=32 time<1ms TTL=127
Reply from 192.168.5.129: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.5.129:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
      Minimum = 0ms, Maximum = 2ms, Average = 0ms

C:\Documents and Settings\Administrator>ping 192.168.5.130

Pinging 192.168.5.130 with 32 bytes of data:

Reply from 192.168.5.130: bytes=32 time=4ms TTL=29
Reply from 192.168.5.130: bytes=32 time<1ms TTL=29
Reply from 192.168.5.130: bytes=32 time<1ms TTL=29
Reply from 192.168.5.130: bytes=32 time<1ms TTL=29

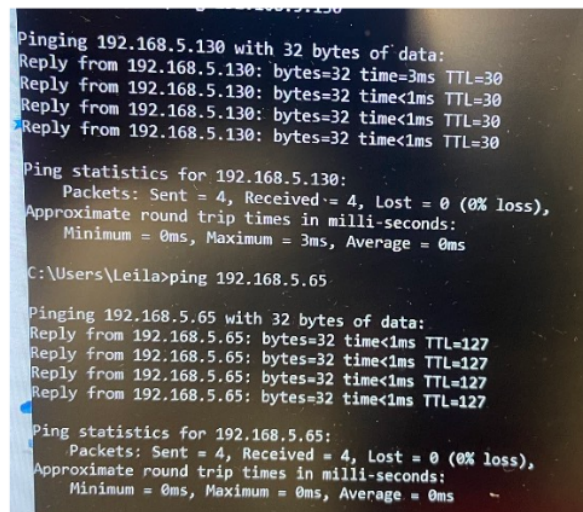
Ping statistics for 192.168.5.130:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
      Minimum = 0ms, Maximum = 4ms, Average = 1ms

C:\Documents and Settings\Administrator>
```

Test indicates the VLANs are communicating

Figure 87 - Network Terminal - Ping Test to PLC & PLC Terminal

Again, the ping test using Windows command prompt was done to confirm communication to the Network Terminal and PLC, thus proving data is crossing the 2 created VLANs.



```
Pinging 192.168.5.130 with 32 bytes of data:
Reply from 192.168.5.130: bytes=32 time=3ms TTL=30
Reply from 192.168.5.130: bytes=32 time<1ms TTL=30
Reply from 192.168.5.130: bytes=32 time<1ms TTL=30
Reply from 192.168.5.130: bytes=32 time<1ms TTL=30

Ping statistics for 192.168.5.130:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
      Minimum = 0ms, Maximum = 3ms, Average = 0ms

C:\Users\Leila>ping 192.168.5.65

Pinging 192.168.5.65 with 32 bytes of data:
Reply from 192.168.5.65: bytes=32 time<1ms TTL=127
Reply from 192.168.5.65: bytes=32 time<1ms TTL=127
Reply from 192.168.5.65: bytes=32 time<1ms TTL=127
Reply from 192.168.5.65: bytes=32 time<1ms TTL=127

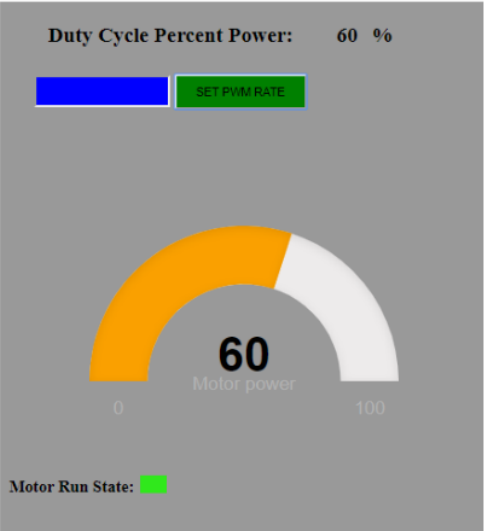
Ping statistics for 192.168.5.65:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
      Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Tests are successful

Figure 88 - PLC Terminal - Ping Test to PLC & Network Terminal

Siemens S7-1200 Web Server:

With the web server now enabled and active, simply navigating to <http://192.168.5.130> brings up the S7-1200 PLC web server home page, where the configured motor switch.htm is available to be clicked and viewed.



Test shows the data flow form the web server of the plc to and from the browser over the VLAN network

Figure 89 - S7-1200 Web Server Motor Test - 60% PWM Output

Monitoring the Tag List for the PLC shows that the inputted '60' from the text field on the web server has been written to the 'QW1000' variable and that the Motor Power gauge is responded with a correct reading.

Name	Address	Display format	Monitor value	Mo
*Motor Speed ...	%QW1000	Hex	16#003C	
*Motor RUN	%IO.4	Bool	TRUE	
webdata.Motor...		DEC+/-	60	

Watch table confirms data is dynamic

Figure 90 - S7-1200 IO Tag List Monitoring - 60% PWM Output

The test was repeated with 90% inputted into the test field and the web server and PLC IO tag list monitored to reflect the changes.

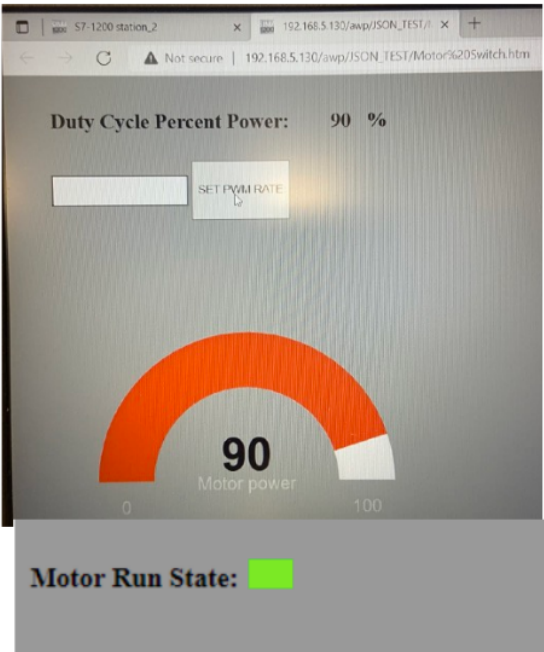


Figure 91 - S7-1200 Web Server Motor Test - 90% PWM Output

Name	Address	Display format	Monitor value	Mod
*Motor Speed ...	%QW1000	Hex	16#005A	
Motor RUN	%I0.4	Bool	TRUE	
webdata.Motor...		DEC+/-	90	

Figure 92 - S7-1200 IO Tag List Monitoring - 90% PWM Output

5. Conclusions & Recommendations

The use of Cisco packet tracer and packet tests has allowed us for a network to be planned out, making the use of hardware as well as software requirements needed to build a network, prior to actual deployment. This allows network engineers to build networks with gateway firewall rules in place ready for security measures to be in place the moment a network is implemented, rather than doing it 'Ad-hoc' after installation.

The final element has encompassed the knowledge and understanding that different networks can be setup, and each network can be configured to hold a certain amount of clients, all dependant upon the subnet, which can be tweaked to change the number of clients.

The element shown that despite the size and/or number of clients connected to a certain LAN, individual LANs (LOCAL area networks) can be joined together to form an overall WAN (wide area network), showing that data can be shared between LANs.

The use of router and gateways allow for 'firewalls' to be introduced. Firewalls give you the facility to block incoming and outgoing data, whether it be through the use of Port numbers, or via specific sensitive IP addresses on the LAN network.

This mean that the data you want to be sent and received can be accurately controlled and monitored to ensure that no sensitive or unrelated data is sent over an unmonitored connection.

The portfolio proves that the OSI network model that 'application, presentation and session' layers were vital to transmit and present data housed within a PLC that would be nearly impossible to understand visually with ease.

The use of a web browser, html and javascript languages allowed for data to be requested, transmitted and received, providing a way for it to be converted to a much easier format to understand. These application and protocols open up functionality and use of Human-Machine Interfaces.

With Industry 4.0 and the use of cloud connected processors, the movement of data from one point to another has revolutionised the industry but this must come with a certain amount of control. The use of Lan and Wan networks allow for routers to be configured to allow communication securely, especially with encryption levels allowing for data to be scrambled and unscrambled, further cementing the idea that encapsulation and decapsulation of data to ensure encryption is complex but achievable.

The use of VPNs allow for P2P connections, creating a virtual 'tunnel' for sensitive data to be transferred across multiple networks. This type of connections is becoming more and more prevalent in connections such as the networks we have investigated in this portfolio.

Because of the S7-1200 web server, improvements could be made to the page showing a time/heartbeat to show that the page is actually refreshing, which is especially useful when remote monitoring a PLC, making sure that the onscreen data is live and successfully refreshing rather than relying on the assumption that its actually refreshing successfully rather than stuck displaying old information.

Citation List

Comer, D.E. (2015) Computer networks and internets. 6th edn. England: Pearson. Available at: <<http://www.vlebooks.com/vleweb/product/openreader?id=sirgar&isbn=9781292061825>> (Accessed: 23 May 2022).

(Imperva, 2022) (online) Available at: <<https://www.imperva.com/learn/application-security/osi-model/>> Accessed 23rd May 2022

(BMC, 2022) (online) Available at: <<https://www.bmc.com/blogs/osi-model-7-layers/>> Accessed 23rd May 2022

(Medium, 2022) (online) Available at: <<https://medium.com/@harishramkumar/difference-between-layer-4-vs-layer-7-load-balancing-57464e29ed9f>> Accessed 23rd May 2022

(Network Encyclopedia, 2022) (online) Available at: <<https://networkencyclopedia.com/encapsulation/>> Accessed 23rd May 2022

(Computer Networking Notes, 2022) (online) Available at: <<https://www.computernetworkingnotes.com/ccna-study-guide/data-encapsulation-and-de-encapsulation-explained.html>> Accessed 29th May 2022

(Afteracademy, 2022) (online) Available at: <<https://afteracademy.com/blog/what-is-data-encapsulation-and-de-encapsulation-in-networking>> Accessed 23rd May 2022

(IONOS, 2022) (online) Available at: <<https://www.ionos.co.uk/digitalguide/server/know-how/broadcast-address/>> Accessed 23rd May 2022

(Homenethowto, 2022) (online) Available at: <<https://www.homenethowto.com/switching/broadcasts/>> Accessed 23rd May 2022

(Techtarget, 2022) (online) Available at: <<https://www.techtarget.com/searchnetworking/definition/port-number>> Accessed 23rd May 2022

Good number of reference sources in list

Appendix

```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 2
Switch(config-vlan)#name vlan2
Switch(config-vlan)#exit
Switch(config)#vlan 3
Switch(config-vlan)#name vlan3
Switch(config-vlan)#exit

%SYS-5-CONFIG_I: Configured from console by console

Switch#show vlan
VLAN Name                Status    Ports
-----
1    default                active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                           Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                           Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                           Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                           Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                           Fa0/21, Fa0/22, Fa0/23, Fa0/24
2    vlan2                  active
3    vlan3                  active
1002 fddi-default          active
1003 token-ring-default    active
1004 fddinet-default        active
1005 trnet-default          active
VLAN Type  SAID      MTU    Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
-----
1    enet    100001    1500   -      -      -      -   -      0      0
2    enet    100002    1500   -      -      -      -   -      0      0
3    enet    100003    1500   -      -      -      -   -      0      0
1002 fddi    101002    1500   -      -      -      -   -      0      0
1003 tr      101003    1500   -      -      -      -   -      0      0
1004 fdnet   101004    1500   -      -      -      ieee -      0      0
1005 trnet   101005    1500   -      -      -      ibm  -      0      0

VLAN Type  SAID      MTU    Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
-----
Remote SPAN VLANs
-----
Primary Secondary Type      Ports
-----
Switch#
```

Figure 93 - VLAN London Switch - VLAN Naming

```

Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int f0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 2
Switch(config-if)#exit
Switch(config)#int f0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 3
Switch#
%SYS-5-CONFIG_I: Configured from console by console
Switch#show vlan

```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/4, Fa0/5, Fa0/6 Fa0/7, Fa0/8, Fa0/9, Fa0/10 Fa0/11, Fa0/12, Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/23, Fa0/24
2	vlan2	active	Fa0/2
3	vlan3	active	Fa0/3
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0
2	enet	100002	1500	-	-	-	-	-	0	0
3	enet	100003	1500	-	-	-	-	-	0	0
1002	fddi	101002	1500	-	-	-	-	-	0	0
1003	tr	101003	1500	-	-	-	-	-	0	0
1004	fdnet	101004	1500	-	-	-	ieee	-	0	0
1005	trnet	101005	1500	-	-	-	ibm	-	0	0

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0
2	enet	100002	1500	-	-	-	-	-	0	0
3	enet	100003	1500	-	-	-	-	-	0	0
1002	fddi	101002	1500	-	-	-	-	-	0	0
1003	tr	101003	1500	-	-	-	-	-	0	0
1004	fdnet	101004	1500	-	-	-	ieee	-	0	0
1005	trnet	101005	1500	-	-	-	ibm	-	0	0

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0
2	enet	100002	1500	-	-	-	-	-	0	0
3	enet	100003	1500	-	-	-	-	-	0	0
1002	fddi	101002	1500	-	-	-	-	-	0	0
1003	tr	101003	1500	-	-	-	-	-	0	0
1004	fdnet	101004	1500	-	-	-	ieee	-	0	0
1005	trnet	101005	1500	-	-	-	ibm	-	0	0

Primary	Secondary	Type	Ports

Figure 94 - VLAN London Switch - VLAN Port Assigning

```

Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int f0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 2
Switch(config-if)#exit
Switch(config)#int f0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 3
Switch#
%SYS-5-CONFIG_I: Configured from console by console
Switch#show vlan

```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/4, Fa0/5, Fa0/6 Fa0/7, Fa0/8, Fa0/9, Fa0/10 Fa0/11, Fa0/12, Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/23, Fa0/24
2	vlan2	active	Fa0/2
3	vlan3	active	Fa0/3
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

Further evidence here of implementation

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0
2	enet	100002	1500	-	-	-	-	-	0	0
3	enet	100003	1500	-	-	-	-	-	0	0
1002	fddi	101002	1500	-	-	-	-	-	0	0
1003	tr	101003	1500	-	-	-	-	-	0	0
1004	fdnet	101004	1500	-	-	-	ieee	-	0	0
1005	trnet	101005	1500	-	-	-	ibm	-	0	0

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0
2	enet	100002	1500	-	-	-	-	-	0	0
3	enet	100003	1500	-	-	-	-	-	0	0
1002	fddi	101002	1500	-	-	-	-	-	0	0
1003	tr	101003	1500	-	-	-	-	-	0	0
1004	fdnet	101004	1500	-	-	-	ieee	-	0	0
1005	trnet	101005	1500	-	-	-	ibm	-	0	0

```

Remote SPAN VLANs
-----
Primary Secondary Type Ports
-----

```

Figure 95 - VLAN London Switch - VLAN Trunk Assigning

1809809

GRADEMARK REPORT

FINAL GRADE

GENERAL COMMENTS

Instructor

74/100

PAGE 1

PAGE 2

Text Comment. Good table of contents

PAGE 3

PAGE 4

Text Comment. Extensive list of figures

PAGE 5

Text Comment. Good outline of task that indicated a good understanding of the requirements (this proves that the brief has been studied).

PAGE 6

Text Comment. The essence of a network link

Text Comment. A very good interpretation of the construction of data packets. Good supporting image with ref source.

PAGE 7

Text Comment. Layers are identified

PAGE 8

Text Comment. The image supports the explanation

Text Comment. This is a significant point

PAGE 9

Text Comment. Good comparison between models

PAGE 10

Text Comment. A very good image that supports the very clear explanation

PAGE 11

Text Comment. Good explanation that is consistent with the diagram illustrated

PAGE 12

Text Comment. Good point identified

Text Comment. Broadcast purpose is explained

Text Comment. Large networks are generally split up into smaller domains to reduce broadcast operations. This makes the network more reliable and faster.

Text Comment. Ports are identified

PAGE 13

Text Comment. Good work here with good supporting ref sources

Text Comment. Research section is covered in good detail and supported with good relevant images and ref sources

PAGE 14

Text Comment. Network Topology is identified

PAGE 15

Text Comment. Very good address scheme method that clearly defines the understanding

Text Comment. The 3 address classes are established with the appropriate subnet masking

PAGE 16

Text Comment. Excellent schematic diagram

PAGE 17

PAGE 18

Text Comment. Static routing tables are configured

PAGE 19

Text Comment. Router report tables indicate correct configuration

Text Comment. Static routing is configured

PAGE 20

PAGE 21

Text Comment. Dynamic routing is configured

PAGE 22

Text Comment. Good diagram indicating function of DHCP

PAGE 23

PAGE 24

Text Comment. DHCP configuration is set along with helper addresses to cross boundaries

PAGE 25

Text Comment. Exclusion addresses are configured

PAGE 26

Text Comment. Test results support static routing protocol function

Text Comment. Test results support the dynamic routing protocol

Text Comment. Good test showing errors due to no helper addresses configured

Text Comment. Error corrected due to helper address allocation

Text Comment. DHCP protocol test indicating the exclusion addresses

Text Comment. Good informative evaluation that sets up a knowledge base for the next element

Text Comment. Good introduction to the scope of the element

Text Comment. Good schematic diagram with network addresses identified

Text Comment. Good effective explanation

Text Comment. Subnet mask is identified

Text Comment. This should start at .16 instead of .1, However the spacing is correct

Text Comment. Address scheme is established for LAN networks

Text Comment. Serial link spacing is correct

Text Comment. Serial addresses are identified

Text Comment. Subnets are identified for both network schemes

Text Comment. The '1' here should be one place to the right

Text Comment. First 4 digits from the right should be 0010

Text Comment. The address for 62 should be 00111110 and 63 would be 00111111

PAGE 36

Text Comment. Error herewith last 2 lines

Text Comment. Correct here

PAGE 37

Text Comment. Error here

Text Comment. Correct

Text Comment. Correct

Text Comment. Correct

PAGE 38

Text Comment. Despite the minor errors in the schematic tables with binary 1ns in wrong places in 3 instances, the configuration is correct

PAGE 39

PAGE 40

Text Comment. Configuration is good

PAGE 41

PAGE 42

Text Comment. Reports indicate configuration is correct and show what is directly connected and routed.

PAGE 43

Text Comment. Good supporting diagram

Text Comment. Report shows Vlans subnetted with trunk protocol configured. The 0/0.2 and 0/0.3 indicate the trunk is setup and the two gateways now exist on the one link.

Text Comment. ACL is configured

Text Comment. Good annotation of report

Text Comment. Test supports the implementation

Text Comment. Test shows the errors in the address tables are typo errors rather than planned.

Text Comment. Vlan test is successful

Text Comment. Denial of service is identified for the address blocked by in the ACL config

Text Comment. Good significant point

Text Comment. Good informative evaluation which identified the effective methods used in the tasks

Text Comment. Good informative introduction that identifies requirements

Text Comment. Good schematic

Text Comment. Very good detailed schematic diagram with VLAN's identified with associated ports

Text Comment. VLAN's are set and named

PAGE 54

Text Comment. Ports are allocated

PAGE 55

Text Comment. Gateway port is disabled

Text Comment. Two new gateway addresses are assigned. One for each VLAN

Text Comment. Report shows the two gateways are configured and active

PAGE 56

Text Comment. Correct

Text Comment. PLC is configured for VLAN with gateway address .158

PAGE 57

Text Comment. Web server is configured and program is downloaded over the VLAN network

Text Comment. Good point identified

PAGE 58

Text Comment. PLC program to run DC motor

PAGE 59

Text Comment. Web program on the PLC server

PAGE 60

Text Comment. Block diagrams are good

PAGE 61

Text Comment. Test indicates the VLANs are communicating

Text Comment. Tests are successful

PAGE 62

Text Comment. Test shows the data flow from the web server of the plc to and from the browser over the VLAN network

Text Comment. Watch table confirms data is dynamic

PAGE 63

PAGE 64

Text Comment. Good conclusion and recommendation

PAGE 65

Text Comment. Good number of reference sources in list

PAGE 66

PAGE 67

PAGE 68

Text Comment. Further evidence here of implementation

GRADING FORM: CSG-RUBIC

RHYS DAVIES

74

RESEARCH-INFORMED LITERATURE



Research is extensive and plenty of relevant ref sources included. 8/10

8

KNOWLEDGE AND UNDERSTANDING



Element 1 is designed with a good schematic address table and implemented using the chosen address scheme. all tasks are present. 8/10
Element 2 had some minor errors in the address tables for /27 and /30 sections. The errors were rectified in the implementation as the results proved. 7.5/10
Element 3 practical is detailed and each step is explained. there is a minor evidence part missing for the trunk protocol. The function calls have not been explained . 6.5/10

22

ANALYSIS



E1 test evidence is included and explained. The tests are successful and in a good order. 3.5/5
E2 - results prove the error in the test tables address scheme has been solved. The test results prove the operation of the network for all CIDR arrangements. The VLAN is developed from the final CIDR design and tests prove the configuration. ACL testing proved successful with evidence of the test outcomes. 8/10
E3 - Practical VLAN test evidence is provided and indicate the correct functioning of the network. The PLC functions are tested with evidence directly from the PLC and browser matching. 8.5/10

20

PRACTICAL APPLICATION AND DEP.



E1 - Implementation from topology design carried out using address schema table method. Testing procedure tested every device in every direction and proved successful. 3.5/5 E2 - implementation address tables have some minor errors which have been solved during the implementation stage. Network was further developed for VLAN configuration and ACL functions implemented. 3/5 E3 - The practical network has been successfully implemented. However the function calls have not been explained. 6.5/10

13

SKILLS FOR PROFESSIONAL PRAC.



A good report despite some minor errors and some content missing. 11/15

11