# ACCA7029 written exam

Matthew Cooze 1911017

May 11, 2021

# Contents


0.1 1 . . . . . 1
0.1.1 1a. In reference with ISP redundancy, explain . . . . . 1
0.1.2 1b. Refer to Figure 1, identify RSTP port roles and explain them. . . . . 3
0.2 2 . . . . . 4
0.2.1 a. Explain the functionality of a Routed port and how it can be enabled on a Switch? . . . . . 4
0.2.2 b. Briefly explain OSPF packet types. . . . . 5
0.2.3 c. With reference to EIGRP, explain the following . . . . 6
0.3 3 . . . . . 6
0.3.1 question . . . . . 6
0.3.2 answer . . . . . 7
0.4 references . . . . . 12


## 0.1 1

### 0.1.1 1a. In reference with ISP redundancy, explain

key:

ISP(internet service provider)

home (customers internet location e.g business, home, workplace )

**i.Single-homed** single homed means you have only one connection to the internet service provider, the advantages of single homed is that it is cost effective, the disadvantage is that there is no redundancy the connection goes down there will be no internet until the connection goes back up.

**ii. Dual-homed** duel homed redundancy works by adding a second link to the same internet service provider, this means if one route stops working the other can start working so you still have internet, this only works if the internet service providers entire network in your local area is not down.

there are 4 main variations of duel homed,for example:

some work with two routers at the customers home both connected to one ISP router,

others work with two ISP routers and one home connected router.

some work using ether-channels to add redundancy between the home router and the ISP router.

lastly one of the more secured ways of duel homed is two routers at home and in the ISP provider

**iii. Multihomed** multi homed redundancy works by adding a second ISP into the mix this allows for much greater redundancy as you have access to the internet through two different providers the advantage of this method is if one ISP network goes down in your area the other should still be up. the disadvantage of this method is you are paying twice over for ISP's.

**single Multihomed** in single multihomed the home connection has one router connected to two ISP's this means as long as one of either ISP's local network is up you will have internet access. the disadvantage of this method is only one customer router meaning if it breaks or goes down the internet is lost till replaced or back up and running.

another option for single multihomed to help reduce this weakness is to use two routers one at each ISP's provider and two at the customer/home connection this means if one router goes down on either side it will have no effect as the other connection will provide access to the network.

**duel Multihomed** a duel multihomed method works by not only being connected to two different ISP's bit by also redimdany links, this means if a connection on one link goes down the second link will take over, if the area network is down the second ISP will still provide network connectivity.

there are different variations of multihomed, for example:

using one customer routers and two different ISP routers, disadvantage if the customer router goes down the network connection is lost.

having two customer routers connected to two different ISP routers, the disadvantage here is that if a router goes down you loose access to one ISP till it is back up and running.

lastly the most secure and redundant method using two customer routers, two service providers, redundancy links and having each customer router connected to both ISP's. the method is the most secure when it comes to maintaining a network connection, the disadvantage of this method is the very high costs as you are paying two network providers for four connections at least.

[4] referenced types of multihomed

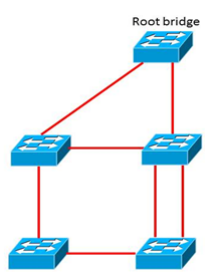
### 0.1.2 1b. Refer to Figure 1, identify RSTP port roles and explain them.

key:

rapid spanning tree (RSTP)

bridge protocol data unit (BPDU)

figure 1 below




there are four port roles to RSTP they are:

- root port.
- designated port.
- alternative port.
- backup port.

**key and description of roles** root port (RT). designated port (DP). alternative port (AP). backup port (BP).

the root port, is the port that gets the best BPDU's these are packets of information containing, ports, switches, port priorities, and lastly addresses. all

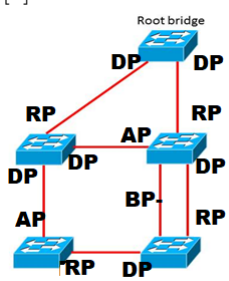
switches except the root bridge must at least one root port to receive BPDu packets to work out and update the best costs for talking to different routers.

the designated port , is the port that can send the BPDU received to the rest of the network this means all connections coming from a root bridge to a switch are a designated port and switches forwarding BPDU to another switch would also be a designated port.

the alternative port, works by blocking a port as they get better DPDU information from another of their connections, for example a switch connected to the root bridge would not accept BPDU from another switch.

the backup port, works by blocking a port as they get better DPDU information from either their own connections, for example a switch connected to the root bridge would not accept BPDU from itself switch from a backup route.

[3]




[1] used to reference labelling of diagram [2] used to work out what type each connection was

## 0.2 2

### 0.2.1 a. Explain the functionality of a Routed port and how it can be enabled on a Switch?

a routed port is a port with an IP address it is designed to forward layer 3 packets, it connects to another mutli-layers switch or router. [5]

it can be enabled by using the following commands from the CLI screen:

enter
conf t
int (g0/1) or (insert interface here no brackets )
no switchport
ip add (0.0.0.1 255.255.255.255) or (insert ip address and mask here no brackets)

[6]

### 0.2.2 b. Briefly explain OSPF packet types.

key:

Designated Router (DR)

link state advertisement (LSA's)

open shortest path first (OSPF)

- hello packet
- database description packet.
- link state update packet.
- link state request packet.
- link state acknowledgement packet.

hello packets are used to search for OSPF neighbours and establish communication with them, it will also establish a DR, the DR will be adjacent to all routers on the network, it will generate and broadcast the LSA's reducing network traffic generated, another function of the DR is to maintain and share the network topology database to all other routers using the same OSPF area's on the network.

database description packets are used to send database updates, this contains all link state information between adjacent partners who share it further. these packets are also used to maintain database content across all routers.

link state update packet. whilst the database is not fully synchronised to the network, routers send out link-state request and link state update packets. this works by sending messages beetween routers, database descriptions one connection at a time, the receiving router will acknowledge and then check if its a newer connection if it is it will be saved, the routers do this in order of highest router ID to lowest

link state request packet. when the descriptions are received the routers will then send out requests for more information about the routers, this will continue until the link-state databases are fully synchronised.

link state acknowledgement packet. each LSA packet received must be acknowledged to prove it has reached the intended destination, this is done by sending the link state acknowledgement packet, they will either be sent back

immediately or after a specified time interval.

[7]

### 0.2.3 c. With reference to EIGRP, explain the following

key:

enhanced interior gateway routing protocol (EIGRP)

**i. Fast convergence** IP fast convergence is all about trying to improve protocols to provide convergence within one second or better[8].
another type of convergence is to bundle network, telephone and multimedia onto a single network,this is included in EIGRP to provide consistent performance and to improve network security. [9]

**ii. Partial updates** this is also known as incremental updates, this is when instead of sending the entire database when one router destination changes the router will only send the changes not the entire table. this is how EIRGP does table updates

[10]

**iii. Multi network layer support** multi layer network support means that EIRGP supports both ip version 4(IPV4) and 6 (IPV6) and can work over both protocols.

**iv. Successor and feasible successor** EIRGP uses the successor and feasable successor to work out its network paths.
a successor is the best path with the least cost to reach a destination, this is stored in the routing table.
a feasible successor is the backup path to reach the same destination that is saved so that it can be used immediately if the successor path fails.

[11]

## 0.3 3

### 0.3.1 question

The University is planning on merging all its locations and bringing it under one network. You have been hired as an IT Infrastructure consultant by UWTSD.

Your task is to lead and work with the IT&S team to successfully complete this migration. The key objectives of this migration are design and implement:

- Secure scalable network
- Network management
- High Availability
- Support Digital Transformation

Your answer should include not only the technical aspects (LAN/WAN design, topology, architecture, choice of devices, redundancy, technologies, implementation, etc) addressing the key objectives but also the entire scope of the project. This should include planning, designing, project management, risk assessments, etc

### 0.3.2 answer

**Secure scalable network**

to make sure the network will always be scalable as needed EIRGP will be used as the main routing protocol, this allows for adding devices and not updating the entire table just appending the new information into the router table and sharing it with all routers on the network.

**Network management**

the network will be both managed campusly and overall, there will be two departments one will manage campus network activity blocking websites and such as needed, or getting the overall to if it is needed blocked completely, the reason for this is some areas of study will need access to materials others do not.

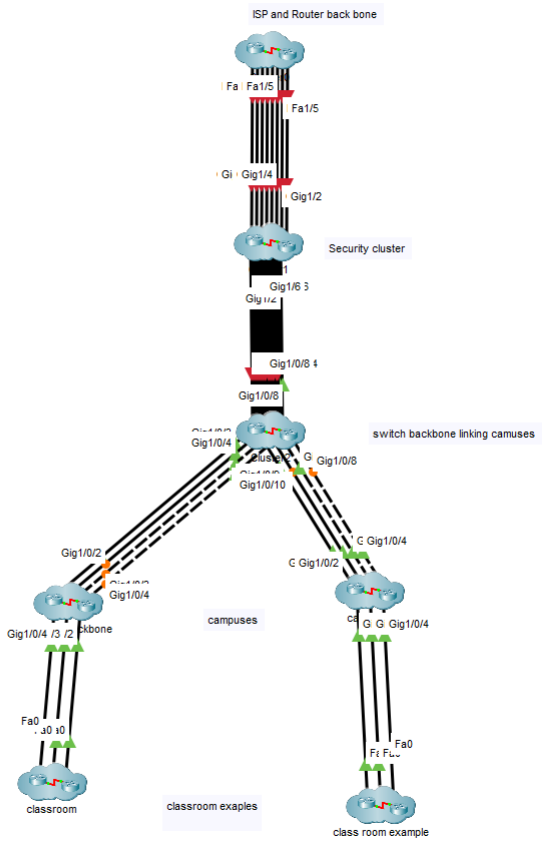
**High Availability**

to make sure there is high availability and that the network never goes down completely without multiple ISP's failing the plan is to use duel multihomed - the most secure and redundant method using two customer routers, two service providers, redundancy links and having each customer router connected to both ISP's.

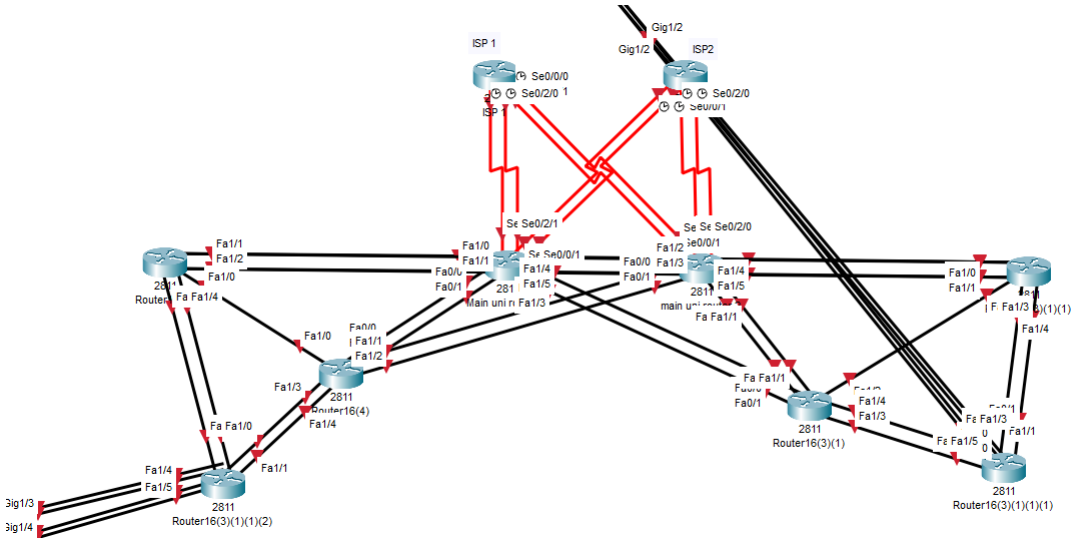
**lan and wan**

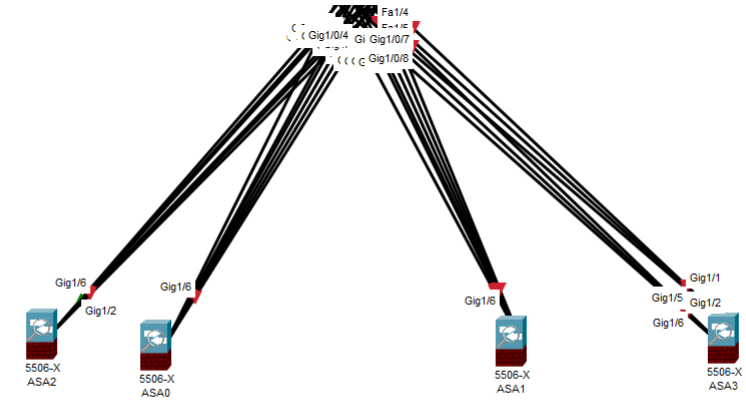
lan will be used in the local campus backbone , wan will be used connecting to the internet and other campuses

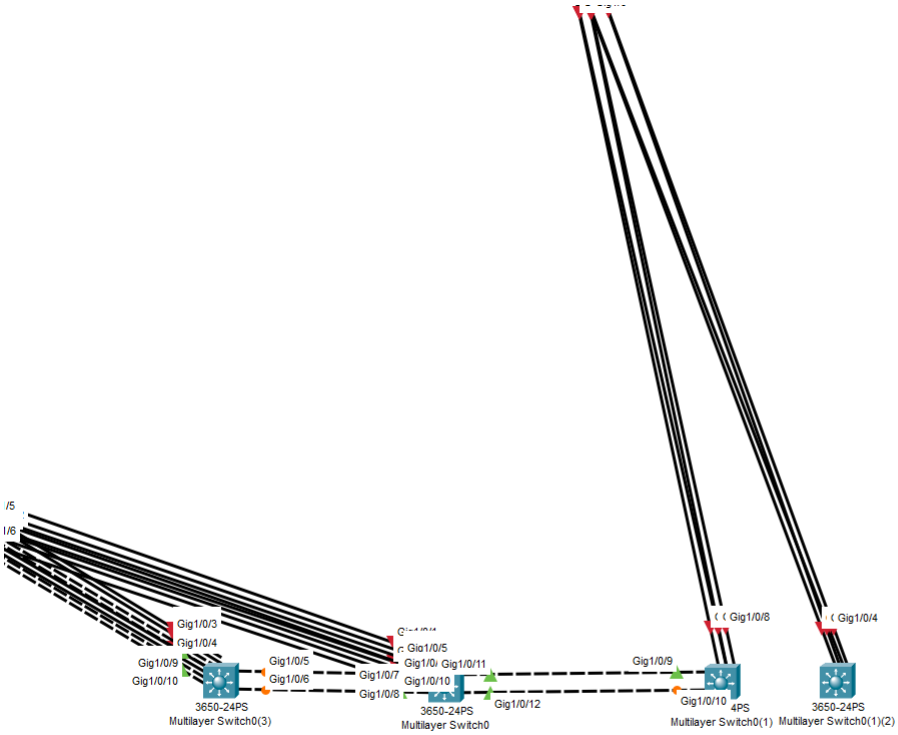
**topology**

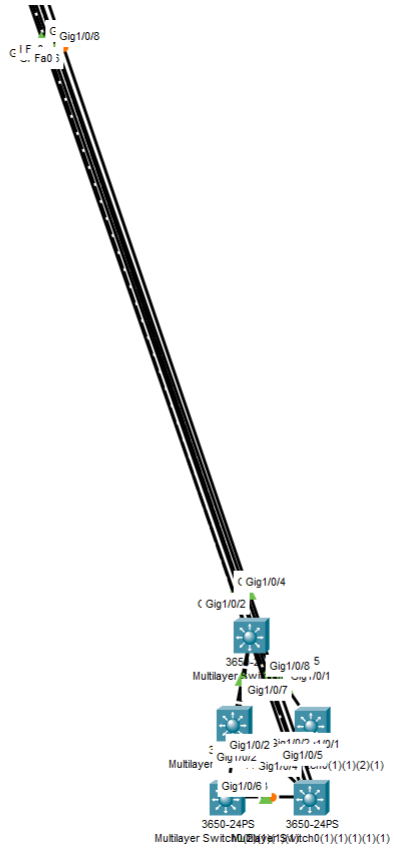


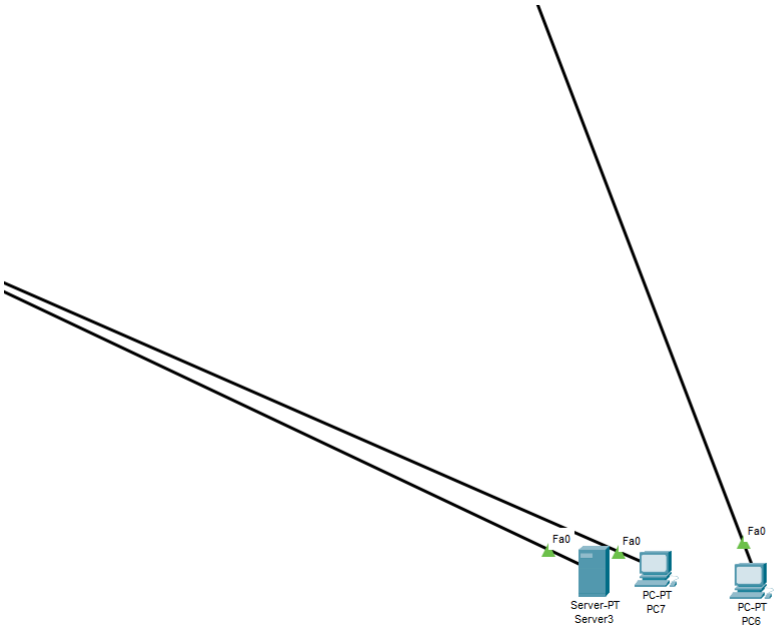

overall topology sub sections of topology


ISP 1
ISP2
Gig1/2
Gig1/2
Se0/0/0
Se0/2/0
Se0/2/0
Se0/2/1
Se0/2/0
Se0/0/1
Se0/0/1
Fa1/1
Fa1/2
Fa1/0
Fa Fa1/4
Fa1/0
Fa0/1
Fa1/1
Fa1/4
Fa1/5
Fa1/3
Fa0/0
Fa0/1
Fa1/3
Fa1/4
Fa1/5
Fa Fa1/1
Fa1/0
Fa1/1
Fa1/4
Fa1/0
Fa0/0
Fa1/1
Fa1/2
Fa1/3
2811
Router16(4)
Fa1/4
Fa Fa1/0
Fa1/1
Fa1/4
Fa1/5
2811
Router16(3)(1)(2)
Gig1/3
Gig1/4
Fa Fa1/1
Fa0/1
2811
Router16(3)(1)
Fa1/4
Fa1/3
Fa1/1
2811
Router16(3)(1)(1)(1)


Fa1/4
Gig1/0/4
Gig1/0/7
Gig1/0/8
Gig1/6
Gig1/2
5506-X
ASA2
Gig1/6
5506-X
ASA0
Gig1/6
5506-X
ASA1
Gig1/1
Gig1/5
Gig1/2
Gig1/6
5506-X
ASA3


Gig1/0/3
Gig1/0/4
Gig1/0/9
Gig1/0/10
3650-24PS
Multilayer Switch0(3)
Gig1/0/5
Gig1/0/6
Gig1/0/7
Gig1/0/8
Gig1/0/5
Gig1/0/11
Gig1/0/10
3650-24PS
Multilayer Switch0
Gig1/0/12
Gig1/0/9
Gig1/0/8
Gig1/0/10
4PS
Multilayer Switch0(1)
Gig1/0/4
3650-24PS
Multilayer Switch0(1)(2)


Gig1/0/8
Gig1/0/4
Gig1/0/2
Gig1/0/8
Gig1/0/7
Gig1/0/2
Gig1/0/5
Gig1/0/6
3650-24PS
3650-24PS




**choice of devices**

the reason for using routers for the first network is to make sure it is easy to expand with EIRGP, the reason for security is to make sure everything coming and and leaving the network is safe and approved, the reason for the large multilayer switches is so multiple campuses can be connected at once with redundancy, and lastly using multiple switches is to cover all the classrooms in the campus with all PCS,servers and other hardware needed.

**risk assessment**

the risk is someone getting into the network in an attempt to bypass security to help prevent this include firewalls, and extra security beetween all campuses.

## 0.4 references

using Texstudio please download pdf as links are inbuilt into references

[1]huawei RSTP Port Roles and Port States 2021 huawei
[2]cisco press STP fig 3-18 2017 cisco press

[3]cisco Understanding Rapid Spanning Tree Protocol (802.1w) August 1, 2017 cisco

[4]networklessons Single/Dual Homed and Multi-homed Designs 2013-2021 networklessons

[5]cisco netacad 1.1 Chapter Practice and Quiz 2021 cisco netacad

[6]cisco press IP Routing in the LAN 2020 cisco press

[7] IBM Packet types for OSPF 2021 IBM

[8] cisco IP Routing Fast Convergence 2012 cisco

[9] vmware What is Network Convergence? 2021 vmware

[10] cisco Cisco Catalyst Switch Module 3110 and 3012 for IBM BladeCenter Software Configuration Guide, Release 12.2(50)SE 2021 cisco

[11] studyccna EIGRP overview 2020 studyccna