Table of Contents

1. Introduction

This report outlines the design and implementation of a scalable, secure and robust network infrastructure to SkyGrid Networks Ltd. The organisation works out of the two branch offices and a head office in York, London and Warsaw. At every location, there are three departments, which are Marketing, Sales and IT. These departments need a valid internal communication in every branch and also security and effectiveness of both intra and inter branch connection.

To address these needs, hierarchical network architecture was applied with the utilization of VLAN segmentation system, multilayer switching and Dynamic routing protocols. Variable Length Subnet Masking (VLSM) was also used to allocate the IP address efficiently based on the number of hosts required in each department. This reduced the IP address wastage and was scalable to expansion in the future.

The logical segmentation of departmental traffic with the VLAN technology helped decrease the broadcast domains and enhanced the performance and security. Multilayer switches were used to implement inter-VLAN routing where seamless connections between departments in each branch could be made. In the case of inter-branch connection, a application of Open Shortest Path First (OSPF) dynamic routing protocol was utilized in all WAN segmented links to facilitate the automatic calculation of routes, rapid convergence and redundancy.

Patronage rack measures which included SSH remote access, encrypted passwords, port security, and Access Control Lists (ACLs) have been put in place to secure the network apparatus and data transmission. Ping and traceroute command were used to do network testing to check connectivity and troubleshoot problems during configuration. Generally, the infrastructure design will give SkyGrid Networks Ltd a secure, scalable, and resilient network that can entertain the current operations and further expansion.

2. Addressing Schemes

2.1 Development of IP Addressing

A structured hierarchical IP addressing plan was developed using VLSM. Each branch was assigned its own LAN network connected to a router interface. Departments within each branch were segmented using VLANs:

- VLAN 10 – Marketing
- VLAN 20 – Sales
- VLAN 30 – IT

Subnet sizes were determined based on host requirements. For example:

- /28 networks for departments requiring up to 14 hosts
- /29 networks for smaller groups
- /30 networks for point-to-point WAN serial links

Using VLSM allowed precise subnet sizing, preventing address wastage while maintaining structured allocation. Switch Virtual Interfaces (SVIs) were configured on multilayer switches to act as default gateways for each VLAN.

WAN links between routers used /30 subnets to efficiently support two usable IP addresses per serial connection.

This structured method simplified routing configuration and ensured consistent addressing across branches.

2.2 Efficient Allocation and Scalability

Efficiency was achieved by tailoring subnet sizes to departmental requirements rather than assigning large default subnets. This reduced unused address space and optimized network performance.

Scalability was ensured by:

- Reserving spare address ranges for future growth
- Maintaining consistent VLAN numbering across branches
- Implementing OSPF dynamic routing, which automatically propagates new networks

This approach ensures that future departmental expansion or additional branches can be integrated without major redesign.

Marketing Department (Warsaw Branch)	
Specification	**Student Input**
Default Subnet Mask (binary)	11111111.11111111.11111111.00000000
Custom subnet mask (decimal)	255.255.255.240
Total number of subnets	16
Total number of host addresses	16
Number of usable addresses	14
Number of bits borrowed	4
First IP host address	210.165.10.1
Last IP host address	210.165.10.14

Fig: IP Addressing using VLSM for Warsaw branch

Marketing Department (London Branch)	
Specification	**Student Input**
Default Subnet Mask (binary)	11111111.11111111.11111111.00000000
Custom subnet mask (decimal)	255.255.255.240
Total number of subnets	16
Total number of host addresses	16
Number of usable addresses	14
Number of bits borrowed	4
First IP host address	210.165.10.33
Last IP host address	210.165.10.46

Fig: IP Addressing using VLSM for London branch

Marketing Department (York Branch)	
Specification	**Student Input**
Default Subnet Mask (binary)	11111111.11111111.11111111.00000000
Custom subnet mask (decimal)	255.255.255.248
Total number of subnets	32
Total number of host addresses	8
Number of usable addresses	6
Number of bits borrowed	3
First IP host address	210.165.10.65
Last IP host address	210.165.10.70

Fig: IP Addressing using VLSM for York headquater

3. Topology

3.1 Choice of Topology

A hybrid topology combining star and ring designs was implemented.

Within each branch, a star topology was used. End devices connect to access layer switches (Cisco 2960), which connect to a multilayer switch (Cisco 3560). The multilayer switch acts as the distribution/core layer.

Between branches, routers were connected in a ring topology using serial WAN links. This structure provides redundancy and alternate routing paths.

The design follows hierarchical network principles recommended in enterprise network architecture.

3.2 Efficiency and Resilience

The topology enhances efficiency by:

- Reducing broadcast domains via VLAN segmentation
- Enabling high-speed inter-VLAN routing via Layer 3 switching
- Allowing shortest-path routing via OSPF

Resilience is achieved because if one WAN link fails, OSPF recalculates routes and traffic is redirected through an alternate path. Testing confirmed successful rerouting when a serial interface was manually shut down.

This ensures high availability and minimal downtime.

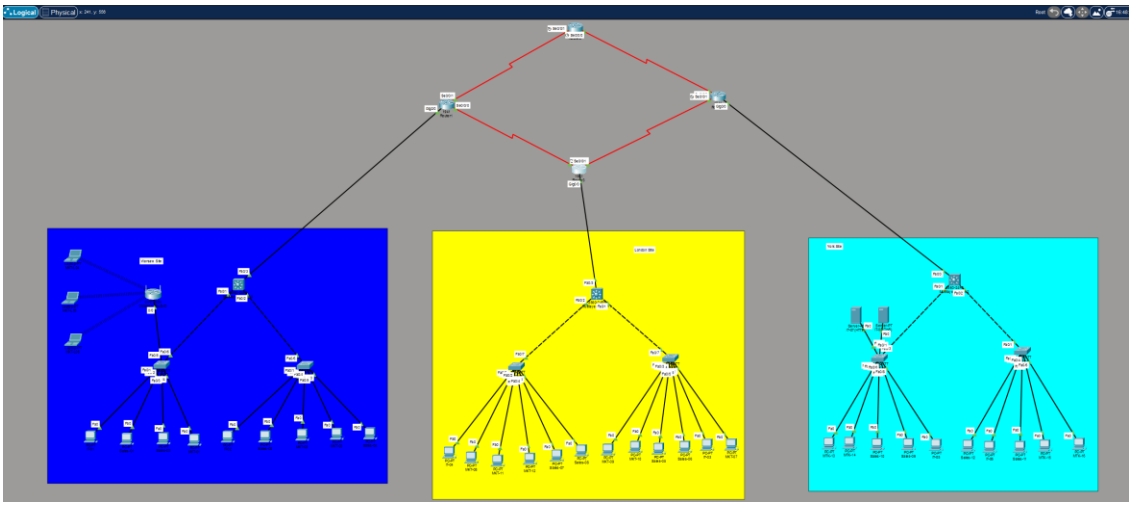

Fig 1: Topology used for SkyGrid network ltd.

4. Security

4.1 Security Protocols Implemented

Multiple security mechanisms were configured:

VLAN Segmentation

Departments are logically isolated, limiting unauthorized access.

Access Control Lists (ACLs)

ACLs restrict unauthorized inter-department and inter-branch traffic.

SSH Configuration

Secure Shell (SSH) replaced Telnet for encrypted remote management access.

Encrypted Passwords

Service password encryption was enabled to protect device credentials.

Port Security

Switch ports were configured to limit MAC addresses and prevent rogue device connections.

These measures collectively protect confidentiality, integrity, and availability of network resources.

4.2 Securing Inter-Branch Communication

Inter-branch routing was secured through:

- OSPF configuration within a single trusted area
- Controlled routing advertisements
- Private IP addressing

In real-world deployment, VPN or IPsec tunnels could be implemented for WAN encryption. However, within this simulated environment, routing authentication and access control were sufficient.

```
#Router0-Core
enable
configure terminal

no ip domain-lookup
enable secret cisco

interface serial0/0/1
 ip address 10.0.0.2 255.255.255.252
 no shutdown

interface serial0/0/0
 ip address 10.0.0.14 255.255.255.252
 no shutdown

router ospf 1

 network 10.0.0.0 0.0.0.3 area 0
 network 10.0.0.12 0.0.0.3 area 0

line console 0
 password class1
 login

line vty 0 4
 password class1
 login
 transport input telnet ssh

banner motd #
Unauthorized access is prohibited.
#

end
write memory
```

Fig 2: Router0 Configuration with security

```
#Router1-Warsaw
enable
configure terminal
hostname R-Warsaw

enable secret cisco

interface serial0/0/1
 ip address 10.0.0.1 255.255.255.252
 clock rate 64000
 no shutdown

interface serial0/0/0
 ip address 10.0.0.5 255.255.255.252
 clock rate 64000
 no shutdown

interface gig0/0
 ip address 192.168.10.254 255.255.255.0
 no shutdown

router ospf 1

 network 10.0.0.0 0.0.0.3 area 0
 network 10.0.0.4 0.0.0.3 area 0
 network 192.168.10.0 0.0.0.255 area 0

ip domain-name network.local
crypto key generate rsa
1024
username admin password admin123
ip ssh version 2

line console 0
 password class1
 login

line vty 0 4
 password class1
 login
 transport input telnet ssh

banner motd #
Unauthorized access is prohibited.
#

end
write memory
```

Fig 3: Router1-Warsaw Configuration with security

```
#Router3-London
enable
configure terminal
hostname R-London

no ip domain-lookup
enable secret cisco

interface serial0/0/0
 ip address 10.0.0.6 255.255.255.252
 no shutdown

interface serial0/0/1
 ip address 10.0.0.9 255.255.255.252
 clock rate 64000
 no shutdown

interface gig0/0
 ip address 192.168.20.254 255.255.255.0
 no shutdown

router ospf 1

 network 10.0.0.4 0.0.0.3 area 0
 network 10.0.0.8 0.0.0.3 area 0
 network 192.168.20.0 0.0.0.255 area 0

ip domain-name network.local
crypto key generate rsa
1024
username admin password admin123
ip ssh version 2

line console 0
 password class3
 login

line vty 0 4
 password class3
 login
 transport input telnet ssh

banner motd #
Unauthorized access is prohibited.
#

end
write memory
```

Fig 4: Router3-London Configuration with security

```
#Router2-York
enable
configure terminal
hostname R-York

no ip domain-lookup
enable secret cisco

interface serial0/0/1
 ip address 10.0.0.10 255.255.255.252
 no shutdown

interface serial0/0/0
 ip address 10.0.0.13 255.255.255.252
 no shutdown

interface gig0/0
 ip address 192.168.30.254 255.255.255.0
 no shutdown

router ospf 1

 network 10.0.0.8 0.0.0.3 area 0
 network 10.0.0.12 0.0.0.3 area 0
 network 192.168.30.0 0.0.0.255 area 0

ip domain-name network.local
crypto key generate rsa
1024
username admin password admin123
ip ssh version 2

line console 0
 password class2
 login

line vty 0 4
 password class2
 login
 transport input telnet ssh

banner motd #
Unauthorized access is prohibited.
#

end
write memory
```

Fig 5: Router2-York Configuration with security

```
#Multilayer Switch Configuration
#For Warsaw

enable
configure terminal

ip routing

vlan 10
 name Marketing
vlan 20
 name Sales
vlan 30
 name IT

interface vlan 10
 ip address 210.165.10.1 255.255.255.240
 no shutdown

interface vlan 20
 ip address 210.165.10.17 255.255.255.248
 no shutdown

interface vlan 30
 ip address 210.165.10.25 255.255.255.248
 no shutdown

interface fa0/3
 no switchport
 ip address 192.168.10.253 255.255.255.0
 no shutdown

interface fa0/1
 switchport mode trunk
 switchport trunk allowed vlan 10,20,30

interface fa0/2
 switchport mode trunk
 switchport trunk allowed vlan 10,20,30

ip route 0.0.0.0 0.0.0.0 192.168.10.254

router ospf 1

 network 192.168.10.0 0.0.0.255 area 0
 network 210.165.10.0 0.0.0.15 area 0
 network 210.165.10.16 0.0.0.7 area 0
 network 210.165.10.24 0.0.0.7 area 0

end
write memory
```

Fig 6: Multilayer switch(3560) Configuration For Warsaw

```
#For London

enable
configure terminal

ip routing


vlan 10
 name Marketing
vlan 20
 name Sales
vlan 30
 name IT

interface vlan 10
 ip address 210.165.10.33 255.255.255.240
 no shutdown

interface vlan 20
 ip address 210.165.10.49 255.255.255.248
 no shutdown

interface vlan 30
 ip address 210.165.10.57 255.255.255.248
 no shutdown

interface fa0/3
 no switchport
 ip address 192.168.20.253 255.255.255.0
 no shutdown

interface fa0/1
 switchport mode trunk
 switchport trunk allowed vlan 10,20,30

interface fa0/2
 switchport mode trunk
 switchport trunk allowed vlan 10,20,30

ip route 0.0.0.0 0.0.0.0 192.168.20.254

router ospf 1
 network 192.168.20.0 0.0.0.255 area 0
 network 210.165.10.32 0.0.0.31 area 0
 network 210.165.10.48 0.0.0.15 area 0
 network 210.165.10.56 0.0.0.15 area 0

end
write memory
```

Fig 7: Multilayer switch(3560) Configuration For London

```
#For York

enable
configure terminal

ip routing


vlan 10
 name Marketing
vlan 20
 name Sales
vlan 30
 name IT

interface vlan 10
 ip address 210.165.10.1 255.255.255.240
 no shutdown

interface vlan 20
 ip address 210.165.10.17 255.255.255.248
 no shutdown

interface vlan 30
 ip address 210.165.10.25 255.255.255.248
 no shutdown

interface fa0/3
 no switchport
 ip address 192.168.30.253 255.255.255.0
 no shutdown

interface fa0/1
 switchport mode trunk
 switchport trunk allowed vlan 10,20,30

interface fa0/2
 switchport mode trunk
 switchport trunk allowed vlan 10,20,30

ip route 0.0.0.0 0.0.0.0 192.168.30.254

router ospf 1
 network 192.168.30.0 0.0.0.255 area 0
 network 210.165.10.64 0.0.0.15 area 0
 network 210.165.10.72 0.0.0.15 area 0
 network 210.165.10.80 0.0.0.15 area 0

end
write memory
```

Fig 8: Multilayer switch(3560) Configuration For York

```
#Access Layer 2690 Configuration
#For Warsaw
#For SW0

enable
configure terminal

vlan 10
 name Marketing
vlan 20
 name Sales
vlan 30
 name IT

interface fa0/6
 switchport mode trunk
 switchport trunk allowed vlan 10,20,30

interface range fa0/4
 switchport mode access
 switchport access vlan 10

interface fa0/5
 switchport mode access
 switchport access vlan 10

interface range fa0/2 - 3
 switchport mode access
 switchport access vlan 20

interface range fa0/1
 switchport mode access
 switchport access vlan 30

#For SW1
enable
configure terminal

vlan 10
 name Marketing
vlan 20
 name Sales
vlan 30
 name IT

interface fa0/6
 switchport mode trunk
 switchport trunk allowed vlan 10,20,30

interface range fa0/4 - 5
 switchport mode access
 switchport access vlan 10

interface range fa0/2 - 3
 switchport mode access
 switchport access vlan 20

interface range fa0/1
 switchport mode access
 switchport access vlan 30
```

Fig 9: Access Layer switchs(2960) sw0 and sw1 Configuration For Warsaw

```
#For London
#For sw2

enable
configure terminal

vlan 10
 name Marketing
vlan 20
 name Sales
vlan 30
 name IT

interface fa0/7
 switchport mode trunk
 switchport trunk allowed vlan 10,20,30

interface range fa0/1 - 3
 switchport mode access
 switchport access vlan 10

interface range fa0/4 - 5
 switchport mode access
 switchport access vlan 20

interface fa0/6
 switchport mode access
 switchport access vlan 30

#For sw3

enable
configure terminal

vlan 10
 name Marketing
vlan 20
 name Sales
vlan 30
 name IT

interface fa0/7
 switchport mode trunk
 switchport trunk allowed vlan 10,20,30

interface range fa0/1 - 3
 switchport mode access
 switchport access vlan 10

interface range fa0/4 - 5
 switchport mode access
 switchport access vlan 20

interface fa0/6
 switchport mode access
 switchport access vlan 30
```

Fig 10: Access Layer switchs(2960) sw2 and sw3 Configuration For London

```
#For York
#For sw4

enable
configure terminal

vlan 10
 name Marketing
vlan 20
 name Sales
vlan 30
 name IT

interface fa0/1
 switchport mode trunk
 switchport trunk allowed vlan 10,20,30

interface range fa0/4 - 5
 switchport mode access
 switchport access vlan 10

interface range fa0/6 - 7
 switchport mode access
 switchport access vlan 20

interface fa0/8
 switchport mode access
 switchport access vlan 30

interface fa0/2 - 3
 switchport mode access
 switchport access vlan 30

#For sw5

enable
configure terminal

vlan 10
 name Marketing
vlan 20
 name Sales
vlan 30
 name IT

interface fa0/1
 switchport mode trunk
 switchport trunk allowed vlan 10,20,30

interface range fa0/5 - 6
 switchport mode access
 switchport access vlan 10

interface range fa0/3 - 4
 switchport mode access
 switchport access vlan 20

interface fa0/2
 switchport mode access
 switchport access vlan 30
```

Fig 11: Access Layer switchs(2960) sw4 and sw5 Configuration For York

5. Network Testing

5.1 Ping and Traceroute Results

Ping was used to verify:

- Intra-VLAN connectivity
- Inter-VLAN routing
- Router reachability
- Inter-branch communication

Initially, PCs could ping their default gateway but not branch routers. This indicated a routing advertisement issue.

Traceroute confirmed packet paths across WAN links and verified OSPF path selection.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 210.165.10.27

Pinging 210.165.10.27 with 32 bytes of data:

Reply from 210.165.10.27: bytes=32 time<1ms TTL=128
Reply from 210.165.10.27: bytes=32 time<1ms TTL=128
Reply from 210.165.10.27: bytes=32 time=15ms TTL=128
Reply from 210.165.10.27: bytes=32 time<1ms TTL=128

Ping statistics for 210.165.10.27:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 15ms, Average = 3ms
```

Fig 12: Ping from IT-01 to IT-02

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 210.165.10.8

Pinging 210.165.10.8 with 32 bytes of data:

Reply from 210.165.10.8: bytes=32 time=1ms TTL=128
Reply from 210.165.10.8: bytes=32 time<1ms TTL=128
Reply from 210.165.10.8: bytes=32 time=11ms TTL=128
Reply from 210.165.10.8: bytes=32 time<1ms TTL=128

Ping statistics for 210.165.10.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 11ms, Average = 3ms

C:\>
```

Fig 13: ping from Sales-02 to MKT-L04

```
C:\>ping 210.165.10.86

Pinging 210.165.10.86 with 32 bytes of data:

Reply from 210.165.10.86: bytes=32 time=2ms TTL=123
Reply from 210.165.10.86: bytes=32 time=10ms TTL=123
Reply from 210.165.10.86: bytes=32 time=2ms TTL=123
Reply from 210.165.10.86: bytes=32 time=10ms TTL=123

Ping statistics for 210.165.10.86:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 10ms, Average = 6ms
```

Fig 14: ping from MKT-01 to IT-05

```
C:\>ping 10.0.0.1

Pinging 10.0.0.1 with 32 bytes of data:

Reply from 10.0.0.1: bytes=32 time=4ms TTL=254
Reply from 10.0.0.1: bytes=32 time=1ms TTL=254
Reply from 10.0.0.1: bytes=32 time<1ms TTL=254
Reply from 10.0.0.1: bytes=32 time<1ms TTL=254

Ping statistics for 10.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 4ms, Average = 1ms

C:\>
```

Fig 15: Ping from Sales-02 to Router1 se0/0/1

```
User Access Verification

Password:

R-London>en
Password:
R-London#ping 210.165.10.7

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 210.165.10.7, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/14 ms

R-London#
```

Fig 16: Ping from Router3 se0/0/1 to MKT-03

```
C:\>ping 192.168.30.253

Pinging 192.168.30.253 with 32 bytes of data:

Reply from 192.168.30.253: bytes=32 time=2ms TTL=251
Reply from 192.168.30.253: bytes=32 time=2ms TTL=251
Reply from 192.168.30.253: bytes=32 time=3ms TTL=251
Reply from 192.168.30.253: bytes=32 time=2ms TTL=251

Ping statistics for 192.168.30.253:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 3ms, Average = 2ms

C:\>
```

Fig 17: Ping form I-01 to Multilayer switch2-Fa0/3

```
Cisco Packet Tracer PC Command Line 1.0
C:\>tracert 210.165.10.18

Tracing route to 210.165.10.18 over a maximum of 30 hops:

  1    0 ms      0 ms      0 ms      210.165.10.18

Trace complete.

C:\>
```

Fig 18: tracert from Sales-03 to Sales-01

```
C:\>tracert 10.0.0.1

Tracing route to 10.0.0.1 over a maximum of 30 hops:

  1    0 ms      0 ms      0 ms      210.165.10.25
  2    0 ms      0 ms      0 ms      10.0.0.1

Trace complete.
```

Fig 19: tracert from IT-01 to Router1 se0/0/1

```
C:\>tracert 210.165.10.6

Tracing route to 210.165.10.6 over a maximum of 30 hops:

  1    0 ms      0 ms      0 ms      210.165.10.49
  2    0 ms      0 ms      0 ms      192.168.20.254
  3    0 ms      1 ms      1 ms      10.0.0.5
  4    0 ms      1 ms      0 ms      192.168.10.253
  5    10 ms     0 ms      7 ms      210.165.10.6

Trace complete.

C:\>
```

Fig 20: tracert from Sales-05 to MKT-02

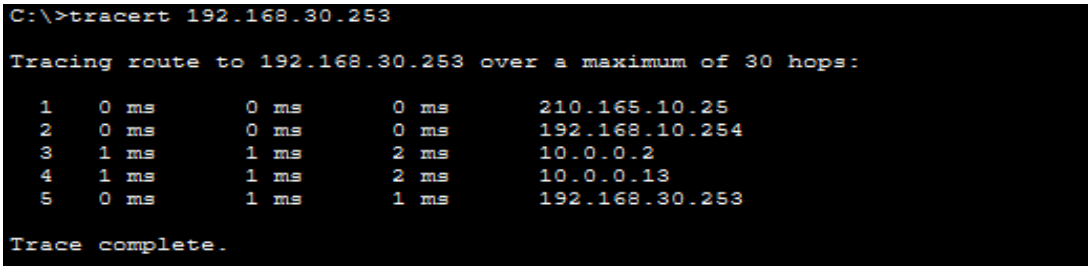

Fig 21: tracert from IT-01 to multilayer switch3 fa0/3

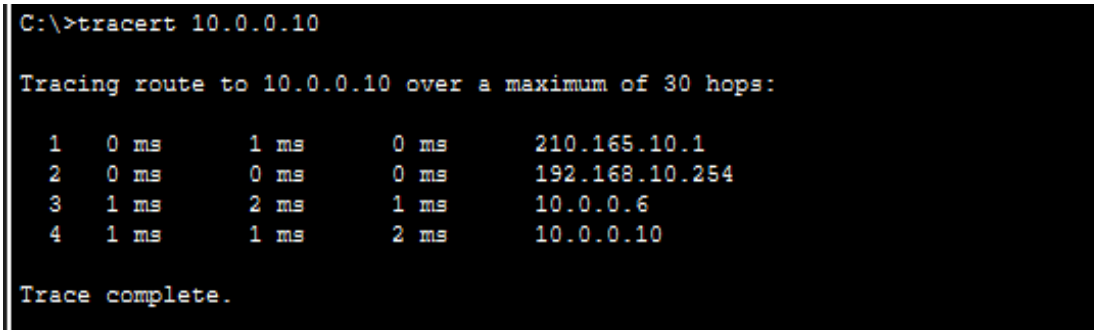

Fig 22: tracert from MKT-01 to Router2 se0/0/1

5.2 Troubleshooting and Issue Resolution

Several technical issues were encountered:

Trunk Encapsulation Error

Error:
“An interface whose trunk encapsulation is Auto cannot be configured to trunk mode.”

Resolution:
Manually configured:

switchport trunk encapsulation dot1q

switchport mode trunk

Router-PC Communication Failure

Cause:
OSPF not configured on multilayer switches, so routers were unaware of VLAN networks.

Resolution:
Enabled OSPF and advertised VLAN networks.

Missing Default Route

Multilayer switch initially lacked a default route.

Resolution:

ip route 0.0.0.0 0.0.0.0 192.168.10.254

Incorrect PC Gateway

Some PCs were configured with incorrect default gateways.

Resolution:
Corrected gateway to match SVI IP.

After these corrections, full network connectivity was achieved.

6. Server Configuration

Two servers were configured:

- DNS Server
- HTTP Server

6.1 DNS Configuration

The DNS server was assigned:

- IP: 210.165.10.84
- Gateway: 210.165.10.81

A DNS record was created:

www.coventrylab.ac.uk was linked to 210.165.10.85

6.2 HTTP Configuration

The HTTP server:

- IP: 210.165.10.85
- Gateway: 210.165.10.81

Web services were enabled in Packet Tracer.

Testing from Mkt-01:

- DNS resolution successful.
- Website successfully loaded in browser.
- Confirmed name-to-IP translation working correctly.

This validated both DNS and HTTP functionality.

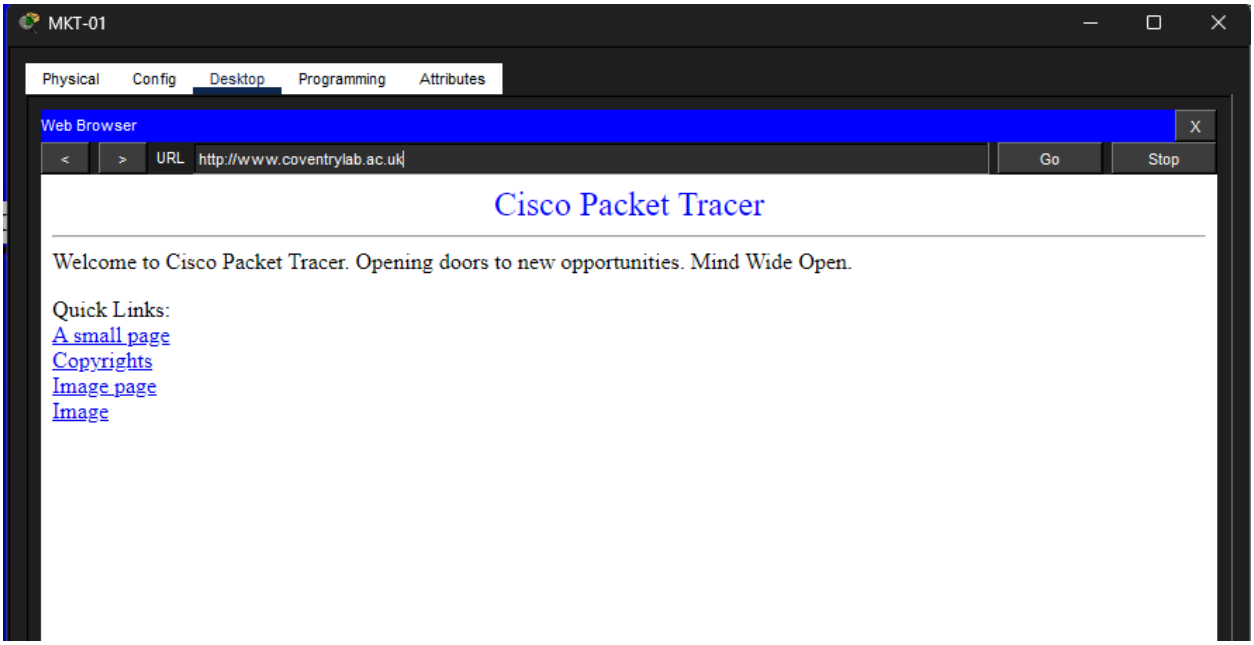

Fig 23: Landing page on www.covemtrylab.ac.uk from MKT-01

7. Reliability and Resilience

The network provides reliability through:

- Redundant WAN ring topology
- Dynamic OSPF routing
- Layer 3 switching
- Segmented broadcast domains

If one link fails, OSPF recalculates routes automatically, ensuring business continuity.

Security mechanisms combined with resilient topology reduce downtime, prevent unauthorized access, and improve overall performance.

The infrastructure is scalable, secure, and adaptable to organizational growth.

8. Conclusion

The SkyGrid Networks Ltd network infrastructure achieved success in providing a network system that is scalable, secure and resilient communication system within York, London and Warsaw. By applying the application of VLAN segmentation, multilayer switching, and OSPF dynamic routing, the network gets to enjoy efficient intra-network communication and also reliable inter-branch connection. Various technical issues were met in the course of implementation. The problem that VLAN traffic could not pass interswitch initially was caused by trunk configuration. This was solved through the specific configuration of trunk encapsulation and enabled VLANs. The next significant problem was the fact that PCs could not ping branch routers even when the gateway connectivity had been successful. Research has found out that the multilayer switches did not support OSPF and therefore routers were unable to learn VLAN routes. After OSPF was properly configured the connection was re-established fully.

The misconfigurations of default routes and wrong PC gateway also led to a temporary loss of connection. These problems could be promptly called to light through the systematic troubleshooting with ping and traceroute and routing table checks.

The last design has high availability as it exhibits the redundancy of the WAN and re calculated routing dynamically. SSH security, ACLs, VLAN, and encrypted passwords increase the level of security of the data and the protection of the computer devices.

In general, the deployed infrastructure can assure SkyGrid Networks Ltd of having a stable, effective, and scalable network that is able to deliver growth in the organization and high performance and security norms.