BS3204: DISTRIBUTED SYSTEM

TROUBLESHOOTING PLAN

Figure 1:Troubleshooting illustration(Signa Tech, 2024)

Table of Contents

Introduction

The following manual offers a methodical way to fix connectivity problems that impact website accessibility and business operations. It focusses on identifying and fixing issues without the need for new upgrades by making use of the current network infrastructure. Identifying important parts, evaluating tools, and carrying out methodical troubleshooting are important portions. The objective is to guarantee effective issue resolution while preserving business continuity and providing suggestions for continuing network upkeep and surveillance.

Case Study for Headquarters

A systematic troubleshooting procedure is used in this case study to address connectivity problems that affect the website and operations of the headquarters. The method finds weak spots and important network elements using the infrastructure that is in place now. In-depth troubleshooting procedures, tool analysis, and a conclusion with practical suggestions are all included. Proactive monitoring and maintenance are used in the process to restore dependable access, enhance performance, and guarantee long-term stability. (Zola & Kirvan 2022).

Identification of Critical Components

The primary network components that guarantee the accessibility of the headquarters website are the HQ Web Server, HQ Router, Switch A, DNS Server, Broadband Modem, and Internet Service Provider (ISP). Switch A, located within the headquarters' "HQ Server Farm" subnet, is directly connected to the HQ Web Server, the website's host. This switch controls packet delivery between the web server and other network components to guarantee effective data flow. All internal and external traffic must be directed through the headquarters router, which serves as the gateway. Internet communications and access to external websites require its fixed public IP address and default gateway issued by its ISP (Cisco, 2023). The broadband modem makes it easier for the headquarters to connect to the internet by connecting to the HQ Router and permitting access from the outside. Because it converts the website's domain name to its matching IP address, the DNS Server—usually operated by the ISP—is crucial to the website's accessibility and makes it simple for people to locate it (Lutkevich & Burke, 2021). These components work together to control traffic flow, preserve the website's functionality, and guarantee that users from both inside and outside the organisation may access it.

Key Network Components

Component	Role in connectivity	Potential issues
HQ Web server	Hosts the HQ website, serving web pages to clients. Located within the 'HQ Server Farm' subnet and connected to Switch A.	Server crashes, software bugs, insufficient resources (CPU, RAM), and security vulnerabilities (e.g., DDoS attacks).
HQ Router	Routes all internal and external network traffic. It has a fixed public IP and a default gateway provided by the ISP.	Misconfigured routes, IP conflicts, hardware failure, and firmware issues.
Switch A	Directly connected to the HQ Web Server, handles data packets between the server and other network components.	Switching loops, port failure, and VLAN misconfigurations
DNS Server	Resolves domain names to IP addresses, critical for clients to locate the HQ website via its domain.	DNS cache poisoning, incorrect DNS records, and server downtime.
Broadband Modem	Facilitates the internet connection to the HQ Router, enabling external access to the HQ Web Server.	Modem malfunctions, synchronization issues, and bandwidth limitations.
ISP	Provides broadband internet service and DNS hosting, essential for external accessibility of the HQ website.	Service outages, poor service quality, and latency issues.

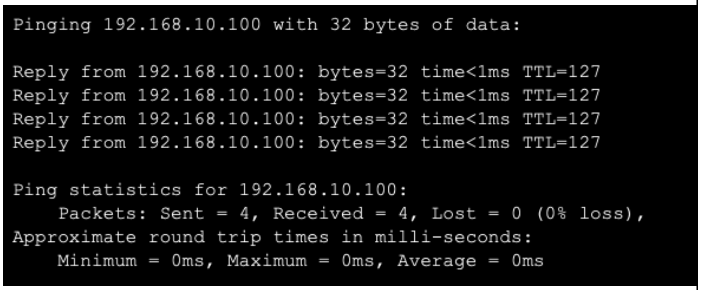
Table 1: Key Network Components

Troubleshooting steps

This section outlines an organised method for fixing intermittent problems with the main office website. The goal of each phase is to identify and address different network and system operational problems that could be influencing the accessibility of a website.

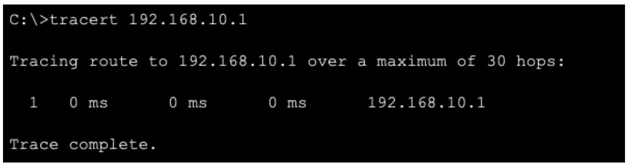
<table>
<tr><th>Step</th><th>Description + Execution Step</th><th>Outcome Analysis</th></tr>
<tr><td>1</td><td>The first step is to check network connectivity and ensure the headquarters website is accessible from various locations, both inside and outside the network. Use the ping command to test basic reachability and identify any immediate connection issues. Then, run traceroute to trace the data path to the website, helping to detect unavailable routes or high latency (Manthena, 2024).</td><td>

Ping Response:



```
Pinging 192.168.10.100 with 32 bytes of data:

Reply from 192.168.10.100: bytes=32 time<1ms TTL=127
Reply from 192.168.10.100: bytes=32 time<1ms TTL=127
Reply from 192.168.10.100: bytes=32 time<1ms TTL=127
Reply from 192.168.10.100: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.10.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

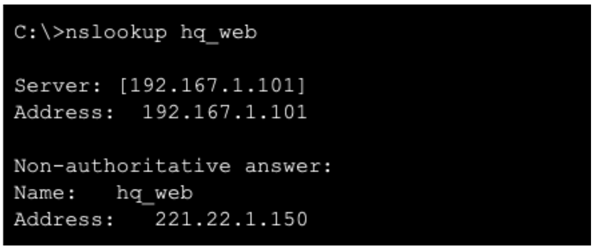
Traceroute Response:



```
C:\>tracert 192.168.10.1

Tracing route to 192.168.10.1 over a maximum of 30 hops:

  1   0 ms      0 ms      0 ms      192.168.10.1

Trace complete.
```

</td></tr>
<tr><td>2</td><td>The second step is to ensure that the DNS properly resolves the website's domain name to the correct IP address. Make that the domain name correctly points to the IP address of the HQ Web Server by using tools like nslookup or dig to query DNS records. This aids in identifying and averting DNS-related problems that can make the website unavailable (Sharma, 2024).</td><td>

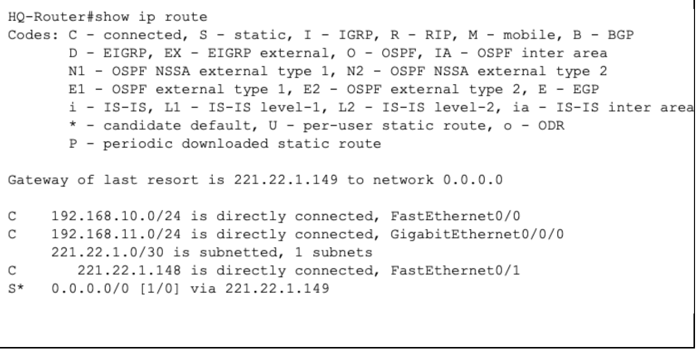
Nslookup response:



```
C:\>nslookup hq_web

Server:  [192.167.1.101]
Address:  192.167.1.101

Non-authoritative answer:
Name:   hq_web
Address:   221.22.1.150
```

</td></tr>
<tr><td>3</td><td>The third step is to review the network and switch configurations to ensure that traffic is properly routed to and from the headquarters web server. Examine route tables, NAT configurations, and access control lists (ACLs) through the router and switch management interfaces.</td><td>

Ip Route response:

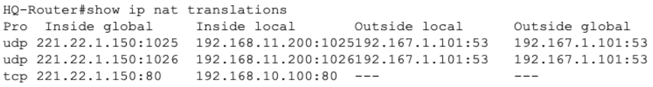


```
HQ-Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, 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 221.22.1.149 to network 0.0.0.0

C    192.168.10.0/24 is directly connected, FastEthernet0/0
C    192.168.11.0/24 is directly connected, GigabitEthernet0/0/0
     221.22.1.0/30 is subnetted, 1 subnets
C       221.22.1.148 is directly connected, FastEthernet0/1
S*   0.0.0.0/0 [1/0] via 221.22.1.149
```

</td></tr>
</table>

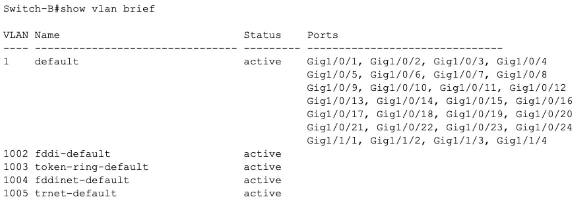
<table>
<tr>
<td></td>
<td>Identify and repair any setup problems, such as misconfigured VLANs or erroneous routing entries, that may impede data flow. (Dooley, 2023).</td>
<td>

Nat Translations response:



```
HQ-Router#show ip nat translations
Pro  Inside global      Inside local       Outside local      Outside global
udp 221.22.1.150:1025  192.168.11.200:1025192.167.1.101:53   192.167.1.101:53
udp 221.22.1.150:1026  192.168.11.200:1026192.167.1.101:53   192.167.1.101:53
tcp 221.22.1.150:80    192.168.10.100:80  ---                ---
```

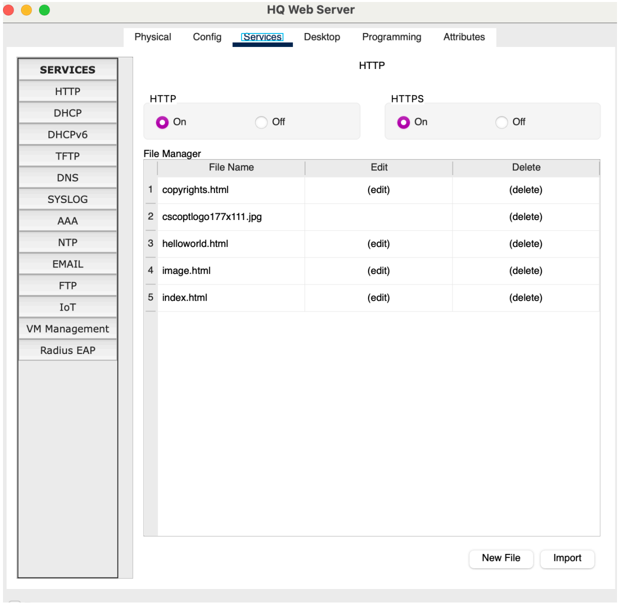
Vlan Brief response:



```
Switch-B#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gig1/0/1, Gig1/0/2, Gig1/0/3, Gig1/0/4
                                                Gig1/0/5, Gig1/0/6, Gig1/0/7, Gig1/0/8
                                                Gig1/0/9, Gig1/0/10, Gig1/0/11, Gig1/0/12
                                                Gig1/0/13, Gig1/0/14, Gig1/0/15, Gig1/0/16
                                                Gig1/0/17, Gig1/0/18, Gig1/0/19, Gig1/0/20
                                                Gig1/0/21, Gig1/0/22, Gig1/0/23, Gig1/0/24
                                                Gig1/1/1, Gig1/1/2, Gig1/1/3, Gig1/1/4
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

</td>
</tr>
<tr>
<td>4</td>
<td>The fourth stage is to evaluate the HQ Web Server's general health by looking at important performance parameters including CPU usage, RAM utilisation, disc space, and server load. Use server monitoring solutions that can provide both historical and real-time information. This guarantees that the server is working at peak efficiency and aids in the detection of potential problems, such as high CPU consumption or limited disc space, that could affect website performance (Barney, 2023).</td>
<td>

Web server:



HTTP

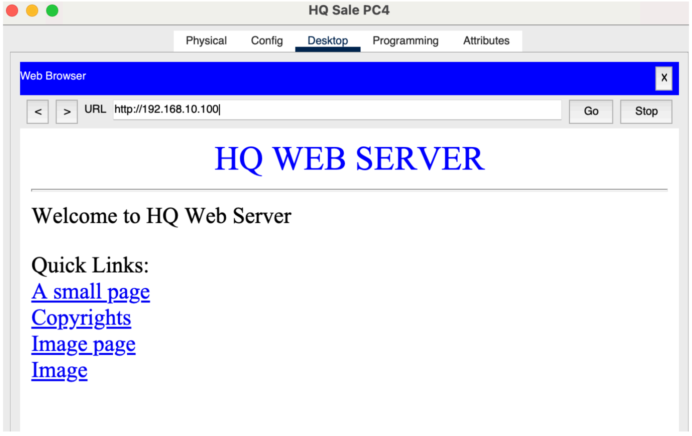
HTTP ● On ○ Off

HTTPS ● On ○ Off

File Manager

	File Name	Edit	Delete
1	copyrights.html	(edit)	(delete)
2	cscoptlogo177x111.jpg		(delete)
3	helloworld.html	(edit)	(delete)
4	image.html	(edit)	(delete)
5	index.html	(edit)	(delete)

Web Server Response:



URL http://192.168.10.100

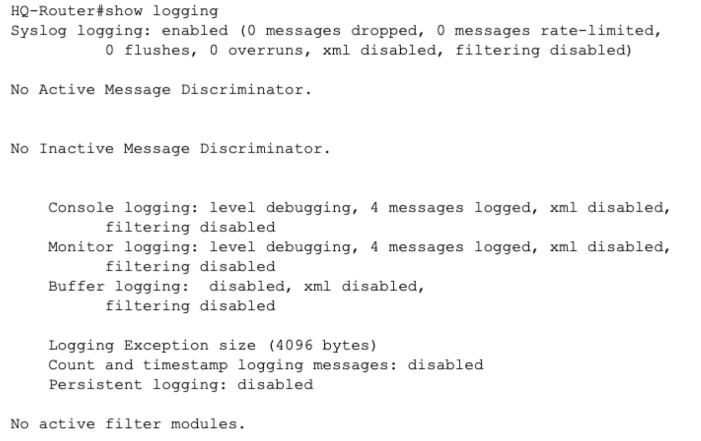
HQ WEB SERVER

Welcome to HQ Web Server

Quick Links:
A small page
Copyrights
Image page
Image

</td>
</tr>
<tr>
<td>5</td>
<td>The fifth stage involves reviewing logs from the server,</td>
<td>Logging Response:</td>
</tr>
</table>

<table>
<tr>
<td></td>
<td>firewall, and network devices with log analysis tools. After the website has been deemed inaccessible, this stage assists in determining potential causes by reviewing logs for mistakes or aberrant activity. Look for specific error messages or patterns that may indicate the underlying reason of the website's problems(Schiller et al. 2007)</td>
<td>



```
HQ-Router#show logging
Syslog logging: enabled (0 messages dropped, 0 messages rate-limited,
          0 flushes, 0 overruns, xml disabled, filtering disabled)

No Active Message Discriminator.


No Inactive Message Discriminator.


    Console logging: level debugging, 4 messages logged, xml disabled,
          filtering disabled
    Monitor logging: level debugging, 4 messages logged, xml disabled,
          filtering disabled
    Buffer logging:  disabled, xml disabled,
          filtering disabled

    Logging Exception size (4096 bytes)
    Count and timestamp logging messages: disabled
    Persistent logging: disabled

No active filter modules.
```

</td>
</tr>
</table>

Table 2: Troubleshooting Steps

Tools and Justification

The HQ website's intermittent accessibility problems are effectively troubleshooted using a range of specialised technologies. Every tool is chosen according to its distinct features and applicability to the previously mentioned troubleshooting procedures. The tools utilised, their functions, and the reasoning behind their selection are listed in the table below.

Network Diagnostic tools

Tool	Purpose	Justification
Ping	To check the basic reachability of the HQ website from various network points.	Simplicity and effectiveness in verifying network connectivity to a host.
Tracer Route	Maps the route data to the website, identifying where packets are being dropped or delayed	Essential for diagnosing path-related issues that could hinder website accessibility.
Nslookup	Queries DNS servers to ensure the website's domain name resolves to the correct IP address.	verifying and troubleshooting DNS resolution issues to ensure domain names are correctly linked to their respective IP addresses.
Dig	Performs more detailed DNS queries, providing comprehensive information about the DNS records.	Selected for its ability to offer detailed DNS diagnostics, which is crucial for identifying subtle DNS configuration errors.
Router and Switch management interfaces	Used to inspect and modify the configurations of routers and switches	Accessing and correcting settings that govern traffic flow and access rules, ensuring that network devices are correctly forwarding traffic.
Server monitoring tools	Monitor real-time performance and health metrics of the web server, such as CPU load, memory usage, and disk space.	Provides insights into server health and to detect performance issues before they impact website functionality.
Log Analysis Software	Analysis logs for errors or unusual activities during reported downtimes.	Historical data and logs to identify error patterns or specific incidents that correlate with website accessibility issues.

Table 3: Network Diagnostic Tools

Conclusion

The organised troubleshooting methodology described in this case study is intended to methodically address connectivity problems that impact the headquarters website. Utilising the current network infrastructure, the method finds important network elements, assesses possible vulnerabilities, and implements focused fixes without the need for additional improvements. To guarantee their best performance, the main components of the network—HQ Web Server, HQ Router, Switch A, DNS Server, Broadband Modem, and ISP—are assessed. The function of each component in connectivity is explained in detail, as are any possible problems that can affect performance.

Verifying network connectivity, making sure DNS resolution is correct, examining router and switch configurations, keeping an eye on server health, and looking for problem patterns in logs are all covered in the thorough, step-by-step troubleshooting process. At every step, necessary tools like ping, traceroute, nslookup, and server monitoring software are used, and their selection is justified.

Improved network dependability and successful restoration of website accessibility are the results of this strategy. To avoid such problems and ensure uninterrupted website availability, the case study suggests proactive server maintenance, frequent evaluations of DNS and network setups, and ongoing monitoring.

References

Barney, N. (2023) *What is real-time monitoring?: Definition from TechTarget, WhatIs*. Available at: https://www.techtarget.com/whatis/definition/real-time-monitoring (Accessed: 10 December 2024).

Cisco (2023) *Configure a gateway of last resort that uses IP commands*. Available at: https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/16448-default.html (Accessed: 12 December 2024).

Dooley, K. (2023) *How to troubleshoot routing problems, Auvik*. Available at: https://www.auvik.com/franklyit/blog/how-to-troubleshoot-routing-problems/ (Accessed: 14 December 2024).

Garn, D. (2024) *DNS security best practices to implement now: TechTarget, Search Security*. Available at: https://www.techtarget.com/searchsecurity/tip/DNS-security-best-practices-to-implement-now (Accessed: 12 December 2024).

Kirvan, P. and Zola, A. (2022) *What is troubleshooting and why is it important?, WhatIs*. Available at: https://www.techtarget.com/whatis/definition/troubleshooting (Accessed: 16 December 2024).

Lutkevich, B. and Burke, J. (2021) *What is DNS? How domain name system works, Search Networking*. Available at: https://www.techtarget.com/searchnetworking/definition/domain-name-system (Accessed: 12 December 2024).

Manthena, C.V. (2024a) *Diagnose network issues like a pro using Ping, Traceroute, and MTR*, *Medium*. Available at: https://medium.com/itversity/diagnose-network-issues-like-a-pro-using-ping-traceroute-and-mtr-1699b04feab4(Accessed: 12 December 2024).

Signa Tech (2024) Managed IT Services - Signa Tech: Wisconsin*. Available at: https://signatech.com/services/remote-infrastructure-management-rim/ (Accessed: 18 January 2025).*

Schiller, C.A., Binkley, J., Harley, D., Evron, G., Bradley, T., Willems, C. and Cross, M. (2007) *Botnet Detection: Tools and Techniques*, *Botnets*, pp. 133–215. Available at: https://doi.org/10.1016/B978-159749135-8/50007-X(Accessed: 12 December 2024).

Sharma, H. (2024) *What is DNS lookup and how does it work*, *Mailmodo*. Available at: https://www.mailmodo.com/guides/dns-lookup/ (Accessed: 19 December 2024).