REPORT
DNS Outage and Port 53 Failure Analysis

v1.0.1

Author:

Eldon Gabriel

June 12, 2025

TABLE OF CONTENTS

REVISION HISTORY

Version	Date	Author	Description of Changes
v1.0.0	02/15/2025	Eldon G.	Initial draft.
v1.0.1	06/12/2025	Eldon G.	Added section numbering and conclusion.

SECTION 1.0: DNS FAILURE INVESTIGATION

1.1 Scenario Summary

A disruption in DNS services rendered the company's website, www.yummyrecipesforme.com, inaccessible. Multiple customers reported receiving a **"destination port unreachable"** error. Investigation revealed that the DNS server at IP address `203.0.113.2` was unresponsive on **UDP port 53**, preventing DNS resolution for the domain.

1.2 DNS and ICMP Traffic Analysis

Using packet capture tools such as **tcpdump**, I observed that DNS queries sent over UDP failed to receive a response. Instead, **ICMP messages** returned the error:

```
"udp port 53 unreachable"
```

This confirms that the DNS server was not actively listening on port 53 or had gone offline. Without a response to DNS queries, the browser could not retrieve the **A record** for the domain, halting the resolution process.

1.3 Root Cause Analysis

- **Incident Timestamp:** 13:24:32.192571
- **Issue Confirmed**: DNS server at `203.0.113.2` did not respond to queries on UDP port 53
- **Error Observed:** Repeated ICMP "port unreachable" messages
- **Impact:** The domain www.yummyrecipesforme.com could not be resolved; the website was inaccessible
- **Likely Cause:** Server misconfiguration, offline state, or service crash on port 53

Packet logs showed that all DNS query attempts failed consistently over time, suggesting a persistent outage or misconfiguration.

SECTION 2.0: CONCLUSION

2.1 Key Takeaways

- The DNS failure was caused by an unresponsive or offline DNS server at IP address `203.0.113.2`.
- The failure to respond on **UDP port 53** prevented the resolution of the **A record** for the company's domain.
- The root cause appears to be either server misconfiguration, service outage, or port closure.

2.2 Security Implications and Recommendations

To prevent similar incidents in the future, I recommend the following actions:

✅ **Monitor DNS Services**: Implement real-time health monitoring for all DNS services and ports.

✅ **Deploy Secondary DNS Servers**: Always configure redundant DNS servers to handle queries if the primary server fails.

✅ **Ensure Port Availability**: Regularly test that UDP port 53 is open and responsive with tools like `nmap` or `dig`.

✅ **Log and Alert on ICMP Errors**: Monitor ICMP traffic for signs of DNS or port failures.

✅ **Automate Service Restart Policies**: If DNS services fail, auto-recovery mechanisms should attempt restarts immediately.

Implementing these recommendations will enhance DNS reliability and ensure business continuity for public-facing web services.