Post-Mortem Incident Report: TCP DF Flag Issue

Incident Overview

- **Date**: September 7, 2024
- **Time**: 10:00 AM UTC
- **Incident Title**: Network Communication Failure due to TCP DF Flag
- **Affected Systems**: Internal application servers, VPN network
- **Impact**: Network outage for 500 users, intermittent service failures for critical applications

---

Incident Summary

On September 7, 2024, at approximately 10:00 AM UTC, a network communication failure occurred due to improper handling of the **Don't Fragment (DF)** flag in TCP headers. The DF flag prevented packet fragmentation, causing network communication failures across VPN-connected systems. The result was dropped packets, high latency, and complete loss of service for 500 users attempting to access critical applications.

The issue was traced to oversized packets that exceeded the **Maximum Transmission Unit (MTU)** and were unable to fragment due to the DF flag being set, ultimately resulting in packet loss and system downtime.

Timeline of Events

Time (UTC)	Event Description
10:00 AM	Internal monitoring system reports packet drops and latency spikes on VPN connections.
10:05 AM	Network operations team investigates potential VPN configuration errors.
10:20 AM	User reports indicate widespread connection issues for services using VPN tunneling.
10:30 AM	Diagnostic tools show packet loss; packet capture reveals DF flag set on fragmented packets.
11:00 AM	Network team adjusts MTU settings and disables DF flag on impacted servers.
11:30 AM	Packet loss mitigated; network traffic normalizes.
12:00 PM	Network services fully restored, and all impacted systems are operational.

Root Cause Analysis

The root cause was the **TCP DF flag**, which prevented packet fragmentation. When data packets exceeded the network's MTU, the DF flag caused intermediate devices to drop oversized packets instead of fragmenting them. The issue was aggravated by VPN tunnel overhead, which further increased packet size, leading to more frequent packet drops.

Impact

- **500 users** experienced service interruptions and complete network outage between 10:00 AM and 12:00 PM.
- **Critical applications** relying on VPN were offline for two hours, including [specific applications].
- Loss of productivity for internal teams due to lack of access to the VPN and essential services.

Resolution

1. **MTU Adjustment**: Network MTU was reduced to handle packet size without triggering fragmentation.
2. **Disable DF Flag**: TCP DF flag was disabled on critical servers to allow packet fragmentation.
3. **Testing**: Tests confirmed packet transmission stability after changes were applied.
4. **Monitoring**: Continuous monitoring was implemented to prevent similar issues.

How to fix

Run the command below to allow ICMP packages on the firewall, thus even if the MTU is higher then 1500, the DF flag can split the package and send it normally.

```
sudo iptables -A INPUT -p icmp -j ACCEPT
sudo iptables -A OUTPUT -p icmp -j ACCEPT
```

Preventative Actions

1. **Network MTU Audit**: Review and standardize MTU settings across all systems and VPN configurations.
2. **Enhanced Packet Monitoring**: Implement alerts for packet loss related to DF flags.
3. **Regular Testing**: Conduct routine tests to ensure proper handling of TCP headers and fragmentation across the network.

Conclusion

The issue was caused by the TCP DF flag preventing packet fragmentation, resulting in dropped packets and network outages. Adjusting MTU settings and disabling the DF flag resolved the issue. Moving forward, we will implement additional monitoring and standardization to prevent recurrence.
