Case Study: Nationwide Bank's Intermittent Transaction Failures

Organization:

A large retail bank in the United States with over 500 branches and an internal core banking application hosted in their central data center.

Problem:

Customers and bank tellers were intermittently unable to complete transactions, especially during peak hours. The core banking application would freeze or return timeout errors.

Initial Troubleshooting Steps:

- Application logs showed generic timeouts but no detailed root cause.
- CPU, memory, and disk on the servers were all well within operational limits.
- Network utilization appeared normal at a high level (SNMP, NetFlow).
- Firewall logs showed no dropped packets.

With no clear indicators, packet capture and deep packet inspection were brought in.

Packet Analysis Strategy:

- SPAN (port mirroring) set up on key data center switches.
- Used Wireshark and tcpdump.
- Captured traffic during peak and off-peak hours.

Key Findings from Packet Analysis:

- TCP retransmissions and duplicate ACKs.
- Window size scaling issues.
- Sporadic latency spikes over 800ms between app servers and DB.

Root Cause:

- Some packets routed through a failing Layer 3 switch.
- Interface flapping causing asymmetric routing and packet drops.
- Standard network monitoring didn't catch the degraded link.

Resolution:

- Replaced the faulty switch.

- Adjusted routing.

- Improved network monitoring.

Outcome:

- Transaction failures dropped to zero.

- Core banking performance stabilized.

- Packet analysis adopted as standard response practice.

Lessons Learned:

- Traditional monitoring misses micro-level issues.

- Packet analysis provided root cause visibility.

- Asymmetric routing can cause major issues.

Tools Used:

- Wireshark

- tcpdump

- Riverbed SteelCentral

- Network TAPs and SPAN ports