

# Manage Network Traffic – Network 1

## Introduction

### Explanation of Network Congestion

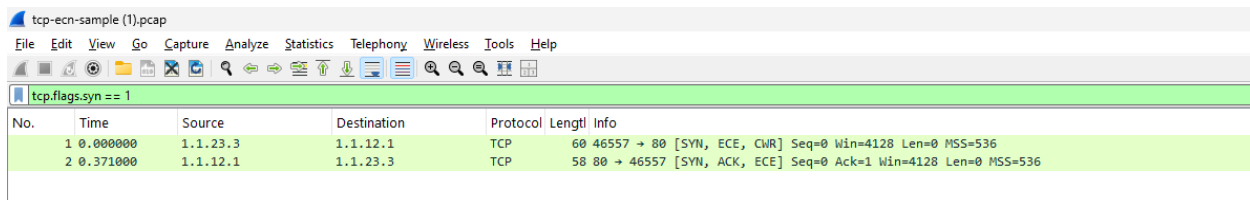
Network congestion is a state where the volume of data traffic on a network exceeds its capacity, leading to degraded performance. This can manifest as increased delays, packet loss, reduced throughput, or jitter, significantly impacting the quality of communication. In modern networks, congestion often arises from a mismatch between high traffic demand and limited resources such as bandwidth or processing power in routers and switches. To address this issue, transport protocols like TCP incorporate congestion control mechanisms. One of these mechanisms is Explicit Congestion Notification (ECN), which allows routers to signal congestion to endpoints without dropping packets, promoting efficient traffic flow and reducing retransmissions.

### What You Are Going to Do in This Task

Introduction well provided, where the intention of the report is clearly stated.

In this task, we will analyze the provided packet capture file (tcp-ecn-sample.pcap) to examine how TCP handles congestion, focusing on the behavior of ECN during the connection lifecycle. The analysis will cover the TCP three-way handshake, the data exchange phase, and the connection termination. We will evaluate key network performance metrics such as latency, jitter, and packet loss, identify any potential issues, and propose recommendations to optimize traffic flow. Additionally, we will develop strategies for traffic control and provide insights into future capacity planning to mitigate congestion effectively.

### Handshake



The image shows a Wireshark packet capture window titled 'tcp-ecn-sample (1).pcap'. The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help) and a toolbar. The packet list pane on the left shows two packets. The packet details pane on the right shows the selected packet's structure.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	1.1.23.3	1.1.12.1	TCP	60	46557 → 80 [SYN, ECE, CWR] Seq=0 Win=4128 Len=0 MSS=536
2	0.371000	1.1.12.1	1.1.23.3	TCP	58	80 → 46557 [SYN, ACK, ECE] Seq=0 Ack=1 Win=4128 Len=0 MSS=536

The TCP handshake is successfully established between the client (1.1.23.3) and the server (1.1.12.1). In Frame 1, the client initiates the connection with a SYN packet, setting the ECE and CWR flags to indicate ECN capability. The server responds in Frame 2 with a SYN-ACK, echoing the ECE flag to confirm support for ECN. This negotiation ensures that both endpoints will use ECN to handle congestion during communication.

[TCP three-way handshake well explained, where correct screenshot is provided.](#)

## TRAFFIC CONTROL FLOW

### Implicit Control

**NYS - The analysis is incomplete - please attach the screenshots and explanation of the ECN and TCP four-way handshake protocol. - JG**

Implicit control mechanisms

notifications. Examples include:

- Congestion Avoidance: TCP detects packet loss as a sign of congestion and reduces the transmission rate by halving the congestion window (CWND).
- Slow Start: Upon connection establishment or after packet loss, TCP starts with a small CWND and gradually increases it to probe the network capacity.
- Retransmission Timeout (RTO): TCP waits for a specific duration before retransmitting lost packets, which prevents further congestion.

### Explicit Control

Explicit control mechanisms, such as Explicit Congestion Notification (ECN), provide feedback without relying on packet loss:

- ECN-capable routers mark packets with the Congestion Experienced (CE) flag in the IP header when congestion is detected.
- Receivers notify senders using the ECN-Echo (ECE) flag in the TCP header, prompting senders to reduce their CWND.
- The Congestion Window Reduced (CWR) flag from the sender confirms its response to congestion.

IDENTIFYING PROBLEMS AND RECOMMENDATIONS

Problem	Description	Recommendation
Latency	Delays between packet transmissions, often caused by congestion or routing inefficiencies.	- Optimize routing paths.
		- Minimize hop counts.
		- Increase bandwidth to reduce delays.
Jitter	Variations in packet delay, affecting real-time applications like VoIP and streaming.	- Deploy QoS to prioritize real-time traffic.
		- Stabilize inter-packet delivery times.
Packet Loss	Packets dropped due to congestion or faulty network links, leading to retransmissions.	- Enable ECN to prevent packet drops.
		- Ensure proper router buffer configurations.
Throughput	Low data transfer rates, often caused by insufficient bandwidth or congestion.	- Use TCP window scaling to optimize data transfer.
		- Upgrade links to support higher bandwidth.
Packet Duplication	Duplicate packets caused by retransmissions or routing loops, wasting network bandwidth.	- Check for routing misconfigurations.
		- Ensure consistent routing paths.
Packet Reordering	Packets arriving out of order, disrupting applications requiring sequential delivery.	- Adjust network paths for consistency.
		- Enable TCP reordering mechanisms.

CAPACITY PLANNING

Aspect	Details
Future Capacity Requirements	Based on current network usage and trends, capacity upgrades should be planned to handle 25-50% more traffic to account for growth and peak demands.
Bandwidth Scaling	Increase current bandwidth (e.g., from 1 Gbps to 10 Gbps) to accommodate rising data volumes and ensure smooth performance during peak loads.
Device Upgrades	Upgrade networking devices like routers and switches to support higher data rates, ECN, and other modern congestion control features.
Segmentation	Use VLANs to separate high-priority traffic (e.g., VoIP and video) from regular traffic to reduce congestion in critical applications.
Monitoring Tools	Deploy real-time monitoring tools to proactively detect traffic bottlenecks and adjust resource allocations before issues arise.
Cloud and Scalability	Migrate non-critical traffic or storage workloads to cloud platforms to reduce strain on on-premises resources and scale dynamically as needed.

## **CONCLUSION**

This analysis addressed network issues such as latency, jitter, packet loss, and congestion. The problems were identified through packet capture analysis, which revealed congestion signals, inefficient traffic flow, and outdated device limitations. The troubleshooting process included examining the TCP handshake and communication phases, diagnosing bottlenecks, and detecting retransmissions. To resolve these issues, ECN was enabled to manage congestion effectively, QoS policies were applied to prioritize critical traffic, and bandwidth upgrades were recommended to accommodate increased demand. These actions, along with traffic segmentation and proactive monitoring, ensure improved network performance and scalability to handle future growth.