INTERNET METROLOGY PROJECT

Analysis of LinkedIn Network Performance

Abstract

This report examines `linkedin.com` network performance across different access networks. Using `ping`, `MTR`, `traceroute`, `whois`, and `dig`, we evaluated latency and connectivity. Results show local connections have lower latency, while intermediate routers and cloud infrastructure block many probes, limiting full Internet mapping.

1 Introduction

The performance of the vast, dynamic Internet is dictated by its interconnected networks and routing. Internet metrology aims to understand and measure how data travels across this system.

This project analyzes connectivity to LinkedIn.com, one of the world's largest professional networking platforms. The study focuses on routing, latency, and connectivity variations across different access networks, times of day, and geographic locations.

2 Methodology

To study LinkedIn's network performance, the following setup was used:

- Access Networks: Local Wi-Fi (INSA LYON), 5G hotspot, VPN for remote access.
- Tools: `ping`, `MTR`, `traceroute`, `whois`, `dig`, Wireshark.
- Temporal Variation: Tests at different times to observe latency and routing changes.
- Data Collected: Latency, hop-by-hop paths, packet loss.

This setup allows comparison across networks and highlights how routing and access type affect performance.

2.1 Domain Information Collection

Before conducting latency and routing measurements, domain information was collected using WHOIS and DIG commands to identify LinkedIn's registrar, DNS configuration, and authoritative name servers. The detailed outputs of these commands are provided in Appendix A — Domain Information.

3 Results

This section presents the results of the measurements, focusing on three main aspects of LinkedIn's network behavior: latency, routing paths, and regional performance differences. Each subsection addresses one of these aspects.

3.1 Latency Analysis

Latency, or round-trip time, measures how long it takes for a packet to travel from the source to the destination and back. To evaluate LinkedIn's network performance, `ping` measurements were collected from three types of access networks: INSA WI-FI, a 5G hotspot, and a VPN simulating access from the USA.

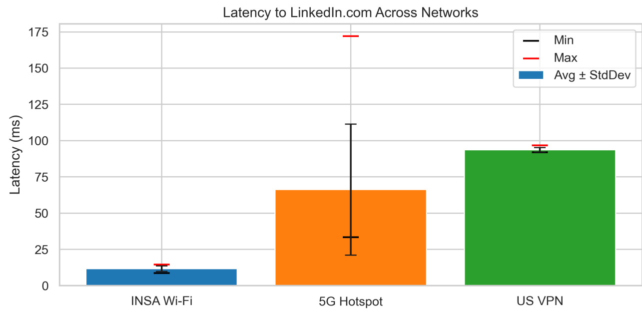

Figure 1: Latency to LinkedIn.com across networks.

Figure 1 presents the results. The bars show the average latency for each network, with error bars representing the standard deviation, while the markers indicate the minimum (black) and maximum (red) observed latency values. As seen in the figure, INSA WI-FI provides the lowest and most stable latency, the 5G hotspot shows higher and more variable latency, and the US VPN has the highest latency with relatively low variability. This visualization highlights the impact of network type and geographic distance on LinkedIn's performance.

Overall, these results confirm that both network type and geographic proximity significantly affect LinkedIn's responsiveness, with local connections achieving the best performance.

3.2 Routing Path Analysis

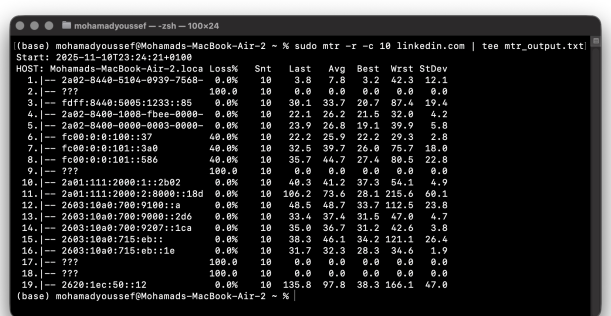

Figure 2: Terminal output of MTR from a 5G connection to linkedin.com

To understand the routing paths from a 5G network to LinkedIn, MTR was used to measure hop-by-hop latency and packet loss, as shown in Figure 2. Unlike standard `traceroute`, `mtr` combines `ping` and `traceroute` functionality, providing both latency and packet loss statistics for each intermediate router along the path. These measurements are critical for evaluating end-to-end performance and understanding how different network types affect connectivity.

This MTR report shows the route taken by packets from a 5G mobile network to LinkedIn over IPv6. The path includes 19 hops in total. Some routers, especially between hops 7–9 and 17–18, show 100% packet loss, which usually happens because certain routers do not answer ICMP messages. Despite this, the last hop (hop 19) successfully reaches LinkedIn's IPV6 server (`2620:1ec:50::12`), which means the connection works correctly. The average latency is around 30 ms, showing a stable connection typical of 5G networks. The route probably goes through several ISP and MICROSOFT AZURE routers, which is consistent with the authoritative DNS servers listed in Appendix A — Domain Information.

Compared to local WI-FI or VPN connections, the 5G network shows slightly higher average latency and more variability, reflecting typical mobile network characteristics, such as dynamic routing and varying link quality. The measured path traverses 19 hops, indicating that network distance and intermediate routing can significantly affect round-trip time.

Overall, this routing analysis demonstrates that packets reliably reach LinkedIn's servers, but network type and path variability play a key role in observed latency and packet loss. These insights are directly relevant to understanding LinkedIn's network performance under different access scenarios.

3.3 Routing Challenges and Security Constraints

Performing Internet cartography, especially toward large commercial platforms like LinkedIn, poses significant challenges due to network security policies and infrastructure design. When executing `traceroute` to `linkedin.com`, most intermediate hops returned no response (* * *), as shown in Figure 3. This behavior is not an anomaly but a direct consequence of how modern networks handle diagnostic probes.

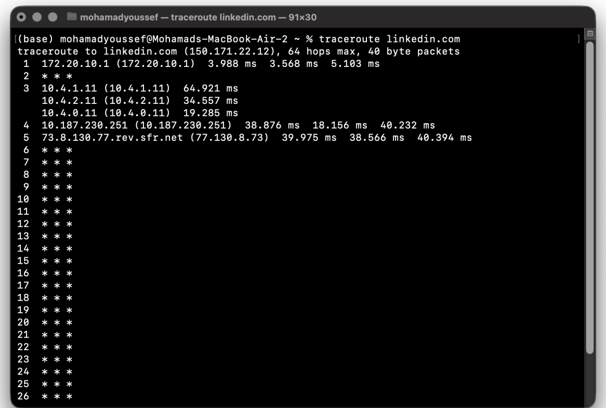

Figure 3: Traceroute output showing blocked intermediate routers when probing `linkedin.com`.

Many Internet routers and autonomous systems, particularly those managed by major cloud providers such as MICROSOFT AZURE, which hosts LinkedIn, intentionally block or de-prioritize ICMP and UDP packets used by tools like `traceroute`. These restrictions are implemented to prevent network mapping, mitigate denial-of-service (DoS) risks, and protect the internal topology of cloud infrastructures. As a result, even though the packets reach the destination successfully, the intermediate route often remains partially invisible.

This limitation illustrates why accurate Internet cartography is complex: the topology of large-scale services cannot be fully reconstructed through end-to-end probing alone. Figure 3 highlights this constraint by showing that the majority of intermediate routers between the local network and LinkedIn's servers remain undisclosed, likely due to NAT, private addressing, and firewall rules that drop unsolicited diagnostic traffic.

The WIRESHARK capture shown in Figure 4 provides a concrete example of how traceroute behaves in practice. The first hops (172.20.10.1) correspond to the local gateway, which correctly returns ICMP *Time-to-Live Exceeded* messages. Subsequent private addresses in the 10.x.x.x range represent routers within the mobile provider's internal network, using NAT for traffic forwarding.

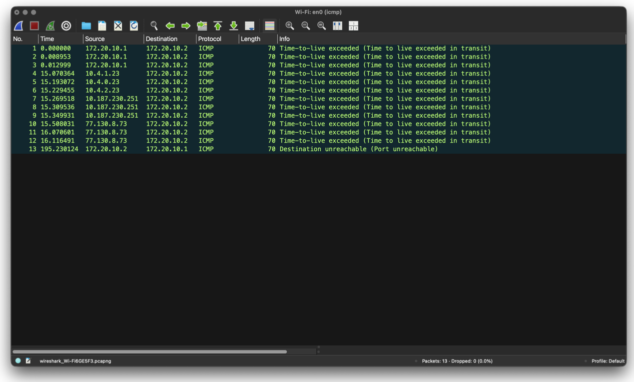

Figure 4: Filtered WIRESHARK capture showing limited IMCP responses during a traceroute to `linkedin.com`.

Beyond these, only one public router (77.130.8.73) replies, while no response is received from LinkedIn's infrastructure. The final message, *Destination Unreachable Port Unreachable*, indicates that the probing sequence was terminated locally after the destination stopped responding. This confirms that most routers and cloud networks block ICMP diagnostic messages, preventing full path reconstruction and highlighting the inherent limitations of Internet cartography tools such as `traceroute`.

In summary, the packet capture shows that `traceroute` used UDP probes. Each packet with increasing TTL triggered ICMP "Time Exceeded" replies from intermediate routers, revealing the path step by step. The final probe returned an ICMP "Port Unreachable" message, while a TCP traceroute would end with a SYN/ACK. This illustrates how `traceroute` combines UDP for probing and ICMP for feedback.

Appendix A — Domain Information

To complement the network measurements, WHOIS and DNS lookup (`dig`) commands were performed to examine the configuration and registration details of `linkedin.com`. These outputs provide insight into the domain's authoritative servers and registration metadata.

Listing 1: Excerpt of WHOIS information for `linkedin.com`

```
Domain Name: LINKEDIN.COM
Registrar: MarkMonitor Inc.
Updated Date: 2025-01-28T17:18:20Z
Creation Date: 2002-11-02T00:00:00Z
Name Server: NS1-42.AZURE-DNS.COM
Name Server: NS2-42.AZURE-DNS.NET
Name Server: NS3-42.AZURE-DNS.ORG
Name Server: NS4-42.AZURE-DNS.INFO
DNSSEC: unsigned
```

This WHOIS output shows that `linkedin.com` is registered with MarkMonitor Inc. The domain has been active since 2002 and is currently maintained, and it does not use DNSSEC, meaning DNS responses are not cryptographically verified. The authoritative name servers for LinkedIn's domain are hosted on Microsoft Azure's DNS infrastructure, providing redundancy and global coverage.

Listing 2: Excerpt of DIG command output for `linkedin.com`

```
; <<>> DiG 9.10.6 <<>> linkedin.com
;; ANSWER SECTION:
linkedin.com. 300 IN A 150.171.22.12
```

The DIG output shows the resolved IPv4 address of `linkedin.com` as 150.171.22.12, indicating the specific server that client requests will reach. This confirms the authoritative DNS resolution and provides context for routing measurements.