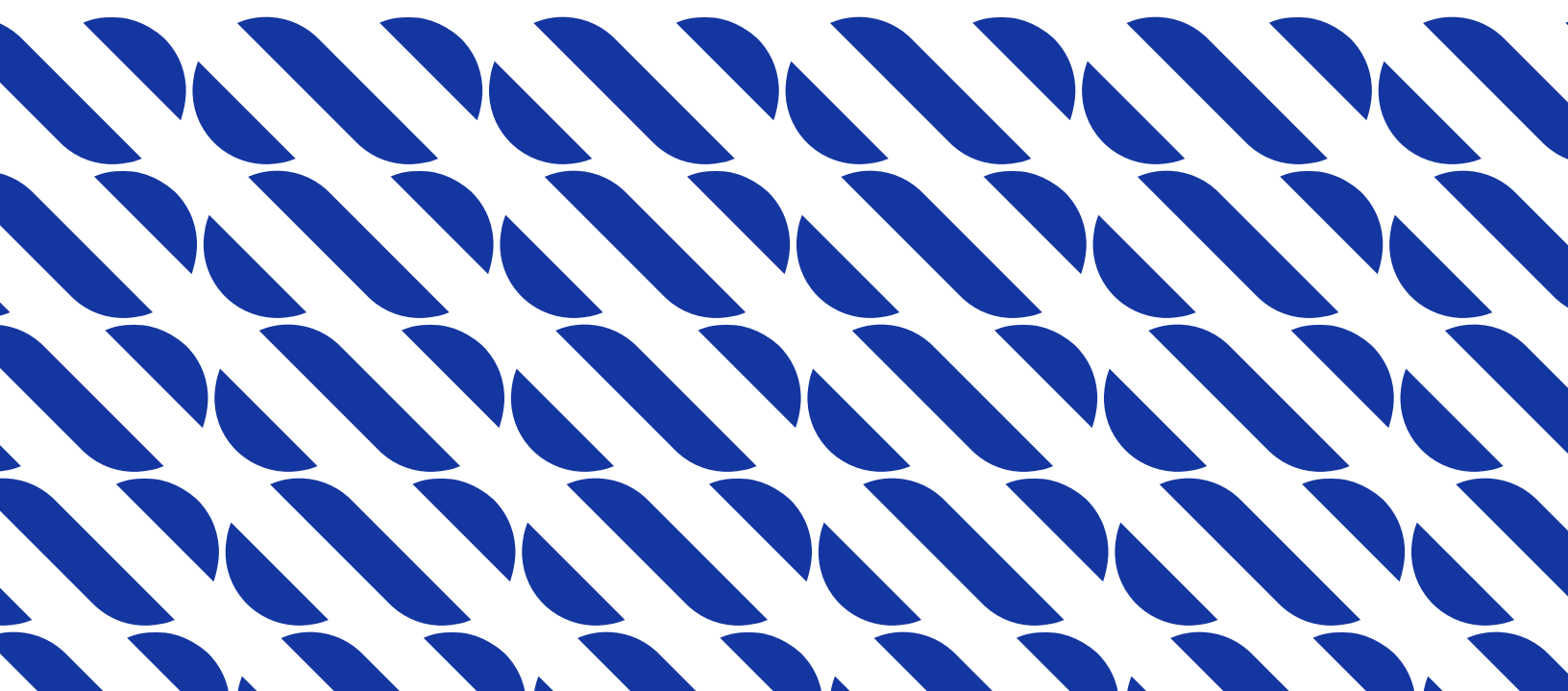




# Cross-Border Enterprise Connectivity

**The infrastructure that defines performance  
for mission-critical operations between Mexico  
and the United States**

---





## Cross-border connectivity: Key infrastructure for mission-critical operations

Companies operating in Mexico increasingly depend on applications, cloud platforms, and corporate systems located outside the country. In this environment, cross-border connectivity is no longer a secondary technical detail—it is a critical factor for performance, availability, and operational continuity.

Flō Networks designs cross-border enterprise connectivity for organizations that require low latency, high availability, and full traffic control between Mexico and the United States, even in mission-critical environments.

**Cross-border connectivity**—also referred to as binational connectivity or connectivity between Mexico and the United States—is **the ability to interconnect a company’s operations in Mexico with infrastructure in the U.S.** in a direct, secure, and predictable way, including public cloud platforms, corporate data centers, mission-critical business applications, and multinational enterprise networks.

Unlike generic international connectivity, cross-border connectivity is designed as a complete network architecture, optimized for continuous, high-volume, bidirectional traffic flows.

**Cross-border connectivity is critical for companies in Mexico.** Even with the growth of local cloud regions, **a significant portion of enterprise traffic in Mexico still crosses the border.** This is especially true for:

- Multinational organizations
- Nearshoring operations
- Advanced manufacturing
- Financial services
- Enterprise SaaS platforms

When the network is not designed for this traffic pattern, **common issues appear, like unpredictable latency, packet loss, inconsistent application performance, intermittent disruptions, or limited end-to-end visibility.**

A properly designed cross-border connectivity architecture eliminates these risks at the network design level, not as an afterthought.

### Cross-border connectivity vs traditional international Internet

Traditional international Internet	Cross-border enterprise connectivity
Dynamic, uncontrolled routes	Engineered and optimized routes
Traffic mixed with public Internet	Segregated enterprise traffic
Variable latency	Consistent latency
Limited visibility	End-to-end monitoring
Designed for general access	Designed for mission-critical operations

---

## Design your cross-border connectivity with Flō

Flō Networks is an enterprise carrier built for mission-critical environments in Mexico, with an infrastructure focused on high-performance cross-border connectivity between Mexico and the United States.

Our approach is based on: **Carrier-grade network architecture**

**Controlled infrastructure**

**Low latency and high availability**

**Native integration with cloud and enterprise networks**

**Operations designed for business continuity.**

If your operations in Mexico depend on applications, systems, or infrastructure located in the United States, cross-border connectivity is not optional.

Let's talk about how to design a network architecture aligned with your technical and operational goals.

[flo.net](https://flo.net)

**When it comes to the role of international fiber crossings**, cross-border connectivity depends directly on it, as they determine:

- Where traffic exits Mexico
- How quickly it reaches the United States
- How many alternative routes exist
- How resilient the network is during failures

An enterprise-grade architecture requires **multiple international crossings, route diversity, and operational control**. Without this, binational connectivity becomes a single point of failure.

In enterprise environments, cloud connectivity is inherently cross-border, even when local cloud regions exist.

A properly designed cross-border connectivity architecture enables direct and stable access to cloud platforms, lower latency for mission-critical applications, greater predictability than VPNs or public Internet, and efficient integration with multicloud environments.

The result is better application performance, higher productivity, and lower operational risk.

### Common use cases

**Nearshoring and manufacturing:** Integration of plants in Mexico with corporate systems in the U.S., with stable latency for ERP, MES, and inventory control.

**Retail and services:** Reliable synchronization of POS, inventory, and core platforms across countries.

**Financial services:** Secure, encrypted, and predictable connectivity for critical systems and regulatory compliance.

**Multinational enterprises:** Unified corporate network with centralized visibility of binational traffic flows.

Empowering growth, nurturing competitiveness, and fostering success in a rapidly evolving, technology-driven landscape – this is the Flō Networks promise.