Flō NETWORKS

How to connect multiple locations in Mexico without disjointing your network

A practical approach to standardizing multi-site connectivity and preparing the network for hybrid and multicloud operation.

Why this guide

When a company operates multiple locations, the network often grows in stages, with different providers by region, different policies by site, and cloud connectivity resolved on a case-by-case basis.

That works—until it doesn't.

Disjointing becomes a silent cost: inconsistent performance, slow change, and complex operation.

What you will achieve with this approach

- **Standardize** multi-site connectivity with repeatable templates
- **Reduce disjointing** with less variation between sites and less operational complexity
- **Improve control** with central visibility and consistent policies
- **Prepare your network for cloud and multicloud** without improvising by using internet exits per site

The 6-step framework (quick overview)

1. Classify sites by operational role
2. Define a site standard (2–4 templates)
3. Choose your backbone (Internet + SD-WAN / Private WAN / Hybrid)
4. Integrate the cloud as part of the network
5. Design resilience where the business needs it
6. Implement operational governance and avoid disjointing

How to use this guide

Read it through once, then use it as a checklist to:

- Perform an internal diagnosis
- Compare alternatives
- Evaluate proposals

Step 1: Classify your locations by operational role

The common mistake

Classify locations by city or region.

The real challenge lies in **what each location does and the risks it is exposed to.**

Recommended classification

A. Branches/Points of Sale

- Typical apps: POS, payments, inventory, lightweight ERP/CRM, collaboration
- Risk: outages impact revenue and immediate operations
- Priority: continuity + prioritization by application + visibility

B. Warehouses / logistics / distribution

- Typical apps: WMS, handhelds, IoT, video surveillance, integrations
- Risk: Disruptions affect dispatch, inventory, and timing
- Priority: stability + capacity + segmentation and security

C. Corporate/regional offices

- Typical apps: ERP/CRM, collaboration, VoIP, internal systems
- Risk: productivity and data access
- Priority: consistent performance + control + optimized routes

D. Industrial plants/environments

- Typical apps: OT/IT, monitoring, control, integrations
- Risk: operational continuity and enhanced security
- Priority: strict segmentation + resilience + low variation

E. Hubs / data centers / cloud on-ramps

- Function: aggregation, interconnection, private cloud connectivity
- Priority: high availability, capacity, redundant architecture

Result of this step

Build a simple inventory: each site has a role and an operational/technical priority that allows you to standardize your network.

Step 2: Define your site standard (repeatable templates)

What is a site standard?

It is a technical and operational template that defines how a site connects and operates, including policies, visibility, security, and resilience. The goal is to reduce unique designs per location.

Suggested templates (example)

Type 1 Site: Critical (A)

- Dual connection (main + backup)
- Automatic switching
- Application prioritization
- Clear segmentation (corporate, guests, IoT, cameras)

Type 2 Site: Important (B)

- High-quality primary connection + backup based on criticality
- Consistent policies
- Centralized visibility
- Basic security controls and segmentation

Type 3 Site: Light (C)

- Efficient connectivity, without losing control
- Basic security and minimal segmentation
- Standardized monitoring and metrics
- Escalation plan if criticality increases

Sede Tipo 4: Hub / Node (H)

- High-capacity
- Priority redundancy
- Cloud interconnection (where applicable)
- Resilience-oriented design and aggregated traffic

What determines this step

- Where redundancy is required.
- Where application-level control is required.
- Which locations should be integrated into the cloud privately.
- Which elements should be consistent across all locations.

Flō NETWORKS

Step 3: Choose your backbone

Practical rule for deciding

- **WAN/private network or hybrid:** If the business depends on network consistency.
- **SD-WAN over the internet:** If the business depends on rapid expansion, and access is good.
- **A hybrid usually provides the best balance:** If there is cloud and critical apps.

Tres modelos que verás en la práctica

	When It Is appropriate	Advantages	Risks
Internet + SD-WAN (Overlay)	You need deployment speed	Central orchestration, consistent policies	Overlay does not replace poor access
	The underlying access per location is stable and of good quality	Segmentation and prioritization by application	
	You want central control and segmentation by application	Easy to add sites	Last mile variation is a variation in experience
WAN / Private Network	You need predictable performance between sites	More consistent performance	More careful initial design
	Critical applications between sites	Less dependence on public internet	
	You want greater route control and clearer SLAs	Better for sensitive operations and critical traffic	Requires good capacity and node planning
Hybrid	Mix of critical and lightweight sites	Consistency where it matters + flexibility where it's needed	If the capabilities of the Internet and private networks are poorly integrated, the risks associated with the previous options may persist
	You need consistency and control without overdesigning everything	Operational standardization and scalability	
	You want to integrate a private cloud without disjointing	Better total cost when designed by criticality	

Flō NETWORKS

Step 4: Cloud and multicloud as part of the network

The pattern that causes problems

When each site connects to the cloud via the public internet without a common design, the result is often variable latency, packet loss, inconsistent experiences, and more difficult operation.

Recommended approach

Define the cloud as an **extension of your network**, with consistently designed connectivity.

When dedicated cloud connectivity is appropriate

- Cloud applications are critical to operations
- High traffic volume to the cloud
- Need for stability and traffic control
- Security, compliance, or segmentation requirements
- Multi-cloud strategy (if you have multiple providers or regions)

What dedicated connections solve

- Greater stability and predictability for cloud apps
- Less variation by time, location, or congestion peaks
- More control over routes and performance
- A more solid foundation for operational continuity

How to integrate Multicloud

If your company uses multiple clouds, avoid undertaking a project for each cloud by designing a repeatable approach to operating environments, such as:

- Amazon Web Services (AWS)
- Microsoft Azure
- Google Cloud
- Oracle Cloud
- IBM Cloud

Step 5: resilience and continuity (Where It Applies and Where It Doesn't)

Resilience cannot be bought. It is designed based on operational criticality.

Three practical levels

Level 1: High resilience (critical sites, hubs, key CEDIS)

- Dual path
- Automatic switching
- Monitoring with clear thresholds
- Prioritization by application

Level 2: Medium resilience (important sites)

- Backup based on impact
- Consistent policies
- Visibility and metrics
- Ability to scale to Level 1 if operation changes

Level 3: Efficient resilience (low-traffic locations)

- Efficient connectivity
- Basic security and segmentation
- Control and visibility for operation and diagnostics

Metrics to consider


Latency (ms)


Actual availability per location


Jitter (variation)


Performance per critical application


Packet loss

Flō NETWORKS

Step 6: Operational governance

Minimum elements of governance

Without governance, the network disjoints again, even if the initial design is good.

Visibility and control	✓ Dashboard by location and by application
	✓ Consistent segmentation (users, IoT, cameras, guests, etc.)
	✓ Prioritization by application rather than generic ports
Change management	✓ Repeatable process for new locations
	✓ Configuration and validation standard
	✓ Living documentation with templates and exceptions
Operation and support	✓ Escalation model
	✓ Response times and criteria
	✓ Regular reports on trends, incidents, and improvements

The result is that connectivity is no longer a project but has become an operational platform ready for growth.

Flō NETWORKS

Checklist: Connecting Multiple Locations Without Disrupting the Network

Check if you have already defined or implemented this.

This guide provides a simple framework for organizing internal discussions and evaluating multi-site connectivity proposals. With clear site classification, repeatable standards, and a consistent cloud or multicloud strategy, you can reduce disjointedness and regain operational control without slowing down growth.

Strategy

- [ ] I have classified the sites by operational role (A, B, C, or Hub).
- [ ] I have defined which apps are critical by site type.
- [ ] I have defined the consistency objective (what “good” means for my company).

Standarization

- [ ] I have 2–4 site standard templates.
- [ ] I know which sites require high, medium, and efficient redundancy.
- [ ] Segmentation policies are defined and repeatable.

Architecture

- [ ] I chose a model (Internet+SD-WAN / Private WAN / Hybrid) for clear reasons.
- [ ] I can prioritize traffic by application.
- [ ] I have centralized visibility by location and by application.

Cloud and Multicloud

- [ ] The cloud is part of the architecture (not “internet access” by location).
- [ ] I know when dedicated cloud connectivity is appropriate.
- [ ] I have a repeatable approach for operating in a multicloud environment.

Operation

- [ ] I have defined operational metrics (latency, jitter, loss, availability).
- [ ] I have a process for adding locations without reinventing the design.
- [ ] I have a clear support and escalation model.

Common mistakes

- Designing by city rather than by operational role.
- Purchase SD-WAN, expecting it to fix a poor last mile.
- Resolving the connection to the cloud headquarters by headquarters using the public internet.
- Making redundancy the same for everything (increases cost without increasing actual continuity).
- Not defining operational governance from the outset.