# Ataya Chorus for Private 5G Deployment with LEO Satellite Backhaul

Communication Service Providers (CSPs) and enterprises deploying private 5G networks face a fundamental challenge: how to connect network infrastructure in remote locations where traditional fiber connectivity is unavailable or cost prohibitive. Remote operations across mining, agriculture, maritime, energy, and construction have historically faced an impossible choice—invest millions in fiber infrastructure with months of deployment time or settle for unreliable connectivity that cannot support modern industrial operations.

This post explores deployment architectures for Ataya Chorus, a cloud-managed private 5G platform running on AWS, with Low Earth Orbit (LEO) satellite serving as the backhaul connectivity for remote site deployments. Ataya Chorus is a cloud-managed 5G solution where the 5G Control Plane runs entirely on AWS infrastructure, while the User Plane Function (UPF) is deployed at the edge—embedded directly in the 5G radio access points. This distributed architecture, combined with LEO satellite backhaul, enables private 5G deployments in locations previously considered impractical for enterprise-grade cellular connectivity.

## The Architecture with LEO Satellite Integration

Low Earth Orbit (LEO) satellite constellations such as Starlink, OneWeb, and Amazon Leo provide high-throughput, low-latency connectivity to remote locations worldwide. When integrated with Ataya Chorus, a LEO satellite service serves as the backhaul link connecting the edge-deployed UPF to the 5G Core Network running on AWS.

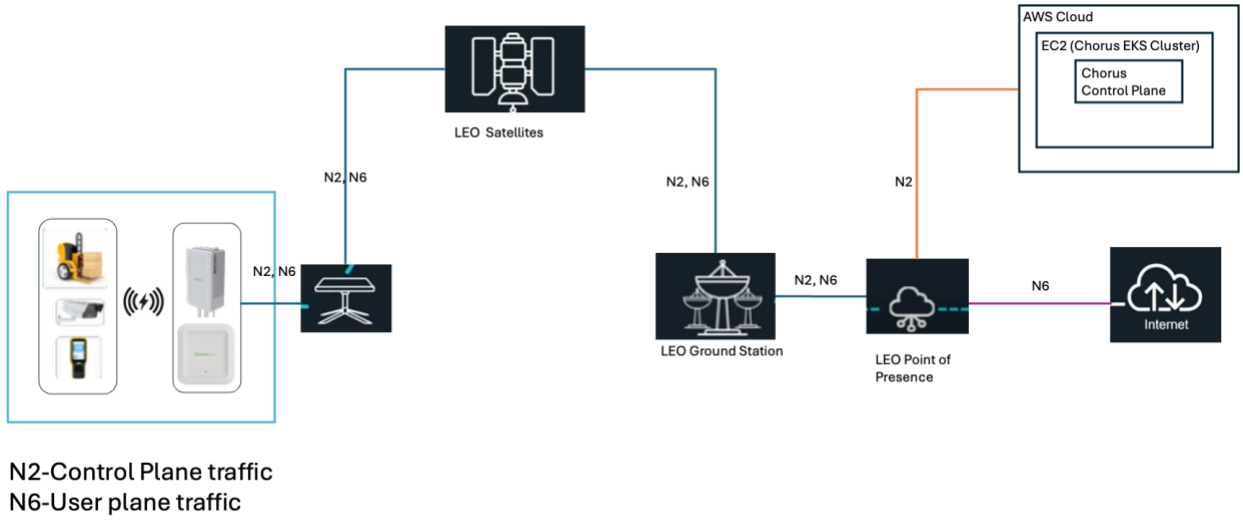


***Figure 1: 5G Integration with LEO Satellite Backhaul***

The LEO satellite terminal connects directly to the 5G radio access point (AP). The AP houses a 5G NR gNB and an embedded User Plane Function (UPF), creating a secure, encrypted tunnel to the Chorus cloud infrastructure on AWS. All control plane signaling and management traffic flows through this satellite link, while user data traffic is processed locally at the edge by the UPF, with outbound traffic to the internet routed through the satellite link. Traffic between the

gNB (inside the AP) and UPF is processed entirely at the edge site. The UPF performs Network Address Translation (NAT) to translate User Equipment IP addresses (UEIP) to the UPF Elastic Network Interface before routing traffic towards the internet. More formally using 3GPP interface specifications:

- N2 (control plane signaling) traffic goes over satellite to Ataya Core at AWS
- N3 (user plane data) traffic processed locally inside the radio unit between gNB and embedded UPF.
- N6 (data network/internet) traffic goes over satellite link and exits to the Internet at the PoP.

**Key performance characteristics include:**

- **Latency:** 50-70 milliseconds round-trip time with local breakout for real time edge processing
- **Throughput:** Up to 1 Gbps sustained bandwidth per terminal
- **Reliability:** 99% uptime with automatic failover capabilities
- **Coverage:** Global coverage including remote regions previously unreachable by terrestrial networks
- **Deployment Time:** Hours to days versus 6-18 months for traditional fiber installations

## Ataya Chorus Architecture

Ataya Chorus follows a cloud-native architecture with clear separation between control plane and user plane functions. It also embodies a separation of 5G Core

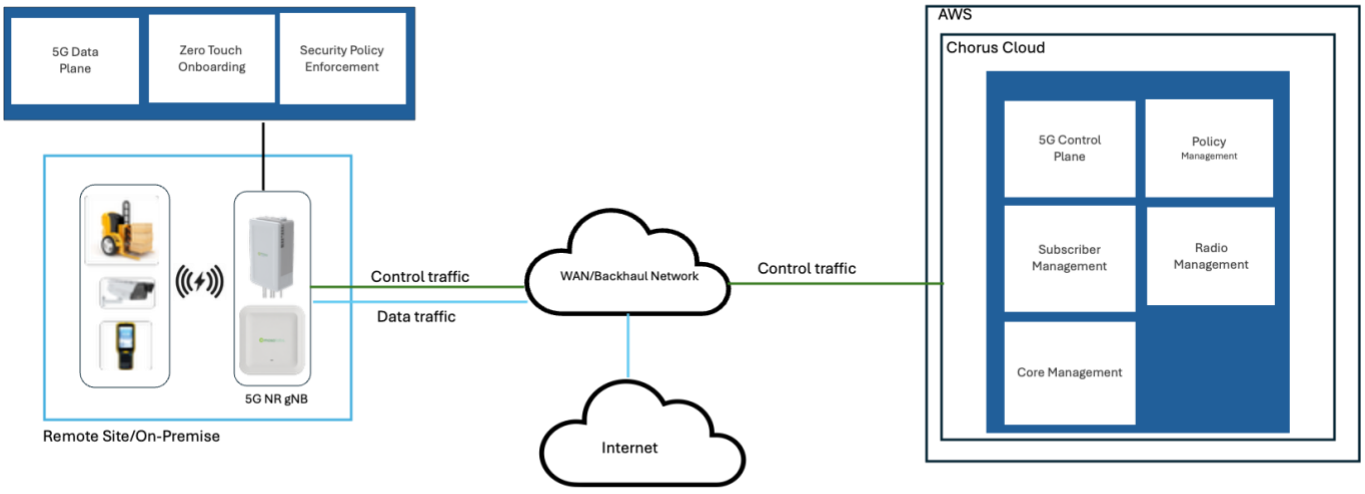


*Figure 2: Ataya Chorus Functional Architecture*

**Architecture Details:**

- 5G Control Plane functions (AMF, SMF, etc.) run on AWS EKS clusters. Control plane traffic is securely transported over a gRPC connection.
- 5G Management Plane for centrally managing the edge and radio runs on AWS EKS cluster.

- 5G Data Plane and Security Enforcement is implemented in 5G AP at remote site.
- 5G-NR gNB integrated small cell, indoor and outdoor.
- 3GPP Release 16 capable with RedCap (Reduced Capability) device support.
- Support for multiple Private 5G bands including n48 (CBRS), n77, n78, and n79.

**Security details:**

- SIM-based device authentication — 5G's native subscriber authentication (5G-AKA) means only authorized UEs with provisioned SIMs can access the network, unlike Wi-Fi where credential sharing is common
- Encrypted air interface and backhaul — NR air interface encryption plus encryption for the satellite backhaul segment, so data is protected end-to-end even over a shared satellite link
- Network slicing / policy enforcement — Ability to segment traffic by application or user group with different QoS and security policies, enforced at the UPF at the edge
- Zero-trust posture at the edge — Since the UPF sits in the AP, security enforcement happens locally even if the satellite link is interrupted — unauthorized devices can't access the local network
- Centralized policy management — Security policies defined centrally in AWS and pushed to all sites, ensuring consistent enforcement across distributed remote deployments

**Use Cases:**

- Remote mining operations requiring secure Internet access for equipment telemetry and monitoring
- Offshore energy platforms with cloud-based application dependencies
- Temporary construction sites needing Internet connectivity for project management systems
- Agricultural operations with IoT devices sending data to cloud analytics platforms

**Considerations:**

- All user plane traffic traverses the LEO satellite link (up and down)
- Latency includes satellite round-trip time (~50-70ms) plus Internet latency
- Simplified management via centralized dashboards hosted in AWS

## Ataya Chorus Architecture Benefits for Satellite Deployment

Ataya Chorus is specifically designed for cloud-managed deployment scenarios, making it well-suited for satellite backhaul integration:

### Distributed User Plane Architecture

By embedding the UPF directly in the AP, Ataya Chorus minimizes backhaul bandwidth requirements. Only N2 control plane signaling and PFCP session management traffic (N4) traverses the LEO satellite link to AWS. User plane data (N3 interface) is processed entirely at the edge, with only N6 data network traffic consuming backhaul capacity based on the selected breakout design. Traditional 5G architectures requiring centralized UPF deployment would consume significantly more satellite bandwidth.

### Zero-Touch Deployment

Chorus Agent software enables automatic cloud discovery and configuration synchronization. When a new radio access point is deployed at a remote site and connected via LEO satellite, it automatically discovers the Chorus cloud infrastructure on AWS, downloads appropriate configuration, and registers itself with the 5G core network. This plug-and-play capability eliminates the need for on-site technical personnel for initial deployment and configuration.

### Multi-Tenant Cloud Architecture

Chorus runs as a multi-tenant platform on AWS, enabling managed service providers to operate private 5G networks for multiple customers from a single cloud infrastructure. Each tenant receives isolated 5G core network instances with independent configuration, subscriber management, and policy control. This architecture significantly reduces operational complexity and cost for managed service providers deploying private 5G networks across multiple remote customer sites.

### Elastic Scalability

Control plane functions run on Amazon EKS with horizontal auto-scaling, automatically adjusting capacity based on the number of connected sites and active sessions. This cloud-native architecture enables efficient resource utilization and eliminates the need for capacity planning typical of on-premises 5G core deployments. Operators only pay for the AWS compute and storage resources actually consumed.

## Industry Applications

The combination of Ataya Chorus and LEO satellite backhaul addresses connectivity challenges across multiple industries:

### Mining and Natural Resources

Remote mining operations can deploy private 5G for autonomous vehicle fleets, equipment telemetry, safety monitoring systems, and worker communications. The low latency (~50ms) supports real-time control applications, while LEO satellite backhaul eliminates the need for costly fiber installation across vast mining sites.

### Maritime and Offshore Energy

Offshore oil platforms, wind farms, and maritime vessels require secure, reliable connectivity for SCADA systems, environmental monitoring, and crew communications. Private 5G with LEO satellite backhaul provides enterprise-grade connectivity independent of cellular coverage or undersea cable infrastructure.

### Agriculture and Precision Farming

Large agricultural operations spanning thousands of acres can deploy private 5G for precision farming equipment, drone operations, IoT soil sensors, and automated irrigation systems.

### Construction and Temporary Sites

Construction sites benefit from rapid deployment (days versus months) of enterprise-grade connectivity for equipment automation, safety monitoring, project management systems, and security cameras. When the project concludes, the equipment can be relocated to the next site without fiber infrastructure abandonment costs.

### Transportation and Logistics

Remote transportation hubs, intermodal facilities, and logistics centers require secure connectivity for inventory management systems, autonomous vehicle charging/maintenance stations, and package tracking infrastructure.

### Emergency Response and Disaster Recovery

Rapid deployment capabilities enable emergency services to establish private 5G networks in disaster zones where terrestrial infrastructure has been damaged. First responders gain secure, high-bandwidth connectivity for command-and-control systems, real-time video streaming, and inter-agency coordination.

## Conclusion

The integration of Ataya Chorus cloud-managed 5G with LEO satellite backhaul represents a transformative approach to private network deployment. By combining cloud-native 5G core infrastructure on AWS with LEO satellite connectivity, enterprises can deploy enterprise-grade cellular networks in locations previously considered impractical due to the cost and time required for traditional fiber backhaul.

**TAGS:** 5G, Private 5G, LEO Satellite, Starlink, OneWeb, Kuiper, AWS, Edge Computing, Private Networks, Industrial IoT

**3GPP Interface and Acronym Reference:**

| Term | Description |
|---|---|
| **gNB** | Next Generation Node B — the 5G base station (radio) that provides wireless connectivity to user devices |
| **UPF** | User Plane Function — handles user data traffic (forwarding, routing, NAT). In Ataya Chorus, embedded directly in the radio access point at the edge |
| **AMF** | Access and Mobility Management Function — manages device registration, connection, and mobility in the 5G core network |
| **SMF** | Session Management Function — manages data sessions between user devices and the network, including IP address assignment and QoS policy |
| **UE** | User Equipment — any device that connects to the 5G network (phones, sensors, IoT devices, laptops, etc.) |
| **N2 Interface** | Control plane interface between the gNB (radio) and the AMF in the 5G core. Carries signaling for device registration, handovers, and session setup |
| **N3 Interface** | User plane interface between the gNB and the UPF. Carries the actual user data traffic (e.g., internet browsing, video, IoT data) |
| **N4 Interface** | Session management interface between the SMF and UPF using the PFCP (Packet Forwarding Control Protocol). Controls how the UPF handles and routes traffic |
| **N6 Interface** | Data network interface between the UPF and external networks (e.g., the Internet or enterprise applications). This is where user traffic exits the 5G network |

| | |
|---|---|
| **NAT** | Network Address Translation — translates private device IP addresses to a routable address before traffic exits to the Internet |
| **5G-AKA** | 5G Authentication and Key Agreement — the native 5G protocol for securely authenticating devices using SIM credentials |
| **QoS** | Quality of Service — policies that prioritize certain types of traffic (e.g., real-time video over background downloads) to meet application performance requirements |
| **RedCap** | Reduced Capability (3GPP Release 17) — a lighter 5G NR device category designed for IoT sensors, wearables, and industrial monitors that need 5G connectivity but not full smartphone-class throughput |