



The journey towards digital ATM

Evolving ground-to-ground communication networks for safe, efficient air travel

White paper

Air navigation service providers (ANSPs) are working to make digital air traffic management (ATM) a reality by embracing modern technologies such as trajectory-based operations (TBO) and video analytics. Together with cloud computing and artificial intelligence (AI), these technologies promise to help them revolutionize ATM and ensure safe, efficient, resilient and sustainable air travel.

To turn this promise into reality, ANSPs need to make sure their mission-critical IP/MPLS wide area networks (WANs) can keep pace with the communication demands of the digital ATM infrastructure and emerging innovations, as well as counter more complex cyber threats. This paper explains how new WAN capabilities and innovative use cases such as segment routing, operational technology (OT) cloud networking, networking for AI workloads and zero-trust quantum-safe networking can help ANSPs use their WANs to unlock the full potential of digital ATM.

Contents

Introduction	3
Networking is fundamental to ATM digitalization	3
The next frontier in ATM digitalization	5
Trajectory-based operations	5
Video analytics	6
Evolving IP/MPLS WAN for the next digital frontier	6
Harnessing the full power of segment routing in the IP/MPLS WAN	6
OT cloud networking	6
Networking for AI workloads	8
Zero-trust WAN security in the quantum era	9
Conclusion	10
Abbreviations	11

Introduction

Aviation is an essential component of the global transport infrastructure. It connects people, countries and economies and is a key driver for prosperous societies. Following a period of unprecedented disruption in the early 2020s, air traffic has made a strong recovery and is poised to resume its long-term growth trajectory. This renewed expansion, coupled with increasing aviation industry and government focus on more sustainable flying, presents several critical challenges for air navigation service providers (ANSPs), including:

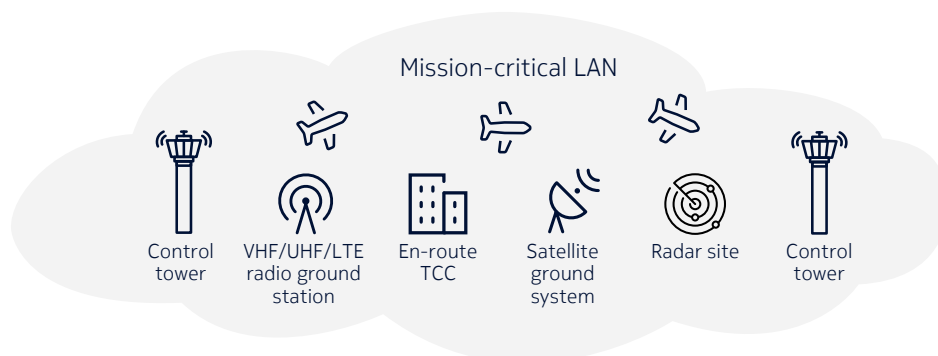
- Ensuring the highest levels of safety and security.
- Optimizing flight trajectories to reduce fuel consumption, carbon emissions and delays.
- Increasing airspace capacity and resilience to safely integrate a new class of unmanned aircraft systems (UASs), specifically those designed for advanced air mobility (AAM), as well as electric vertical takeoff and landing (eVTOL) aircraft.
- Improving operational efficiency to manage traffic growth, a goal that is leading to the adoption of remote tower operations.

To address these challenges, ANSPs are transforming their air traffic management (ATM) infrastructure with digital technologies. This transformation journey involves modernizing key communication, navigation and surveillance (CNS) applications. For example, ANSPs are expanding pilot communications by adding data capabilities alongside traditional voice radio with controller-pilot data link communications (CPDLC). They are also enhancing surveillance with Automatic Dependent Surveillance-Broadcast (ADS-B) and multilateration (MLAT) technologies that complement primary and secondary surveillance radar (PSR/SSR). These advancements improve communication, data collection and sharing among ground systems, which in turn enhances efficiency, cost, sustainability and safety.

Networking is fundamental to ATM digitalization

ANSPs need a robust and resilient aeronautical telecommunication network (ATN) to realize their digitalization ambitions. The backbone of the ATN is a ground-to-ground communication network, or mission-critical wide area network (WAN), that provides extensive connectivity for all ATM infrastructure. This includes connecting departure and destination control towers, en-route traffic control centers (TCCs), weather stations, and facilities such as UHF/VHF/4G/5G radio and satellite ground stations (Figure 1). The network must ensure resilient and secure connectivity for all CNS systems, including ground-to-ground and air-to-ground (A2G) backhaul.

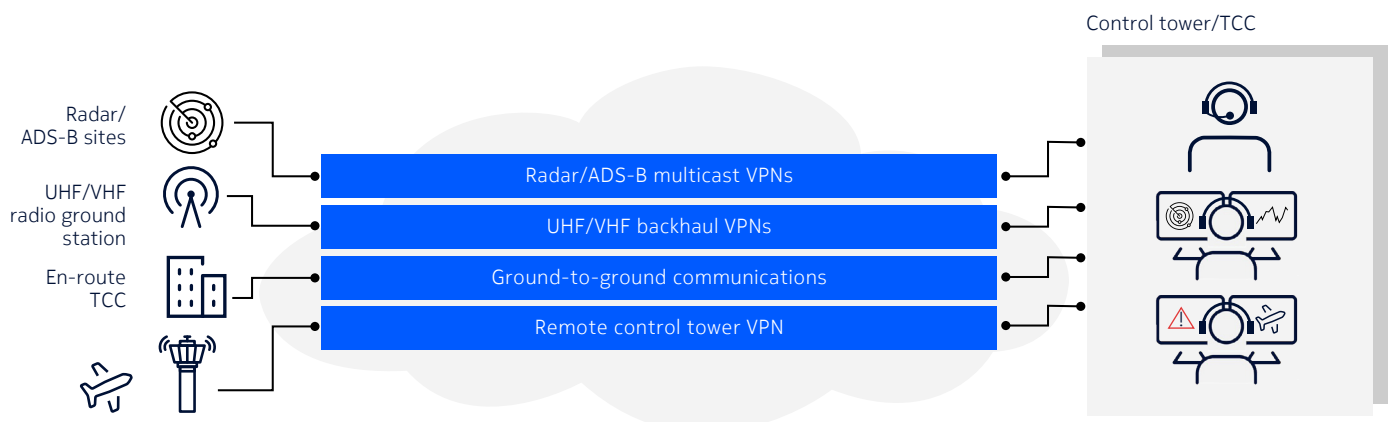
Figure 1. A mission-critical WAN provides ground-to-ground connectivity along the flight path



The WAN is a dedicated converged network that leverages IP/MPLS technology to provide the following fundamental mission-critical networking capabilities:

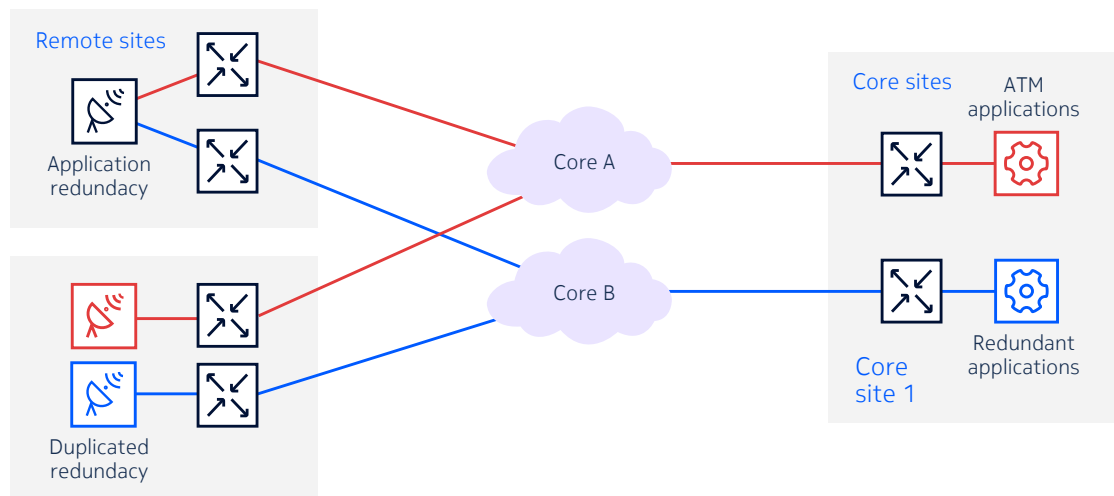
- **Multiservice networking:** Having a network that can support multiple services is crucial for meeting the diverse communications needs of a modern ATM system. With IP/MPLS virtual private networks (VPNs), each CNS application—from real-time ADS-B and radar to best-effort IT services—is carried in its own VPN (Figure 2). To optimize network efficiency, the VPN must also support IP multicast to enable the simultaneous delivery of data streams from a single source to multiple recipients (e.g., a radar station sending data to multiple air traffic stations and servers). IP multicast is becoming increasingly important because modern applications such as remote tower operations and video analytics rely on the efficient transport of video feeds to multiple locations.

Figure 2. A multiservice WAN serving numerous ATM applications



- **Strong resiliency:** A network outage, such as the loss of a radar feed or A2G voice communications, could lead to severe disruptions in ATM and jeopardize flight safety. To prevent such failures, the communication network must harness the extensive redundancy features of IP/MPLS, including fast reroute capabilities. Furthermore, because of the criticality of ATM traffic, ANSPs may implement a dual-core network architecture to ensure the highest possible network availability (Figure 3).

Figure 3. A dual-core ANSP network architecture



- **Deterministic quality of service (QoS):** ANSPs rely on a diverse range of applications, so QoS is crucial in the WAN. Deterministic QoS capabilities ensure that safety-critical, real-time applications such as A2G communications and remote tower video and radar feeds receive strict, low-latency network performance. This prioritization protects them from being impacted by less-demanding traffic, such as CCTV or IT business systems. It guarantees that all applications consistently meet their specific performance objectives (Table 1).

Table 1. A reference QoS profile for ATM applications

Application	Latency budget	Bandwidth	Criticality
A2G voice communications	Low	Low	High
Remote tower video	Low	High	High
Radar feed	Medium	Low	High
ADS-B	Medium	Low	High
CCTV	Medium	High	High
Weather observation	High	Low	Medium
IT business systems	High	Medium	Low

- **Full interoperability with legacy TDM applications:** While TDM and SDH/SONET network equipment is moving from end-of-life to end-of-support, many deployed ATM applications that are based on TDM, such as radar, VHF and emergency communications, will remain in use for years to come. The IP/MPLS WAN needs to support TDM circuit emulation capability and the necessary legacy interfaces, including V.24/RS-232, E&M and FXS/FXO, to enable graceful application migration.

The next frontier in ATM digitalization

As they gather momentum on their digitalization journey, ANSPs are exploring and trialing the latest ATM system innovations. Many of these advancements are powered by cloud computing today and will eventually be driven by artificial intelligence (AI). They will play a pivotal role in reshaping the way aviation is managed, provide a foundation for future automation and give controllers new tools that will help them make faster, data-driven decisions. Specific innovations such as trajectory-based operations (TBO) and video analytics are enabling smarter, more responsive and more resilient ATM capabilities.

Trajectory-based operations

As a core element of a modernized ATM system, TBO represents a foundational shift toward collaborative and data-rich air traffic control (ATC). This concept moves beyond traditional, voice-based control to a system that continuously calculates, shares and optimizes the four-dimensional (latitude, longitude, altitude and time) trajectory of every aircraft. To support this system, sophisticated TBO software applications such as traffic flow and time-based management systems must be hosted in a significant pool of real-time compute power. This pool is best supported by a virtualized cloud compute environment.

By leveraging technologies such as ADS-B to enable continuous surveillance, AI to analyze atmospheric data such as wind conditions in real time, and CPDLC to send revised flight plans, controllers can enable more strategic planning and optimized routing mid-flight, thereby saving fuel and time. The success of TBO hinges on resilient, low-latency communication systems that can ensure reliable data exchanges between flight crews and air traffic controllers, and resilient ADS-B data transport to the TBO software running in a dynamic, elastic cloud compute pool.

Video analytics

ANSPs and airport operators are making increasing use of video analytics to bolster situational awareness and safety. By integrating AI with live video feeds from runway monitoring, airside surveillance and tower operations, video analytics systems can automatically detect potential safety hazards such as runway incursions, unauthorized access or foreign object debris (FOD). By deploying video analytics on a combination of central and edge cloud platforms, ANSPs and airport operators can achieve faster response times, greater operational reliability and improved overall security across the airside environment.

Evolving IP/MPLS WAN for the next digital frontier

Advancements such as TBO and video analytics impose a new set of ground-to-ground communication requirements on the WAN. To meet these new requirements and counter increasingly sophisticated cyber threats, ANSPs must continue to evolve their WANs. As new ATM applications incorporate cutting-edge technologies such as cloud computing, the underlying network infrastructure needs to adapt. This evolution requires the WAN to provide enhanced capabilities, robust security and seamless connectivity to data centers and cloud platforms.

Harnessing the full power of segment routing in the IP/MPLS WAN

As ANSPs deploy more ground-based infrastructure such as sensors and radio stations, they continue to expand their networks. One proven strategy is to extend the IP/MPLS network with segment routing to simplify the network control plane, increase service scalability and control, and add network capabilities to support new digital innovations.

Segment routing offers an approach for distributing labels to routers in IP/MPLS networks. It uses routing protocols (OSPF or IS-IS) that already run in the network and adds segment routing extensions to distribute labels, also known as segment IDs (SIDs). By simplifying label management and distribution, segment routing enables the network to scale massively to support future growth. IP/MPLS networks can seamlessly migrate to Segment Routing over MPLS (SR-MPLS) without impacting the existing network hardware and routing design. The migration simplifies path establishment and enables better control of data traffic to maximize availability, eliminate common mode failure scenarios and make more efficient use of transport infrastructure.

When combined with a Path Computation Engine (PCE) function in the transport network manager, the IP/MPLS transport network provides enhanced capabilities for sophisticated network path computation and traffic engineering. It enables more effective load sharing with high data flow granularity by allowing fine-grained control over packet forwarding paths. With PCE, ANSPs can efficiently monitor the use of links and eventually adapt the network's behavior to address network events such as congestion or new application deployments.

OT cloud networking

Critical ATC service applications—such as those for managing tracking, flight plans and weather forecasts—are starting to be developed and deployed in more flexible cloud environments to take advantage of their scalability and elasticity. Consequently, ANSPs need to build new compute facilities to host segregated, on-premises servers, known as an operational technology (OT) cloud.

The OT cloud is a key component of the digital ATM infrastructure. It serves as a platform for:

- Enhancing application performance and agility, which enables ANSPs to adapt to a changing operational environment without compromising the availability and performance of critical applications.
- Embracing emerging and innovative technologies such as AI-powered video analytics and cloud-based applications that support TBO.

Because applications hosted in the OT cloud continually communicate with airfield sensors, surveillance systems and other ground-based assets, the data center network is now part of the mission-critical connectivity infrastructure. The data center network needs to interwork seamlessly with the IP/MPLS network to provide end-to-end mission-critical connectivity for ATM applications.

OT cloud networking is a response to this new requirement. It extends mission-critical connections from the IP/MPLS WAN into the data center network, which is composed of the data center gateway and data center fabric. The data center fabric is made up of leaf switches that connect to servers and spine switches that serve as the aggregation layer. The data center gateway serves as the interworking gateway between the fabric and the IP/MPLS WAN.

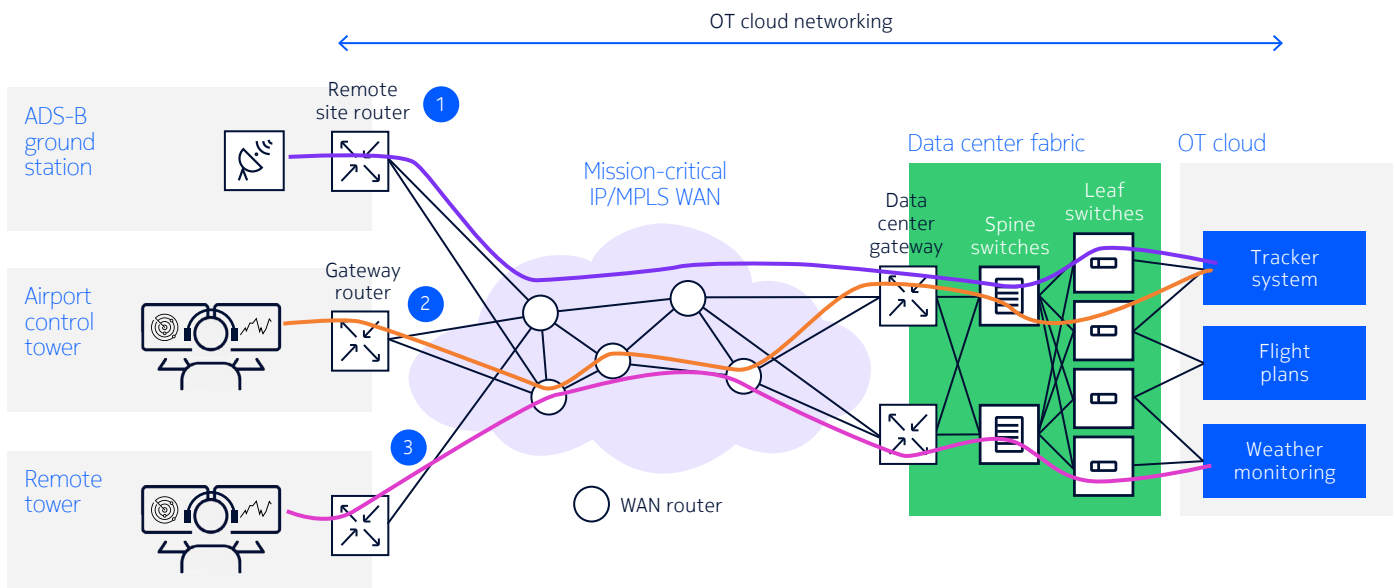
Through the gateway, the backbone can harness Ethernet Virtual Private Network (EVPN) service and Border Gateway Protocol (BGP) routing in the IP/MPLS transport and data center network domains to seamlessly interwork with the data center fabric at the service and IP layers. This interworking gives the network the agility required to support dynamic end-to-end networking that connects intelligent assets across the infrastructure to centralized OT application software hosted in the OT cloud.

Figure 4 illustrates how an OT cloud networking deployment can support three use cases:

1. An ADS-B ground station feeding real-time surveillance data to the central tracker system.
2. An air traffic controller retrieving real-time data from the aircraft tracker system through their surveillance display.
3. A controller in a remote tower receiving weather information and operational data for a remote airfield.

For each of these use cases, the data center fabric, in conjunction with the WAN, carries mission-critical data that is essential for ANSP operations.

Figure 4. OT cloud networking communications supporting mission-critical ATC applications



Networking for AI workloads

AI encompasses branches ranging from deep learning and computer vision to generative AI, agentic AI and artificial general intelligence (AGI), and offers immense potential to enhance aviation operations. It can and certainly will help air traffic controllers make faster, data-driven decisions that improve safety, efficiency, resiliency and sustainability for aviation transport.

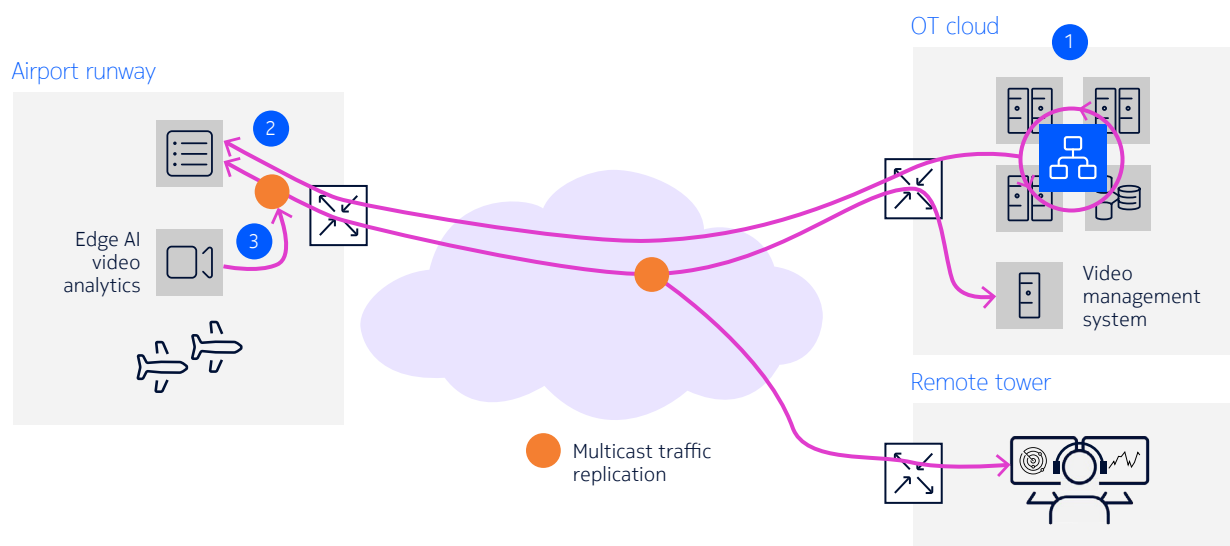
The deployment of AI for aviation will involve two key phases: training and inference. The process begins with data collection and training, where operational data from sensors, cameras and historical records is gathered and processed using on-premises graphics processing unit (GPU)-accelerated servers in the private OT cloud or, eventually, AI platform services from cloud providers (GPU-as-a service, or GPUaaS). A high-performance network is essential for ensuring efficient data processing and training of AI models.

Once the models are trained, they might need to be strategically deployed across the infrastructure, from the central data center to operation centers and airports, to support real-time inference. This deployment relies on a robust, extensive mission-critical WAN and data center network infrastructure to ensure seamless data flow between sensors and CCTV cameras and AI workloads.

This extensive network infrastructure is crucial for harnessing of the power of AI workloads, such as AI-powered video analytics for remote tower operations. For this use case, air traffic controllers located at a remote control center depend solely on multiple high-resolution video feeds for primary situational awareness. An AI-powered video analytics system can act as an intelligent assistant, processing all video streams to automatically detect potential safety hazards, such as runway incursions, unauthorized access to restricted areas or FOD. It can also detect if a landing aircraft's gear has not been deployed on final approach. By identifying these events automatically, the system can instantly alert the air traffic controllers. This drastically reduces their cognitive load and enables a faster response time.

To enable this powerful capability, an ANSP needs a highly robust, low-latency and high-bandwidth network infrastructure. This typically involves a three-step lifecycle, as illustrated in Figure 5 and described below.

Figure 5. AI networking across ATN network infrastructure



1. **AI model pre-training:** The process begins with the resource-intensive training of the AI model. This occurs in a GPU cluster housed within an on-premises data center or accessed through a third-party GPU-as-a-service offer. The data center fabric provides ultra-high speed Ethernet links (from 100–800 gigabits) that deliver ultra-low latency and lossless transmission, directly enabling highly efficient GPU-to-GPU communication critical to accelerate model development in the OT cloud.
2. **Model deployment:** Once the model is trained, it may be securely and efficiently replicated over the IP/MPLS WAN to edge AI video analytics servers deployed at local airports. This step ensures that the intelligence is delivered to the edge, where it is needed most. The WAN is a critical conduit for this process because it ensures high-performance multiservice networking for timely model downloads and updates.
3. **Real-time inference:** The deployed model is now ready to serve air traffic controllers in real time. Numerous video streams are fed into the edge AI GPU servers, remote tower and video management system in the OT cloud. To optimize network resources, the network infrastructure uses IP multicast to replicate video streams only when necessary, providing an efficient live feed for AI processing and controller displays. When the edge analytics system detects an event, it alerts the controllers immediately and indicates that actions must be taken.

Zero-trust WAN security in the quantum era

ANSPs are high-value targets for malicious actors in cyberspace. As ATM operations become increasingly digitalized, the attack surface of ATM infrastructure expands significantly. Protecting the confidentiality, integrity and availability of application data as it traverses the WAN is paramount for ensuring safe and efficient air operations.

An impregnable cyber defense requires a zero-trust approach combined with a multilayer defense-in-depth framework that extends across the ATM infrastructure, networks and applications. ANSPs can turn the WAN into a strong first line of cyber defense by implementing a comprehensive suite of security tools, including network segmentation through IP/MPLS services, network access control, IP and Media Access Control (MAC) filtering, and role-based network management.

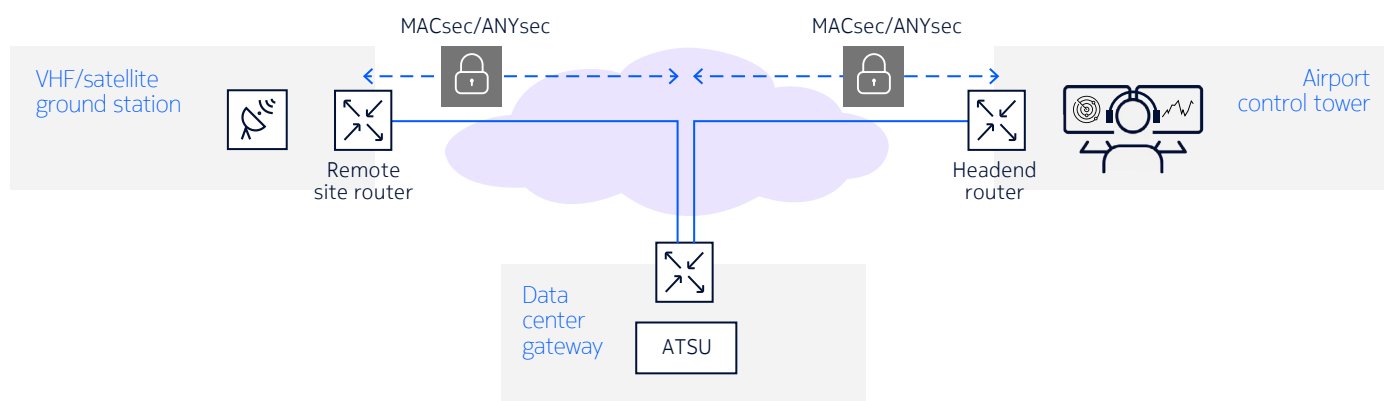
However, as bad actors gain access to more sophisticated resources and evolve their attack methods, ANSPs will need to adapt their security posture. With the arrival of cryptographically relevant quantum computers (CRQCs) looming, many current network security measures will soon become vulnerable. To ensure an effective defense against current attacks and emerging quantum threats, ANSPs must strengthen the transport network security posture with quantum-safe encryption.

Traditional encryption methods have been effective against various types of attacks, including eavesdropping, man-in-the-middle (MITM) and denial of service (DoS) attacks. However, the rapid advancement of quantum computing and quantum algorithms is poised to upend the cybersecurity landscape. For example, bad actors running Shor's algorithm on a quantum computer could break the protection provided by asymmetric key encryption schemes such as Diffie-Hellman. They could then eavesdrop on ATM communications.

The confidentiality of ATM data may not seem significant, but once bad actors capture, decrypt and analyze the data, they can begin launching targeted MITM and DoS attacks on critical systems such as CPDLC. For instance, consider a typical CPDLC communications scenario where a controller composes and sends a text-based clearance to climb to the air traffic services unit (ATSU). The ATSU would then queue and route the message to a VHF or satellite ground station for over-the-air transmission to the pilot. If CPDLC communications have been compromised, a bad actor could tamper with the clearance to climb and change it to a clearance to descend to a new altitude, which could result in a conflict with other air traffic.

It may take a considerable period for system suppliers to incorporate post-quantum cryptography algorithms into their applications and for ANSP operators to upgrade to these versions. But ANSPs can protect their infrastructure against quantum attacks today by implementing MACsec at the data link layer or ANYsec at the service layer. This approach can thwart quantum attacks by ensuring security across the ATM infrastructure, from ground stations to data centers and control centers (Figure 6).

Figure 6. Quantum-safe protection in the WAN



Conclusion

A safe, efficient and modern aviation system is a major pillar of a prosperous, open and connected global society. By efficiently and reliably connecting cities around the world, an aviation system can ensure better links between people and businesses, which improves the social quality of life and facilitates economic expansion.

To serve current and future aviation needs, ANSPs must prepare to explore the power of cloud computing and AI to drive next-generation applications such as AI-powered video analytics and TBO, which are increasingly deployed in private OT cloud environments. These systems demand more dynamic, resilient and data-intensive ground-to-ground communications than ever before. ANSPs need a modern, converged IP/MPLS WAN to act as the nexus of this new, connected ATM ground infrastructure. Nevertheless, this network must also be capable of seamlessly transporting legacy TDM-based applications during the long transition.

Looking ahead, ANSPs also face the challenge of securing this digital infrastructure against new threats, including those posed by emerging quantum computing capabilities. Given the long lifespan of ATM infrastructure, the network will need to incorporate quantum-safe cryptography to provide the infrastructure with long-term data security to ensure the integrity of mission-critical systems.

To navigate this complex transformation, ANSPs require a technology partner with a broad portfolio of products and services—from IP/MPLS and data center fabric to microwave—that can help them plan and transform their ATM networks today while ensuring readiness for the future.

Nokia addresses this need with an extensive product portfolio that spans IP/MPLS, data center fabric, packet optical, microwave, 5G, LTE and security. We complement this portfolio with a full suite of professional services, including network audit, design and engineering practices. With this combination of proven technology and expertise, we offer unique capability and flexibility to help ANSPs modernize their networks to maximize the benefits of digital air navigation services.

To learn more about Nokia ANSP and IP/MPLS solutions, visit our [ANSPs](#) and [IP Networks](#) web pages.

Abbreviations

A2G	air to ground
ADS-B	Automatic Dependent Surveillance–Broadcast
AGI	artificial general intelligence
AI	artificial intelligence
ANSP	air navigation service provider
ATC	air traffic control
ATM	air traffic management
ATN	aeronautical telecommunication network
ATSU	air traffic services unit
BGP	Border Gateway Protocol
CCTV	closed circuit television
CNS	communication, navigation and surveillance
CPDLC	controller–pilot data link communications
CRQC	cryptographically relevant quantum computer
DoS	denial of service
EVPN	Ethernet Virtual Private Network
eVTOL	electric vertical takeoff and landing
FOD	foreign object debris
FXO	foreign exchange office
FXS	foreign exchange subscriber
GPU	graphics processing unit
GPUaaS	GPU as a service
IP	Internet Protocol
IS-IS	Intermediate System to Intermediate System
IT	information technology
MAC	Media Access Control
MITM	man in the middle
MLAT	multilateral
MPLS	Multiprotocol Label Switching
OCC	operations control center
OSPF	Open Shortest Path First



OT	operational technology
PCE	Path Computation Engine
PSR	primary surveillance radar
QoS	quality of service
SDH	Synchronous Digital Hierarchy
SID	segment identifier
SONET	Synchronous Optical Networking
SR-MPLS	Segment Routing over MPLS
SSR	secondary surveillance radar
TBO	trajectory-based operations
TCC	traffic control center
TDM	time-division multiplexing
UAS	unmanned aircraft system
UHF	ultra-high frequency
VHF	very high frequency
VPN	virtual private network
WAN	wide area network

About Nokia

At Nokia, we create technology that helps the world act together.

As a B2B technology innovation leader, we are pioneering networks that sense, think and act by leveraging our work across mobile, fixed and cloud networks. In addition, we create value with intellectual property and long-term research, led by the award-winning Nokia Bell Labs.

Service providers, enterprises and partners worldwide trust Nokia to deliver secure, reliable and sustainable networks today – and work with us to create the digital services and applications of the future.

Nokia is a registered trademark of Nokia Corporation. Other product and company names mentioned herein may be trademarks or trade names of their respective owners.

© 2025 Nokia

Nokia OYJ
Karakaari 7
02610 Espoo
Finland
Tel. +358 (0) 10 44 88 000

Document code: 1610950 (October) CID207463