NOKIA

Re-imagining the airport network for 2020 and beyond

Enabling network flexibility, agility, and speed with IP/MPLS

Strategic White Paper

Contents

Introduction

Air traffic is growing at an enormous rate. Since the first commercial flight on January 1, 1914, airlines have carried 2.97 billion passengers more than 5.4 trillion kilometers.[1] More recently, aviation has been playing a pivotal role in the globalization process. Rapid, reliable, and affordable air transportation of people and goods are redefining this role.

That's important because, on a daily basis, the airport is the hub of air transportation. For hundreds of thousands of passengers-it's where the journey begins and ends. Given the escalating use of airports, it's not surprising that today's airport operators, private or public, are facing momentous challenges:

- Enhancing safety and security due to increasing air traffic and security threats
- Improving flight punctuality to compete with other modes of transportation
- Enriching passenger services to increase airport competitiveness
- Generating new revenues to achieve self-sufficiency
- Attaining more efficiencies to keep operational costs down

The stakes for airport operators are high. Today, operators globally are rapidly expanding and modernizing their airport infrastructure. They are competing fiercely to attract more flights and passengers. That's why airport operators are revamping their communications networks- a crucial part of airport infrastructure.

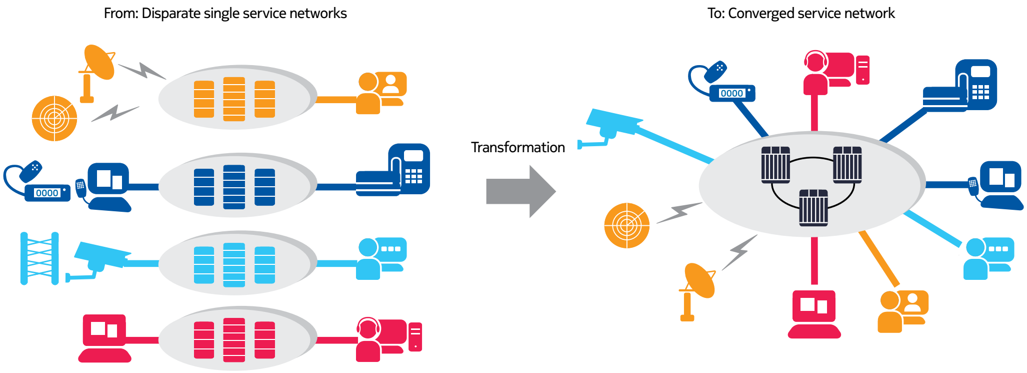
Achieving a single, converged network for efficiency

Airports are like condensed smart city housing. Hundreds, even thousands of enterprises, including airlines, shops, restaurants, service companies, government agencies (air traffic control, customs and border control) and public safety organizations are airport tenants. Millions of passengers pass through airports each year, and up to tens of thousands of employees work there. To accommodate today's broad communication needs, airport operators have typically deployed multiple separate networks - for instance, a communications network for air traffic management, another for CCTV video protection, still another for private mobile radio/land mobile radio (PMR/LMR)

[1] Aviation statistics can be found in the report titled Aviation: Benefits Beyond Borders, published by Air Transport Action Group (ATAG), http://aviationbenefits.org/media/26786/ATAG__AviationBenefits2014_FULL_LowRes.pdf

and emergency communications, and another for LAN/Wi-Fi®. Each network has been deployed at different times along with different infrastructure projects paid for from isolated budgets. The result is a plethora of networks built with different technologies and managed by disparate network managers. Is it any surprise that the network infrastructure has become unwieldy to manage and costly to operate? What's more, this disparate collection of network architectures discourages departmental collaboration and information sharing-both of which are crucial to seamless operations and optimal efficiency. The challenge is clear: To prepare the airport infrastructure for growth toward 2020 and beyond, transformation to a converged network has become the prime goal. (Figure 1).

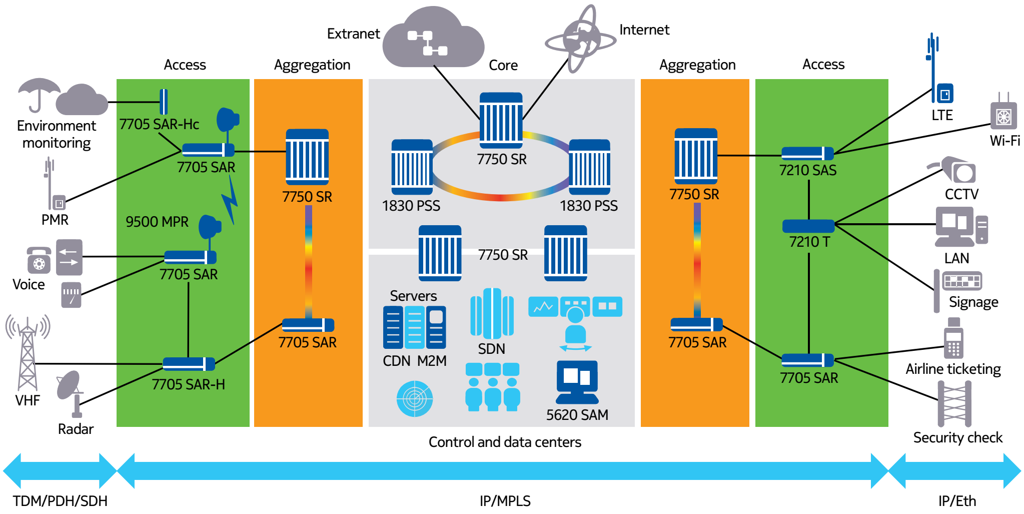
Figure 1. Transforming multiple networks into a converged network


From: Disparate single service networks
To: Converged service network
Transformation
0000
0000

Modernizing networks for growth

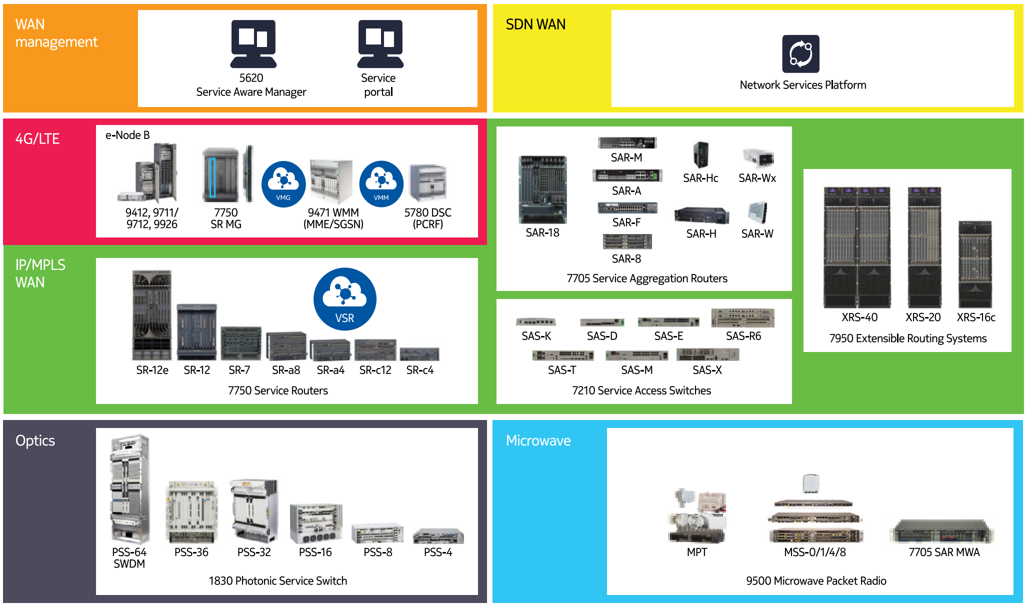
The transformation to a converged network enables operators to tackle the projected increase in air traffic, adopt next-generation, bandwidth-intensive applications, including high-resolution video-in addition to facilitating collaboration in order to achieve higher efficiency. A service-aware, converged IP/MPLS network integrated with a transport layer, such as packet microwave and dense wavelength division multiplexing (DWDM), permits flexible deployment while also assuring sufficient bandwidth for future growth in demand. Figure 2 represents an airport network transformation blueprint. The blueprint depicts a service-aware, IP/MPLS network layered on state-of-the-art packet microwave and DWDM optics technology. A service-aware capability is particularly crucial for a converged network that carries mission-critical operational and IT traffic. At the same time, airport operators need to implement this blueprint without compromising the performance of mission-critical applications, such as air traffic control (ATC), anti-collision systems, emergency communications, CCTV and SCADA.

Figure 2. Airport network transformation blueprint



Executing a successful network transformation requires a comprehensive product portfolio of IP/MPLS routers, optics, and microwave equipment. Equally important is the requirement to complement existing land mobile radio (LMR) or PMR and VHF communications with broadband 4G Long Term Evolution (LTE) radio technology. This enables the deployment of additional ultra-broadband wireless communications services for increased safety and efficiency. For its part, Nokia has an innovative and field-proven product portfolio that has been deployed in mission-critical networks around the world (Figure 3).

Figure 3. Nokia airport network transformation product portfolio



Network modernization with an IP/MPLS network

The Nokia IP/MPLS network solution is not just a standard IP/MPLS network; it's a service-aware, converged IP/MPLS network, fully integrated with transport technology.[2] For these reasons, it plays an integral role in airport operators' plans to modernize their networks.

A converged network architecture achieves savings and significantly increases efficiencies. Even so, there are always concerns that, with network transformation, performance will degrade, jeopardizing application performance-particularly mission-critical applications such as ATC, the anti-collision system, CCTV, SCADA, emergency communications and PMR/LMR. As a result, it is imperative that the network solution have the following attributes to ensure performance:

1. Flexible, service-aware VPN for optimal application delivery and multi tenancy operations Flexible VPN configuration

A virtual private network (VPN) service is necessary to allow multiple tenants to share the same infrastructure. The transport of multiple tenants' applications data on a converged network requires the complete separation of forwarding tables for IP and Ethernet, as well as cross-connect virtual circuits to assure traffic isolation and protection from external attempts to penetrate the network. To support the wide and diverse set of applications deployed by tenants, a flexible VPN portfolio capable of supporting Layer 1, Layer 2, and Layer 3 VPNs-in a point-to-point, multipoint, or hierarchical configuration-is also essential.[3] With this service versatility, operators can design and implement a VPN to deliver traffic optimally for any application. To support agency collaboration, techniques such as IP route leaking can also be used with a stateful firewall to enable inter-VPN communications. Table 1 encapsulates how different VPN technologies can be mixed and deployed for different applications.

[2] For more discussion on attributes of a converged IP/MPLS network, please read the white paper entitled "MPLS for Mission-Critical Networks"

[3] For a more detailed discussion of MPLS-based VPN, please read "MPLS for Mission-Critical Networks: Converging robust, reliable services for critical applications"

Table 1. Multiservice VPN supporting all applications

Service	Service Type	Remark
Airline office	IP VPN	IP service facilitates multi-point communication
CCTV	Hierarchical VPN	PIM-enabled IP core with Ethernet pseudowire access
IP telephony (VoIP)	IP VPN or hierarchical IP VPN	IP forwarding with high QoS performance
Tenants network	VPLS	L2 service waives the need to manage tenant's IP address
Passenger display, digital signage	VPLS with IGMP Snoop or multicast VPN	IGMP Snoop in VPLS and LANs for optimized traffic delivery
Land mobile radio	Point-to-point VLL	Integrated synchronization
Security alarm	Dry contact port to SNMP alarm	Translate dry contacts status to SNMP alarms

QoS management

In a converged network carrying numerous applications, service awareness is crucial for application performance assurance. As application traffic enters the network edge, each application is assigned different forwarding classes (Table 2). The edge router treats each application's traffic with an individualized quality of service (QoS) policy, including its own set of traffic queues and traffic rates. This ensures that no application can be sent beyond the agreed rate, and thus negatively impact the rest (Figure 4). Hierarchical QoS renders further flexibility to each service to consume its assigned bandwidth.

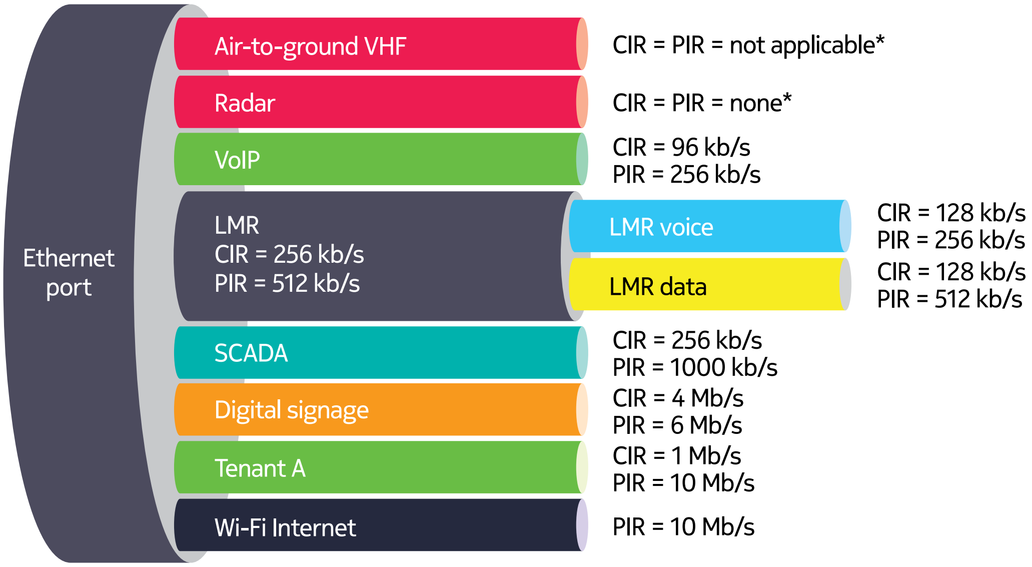
Table 2. A QoS classification example

Application	Forwarding Class
Radar, Air-to-ground VHF communications	High-1
VoIP, LMR/PMR voice	Expedited forwarding
SCADA	High-2
LMR/PMR data	Low-1
Tenants/digital signage	Assured forwarding
Wi-Fi Internet	Best effort

Cross-layer OAM

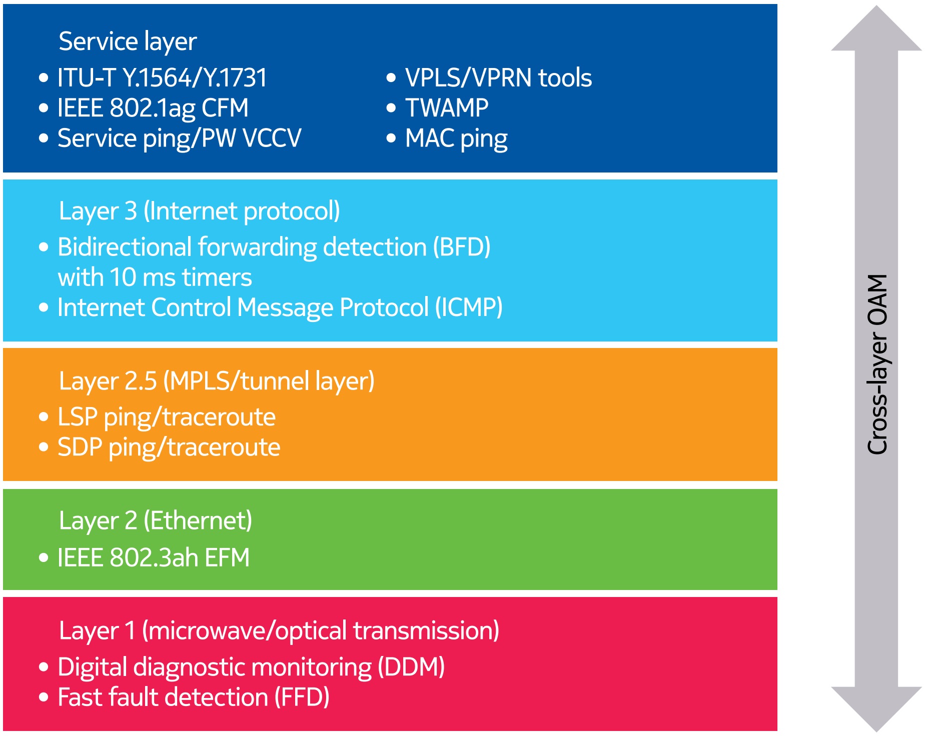
To help operators operate, monitor, and troubleshoot networks, the operations, administration, and management (OAM) tool is crucial (Figure 5). A multi-layer OAM suite provides operators with a wide range of capabilities to monitor and operate the network. In addition to the traditional OAM tool at the transport, link, and network layers, service layer OAM measurement allows operators to continuously monitor delivery performance for VPNs carrying mission-critical applications. This lets them take pre-emptive measures, if necessary. Depending on the type of VPN, OAM tools such as ITU-T Y.1564/Y.1731, service-level CPE and MAC pings are essential to monitor each VPN's health to ensure that the application's connectivity and QoS objectives are met at all times. With the ITU-T Y.1564 methodology, Ethernet test frame generation as a test head is another useful OAM tool that verifies availability of service bandwidth, as required.

Figure 4. Service-aware QoS ensures service-based bandwidth resource partition



*Traffic is always serviced regardless due to its TDM nature

Figure 5. A cross-layer OAM suite


Service layer
• ITU-T Y.1564/Y.1731
• IEEE 802.1ag CFM
• Service ping/PW VCCV
• VPLS/VPRN tools
• TWAMP
• MAC ping
Layer 3 (Internet protocol)
• Bidirectional forwarding detection (BFD) with 10 ms timers
• Internet Control Message Protocol (ICMP)
Layer 2.5 (MPLS/tunnel layer)
• LSP ping/traceroute
• SDP ping/traceroute
Layer 2 (Ethernet)
• IEEE 802.3ah EFM
Layer 1 (microwave/optical transmission)
• Digital diagnostic monitoring (DDM)
• Fast fault detection (FFD)
Cross-layer OAM

2. High scalability for future growth

To meet future application needs, the network must scale in capacity, control plane, and link bandwidth. An IP/MPLS router family ranging from a terabit core router supporting a 400 Gb/s slot in a central office to a multi-gigabit, hardened outdoor router enables operators to extend and scale IP/MPLS from the airport building into the field, including runways and surrounding countryside. The net result is an extensive network covering the whole area.

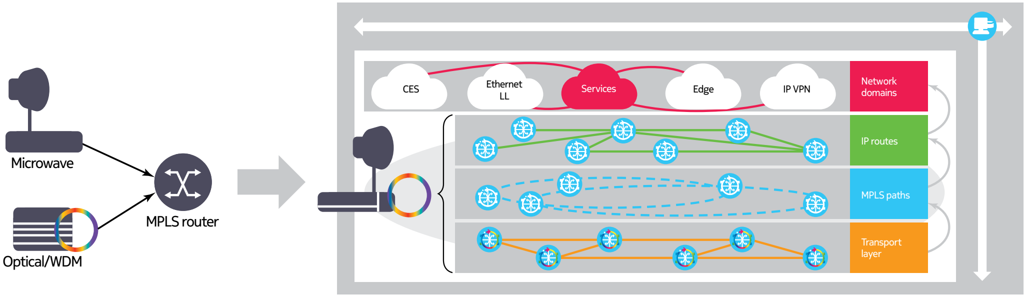
Advanced technologies, such as optical coarse wavelength division multiplexing (CWDM) and DWDM, high-order microwave modulation, MPLS-aware compression and Cross-Polarization Interference Cancellation (XPIC) are effective means to maximize the use of deployed fiber and microwave spectrum to handle future traffic growth.[4]

[4] Consult the blog for a more detailed discussion of the strategy to increase microwave link capacity:

3. Tight integration of optical and microwave transmission for operational elegance

Whether it's an environmentally controlled office or a remote outpost, the network needs to reach all sites. Different transmission technologies, such as optics or microwave, must be used flexibly. Modern IP/MPLS routers now have natively integrated transmission technologies, such as CWDM, DWDM and microwave. Instead of deploying individual nodes and disparate network managers, a converged network with an IP/MPLS router and consolidated transmission layer can be managed by a cross-layer network manager (Figure 6).

Figure 6. Cross-layer network manager for an IP/MPLS router integrated with transmission technology



4. Strong resiliency for high survivability

Any airport network outage entails operations disruption and economic loss. It can even impact airport and flight safety. It's imperative, therefore, that the network is robust, providing strong resiliency like SDH/SONET legacy networks.

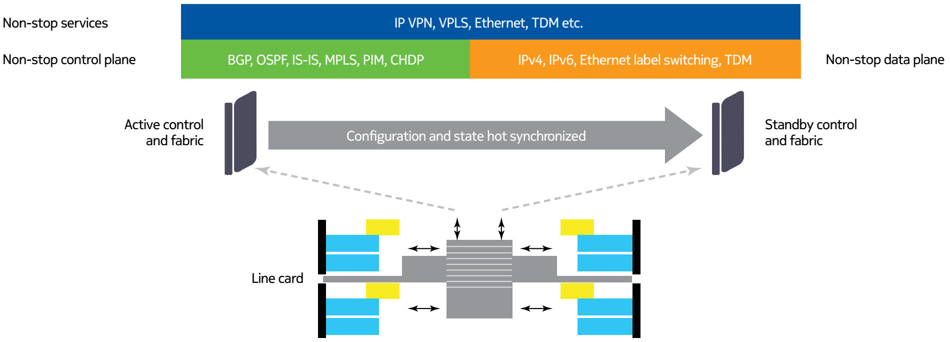
An IP/MPLS converged network is designed for high resiliency at each network level-from transmission to the service layer (Table 3). If a network failure occurs, the network uses a best-fit approach to coordinate multiple recovery mechanisms at all layers to achieve the best restoration performance.

Table 3. Multi-layer resiliency and recovery protection

Service layer	• PW redundancy • MC-LEG/MC-APS
IP layer	• IP ECMP • Non-stop routing • VRRP
MPLS layer	• MPLS FRR/standby LSP/ECMP • Non-stop signaling
Link layer	• 802.3ad Ethernet LAG • ML-PPP/ATM IMA
Transmission layer	• SONET/SDH 1+1 APS • Microwave 1+1, N+0, XPIC

For the IP/MPLS router, a nodal control and hitless switching complex capability with hitless 1+1 protection that encompass non-stop routing, signaling, and services in a compact platform, is also a key redundancy protection mechanism. If the control and switching complex fail, the switching to standby complex is undetected by other network nodes. This ensures network stability, does not disrupt applications, and maintains airport operations continuity (Figure 7).

Figure 7. The paradigm of non-stop networking


Non-stop services
IP VPN, VPLS, Ethernet, TDM etc.
Non-stop control plane
BGP, OSPF, IS-IS, MPLS, PIM, CHDP
IPv4, IPv6, Ethernet label switching, TDM
Non-stop data plane
Active control and fabric
Configuration and state hot synchronized
Standby control and fabric
Line card

Just as important, a network that carries mission-critical traffic demands network vigor that can withstand multiple fault failures. The network must be multi-fault tolerant as long as physical reachability exists so that the airport can continue to operate. It is noteworthy that other types of packet transport technology, such as Carrier Ethernet, cannot offer the same level of multiple fault resiliency as IP/MPLS.[5]

[5] For more detailed discussion, please read "MPLS for mission-critical microwave networks: Building a multi-fault tolerant microwave network.".

5. Rich legacy interface portfolio[6] for seamless TDM migration

In many airports, legacy applications and TDM-based equipment are still in service. This is particularly true of mission-critical equipment used in air traffic control, including radar, air-to-ground VHF radio, PMR communication systems and SCADA. To migrate TDM applications to a converged IP/MPLS network, it is imperative that legacy interfaces, such as E1/T1, ITU-T G.703 co-directional, E&M, FXS/FXO and serial are supported and that VPN services can be provisioned within an acceptable range of delay and jitter. To ensure a smooth migration process, network operators must also clearly define and understand applications' QoS requirements, as well as implement engineering guidelines when designing and deploying their networks.[7]

6. Strong network protection for secure operation

The airport is the air transportation hub of both passengers and freight. Any network disruption due to a cyberattack can lead to air traffic chaos, economic loss, and possibly even loss of human life. To help airport operators address the broad spectrum of security challenges, the American Institute of Aeronautics and Astronautics (AIAA) has taken the initiative to create an aviation cybersecurity framework.[8]

Following the ITU-T X.805 security framework based on the Nokia Bell Labs security model to fortify a network perimeter, security considerations need to be given to the infrastructure, as well as the network and services layers. For the infrastructure layer, it is necessary to protect management, control, and data planes with comprehensive authentication and logging, packet filtering, and IP Security (IPSec). For the services layer, features such as service-aware network group encryption (NGE), which encrypts at the MPLS layer, stateful firewall and network resource partitioning, are pivotal to defend service integrity.[9] Encryption at the optical and microwave layers is also available to protect the data.[10]

[6] The Nokia 7705 SAR product family has a broad portfolio of legacy interfaces. Please read the 7705 SAR Legacy Interface Card data sheet

[7] For a detailed discussion of TDM migration, please read "Transformation of mission-critical communications networks: Migrating from SDH/SONET networks to IP/MPLS networks.".

[8] https://www.aiaa.org/uploadedFiles/Issues_and_Advocacy/AIAA-Cyber-Framework-Final.pdf

[9] For a more detailed discussion of network security, please read "7705 Service Aggregation Router: Security overview for mission-critical networks" and "Seamless Encryption for Mission-Critical Network".

[10] For transmission layer encryption at optics and microwave layer, please read footnote 12 below and "Security for Microwave Links: Risks and Mitigations for Point-to-Point Microwave", respectively.

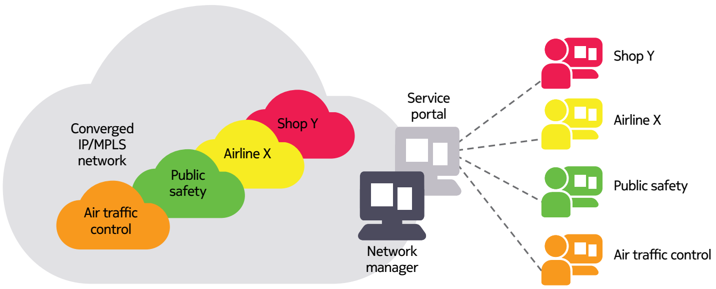
7. Dynamic management

The traditional boundaries of element, network, and service management have made the tasks of service provisioning, network configuration, performance monitoring and troubleshooting complicated, cumbersome, and error prone. An effective cross-layer, service-aware manager can simplify the complexities. The Nokia 5620 SAM helps operators achieve significant efficiencies with an easy-to-use GUI, service templates and scripting, a scalable collection of network and OAM statistics-in addition to powerful cross-layer fault correlation.[11]

Airports operate in multi-tenant settings and serve a broad variety of clients. These can include government agencies, such as customs and transportation security, large enterprise such as airlines, and small- and medium-size enterprises, such as shops and restaurants. Moreover, each of these tenants employ different applications-from mission-critical radar systems, to CCTV video, to simple but business-critical point-of-sale terminals. As a result, airport operators must be able to handle very different communications requirements-for connectivity both in and outside the airport to the Internet and headquarters.

On top of that, IT departments of individual agencies and tenants may want to view the performance and status of their services, as well as provision and modify service parameters. To address this challenge, airport operators can make available to each client a service portal with a tailored span of network and scope-of-command control. With this portal, clients can have instant access to their own portion of the network and perform tasks within the scope-of-control policy (Figure 8). Furthermore, this helps airport operators to offer better service to their customers while reducing operations costs.

Figure 8. Service portal allows users to manage their own span of network



[11] Click here to learn more about how the Nokia 5620 SAM helps operators manage networks effectively.

8. Readying for future evolution to SDN[12]

A converged IP/MPLS WAN solution can provide a robust, resilient, QoS-enabled, fully managed, shared, converged network that scales and reliably connects numerous agencies and applications. With the use of MPLS-traffic engineering, operators can also have full control of QoS performance for different services. For example, services carrying mission-critical operational voice communications need to be placed on short-latency paths, while bandwidth-intensive services need to be placed on high-bandwidth paths. The traditional mode of operation is to first use off-line tools to compute a suitable path to fulfill a service requirement; it then gets provisioned by means of the network manager. In this case, even if bandwidth consumption decreases over time, the path remains open until the next cycle of network optimization. This can lead to inefficient use of network resources. If users need a new application, they will have to wait for network operators to provision a new service-a delay of days or even weeks.

As applications powered by cloud computing become prevalent, they are also becoming more dynamic. Bandwidth requirements and traffic patterns can quickly change depending on the seasons and time of the day. This makes it necessary for the users themselves, within an assigned boundary, to have more control of network resources.

The software-defined network (SDN) paradigm provides a dynamic and more efficient way to define, provision, and activate services in order to respond rapidly to changing needs. Leveraging centralized intelligence collected in the network can be of great assistance. This intelligence includes utilization and real-time delay performance, as well as powerful analytics and self-tuned adaptive routing algorithms. Through a standard RESTful API, services can be provisioned and placed on the best path, fulfilling QoS requirements while also optimizing overall use of network resources. If bandwidth usage of applications in the network changes, paths for all services can be re-calculated to optimize QoS performance and network resource utilization.

Moreover, with network slicing, the shared network can be modeled as multiple, virtual, separate network infrastructures-one for each user or tenant. To satisfy each user's unique requirements, each network slice can have distinct network characteristics, such as low latency. With a service abstraction methodology, service provisioning and parameter changes can even be automated without operator intervention. By giving each user or tenant the flexibility to use the network slice, the tenant can tackle new field situations adeptly and rapidly adopt new cloud-based applications.

[12] Click here for more information on SDN.

As an SDN WAN infrastructure, comprising a robust and QoS-enabled converged network, as well as an intelligent SDN controller-the Network Services Platform (NSP) enables operators to achieve fully unified network control and service management, which can optimally and swiftly use network resources. At the same time, it can also empower users and tenants to respond to the dynamic, on-demand ICT environment ushered in by the cloud era. This new paradigm can also be extended to manage a complex network architecture that spans disparate transport domains, technologies, and vendors.

Conclusion

Airport operators are at a tipping point today. To remain competitive and meet the challenges of rapid air traffic growth, operators are expanding and transforming airport infrastructure. They are relying more than ever on mission-critical and IT applications that require a flexible, agile, and dynamic communications network. The network has become an integral part of airport infrastructure connecting all facilities-from the air traffic control tower, to airline check-in kiosks, to passenger amenities, to Wi-Fi hotspots-both internally and externally to the data center and internet.

A service-aware, converged IP/MPLS network has been proven to meet these requirements. With a comprehensive and innovative product portfolio that covers IP/MPLS, microwave, optical transmission, SDN and LTE-complemented by full suite of professional services, including audit, design, and engineering practices[13]-Nokia has the unique capability and flexibility to help airport operators plan and transform their networks for 2020 and beyond.

Acronyms

1830 PSS	Nokia 1830 Photonic Service Switch
5620 SAM	Nokia 5620 Service Aware Manager
5780 DSC	Nokia 5780 Dynamic Services Controller
7210 SAS	Nokia 7210 Service Access Switch
7450 ESS	Nokia 7450 Ethernet Service Switch
7705 SAR	Nokia 7705 Service Aggregation Router
7750 SR	Nokia 7750 Service Router
7950 XRS	Nokia 7950 Extensible Routing System
9412	Nokia 9412 eNodeB Compact e-NodeB
9471 WMM	Nokia 9471 Wireless Mobility Manager

[13] Click here to learn more about professional services

9500 MPR	Nokia 9500 Microwave Packet Radio
9711	Nokia lightRadio™ 9711 Indoor Base Stations
9712	Nokia lightRadio™ 9712 Outdoor Base Stations
9926	Nokia 9926 eNodeB
AIAA	American Institute of Aeronautics and Astronautics
ATC	air traffic control
ATM	asynchronous transfer mode
BGP	Border Gateway Protocol
CCTV	closed circuit television
CES	circuit emulation service
CIR	Committed Information Rate
CWDM	coarse wavelength division multiplexing
DHCP	Dynamic Host Configuration Protocol
DWDM	dense wavelength division multiplexing
E&M	earth and magneto
ECMP	equal-cost multipath
eNodeB	Evolved Node B
FR	Frame Relay
FRR	Fast Reroute
FSO	Foreign xChange Office
FSX	Foreign xChange Subscriber
ICT	information and communications technology
IGMP	Internet Group Management Protocol
IMA	Inverse Multiplexing for ATM
IPSec	IP Security
IS-IS	Intermediate System-to-Intermediate System
IT	information technology
LAG	Link Aggregation Group
LMR	land mobile radio
LSP	label-switched path

LTE	Long Term Evolution
MC-APS	Multi-chassis Automatic Protection Switching
MC-LAG	Multi-chassis Link Aggregation Group
ML-PPP	Multilink Point-to-Point Protocol
MPLS	Multiprotocol Label Switching
NGE	network group encryption
OAM	operations, administration and maintenance
OSPF	Open Shortest Path First
PDH	Plesiochronous Digital Hierarchy
PIM	Protocols for IP Multicast
PIR	Peak Information Rate
PMR	professional or private mobile radio
PW	pseudowire
QoS	quality of service
SCADA	Supervisory Control and Data Acquisition
SDH	Synchronous Digital Hierarchy
SNMP	Simple Network Management Protocol
SONET	Synchronous Optical Network
TDM	time division multiplexing
VHF	very high frequency
VLL	virtual leased line
VoIP	voice over IP
VPLS	virtual private LAN service
VPN	virtual private network
VRRP	Virtual Router Redundancy Protocol
VSC	Virtualized Services Controller
VSD	Virtualized Services Directory
Wi-Fi®	Wireless Fidelity
XPIC	Cross-Polarization Interference Cancellation

References

1. Nokia 1830 Photonic Service Switch.
2. Nokia 5620 Service Aware Manager.
3. Nokia 7210 Service Access Switch.
4. Nokia 7450 Ethernet Service Switch.
5. Nokia 7705 Service Aggregation Router.
6. Nokia 7750 Service Router.
7. Nokia 9500 Microwave Packet Radio.
8. International Engineering Task Force. RFC 4090: Fast Reroute Extensions to RSVP-TE for LSP Tunnels. May 2005.
9. International Engineering Task Force. RFC 4364: BGP/MPLS IP Virtual Private Networks (VPNs). February 2006.
10. International Engineering Task Force. RFC 4553: Structure-Agnostic TDM over Packet (SAToP). June 2006.
11. International Engineering Task Force. RFC 5086: Structure-Aware Time Division Multiplexed (TDM) Circuit Emulation Service over Packet Switched Network (CESoPSN). December 2007.
12. International Engineering Task Force. RFC 6718: Pseudowire Redundancy. August 2012.

Nokia Oyj
Karaportti 3
FI-02610 Espoo
Finland
Tel. +358 (0) 10 44 88 000

Product code: PR1509014420EN

nokia.com