NOKIA

Port digitalization through a converged wireless network

White paper

NOKIA

Contents

Port terminals must digitalize to meet expanding demand	3
Rethinking the wireless network	3
The converged wireless network: key to port digitalization	5
Overview of the converged wireless network blueprint	5
Service convergence	6
Utmost end-to-end resiliency for reliable communications	7
Deterministic QoS for assured data delivery	10
Robust network defense for secure communications	11
Evolving for the future	11
Seamless data center fabric interworking	11
Machine-to-machine communications	12
The coming of 5G	12
Summary	13
Abbreviations	13

NOKIA

Port terminals must digitalize to meet expanding demand

Port terminals are the nexus of the sea freight industry where container shipping and land transport meet. They play a critical role in moving goods and materials essential for international commerce and global supply chains.

As the world economy expands, sea freight increases. To serve a growing freight volume and stay competitive, port terminal operators need to increase handling capacity and improve efficiency while maintaining safety. They also aim to reduce carbon emissions for sustainability.

To meet these challenges, many port terminal operators are embracing and investing in digitalization. They seize digital technology advancement and adopt smart applications across their operations. These range from remote control and automation of container handling equipment (CHE) such as rubber-tired gantry (RTG) cranes and straddle carriers to predictive maintenance to IoT telemetry.

Rethinking the wireless network

Digitalization requires a reliable, efficient and secure communication network to connect application subsystems like programmable logic controllers (PLCs) or cameras mounted on CHE and in the control center. Some of these applications are delay-sensitive or bandwidth-intensive (see Table 1). Some require Layer 2 Ethernet connectivity while some Layer 3 IP with multicast. As CHE is mobile, the communication infrastructure is naturally built on wireless technology, which has limited bandwidth when compared to fiber, and only primitive network service capability. Supporting a mixed set of services as in Table 1 places immense strain on today's wireless networks.

Table 1. Typical applications and associated QoS requirements

	Latency tolerance	Bandwidth	Reliability	Criticality	Connectivity required
CHE remote control with Profinet	Low	Low	High	High	Layer 2 Ethernet
Video surveillance	Medium	High	Medium	High	Layer 3 IP multicast
CHE monitoring	Low	Low	Medium	Medium	Layer 3 IP
Telemetry	High	Low	Low	Medium	Layer 3 IP

Unleashing the full power of digitalization requires a rethink of the wireless network to meet the following requirements.

Service convergence over wireless network

The concept of service convergence is new for wireless networks. Service convergence is about dividing a physical network into dedicated segregated virtual partitions for different application domains such as automation control and CCTV. The traditional network paradigm for service convergence in a wireless network such as Wi-Fi can be one of two options.

1. Deploying multiple wireless networks (Figure 1a)
2. Resorting to virtual network partitioning, e.g., with the use of a service set identifier (SSID) in Wi-Fi networks (Figure 1b); a new SSID is created with every new industrial application.

Option 1 demands high network operation costs. It also impedes new application deployment, because a new network is required. Option 2 requires a new network partition to be created and administered for each application, which still stifles deployment velocity. Furthermore, network partitions lack proper application awareness to meet the network quality of service (QoS) such as the delay and bandwidth needed by real-time applications like automation or remote control. When bandwidth resource contention occurs, the network would be challenged to constantly maintain the right level of QoS for each application. The ideal option is to harness the multiservice capability of IP/MPLS to usher in application awareness. This eliminates the need to build multiple networks or administer multiple partitions (Figure 1c).

Figure 1a. Multiple Wi-Fi networks

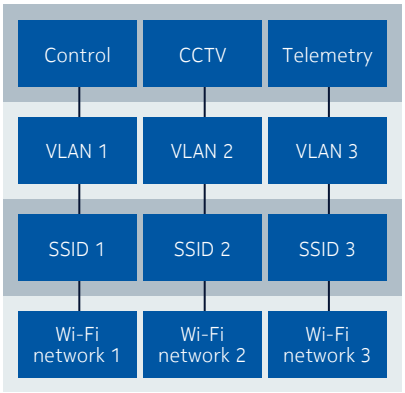


Figure 1b. Wi-Fi network with SSID partitions

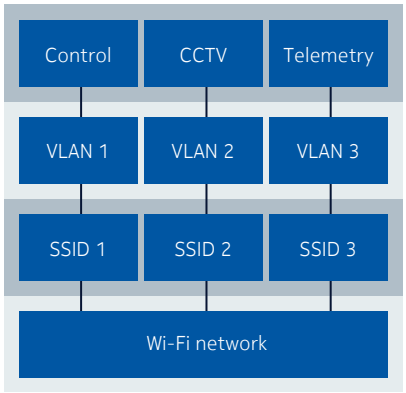
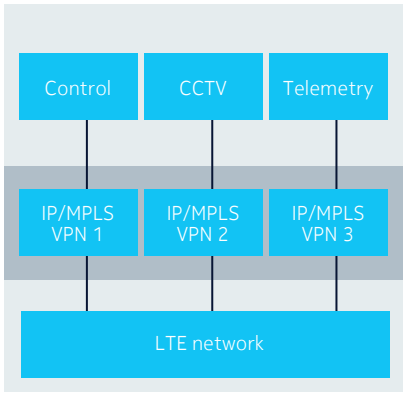


Figure 1c. Application-aware converged wireless network



Utmost resiliency

Digital applications require connectivity 24 x 7. Any communication outage can disrupt the operation or degrade application performance, causing significant productivity loss or even endangering personnel safety. Therefore, operators should strive to design and deploy the network with utmost network resiliency.

Reliable data delivery

Because of a wireless network's restricted bandwidth when compared to that of a fiber network, it is more difficult to constantly deliver data. As a result, deterministic QoS capability is necessary to deliver data in an assured manner for consistent high application performance, particularly for automation and remote control applications.

Rigorous security

Digital transformation ushers in wide use of information and communications technology in terminal operations, expanding the attack surface and engendering new vulnerabilities in the infrastructure. Consequently, cyber security has become a top concern.

Evolving for future needs

Container automation is in its infancy. Most operators are trialling remote control from the control center. In time, CHE can execute automatic gantry and automatic hoisting under human supervision. As the level of automation increases, machine-to-machine (M2M) communications would start to become more common. Furthermore, terminal applications are adopting cloud technology. The wireless network also needs to interwork with the data center fabric network seamlessly.

The converged wireless network: key to port digitalization

To address all these needs, operators need to evolve to a converged wireless network. The rest of this paper provides an overview of the converged wireless network blueprint, then discusses its four essential attributes: service convergence, multi-fault network resiliency, deterministic QoS, and network security.

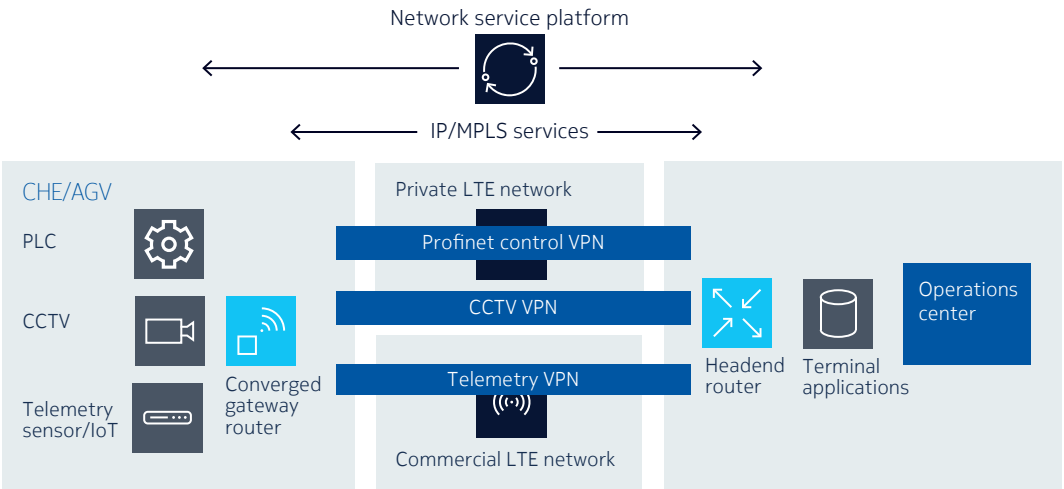
Overview of the converged wireless network blueprint

The network blueprint (see Figure 2) is grounded in standards-based IP/MPLS and LTE. The cornerstone is a converged gateway router mounted on CHE and an automated guided vehicle (AGV). It is an IP/MPLS gateway with an LTE interface that brings IP/MPLS services wirelessly out to CHE and AGV in the docks and the yards with the following capabilities:

- Ubiquitous IP/MPLS services for smart onboard applications including automation, telemetry, global positioning and CCTV
- Advanced Layer 2 (Ethernet) and Layer 3 (IP) VPN services to support Profinet and standard IP applications
- IP multicast for efficient CCTV transport
- Deterministic QoS for delay-sensitive applications such as remote control with Profinet
- Enhanced any-to-any multipoint connectivity for new automation applications that require M2M communications between autonomous equipment in the dock or the yard
- Utmost resiliency to avoid disruptions
- Robust security to address a growing range of cyber security threats.

The converged wireless network runs atop a private LTE (P-LTE) network deployed and operated by port terminal operators using dedicated or shared spectrum. When P-LTE is not feasible due to spectrum unavailability or other reasons, LTE service from commercial carriers is a viable alternative. However, since it is challenging to assure network performance, particularly latency and reliability in a commercial LTE network, the applications supported would be limited to those not requiring stringent delay such as video surveillance, CHE monitoring and telemetry. Real-time applications such as CHE remote control and automation would not be feasible.

Figure 2. Converged wireless network blueprint



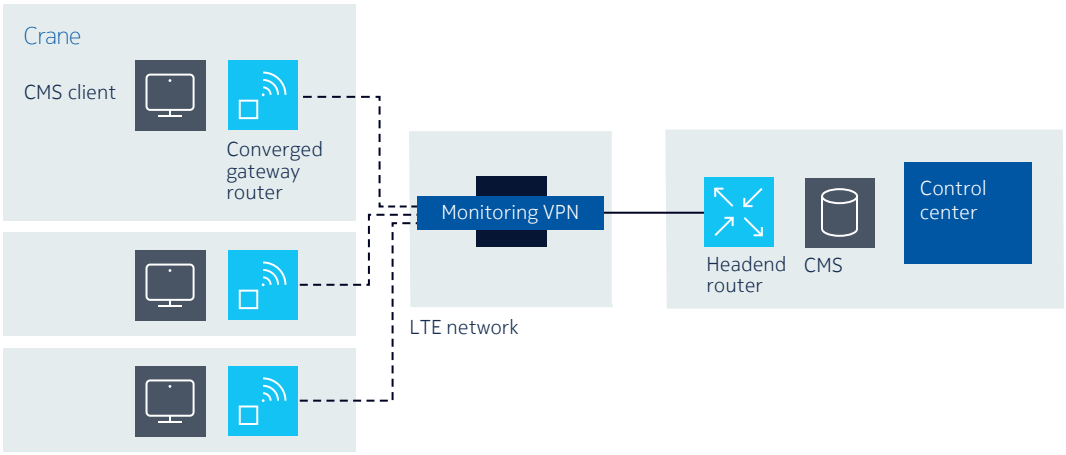
Service convergence

Terminal digitalization ushers in many new, smart applications, heightening the need for service convergence. Harnessing the multiprotocol Layer 2 and Layer 3 service capabilities of IP/MPLS over LTE brings service convergence to container terminals for key use cases ranging from a crane monitoring system (CMS) to Profinet for remote control and automation to CCTV.

CMS with Layer 3 IP VPN

CMS is key for remote real-time monitoring of crane performance and operations that result in improved safety and increased efficiency. IP VPN service provides IP connectivity between remote CMS clients and the central CMS for transmission of crane operational data (Figure 3).

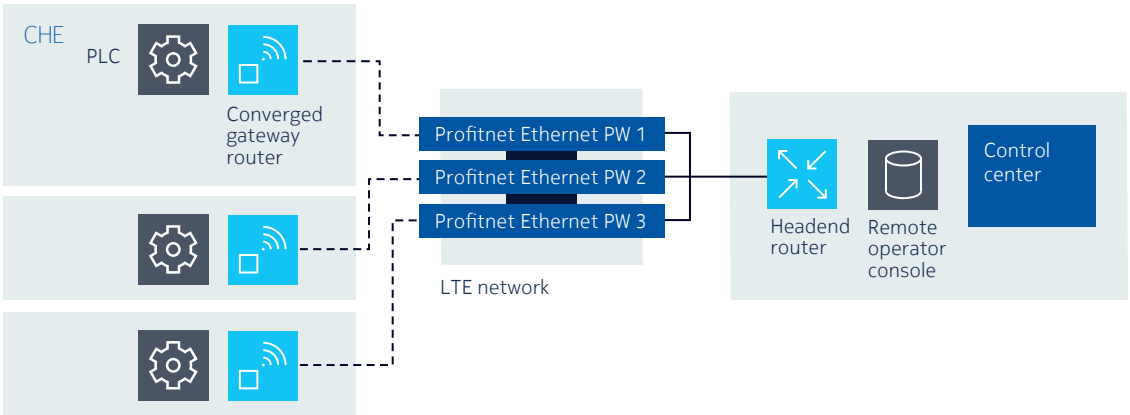
Figure 3. IP VPN for crane management system



Profinet for remote crane control and automation with Layer 2 VPN

Remote control operation can significantly increase efficiency since one person can operate multiple cranes, whereas manually driven cranes require one person per crane. Remote control operation uses Profinet atop Ethernet protocol. Therefore, a Layer 2 VPN using Ethernet pseudowire (PW) technology is ideal to support communication. An Ethernet PW is a point-to-point Ethernet connection linking the PLC on the CHE with a control session on the remote operator console in the control center (Figure 4).

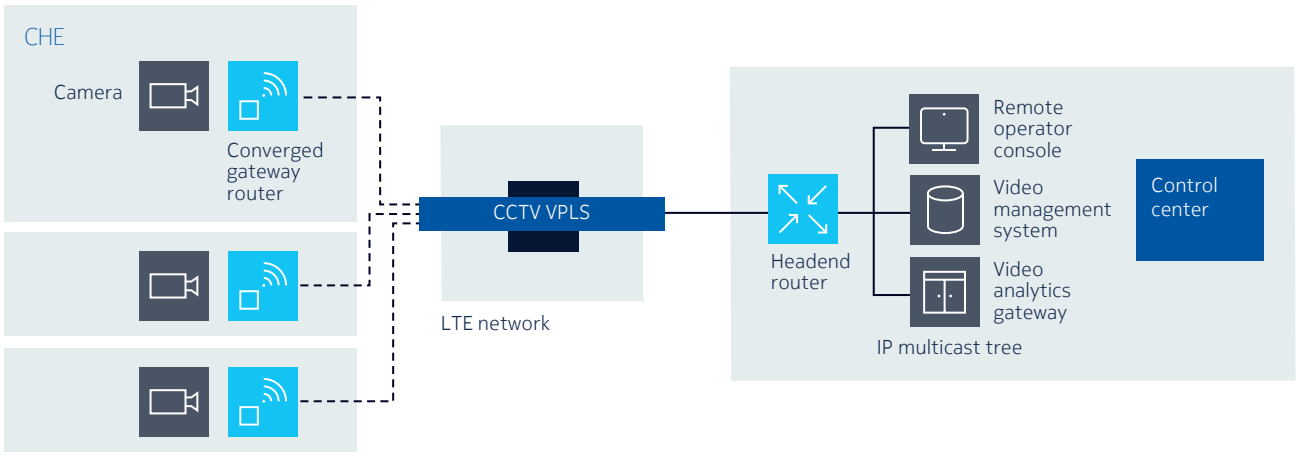
Figure 4. Point-to-point Layer 2 VPN for remote control operations



CCTV

CCTV is pivotal for operators to control or supervise an automated crane remotely. While CCTV cameras continuously stream video to the console, the streams are also sent to the video management system for archiving, as well as a video analytics gateway for real-time anomaly detection. The gateway router sends IP multicast packets with VPLS to the headend router, which will deliver traffic on IP multicast trees (Figure 5).

Figure 5. Multipoint Layer 2 VPN with IP multicast for CCTV



Utmost end-to-end resiliency for reliable communications

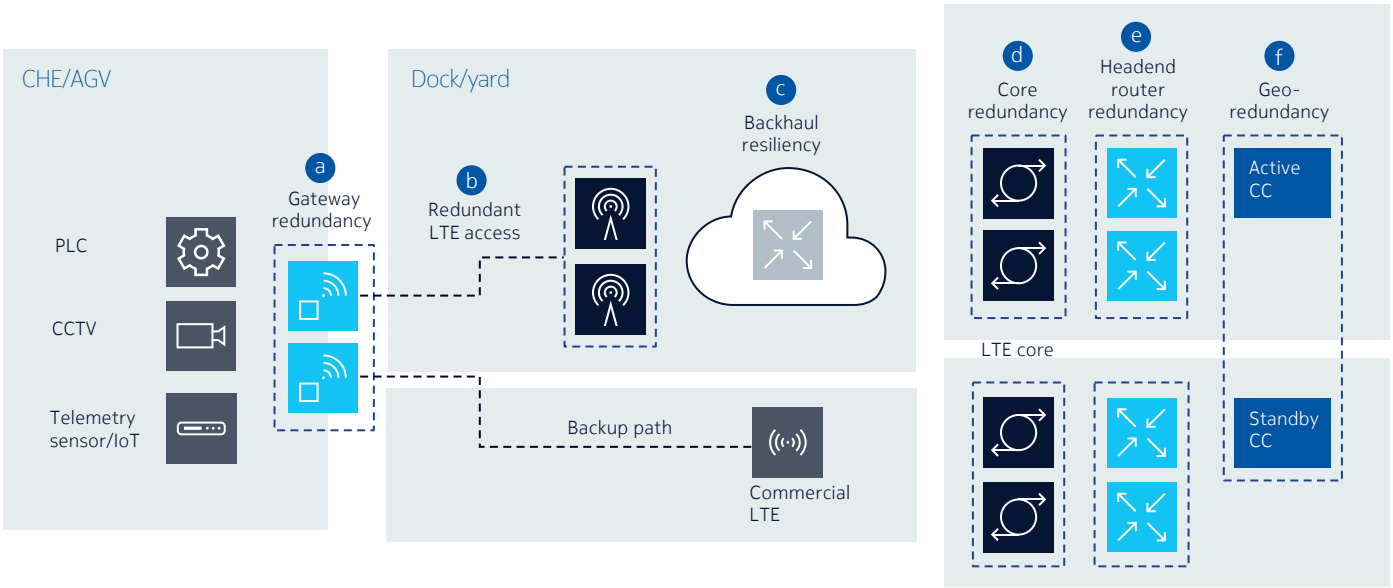
As seen in the converged wireless network blueprint in Figure 2, the scope of the connection is more than just the LTE link between the converged gateway router and the LTE base station (eNB). The connection extends all the way to the headend router in the control center, where terminal applications such as CMS, terminal operating system and video analytics reside.

If there is a fault along the whole communication path, operators would lose oversight and control of the CHE or AGV, affecting safety and productivity. Accordingly, the network needs to have full redundancy protection along the end-to-end communication path (see Figure 6).

The key protected elements in the converged wireless network are:

a. Redundant converged gateway router
b. Redundant LTE access
c. Backhaul resiliency
d. Core redundancy
e. Redundant headend router
f. Geo-redundant control center.

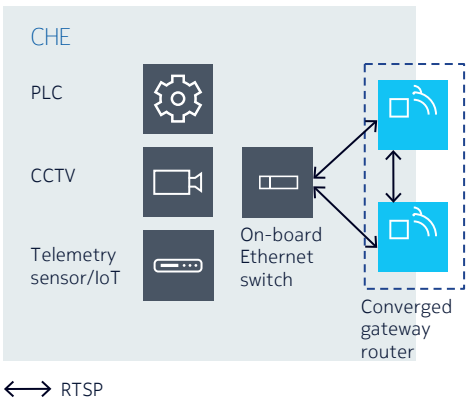
Figure 6. End-to-end network redundancy



a. Redundant converged gateway router

All onboard application traffic is first processed by the converged gateway router. Therefore, it is critical to deploy a redundant pair for high-availability crane operation. The use of Rapid Spanning Tree Protocol (RSTP) with the on-board Ethernet switch can enable rapid redundant switching when the active gateway router fails, quickly restoring connectivity for onboard devices. (Figure 7).

Figure 7. Deploying redundant gateway router pair



b. Redundant LTE access

The gateway router connects with the eNB of the LTE network. If the eNB fails, wireless communications in the area covered by the failed eNB stop completely. Therefore, it is necessary to have highly available LTE access. This can be attained with overlapping eNB coverage. If the applications do not require stringent latency assurance, using commercial LTE service as backup is another redundancy option.

c. Backhaul resiliency

The backhaul network connects all eNBs with the LTE core. While IP/MPLS has many resiliency capabilities, including nonstop routing, fast reroute and secondary label-switched path protection, it is crucial that the backhaul network have rich and diverse connectivity so that IP/MPLS can still reroute data around multiple failure points.

d. Redundant LTE core

The LTE core terminates all LTE radio traffic originated from the converged gateway router. It forwards all data to application servers hosted in the control center. LTE core equipment failure would render the whole network inoperable, stopping all onboard applications.

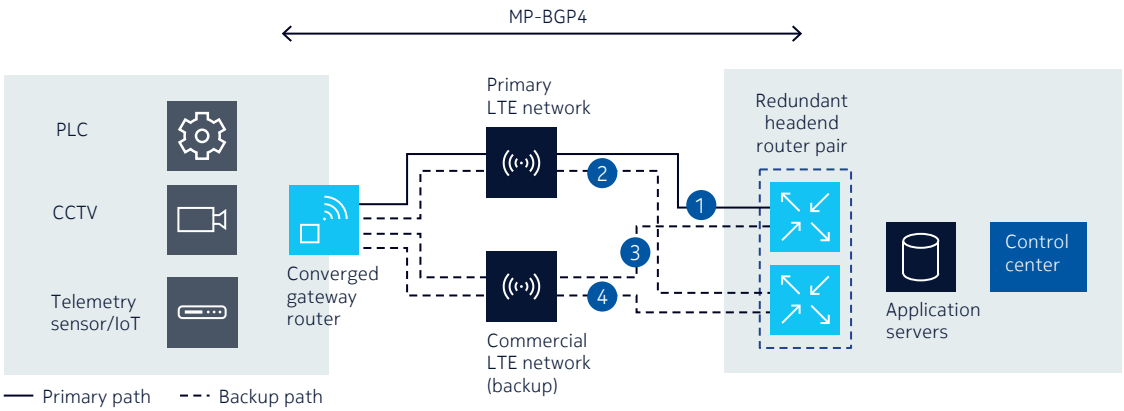
Consequently, it is necessary to deploy the LTE core in high availability (HA) mode, with an active core and a standby core. A typical redundancy implementation requires the standby core to re-establish LTE sessions with all gateway routers during protection switching; this process disrupts all communications for minutes.

HA technology allows the active and standby cores to constantly synchronize the state information of all sessions, enabling graceful switching and eliminating any disruption to all applications.

e. Redundant headend router

The headend router, located at the control center, terminates IP/MPLS services and forwards traffic to application servers. It is imperative that the headend router be protected with node redundancy via backup headend routers located in the control center. If a commercial LTE service is used as a backup, it is essential that the converged gateway router have the capability and scalability to establish multiple Multiprotocol Border Gateway Protocol-4 (MP-BGP-4) control sessions with the redundant headend router pairs via the primary and backup commercial LTE networks (see Figure 8).

Figure 8. Redundant headend router deployed



The gateway router monitors the operational status of all sessions. When the primary headend router fails, the router detects a status change of session and switches traffic from the primary path (Path 1 in Figure 8) to a backup path (Path 2 in Figure 8) to connect to the backup headend router.

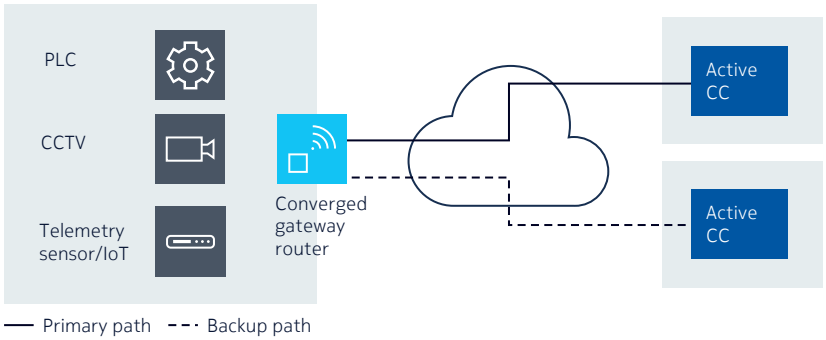
The backup headend router maintains BGP routing information to the gateway routers so they can keep communicating with each other.

If a second failure occurs in the primary LTE network, the router also detects the change of the control session with the backup headend router, then switches from Path 2 to Path 4 in Figure 8. As Path 4 would traverse through a commercial LTE network, this fall back switching option is only for applications that do not require stringent latency assurance.

f. Geo-redundant control center

The control center is the nexus of terminal operations where operators monitor, control and plan. If it goes down, terminal operation stops. Hence geo-redundant protection for the control center is an integral element of the operator's business continuity plan (Figure 9).

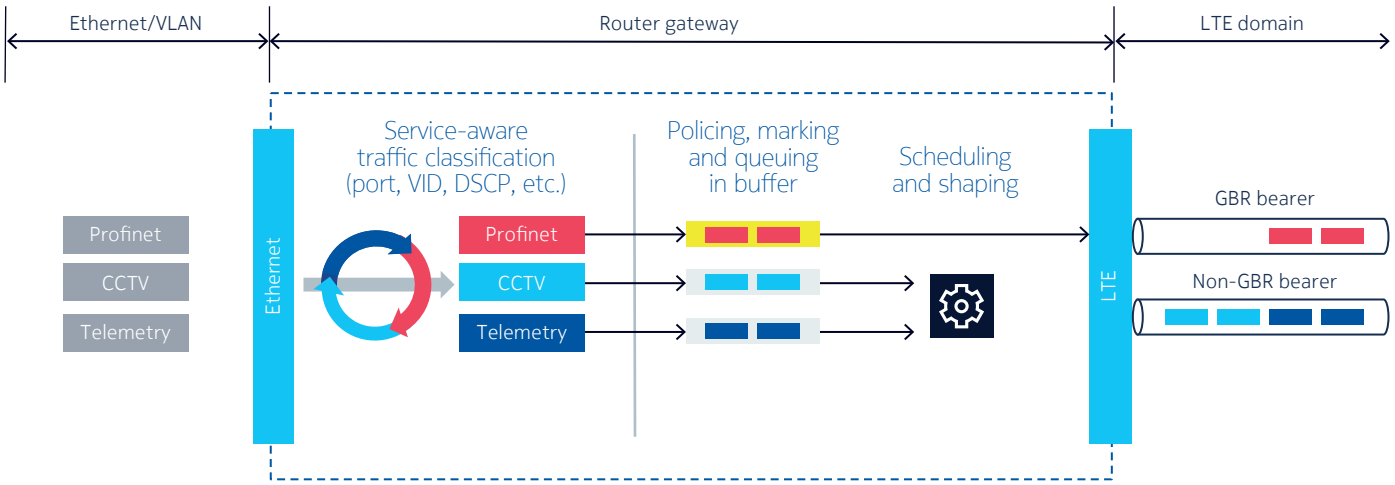
Figure 9. Geo-redundant control centers



Deterministic QoS for assured data delivery

Remote control and automation require deterministic QoS from the network. The router gateway combines the use of Ethernet VLAN ID (IEEE 802.1q), IEEE 802.1p tag, DiffServ, MPLS traffic class and LTE QoS Class Identifier (QCI) for advanced traffic classification, queuing, buffering and shaping to ensure that Profinet control messages are consistently delivered within the delay budget (see Figure 10).

Figure 10. Router gateway provides deterministic QoS with advanced data traffic management

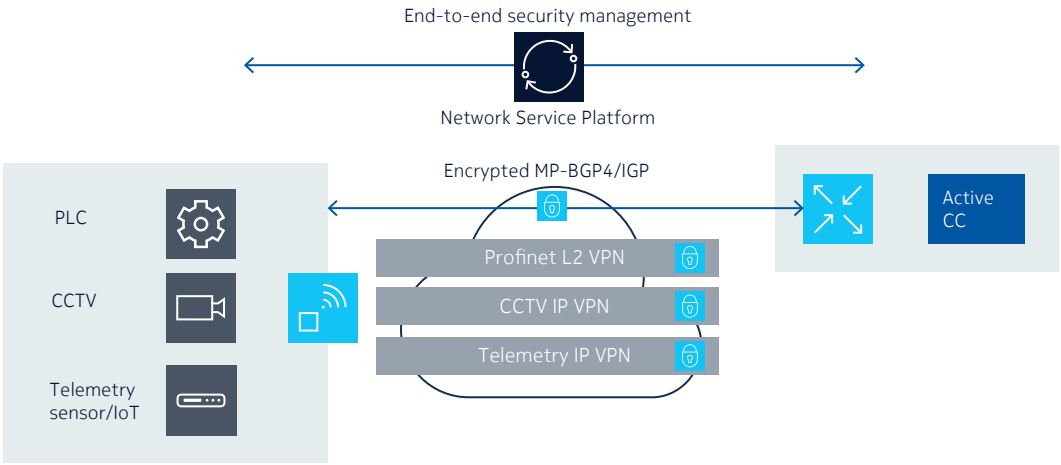


Robust network defense for secure communications

Today's encryption mechanisms were originally designed to protect point-to-point IP flows. They are not designed for a multiprotocol, multiservice, multipoint environment as in a container terminal network.

The converged gateway router has a group-based, service-aware encryption approach called Network Group Encryption (NGE) technology[1], to safeguard traffic on a per-service basis. It also universally encrypts all protocols including Ethernet (which is ideal to protect Profinet messages), IP, and even network control plane traffic like MP-BGP-4 and IGP like IS-IS and OSPF. With service awareness, NGE can be applied on a per-application basis, with each application domain having its own security policy for encryption key and key renewal frequency, all centrally managed from a network services platform (Figure 11).

Figure 11. NGE offers service-aware protection for application and control traffic



Evolving for the future

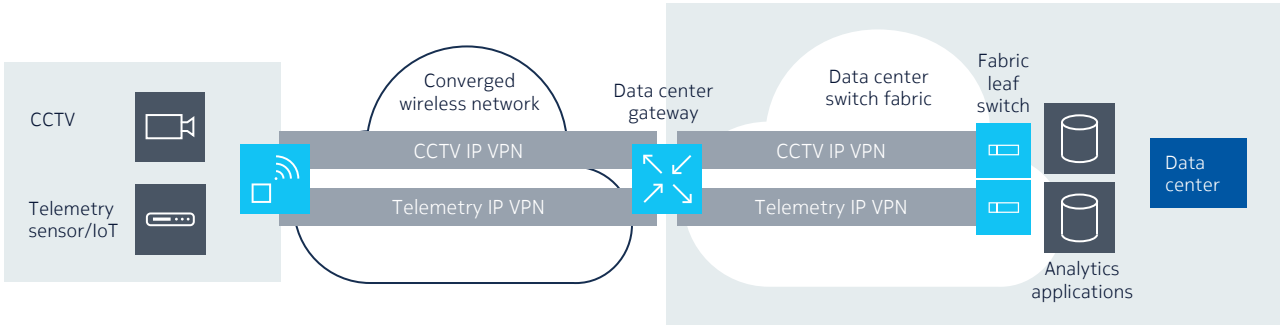
As the digitalization journey continues, operators' needs evolve. The converged wireless network blueprint can also evolve to support future needs.

Seamless data center fabric interworking

More sensors will be installed on CHE as operators start to embrace predictive maintenance and digital twin technologies, which are increasingly cloud-based residing inside their data centers. The IoT sensors would need to communicate with application servers inside a data center. As a result, the VPN services in the converged wireless network need to be able to extend into the data center network fabric. With the use of an IP/MPLS data center gateway, the converged wireless network can have seamless service interworking with the data center switch fabric, forming an end-to-end (E2E) VPN for each individual application domain, which comprises all field sensors and analytics application workloads residing inside data centers (Figure 12).

1 To learn more about NGE, read the Nokia application note "Network Group Encryption"

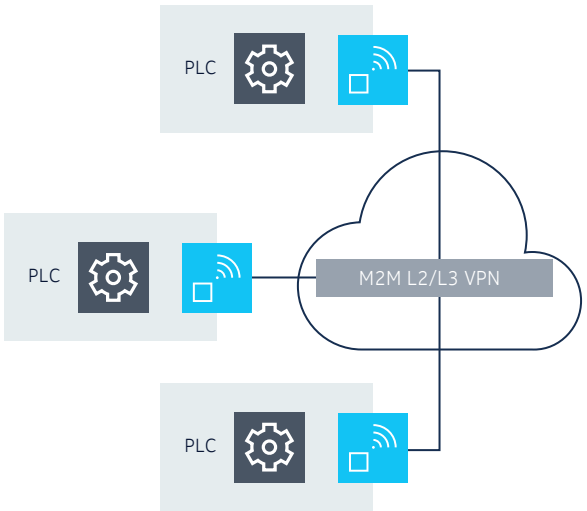
Figure 12. E2E connection between machines and applications in the cloud



Machine-to-machine communications

CHE operation today is mostly manual and is gradually migrating to remote control. As automation technology matures, the level of CHE automation would increase. Accordingly, machine-to-machine (M2M) communications between CHE (e.g. a straddle carrier and an AGV) would become important. With the blueprint, the operator can provision an VPLS or VPRN service wirelessly connecting the CHE equipment, with all converged route gateways peering to each other at Ethernet or IP layer directly, optimizing automation response time (Figure 13).

Figure 13. Converged wireless network facilitates direct M2M communications



The coming of 5G

With its seamless migration path to 5G, LTE is the prevalent choice for critical infrastructure operators to meet their wireless connectivity needs. While LTE can meet the needs of industrial applications today and tomorrow, as we look ahead to 5G, we can begin to imagine new applications such as fully autonomous CHE, the highest level of automation. The converged wireless network blueprint is adaptable and flexible to evolve to 5G for such applications.

NOKIA

Summary

Port terminal operators are embracing digitalization to increase capacity, improve efficiency and drive down carbon emissions. A converged wireless network is foundational to the digitalization journey by providing application-centric communications that enable operators to adopt and harness the power of smart, digital port applications.

With a broad communications product portfolio spanning IP/MPLS and LTE/5G to packet microwave and packet optical transport, along with cyber security, Nokia has the unique capability and flexibility to help utilities transform their networks. This product portfolio is complemented by a full suite of professional services, including audit, design and engineering practices.

To learn more about Nokia for port terminals and our converged IP/MPLS capability, visit our Maritime web page and the award-winning 7705 SAR web page.

Abbreviations

AGV	automated guided vehicle
BGP	Border Gateway Protocol
CHE	container handling equipment
CMS	crane monitoring system
eNB	enhanced Node B
GBR	guaranteed bit rate
IoT	Internet of Things
IS-IS	Intermediate System-to-Intermediate System
LTE	Long Term Evolution
M2M	machine-to-machine
MP-BGP-4	Multiprotocol Border Gateway Protocol-4
MPLS	Multiprotocol Label Switching
NGE	Network Group Encryption
OSPF	Open Shortest Path First
P-LTE	private LTE
PLC	programmable logic controller
PW	pseudowire
QoS	quality of service
RTG	rubber-tired gantry
RSTP	Rapid Spanning Tree Protocol
SSID	service set identifier
VLAN	virtual local area network
VPLS	virtual private LAN service
VPN	virtual private network
VPRN	virtual private routed network

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

Document code: 1419373278534596370 (September) CID210812