Re-imagine the station network for digital rail

White paper

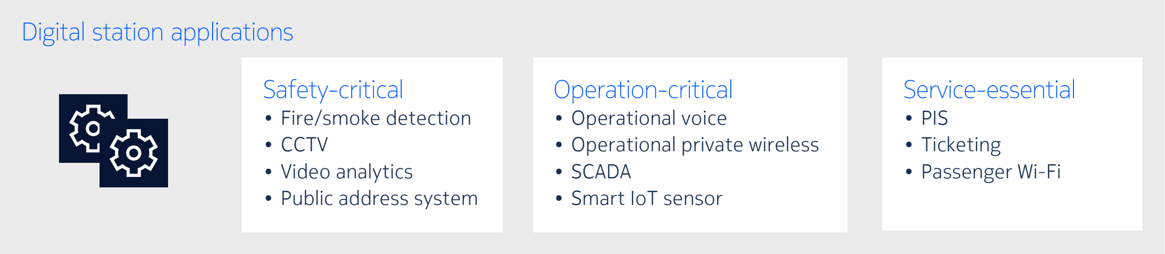
Contents

The advent of digital stations

The rail system is a network of train stations where the journey starts and ends. As mobility needs increase, people are taking the train more often. As a result, more passengers will flow through train stations. Sometimes, train stations even become a popular rendezvous point for citizens to meet, dine and socialize, increasing station usage. To support the traffic growth, train stations need to transform to serve the ever-growing needs of passenger and station operations.

Today, rail operators (abbreviated as operators hereafter) are already using applications such as public announcements and passenger information systems (PIS) in train stations. With an ever-growing number of people using train services and station facilities, operators need to embrace the paradigm of digital stations, adopting more digital technologies such as CCTV and video analytics to improve situational awareness, SCADA and predictive maintenance so as to increase station equipment operational efficiency and reliability, and high-coverage Wi-Fi for passengers.

Figure 1. Operators adopting new and existing digital applications in train stations



Digital station applications

Safety-critical
- Fire/smoke detection
- CCTV
- Video analytics
- Public address system

Operation-critical
- Operational voice
- Operational private wireless
- SCADA
- Smart IoT sensor

Service-essential
- PIS
- Ticketing
- Passenger Wi-Fi

Current station networks fall short of new needs

Digital stations require an expansive station network to connect digital equipment in the stations with the operation and control centers (OCCs). Operators have been operating station networks for many years. Many have Ethernet networks deployed in the station as extended enterprise LANs. This paradigm works well when the number of applications and application subsystems to be connected are few. However, the advent of the digital station ushers in many new applications with new network requirements that stretch beyond current station LAN capabilities. Four major challenges can be identified:

a. Connecting and powering a plethora of equipment with bandwidth for growth

In addition to typical station applications such as operational telephony, ticketing and passenger information displays new applications such as CCTV and Wi-Fi deployed in digital rail stations have cameras and access points expansively installed. With stations hosting more amenities and more passengers, it is no longer uncommon to have more than hundreds of cameras and a few dozen or even hundreds of access points in one station. Some stations would also have time displays in every corner for passengers' convenience. With the increase in station equipment, the access switch in the new station network needs to scale up in Ethernet port density. Also, the access switch needs to provide high wattage for high fan-out of Ethernet with power over Ethernet (PoE) technologies, avoiding separate power cabling.

Furthermore, the volume of data to be transported in the station network has surged immensely. The switch capacity needs to increase and the switch trunk Ethernet port needs to scale beyond 1 Gbps to 10 Gbps for the multitudes of video streams and Wi-Fi data.

b. High resiliency and deterministic quality of service (QoS)

Applications like voice communications, CCTV and public address systems are critical to station safety and situational awareness. Network outages make these applications fail to detect anomalies and to alert passengers and staff about danger in the station. Therefore, the station network needs to support redundancy protection to quickly restore communication service for high application availability.

As the network would carry delay-sensitive data such as emergency voice communications and life-critical applications like public announcement systems (PAS), deterministic QoS is necessary to ensure the data of those applications are delivered with priority.

c. Distribution of time synchronization

Operators are embracing predictive maintenance technology for the rail infrastructure including station equipment such as escalators and ventilation. They need ubiquitous connectivity to connect sensors to monitor the operating conditions of the equipment. As operators deploy new generations of train-to-ground communication systems based on LTE or 5G, they can extend the wireless coverage to cover the station with small cells for such purpose. Bringing in GPS/GNSS signals for time synchronization is very often not feasible, particularly for underground stations. The station network can play a pivotal role to distribute time synchronization using IEEE 1588 and Network Time Protocol (NTP).

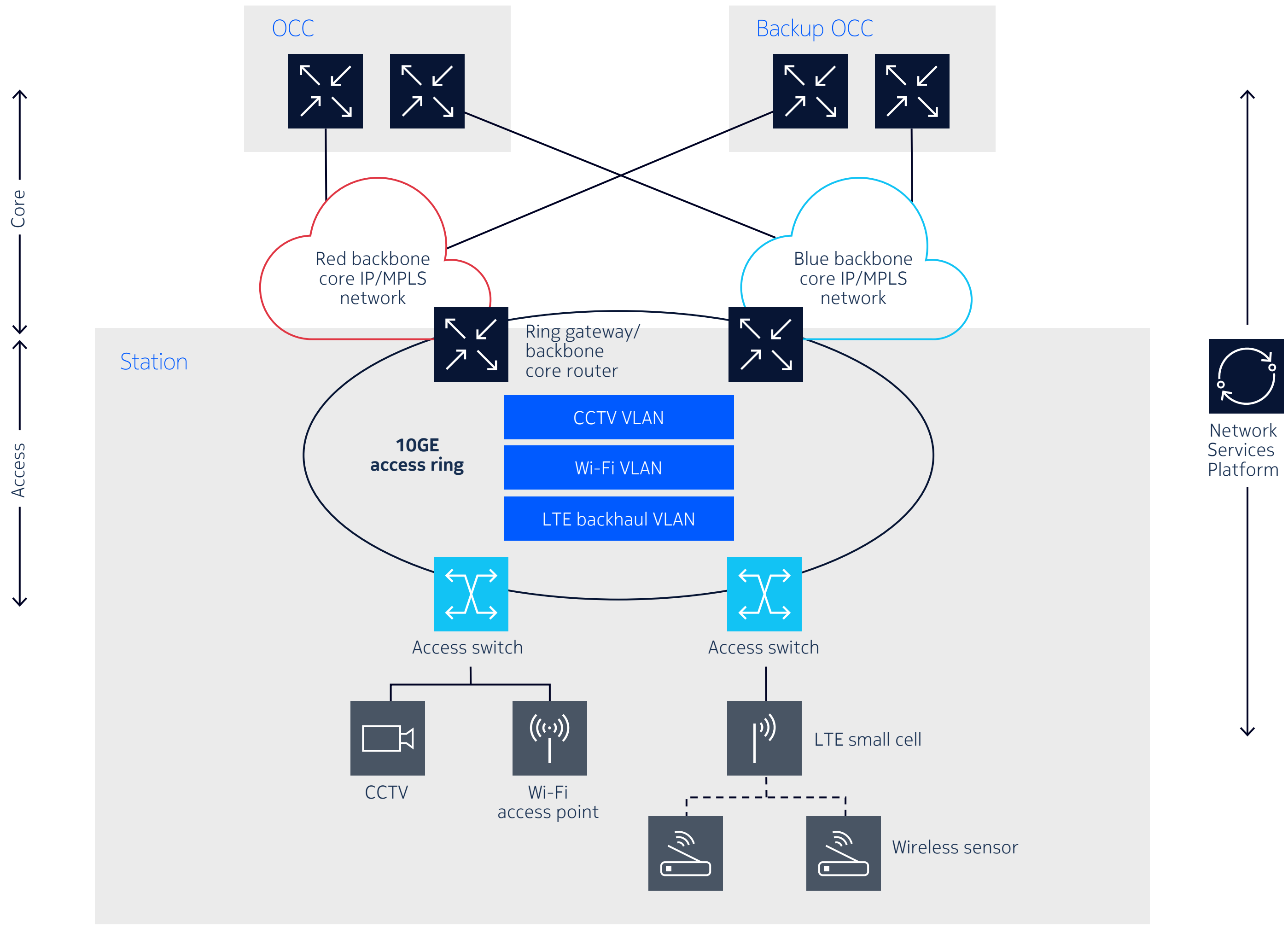
d. Cyber security

With the rise of cyber threats, cyber security has become a top concern for operators. The station network itself needs to evolve to become part of the cyber defense framework.

The Nokia digital station network blueprint

In face of these gaps, operators need to re-imagine their station networks. While the actual network design varies depending on each operator’s requirements and topology constraints, this white paper attempts to build a blueprint network (Figure 2) as a reference architecture that can tackle the challenges explained above.

Figure 2. The Nokia digital station backhaul blueprint



This blueprint comprises an access Ethernet ring that would interconnect to the red/blue redundant backbone core network domains.

In the access ring, instead of 1 Gbps found in station networks today, the blueprint access switch utilizes the fiber system to form a 10 Gbps access ring based on ITU-T G.8032 Ethernet Ring Protection Switching (ERPS) technology.

The ring connects access switches along the way, collecting all data from station equipment at each switch location to the ring gateway router pair in the station. The ring gateway router pair will form the redundant backbone core network pair (red and blue pair) with router pairs in other stations, connecting to OCCs.

The network blueprint is built with:

- Nokia 7210 Service Access Switch – Dxp (SAS – Dxp) as the access switch
- The 7210 SAS-Dxp family has a series of compact, fanless and AREMA-compliant temperature-hardened Ethernet switching platforms with DIN rail-mounting flexibility for a space-constrained outdoor cabinet. With a high PoE port density and large power capacity, it can connect and power many CCTV cameras and VoIP phones using PoE technology (PoE, PoE+, PoE++/HPoE)[1]. It can distribute synchronization with IEEE 1588v2 Packet Timing Protocol (PTP) and NTP.
- Nokia IP/MPLS platform as ring gateway and backbone core router
- Nokia offers a wide and versatile range of IP/MPLS platforms comprising the 7750 Service Router (SR), 7250 Interconnect Router (IXR) and 7210 Service Access Switch (SAS), bringing IP/MPLS services with high performance, scalability and flexibility. Deployed as the access ring gateway, it joins the access network with the redundant backbone core networks, aggregating data from all subtending access rings and delivering them to OCCs over the blue or red backbone core networks with dedicated, tailored IP/MPLS services.
- Nokia Network Services Platform (NSP) for cross-domain cross-layer management
- The NSP is a unified services and network manager, overseeing access domain and backbone core domains. As a cross-domain cross-layer manager, it unifies communications service management and performance management tasks in both the access and backbone core domains, greatly simplifying network operations and enabling operators to respond quickly to new connectivity demand and ensure high end-to-end service performance and reliability.

How the blueprint overcomes the gaps

The station network blueprint supports multiservice. With a service-centric approach, the access switch can scalably offer different point-to-point and multipoint Ethernet services with tailored QoS profiles for each individual station application (Table 1).

Table 1. Application-aware QoS profile reference example

	Latency	Bandwidth	QoS class	Criticality
Emergency call system	Low	Low	High-1	High
PA system	Medium	Low	High-1	High
Time/clock distribution	Low	Low	High-1	High
CCTV	Medium	High	High-2	High
Ticketing system	High	Low	Low-1	Medium
PID	High	Medium	Low-2	Medium
Passenger Wi-Fi	High	High	Best effort	Low

Additionally, the network blueprint brings the following capabilities to overcome the station network challenges described in the earlier section.

[1] Pan-tilt-zoom (PTZ) cameras, Wi-Fi access points and public announcement systems need more than 15 watts. They can benefit from PoE+, PoE++ and HPoE support on the high-wattage switches.

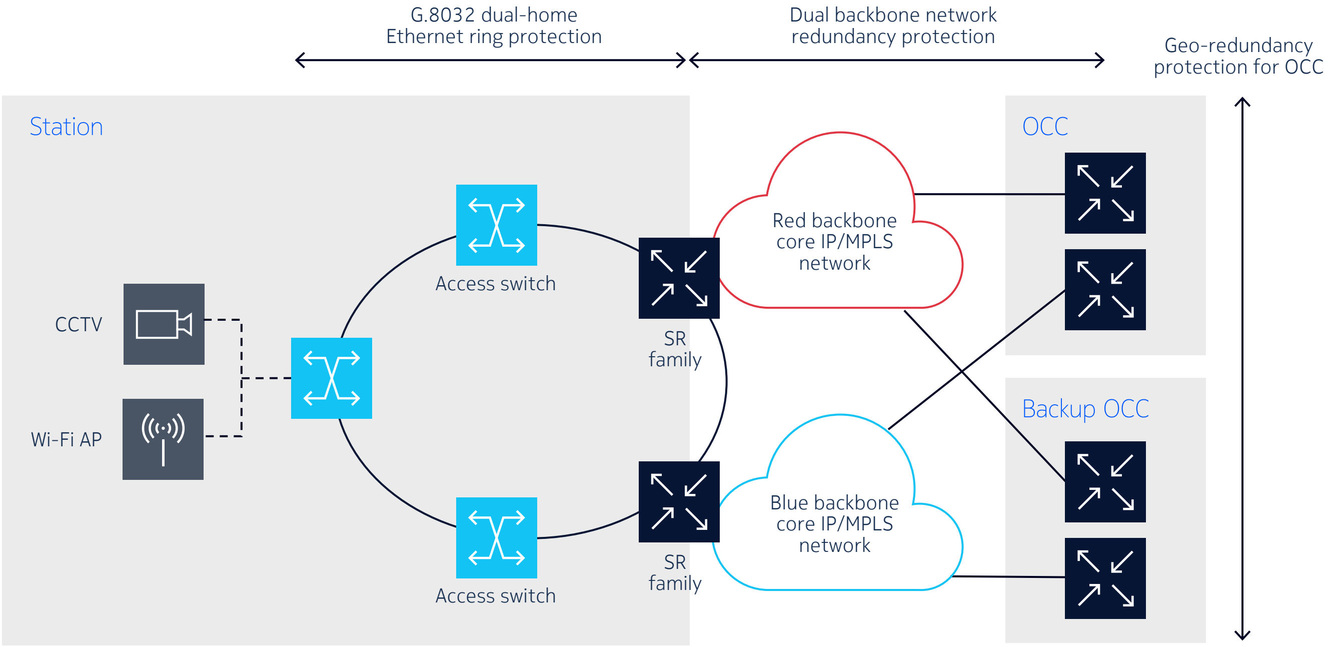
High fan-out 10GE access ring for future data growth

With a compact, space-efficient, DIN-rail mounting-capable chassis, the 7210 SAS-Dxp in the blueprint can tremendously scale up the access ring bandwidth, Ethernet port fan-out and wattage supplied when connecting to multitudes of equipment ranging from CCTV cameras, Wi-Fi access points and VoIP phones. It also supports 10GE (10 Gbps Ethernet) to form a 10GE access ring, providing immense bandwidth to satisfy the unrelenting demand today and tomorrow. Its flexible mounting options (DIN, wall and rack) allow it to be deployed anywhere in the station and rail infrastructure.

Redundancy protection for high resiliency

The access ring is based on ITU-T G.8032 Ethernet Ring Protection Switching. The access switch dual-homes on a redundant gateway router pair. This dual-home ring seamlessly internetworks with the dual backbone core network to connect with the active and standby OCCs (Figure 3).

Figure 3. End-to-end redundancy protection



Access ring with redundant gateway

ITU-T G.8032 is a protection switching technology for Ethernet rings where data is forwarded in one direction to the gateway. When a link or a node along the ring fails, the adjacent nodes will rapidly detect it. The upstream adjacent node will then inform all other ring switches upstream to switch the traffic in the other direction.

As the ring gateway is the only exit point for all ring traffic, when it fails, all ring traffic will be "blackholed" (Figure 4a). Therefore, it is important to provide nodal redundancy protection for the gateway. The fact that the ring switch is dual-homed, i.e. doubly connected to a redundant gateway pair, brings a significant boost to resiliency, as described in Figure 4b:

1. The active gateway is no longer reachable because of a failure, being the gateway itself, or an element in the path (fiber or switch) and the failure is detected by the standby gateway.
2. The standby gateway then assumes the role of active gateway for the devices affected by the failure.
3. On learning of the redundancy switching at the gateway, all ring nodes affected by the failure will forward data in the other direction to reach the newly active gateway.
4. Data continues the journey to the backbone core network.

Figure 4a. Single-home G.8032 ring "blackholes" traffic when gateway fails

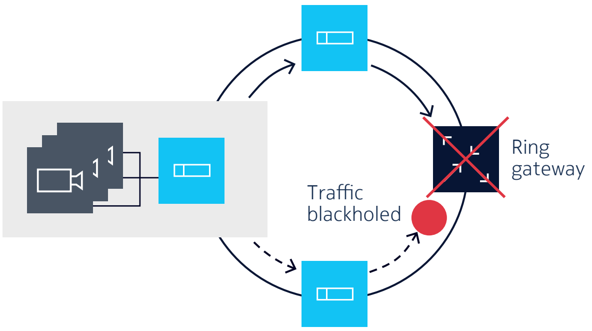
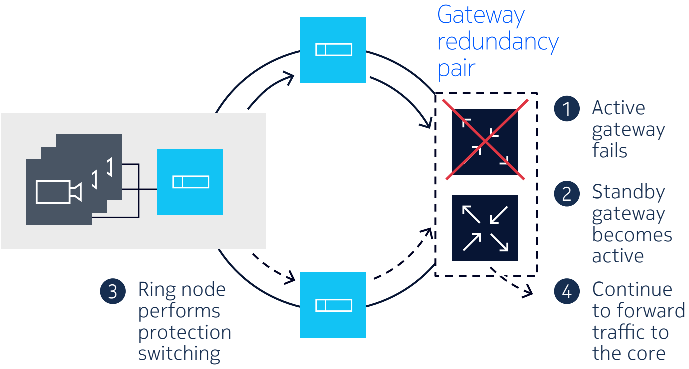


Figure 4b. Dual-home G.8032 ring protects from gateway failure


Gateway redundancy pair
1 Active gateway fails
2 Standby gateway becomes active
3 Ring node performs protection switching
4 Continue to forward traffic to the core

Ring gateway pair interworks with the redundant core networks and OCC pairs

Operators deploy redundancy protection for their backbone core network and OCC. It is important that the access ring can internetwork seamlessly with such redundancy provisions. As the ring gateway pair supports IP/MPLS, with its field-proven redundancy and flexibility, the access ring can connect station equipment seamlessly to either OCC through either core network.

Synchronization distribution

Operators can expand the train-to-ground LTE network to extend wireless coverage to the station with small cells. This allows for rapid deployment of non-critical sensors to support station equipment conditioning monitoring for predictive maintenance. It's not always practical to bring GPS/GNSS signals to small cells for time synchronization, particularly in underground stations. Using IEEE 1588v2 Packet Timing Protocol (PTP) is a viable and recommended technical option to distribute highly accurate frequency and time synchronization from the backbone core network through the station network to small cells deep in the station.

A 1588v2 synchronization architecture is based on a hierarchical topology of 1588v2 clocks (see Figure 5) where synchronization is distributed downstream to each 1588v2 clock, of which there are the following types:

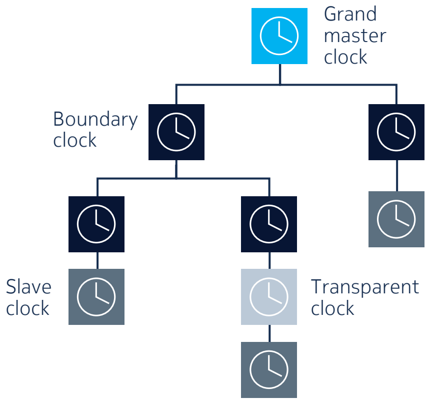
a. Grand master clock (GMC) – the primary clock reference with a high-precision time source, typically a GPS signal or atomic clock; acts as a master clock to other clocks below it in the hierarchy

b. Boundary clock (BC) – acts as a slave clock to the upstream master clock and master to the downstream slave clock

c. Transparent clock (TC) – forwards all 1588v2 messages received downstream; it has hardware-based capabilities to modify timestamp information in the messages to account for any delays it causes; it has no master/slave peering relationship to other 1588v2 clocks.

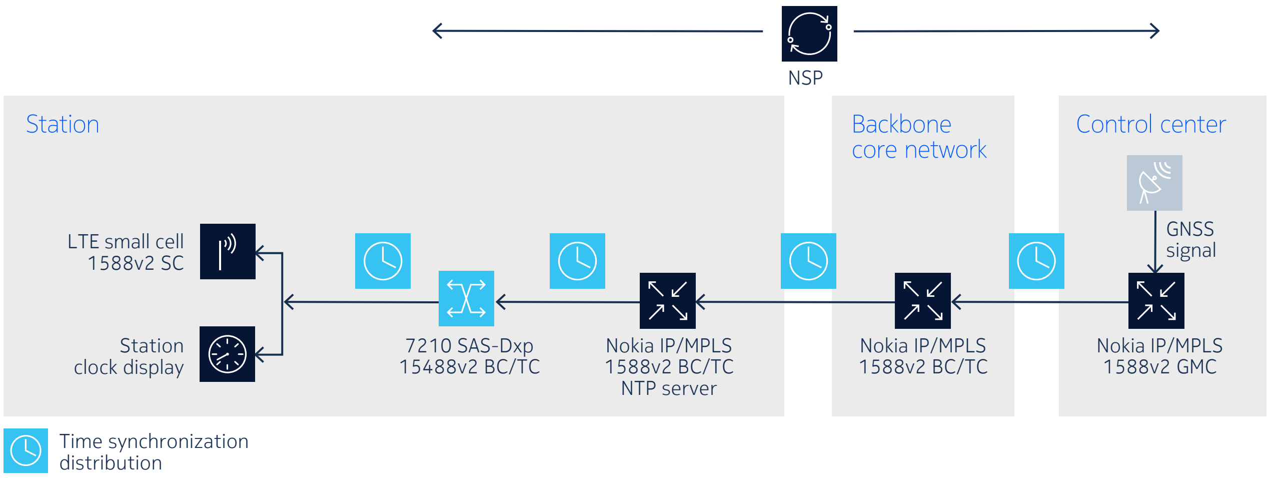
d. Slave clock – receives PTP messages from associated master clock to recover frequency, phase and time information.

Figure 5. A hierarchical 1588v2-based synchronization architecture



The station network blueprint incorporates 1588v2 to distribute synchronization to small cells and other station equipment that needs time synchronization (Figure 6). The blueprint also distributes NTP for local distribution for equipment requiring less precise time synchronization.

Figure 6. Station network blueprint integrated with 1588v2



End-to-end encryption and device authentication

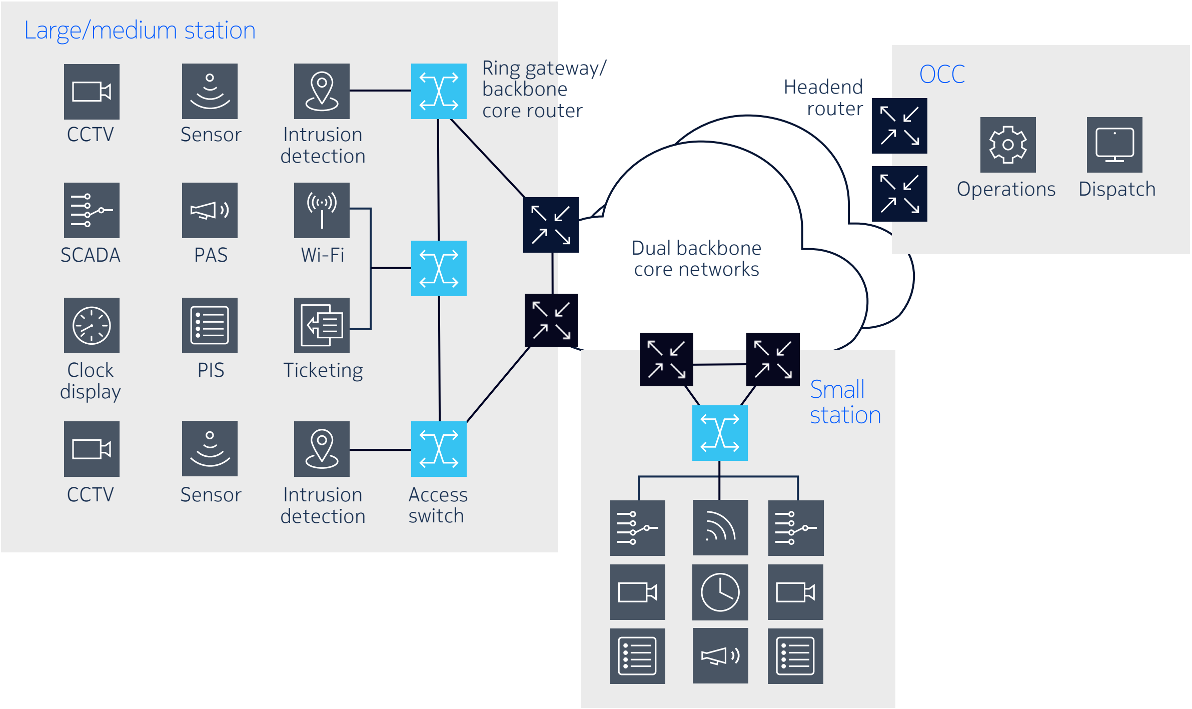
Rail infrastructure is a high-profile target for cyberattacks. As cyberattacks evolve, a multi-layer cyber defense is necessary. The station network blueprint forms a formidable defense perimeter, stopping illicit traffic from harnessing its security features:

1. Encrypting CCTV traffic: By harnessing the power of MACsec in the Ethernet access domain at 10 Gbps speed, the confidentiality, integrity and authenticity of station data is safeguarded in the access network.
2. Authentication: By capitalizing on IEEE 802.1X authentication capability, operators can ensure only legitimate devices are attached to the Ethernet port of the switches.

Converged station networking for large and small stations

Operators are embracing more and more applications and installing digital devices everywhere in the stations. The blueprint can evolve and scale to embrace them as a converged station network foundation for digital rail operators (Figure 7).

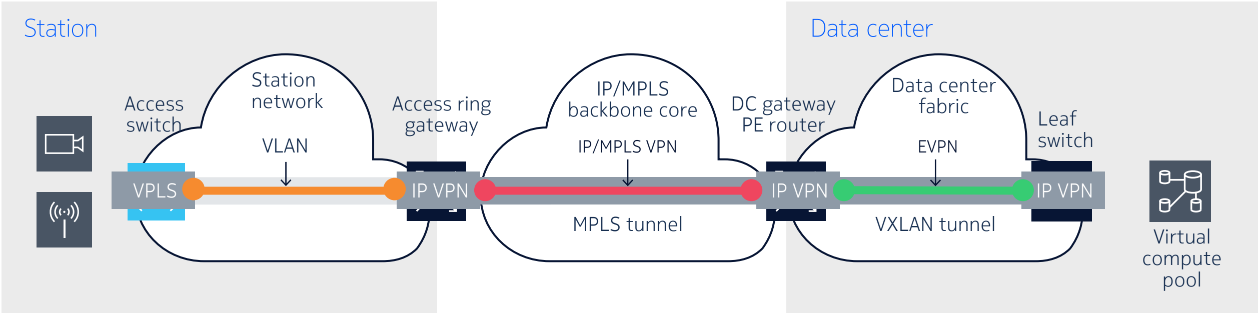
Figure 7. A converged station network blueprint



Looking ahead - interconnection with the data center

The blueprint has more to offer. As more and more rail applications are taking advantage of cloud computing, application software (or workloads in IT terminology) are now running in a pool of virtual compute resources in data centers run by the operators. Therefore, the blueprint needs to provide connectivity that can be extended into the data center. Its ring gateway router can form the IP/MPLS backbone core network that interconnects the data center network fabric through the IP/MPLS provider edge (PE) router acting as the DC gateway, forming end-to-end communications between station equipment and the application workload in the data center virtual compute pool (Figure 8).

Figure 8. Seamless interconnection from station to data center



Conclusion

Rail operators are at a critical juncture. Population mobility needs are increasing at a rapid pace and will continue to do so in the foreseeable future. This growth in train traffic poses great challenges for operators to provide reliable, sustainable and safe urban mobility. In addition to digital railway operational technologies like automatic train operation, digital station applications are also pivotal to serve the passengers as they begin and end the train journey. A new station network blueprint that can support new, emerging and future station applications is key to the digital station transformation.

Nokia's broad communications product portfolio spans IP/MPLS, data center networking, LTE/5G, packet optical and microwave. This portfolio is complemented by a full suite of professional services, including audit, design, engineering practices and integration for the railway industry. With this broad range of products and services, Nokia has the unique capability and flexibility to help operators plan and transform their urban railway networks to be ready for the future.

To learn more about Nokia solutions for railways, visit our Railways web page.

Abbreviations

BC	boundary clock
CCTV	closed circuit television
ERPS	Ethernet Ring Protection Switching
GMC	grand master clock
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
HPoE	high-power PoE
IXR	Interconnect Router

LAN	local area network
LTE	Long Term Evolution
MACsec	Media Access Control Security
MPLS	Multiprotocol Label Switching
NSP	Network Services Platform
NTP	Network Time Protocol
OCC	operations and control center
PAS	public announcement system
PE	provider edge
PID	passenger information display
PIS	passenger information system
PoE	power over Ethernet
PTP	Packet Timing Protocol
PTZ	pan, tilt and zoom
QoS	quality of service
SAS	Service Access Switch
SCADA	Supervisory Control and Data Acquisition
SR	Service Router
TC	transparent clock
TDM	time division multiplexing
VLAN	virtual LAN
VPN	virtual private network
VRRP	Virtual Router Redundancy Protocol

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

Document code: (February) CID212273