NOKIA

Ready your city network for CCTV traffic

Smart city network evolution

Application note

NOKIA

Abstract

CCTV systems used to be deployed at key city locations for public safety and security monitoring. In recent years, the CCTV application has evolved. With intelligent analytic capability, a CCTV camera can be turned into a multi-purpose sensor detecting anomalous situations such as crowd formation or just for simply reading a license plate. Consequently, more cameras are deployed in more locations using more bandwidth. These increases in CCTV traffic and the number of cameras put immense strain on a city's backhaul network. Here we discuss the Nokia CCTV backhaul network blueprint to address this concern and more.

NOKIA

Contents

NOKIA

CCTV – the safety pillar of smart cities

CCTV, also commonly known as video surveillance, was initially developed and deployed in the late 1970s. It allows users to remotely transmit live pictures to a television screen where real-time situations can be monitored and recorded. Its initial application was to monitor high-risk security targets such as banks. Later, it was installed by city governments in central business districts to monitor road traffic and in major city infrastructure such as pumping stations for the water and sewage systems to monitor industrial processes.

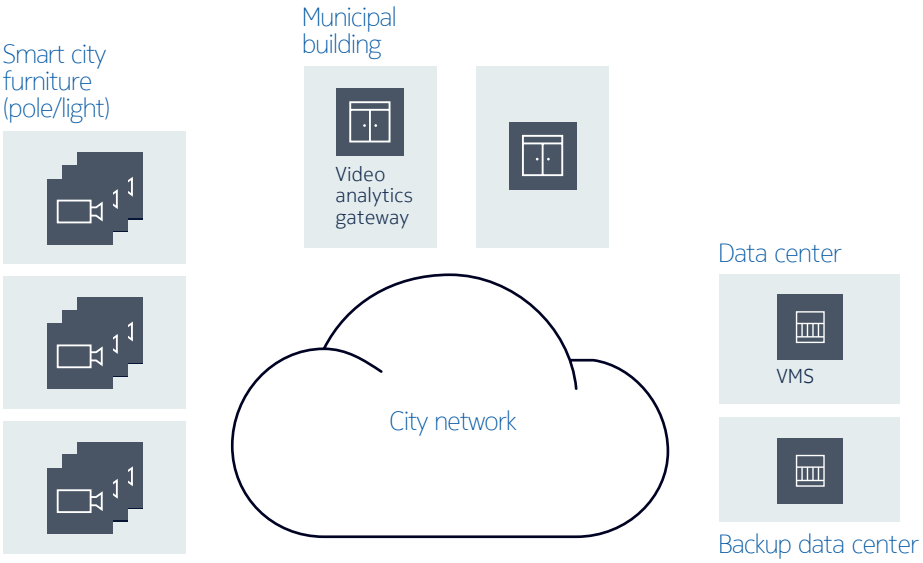
Today, as part of the smart city evolution, city governments are deploying CCTV cameras pervasively. Cameras are installed on utility poles, traffic lights and streetlights across the cities for crime prevention, traffic detection and license plate recognition. Complemented by advanced video analytic capabilities, cities can also use each camera as a multi-purpose sensor. In addition to attaining high situational awareness, it can detect abnormal behavior and identify objects of interest.

A CCTV system architecture

CCTV systems have evolved from purely analog to today's IP-based intelligent digital systems, which comprise the following major components (Figure 1):

- IP video cameras: installed on light poles, traffic lights and intersections to provide video streams typically over an Ethernet port.
- Video management systems and storage: dedicated servers and storage in data centers or clouds that run video management applications for video control, recording and storage; camera management controls, including pan, tilt and zoom (PTZ); and services for video clients, from which operators can view the video stream in real time.
- Video clients: computers capable of accessing services from video servers, such as live feed from a specific camera or a section of archived footage; there can be multiple video clients, one in the network operations center and others in the control and command center, each watching the same video streams at the same time.
- Video analytics gateway: Dedicated servers that run intelligent analytic applications. Harnessing the power of computer vision and artificial intelligence, the gateway analyzes live video streams to detect anomalies and alert operators. For scalability and faster response time, gateways are distributed in a number of city hub locations such as municipal buildings. Each gateway would receive live video streams from a set of cameras and perform real-time analysis, essentially turning CCTV cameras into video sensors, broadening the capability and use case.
- Communications network: a network that backhauls video traffic to the back end where servers, gateways and clients reside.

Figure 1. A smart city CCTV system deployment blueprint



Current city networks fall short of CCTV backhaul

Cities have been deploying and operating networks for many years. Many already have TDM/SONET/SDH-based city networks that are beyond end-of-support as well as IP/Ethernet networks deployed as extended enterprise LANs. Sometimes cities also utilize communications services offered by network service providers.

City networks connect municipal facilities, supporting IT applications and industrial applications including SCADA to monitor city infrastructure such as the water and sewage systems and metro rails.

However, the advent of CCTV brings new network requirements that stretch beyond current city network capabilities. Four major gaps can be identified:

a. Surge in number of cameras and bandwidth capacity

   With CCTV camera deployment becoming extensive, more cameras are installed in more locations. The volume of video data to be transported by the communications network has surged immensely. The city network needs to scale up its network to connect more cameras with higher bandwidth capacity.

b. Efficient traffic replication

   From each camera, the video stream needs to be delivered to multiple destinations: video analytic gateway, active and standby video management system (VMS), just to name a few. The network needs advanced functionality to build a point-to-multipoint path to efficiently deliver all streams.

c. High resiliency

   Video is becoming a critical tool used by public safety agencies to attain high situational awareness when carrying out emergency responses. Network failure can jeopardize the safety of first responders and affect response effectiveness. Therefore, the city network needs to fully harness network redundancy protection capabilities for backhaul resiliency.

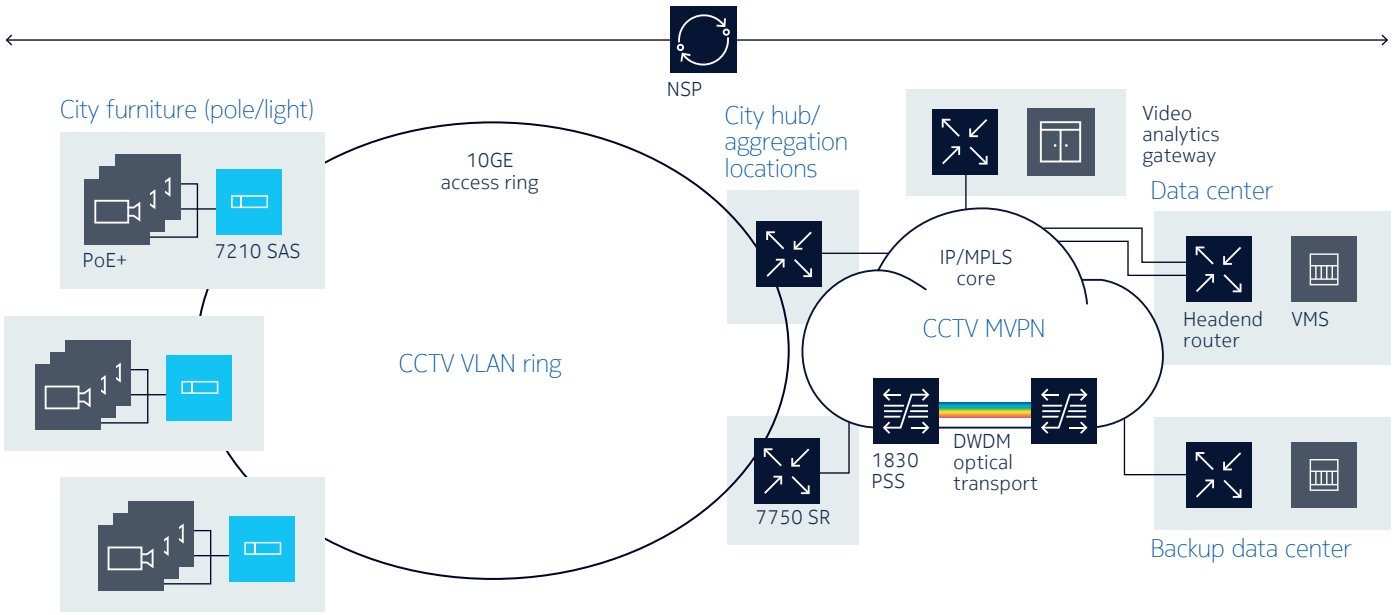
d. Cyber security

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

The Nokia CCTV backhaul network blueprint

Smart cities need to re-imagine their networks for CCTV backhaul. While the actual network design varies depending on each city's requirements and topology constraints, this application note attempts to build a blueprint network (Figure 2) as a reference architecture that can tackle the challenges explained above.

Figure 2. The Nokia CCTV backhaul blueprint



Comprising an access domain and a core domain, this network blueprint utilizes the fiber system to form a 10 Gb/s access ring based on ITU-T G.8032 Ethernet Ring Protection Switching (ERPS) technology. The ring connects access switches along the way, collecting all CCTV traffic to an aggregation router in a city hub location. Leveraging IP/MPLS and multicast VPN (MVPN), the aggregation then sends all aggregated traffic into the core domain toward the headend routers in data centers and video analytic gateways in other hub locations.

The network blueprint is built with:

- Nokia 7210 Service Access Switch (SAS) as the access switch

  The 7210 SAS-Dxp-16p/24p family members are a series of compact, fanless and 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].

- Nokia 7750 Service Router (SR) as aggregation and headend routers

  The 7750 SR is a family of IP/MPLS service routers with high performance, scalability and flexibility. Deployed at city hub locations as the ring gateway router, it straddles between the access and core domains, aggregating CCTV traffic from all subtending access rings and delivering them to data centers over the core domain.

1 PTZ cameras with heaters and blowers and VoIP phones with cameras need more than 15 W or even 60 W of power. They can benefit from PoE+, PoE++ and HPoE support on the switches.

- Nokia 1830 Photonic Service Switch (PSS) for DWDM optical transport

  The 1830 PSS is a family of packet optical platforms. It is the foundational DWDM optical transport backbone in the core domain.

- Nokia Network Services Platform (NSP) for cross-domain cross-layer management

The NSP is a unified services and network manager, overseeing access domain, core domain and optical transports. It simplifies network operations and enables operators to respond quickly to fast-changing demand and ensure high service performance and reliability.

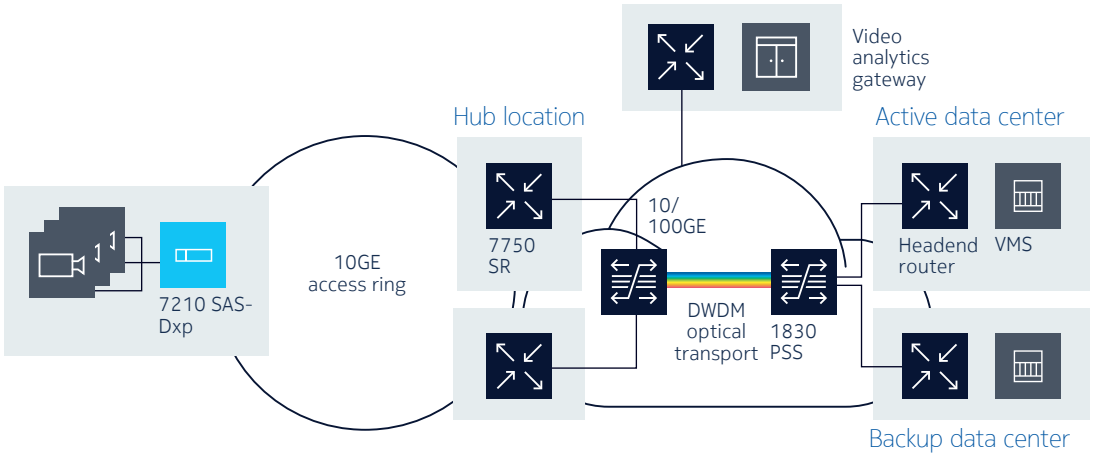
How the blueprint helps overcome the gaps

To help overcome the challenges described earlier, the network blueprint brings the following capabilities to the smart city network infrastructure.

10 Gb/s access and DWDM scale-up for CCTV data growth

From access to core, the network blueprint can scale up to satisfy the unrelenting demand of bandwidth to support more cameras with higher video resolution (Figure 3). In the access domain, instead of a typical 1GE access ring, the access switches can form a 10GE ring. In the core domain, depending on bandwidth utilization, 10GE or 100GE links can be deployed between the aggregation and headend routers. The DWDM links in the optical transport backbone can further significantly scale up the bandwidth capacity, not just for connecting all backhaul routers, but potentially for other use cases including data center interconnect or metro wavelength services for other parties.

Figure 3. The blueprint scales to ever-growing bandwidth demand



IP multicast for efficient multi-receiver delivery

After CCTV traffic is collected at the hub site, the aggregation router needs to send the traffic to multiple destinations, namely the video analytic gateway and the video management systems. If city networks have no IP multicast support, each CCTV camera needs to send an individual copy of the video stream, one for each destination, tripling the amount of bandwidth required in the core network (Figure 4a). The network blueprint uses a dedicated MVPN for efficient data delivery. Using a point-to-multipoint (P2MP) label switched path (LSP), a bandwidth-optimal distribution tree is built in the core network where traffic is replicated only when it is necessary (Figure 4b). This greatly optimizes bandwidth utilization and improves network economics.

Figure 4a. Non-multicast network requires three streams per camera

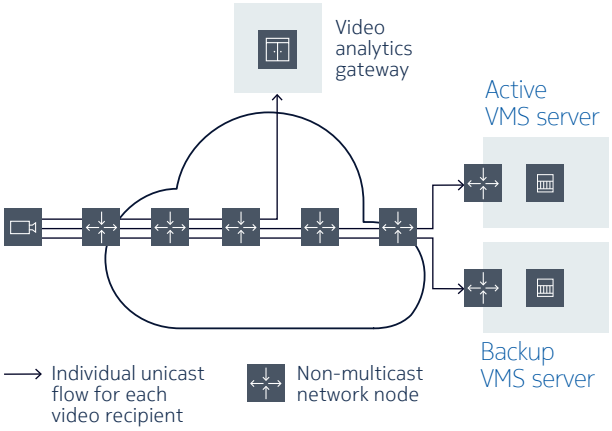
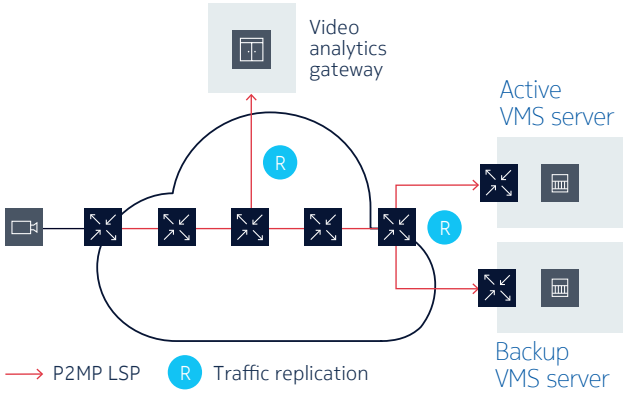


Figure 4b. Multicast tree using P2MP LSP reduces bandwidth utilization



End-to-end redundancy protection for high resiliency

Video traffic starts from the access ring, reaching the ring gateway, where it aggregates traffic from all attached rings and delivers through the core to the video analytic gateway and VMS. If a link or a component in the path fails, the video streams cannot be delivered for real-time analysis and storage. Therefore, the network blueprint needs to have a full set of robust protection mechanisms deployed along the path to ensure reliable delivery.

The key elements in the end-to-end redundancy protection are (Figure 5):

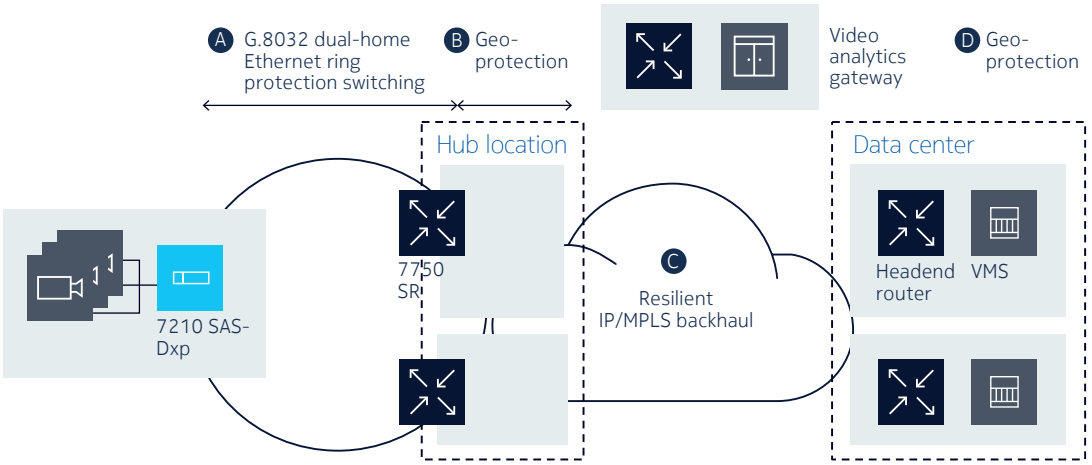
a. G.8032 dual-home Ethernet Ring Protection Switching (ERPS)

b. Redundant gateway router pair with geo-protection

c. Resilient IP/MPLS backhaul

d. Geo-protection of redundant VMS pair

Figure 5. End-to-end redundancy protection



G.8032 dual-home ERPS

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 and 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 6a). Therefore, it is important to provide nodal redundancy protection for the gateway. The G.8032 dual home protection brings a significant boost to resiliency with a redundant gateway pair in the following way (Figure 6b):

1) The active gateway fails and is detected by the standby gateway.
2) The standby gateway then assumes the role of active gateway.
3) On learning of the redundancy switching at the gateway, all ring nodes will forward traffic in the other direction to reach the newly active gateway.
4) CCTV traffic continues the journey to the core.

Figure 6a. Single-home G.8032 ring "blackholes" traffic when gateway fails

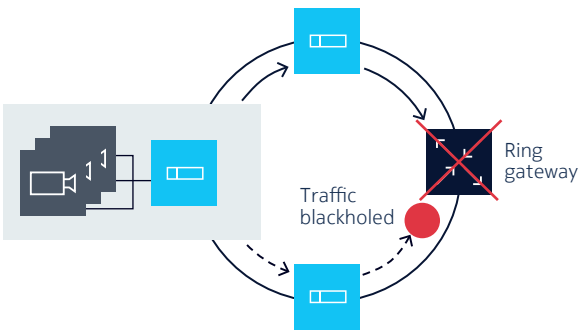
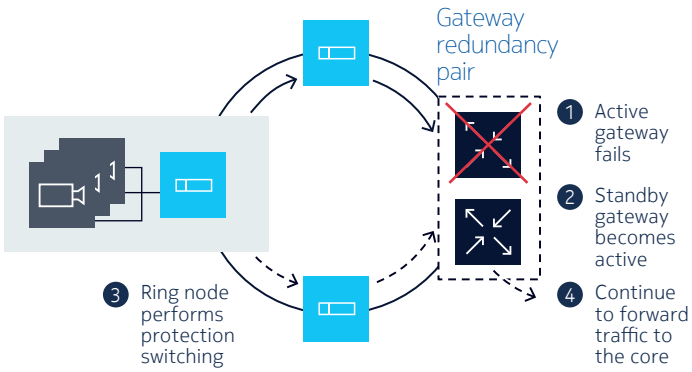


Figure 6b. Dual-home G.8032 ring protects from gateway failure



Geo-protection of the gateway pair

While multi-chassis G.8032 can protect traffic from a gateway failure, when the hub location where both gateways are co-located is struck by incidents such as fire or severe weather, both gateways can be affected. Locating the gateway pair in two different hub locations brings geo-redundancy protection. When one site is affected, the protecting gateway in the other site can take over.

Resilient IP/MPLS in the core domain

IP/MPLS brings strong multi-layer redundancy protection to the core domain as shown in Table 1. When there is a failure in the core domain, the network can invoke the necessary protection scheme to recover and restore the connectivity.

Table 1. Multi-layer IP/MPLS core resiliency

Service layer	• Multi-chassis pseudowire redundancy • Multi-chassis-Link Aggregation Group (MC-LAG)
MPLS layer	• MPLS Fast Reroute/standby Label Switched Path • Label Distribution Protocol (LDP) Equal Cost Multipath (ECMP) • Non-stop signaling
IP layer	• IP Equal Cost Multipath (ECMP) • Non-stop routing • Virtual Router Redundancy Protocol (VRRP)
Link layer	• G.8032 ERPS • 802.ad Ethernet LAG • Microwave 1+1/2+0

Geo-redundant VMS pair

VMS plays a central role in the CCTV system. Therefore, its survivability is critical. It is imperative that the active and backup VMS pair be housed in separate data centers and receive all video streams for disaster recovery and business continuity. When one site fails, city staff can immediately access the backup with full information. With the use of IP multicast in the core domain, all video streams are delivered to both VMS in two locations with optimal bandwidth efficiency so that city staff can have all necessary information at hand from either location.

End-to-end encryption and firewall as the first line of defense

Smart city infrastructure is a high-profile target for cyberattacks. As cyberattacks evolve, a multi-layer cyber defense is necessary. The backhaul 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 and the core domain, the confidentiality, integrity and authenticity of CCTV data is safeguarded.
2. Filter illicit traffic flows – By capitalizing on the capability of firewall and IP filtering in aggregation and headend routers, illicit IP flows are stopped, thwarting unauthorized attempts to compromise the CCTV system.

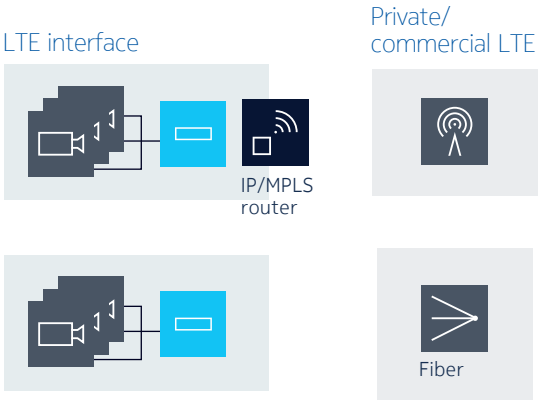
The blueprint has more to offer

While overcoming the gaps in city network capabilities, the blueprint is also expandable and scalable for more challenges.

Expanding blueprint network access with wireless medium

While cities are aggressively installing fiber for their connectivity needs, there are still many “unfibered” locations. City networks need to adopt wireless access where necessary. The network blueprint can deploy a compact IP/MPLS router with LTE interface to backhaul the traffic over a private or commercial LTE network, complementing fiber access.

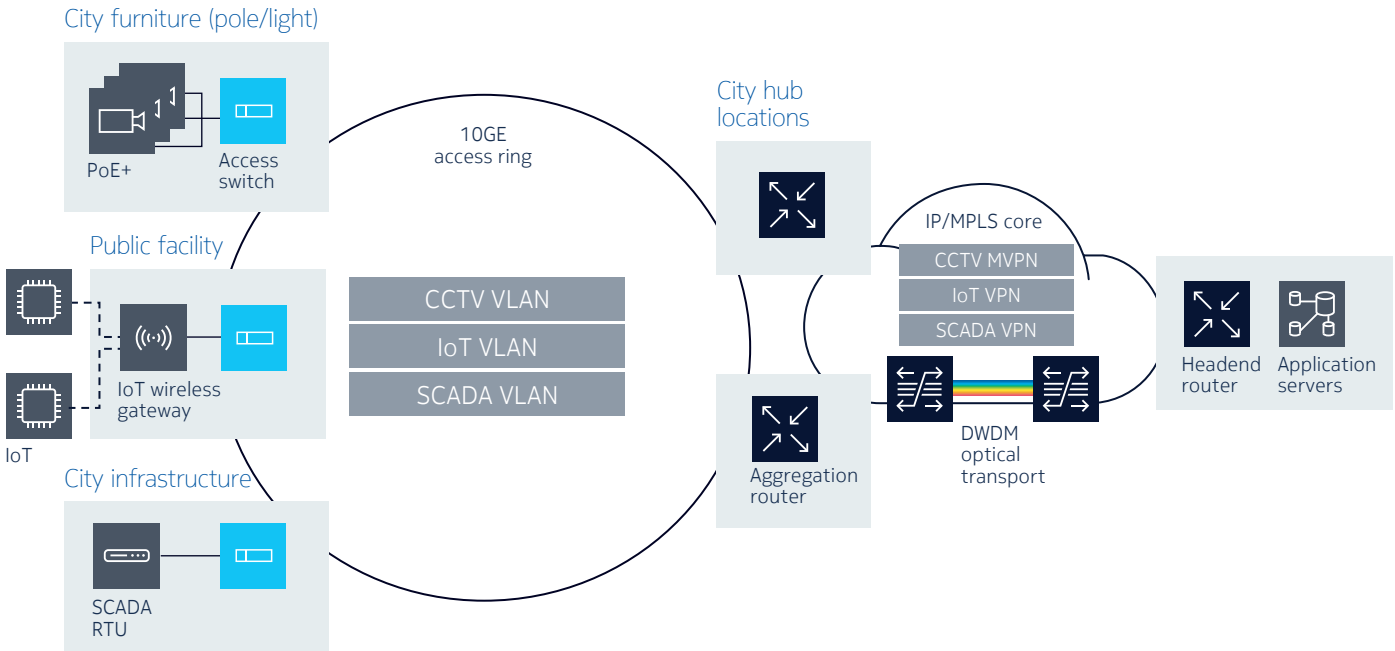
Figure 7. Wireless access complements fiber to bring CCTV everywhere



Ready to do more

As city governments are under constant budget constraints, it is imperative to optimize network economics for the backhaul network. Harnessing the power of IP/MPLS services, the backhaul network blueprint, with extensive network coverage and abundant bandwidth resources, is ideal to serve as the converged network service platform for a small city. It can connect multitudes of devices and support many more smart city applications, from IoT sensors to SCADA to city IT systems (Figure 8).

Figure 8. The blueprint serves as a converged smart city network



Conclusion

From video protection to situational awareness and intelligent traffic management, smart cities are increasingly dependent on CCTV everywhere to provide real-time information and, with video analytics, act as smart sensors. However, today's city networks face immense challenges to backhaul CCTV streams. Adopting the Nokia CCTV backhaul blueprint based on dual-homing G.8032 ERPS and IP/MPLS core can overcome the backhaul challenges. Moreover, it can evolve as a smart city communication platform to scale for future bandwidth growth and to embrace emerging applications.

To find out more about how Nokia can support smart cities, visit our smart city webpage.

Abbreviations

CCTV	closed circuit television
DWDM	dense wavelength division multiplexing
ECMP	equal cost multipath
ERPS	Ethernet Ring Protection Switching
HPoE	high-power power over Ethernet
IPsec	IP security
LDP	Label Distribution Protocol
LSP	label switched path
LTE	long term evolution
MACsec	media access control security
MC-LAG	Multi-chassis Link Aggregation Group
MPLS	Multiprotocol Label Switching
MVPN	multicast VPN
P2MP	point to multipoint
PoE	power over Ethernet
PSS	Photonic Service Switch
PTZ	pan, tilt and zoom
SAS	Service Access Switch
SCADA	supervisory control and data acquisition
SDH	synchronous digital hierarchy
SONET	synchronous optical networking
SR	Service Router
TDM	time division multiplexing
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: 1380555622786510142 (June) CID210590