NOKIA

Delivering a public sector shared network architecture

Reduce OPEX and mitigate risk with shared WANs

Strategic white paper

A multitude of influences are putting sustained pressure on state and local governments to find innovative ways to modernize information communications infrastructure. Aging infrastructure needs to be transformed to ensure sustainable, reliable, anytime connectivity for citizens and agencies alike.

An intelligent communications network for shared use among different agencies offers a framework to conserve financial and employee resources by building a resilient, flexible, scalable and secure foundation. This paper discusses the benefits of modernizing your communications infrastructure. Learn about design of a WAN for disaster preparedness, simplified network management, shared services network, an ROI model, and business and technology risks.

Contents

Public sector challenges

Many influences are putting sustained pressure on state and local governments to find innovative ways to modernize information communications infrastructure. Some of those influences are:

- Rapidly growing urban populations
- Greater expectations from constituents
- Increasing budget constraints
- Advantages of cloud services.

Aging infrastructure needs to be transformed to ensure sustainable, reliable, anytime connectivity for citizens and agencies alike.

An intelligent communications network for shared use among different agencies offers a framework to conserve financial and employee resources and increase efficiencies by building a resilient, flexible, scalable and secure foundation.

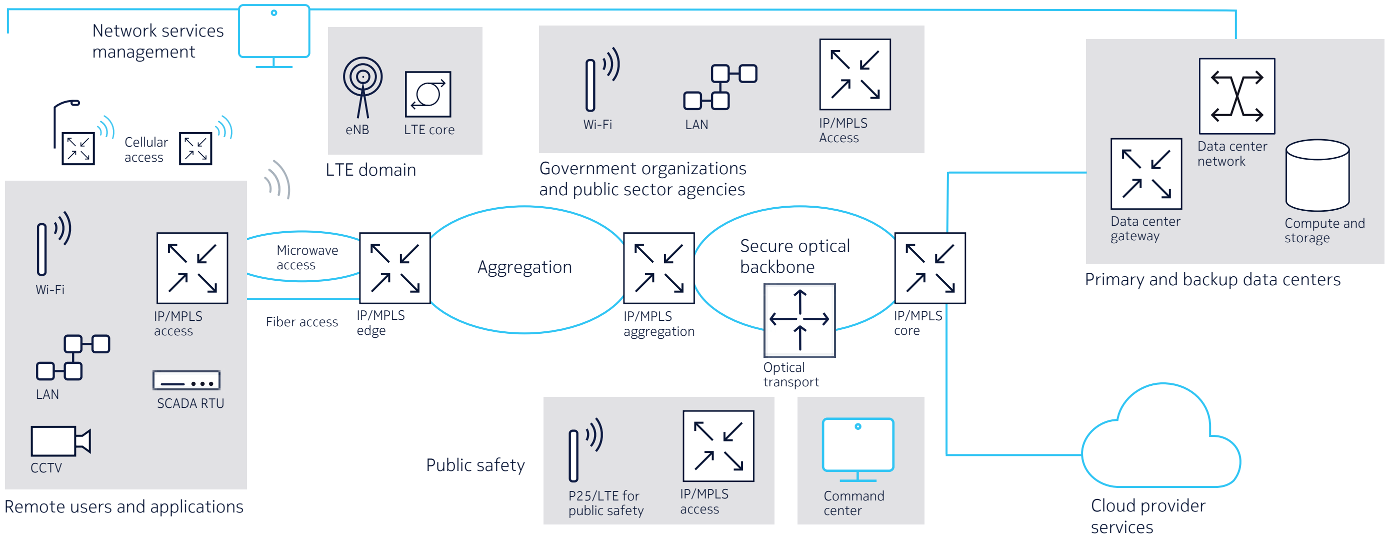
This paper discusses the benefits of modernizing your communications infrastructure. Learn about:

- Building a resilient and cost-effective WAN architecture for robust disaster preparedness
- Simplifying network management while enhancing agility in service provisioning
- Creating an ROI model that quantifies the business drivers and benefits of shared municipal WANs
- Identifying and mitigating business and technology risks
- Planning for the evolution to a cloud-based architecture with minimal network impact.

Nokia is working with local and regional public sector organizations to deliver services across a single, centrally managed network infrastructure to help the organizations meet targets for operational and financial efficiency.

Figure 1 shows a shared network architecture that utilizes all the transport mechanisms at an organization’s disposal. By implementing secure, reliable technologies in the network, such as IP/MPLS, secure optical, and network and service management to simplify provisioning, the network achieves low operational cost, high availability, flexibility and security.

Figure 1. Shared architecture for public sector



Resilient and secure WANs

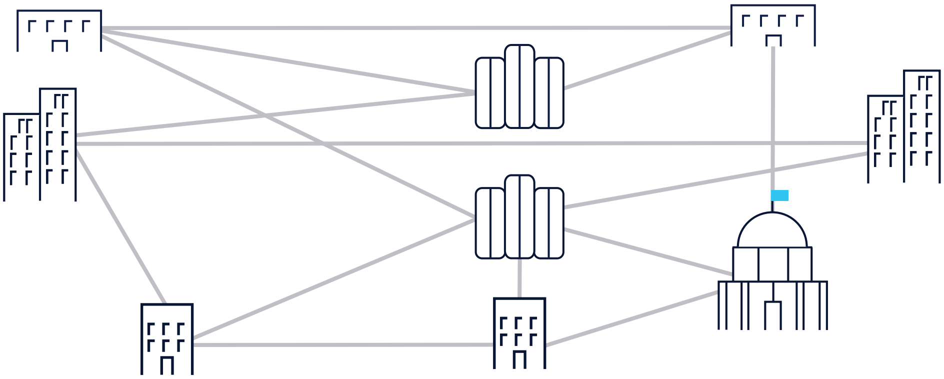
Building a resilient, secure and cost-effective WAN architecture delivers robust disaster preparedness.

Many of today's networks contain purpose-built point-to-point connections similar to those in Figure 2. The networks have grown over time, expanding by need without much thought about how the additional links will behave during an incident or disaster that takes down key links. The additional links also consume more equipment ports and physical transport facilities.

Legacy equipment and protocols also need to be considered, and their data transported. In many cases, multiple data lines come into shared facilities, increasing operational costs and contributing to data transport inefficiency. Consolidating or converging these lines to a high-bandwidth transport mechanism such as fiber or microwave will reduce overall costs, provide security for customers and standardize data transport across the network.

Figure 2 shows a purpose-built network configuration.

Figure 2. Purpose-built point-to-point

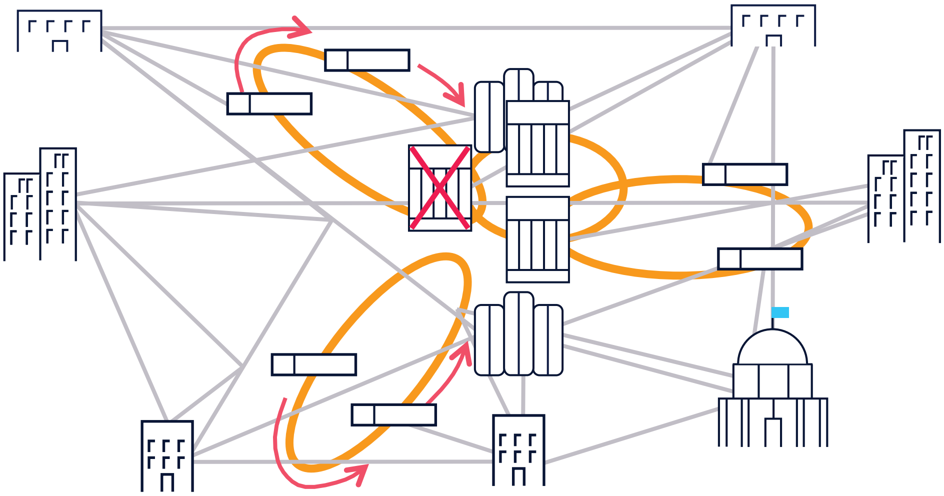


Point-to-point connections satisfy connectivity with multiple links

Links can be consolidated to data centers and major fiber points of presence, and optimized for agency and government communications efficiency. Rings can be added for aggregation and reliability (see Figure 3).

When a link drops, data service beyond the link in a conventional network is disrupted for the duration of the outage. Building in resilience by adopting the convergence concept through a shared services municipal network using IP/MPLS reduces reliance on point-to-point links, enabling automatic data path recovery. Additional savings can be realized by converging data service requirements, keeping each user's data separate and secure through the use of VPNs over common transport paths.

Figure 3. Flexible connectivity and increased reliability



Shared infrastructure approach yields feasible connectivity and increased service reliability

In the shared architecture, a resilient IP/MPLS mesh is built over a secure optical infrastructure that uses encrypted optical links in a multiple ring topology. This provides a highly flexible, scalable, reliable and secure shared infrastructure that enables intelligent communications for multiple public agencies. A separate VPN for each public agency ensures that communications are kept separate while also allowing communications between agencies. A secure and scalable key server manages the encryption keys.

Multiple paths for data delivery are defined in the architecture; each packet must have a redundant and resilient path from end to end in the event of a service disruption or link failure.

The architecture also enables cloud data center interconnect (DCI) to provide secure and automatic backup of data between primary and backup data centers. This ensures business continuity and recovery of business- and mission-critical data in the event of a network failure or major disaster.

Legacy protocols can be transported over IP/MPLS and traverse through the network as packet traffic. At the other end of the connection, legacy systems can be directly connected. The legacy equipment can operate without interruption and users can enjoy the same level of service at lower cost and over a resilient network. An example of utilizing shared infrastructure for this purpose is in services that use legacy SCADA systems

Many of these systems rely on legacy interfaces such as RS-232 and TDM-based transmission protocols such as a T1 line to ensure delivery of the signal to the system at the right time and over the right channel. Maintaining the TDM circuits and paying for a low-data-rate transmission instead of moving to a more cost-effective high-data-rate connection is not the best utilization of those links. Migrating to IP/MPLS and transporting the data across shared infrastructure reduces monthly recurring costs and allows the legacy system to operate into the future without the need to change anything in it.

Situational awareness is another area that shared infrastructure can help improve. Accessing data during an incident or event can stress a traditional network, overloading connection paths and impeding traffic management. Implementing the shared infrastructure strategy can prioritize traffic, increase bandwidth where needed, and enable use of cloud data and applications.

With shared infrastructure, disruptions are minimized and can be dealt with easily and quickly. Downtime is reduced, and managing repairs is less costly.

Simplified network management

A shared architecture simplifies network management while enhancing agility in service provisioning.

After the architecture for the network is defined, it is important to think about how to provision and manage it. The Nokia Network Services Platform (NSP) enables simple and flexible network management.

The Nokia NSP is the network management software that monitors and controls traffic on the network as well as examining the health of the network. It simplifies provisioning and many of the tasks that often increase network maintenance costs. It enables the network operator to configure circuits and permissions through a GUI, avoiding time-consuming and error-prone command line interface (CLI) programming.

The NSP monitors network health while keeping human managers informed of alarms and conditions. It provides fault analysis tools that help pinpoint root causes, enabling quick and efficient network troubleshooting and restoration. In one particular case, provisioning after a major disaster took days instead of months. When downtime costs thousands of dollars per hour, the cost savings are huge.

Shared services management

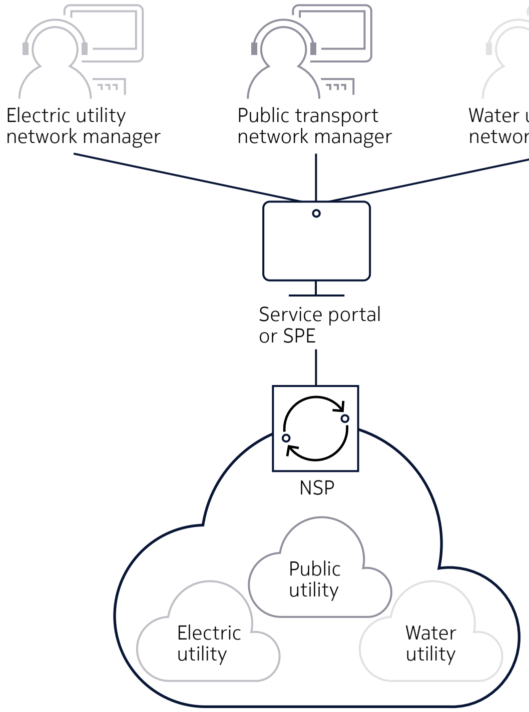
Shared services management enables agencies to manage their own VPNs.

In the shared infrastructure model, the agencies often need to perform common network performance tasks on their VPN(s), including port status monitoring, network performance and statistics gathering, troubleshooting and even provisioning with resources allocated to them. For many agencies, they need instant access to their allocated VPN assets to monitor the VPN connectivity and performance in real time.

In a legacy network with purpose-built, point-to-point connections, agencies need to wait to receive the network operator's weekly or monthly report to see VPN connectivity and performance. When they want to change a parameter in the VPN (for example, increase the bandwidth or alter the connectivity), they need to submit a change request form electronically and wait for days or even weeks. This customer care paradigm does not meet the expectations or needs of the agencies.

The Nokia Service Portal supports a web-based self-service customer portal. This self-service capability, with proper customer policy enforced, enables end customers—the agencies—to have control of their VPNs so they can manage service changes, additions and deletions. The agencies also have real-time access to VPN performance and port status, and can carry out operations, administration and management (OAM) tests if required. The scope of control can be tailored by the customer policy individually, as shown in Figure 4.

Figure 4. Service Portal enabling shared services management



ROI model for the WAN

The following case study creates an ROI model that quantifies the business drivers and benefits of shared WANs.

This case study compares the business benefits of shared infrastructure with a legacy point to-point fiber network based on a purpose-built approach. Consider a city facing the following challenges:

- A growing demand for connectivity and more bandwidth from city agencies
- A limited network of point-to-point fiber and a variety of legacy technologies
- An operations staff, most of whom were retiring.

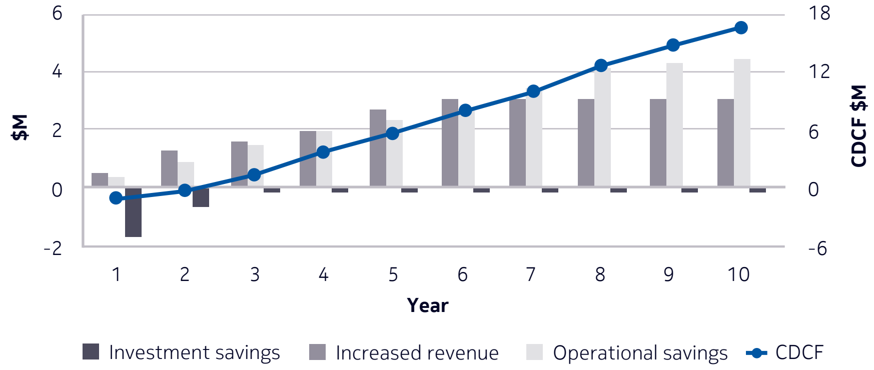
In addition, the city wanted a solution to meet the following needs:

- An agile and resilient network that could accommodate higher bandwidth apps as well as the Internet of Things (IoT), such as traffic controllers, bus stops, water services and security cameras
- A unified network management system (for the network operations center) and a partitioned network management system to provide city agencies with autonomous control
- A plan to sell more dark fiber to help offset the cost of the network deployment.

The city asked whether a converged, shared services infrastructure was more economical than a purpose-built network with point-to-point connections.

Nokia Bell Labs developed a business model that compared shared infrastructure with the city's legacy point-to-point fiber network. The business model showed that shared infrastructure achieved payback in 2.3 years over their legacy network, as shown in Figure 5.

Figure 5. Business modeling results comparing shared with point-to-point



Category	10 years Total ($M)
Increased revenue	$22.54
Operational savings	$25.18
Investment savings	$-3.17
NPV	$16.68
Payback	2.3 years

Investment enables more connection points, more revenue, less OPEX

The business model determined that the shared infrastructure investment enables more connection points, more revenue and less OPEX.

The key benefits of the shared business model were as follows.

- Agencies could deploy their own high-speed services (e.g., 1 Gb/s) to users in hours compared to the legacy system, which took six weeks per circuit.
- Twelve times as many IoT devices could be deployed over the same amount of fiber through the use of IP/MPLS.
- A bandwidth-based, distance-insensitive cost model could be used with agencies, which simplified budget planning and encouraged additional deployment of services.
- Additional dark fiber could be sold, generating $22 million in external revenue.
- A resiliency benefit could be realized: Six days' faster recovery and over $3 million in savings following a natural disaster versus the same scenario with the legacy network.
- The city could double their workload without hiring additional IT operations staff.

Shared risk mitigation

Creating a shared services network introduces additional business and technology risks, which must be identified and mitigated.

The network must be able to provide a secure, reliable and scalable service that meets or exceeds the combined requirements of each tenant's applications and services. This can be accomplished with the MPLS technology and management tools built into the network design.

Support for a shared architecture model has three key requirements:

- Traffic isolation
- Address independence
- Flexible application placement and migration.

The MPLS overlay model in the shared architecture uses VPNs to provide the required traffic isolation. Combining multiple tenants with MPLS gives shared network operators a great deal of flexibility to divert and route traffic around link failures, congestion and bottlenecks while assuring each tenant's individual SLAs.

Because each agency is virtually isolated from others, they are free to use whatever address scheme meets their application requirements. Often, the individual agencies will not even need to change existing addresses.

Because each agency application can have its own use case on the network that is separate from any adjacent use cases, applications required to reside inside of a tenant's network will easily co-exist with other tenants' applications. There will be no interactions between use cases without going through a control point or location (for example, a firewall for Layer 3/Layer 4 traffic). Each group is a closed system that isolates its functions from access outside the group and between each group.

The isolation of traffic of one closed user group from other groups adds to the network security and facilitates flexibility in implementing security and other requirements individually for each group. The protocols used between endpoints within one closed user group can be different from the protocol used within another group. With MPLS, protection mechanisms ensure that reliability requirements are met and that failures can be recovered within specified time limits. In addition, QoS mechanisms ensure that services are prioritized according to specific traffic criticality.

The flexibility to offer each tenant various levels of security, resilience and scalability over a unified infrastructure clearly helps the shared infrastructure deliver value for each agency while mitigating shared technology risks.

SDN adoption

Cloud computing is the evolution of the traditional static IT model into a dynamic, "utility-like" on-demand model. It allows public sector organizations to automatically activate and de-activate resources as needed, dynamically update infrastructure elements and move workloads. Transformation to the cloud is ideal for the shared or multi-tenant operations typical of a multi-agency government because the cloud improves efficiency without the need to create new infrastructures for each new application.

Governments are preparing their data centers and WANs for cloud-optimized services and networking. This will include the adoption of Software Defined Networking (SDN) to enable programmable IP/MPLS and optical transport for improved automation and resource optimization.

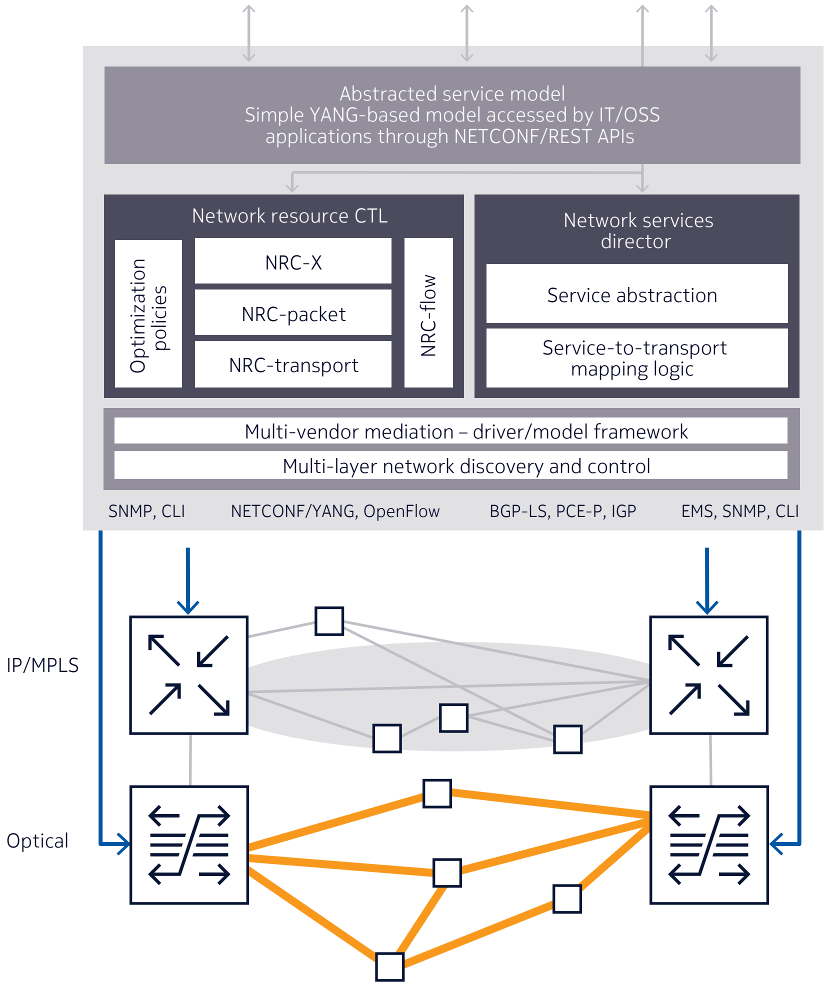
Traditional IP and optical networks employ a siloed paradigm with multiple layers and often with multiple vendors. Network management is domain-based and includes multiple management system silos and integration with complex APIs and provisioning systems.

SDN breaks the siloes and provides dynamic, automated multi-layer resource management and optimization. This enables greater network utilization and capabilities to handle demand spikes and outage events. SDN is essential in the delivery of cloud-based routing and transport.

The Nokia NSP is ready for adoption of the SDN framework.

The high-level capabilities of an SDN framework are outlined in Figure 6.

Figure 6. Shared architecture with SDN


Abstracted service model
Simple YANG-based model accessed by IT/OSS applications through NETCONF/REST APIs
Network resource CTL
Optimization policies
NRC-X
NRC-packet
NRC-transport
NRC-flow
Network services director
Service abstraction
Service-to-transport mapping logic
Multi-vendor mediation – driver/model framework
Multi-layer network discovery and control
SNMP, CLI
NETCONF/YANG, OpenFlow
BGP-LS, PCE-P, IGP
EMS, SNMP, CLI
IP/MPLS
Optical

Conclusion

Adoption of Nokia's shared network architecture will provide a secure, scalable and resilient network with unified management that optimizes operational costs. Nokia's portfolio of products utilized in the design integrate together smoothly to create a successful framework for shared service delivery. Therefore, managing the network becomes easier and less dependent on high-cost experts.

Recovering from a disaster or network interruption is eased by the redundant and resilient nature of the network. The network management system allows for rapid fault analysis and resolution.

Implementation of shared infrastructure has a proven ROI that quickly produces payback for the capital invested—typically in less than three years.

The flexibility to offer each tenant various levels of security, resilience and scalability over a unified infrastructure clearly helps the shared framework deliver value for each agency while mitigating shared technology risks.

Finally, the shared architecture becomes an essential step as governments prepare their data centers and WANs for cloud-optimized networking.

For more information about Nokia solutions for the public sector, visit our Smart City web page.

Acronyms

API	Application Programming Interface
BGP-LS	Border Gateway Protocol – Link State
CCTV	closed circuit television
CDCF	cumulative discounted cash flow
CLI	command line interface
EMS	element management system
eNB	eNodeB
GUI	graphical user interface
IGP	Interior Gateway Protocol
IP	Internet Protocol
LAN	local access network
LTE	long term evolution
MME	Mobility Management Entity
MPLS	Multiprotocol Label Switching
NETCONF	Network Configuration Protocol
NPV	net present value
NRC	network resource control
NSP	Nokia Network Services Platform
OPEX	operating expenditures
OSS	operations support system
P25	Project 25: a suite of standards for digital mobile radio communications
PCEP	Path Computation Element Protocol
QoS	Quality of Service
RESTful APIs	Representational State Transfer APIs
ROI	return on investment

RTU	remote terminal unit
SCADA	supervisory control and data acquisition
SDN	Software Defined Networking
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
TDM	Time Division Multiplexing
VPN	virtual private network

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

Product code: SR1708014830EN (September)