Nokia private network solutions
for real-time healthcare and the cloud

Application note
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>Real-time healthcare and the cloud</td>
<td>3</td>
</tr>
<tr>
<td>Building a secure private optical transport network</td>
<td>5</td>
</tr>
<tr>
<td>Implementing a private IP/MPLS core network</td>
<td>11</td>
</tr>
<tr>
<td>Connecting remote healthcare sites using SD-WAN</td>
<td>16</td>
</tr>
<tr>
<td>Implementing a network support strategy</td>
<td>19</td>
</tr>
<tr>
<td>Conclusion</td>
<td>20</td>
</tr>
<tr>
<td>Acronyms</td>
<td>20</td>
</tr>
</tbody>
</table>
Introduction

Today’s largest, most complex healthcare systems are handling more data than ever before, pushing current IT operations to their limit. Overcoming the key challenges — scalability, reliability, quality of service and security — requires evolving to a real-time healthcare system (RTHS). This new technical and operational model leverages the latest cloud and digital technologies, so clinicians and patients can connect, communicate, and collaborate more effectively.

A robust and intelligent private network infrastructure is crucial for transitioning to the new model. By seamlessly interconnecting hundreds of sites, devices, and data siloes, it enables healthcare organizations to streamline their workflows — and gain anywhere, anytime access to data and knowledge that are crucial for improving patient care.

This Application Note outlines Nokia networking solutions that help healthcare organizations build a private WAN to support RTHS and cloud IT. It shows how healthcare organizations can use Nokia solutions to implement more agile, flexible, and cost-efficient networks for the cloud era.

Real-time healthcare and the cloud

Real-time healthcare systems are evolving to leverage the latest cloud and digital technologies and support new operational models. They promise to enable clinicians to connect, communicate, and collaborate more effectively, and are becoming crucial for highly connected, digitally enhanced, patient-driven care.

Delivering better healthcare requires real-time information and communications for more collaborative, proactive patient care, as well as an adaptive IT infrastructure that responds quickly to changing patient and physician needs. Fundamental to this transformation are network and cloud technologies that accelerate innovation, streamline workflows, and facilitate anywhere, anytime access to data and knowledge that is critical to patient care.

Many healthcare organizations use network services to connect hospitals, data centers, healthcare sites and clinics. Many are attracted by the benefits of virtualized IT and cloud services, such as scalability, agility, and cost efficiency. However, traditional network services are slow to provision and lack the scalability and bandwidth to support modern RTHS applications. Furthermore, virtualized IT and cloud services may not offer the data security, control, and sovereignty to ensure the confidentiality of sensitive medical data, such as electronic health records (EHRs).

In the context of an RTHS and the cloud, healthcare organizations must determine the best approach for their networking needs. Many are turning to private networks and private clouds to support RTHS so they can leverage
the latest technologies to transform their IT infrastructure, meet compliance requirements, and support new applications critical to patient care and safety.

As illustrated in Figure 1, a scalable, secure, and reliable private network that connects major hospitals and healthcare sites can be augmented with new, flexible solutions to connect smaller healthcare sites, clinics, and pharmacies. Secure internet and mobile applications can also be used to connect patients and healthcare workers in the community, enabling remote monitoring and telemedicine.

Figure 1. Private network supporting a real-time healthcare system (RTHS)

A private network enables healthcare organizations to implement a secure private cloud that runs critical healthcare applications, protects confidential patient data, and helps meet regulatory and compliance requirements. Moreover, a private cloud can be augmented with virtual private and hybrid clouds to run non-critical workloads and applications. This combination improves workload distribution, enhances IT responsiveness, and increases efficiency while securing healthcare data.

**Re-architecting the healthcare network**

When building a private network to support a private cloud for real-time healthcare, it is important to start with a high-performance WAN backbone between the main healthcare and data center sites. As illustrated in Figure 1, a backbone that combines optical networking and IP/MPLS provides the core elements of scalability, reliability, quality of service and security — in addition to including the intelligence to separate multiple services and applications with differing requirements.

Existing managed VPN services can be used to connect regional hospital and healthcare sites where continued use of these services makes sense. For small
healthcare sites and clinics, SD-WAN solutions can be used to connect to the private healthcare cloud more easily and at lower cost. SDN can be used to enable data center virtualization, hybrid cloud connectivity, as well as network optimization and automation. Furthermore, secure internet connections and mobile applications can enable remote healthcare and telemedicine in the community.

For most healthcare organizations, re-architecting their existing WAN to include a mix of private WAN infrastructure, managed WAN services, and SD-WAN is likely the best approach to support real-time healthcare and the cloud. At the same time, though, they need to consider the best mix to suit their individual requirements, as well as the best network management and support strategies for such a hybrid WAN environment. The following sequence outlines the options a healthcare organization could take to implement a hybrid WAN that supports its real-time healthcare and cloud strategies:

- Build a private optical network to provide very high-speed, secure transport among major hospital sites and data centers to create a private cloud.
- Implement a private IP/MPLS core to provide reliable connectivity among major healthcare sites and data centers, separate healthcare applications running in the private cloud, and in order to connect to hybrid cloud resources and services.
- Use managed IP/MPLS VPN or cloud connect services to connect larger remote healthcare sites to the cloud where cost/performance is justified or where changes are less frequent and more predictable.
- Implement SD-WAN access to provide more flexible connectivity to the cloud, particularly for smaller remote healthcare sites and clinics, or where changes are more frequent and unpredictable.
- Implement integrated, end-to-end configuration, monitoring and troubleshooting of the WAN infrastructure and, over time, adopt and migrate to SDN-based orchestration and automation of network and IT resources for a more dynamic, flexible, and agile cloud.

A healthcare organization could implement one or more of these options depending on its technical and business requirements. The following sections describe the portfolio of Nokia solutions to help healthcare organizations build a private WAN to support digital technologies and the cloud.

**Building a secure private optical transport network**

Building a secure, private optical transport network, using dark fiber and self-managed optical equipment, provides a healthcare organization with highly scalable, secure, reliable connections among large sites and data centers in a private cloud. Using diverse fiber paths and redundant optical equipment...
provides a high level of resilience. This approach makes sense for healthcare organizations where bandwidth needs are increasing, can change rapidly or unpredictably, or where there is a requirement to manage the evolution of technology for business or competitive reasons.

Organizations can build a secure private optical network using leased or owned dark fiber to offer very high scalability and capacity. Private build is ideal for organizations that want to implement a private cloud as a strategic investment, and require the security, control, and agility that a private cloud provides for business-critical applications. Building a private optical network requires considerable financial investment and qualified personnel with the appropriate technical expertise but provides a more flexible, agile, and easily scalable solution.

The Nokia optical portfolio includes the following products that enable healthcare organizations to build their own private optical networks:

- **Nokia WaveLite** – an easy-to-deploy, secure optical solution for simple, point-to-point private optical networks.

- **Nokia 1830 Photonic Service Switch (PSS)** – a carrier-grade, secure optical solution for private optical networks and more complex ring or mesh topologies.

- **Nokia 1830 Secure Management Server (SMS)** – a centralized, highly secure management server that generates, distributes, and rotates the symmetric keys used to encrypt data.

**Figure 2. A secure private optical backbone to connect main hospital sites and data centers**

**Nokia WaveLite private optical network solution**

Nokia WaveLite is a purpose-built, easy-to-deploy solution that meets the needs of simple point-to-point private optical networks. WaveLite is typically used to build private optical networks that connect a few large sites and data
centers with 10G or 100G links over metro and regional distances of up to 80 kilometers, including the following use cases:

- **Private optical networking**: create simple, private optical networks to connect to large sites, data centers, and cloud providers using dark fiber, wavelength or Ethernet services.
- **Data center interconnect**: implement a scalable, secure, high-speed, low latency DCI solution for privately-owned, multi-tenant, and cloud data centers using dark fiber.
- **Managed private optical network**: build a dedicated private optical network easily and at lower cost, using service provider dark fiber, wavelength, or Ethernet services.

The WaveLite solution is scalable, secure, resilient, efficient and easy to deploy. The solution comprises separate service aggregation and transport components. It features three multiplexing transponders (muxponders) to aggregate multiple clients onto higher rate optical connections using commonly available pluggable optical modules that support metro and regional distances. These muxponders offer a range of client interfaces, including 10/40/100G Ethernet and 8/10/16/32G Fibre Channel, and support AES 256-bit Layer 1 encryption for data security. Optical line-side interfaces include 10/100/200G speeds over metro and regional distances. The WaveLite solution also includes an amplifier module that extends optical reach to support longer distances and a multiplexer/de-multiplexer module that supports multiple channels. All modules can be configured using an on-demand, user-friendly, web-based interface, and can also be managed using the Nokia Network Services Platform (NSP).

**Nokia 1830 PSS business-critical private optical network solution**

The Nokia 1830 PSS is a carrier-grade, secure optical transport solution for business-critical shared or private optical networks, requiring more complex ring or mesh topologies. The 1830 PSS is typically used to connect multiple large sites and data centers with multiple 10G, 100G, and higher links over metro, regional, and long-haul distances, including the following use cases:

- **Private optical networking**: create point-to-point, ring or mesh private optical networks to connect multiple large sites, data centers and cloud providers using dark fiber, wavelength, or Ethernet services.
- **Data center interconnect**: implement a scalable, secure, very high-speed, very low latency point-to-point or ring solution for privately-owned, multi-tenant, and cloud data centers, using dark fiber or wavelength services.
- **Managed private optical network**: Build a dedicated point-to-point, ring, or mesh private optical network to connect multiple large sites, data centers, and cloud providers, using service provider dark fiber, wavelength, or Ethernet services.
The Nokia 1830 PSS provides flexible transport using agile photonics, multi-layer switching capabilities and network intelligence. It is widely used by network operators and service providers worldwide to offer shared optical network services supporting multiple customers simultaneously. It is suitable for healthcare organizations requiring a carrier-grade, business-critical private optical solution and is widely used by sectors such as banking and finance, energy, government, transportation, public sector and utilities. The key features and benefits of the 1830 PSS platform include:

- Chassis sized to match different application needs, including optical access, aggregation, and backbone with capacities ranging from 240 Gb/s to beyond 8 Tb/s.
- Wide range of client interfaces, including 10/40/100G Ethernet, 8/10/16G Fibre Channel, InfiniBand®, OC192/STM64 SONET/SDH and OTU2/OTU2e/OTU3/OTU4 OTN.
- Wide range of software-controlled, line-side interface cards using PSE-2 super coherent silicon technology to optimize data rates and reach with adaptive modulation, variable baud rates, advanced soft decision FEC and optical super channels.
- PSE-2 enables different data rates and reach, including single carrier 400G over metro and regional distances (150km), 200G over long-haul distances (>1,000km), and 100G over ultra-long-haul distances (>5,000km).
- Advanced packet optical transport interfaces, providing MEF 2.0 carrier Ethernet and MPLS-TP capabilities, seamlessly operating with Nokia IP routing platforms through the common service router operating system (SROS) software.
- TDM migration options through Layer 2 packet interfaces and an adjunct service shelf (MSS) providing a flexible means to evolve toward packet services.
- Optical encryption and security capabilities, including AES 256-bit encryption per wavelength, centralized symmetric key management, and optical intrusion detection.

The Nokia 1830 PSS has been certified with multiple vendors for synchronous data replication and interoperability, including Brocade, EMC, HPE and IBM.

Secure private optical networking

Today’s networks are continuously at risk from internal and external security threats. As well as deploying antivirus and firewall defenses, healthcare organizations must establish comprehensive IT security programs that protect their network infrastructure, data centers, as well as virtual and distributed computing and storage resources.

The Nokia portfolio of private optical network solutions enable a comprehensive approach that support integrated Layer 1 hardware encryption of multiple
protocols per client/line interface. The solution provides scalable, efficient, end-to-end security for business-critical applications with the most stringent security requirements. It has also been certified to Federal Information Processing Standard (FIPS) 140-2 Level 2, Common Criteria Evaluation Assurance Level 3+ (CC EAL3+) and ANSSI QS, also known as ISO 15408.

Figure 3. Quantum-proof symmetric keys using AES 256-bit encryption

The solution uses AES 256-bit encryption using symmetric keys that are generally accepted as safe against quantum computing attacks when compared to asymmetric keys, such as RSA-2048, as shown in Figure 3. Layer 1 encryption ensures all data is encrypted, provides lower latency, and is more bandwidth efficient with less overhead than encryption at higher layers. It provides the lowest cost per bit encrypted to ensure no wasted bandwidth while also being protocol agnostic. As it encrypts all data, it ensures privacy by encrypting the source and destination addresses of higher layer data packets, such as Ethernet and IP. Performing the encryption in hardware ensures fast and efficient bulk data encryption, typically adding less than 20 microseconds of end-to-end latency.

**Encryption key management**

The 1830 Secure Management Server is a separate, secure, and scalable key management tool that manages the encryption keys centrally and independently of the 1830 PSS management system. A central key management approach is more scalable and efficient than the distributed key management approach used by most key management systems. A centralized approach also reduces complexity, establishes a single point of trust for key generation, distribution, and rotation, and provides a network-wide view of encryption management.

Security management is also separate from the optical management, allowing two different organizations to jointly manage the overall solution without compromising data confidentiality and security. For example, a healthcare organization’s security team can manage key management and encryption with a service provider managing the optical network.
Optical intrusion detection

The 1830 PSS solution has an optical intrusion detection capability to automatically monitor optical links and wavelengths for unexpected loss of signal strength from unauthorized optical fiber taping and snooping, as shown in Figure 4.

Figure 4. Optical intrusion detection using OTDR

Optical intrusion detection uses optical time domain reflectometry (OTDR) to monitor received optical power on fiber optical networks on a per wavelength basis, and triggers an alarm if optical loss exceeds expected thresholds over time. OTDR is a common tool in fiber plant construction and maintenance. It can be used to pinpoint fiber cuts and isolate where an intrusion has occurred to within a few meters. This allows for quick remedial action. The tool ensures secure private optical networking for the most stringent business-critical applications. It provides latency optimization to allow optical links to be monitored and tuned per wavelength to ensure the lowest latency for synchronous, near-real-time applications, such as business continuity and disaster recovery (BCDR).

As well as optical intrusion detection, the Nokia 1830 PSS has specific physical and logical security features for individual network elements, including secure device configuration, comprehensive logs with intrusion prevention alarms, and highly flexible optical interface redundancy options.¹

Optical management

The Nokia optical portfolio is fully managed by the Nokia Network Services Platform (NSP). The platform provides an efficient way to configure the 1830 PSS, manage private optical networks, as well as automate, optimize, and assure network services across multiple network layers. The NSP module for optical management is the Network Functions Manager for Transport (NFM-T), formerly known as the Nokia 1350 Optical Management System (OMS). It centralizes multiple network management and operations functions in one unified platform for the Nokia optical portfolio.

¹ For more information about the security capabilities of the 1830 PSS, read the white paper, “Secure Optical Transport with the 1830 Photonic Service Switch.”
The NFM-T module supports multiple technologies, services, and network sizes in one integrated network management platform that supports element, network, service management and OSS/BSS integration. It provides common management for end-to-end operations, including service provisioning over multi-technology optical transport networks. The NFM-T module also supports SDN capabilities that enable automation and optimization of network services on-demand. For healthcare organizations, this means provisioning services in a way that makes optimal use of networks assets, reducing OPEX, lowering TCO, and accelerating ROI.

Nokia wavelength tracking for the 1830 PSS provides end-to-end power control, monitoring, tracing and fault localization for multiple fiber paths and wavelengths. It proactively prevents service degradation and enables the delivery of optical SLAs. Wavelength tracking offers an integrated view of all wavelengths across the network and makes it easier to trace wavelength behavior, isolate faults, and monitor performance, including optical latency and signal-to-noise ratios. The 1830 PSS supports latency optimization on its optical line cards to ensure synchronous applications can be optimized, depending on the distance between sites. On-demand latency measurement with hardware time stamping can be used to check end-to-end round trip delay at network commissioning or after activating features, such as line protection.

Implementing a private IP/MPLS core network

Although managed IP/MPLS VPN services provide resilient, reliable, any-to-any connectivity among multiple healthcare sites, these services no longer provide the scalability and cost/performance to support RTHS applications and the cloud. This is particularly the case for the backbone WAN because VPN services are difficult to scale and costly at higher bandwidths required for private/hybrid clouds.

For healthcare organizations, implementing a private IP/MPLS core network using the Nokia 7750 Service Router (SR) provides an alternative solution to support a private/hybrid cloud, and can be augmented with existing IP VPN services, as shown in Figure 5. A private IP/MPLS core network:

- Provides resilient, reliable, any-to-any connections among multiple sites and data centers.
- Assures scalability, control, and predictability in the core — where it is needed most.
- Enables voice, video, and data to be delivered across a single infrastructure.
- Supports multiple services on a common platform across a common infrastructure.
• Enables traffic engineering and QoS for both legacy and cloud applications.
• Secures data with IPSec or network group encryption.
• Delivers more predictable application performance with more stringent SLAs.
• Extends virtualization among multiple SDN-enabled data centers in the cloud.
• Provides connectivity from smaller sites to SDN-enabled data centers and the cloud.
• Integrates and interoperates with existing managed IP/MPLS VPN services.

Figure 5. Implementing a private IP/MPLS core and augmenting with IP/MPLS VPN services

Nokia 7750 Service Router IP/MPLS portfolio

The Nokia 7750 SR portfolio provides an IP/MPLS implementation with a service-oriented approach that focuses on scalability and quality, as well as per-service OAM. With a service-aware infrastructure, healthcare organizations can tailor bandwidth and quality of service to support critical RTHS applications and a private/hybrid cloud.

A private IP/MPLS core also enables the healthcare organization to leverage the lower costs and higher performance of a private optical network or optical transport services. The healthcare organization also benefits from the control, resiliency, reliability and QoS that the Nokia 7750 SR carrier-grade IP/MPLS routers provide, including the following use cases:
• IP/MPLS overlay: implement an overlay to a private optical network to interconnect multiple sites and data centers while separating traffic from different departments and groups.
• IP routing and switching: support for real-time Layer 2 and 3 services, such as Ethernet Private Line (E-LINE) and Private LAN (E-LAN), Virtual Private LAN Service (VPLS) and IP Virtual Private Network (IP-VPN), to interconnect main hospital sites and data centers.

• Traffic engineering: control bandwidth and separate inter- and intra-site traffic or keep sensitive patient data separate from general data for regulatory or compliance reasons.

• Integration with managed VPN services: integrate the core network with existing managed IP/MPLS VPN services that connect remote healthcare sites.

• Network convergence: support voice, video, and data traffic on a single converged IP infrastructure, enabling circuit-based services to run over a packet-based network.

• Advanced network services: convergence of new network services, (such as flexible bandwidth), and legacy network services, (such as leased lines), on a common IP infrastructure.

• Application-aware networking: identify traffic in real-time and apply parameters such as bandwidth and QoS automatically to ensure no compromise on application performance.

• Data center gateway: extend software-defined networking over the WAN, enabling IT virtualization between data centers and to remote healthcare sites.

The Nokia 7750 SR product family provides high-performance networking for cloud, data center, and remote site connectivity applications. The product family delivers high-performance routing and an extensive range of IP functions and applications, and comprises different chassis options for IP/MPLS edge and core networks depending on size, capacity, and functional requirements:

• 7750 SR series: scales system capacity from 1.2 Tb/s to 9.6 Tb/s HD and is equipped with high-density 1/10/40/100 Gb/s interfaces. The 7750 SR uses the highly programmable Nokia FP4 network processor for high-speed intelligent services and applications for the largest healthcare organizations.

• 7750 SR-e series: scales system capacity from 400 Gb/s to 1.2 Tb/s and is equipped with high-density 1/10/40/100GE interfaces. The 7750 SR-e uses the Nokia FP-3 network processor to provide the foundation for future growth and delivers investment protection for mid-to-large healthcare organizations.

• 7750 SR-a series: designed for lower system capacity and interface density without compromising performance and features. The 7750 SR-a is available in 200 Gb/s and 400 Gb/s system capacities with a range of 10/100/1000 Mb/s and 1/10/40/100 GE interfaces. Using the FP-3 network processor, the 7750 SR-a is ideal for small-to-medium healthcare organizations.
The 7750 SR portfolio is complemented by other products that run the same SR-OS software, including the Nokia 7450 Ethernet Service Switch (ESS), the Nokia 7210 Service Access Switch (SAS) and the Nokia 7705 Service Aggregation Router (SAR). These products are designed for IP/MPLS access and aggregation and are available in different chassis options. Depending on the product and chassis option, they support a range of 1/10/40/100 Gigabit Ethernet interfaces. The 7705 SAR also supports a range of legacy interfaces, including serial, analog voice, T1/E1, T3/E3 and OC-n/STM-n.

**Scalability, reliability, and availability**

The Nokia 7750 SR is a highly scalable platform that provides routing, switching, and multiservice capabilities to support RTHS applications with unparalleled reliability and availability. MPLS fast reroute enables the network to reroute connections around a failure. Because the network is service aware, fast reroute can identify and redirect traffic according to priority. Standby MPLS paths can be provisioned to protect the network against node or connection failures. The Nokia IP/MPLS implementation includes non-stop routing and non-stop service capabilities for unparalleled availability and reliability:

- Non-stop routing ensures that a control card failure has no impact on connectivity and services. Routing and MPLS adjacencies, sessions, and database remain intact if there is a switchover due to control card failure.
- Non-stop service ensures that services are not affected when there is a switchover due to a control fabric module failure. Other resiliency features, such as pseudo-wire redundancy, multi-chassis link aggregation group (LAG), multi-chassis automatic protection switching (APS), and synchronization redundancy also help to maximize network resiliency.

**Multiservice support**

The Nokia 7750 SR offers a flexible network and service environment that enables new IP and Ethernet applications and the continuing support of existing legacy TDM services. These new packet applications are typically more bandwidth efficient when deployed over an IP/MPLS network. All services converge at the network edge, where the required packet handling, such as encapsulation and QoS capabilities, is executed. Different applications are transported over dedicated point-to-point, point-to-multipoint, or multipoint-to-multipoint VPNs.

**Quality of service and traffic management**

QoS and traffic management are essential in a healthcare organization environment where multiple voice, video, data services and RTHS applications converge over a common infrastructure. The Nokia 7750 SR can discriminate among various types of traffic, based on a rich set of classification attributes at Layer 1, Layer 2, Layer 2.5, or Layer 3, and prioritize transmission of higher priority traffic over lower priority traffic. It utilizes extensive traffic
management, using an advanced scheduling mechanism to implement service hierarchies. These hierarchies provide maximum isolation and fairness across different traffic types while optimizing uplink utilization.

With multiple levels and instances of shaping, queuing, and priority scheduling, the Nokia 7750 SR can manage multiple traffic flows to ensure that performance parameters for each RTHS application, such as bandwidth, delay, and jitter, are met for each application.

**IP/MPLS management**

The Nokia IP/MPLS portfolio is fully managed by the Nokia Network Services Platform (NSP) that provides an efficient way to configure the 7750 SR, manage private IP/MPLS networks, as well as automate, optimize, and assure network services across multiple network layers. The NSP module for IP/MPLS management is the Network Functions Manager for Packet (NFM-P), formerly known as the Nokia 5620 Service Aware Manager (SAM). It enables end-to-end network and service management across all domains of a converged, all-IP network to deliver unified operations. This NSP module helps healthcare organizations to maximize operational efficiencies through fast provisioning and troubleshooting, proactive assurance, and flexibility that eases network integration. Visually insightful network and service management deliver enhanced network operations and assurance.

The NFM-P module includes an optional Control Plane Assurance Manager (CPAM) that provides visibility of the IP/MPLS routing plane, and an analytics and reporting application to identify, classify, and analyze applications, enabling healthcare organizations to monitor RTHS usage trends and improve application performance and QoS optimization. Service portals are also available to customize the NFM-P module. To help speed up and simplify network integration, the NSP Connected Partner Program certifies network applications from leading vendors. These include fault, performance, inventory and SLA management, network planning, traffic engineering and other applications.

**Converged IP/optical management**

The Nokia NSP offers management of both the Nokia IP and optical portfolios in converged IP/optical healthcare networks. The NSP provides an SDN management platform that can deliver network services quickly, economically, and on-demand. It unifies service automation and optimization, enabling a more dynamic and responsive network for RTHS and the cloud. Instead of a domain-by-domain approach to automation, the NSP solution handles the complex task of provisioning a converged IP/optical network.
The NSP enables policies to be used to define services. For example, a policy for a real-time application, such as business continuity, might define a specific amount of bandwidth, using a network path with the lowest latency and congestion. If this “best path” is not available, a secondary path can be defined and the policy can switch to the best path when the congestion or bandwidth frees up. This agile and flexible approach is critical to enabling dynamic network services and operations for real-time healthcare and the cloud, as shown in Figure 6.

**Connecting remote healthcare sites using SD-WAN**

Many healthcare organizations use IP/MPLS VPN services to provide secure, resilient, reliable, and any-to-any connectivity among multiple sites, particularly smaller healthcare sites and clinics. Although IP/MPLS VPN services are widely available from many different service providers, they are costly to scale and inflexible — often requiring weeks for moves, adds, and changes. Healthcare organizations need more dynamic, agile, and flexible ways to connect sites when implementing RTHS and moving to the cloud. This is particularly the case when new sites need to be connected and adds, moves, and changes are more frequent for existing sites – particularly if the staff at these sites have little or no networking expertise.
SD-WAN solutions can connect remote healthcare sites to the private cloud more easily, flexibly and at lower cost, as shown in Figure 7. They use secure broadband or internet connections delivered over copper, fiber or wireless, as well as or instead of traditional leased lines or IP/MPLS VPNs. Sites can have multiple connections from different service providers to provide additional capacity and resiliency, or for different types of traffic. Network functions, such as DNS, DHCP, switching, routing, firewall, encryption, WAN optimization and load balancing, are implemented in software as virtual network functions (VNFs). A central policy manager defines, deploys, and enforces overall network functions and advanced services, including network security, and a central network controller downloads the software to server-based appliances or standard servers that act as virtual customer premises equipment (CPE) at each enterprise site.

**Nokia Virtualized Network Services (VNS) solution**

The Nuage Networks Virtualized Network Services (VNS) solution from Nokia provides networking services that remove the limitations of traditional VPNs. The solution, shown in Figure 7, provides an easily deployed, centrally managed, policy-based and software-defined WAN based on standard, server-based appliances. Some benefits of the solution are that it:

- Provides centralized management and policy-based control of network services tailored to the individual requirements of the business.
- Separates network service from network transport, which provides the flexibility needed to choose the most appropriate network connectivity, technology, and backup options for each site.
- Quick and simple moves, adds, and changes to ensure network services match the dynamic business environment.
- Advanced functionality such as firewall, encryption, DNS and DHCP that reduces the requirement for specialist security and network devices at remote healthcare sites.
- Increased network-wide visibility to ensure a more consistent quality of experience for users accessing cloud applications and to reduce the costs associated with compliance and auditing.
The VNS solution includes three key functions that work in concert to lower operational overhead while increasing the network’s ability to respond to changing business needs:

- The Virtualized Services Directory (VSD) is a programmable policy and analytics engine. It provides a comprehensive set of common network functions, such as firewalling, load balancing, IP address management, and domain name services. A flexible network policy framework is used to select these common network functions and to define and enforce policies across the network. The VSD allows the network to be managed centrally, including moves, adds, and changes, using an intuitive graphical user interface. Policies can be viewed and changed on a single site, multiple sites, or network-wide basis. The VSD also collects and reports information about the network and site-specific traffic.

- The Virtualized Services Controller (VSC) is a powerful SDN controller. It provides a robust network control plane function for the network services, maintaining a full view of the network and service topologies. Through the VSC, virtual routing and switching constructs are established to program the network-forwarding plane using the OpenFlow™ protocol. Multiple VSC instances can be federated within and across the network to meet changing business requirements.

- The Network Services Gateway (NSG) provides the network forwarding plane function for the network services. It encapsulates and de-encapsulates user traffic, enforcing Layer 2 to Layer 4 network policies as defined by the VSD. It also enables advanced services defined in the VSD, including network functions such as load balancing, firewall, IPSec, DNS and DCHP.
The NSG acts as virtual CPE and is available as a hardware-based option in four different form factors to meet diverse network throughput, interface, and functionality requirements, or as a software-based option that can be deployed on standard x86-based servers. Enterprises can select the appropriate option depending on the number of users, application needs and operational requirements at each remote site.

Implementing a network support strategy

The implementation of a support strategy for digital technologies and the cloud must embrace both network and IT support. Healthcare organizations can provide in-house support by investing in personnel with the necessary skills or they can outsource support to an appropriate network or cloud specialist, such as a service provider or systems integrator. Alternatively, a healthcare organization can outsource some aspects of support, such as network management, while controlling others, such as security management, as part of its overall IT security strategy.

Nokia Services portfolio

Nokia provides a comprehensive range of consulting, professional, support and managed services for its optical, IP/MPLS, SD-WAN and SDN solutions. These services enable healthcare organizations to implement a network and IT support strategy to achieve the right balance between risk reduction and cost, when implementing a private optical network. In most cases, each healthcare organization’s requirements are different, so Nokia is able to customize its services to meet these individual needs:

- Consulting services such as network analysis and modelling, as well as high-level network design
- Professional services such as consultancy, design, installation and integration
- Support services, including product support, maintenance, and repair
- Managed services, including 24/7 management, using Nokia network operations centers (NOCs).

Nokia build, operate, and transfer services provide a comprehensive solution for healthcare organizations to cost-effectively roll out, operate, and manage their networks, reduce time-to-market and operational risks, and alleviate expertise and resource constraints. Whichever approach a healthcare organization chooses, Nokia implements an end-to-end approach to services across both network and IT domains.
Conclusion

With the move to RTHS and the cloud, and with the increasing availability of more agile and flexible SD-WAN solutions, healthcare organizations need to re-evaluate and determine the best approach to their WAN needs.

Nokia provides private WAN solutions that support a healthcare organization's RTHS and cloud strategy. Our solutions enable healthcare organizations to implement a private cloud for critical business applications and to augment it with virtual private or hybrid cloud services for less critical and on-demand applications. Organizations can build an integrated IP/optical network to connect their main hospital sites and consolidate data centers, offsetting the cost with more flexible, efficient, and lower cost SD-WAN solutions to connect remote healthcare sites and clinics.

For healthcare organizations undergoing the transformation to RTHS and the cloud, Nokia private WAN solutions provide the scalability, security, and control required to enable a private cloud while reducing costs, providing flexibility, and increasing agility to support virtual private and hybrid cloud models.

Acronyms

CPE          Customer premises equipment
DWDM         Dense Wave Division Multiplexing
GDPR         General Data Protection Regulation
IoT          Internet of Things
MPLS         Multi-protocol label switching
MRC          Monthly recurring charge
NAT          Network address translation
NOC          Network operations center
RTHS         Real-time healthcare system
SDN          Software-defined network
SD-WAN       Software-defined wide area networking
SLA          Service level agreement
VNF          Virtualized network function
VPN          Virtual private network
WAN          Wide area networking