IP-optical networks for research and education

Providing high-performance, scalable and secure connectivity

Application note

Abstract

Research and education networks (RENs) have long been where networking innovation happens first. Often years ahead of commercial service providers, RENs adopt advanced technologies to connect research communities, accelerate discovery and support data-intensive collaboration. With innovations in photonic transport, IP routing, open software control, automation and security, RENs can deliver the scalable, secure and sustainable IP-optical infrastructure needed for the next era of education, science and industrial research.

Contents

Introduction

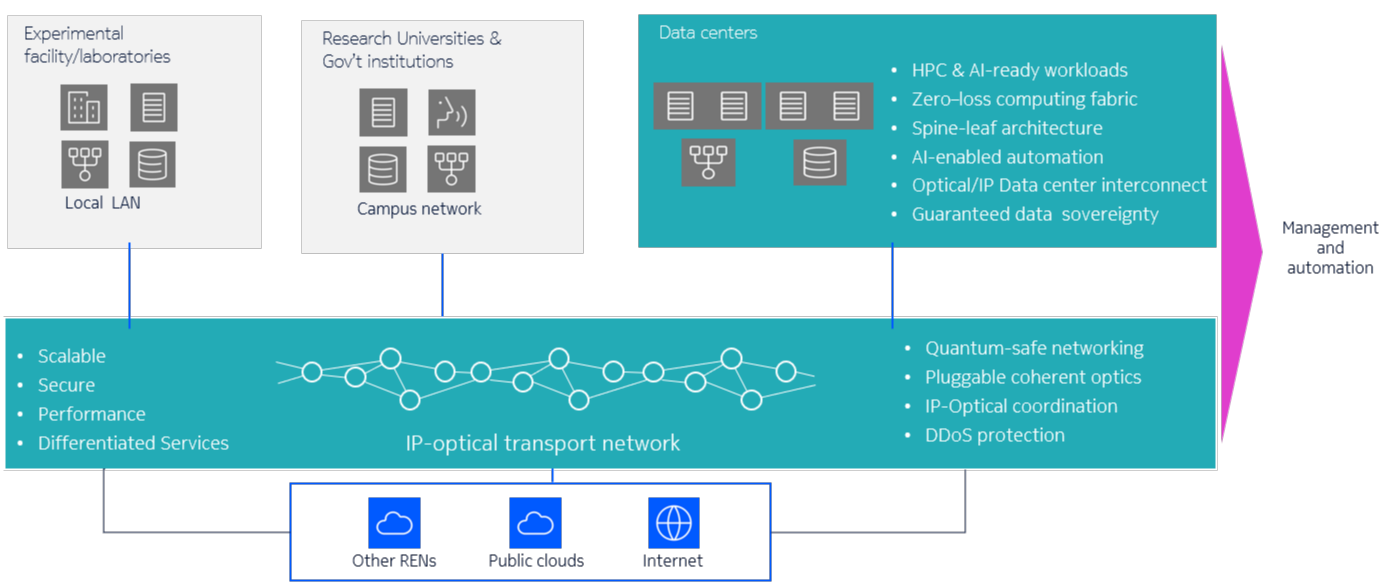
RENs emerged to meet a need that commercial networks were not designed to address: sustained, high-performance collaboration among universities, laboratories, research institutions and public-sector science communities. Over time, they evolved from specialized academic backbones into critical digital infrastructure that connects national and regional research ecosystems with campuses, data centers, high-performance computing facilities, cloud platforms and global peers.

This evolution is accelerating as research workflows become more distributed, data-intensive and time-sensitive. AI models, HPC clusters, scientific instruments, research clouds and shared data repositories generate traffic patterns that are difficult to predict and increasingly difficult to serve with static or siloed network designs.

As a result, RENs need networks that can scale capacity efficiently, provide deterministic performance, protect sensitive research data, and simplify operations across IP, optical, data center and cloud domains. Modern IP-optical architectures give RENs the flexibility to connect distributed communities and resources while improving resiliency, security, automation and sustainability.

Purpose and goals of RENs

RENs exist to enable the collaboration, connectivity and trusted data exchange that modern research and education depend on. By connecting universities, laboratories, public-sector research organizations, cloud platforms and high-performance computing resources, RENs help accelerate scientific discovery, support digital education and enable innovation across national and regional research ecosystems.



Enable global, national and regional research collaboration

Scientific discovery depends on the ability to share knowledge, data and expertise across institutions and borders. RENs provide the trusted connectivity that allows researchers, educators and students to collaborate securely and efficiently, helping turn distributed expertise into faster innovation.

Provide high-capacity cloud and HPC connectivity

As research becomes more data-intensive, RENs must support terabit-scale connectivity between universities, research institutions, government facilities, HPC centers, data repositories and cloud platforms. This capacity allows research communities to move, analyze and share large data sets in near real time while maintaining performance, reliability and control.

Protect identity, data and research integrity

Because RENs carry sensitive academic, government and industry-sponsored research, they must protect user identity, data confidentiality and service integrity across a broad and distributed environment. Security must be built into the network architecture to support trusted collaboration without slowing the exchange of ideas and data.

Achieving these goals requires RENs to overcome a growing set of network, security and operational challenges as research becomes more distributed, data-intensive and dependent on cloud and high-performance computing resources.

REN networking and security challenges

The higher-education landscape is exceptionally complex. Research institutions and universities—some with tens of thousands of students, researchers, faculty and staff—need to support robust communications and collaboration. The network is the foundation for almost everything that happens at these institutions and for collaborative research among scientists and students within and across various universities and research organizations. Legacy networking infrastructure may not be up to the task.

With the proliferation of complex networks comes the increased risks of cyber attack. With sensitive research in advanced fields such as genomics, medicine and high-tech in the higher-education institutions, the data that is shared, the devices and users are subject to cyber attack and IP theft. The RENs, because they are also a provider of the internet exchange, can be at the center of distributed denial of service (DDoS) and ransomware attacks.

Due to their large footprint, RENs also pose challenges of network management—specifically to monitor and configure the vast number of devices, often from multiple vendors. Network automation with artificial intelligence/machine learning (AI/ML) tools are needed for agile configuration and compliance management.

The challenges include complexity, scalability, automation and security.

Network complexity

Many networks support different organizations: interconnectivity (WAN, data center, cloud) poses significant network complexity.

Scalability

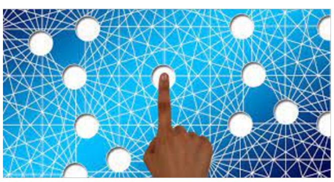
Networks connect millions of users and thousands of components over wide areas.

Automation

Complexity and scale of the networks can result in management and provisioning challenges. Network automation tools helps meet the challenge.

Security

Given the complexity and scale of the network, the security perimeter is vast. Securing data against multiple attack vectors requires defense-in-depth solutions.



Network complexity

The large number of researchers and scientists belonging to different organizations and their interconnectivity (WAN, data center, cloud) pose significant network complexity challenges.

Scalability

NRENs span states, countries and continents, and they connect thousands of components and millions of users. The networks need to be highly scalable in a sustainable manner.

Automation

The complexity and size of the networks can result in management and provisioning challenges. Network automation tools can help alleviate these challenges. Intent-based network management and automation are critically important to the network and security administrators at the network operations center (NOC) of a REN. The lack of resources and expense of staffing is a gating factor in R&E institutions, and most of them are funded by non-profit organizations.

Security

Given the complexity and size of the RENs, the security perimeter is extremely vast. The nature of the data is sensitive and confidential. The reliability of RENs can be tested by DDoS threats, quantum computing attack, and other types of attacks.

To achieve these goals and address these challenges, RENs must deliver a set of high-performance IP and optical services that support internet access, secure collaboration, cloud connectivity and specialized research workloads.

Core IP services for RENs

RENs need to provide a variety of IP services, including internet transit, Layer 2/Layer 3 (L2/L3) VPNs and security.

Internet transit

Transit allows traffic from an ISP or customer network to cross or "transit" the transit provider network to connect to the rest of the internet.

Internet transit is also referred to as internet or IP transit.

RENs provide reliable, high-performance and secure IP transit service to their customers—the R&E institutions.

L2/L3 VPN

The VPN service can be used for connectivity between clusters, grids, clouds and high-performance computing centers (HPCs), allowing them to share distributed resources.

VPNs are used in a variety of ways, from a long-term infrastructure with a high demand for intensive network usage to quick point-to-point connections for a conference demonstration.

L3 VPNs are offered for many-to-many or one-to-many environments and data isolation across the REN for assured performance (10G to 100G) and security.

Security

RENs carry data from many users. Some of this traffic is government-related research; other traffic is industry-sponsored research. All of this has implicit value to someone and is a potential target.

The REN team needs to secure the logical and physical infrastructure of the REN and all data crossing the network, responding to network security incidents and mitigating breaches, weaknesses and risks.

Essentially, this security relates to the prevention, detection, reporting and mitigation of incidents targeting the REN infrastructure.

Technologies pertinent to RENs

In this section we discuss technologies that help RENs support AI-driven discovery, high-performance computing (HPC), data-intensive scientific instruments, cloud interconnect and secure campus services. These include IP networking solutions such as Ethernet VPN (EVPN) and segment routing, high-capacity IP/optical transport, coherent routing, data center interconnect, multi-layer security, automation and sustainability-focused operations.

AI, HPC and cloud-ready connectivity

Modern research increasingly depends on AI modeling, high-performance computing clusters and scientific instruments that generate massive data sets. RENs therefore need high-capacity, low-latency and deterministic connectivity that can move data between campuses, laboratories, supercomputing facilities, public clouds and private research clouds without compromising reliability or security.

EVPN

There is inherent complexity in today's networking environment. There are a wide range of services, each using different protocols to deliver each service: L2 VPN, L3 VPN, data center interconnect (DCI) and software-defined wide area network (SD-WAN). This leads to management complexity and increased service delivery costs for new services.

In addition, services cross multiple WAN domains, multiple cloud domains, multiple branches and multiple exchanges. Finally, there is the added challenge of automation to deliver on-demand services with cloud-speed interconnect.

EVPN unifies service delivery with network and operational simplification. EVPN has a single control plane, the flexibility for any data plane plus extensive interworking functions. In addition, EVPN is common to the data center and WAN; this ensures seamless service delivery across WAN and data center boundaries.

Finally, agile and dynamic services require end-to-end orchestration across all services. Cloud-friendly EVPN enables end-to-end orchestration to simplify operations support system management and provisioning with a single VPN technology that unifies service delivery through service automation and rapid service enablement.

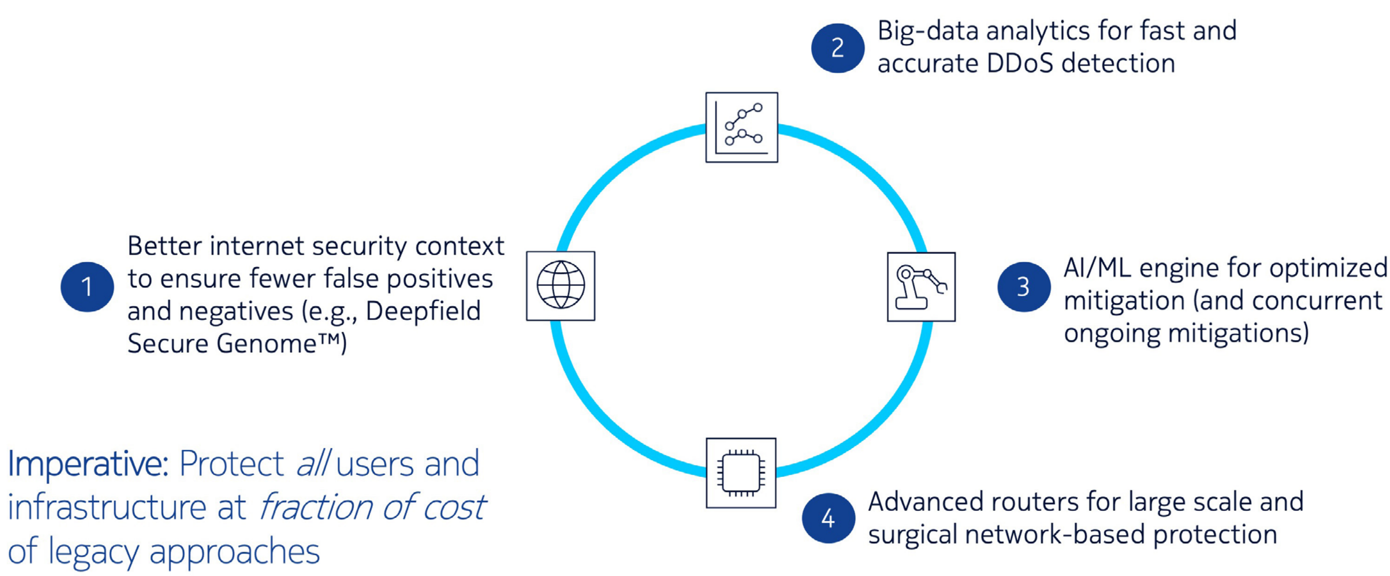
Segment routing

Segment routing is a source routing tunneling mechanism in which the paths are encoded as sequences called segments, which are advertised by link-state routing protocols: Intermediate System-to-Intermediate System (IS-IS) and Open Shortest Path First (OSPF). The biggest advantage of segment routing is that it removes all the protocol complexity. Segment routing is becoming the unified transport layer of choice because it is simple to understand, provides the path control and protection you need, and is very scalable and stateless.

Advanced DDoS protection

RENs require next-generation DDoS protection that leverages big data analytics, AI/ML and advanced routing technology (see Figure 1).

Figure 1. Next-generation DDoS protection

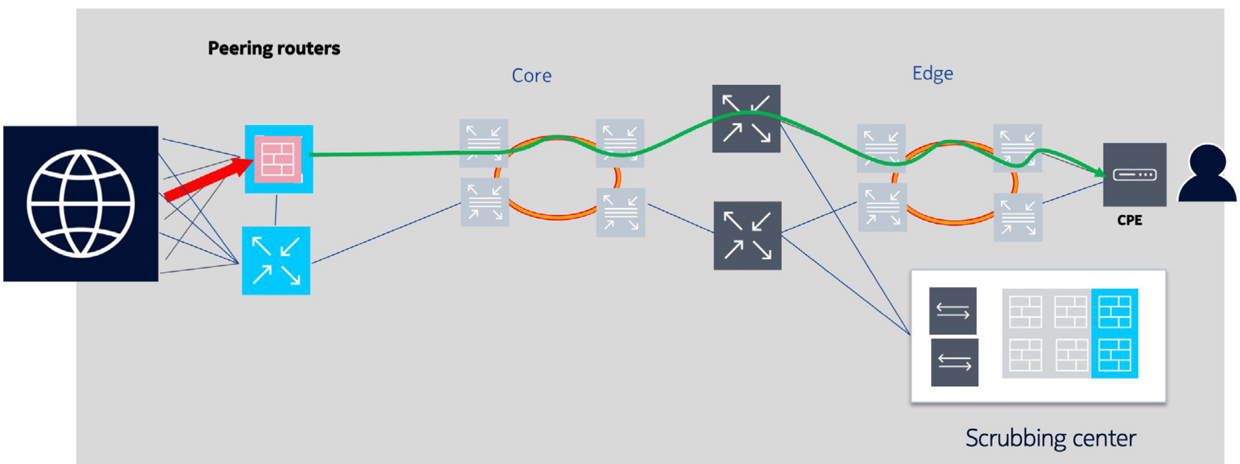


As shown in Figure 2, advanced routers can also be part of the DDoS defense by:

- Leveraging the latest network processing for in-line, terabit-scale, deep filtering
- Stopping attacks at the network edge
- Building a surgical filter list for each attack.

Advanced routers do all of these things without any service performance degradation.

Figure 2. Advanced routers for network-based DDoS mitigation

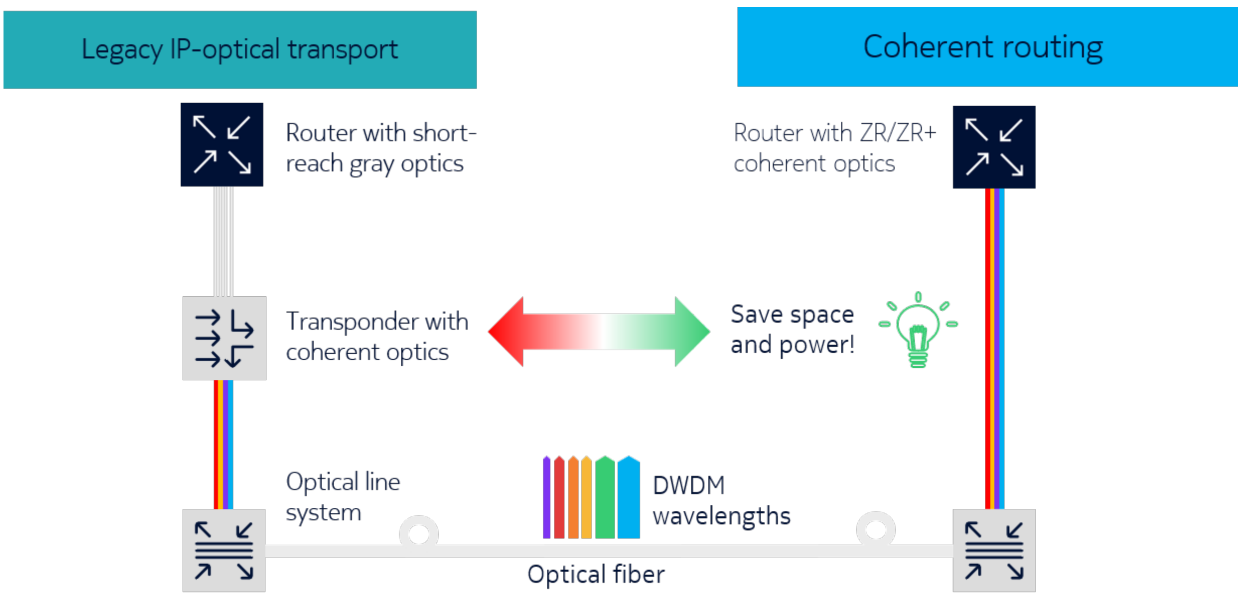


100G/400G/800G coherent routing

Conventional IP networks deploy short-reach gray optics to connect to a transponder with dense wave division multiplexing (DWDM) optics. The DWDM optics emit tunable wavelengths with coherent detection that can be carried across the optical transport network over any distance.

Coherent routing (see Figure 3) leverages profile-optimized 100GE, 400GE and 800GE digital coherent optics to interconnect IP routers directly and efficiently over coherent DWDM wavelengths that can span distances of hundreds or even thousands of kilometers. It delivers the value of IP over DWDM technology to any network, enabling a smooth evolution for legacy networks and services.

Figure 3. Coherent routing using DWDM optics



This approach saves on cost, space and power by eliminating the additional optical-electrical-optical conversion in external DWDM transponders while achieving similar port densities to conventional IP-optical interfacing methods using gray optics.

Coherent routing can be deployed over a DWDM optical layer as well as over dedicated fiber spans.

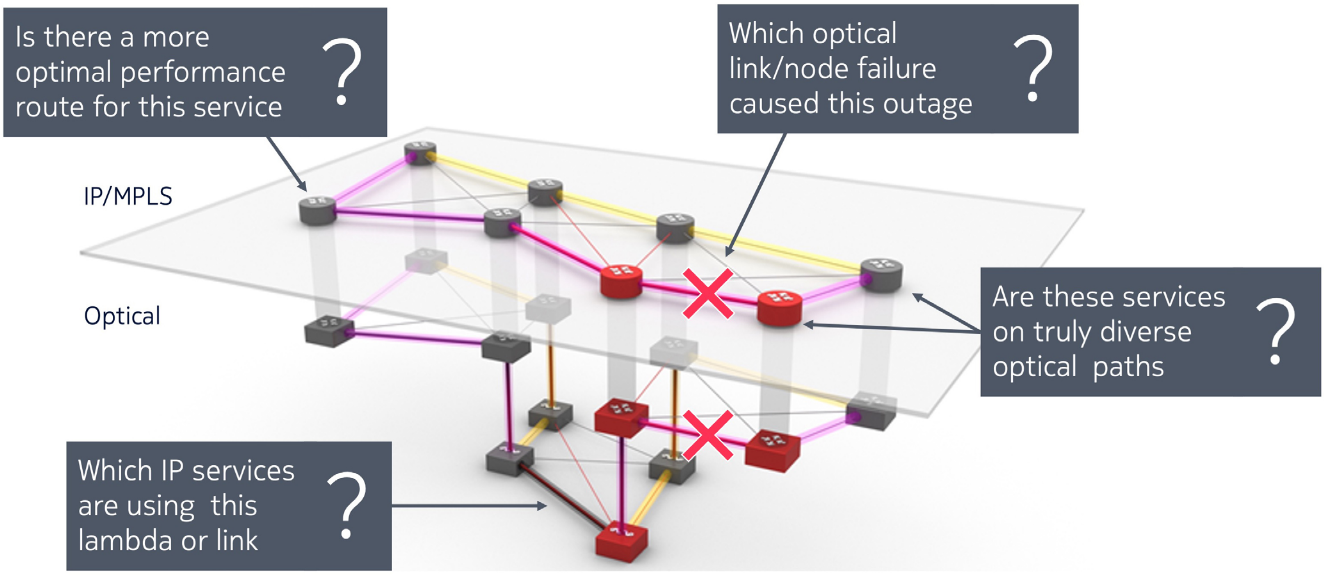
IP-optical coordination

In recent years IP routing and optical transport have gone through a significant technology evolution to address the connectivity and capacity needs of the digital era.

However, IP routing and optical transport are in many cases still deployed and operated as separate domains; this makes it difficult to coordinate and automate cross-domain service provisioning and assurance processes. The separate domains also duplicate functions and costs.

Figure 4 shows the multi-layer management and coordination challenges caused by separate IP and optical layers in a network.

Figure 4. Interdependencies and cross-impacts of separate IP and optical layers

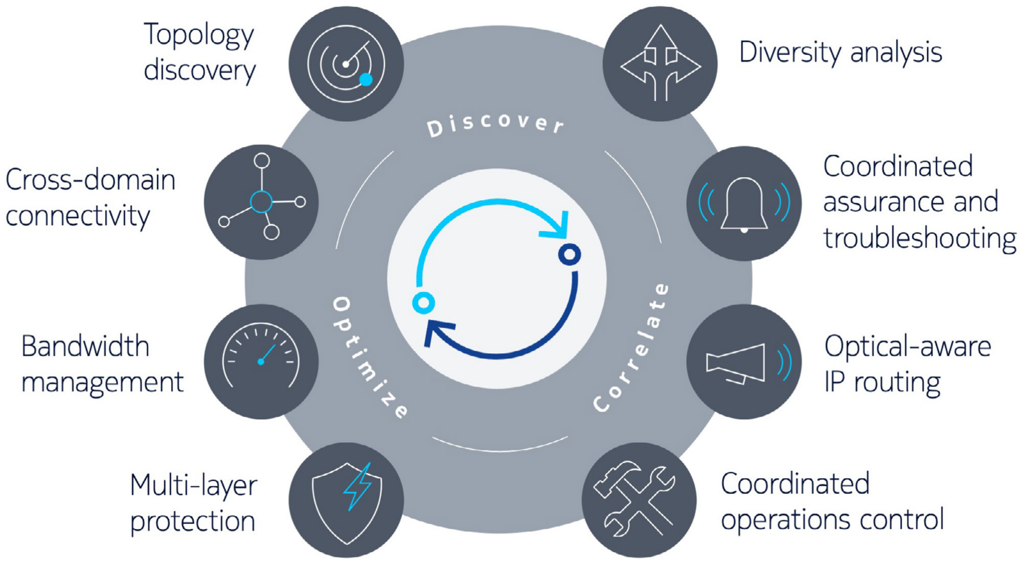


The advent of pluggable coherent optics delivered via Nokia Coherent Routing helps network operators build faster and more efficient IP transport solutions for 100 Gb/s, 400 Gb/s and 800 Gb/s connectivity. Coherent routing also scales and simplifies network operations by managing and coordinating IP routing and optical transport domains through automation.

The IP-optical coordination and automation shown in Figure 5 delivers the following operational benefits:

- Streamlined operations, for OPEX savings
- Better network utilization, for CAPEX savings
- Higher quality and reliability, for improved customer satisfaction
- Faster service provisioning, for faster time to revenue.

Figure 5. IP-optical coordination and automation



Data center interconnect and campus reach

IP/optical networking can support REN services across national backbones, regional aggregation, research data centers and campus environments. This enables REN operators to scale connectivity between high-performance computing sites, data repositories, internet exchanges and education campuses while maintaining service separation, predictable performance and operational control.

Taken together, these technologies form the foundation of a modern REN architecture: high-capacity IP-optical transport, simplified service delivery, secure connectivity, automation and support for AI, HPC, cloud and data center interconnect use cases. The next section shows how these capabilities can be brought together in an integrated Nokia solution for research and education networks.

Putting this all together with Nokia

Nokia's research and education solution can be organized across three complementary domains: a transport and WAN foundation that connects campuses, research sites, cloud on-ramps and national backbones; a data center interconnect foundation that links distributed research data centers, HPC facilities and cloud environments; and a data center fabric foundation that supports AI, HPC and cloud workloads inside research data centers. Across these domains, Nokia helps RENs scale capacity more efficiently by combining coherent optics, silicon-powered routing, compact platforms and automation to reduce space, power and operational complexity while supporting long-term sustainability goals.

Built on proven Nokia operating systems

A key strength of the Nokia portfolio is the common software foundation that helps RENs simplify operations across backbone, edge, DCI and data center domains. Nokia SR OS supports scalable routing, MPLS, segment routing, EVPN, service assurance and deterministic QoS for high-performance WAN and DCI services. Nokia SR Linux brings an open, Linux-based and automation-ready operating system for modern transport, WAN and data center fabric environments, with model-driven management, streaming telemetry and extensibility for cloud-native operations. Together, SR OS and SR Linux give RENs a consistent, programmable and resilient foundation for secure service delivery, automation and operational simplicity.

Transport and WAN infrastructure for REN connectivity

The transport and WAN layer gives RENs a scalable, resilient foundation for connecting national and regional backbones, campuses, laboratories, HPC facilities, research data repositories, cloud on-ramps and internet exchanges. Nokia brings together coherent optical transport, IP routing, built-in encryption, Deepfield IP network intelligence, DDoS-aware capabilities and automation to help RENs scale capacity, protect critical services and deliver predictable performance across large, distributed environments.

Nokia applies a multi-layer cybersecurity approach that helps RENs protect users, data and services without adding operational complexity. This approach combines trusted SR OS and SR Linux platforms, quantum-safe multi-layer cryptography, Deepfield IP network intelligence and automated DDoS protection. Together, these capabilities help secure research collaboration, internet transit, cloud access, DCI and backbone services from the access edge to the WAN and optical core.

For RENs, quantum-safe protection is especially relevant because sensitive research data may retain value for years. By applying a defense-in-depth approach across both IP and optical layers, RENs can strengthen crypto resilience, reduce exposure to harvest-now-decrypt-later risks, and protect high-value collaboration, cloud access and data center interconnect services without forcing a wholesale network redesign.

The Nokia WAN portfolio supports this modernization with capabilities for scale, security, automation and sustainability. Coherent optical transport and IP routing provide high-capacity connectivity; access and aggregation platforms extend services closer to campuses and research sites; Deepfield adds IP network intelligence and DDoS protection; NSP supports IP and multi-layer WAN automation; and WaveSuite supports optical network automation for faster, more efficient wavelength operations.

Nokia NSP and WaveSuite for IP and optical automation

Nokia NSP and WaveSuite help RENs turn IP-optical coordination into operational simplicity. NSP enables service provisioning, IP and optical resource coordination and performance assurance across backbones, regional networks, campuses, cloud on-ramps and research sites. WaveSuite focuses on optical planning, provisioning, monitoring and optimization, helping teams scale wavelength services with less manual effort and greater consistency.

Nokia Deepfield for IP network intelligence and DDoS protection

Nokia Deepfield gives RENs the visibility and automated protection needed for secure, high-capacity internet-facing services. By analyzing traffic patterns, security context and attack behavior in real time, Deepfield helps protect internet transit, peering, cloud access and research collaboration services at the network edge while supporting faster detection, response and mitigation of DDoS threats.

Nokia IP routing portfolio

Nokia's IP routing portfolio gives RENs a flexible foundation for secure access, aggregation, service routing, backbone growth and data center interconnect. The Nokia 7210 Service Access System (SAS), 7705 Service Aggregation Router (SAR) and 7250 Interconnect Router (IXR) extend secure services closer to campuses, institutions and distributed research sites, supporting IP/MPLS, segment routing, Carrier Ethernet and legacy service migration with consistent QoS and resilience. For larger-scale service routing, the Nokia 7730 Service Interconnect Router (SXR) and 7750 Service Router (SR) families provide the capacity, security and automation-ready operations needed for REN scale and DCI. The 7730 SXR extends deterministic IP services deeper into access, aggregation, campus edge and distributed research locations, while the 7750 SR delivers high-capacity IP edge and core routing, advanced services and security at scale for cloud access, backbone expansion and data-intensive AI/HPC workloads.

Nokia Optical transport Portfolio

Nokia's optical transport portfolio gives RENs the ability to construct a network matched to their institutional needs, be it in support of a coherent routing solution as described above or through delivery of optical layer manages services to member institutions. The portfolio is designed to deliver flexibility through chassis and transponder modules which can match the capacity, service type and optical wavelength requirements of any network.

Nokia 1830 PSS (Photonic Service Switch)

The 1830 SS is a multi-reach photonic platform utilizing coherent detection and Nokia's industry leading PSE coherent signal processors. Building on the zero-touch photonics approach, which enables easier operations for reduced costs and faster wavelength services deployment, the 1830 PSS exceeds requirements for NREN networks. Several chassis sizes are offered to match the needs of each network node, with modules that perform optical transponding, multiplexing and other functions.

Nokia 1830 PSI-M (Photonic Services Interconnect – Modular)

The Nokia 1830 PSI-M platform provides industry-leading performance, scalability and simplicity for DCI applications. The massive shift to cloud-based IT services by enterprises, communications service providers and internet content providers is dramatically lowering software application costs while expanding computation and storage scalability. The 1830 PSI-M offers optimized optical network solutions for the cloud era.

Nokia 1830 GX (Global Express)

The 1830 GX Series provides industry-leading flexibility in an open compact modular solution, with support for transponder, switchponder and OLS in a single platform. With 300-mm and 600-mm chassis options, it can be optimized for virtually any application, from DCI and metro to long-haul and subsea. With seamless support for multiple generations of optical engines, from 200G through 2.4 Tb/s (2 x 1.2 Tb/s per wavelength), as well as game-changing Super C and Super L functionality, the 1830 GX solution provides industry-leading economics and unmatched network scalability with up to 100 Tb/s of capacity per fiber.

Data center fabric for AI, HPC and cloud workloads

REN data centers increasingly need high-performance fabrics for AI training, HPC, cloud services, research storage and science DMZ environments. Nokia data center fabric solutions combine SR Linux, high-performance switching platforms and Event-Driven Automation (EDA) to support reliable leaf-spine designs, predictable performance, real-time telemetry, digital twin validation and operational simplicity across front-end, back-end and management networks.

Nokia Event-Driven Automation for data center fabric operations

Nokia Event-Driven Automation (EDA) provides the automation and operations layer that helps REN teams deploy and operate data center fabrics with greater confidence. Built for cloud-native, intent-based operations, EDA supports design, validation, deployment and lifecycle operations with digital twin capabilities, pre- and post-checks, revision control, rollback and event-driven workflows. This helps reduce human error and improve reliability for AI, HPC, research cloud and science DMZ environments.

Nokia data center fabric portfolio

Nokia 7215 Interconnect System (IXS), 7220 Interconnect Router (IXR) and 7250 Interconnect Router (IXR) platforms give RENs a flexible foundation for scaling data center fabric connectivity. The 7215 IXS supports resilient out-of-band management, the 7220 IXR provides high-density leaf and spine switching, and the 7250 IXR scales to high-capacity spine, super-spine, aggregation, DCI and WAN-facing roles. Together, they help RENs support AI, HPC, research cloud and science DMZ workloads with predictable performance, operational consistency and room for growth.

Data center interconnect for distributed research infrastructure

Data center interconnect (DCI) is a critical capability for RENs because research workloads increasingly span multiple data centers, campuses, HPC facilities, cloud on-ramps and science DMZ environments. Nokia helps RENs build DCI and data center gateway (DCGW) capabilities as an integrated function across IP, optical and data center domains, combining high-capacity transport, low-latency connectivity, service-aware routing, encryption, traffic engineering and automation. The DCGW function provides a scalable and secure entry and exit point between data center fabrics, WANs, public clouds, internet peering and distributed research sites, enabling service interworking and policy control across domain boundaries.

RENs can also use coherent pluggable optics as a simple and economical way to scale DCI connectivity, adding high-speed coherent wavelengths directly where capacity is needed while reducing the need for separate transponder equipment, space and power. This allows RENs to extend secure, deterministic services between distributed research sites, stitch EVPN-based services across WAN and data center boundaries, and support AI, HPC, research cloud and storage environments with predictable performance, operational simplicity and end-to-end visibility.

Conclusion

RENs are entering a new phase in which AI, high-performance computing, cloud services and data-intensive scientific instruments are reshaping network requirements. To accelerate discovery, RENs need infrastructure that can move massive data sets reliably, securely and efficiently across campuses, research centers, public institutions, internet exchanges and cloud environments.

The deployment of a ubiquitous, national IP and optical REN provides the community with an essential backbone to connect educational institutions, enable research collaboration and foster economic development.

Nokia offers a comprehensive IP/optical networking portfolio for RENs, combining scalable routing, coherent optical transport, data center interconnect, automation and multi-layer security. Together, these capabilities help RENs deliver high-capacity, sustainable and secure connectivity for AI-driven research, education services and cross-institution collaboration.

For more information about Nokia research and education network solutions, please visit:

www.nokia.com/public-sector/research-and-education/research-and-education-networks/

Abbreviations

AI	artificial intelligence
BGP	Border Gateway Protocol
CAPEX	capital expenditures
CE	customer equipment
CPE	customer premises equipment
CWDM	coarse wave division multiplexing
DCGW	data center gateway
DCI	data center interconnect
DDoS	distributed denial of service
DWDM	dense wave division multiplexing
EDA	Nokia Event-Driven Automation
EVPN	Ethernet VPN
HPC	high-performance computing
IP	Internet Protocol
ISP	internet service provider
MEF	Metro Ethernet Forum
ML	machine learning
MPLS	Multiprotocol Label Switching
NSP	Nokia Network Services Platform
OPEX	operating expenditures
OTN	optical transport network
PSI-M	Nokia 1830 Photonic Services Interconnect - Modular
PSS	Nokia 1830 Photonic Service Switch
SDH	Synchronous Digital Hierarchy
SDI	serial digital interface
SONET	Synchronous Optical Networking
SR	Nokia 7750 Service Router
TDM	Time Division Multiplexing
VPN	virtual private network
WAN	wide area network

About Nokia

At Nokia, we create technology that helps the world act together.

As a B2B technology innovation leader, we are pioneering networks that sense, think and act by leveraging our work across mobile, fixed and cloud networks. In addition, we create value with intellectual property and long-term research, led by the award-winning Nokia Bell Labs, which is celebrating 100 years of innovation.

With truly open architectures that seamlessly integrate into any ecosystem, our high-performance networks create new opportunities for monetization and scale. Service providers, enterprises and partners worldwide trust Nokia to deliver secure, reliable and sustainable networks today – and work with us to create the digital services and applications of the future.

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

Document code: CID 212828