Connecting clouds with Nokia Data Center Gateways

Ensure reliable, high-performance interconnectivity for data centers, clouds, WANs and the internet

Introduction

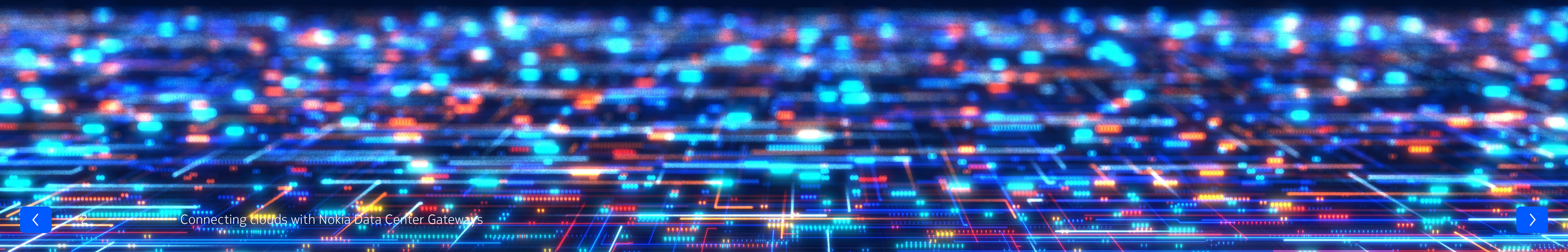
Data centers are the backbone of Data centers are the backbone of businesses in the digital age. As businesses expand globally, their data centers are no longer isolated entities. Instead, they are part of a complex network of interconnected data centers that work together to meet the service demands of customers and users.

This has created the need for robust and reliable network connectivity to enable seamless communication and data transfer between different locations.

The network connectivity directly impact the performance, security and availability of business-critical applications and services. Data Center Gateways (DCGWs) address growing connectivity needs by providing a reliable and scalable entry and exit point. DCGW enable organizations to connect data center fabrics, also known as clouds (both private and public), while ensuring the integrity and availability of their data and applications.

The role of the DCGW will become even more important and demanding as more organizations make artificial intelligence (AI) applications a key part of their operations. AI applications require greater performance and scale and are often highly scrutinized mission-critical applications. Mass market adoption of AI will push data center networks to their limits relative to performance and scalability.

This e-book examines the key features, capabilities and benefits of DCGWs



Modern cloud technologies

Modern data center designs use Ethernet VPN (EVPN), Virtual Extensible LAN (VXLAN) and Border Gateway Protocol (BGP) protocols to deliver highly scalable network overlay solutions that support single-tenant and multi-tenant environments.

- VXLAN provides the overlay network, allowing for network virtualization and micro-segmentation. Virtual tunnel endpoints (VTEPs) encapsulate layer 2 Ethernet frames with VXLAN headers for transmission over the underlying IP network.
- EVPN provides the mechanism for this overlay, managing the distribution of Media Access Control (MAC) and IP address information by leveraging the BGP protocol.
- BGP serves as the transport control mechanism for EVPN routes, enabling efficient and scalable route distribution across the data center.

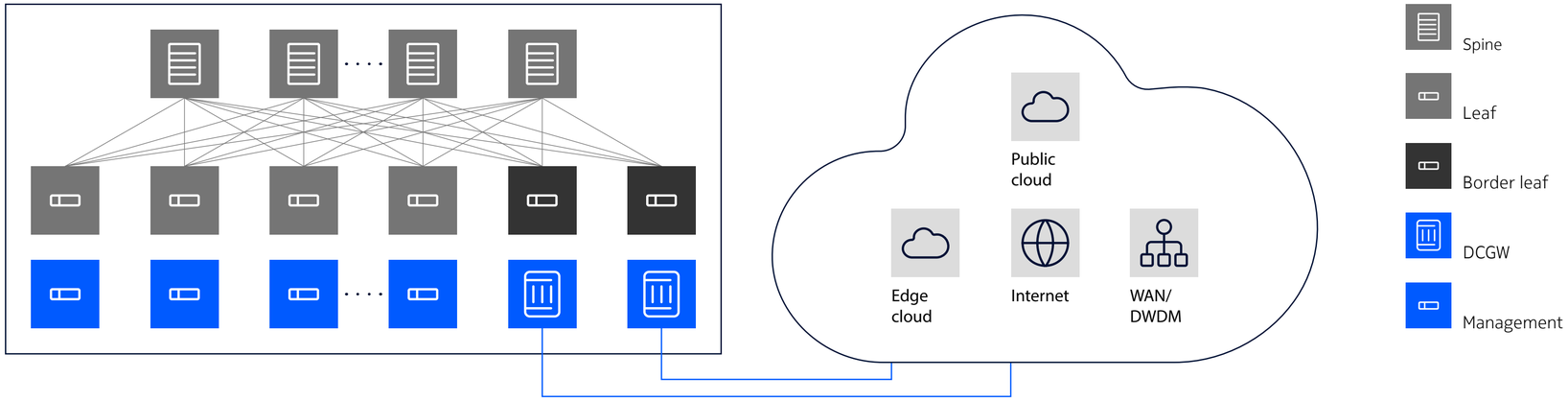
These technology enablers supersedes designs previously used in building data center fabrics because it allows for efficient layer 2 extension over layer 3 domains. It dramatically improves scalability by significantly reducing flooding and by handling broadcast, unknown unicast and multicast (BUM) traffic with enhanced efficiency, leading to optimized network utilization.

EVPN provides support for layer 2 and layer 3 services. It offers the flexibility required to meet diverse application requirements, along with enhanced mobility for virtual machines and containers. This facilitates dynamic resource allocation and improves overall system agility.

In addition, internet exchange providers (IXPs) can use an EVPN framework to support IP peering, which allows them to connect networks to the internet and peer them with other networks.

With network programmability, data center networks can achieve high reliability, simplicity and adaptability by using tools that eliminate human error. This reduces disruptions and service downtime to near-zero levels. It also decreases operational effort by enabling streamlined lifecycle management and seamless integration with a diverse array of IT service management systems, event notification platforms and cloud management solutions.

Data center networking components



The data center networking infrastructure is composed of interconnected elements that collectively enable seamless communication and data transfer between diverse resources.

The network fabric serves as the backbone of the data center network and facilitates the flow of information between storage systems, compute nodes and other critical components.

Spine nodes

Spine nodes function as non-blocking layer 3 switches with high port density and bandwidth capabilities. These nodes connect to each leaf node in a full-mesh topology and create a robust and scalable network fabric. Importantly, spine nodes connect only to leaf nodes and not to each other, maintaining a clear hierarchical structure.

The concept of layered spine architecture is used in large-scale deployments with multiple pods. In this architecture, spine nodes also connect to all spine nodes at the higher layer. This design allows for easy capacity expansion through the addition of more spine nodes when uplink oversubscription occurs. In addition to their primary routing functions, spine nodes often serve as EVPN route reflectors for leaf nodes.

Leaf nodes

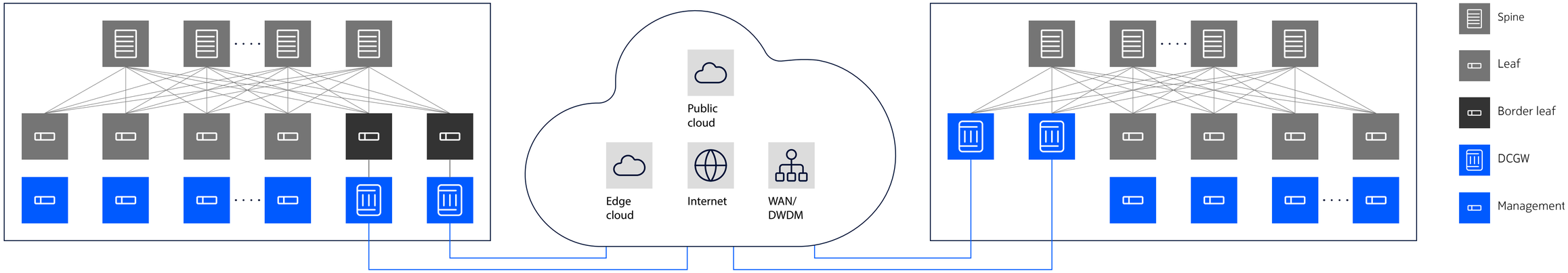
Leaf nodes combine layer 3 routing and layer 2 switching capabilities. These nodes feature high port density, support for various port speeds and optical transceivers, and a full non-blocking architecture. They connect directly to host devices or servers and are often deployed in pairs to ensure rack-level resiliency.

Each leaf node maintains connections to every spine node in the fabric. However, for large-scale deployments with multiple pods, the leaf nodes connect to local spine nodes that are part of the pod. Leaf nodes also function as hardware virtual tunnel endpoints (HW-VTEPs). In this role, they facilitate the creation of layer 2 and layer 3 VPN services and enable overlay connectivity between virtual and physical endpoints.

Border leaf nodes

Unlike typical leaf nodes that connect directly to servers, border leaf nodes provide a simple gateway function between the data center fabric and external networks. The border leaf node connects to every spine node to ensure full connectivity within the data center fabric. It acts as a termination point for EVPN encapsulation that exists within the data center and provides a VLAN hand-off to the provider edge (PE) router that resides at the edge of the wide area network (WAN).

This setup requires manual configuration for each service, which makes it unpractical, especially for multi-tenant data center designs. Known as a “decouple model,” it requires two devices: a border leaf node and a PE node. It is typically implemented when the data center and WAN are operated by different administrative entities and clear demarcation is needed.



Data center networking components

Data Center Gateway nodes

The DCGW acts as a comprehensive solution for traffic flowing between data centers or between data centers and external networks. The gateway participates in the data center fabrics EVPN/VXLAN infrastructure, connects to every spine node, and plays the role of border leaf node. The gateway also participates in the multiprotocol label switching (MPLS) and Segment Routing IPv6 (SRv6) infrastructure and plays the role of PE router. It reduces the number of devices required by integrating the border leaf and PE nodes into a single node. This approach is ideal in scenarios where the data center and WAN are operated by the same administrative entity.

Known as the “integrated model,” this approach provides many advantages compared to the decoupled model, including greater scalability, easier management and enhanced integration between the domains. In certain large-scale deployments featuring multiple pods, border leaf nodes can act as aggregation points for all the links originating from the hierarchical spine layers. This approach minimizes the number of interfaces required on the DCGW nodes.

This e-book focuses on the integrated model because it is the most widely deployed solution.

Management nodes

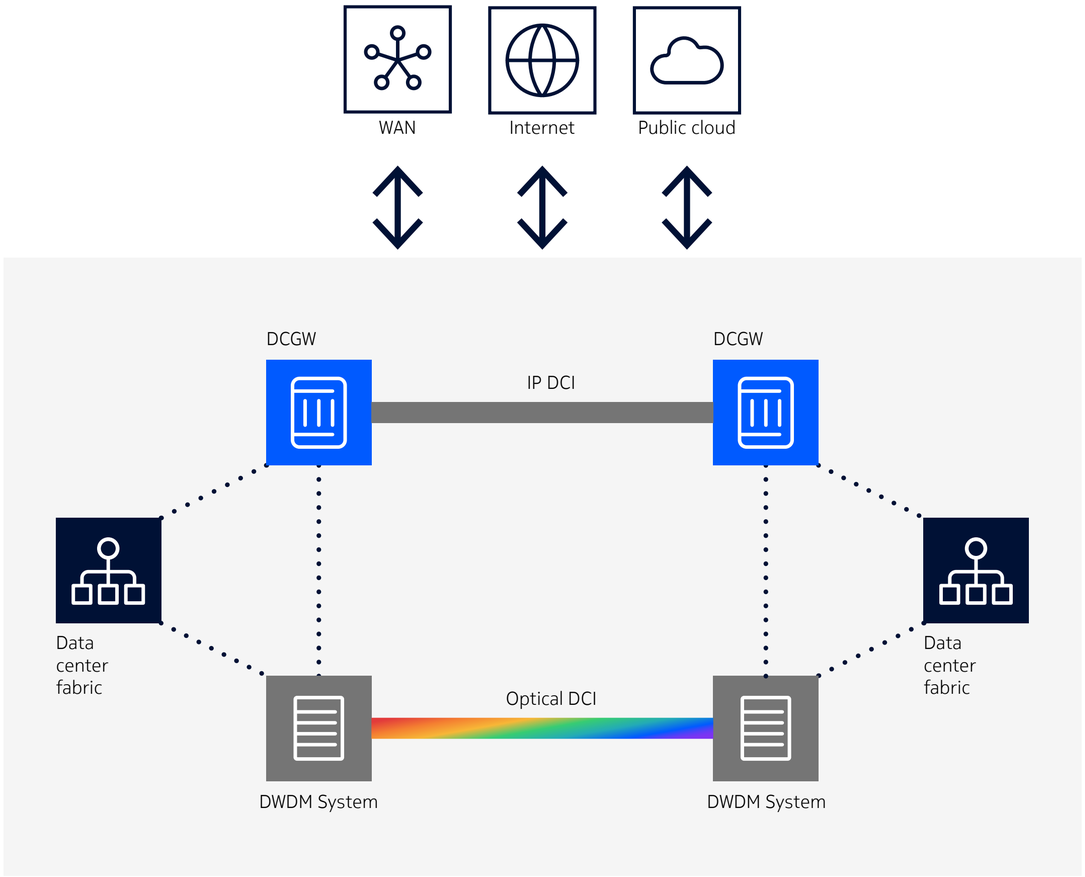
A top-of-rack (ToR) management switch is used to connect all servers, spine nodes and leaf nodes to the out-of-band management network. The ToR design commonly deploys one dedicated switch for each server rack. The out-of-band network is a separate physical and logical network dedicated to management and node provisioning. Its main objective is to provide an alternative path for critical equipment during initial turn up or in case of in-band network failures.

DCGW use cases and requirements

The DCGW supports a comprehensive set of use cases, including IP and optical DCI, IP peering and hybrid cloud interconnection.

Each use case mandates a certain set of capabilities and features, which are described in the following pages.

The DCGW in the cloud networking ecosystem



IP data center interconnect use case

DCGWs enable organizations to support IP Data Center Interconnect (DCI) across diverse WAN technologies, including IP-only networks, MPLS (using LDP, RSVP or SR-MPLS) and emerging SRv6 tunnels. Supporting a diverse range of technologies enables organizations to build more flexible and agile connections between their geographically distributed clouds.

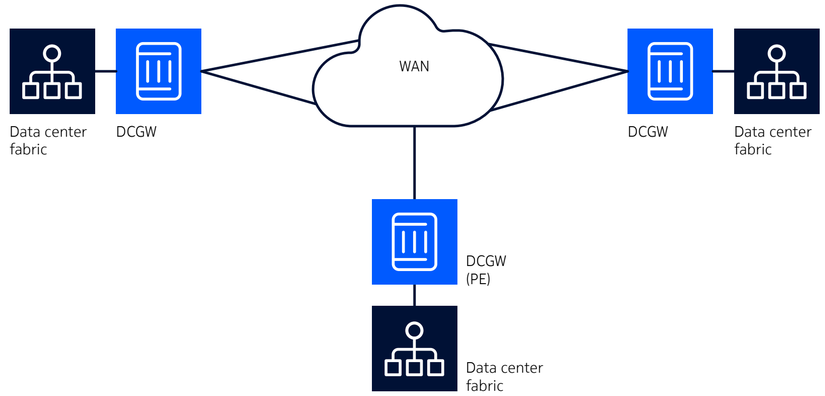
The DCGW allows seamless interworking of services between data center and WAN environments, along with legacy data centers built in the pre-EVPN era. For instance, the gateway enables smooth integration of EVPN services in the data center with IP-VPN or Virtual Private LAN Service (VPLS), or with EVPN in the WAN. This interworking ensures consistent service delivery and simplifies network management across the entire infrastructure. It provides the best performance for scaling single- or multi-tenant data center infrastructure.

Modern DCI solutions prioritize performance and security. The DCGW offers low-latency, line-rate traffic encryption, which ensures that data transfer across data centers remains secure without compromising speed or performance.

Because of the nature of Ethernet or IP and the various interface speeds of these interconnections, buffering and Quality of Service (QoS) mechanisms are essential for maintaining optimal application performance across interconnected data centers.

By leveraging the WAN, organizations can achieve greater network agility, improved resource utilization and enhanced operational efficiency while maintaining the high levels of security and performance required for today's distributed data center deployments.

DCGW can assume the role of a Provider Edge (PE) router, and it will be managed by the WAN network team.



IP peering for data centers use case

Data center internet peering has become an essential strategy for organizations seeking to optimize network performance and resilience. By leveraging internet peering, data centers can establish direct connections with multiple internet service providers (ISPs) and content delivery networks (CDNs) to significantly enhance their reach and improve the user experience.

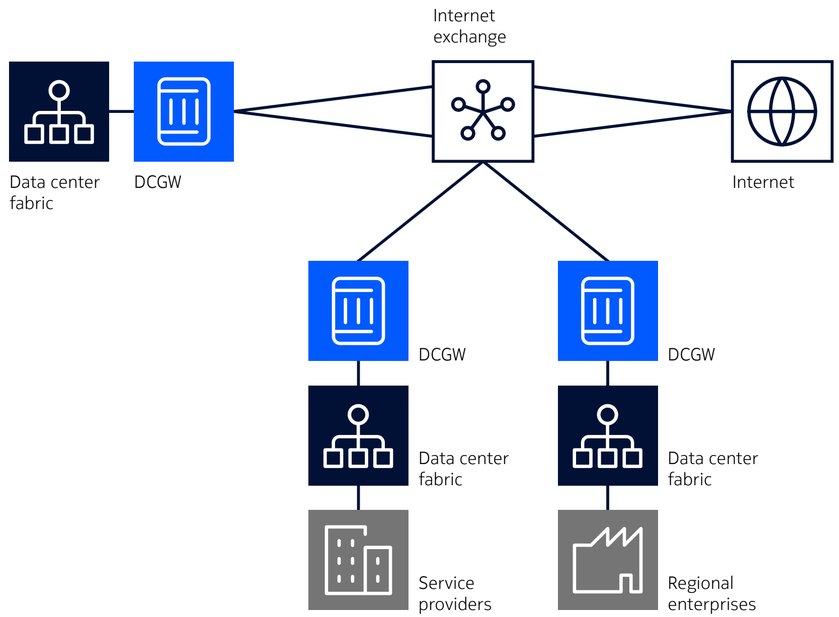
A key aspect of this approach is the implementation of multiple internet BGP feeds. This multi-homing strategy provides several benefits:

- **Increased resiliency**: By connecting to multiple ISPs, data centers can maintain internet connectivity even if one provider experiences issues.
- **Improved performance**: Multi-homing allows for intelligent traffic routing, which directs users to the most efficient path.
- **Enhanced user experience**: Reduced latency and improved routing lead to faster, more reliable connections for end users.

Security is paramount in internet peering scenarios, and DCGW solutions offer robust protection mechanisms, including:

- **Distributed denial of service (DDoS) mitigation**: Advanced systems can detect and mitigate DDoS attacks to protect the data center against volumetric threats.
- **Traffic filtering**: Sophisticated filtering techniques identify and block malicious traffic before it enters the data center fabric.
- **Policy-based redirection**: Suspicious traffic can be automatically routed to security appliances for deeper inspection, ensuring thorough protection without compromising performance.

By implementing these internet peering strategies, cloud providers can achieve improved network performance, enhanced security and greater control over their connectivity. This approach leads to a better experience for end users and supports more efficient and resilient operations for the organization as a whole.



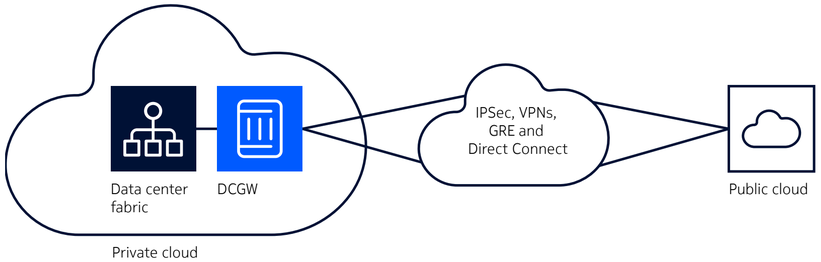
Hybrid cloud interconnect use case

Hybrid cloud interconnect is a crucial strategy for organizations seeking to optimize their digital infrastructure and leverage the strengths of various cloud environments. This approach creates a robust and flexible ecosystem for modern applications and services.

Connectivity between on-premises infrastructure and public cloud requires secure and scalable architectures to facilitate smooth data and workload migration. These aims can be achieved through encapsulation and tunneling techniques such as IPsec VPNs and Generic Routing Encapsulation (GRE), or simply through direct connect services offered by cloud providers.

By implementing hybrid cloud interconnect strategies, organizations can create a cohesive and efficient infrastructure that spans multiple cloud environments. This approach enhances overall system performance and reliability and provides the flexibility that organizations need to adapt to evolving technological landscapes and business requirements in the AI-driven era.

Private cloud to public cloud connectivity requires secure and scalable architectures to facilitate smooth data and workload migration.



Nokia 7750 Service Router Data Center Gateway advantages

Built on the powerful and field-proven Nokia 7750 Service Router (SR), the Nokia DCGW provides all the characteristics that modern data centers need to support traditional and AI workloads.

Reliability

The Nokia 7750 SR offers exceptional reliability. At its core, the 7750 SR leverages the Nokia FP network processor to provide deterministic packet forwarding performance under all network loading conditions. This ensures consistent and predictable operation even during peak traffic periods. A combination of deep ingress and egress buffering, packet pre-classification and pre-buffering, and granular QoS capabilities ensures superior performance for critical applications across multiservice IP networks.

The 7750 SR supports non-stop routing and in-service software upgrades, which allow for seamless failover and minimal service interruption during software upgrades and hardware failures. These reliability features, coupled with the router's high-performance architecture, make the 7750 SR an invaluable asset for building resilient and dependable network infrastructures.

Nokia 7750 Service Router Data Center Gateway advantages

Scalability

The 7750 SR offers unrivaled scalability to meet the growing capacity demands. Its high-density design supports a wide range of high-speed interfaces, including 800GE and 400GE. The router also offers flexible breakout capabilities for lower speeds to enable efficient network expansion and increased bandwidth. The powerful FP network processor allows the 7750 SR to handle a substantial number of BGP sessions while maintaining multiple copies of the full internet routing table. These capabilities ensure robust and reliable routing performance even in large-scale deployments.

The 7750 SR supports advanced streaming telemetry capabilities for all counters to provide real-time visibility into network performance and enable proactive monitoring and troubleshooting. This comprehensive scalability, combined with the router's ability to stream flow-level data and insights in near-real time, allows network operators to efficiently manage network growth, optimize performance and respond quickly to changing traffic patterns and demands.

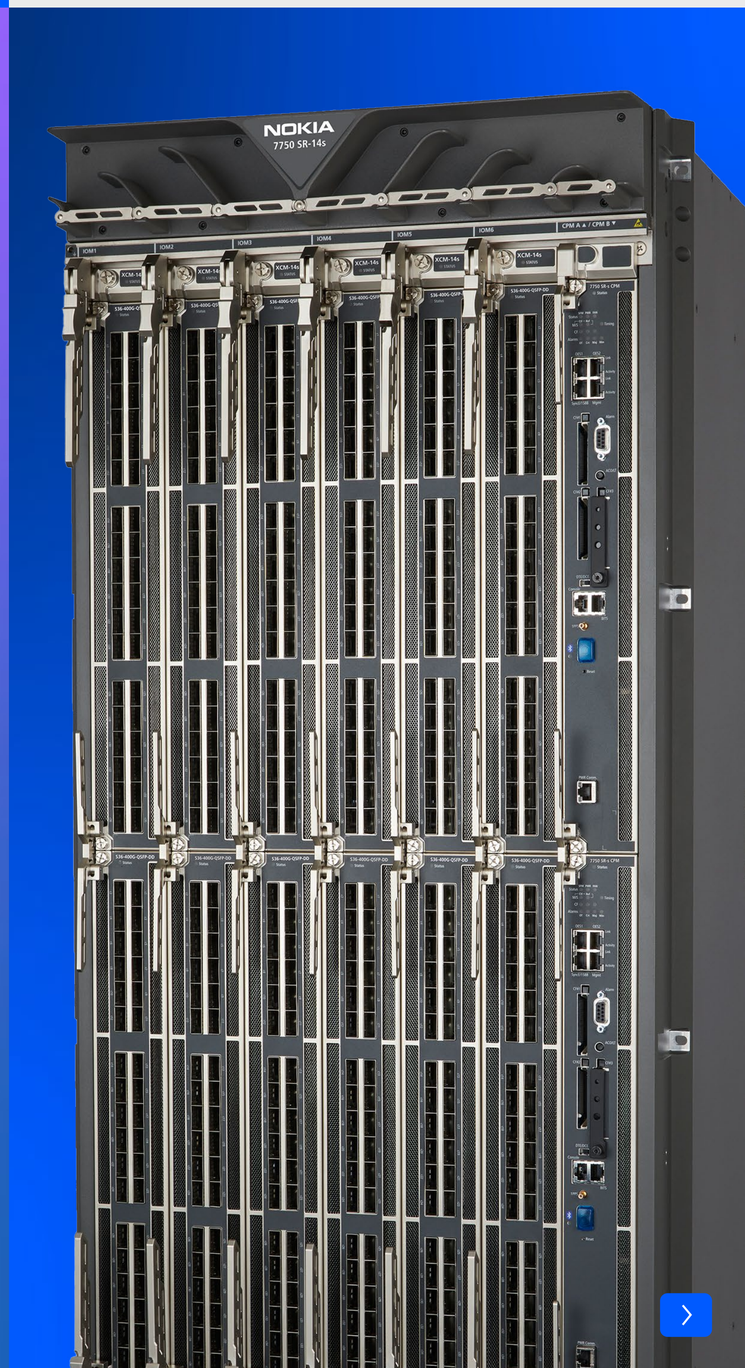
Nokia 7750 Service Router Data Center Gateway advantages

Multiprotocol versatility

The 7750 SR offers exceptional multiprotocol versatility by supporting a wide range of services that are typically found in IP networks, including VPLS, IP-VPN and EVPN. For transport technologies, the 7750 SR accommodates various protocols and encapsulation methods, including VXLAN, GRE, SR-MPLS, RSVP-TE, LDP and SRv6, to enable efficient traffic routing and network optimization over multiple domains. Robust layer 2/layer 3 multicast capabilities built into the router, including EVPN mLDP and OISM, ensure efficient delivery of multicast traffic across the network infrastructure.

The SR OS also provides the industry's most flexible interworking capabilities between legacy and modern IP protocols and encapsulation at the control and data plane levels for seamless, automated, scalable and fast convergence network designs.

The 7750 SR incorporates comprehensive operations, administration and maintenance (OAM) features, including TWAMP, STAMP, s-BFD, CFM and EFM. These features enable proactive network monitoring, troubleshooting and performance management. They also support high-scale deployments.



Nokia 7750 Service Router Data Center Gateway advantages

Security

The 7750 SR offers robust security features that provide comprehensive protection for modern networks. Its multilevel DDoS mitigation capabilities, powered by Nokia Deepfield Defender in combination with the router's hardware, can effectively mitigate DDoS attacks at the network edge.

To support data center confidentiality, integrity, and availability, the 7750 SR supports quantum-safe IP cryptography as part of Nokia's Quantum-Safe Networks, featuring certified onboard quantum-safe key generators with quantum-safe entropy and strength. It also supports key rotation and delivery, enabling a range of key generation, configuration, and management options for our IP cryptography solutions.

Operators have the choice of multiple traffic encryption capabilities: IPsec for end-to-end encryption, MACsec for hop-by-hop encryption or ANYsec, which combines the best of both technologies.

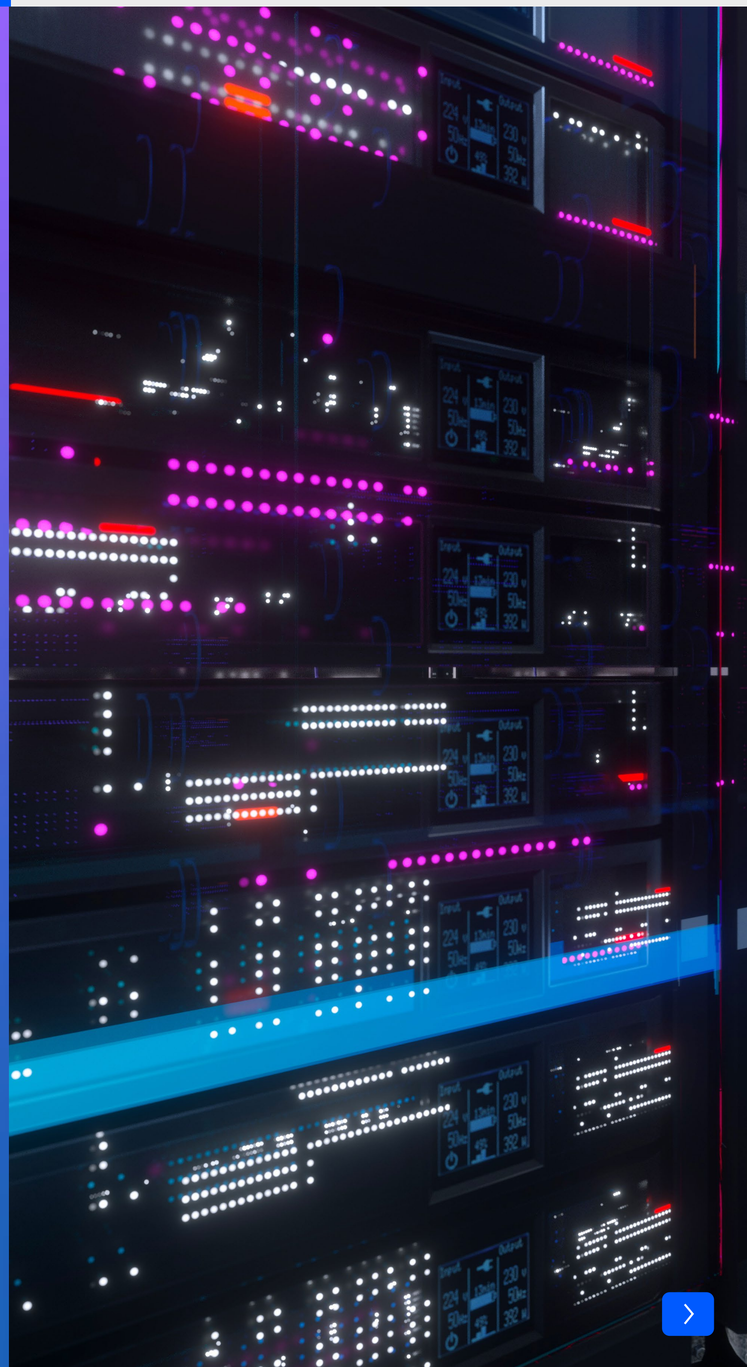
The 7750 SR incorporates advanced distributed control plane protection mechanisms and peering router security features to protect critical routing functions from potential attacks. The SR OS secure boot feature enhances its security posture by ensuring the integrity of the system from startup.

Nokia 7750 Service Router Data Center Gateway advantages

Modern automation capabilities

The 7750 SR offers powerful modern automation capabilities that significantly reinvent network operations and management. It enables model-driven management using YANG-based data modeling for programmability, and supports interfaces such as NETCONF, gRPC (gNMI and gNOI), and the model-driven CLI (MD-CLI). The router also facilitates multivendor software-defined networking (SDN) control and integration through OpenFlow, Path Computation Element Protocol (PCEP) and model-driven network element management. Collectively, these features provide a comprehensive suite of tools for advanced network automation and programmability.

This combination of automation, standardized configuration and real-time telemetry empowers network operators to make data-driven decisions, optimize network performance and respond quickly to changing network conditions. The end results are improved service quality and reduced operating costs.



Nokia 7750 Service Router Data Center Gateway advantages

Sustainability

The 7750 SR enables highly sustainable IP networking by offering innovative features that significantly reduce the network's energy consumption and environmental impact. Silicon innovation is the largest driver of energy savings by consolidating the on-package network processing unit, with smaller geometry and integrated memory design.

The energy usage is reduced to an even greater degree when combining the innovative approach to selectively deactivating idle line card/system components, and the use of next-generation optics and 800GE routing.

The mechanical cooling and line card designs incorporate belly-to-belly cages, dual-sided printed circuit boards (PCBs), honeycomb mesh air intakes, intelligent fan control, and airflow that minimizes turns. The 7750 SR enables operators to take advantage of full router density by utilizing high-powered digital coherent optics (DCOs), resulting in significant energy savings by minimizing the need for additional optical equipment.

These sustainability-focused capabilities lead to reduced emissions and a lower carbon footprint, making the 7750 SR an ideal choice for service providers and enterprises committed to building environmentally responsible, high-performance IP networks.

Nokia 7750 Service Router Data Center Gateway portfolio

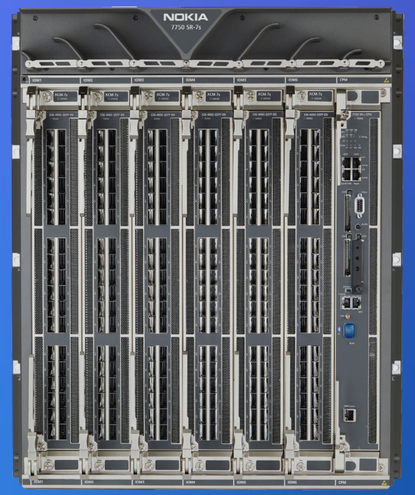
The Nokia 7750 SR portfolio includes the 7750 SR-1x series, 7750 SR-s series, 7750 SR series, 7750 SR-a series, and 7750 SR-e series, with systems that scale up to 216 Tb/s full duplex and offer flexible pay-as-you-grow licensing options. Operators can tailor each system to meet their exact networking requirements in the most economical way.

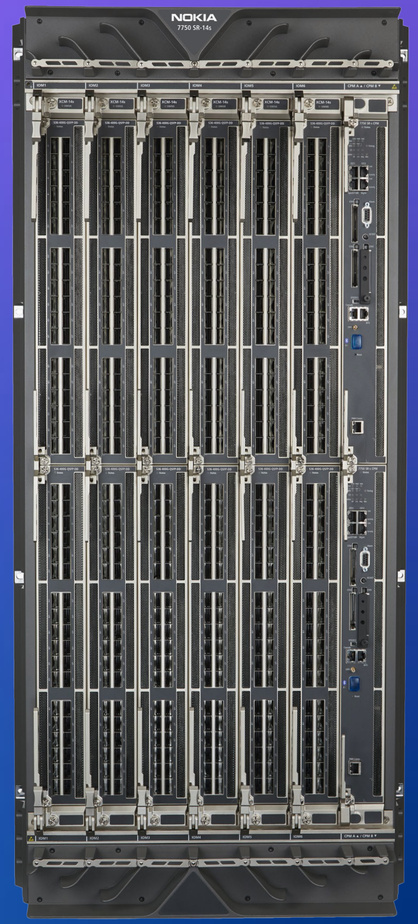
The 7750 SR maintains deterministic performance at full scale and under all network loading conditions. Multiple demanding applications can run on a single system without performance degradation.

Nokia and its customers have tested the 7750 SR extensively in the world's largest and most demanding networks over a period of decades.

The 7750 SR portfolio delivers exceptional performance across a diverse range of applications, including:

- Edge router
- Core router
- Backbone router
- Peering router
- DCGW
- IP security gateway
- Broadband edge gateway
- Multi-access IP aggregation





Evolving data center connectivity with optical DCI

Fiber optic networks offer superior scalability and bandwidth capacity for interconnecting data center fabrics compared to traditional Ethernet services. Coherent technology and Dense Wavelength Division Multiplexing (DWDM) support the growing demands of modern computing environments by enabling efficient, high-performance connectivity between data centers.

Depending on the distance, speed and capacity requirements, operators can use either of these options to provide optical connectivity.

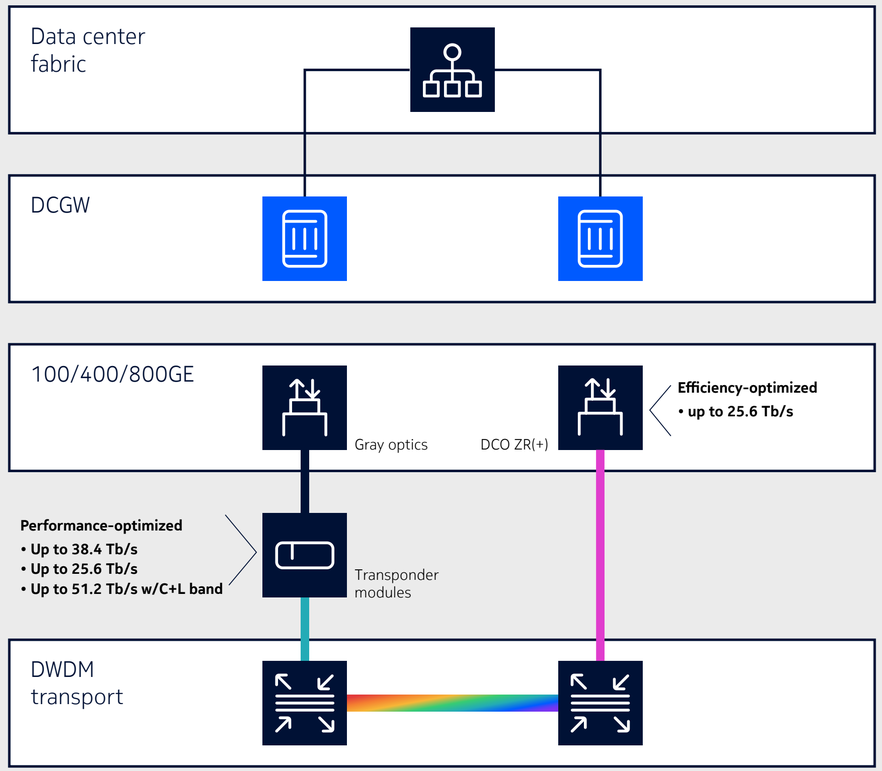
The Nokia DCGW can use pluggable DCOs with speeds ranging from 100G to 400G per DWDM wavelength. Support for 800G per wavelength is expected to be available soon. This approach allows operators to use full router density with optical transponders while minimizing the number of devices they need for metro and regional use cases.

For simple, short-distance, single-span networks, 400ZR technology is the perfect choice because of its simplicity and cost-effectiveness. The more capable 400ZR+ option, designed to address extended reaches, including flexible Ethernet rates and modulation types, can be used over reconfigurable optical add–drop multiplexer (ROADM) networks. The Nokia Coherent Routing solution provides simplified IP–optical coordination based on standard transport interfaces.

For an IP-centric solution, a single pair of fibers can carry 3.2 Tb/s over a distance of up to 120 km by leveraging the pluggable line system (QSFP-LS) solution.

For maximum capacity over the fiber optic cable and to get even higher reach, the DCGW leverages high-performance optical transponders that can operate over multiple optical spectrum bands. Nokia sixth-generation super-coherent Photonic Service Engine (PSE-6s) opens a new frontier in scalable, high-performance and power-efficient optical networking. The PSE-6s supports speeds up to 1.2Tb/s per wavelength and delivers the highest capacity and transmission performance available in real-world networks.

Optical Data Center Interconnect



Summary

The Nokia DCGW offers exceptionally versatile deployment options. Network operators can choose between fixed and modular configurations that offer a wide range of interface options to meet the varied connectivity needs of modern data center networks.

The Nokia DCGW also enables operators to interconnect data center fabrics securely and effectively over any transport technology to provide the scale and the reliability required for the always-connected, AI-driven world.

Find out more

- Nokia Data Center Gateway
- Nokia Data Center Networks
- Nokia Ethernet VPN (EVPN)
- Nokia Segment Routing
- Nokia Coherent Routing
- Nokia Optical DCI solution
- Nokia IP network security

References

- EVPN Interworking with IPVPN
- RFC 9625: EVPN Optimized Inter-Subnet Multicast (OISM) Forwarding
- RFC 9014: Interconnect Solution for Ethernet VPN (EVPN) Overlay Networks
- Ethernet VPN Virtual Private Wire Services Gateway Solution
- Domain Path (D-PATH) for Ethernet VPN (EVPN) Interconnect Networks

Nokia OYJ
Karakaari 7
02610 Espoo
Finland

Tel. +358 (0) 10 44 88 000

CID:214741

nokia.com

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.

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.