Cloud interconnect solutions for enterprise and public sector

Data center interconnect solutions for the cloud era

Application Note
Abstract

Cloud interconnect provides data center interconnect (DCI) solutions for the cloud era, allowing large enterprises, industries and public sector customers to connect their data centers in a private cloud of virtualized compute and storage. These virtualized data centers use software-defined networking (SDN) to automatically allocate resources and balance workloads across servers and multiple sites.

Enterprises looking to outsource some of their IT to cloud providers can use cloud interconnect as a way to match cost models to their business needs. Cloud interconnect solutions can also connect data centers in an enterprise’s private cloud with IT assets hosted in third-party data centers, such as service provider or carrier-neutral co-location facilities. This allows enterprises to implement flexible, more cost effective virtual private and hybrid cloud models that embrace public cloud services.

Nokia offers a choice of cloud interconnect solutions that provide the flexibility, scalability and security to support current DCI needs — along with the capacity, performance and agility required to support cloud interconnect across different cloud types.
## Contents

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abstract</td>
<td>2</td>
</tr>
<tr>
<td>Introduction</td>
<td>4</td>
</tr>
<tr>
<td>Enterprise use of cloud services</td>
<td>5</td>
</tr>
<tr>
<td>Cloud interconnect — DCI for the cloud</td>
<td>7</td>
</tr>
<tr>
<td>Nokia solutions for cloud interconnect</td>
<td>8</td>
</tr>
<tr>
<td>Implementing private cloud interconnect using secure optical transport</td>
<td>10</td>
</tr>
<tr>
<td>Expanding cloud interconnect to the virtual private cloud</td>
<td>12</td>
</tr>
<tr>
<td>Using Ethernet and IP VPNs for cloud interconnect</td>
<td>13</td>
</tr>
<tr>
<td>Extending data center virtualization over the cloud</td>
<td>15</td>
</tr>
<tr>
<td>Extending cloud interconnect to hybrid clouds and public cloud services</td>
<td>16</td>
</tr>
<tr>
<td>Summary</td>
<td>17</td>
</tr>
<tr>
<td>Acronyms</td>
<td>17</td>
</tr>
</tbody>
</table>
Introduction

Today, many large enterprises, government and public center organizations, and companies operating across a range of industries, use data center interconnect (DCI) solutions to consolidate and link data centers and create a private cloud of virtual machines and storage.

Increasingly, these organizations are using software-defined networking (SDN) to automatically allocate resources and balance workloads in and across multiple data centers. In addition, they are looking to outsource non-critical IT to cloud providers as a way to match cost models to business needs. Currently, it’s difficult for organizations to scale their IT quickly and cost effectively to match the growing demand for compute and storage. As a result, they want to adopt more agile, outsourced, operating expense (OPEX)-based cloud IT models.

As these organizations move to cloud IT, they need DCI solutions — cloud interconnect — that take full advantage of the new cloud ecosystem. Private, virtual private and public clouds, as well as hybrid cloud models, all offer unique benefits. The right cloud interconnect solution can help deliver benefits a large organization needs most — whether that includes control, security, flexibility, agility or lower costs.

Nokia offers organizations a choice of DCI solutions for cloud interconnect. These solutions provide the flexibility, scalability and security to support current DCI needs — along with the capacity, performance and agility needed to support cloud interconnect across different cloud types. Our DCI solutions include packet optical transport, IP/MPLS routing and SDN solutions for both the data center and the WAN. They support wavelength, Ethernet and IP to let organizations choose the best solution to meet their business needs. By offering unified IP/optical management and the potential of simplified, automated and on-demand networking with WAN SDN, Nokia can deliver dynamic, cost-effective cloud interconnect solutions for the cloud era.

Nokia DCI solutions are used by many enterprises in the financial, healthcare, consumer and industrial sectors for business-critical applications. These solutions are also widely deployed in the government, oil and gas, transportation and utility sectors for mission-critical applications, as well as by many leading service providers and network operators.
Enterprise use of cloud services

A survey by Penn Schoen Berland examined 1500 large enterprises in the US and 750 in the UK and produced some revealing findings. First, among the organizations using cloud-based services, approximately 3 out of 5 are already using some form of cloud computing. In addition, 74 percent of large enterprises in the US have adopted private clouds. Thirty-five percent have adopted public cloud services, and 22 percent have adopted a hybrid cloud model. The figures are very similar for large enterprises in the UK.¹

Several types of cloud are often referred to when discussing enterprise cloud IT:

- **Private cloud:** The enterprise data centers and DCI network are completely dedicated to and operated by or on behalf of the enterprise.

- **Virtual private cloud:** The enterprise data centers are virtualized, which allows them to include remote data centers owned by a communications service provider (CSP) or carrier-neutral provider (CNP).

- **Public cloud:** An internet cloud content provider (ICP) offers cloud services for enterprises to use on a pay-as-you-go basis.

- **Hybrid cloud:** This cloud model combines private and public clouds, with orchestration of resources across the private-public boundary.

Figure 1 shows how an enterprise might implement these types of clouds. The white paper “Cloud Interconnect for the Enterprise” explains the different types of cloud in more detail, outlines how to achieve the right cloud balance and explores how to adopt cloud interconnect.

1 “A window into large enterprise IT – A Penn Schoen Berland survey of senior decision makers,” a report for Nokia, October 2015.
Key points to consider when deciding on a cloud strategy

Each enterprise needs to determine the right balance of private, virtual private and public clouds to meet its needs, including:

- **Virtualization and resource sharing:** Enterprises need to balance the benefits of flexibility and lower cost offered by virtualization in a public or hybrid cloud brings with the possible security implications of sharing common infrastructure.

- **Control and security:** Client confidentiality, data security and compliance are a major concern for many enterprises and may limit the use of public and hybrid clouds to non-business-critical applications and services.

- **Cost factors:** For many enterprises, the reduced capital outlay and lower operating costs of public and hybrid clouds outweigh the possible security and control issues, particularly for non-critical applications and services.

The volume of data exchanged between data centers must be considered when implementing a DCI strategy for the cloud — particularly between an enterprise’s primary and backup data centers located in the same metropolitan area. Today, most enterprise DCI applications require bandwidth of between 1 Gb/s and 10 Gb/s. However, other factors will place an increasing strain on enterprise DCI networks, requiring bandwidth up to 100 Gb/s and beyond.

Factors driving higher capacity DCI bandwidth

- **Convergence within the data center:** The growth of 10 Gigabit Ethernet (GE), 25 GE and 40 GE network adapters — and the eventual migration of data center network fabrics to 40 GE and 100 GE in the core — will increase traffic within and between data centers.

- **Adoption of cloud IT:** Virtualization of data center servers and storage means that a single request by a user or application can trigger multiple data exchanges between servers in one data center, as well as servers in different data centers.

- **Rapid advances in storage technology:** Flash memory, solid-state drive (SSD) storage, Gen 6 Fiber Channel supporting 32 Gb/s and 128 Gb/s, and software-defined storage will make cloud-based storage more compelling.

- **Continuous data availability and mobility:** Distributing virtual compute and storage resources across physical devices and locations may require more DCI bandwidth to ensure business-critical applications remain up and running at all times.

- **Dynamic allocation of resources:** Dynamic allocation of server, storage and network resources across cloud boundaries will be essential for resource sharing, application workload balancing and greater operational efficiency.
Cloud interconnect — DCI for the cloud

Cloud interconnect provides multiple options for data center interconnect for the cloud and offers several advantages over traditional DCI solutions, including:

- **Scalable, flexible bandwidth:** Mobility, personal devices, new applications and explosive data growth have created demand for easily scalable bandwidth. Cloud interconnect supports optical wavelength, Ethernet and IP capabilities for different cloud applications. It delivers very high bandwidth — and allows optical, Ethernet and IP bandwidth to be increased and decreased flexibly as needed.

- **Multi-site, multi-technology, multi-cloud capabilities:** Cloud interconnect more easily shares data, distributes applications and balances workloads across different cloud types, between multiple locations and between different cloud providers. It provides multi-site, multi-technology capabilities with the high performance, reliability and quality of service required to connect multiple data centers in the cloud.

- **Agile, dynamic provisioning:** Cloud interconnect supports orchestration of network resources across cloud boundaries to ramp up or turn down resources when and where required. It supports provisioning of bandwidth and orchestrates network resources dynamically, quickly and easily — between different locations, across multiple data centers and across different types of cloud and cloud provider.

Cloud interconnect delivers the capacity, flexibility and security enterprises need for fast turn-up of cloud IT. At the same time, cloud interconnect helps ensure business continuity, improve asset utilization and reduce costs.

**The benefits of a cloud interconnect strategy**

Implementing a cloud interconnect strategy has several key benefits, including:

- **Security:** Dedicated cloud interconnect offers more secure transport connections than the public internet. When cloud interconnect is combined with existing private WAN backbone and managed services (such as IP VPNs), multiple enterprise large sites, branch offices and remote locations can use cloud resources.

- **Cost:** Private cloud interconnect can reduce costs because traffic does not have to be routed over an ISP's connection to the internet. Instead, traffic is transported directly to the cloud provider. Cloud interconnect based on managed wavelengths or carrier Ethernet generally offers much higher bandwidth and costs less to transport large amounts of data, compared to the public internet.

- **Performance:** Bandwidth, latency, response time, quality of service and reliability are more consistent with dedicated cloud interconnect. Depending on the point of interconnection, the link may support latency-sensitive applications and workloads that cannot run over the public internet.

- **Flexibility:** Access to a variety of cloud services, including virtual private, hybrid and public, can be implemented over the same dedicated cloud interconnect link. As a result, different workloads can be allocated to resources that have the appropriate price/performance profile.
Nokia solutions for cloud interconnect

Nokia offers a choice of cloud interconnect solutions that provide the flexibility, scalability and security to support current DCI needs — along with the capacity, performance and agility needed to support cloud interconnect across different cloud types. Nokia cloud interconnect solutions provide a multi-layer architecture that includes packet optical transport, IP/MPLS routing and SDN solutions for both the data center and the WAN, as shown in Figure 2.

Figure 2. Nokia integrated IP/optical and SDN solutions for agile, efficient and cost-optimized cloud interconnect

At the optical transport layer, the Nokia 1830 Photonic Service Switch (PSS) provides the foundation for cloud interconnect with flexible, scalable, secure and low latency optical transport for cloud interconnect, and between geographically diverse data centers.

At the IP layer, the Nokia 7750 Service Router (SR) provides IP and Ethernet VPN capabilities, with a data center gateway function that allows integration between SDN-enabled data centers, the wide area network (WAN) and remote business locations.

At the SDN overlay layer, the Nokia Nuage Networks Virtualized Services Platform (VSP) virtualizes and automates network connectivity and services within and across data centers, and across virtualized, bare metal and container-based applications, independent of the physical network underlay components.
Organizations can use the Nokia 1830 PSS to construct a private cloud using leased or owned dark fiber to offer very high scalability and capacity for cloud interconnect. 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. Private build requires considerable financial investment and qualified personnel with the appropriate technical expertise but provides a more flexible, agile, easily scalable cloud interconnect solution. It also enables connections to virtual private and hybrid clouds to provide business continuity and disaster recovery (BCDR), expand capacity when needed, or host non business-critical applications.

The Nokia 1830 PSS also enables organizations to use managed Carrier Ethernet and wavelength services offered by network operators and service providers for cloud interconnect. These managed services provide dedicated high-speed bandwidth, but can be expensive and inflexible, and take time to provision. However, they are ideal for providing high-speed connectivity between the private cloud and virtual private and hybrid clouds. Some examples of this include: asynchronous DCI between geographically dispersed data centers in the private cloud; connecting to a tertiary backup data center in a co-location facility; and hosting non business-critical applications.

The Nokia 7750 SR supports IP/MPLS-based Ethernet and IP VPNs to provide the secure multi-site connectivity and quality of service many organizations need. They can use the 7750 SR to implement IP/MPLS VPNs that enable remote sites and users access to data center applications over the private cloud. Using the data center gateway function of the 7750 SR extends the benefits of server virtualization across multiple data centers in the cloud and distributes cloud applications to remote sites and users.

Alternatively, organizations can use managed VPN services provided by a network operator or service provider. However, managed VPN services may not offer cost-effective bandwidth in all required locations or the responsiveness required by some cloud applications. In such cases, a software-defined WAN solution, such as the Nokia Virtualized Network Services (VNS) platform, provides an agile, flexible and more dynamic approach to connect remote sites and users. The Nokia VNS also integrates easily with the Nokia VSP to virtualize and automate network connectivity and services within and across data centers.

By combining the 7750 SR with the 1830 PSS, organizations can build an integrated IP/optical solution for cloud interconnect that improves efficiency, reduces costs and increases agility. With unified IP/optical management and the potential of simplified, automated and on-demand cloud interconnect provided by the Nokia Network Services Platform, organizations can implement dynamic, cost-effective cloud interconnect solutions.
Implementing private cloud interconnect using secure optical transport

Private clouds are suitable for business-critical applications and sensitive information because they offer the highest level of security and control and the lowest level of risk. Typically, a private cloud connects a primary data center to a secondary data center in the same area and, in some cases, a third data center in another area that provides additional resiliency in case of major incidents. Private clouds — also known as on-premises clouds — support virtualization, with applications and data distributed across the organization’s own data centers.

The 1830 PSS provides optical wavelength division multiplexing (WDM) with transport-grade reliability to meet most private cloud interconnect requirements. It supports speeds of 10, 40 and 100 Gb/s and beyond, while meeting stringent performance, latency and reliability requirements. The 1830 PSS also supports 400G coherent optical transport on a single-carrier wavelength using the second generation of the Nokia Photonic Service Engine (PSE-2). The 1830 PSS supports both short reach coarse wavelength division multiplexing (CWDM) and medium/long reach dense wavelength division multiplexing (DWDM) optical interfaces depending on distance requirements.

In addition, the 1830 PSS supports multiprotocol data center aggregation for Ethernet (LAN), Fibre Channel (SAN) and InfiniBand® (HPC), and has the following DCI certifications:

• Approved WDM product for IBM GDPS transport
• Brocade and EMC certification, including VPLEX for continuous storage availability
• Certified with HP 3PAR Remote Data solution and tested for up to 5ms round-trip-delay/500km between sites
• FIPS 140-2 Security Level 2 and Common Criteria/Evaluation Assurance Level 2+

The 1830 PSS is used extensively by enterprise, industry and public sector customers — as well as by many service providers worldwide. As well as the foundation for private cloud interconnect, the 1830 PSS provides traditional DCI solutions for secure, near-real-time business continuity and disaster recovery (BCDR) of business-critical data and applications across multiple data center locations. With metro, regional and long haul options, the 1830 PSS provides secure asynchronous data replication and recovery over national and continental distances with synchronous data replication and recovery at rates and over distances not normally achievable between geographically diverse datacenters.
The 1830 PSS supports efficient wavelength switching between source and destination using tunable-reconfigurable optical add-drop multiplexing (T-ROADM). For larger enterprise, industry and public sector customers with more complex requirements, the 1830 PSS supports full Layer 2 Carrier Ethernet services over the optical network, and a Generalized Multiprotocol Label Switching (GMPLS) control plane to enable automated setup, provisioning and restoration of the optical layer, decreasing costs and increasing uptime. The 1830 PSS also supports latency optimization on its optical line cards to ensure synchronous DCI applications can be optimized depending on the distance between sites. On-demand latency measurement with hardware timestamping can be used to check end-to-end round trip delay at network commissioning or after activating features such as line protection.

Figure 3 shows how an enterprise can implement private cloud interconnect using the 1830 PSS, either through a private build or via a managed solution from a service provider.

Figure 3. Secure private cloud using encrypted optical DWDM with the 1830 PSS

Benefits of secure private cloud interconnect using the Nokia 1830 PSS
• On-the-fly, AES 256 bit layer 1 hardware encryption
• Low latency adds <20 nanoseconds
• Separate centralized key management tool
• Optical intrusion detection
• Latency optimization

Optical cloud interconnect security features

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

The Nokia 1830 PSS supports an integrated layer 1 hardware encryption option with in-flight encryption per client/line interface to provide scalable, efficient, end-to-end security between data centers across the cloud. Optical intrusion detection tools monitor links for unexpected loss of signal strength from unauthorized optical fiber taping and snooping, and can find and pinpoint fiber cuts, providing secure cloud interconnect for the most stringent business-critical applications. The platform uses FIPS 140-2 certified AES-256 layer 1 hardware encryption that provides the most efficient approach for bulk data encryption, adding less than 20 nanoseconds of latency. A latency optimization tool ensures the lowest latency per optical connection for synchronous near-real-time cloud applications.
A separate, secure and scalable key management tool manages the encryption keys centrally and independently of the 1830 PSS management system. A central key management approach reduces complexity and establishes a single point of trust compared to the distributed approach used by most key management systems. Security management is also completely separate from the optical management, allowing two different organizations to jointly manage the overall solution without compromising data confidentiality and security. For example, a bank cyber security team can manage key management and encryption with a service provider managing the optical network.

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, highly flexible optical interface redundancy options, and the optical intrusion detection feature. The white paper “1830 PSS - Secure Optical Transport” has more information about the security capabilities of the 1830 PSS.

Expanding cloud interconnect to the virtual private cloud

Enterprises can expand their private clouds to include virtual private clouds that add data center resources owned or hosted by a third party, such as a communication service provider (CSP) or a carrier-neutral provider (CNP). The private cloud connects securely to a CSP or CNP data center by extending the enterprise’s own cloud interconnect solution, or using a managed cloud interconnect solution from a CSP, as shown in Figure 4. Assets or resources used in the virtual private cloud become part of the private cloud but are remotely located and hosted in the CSP or CNP data center.

Figure 4. Using cloud interconnect to expand private cloud to virtual private cloud

Connection between the private cloud and virtual private cloud can be implemented using Layer 2 Carrier Ethernet transport over optical WDM. Organizations already using the 1830 PSS for private cloud interconnect can simply add Carrier Ethernet transport capabilities with QoS, OAM and protection to provide the connection to the virtual private cloud.
Alternatively, the connection between the private cloud and virtual private cloud can be implemented using IP/MPLS-based Carrier Ethernet services using the 7750 SR. Both the 1830 PSS and the 7750 SR use Nokia Service Router Operating System (SR-OS) software. SR-OS is fully compliant with and certified to Metro Ethernet Forum (MEF) Carrier Ethernet 2.0 (CE 2.0) and fully interoperable with 3rd party CE 2.0-certified devices.

Both the 1830 PSS and 7750 SR use the Nokia 5620 Service Aware Manager (SAM) system for end-to-end IP and optical provisioning, troubleshooting and maintenance. This enables operational cost savings when using Nokia optical and IP/MPLS solutions in the same private cloud. As these solutions are also used extensively by network operators and service providers worldwide, enterprises can often supplement their private cloud interconnect with managed cloud interconnect services from their service provider, ensuring end-to-end interoperability.

Using Ethernet and IP VPNs for cloud interconnect

IP/MPLS-based Ethernet and IP VPNs can be used for private cloud interconnect and for connecting to virtual private and hybrid clouds where less stringent latency, lower bandwidth and regional, national or international connectivity are required. They can also be used for remote site access to applications hosted in the data center, or integration with the private WAN.

The 7750 SR provides high-performance, multiservice routing and delivers exceptional performance, scale and reliability. The product supports a wide range of interfaces, including 10Gb/s, 100Gb/s and 400Gb/s Ethernet as well as ATM and SONET/SDH interfaces for connection to legacy private WAN environments. It is designed to deliver multiple advanced IP/MPLS-based services concurrently in very large networks, such as Layer 2 Virtual Private LAN Service (VPLS), MEF CE 2.0-certified services and Layer 3 IP VPNs, IPv6 VPNs and multicast VPNs. Service intelligence enables granular control of services and drives operational efficiency. The product uses the Nokia SR OS and is managed by the 5620 SAM for end-to-end provisioning, troubleshooting and maintenance.

The Nokia 7750 SR supports highly scalable IP/MPLS services with unmatched performance, security and reliability for cloud interconnect applications. Redundant hardware, non-stop routing and non-stop forwarding ensure end-to-end services are not interrupted by link and equipment failures or software upgrades. Link, nodal and path protection capabilities ensure highly available services and protect against service interruptions.

Security capabilities across different layers include:

- line-rate filtering
- service mirroring
- administration
- routing and control authentication

Benefits of Ethernet and IP VPNs for cloud interconnect using the 7750 SR

- High performance, scalable, multi-site connectivity
- Supports wide range of Ethernet and IP VPNs
- Comprehensive high availability and reliability features
- Cloud-level application assurance
- Integrates easily with existing enterprise WAN infrastructure
• logging, reporting and auditing
• network traffic control network topology analysis
• Layer 2 and Layer 3 resource control on per-customer, per-service, per-port, per-module and per-platform bases
• Layers 2 to 7 monitoring and application control

**Integrated IP/optical with common management and service assurance**

Combined with the Nokia 7750 SR, the Nokia 1830 PSS provides a cost-effective, highly efficient integrated IP/optical solution to meet different cloud interconnect needs, with multiple reliability and high availability features to support business and mission-critical applications. Fully redundant platforms — with disaster recovery technologies at the optical transport and IP routing layers — provide node-, network- and application-level protection.

The 5620 SAM leverages multi-domain, multi-layer management to provide common management across both the IP and optical domains to unify workflows and achieve maximum efficiency. Proactive assurance and advanced monitoring capabilities across elements, infrastructure layers, and services in the integrated IP/optical network, rapidly detect and isolate problems before they can impact services and end users. Integrated views across multi-domain and multi-technology layers spanning physical, routing, MPLS and IP/optical service topologies simplify and accelerate troubleshooting.

End-to-end power control, monitoring, tracing and fault localization for individual wavelength channels — enabled through the Nokia Wavelength Tracker technology — proactively prevent service degradation by enabling delivery of true optical SLAs. Integrated IP/optical performance and SLA monitoring using comprehensive service-aware diagnostics validate end-to-end data services and IP/optical paths. Fast and easy configuration and multi-vendor scripting workflows reduce the risk of errors and speed network deployment time.

**Application assurance and cloud interconnect**

Two common challenges for cloud interconnect are how to address performance for applications hosted in the data center and how to track application usage and bandwidth to/from the data center. Nokia IP/MPLS solutions meet these challenges using Application Assurance, which provides extensive application monitoring and reporting.

Application policies can be enforced across multiple touch points, including the data center, and at any point in the network. This distributed, network-based application assurance capability can also provide SLA measurement for business-critical applications hosted in the data center — right down to the remote sites and users accessing the application. SLA guarantees can be provided for users while enabling performance monitoring of applications as they transit the network.
Extending data center virtualization over the cloud

To address the speed and efficiency constraints of the data center network, SDN-based solutions are used increasingly to virtualize the data center network and automate network service delivery. Using SDN technology, enterprises can now build a robust and scalable data center networking infrastructure. This infrastructure can deliver secure virtual slices of readily consumable compute, storage and networking resources instantaneously across thousands of applications and user groups. The deployment of private, virtual private and hybrid clouds means this connectivity needs to be extended seamlessly across the WAN between data centers and to end users.

Figure 5 shows the role of the Nokia 7750 SR as a data center gateway. This example uses IP/MPLS to enable seamless connectivity between SDN-enabled data centers and remote sites in the private cloud. These remote sites can be connected via IP/MPLS or SD-WAN, an emerging way of connecting remote sites that virtualizes network resources.

Figure 5. Extend SDN over the private cloud for seamless data center virtualization

Nokia has implemented data center virtualization technologies, such as network virtualization overlay (NVO) and virtual extensible LAN (VXLAN) in the 7750 SR.

VXLAN is the de-facto overlay data plane standard for data center networking. It encapsulates Ethernet in IP, can be routed by IP and terminated on computer infrastructure or SDN-enabled network equipment, such as the Nokia VSP. The underlay network may be any IP network that uses existing routing, resiliency and load balancing mechanisms. Overlays can be viewed as a tunnel between two end points within the data center. They provide a number of benefits, including VPNs for multi-tenancy, network virtualization for location independence of resources within the data center, improved resource allocation and protection from topology or technology changes.
Nokia has combined NVO and VXLAN with emerging technologies, such as Ethernet VPN (EVPN), in the SR-OS software to enable a data center gateway function on the 7750 SR. Based on well-established routing protocols and operational experience used in IP/MPLS networks, EVPN provides an overlay control plane. When combined with VXLAN as the overlay data plane, EVPN enables data center virtualization to be extended across the cloud. The application note Seamless Data Center Interconnect explains the data center gateway capabilities of the 7750 SR in more detail.

Using the data center gateway function, customers can simultaneously and securely connect multiple virtualized, cloud-based data centers and remote sites across the private cloud. As the data center gateway function uses industry standard protocols, customers can also connect to data center resources in third-party data centers hosted in virtual private and hybrid clouds. Cloud bursting and hybrid cloud services are made possible in a highly dynamic and robust way as an extension of the enterprise private cloud.

Extending cloud interconnect to hybrid clouds and public cloud services

Public and hybrid clouds offer enterprises the highest flexibility by enabling access to resources and services when, where and for as long as required. They also reduce cost significantly by reducing CAPEX in favor of OPEX, but they may not provide the level of control, security and compliance some enterprises need for some applications.

As shown in Figure 6, an enterprise can use private cloud interconnect or a managed cloud interconnect service to connect to public cloud services hosted in a CSP or CNP co-location data center to create a hybrid cloud. Alternatively, an enterprise can use a secure public internet connection or dedicated cloud interconnect provided by a network provider, service provider or cloud provider to access the public cloud.

Figure 6. Extending cloud interconnect to hybrid clouds and public cloud services
Summary

Enterprise, industry and public sector customers need to consider new approaches to meet current DCI and future cloud interconnect needs because of the impact of cloud computing, virtualization of data center architecture and SDN.

Nokia cloud interconnect solutions provide a choice of technologies to help de-risk the provisioning of cloud interconnect to support private, virtual private and hybrid cloud models. Nokia solutions include high performance, low latency, secure optical WDM solutions for synchronous applications, as well as IP/MPLS solutions that provide high performance, multi-site connections with advanced QoS and traffic engineering between multiple data centers and multiple cloud types.

Nokia data center network virtualization and SDN solutions deliver unrestricted data center networking within the data center and across the cloud to greatly simplify operations, reduce costs and increase agility.

Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>BCDR</td>
<td>business continuity and disaster recovery</td>
</tr>
<tr>
<td>CE</td>
<td>Carrier Ethernet</td>
</tr>
<tr>
<td>CNP</td>
<td>carrier-neutral provider</td>
</tr>
<tr>
<td>CSP</td>
<td>communications service provider</td>
</tr>
<tr>
<td>CWDM</td>
<td>coarse wavelength division multiplexing</td>
</tr>
<tr>
<td>DCI</td>
<td>data center interconnect</td>
</tr>
<tr>
<td>DWDM</td>
<td>dense wavelength division multiplexing</td>
</tr>
<tr>
<td>EVPN</td>
<td>Ethernet VPN</td>
</tr>
<tr>
<td>GMPLS</td>
<td>Generalized Multiprotocol Label Switching</td>
</tr>
<tr>
<td>ICP</td>
<td>internet cloud provider/internet content provider</td>
</tr>
<tr>
<td>MPLS</td>
<td>Multiprotocol Label Switching</td>
</tr>
<tr>
<td>NVO</td>
<td>network virtualization overlay</td>
</tr>
<tr>
<td>QoS</td>
<td>Quality of Service</td>
</tr>
<tr>
<td>SaaS</td>
<td>software as a service</td>
</tr>
<tr>
<td>SDN</td>
<td>software-defined network</td>
</tr>
<tr>
<td>SD-WAN</td>
<td>software-defined WAN</td>
</tr>
<tr>
<td>T-ROADM</td>
<td>tunable-reconfigurable optical add-drop multiplexing</td>
</tr>
<tr>
<td>VPLS</td>
<td>Virtual Private LAN Service</td>
</tr>
<tr>
<td>VPN</td>
<td>virtual private network</td>
</tr>
<tr>
<td>VXLAN</td>
<td>virtual extensible LAN</td>
</tr>
<tr>
<td>WDM</td>
<td>wavelength division multiplexing</td>
</tr>
<tr>
<td>GMPLS</td>
<td>Generalized Multiprotocol Label Switching</td>
</tr>
<tr>
<td>ICP</td>
<td>internet cloud provider/internet content provider</td>
</tr>
<tr>
<td>MPLS</td>
<td>Multiprotocol Label Switching</td>
</tr>
<tr>
<td>NVO</td>
<td>network virtualization overlay</td>
</tr>
<tr>
<td>QoS</td>
<td>Quality of Service</td>
</tr>
<tr>
<td>SaaS</td>
<td>software as a service</td>
</tr>
<tr>
<td>SDN</td>
<td>software-defined network</td>
</tr>
<tr>
<td>SD-WAN</td>
<td>software-defined WAN</td>
</tr>
<tr>
<td>T-ROADM</td>
<td>tunable-reconfigurable optical add-drop multiplexing</td>
</tr>
<tr>
<td>VPLS</td>
<td>Virtual Private LAN Service</td>
</tr>
<tr>
<td>VPN</td>
<td>virtual private network</td>
</tr>
<tr>
<td>VXLAN</td>
<td>virtual extensible LAN</td>
</tr>
<tr>
<td>WDM</td>
<td>wavelength division multiplexing</td>
</tr>
</tbody>
</table>

Nokia is a registered trademark of Nokia Corporation. Other product and company names mentioned herein may be trademarks or trade names of their respective owners.

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

Product code: PR1601017887EN (March)