Nokia 1830 PSS business-critical cloud DCI solutions
Scalable, reliable, secure data center interconnect for large enterprises, government, and the energy, transportation and utility sectors
Your DCI challenges
Whether you’re a large enterprise, government or are in the energy, transportation or utility sector, your business-critical data volumes are pushing into terabyte territory. You may also be increasingly reliant on cloud-based apps. In this environment, the cost benefits of using traditional data center interconnect (DCI) services to link and transport traffic between data centers for critical applications is eroding.

You still require a high-speed, low-latency and secure private optical network to connect multiple sites. Your DCI still needs to ensure synchronous replication of data for business continuity and disaster recovery. However, as you consolidate data centers and move to the cloud, you need business-critical cloud DCI solutions to take full advantage of the benefits of the cloud. You want the scalability, control, reliability and security of a private optical network with the agility, flexibility and lower costs of the cloud.

New cloud DCI models
Large enterprises, government and the public sector, and the energy, transportation and utility sectors are using private optical networks to build private clouds for business-critical applications. They also want to move to more flexible cloud IT models that outsource some IT needs and less-critical applications to third parties.

Multiple data centers owned and operated by different entities can be part of the cloud IT model:
- Enterprise and system integrator (SI) data centers
- Communications service provider (CSP) multi-tenant data centers
- Carrier-neutral provider (CNP) co-location data centers
- Internet content/cloud provider (ICP) data centers

In the cloud IT model, workloads run on virtualized servers and storage in data centers in the cloud (see Figure 1). These data centers can either be on-premises data centers owned or dedicated to the organization (private cloud) or off-premises data centers run by a third party such as a CSP or CNP (virtual private cloud).

Some organizations may also choose to run less-critical applications using public cloud services provided by ICPs. This approach enables organizations to run more critical workloads in-house using a private and/or virtual private cloud and run less critical workloads using more flexible pay-as-you-go public cloud services.

Organizations can create a hybrid cloud by combining private cloud and/or virtual private cloud with public cloud, allocating resources and balancing workloads as appropriate across the different cloud types to match cost models to business needs.

Figure 1. Cloud DCI

Resources
- Business-critical Cloud DCI animation
- Cloud DCI ecosystem white paper
- Cloud DCI for enterprise white paper
- Cloud DCI solutions web page
Cloud drives the need for scalable, reliable, secure DCI

When planning for cloud DCI, it is important to determine how much bandwidth you need, particularly for future cloud IT needs.

DCI bandwidth is likely to grow significantly because of data center consolidation, which drives convergence of data center architecture. Upgrading data center servers and switch fabrics increases traffic within the data center but it also increases traffic between data centers.

Distributed cloud applications are also driving traffic between data centers, which is growing faster than either traffic to end users or traffic within the data center. Enterprise applications running in third-party cloud data centers also drive the need for secure DCI.

The Global Cloud Index predicts that by 2020, DCI traffic will account for almost 9 percent of total data center traffic. A recent Nokia Bell Lab study indicates a 430 percent increase in DCI traffic in metropolitan area networks between 2015 and 2020 due to the cloud.

Cloud DCI—managed service or private-build?

CSPs often provide managed DCI services to enterprise, industry, government and public sector organizations as part of their managed network services portfolios. Managed DCI services are a suitable solution for small to medium enterprises (SMEs) and for large organizations that prefer to outsource their networking and DCI needs.

For organizations that need very high bandwidth, physical security and complete control of their data centers, their network and the data that flows over it, self-build private cloud DCI using dark fiber can provide a more cost-effective, scalable and secure solution.

The costs of private cloud DCI can be significantly less than a managed DCI solution, especially when consolidating data centers (see Figure 2). The reason is that the cost of dark fiber linking fewer consolidated data centers in a private cloud is often less than the cost of managed DCI between multiple data centers.

Resources

- Cloud DCI for enterprise brochure
- Cloud DCI – build or buy? white paper
- Cloud DCI case study customer case study
- Cloud DCI professional services brochure

Nokia business-critical cloud DCI solutions

Business-critical DCI demands high-capacity, high-performance network interfaces with high security and very low latency. Cloud IT and the dynamic nature of cloud services also create new demands and requirements. The Nokia 1830 Photonic Service Switch (PSS) provides key capabilities to meet these requirements, including:

- Scalable, reliable bandwidth combined with flexible reach to meet the scalability, capacity and distance requirements for business-critical DCI applications. The 1830 PSS supports ultra-high capacity, short-reach metro connections to very-high capacity, ultra-long reach subsea connections on the same network interface cards.

- Secure optical transport to protect data in-flight between data centers from theft and intrusion. Nokia uses independently certified and government-approved AES 256-bit encryption with symmetric keys generated by the 1830 Security Management Server (SMS) to ensure key integrity. This encryption is complemented by intrusion detection and isolation mechanisms.

- High-capacity optical line-side interfaces with support for wavelength and Ethernet services. Multiple client interfaces, such as Ethernet, Fibre Channel, InfiniBand and SONET/SDH, accommodate legacy requirements.

- Close integration with Nokia’s IP/MPLS portfolio to provide multi-technology, multi-site, multi-cloud capabilities to share data, distribute applications and balance workloads across different data centers, between multiple locations and between different cloud service providers.

- Agile, dynamic provisioning of network connections and services, to ramp up bandwidth when and where required. The Nokia Network Services Platform (NSP) provisions bandwidth and orchestrates network resources dynamically, quickly and easily—between different locations, across multiple data centers, and across different clouds and cloud types.

The Nokia 1830 PSS is used by many large enterprises in the financial, healthcare, consumer and industrial sectors as well as by government and public sector agencies to support business-critical DCI applications and private cloud environments. These solutions are also widely deployed in the energy, transportation and utility sectors for mission-critical DCI applications and by many service providers worldwide to provide managed DCI services.

Resources

- Cloud DCI solutions for large enterprise application note
- Cloud DCI solution for government application note

“The Nokia DCI solution was selected because it met all our objectives. It met our immediate needs by providing a common infrastructure that consolidated multiple IT infrastructures, simplified processes and lowered costs. It also provided a core backbone that can support a single private cloud infrastructure. This gave us the agility, flexibility and control to expand DCI capacity and leverage cloud IT to meet future needs.”

Technical lead for the integration project of a major French retail bank
Private-build secure DCI using dark fiber

An organization can build its own secure DCI solution to support a private cloud using the Nokia 1830 PSS and point-to-point fiber. Typically, data centers are in the same metro area up to 70 km (43.5 miles) apart but can be connected over regional and long haul distances depending on capacity and latency requirements. Private-build DCI using dark fiber is best for large organizations that need very high bandwidth, physical security and complete control over their data centers and DCI.

Managed DCI service provided by a CSP

An organization can build a private/virtual private cloud by outsourcing its DCI to a CSP that provides a fully managed DCI service using Carrier Ethernet or wavelength services. Organizations typically use managed DCI services over regional or long haul distances.

Direct connect to a cloud service provider

An organization can implement a hybrid cloud to augment its private cloud by using direct connect services to connect to public cloud services offered by an ICP. An organization can also use hosted IT services in off-premises, multi-tenant data centers offered by a CSP or colocation facilities offered by a CNP. These are typically located in the same metro area as the organization.
Nokia business-critical cloud DCI using the 1830 PSS

Nokia business-critical cloud DCI is based on the 1830 PSS portfolio (see Figure 3), and typically supports the following DCI applications:

- Synchronous business continuity and disaster recovery (BCDR)
- Continuous data availability and real-time data replication
- High-frequency/high-volume applications such as financial trading
- Secure mirroring or replication of mission-critical data
- Long-distance data backup and asynchronous replication
- Private/hybrid cloud connectivity.

The 1830 PSS is optimized for optical networking applications, from interconnecting data centers to efficiently scaling large metro, regional and long haul multi-layer, multiservice optical networks.

Each platform in the 1830 PSS portfolio leverages common software, hardware, management and control to offer seamless operations across the portfolio.

The 1830 PSS platforms can be used to implement multiple DCI services, including:

- Data center and cloud access
- High-performance, point-to-point DCI over dark fiber
- Multiservice metro DCI transport and aggregation
- Regional and long haul DCI.

The platforms support a range of client interfaces including 10/100G Ethernet, 4/8/10/16G Fibre Channel and 5G DDR InfiniBand. The platforms also support OTU1, OTU2 and OTU4 client interfaces and as well as legacy SONET/SDH services. The platforms also support next-generation dense wavelength division multiplexing (DWDM) multiservice transport and enable agile, scalable and highly secure 10/100G DCI networks and cloud services.

The 1830 PSS platforms provide 10G/100G Layer 1 security using independently certified AES 256-bit symmetric encryption. The 1830 SMS delivers highly secure, centralized key generation and management. An optional optical time-domain reflectometer (OTDR) unit provides real-time fiber intrusion detection and latency optimization.

Figure 3. Nokia DCI using the 1830 PSS

The platforms support a range of client interfaces including 10/100G Ethernet, 4/8/10/16G Fibre Channel and 5G DDR InfiniBand. The platforms also support OTU1, OTU2 and OTU4 client interfaces and as well as legacy SONET/SDH services. The platforms also support next-generation dense wavelength division multiplexing (DWDM) multiservice transport and enable agile, scalable and highly secure 10/100G DCI networks and cloud services.

The 1830 PSS platforms provide 10G/100G Layer 1 security using independently certified AES 256-bit symmetric encryption. The 1830 SMS delivers highly secure, centralized key generation and management. An optional optical time-domain reflectometer (OTDR) unit provides real-time fiber intrusion detection and latency optimization.

Resources
- Nokia 1830 PSS web page
- Cloud DCI for large enterprise web page
- DCI for the cloud ecosystem article
- Nokia secure optical transport video
- Nokia secure optical transport brochure
Nokia Layer 1 optical encryption for secure business-critical DCI

With the rapid growth of DCI and the move to cloud IT, the need to secure data in-flight over the network has become much more important. Encryption has become a critical requirement for banks, government agencies, transportation, utilities and other organizations that need secure DCI.

Nokia Layer 1 optical encryption has several advantages over encryption at higher layers:

- **Bandwidth efficiency** – Provides bulk encryption at data rates of 10G and 100G for economies of scale and does not waste bandwidth compared to MACsec or IPSec
- **Low latency** – Almost no additional latency is incurred, unlike higher-layer encryption technologies
- **Transparency** – Provides protocol-independent encryption to enable multiple types of client traffic to be secured: Ethernet, Fibre Channel, InfiniBand, Optical Transport Network (OTN) and SONET/SDH
- **Management** – Simplifies operation because there is only one encrypted circuit to manage per optical link instead of multiple tunnels.

Nokia “quantum proof” Layer 1 encryption with AES 256 symmetric keys

Nokia Layer 1 encryption protects against attack by the latest quantum computers, ensuring the highest level of security through AES 256-bit encryption using symmetric keys (see Figure 4). It provides the strongest independently certified encryption available to protect against the possibility of attack using the most powerful computers, including quantum computers.

Figure 4. AES 256 symmetric keys

Asymmetric RSA-2048

<table>
<thead>
<tr>
<th>Effective security strength</th>
<th>Security under quantum attack</th>
</tr>
</thead>
<tbody>
<tr>
<td>112 bit key strength</td>
<td></td>
</tr>
</tbody>
</table>

Symmetric AES-256

<table>
<thead>
<tr>
<th>256 bit key strength</th>
</tr>
</thead>
</table>

Exceeds NSA recommendations for classified data

Resources

Nokia secure optical transport for the 1830 PSS white paper

Quantum-proof over 1,000,000 years to successful quantum computer attack*

* Using quality key refreshed every hour
Nokia optical intrusion prevention and detection

Data hacking of optical fiber is relatively easy using simple tools to tap into the fiber and capture leaking light without interfering with passing traffic. Such an attack can be performed by anyone with physical access to fiber and is very hard to discover. This has increased the need for security over optical fiber networks for applications such as DCI.

Nokia provides optical fiber intrusion detection by measuring fiber optic power levels at multiple measurement points for all wavelengths traveling through an 1830 PSS optical network. When the power level between two measurement points is abnormally attenuated, an alarm warns operators of potential intrusion. Without this type of detection, optical intrusion might go unnoticed by operators and/or users because the network and the services continue to function without any quality issues.

The 1830 PSS also supports an OTDR capability that characterizes the optical fiber by injecting a series of optical pulses. OTDR then extracts, from the same end of the fiber, light that is scattered or reflected back from points along the fiber. This process forms a “fingerprint” of the fiber, which can be checked to identify fiber cuts, taps or tampering. OTDR can also precisely identify locations based on the time delay of the reflections. The process is similar to how radar works.

When combined with optical intrusion detection and monitoring software, OTDR provides intelligent physical layer security for optical DCI networks.

Figure 5 illustrates optical intrusion detection and OTDR.

**Resources**

Nokia 1830 PSS OTDR unit data sheet
# Nokia 1830 PSS product portfolio for business-critical DCI

<table>
<thead>
<tr>
<th>Features</th>
<th>1830 PSS-4</th>
<th>1830 PSS-8</th>
<th>1830 PSS-16</th>
<th>1830 PSS-32</th>
</tr>
</thead>
<tbody>
<tr>
<td>DCI application</td>
<td>DCI access or DCI for small to medium data centers</td>
<td>High-capacity, high-density metro DCI</td>
<td>High-capacity, high-density DCI for metro/regional/long haul</td>
<td>Very high-capacity, high-density DCI for regional/long haul</td>
</tr>
<tr>
<td>Typical DCI service support</td>
<td>10G Wavelength services</td>
<td>10G/100G Wavelength services</td>
<td>10G/100G Wavelength services</td>
<td>100G/200G Wavelength services</td>
</tr>
<tr>
<td></td>
<td>10G CE 2.0 services</td>
<td>10G/100G CE 2.0 services</td>
<td>10G/100G CE 2.0 services</td>
<td>100G CE 2.0 services</td>
</tr>
<tr>
<td>Capacity and performance</td>
<td>240 Gb/s</td>
<td>800 Gb/s</td>
<td>1.6 Tb/s</td>
<td>8 Tb/s</td>
</tr>
<tr>
<td>Interface card slots (full/half)</td>
<td>2/4</td>
<td>4/8</td>
<td>8/16</td>
<td>16/32</td>
</tr>
<tr>
<td>Controller card slots</td>
<td>1 unprotected</td>
<td>2 protected</td>
<td>2 protected</td>
<td>2 protected</td>
</tr>
<tr>
<td>Power modules</td>
<td>Redundant power modules</td>
<td>Redundant power modules</td>
<td>Redundant power modules</td>
<td>Redundant power modules</td>
</tr>
<tr>
<td>Power options</td>
<td>-48V DC or +24V AC</td>
<td>48V DC, 110/220V AC with integrated AC power filter</td>
<td>48V DC, 110/220V AC with external converter</td>
<td>48V DC, 115/240V AC with external converter</td>
</tr>
<tr>
<td>Power requirements</td>
<td>Max. 347 W; typical 220 W</td>
<td>Max. 1200 W; typical 520 W</td>
<td>Max. 2400 W; typical 1350 W)</td>
<td>Typical 440 W – 1270 W</td>
</tr>
<tr>
<td><strong>Nokia 1830 PSS Quad 10G Encryption Transponder card (11QPEN4)</strong></td>
<td><strong>Nokia 1830 Secure Management Server (SMS)</strong></td>
<td><strong>Nokia 1830 PSS 100G/200G Uplink card (1UD200)</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----------------------------------------------------------------</td>
<td>-----------------------------------------------</td>
<td>--------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A single-slot card that supports four independent multi-rate 10G channels, including 8G/10G Fibre Channel (FC), 10 Gigabit Ethernet (10GE), Optical Transport Unit 2 (OTU2) and 5G DDR InfiniBand. It provides low latency (&lt;10 μs), wire-speed Layer 1 encryption using AES 256. The solution is independently certified to FIPS 140-2 Level 2, CC EAL2+ and is approved by DISA IOC/JITC.</td>
<td>A highly scalable, secure and unified key management server. It provides a centralized, single point of trust for the management of AES 256-bit symmetric encryption keys used by the Nokia 1830 PSS encryption cards for secure business-critical DCI applications. The solution is independently certified to FIPS 140-2 Level 3, CC EAL4+, ANSSI QR and has achieved European restricted and NATO restricted certifications.</td>
<td>A single-slot 100G/200G coherent DWDM uplink card for any client card connected to the 1830 PSS-8/16/32 distributed packet/OTN fabric. This compact card provides a 100G PDM-QPSK network interface with SD-FEC and hard decision FEC (HD-FEC) or a 200G PDM-16QAM network interface with SD-FEC.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Nokia 1830 PSS Universal 100G Encryption card (S13X100)</strong></th>
<th><strong>Nokia 1830 PSS 20x10G Multi-rate card (20P200)</strong></th>
<th><strong>Nokia 1830 PSS 500G DWDM Muxponder (D5X500)</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>A single-slot card that supports transponder, muxponder, uplink and ADM applications. The module supports 8G/10G/16G FC, 10/40/100 GE and OTU2/OC-192/STM-64 client ports and a 100G WDM coherent (PDM-QPSK) network port. It provides wire-speed low latency (&lt;10 μs), Layer 1 encryption using AES 256 and is independently certified to FIPS 140-2 Level 2 and CC EAL2+.</td>
<td>A single-slot card that supports a variety of applications, including multi-rate muxponder client ports when connected to 100G to 500G uplink cards or add-drop multiplexor client ports when connected to a pair of 100G to 500G uplink cards. This flexibility is provided by the 1830 PSS-8/16, which supports the flexible interconnect of cards to address many DCI deployment applications.</td>
<td>A dual-slot card for the 1830 PSS-8/16/32 that enables high-density 100G network connections by transporting up to five 100G services in a compact form factor. A single card can support flexible deployments ranging from metro to ultra-long haul. The card is programmable to offer efficiency, agility and flexibility, optimizing deployments by reducing network interface requirements.</td>
</tr>
</tbody>
</table>

For more information about how Nokia business-critical cloud DCI solutions can provide scalable, reliable and secure DCI for your organization, please visit our [Cloud Data Center Interconnect web page](#).
Benefits

- Scales network capacity, reach and density with sub-10G, 10G, 40G and 100G services
- Enables efficient DWDM transport with flexible, rate-adaptive 100G to 500G coherent line-side interfaces
- Supports wavelength routing that is colorless, directionless and contentionless with Flexgrid (CDC-F) and reconfigurable optical add/drop multiplexer (ROADM) capability
- Supports Ultra-Wideband C+L band CDC-F wavelength routing to maximize fiber capacity and wavelength agility
- Provides fixed OADM and highly integrated single-slot integrated ROADM (iROADM) capability
- Supports 200G wavelength distances of 2,000 km (1,242.7 miles), providing an evolution from 100G to 200G DWDM long haul
- Supports 100G wavelength distances of 3,000 km to 7,500 km (1,864 miles to 4,660 miles), thereby supporting ultra-long haul without costly regeneration
- Optimizes transport wavelength spectral efficiency for both capacity and distance, maximizing achievable fiber bandwidth without compromising wavelength availability
- Provides efficient bandwidth management capabilities at the 100G and sub-100G levels
- Supports MEF Carrier Ethernet 2.0 E-Line, E-LAN and E-Tree services and Multiprotocol Label Switching - Transport Profile (MPLS-TP) services
- Enables IP/optical integration via the Generalized Multiprotocol Label Switching (GMPLS) user-network interface (UNI)
- Supports ITU-T G.8262 SyncE for frequency synchronization distribution and IEEE 1588v2 packet-based time/phase synchronization distribution
- Enables 50-ms protection with advanced wavelength frequency and high-speed phase recovery capabilities, plus ultra-fast wavelength multi-layer protection and restoration.
- Supports 500G single-carrier wavelength
- Integrated packet transport with MEF CE 2.0-certified packet interface cards
- Fully managed end-to-end packet solution with common service OAM across optical and Ethernet/IP/MPLS services
- Management via the Nokia 1350 Optical Management System (OMS)
- Support for transport software-defined networking (T-SDN) and centralized, multi-layer control via the Nokia NSP
- Integrated network planning tools for optimized multi-layer network planning/deployment, commissioning and optical power balancing.

Technologies

- Nokia Photonic Service Engine version 2 (PSE-2) Super Coherent Technology electro-optics supports multiple modulation formats for maximum wavelength scalability over various distances and qualities of fiber
- Flexible-rate DWDM coherent interfaces with aggregate payload capacity ranging from 100G to 500G
- Next-generation, latency-adjustable, soft decision forward error correction (SD-FEC) over extreme distances and challenging fiber environments
- Spectrally efficient 400G single-carrier wavelength
- Integrated Nokia wavelength tracking technology supports unique and powerful wavelength operations, administration and maintenance (OAM)
- Integrated Nokia wavelength tracking technology supports unique and powerful wavelength operations, administration and maintenance (OAM)
- Integrated Nokia wavelength tracking technology supports unique and powerful wavelength operations, administration and maintenance (OAM)
- Enables IP/optical integration via the Generalized Multiprotocol Label Switching (GMPLS) user-network interface (UNI)
- Supports ITU-T G.8262 SyncE for frequency synchronization distribution and IEEE 1588v2 packet-based time/phase synchronization distribution
- Enables 50-ms protection with advanced wavelength frequency and high-speed phase recovery capabilities, plus ultra-fast wavelength multi-layer protection and restoration.
- Supports 500G single-carrier wavelength
- Integrated packet transport with MEF CE 2.0-certified packet interface cards
- Fully managed end-to-end packet solution with common service OAM across optical and Ethernet/IP/MPLS services
- Management via the Nokia 1350 Optical Management System (OMS)
- Support for transport software-defined networking (T-SDN) and centralized, multi-layer control via the Nokia NSP
- Integrated network planning tools for optimized multi-layer network planning/deployment, commissioning and optical power balancing.

Resources – data sheets

- Nokia 1830 PSS portfolio
- Nokia 1830 PSS 10G Encryption Card
- Nokia 1830 PSS 100G Encryption Card
- Nokia 1830 PSS 20x10G Multi-rate Card
- Nokia 1830 PSS 100G/200G Uplink Card
- Nokia 1830 PSS 200G Transponder
- Nokia 1830 PSS 500G Muxponder Card
- Nokia 1830 Secure Management Server
About Nokia

Nokia is a global leader in the technologies that connect people and things. Powered by the innovation of Bell Labs and Nokia Technologies, the company is at the forefront of creating and licensing the technologies that are increasingly at the heart of our connected lives.

With state-of-the-art software, hardware and services for any type of network, Nokia is uniquely positioned to help communication service providers, governments, and large enterprises deliver on the promise of 5G, the Cloud and the Internet of Things. http://nokia.com

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.
Product code: SR1704009607EN (May)
© 2017 Nokia