Many enterprises use data center interconnect (DCI) solutions to connect data centers and create a private cloud of virtual machines and storage. But as enterprises increasingly adopt the cloud and move to cloud IT models, their DCI solutions need to enable them to take full advantage of the new cloud ecosystem.

Private, virtual private, public and hybrid clouds all have unique benefits to offer. And the right DCI solution for the cloud can help deliver the benefits an enterprise needs most — whether those include control, security, flexibility, agility or lower costs. This white paper provides a high-level overview of the new cloud ecosystem from an enterprise perspective and looks at the key requirements for cloud DCI, also known as cloud interconnect.
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>Enterprise use of cloud services</td>
<td>4</td>
</tr>
<tr>
<td>The different types of cloud</td>
<td>4</td>
</tr>
<tr>
<td>Private clouds</td>
<td>5</td>
</tr>
<tr>
<td>Virtual private clouds</td>
<td>6</td>
</tr>
<tr>
<td>Public clouds</td>
<td>7</td>
</tr>
<tr>
<td>Hybrid clouds</td>
<td>8</td>
</tr>
<tr>
<td>How enterprises can achieve the right cloud balance</td>
<td>9</td>
</tr>
<tr>
<td>Adopting a DCI strategy for the cloud</td>
<td>9</td>
</tr>
<tr>
<td>Cloud interconnect – DCI for the cloud</td>
<td>11</td>
</tr>
<tr>
<td>The benefits of cloud interconnect</td>
<td>11</td>
</tr>
<tr>
<td>Nokia cloud interconnect solutions for enterprise and public sector</td>
<td>12</td>
</tr>
<tr>
<td>Acronyms</td>
<td>13</td>
</tr>
</tbody>
</table>
Introduction

Enterprise DCI solutions have traditionally focused on near-real-time business continuity and disaster recovery (BCDR). Their goals have been to securely back up and replicate business-critical data and applications for multiple data center locations. For many large enterprises, a private optical DCI solution is still a valid option for BCDR, particularly when network performance, data security, sovereignty and integrity, and regulatory compliance are crucial business priorities.

But significant changes are underway. DCI solutions are expanding into a new role — connecting enterprise data centers in a private cloud of virtualized compute and storage. These solutions use software-defined networking (SDN) to automatically allocate resources and balance workloads across multiple sites.

In addition, enterprises are increasingly looking to outsource their IT to cloud providers as a way to match cost models to their business needs. Currently, it’s difficult for enterprises to scale their IT quickly and cost effectively to match the growing demand for compute and storage. As a result, they want to move from a self-build CAPEX-based IT model to a more agile outsourced OPEX-based cloud IT model.

As large enterprises move to cloud IT, they need cloud DCI solutions — often called cloud interconnect — that can take full advantage of the new cloud ecosystem. Private, virtual private and public clouds, as well as hybrid cloud models, all have unique benefits to offer. Figure 1 shows the different types of clouds and the participants in the cloud ecosystem. The white paper Cloud ecosystem and the role of cloud interconnect explains the different participants and their roles in the cloud ecosystem in more detail.

Figure 1. Emerging cloud ecosystem and the different participants

The right cloud DCI solution can help deliver the cloud IT benefits a large enterprise needs most — whether those include control, security, flexibility, agility or lower costs.
But there’s no one-size-fits-all model. Cloud DCI solutions vary according to an enterprise’s capitalization, size, IT assets — and the amount of data it wants to store in the cloud. Large enterprises need flexible cloud DCI solutions that enable different approaches according to individual business models. Also, emerging technologies such as software-defined WAN (SD-WAN) mean that large enterprises must consider new approaches to meet future DCI needs for the cloud era.

**Enterprise use of cloud services**

A survey by Penn Schoen Berland examined 1,500 large enterprises in the US and 750 in the UK and produced some revealing findings. First, among the organizations using cloud-based services, approximately three out of five are already using some form of cloud computing. In addition, as Figure 2 shows, 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

**Figure 2. Adoption of private, public and hybrid cloud services by large enterprises**

![Diagram showing adoption rates](image)

**The different types of cloud**

Several types of cloud are often referred to when discussing enterprise cloud IT, as shown in Figure 1. However, their market definitions can be confusing. So it’s helpful to keep in mind that the cloud is a delivery model, not a product. Here are some generally understood definitions:

- **Private cloud**: The enterprise data centers and DCI network are completely owned and operated by 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 cloud boundary.

¹ "A window into large enterprise IT – A Penn Schoen Berland survey of senior decision makers," a report for Nokia, October 2015
The following sections explain how an enterprise might implement these types of clouds.

**Private clouds**

When an enterprise owns and operates its own data centers and DCI solutions, they have a private cloud. This type of cloud is often chosen for running business-critical applications and handling business-critical information, because it offers the highest level of security and control and the lowest level of risk. Typically, a DCI network connects a primary data center to a secondary data center in the same area, as shown in Figure 3. In some cases, a third data center in another area provides additional resiliency in case of major incidents.

Private clouds — also known as on-premises clouds — can support virtualization, with applications and data distributed across the organization’s own data centers. Virtualization lets enterprises quickly assign and share IT assets. For example, the business can easily redistribute workloads or reassign capacity for short-term projects. Some customers describe this approach as providing “the advantages of cloud functionality within the safety of their organization.”

Enterprises use private clouds in the following ways:

- Finance and healthcare companies often choose private clouds, because they help maintain client confidentiality, data security, sovereignty and compliance, as well as business continuity and disaster recovery.
- Localized data centers can be combined with high-speed, low-latency optical DCI solutions that support time-sensitive applications, such as high-frequency financial trading.
- Large manufacturers and retailers often use data centers in far-flung regions to track suppliers, take customer orders and support logistics. IP/optical DCI networks then support critical applications and data backup and recovery across multiple sites.

While private clouds have many benefits, they can be costly. Capital investments are needed regularly to increase capacity or make architecture changes. Qualified staff must be paid to operate the data centers and DCI network, maintain IT resources and keep data secure. And all project and technology risk falls on the enterprise.

Enterprises want to retain the performance, control and security provided by a private cloud for their business-critical and proprietary applications that may also have availability, reliability or regulatory requirements. But they often want to add more cost-effective and flexible options for less-sensitive applications and data. New cloud DCI models are now emerging to meet the demand for enterprise compute and storage more economically.

---

2 "A window into large enterprise IT – A Penn Schoen Berland survey of senior decision makers," a report for Nokia, October 2015
Virtual private clouds

Virtual private clouds allow an enterprise to expand its private cloud cost effectively. In this case, the cloud adds data center resources owned by a third party, such as a CSP or a CNP. Figure 3 shows how that works. The private cloud connects securely to a CSP or CNP data center by extending the enterprise’s own DCI solution. The connection can also be made using a managed DCI solution, for example from a CSP.

From an enterprise perspective, any assets or resources used in the virtual private cloud become part of their private cloud. But the additional assets or resources are remotely located in the CSP or CNP data center. The enterprise can install and manage its own compute, storage and network assets and just pay for space and power, or they can lease the resources they need from the provider.

Virtual private clouds can be used in the following ways:

- An enterprise could use a virtual private cloud for less-critical applications, as a way to augment its own private cloud.
- It could also use its private cloud to back up business-critical data, while simultaneously using a virtual private cloud to improve workload distribution.

Virtual private clouds, also known as hosted clouds, provide greater flexibility for less-critical business operations. They also allow CAPEX and OPEX to be matched to enterprise IT needs, without sacrificing performance, control and security. The perceived loss of these factors is among the top reasons cited by enterprises for not moving to cloud IT. Virtual private clouds, like virtual private networks, keep different enterprises’ services and data separate from each other. They are also able to meet the performance, control, security and performance requirements of most enterprises.

---

3 “A window into large enterprise IT – A Penn Schoen Berland survey of senior decision makers,” a report for Nokia, October 2015
Public clouds

Public clouds give the enterprise another way to augment its private cloud. In this case, it uses resources or services provided by an internet content or cloud provider (ICP). As shown in Figure 3, the enterprise can use a managed DCI solution or the internet to access the public cloud. Then public cloud resources and services are used on a pay-as-you-go basis. In other words, the enterprise only pays for the resources and services it consumes, based on the time they are used for. These public cloud resources and services remain separate from the enterprise’s private cloud.

The ICP may host resources and services in their own data centers, but increasingly they are hosting them in CSP or CNP data centers. For example, many cloud providers such as Amazon Web Services, Microsoft Azure, Google Compute Engine and IBM SoftLayer — as well as SaaS companies such as salesforce.com — are locating their services in CSP and CNP facilities. They are doing so mainly because these facilities bring ICP resources and services closer to enterprise customers, improve the end-user experience, and provide a convenient and lower-cost way of interconnecting with service providers collocated in the same facility.

Large enterprises, systems integrators and industry organizations in some vertical markets are also recognizing the benefits of collocating assets or using resources in CNP facilities. The advantages include:

• Better access to ICPs
• More connectivity
• Better peering points with CSPs
• Greatly improved application performance for an increasingly mobile work force.

These benefits can also extend to enterprise partners providing critical services such as logistics, marketing and customer support.

Public clouds are used in the following ways:

• Enterprises can use public cloud capacity and services for non-critical and customer-facing applications, a method that augments private clouds used for key business applications.
• For example, a retailer may outsource its web presence, online ordering and inventory control applications to a public cloud provider to improve customer experience and the supply chain.
• Simultaneously, it uses public cloud capacity when needed for non-critical applications or services, while continuing to run the company’s ERP and CRM applications in its private cloud to maintain security and control.

Public cloud models potentially give enterprises greater freedom to choose between multiple cloud providers based on economic considerations, application performance and business requirements. But when public cloud services are used outside the private enterprise environment, there are some important management considerations, including:

• Control of public cloud compute and storage resources
• Control of non-standard or “shadow IT” applications and services
• Ensurance of data security, compliance and sovereignty
• Implications for the budget, including the impact on OPEX
• Possible consequences from the lack of consistent and enforceable SLAs from many public cloud providers.
Despite some clear limitations, controlled use of public clouds has a role to play in most large enterprises. Because this type of cloud can provide greater flexibility and agility, while reducing costs, it is particularly useful for non-business-critical applications and data — as well as for occasions when capacity must be ramped up quickly to meet demand.

Hybrid clouds

A hybrid cloud model combines private, virtual private and public clouds and orchestrates resources across the private-public cloud boundary. This approach enables data to move between clouds and allows resources to expand and contract seamlessly to meet changing workloads. The ultimate goal of the hybrid cloud is fluid, effortless workload portability across public and private cloud platforms.

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 costs significantly by reducing CAPEX in favor of OPEX. However, this cloud model may not provide the level of control, security and compliance that some enterprises need for some applications.

Enterprises can use hybrid clouds in the following ways:

- An enterprise might use a hybrid cloud for non-critical workloads and to improve IT responsiveness to users, for example, with self-service access to specific applications and services.
- Hybrid clouds allow more efficient use of critical internal resources by providing dynamic capacity expansion for highly variable workloads.
- They also allow occasional access to services or applications that are too expensive to implement or host in-house.

Hybrid cloud models also give enterprises greater freedom because they combine the benefits of private cloud with public cloud services. However, enterprises face both business and technical challenges when implementing a hybrid cloud, such as those indicated in Table 1.

Table 1. The business and technical challenges of hybrid clouds

<table>
<thead>
<tr>
<th>Business challenges of hybrid clouds</th>
<th>Technical challenges of hybrid clouds:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obtaining the skills and knowledge needed to address the complexity of hybrid clouds</td>
<td>Dynamically connecting to and disconnecting from different cloud services</td>
</tr>
<tr>
<td>Maintaining data security, privacy and sovereignty when shared across hybrid clouds</td>
<td>Maintaining data transport speeds, QoS and reliability across hybrid clouds</td>
</tr>
<tr>
<td>Keeping the hybrid cloud IT environment from becoming a bottleneck to business</td>
<td>Delivering high-quality application and service performance across hybrid cloud boundaries</td>
</tr>
<tr>
<td>The cost of adapting applications to fit hybrid cloud models</td>
<td>Orchestration of network resources across hybrid cloud boundaries</td>
</tr>
<tr>
<td>Making the business case for hybrid clouds compared with using public cloud services</td>
<td>Preventing service interruptions in hybrid cloud environments</td>
</tr>
</tbody>
</table>

Clearly, hybrid clouds have much to offer an enterprise. But for most organizations, they will be a work in progress as their challenges are addressed over time.
How enterprises can achieve the right cloud balance

Every enterprise needs to determine the right balance of private, virtual private and public clouds to meet its needs. Here are some points to consider when deciding on a cloud strategy that supports a company’s business priorities:

• **Virtualization and resource sharing**: Virtualization brings the benefits of flexibility and lower cost. While most enterprises are willing to use virtualization and resource sharing in a private cloud, some see this as a possible security weakness when used in a virtual private or public cloud. It’s true that individual enterprises share a common network infrastructure, as with a virtual private network. But each enterprise’s data travels over a dedicated virtual path across the physical network, and the data is not visible to any other enterprise.

• **Control and security**: When client confidentiality and data security, compliance and sovereignty are major concerns, many enterprises may limit their use of public and hybrid clouds to non-business-critical applications and services. Other enterprises attracted to the flexibility and cost savings of public and hybrid clouds should carefully consider the security and compliance implications.

• **Cost factors**: Large enterprises have the capital and human resources to implement private and virtual private clouds. But for many enterprises, the reduced capital outlay and lower operating costs of public and hybrid clouds are very important considerations. For most enterprises, they will outweigh security and control issues, particularly for non-critical applications and services.

Adopting a DCI strategy for the cloud

Implementing a DCI strategy to deliver the benefits of the cloud can be a sometimes daunting and complex task, even for a well-resourced large enterprise. One primary reason is that, with the rapid growth in cloud IT, the volume of data exchanged between cloud data centers is increasing rapidly — particularly between an enterprise’s primary and backup data centers located in the same metropolitan area.

In a recent update to its study of metro network traffic growth, Nokia Bell Labs predicts that traffic between enterprise data centers in metro networks will increase by 430 percent from 2015 to 2020, due almost entirely to the adoption of cloud IT. However, this traffic is associated with more than data backup and recovery between data centers. It also includes users and applications accessing data in cloud data centers.

To address this rapid growth in data traffic, many large enterprises are using optical wavelength division multiplexing (WDM) solutions. These provide scalable bandwidth and offer the best cost-performance ratio and lowest latency required for near-real-time DCI applications such as BCDR. Some large enterprises acquire, lease or build dark fiber connections between their data center sites with optimal paths, and deploy and manage their own WDM equipment in a private network. Others use managed DCI solutions such as managed wavelength or Carrier Ethernet services from a CSP.

---

In most cases, today’s large enterprise DCI applications require bandwidth of between 1 Gb/s and 10 Gb/s. However, the following factors can place an increasing strain on enterprise DCI networks, requiring bandwidth up to 100 Gb/s and beyond:

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

- **Adoption of cloud IT:** As the virtualization of data center servers and storage increases, 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:** Storage performance is increased and latency is reduced by advances such as flash memory, solid-state drive (SSD) storage, Gen 6 Fiber Channel supporting 32 Gb/s and 128 Gb/s, and software-defined storage — making cloud-based storage more compelling.

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

- **Dynamic allocation of resources:** As IT is virtualized within and across clouds, dynamic allocation of server, storage and network resources across cloud boundaries becomes essential for resource sharing, application workload balancing and greater operational efficiency.

Cloud IT requires scalable and flexible bandwidth to support data traffic increases between data centers in the cloud. Enterprises must choose the best option to meet their needs:

- **The internet scales massively and provides any-to-any connectivity.** But it does not provide the cost-effective bandwidth, security, performance and QoS that enterprises need to run their business-critical applications in the cloud.

- **Managed IP VPN services** provide the multi-site connectivity, security and QoS enterprises need, but they may not offer cost-effective bandwidth and performance in all required locations.

- **Carrier Ethernet and managed wavelength services** provide dedicated, secure and very high bandwidth, but they can be expensive unless justified for use on connections with very high traffic volumes.

Virtualization of cloud IT promises dynamic allocation of server and storage capacity across multiple data centers to improve resource utilization, improve efficiency and reduce costs. Orchestrating server, storage and network resources in private and virtual private clouds is possible today because the environment is bounded and self-contained. But achieving those same goals in hybrid clouds — across private-public cloud boundaries — is much harder.

Most managed services (regardless of the technology used) are currently unable to dynamically orchestrate network resources and maintain SLAs across private-public cloud boundaries. This will change as cloud services become more widely deployed and more important to enterprise IT operations. New dynamic approaches to WAN networking such as carrier SDN and SD-WAN will automate and orchestrate network resources to deliver dynamic provisioning, flexible bandwidth, enforceable SLAs and usage-based charging for cloud DCI services.
Cloud interconnect – DCI for the cloud

Traditionally, DCI networks have focused on bandwidth and latency as part of ensuring business continuity and disaster recovery. But the move to the cloud demands new objectives and requirements. Cloud interconnect provides some key capabilities to meet the dynamic nature of the cloud:

• **Scalable, flexible bandwidth:** Mobility, personal devices, new applications and explosive data growth demand more scalable and flexible bandwidth. Cloud interconnect solutions must be able to deliver very high bandwidth — and increase and decrease bandwidth flexibly as needed.

• **Multi-site, multi-technology, multi-cloud:** Cloud interconnect solutions need to share data, distribute applications and balance workloads across different cloud types, between multiple locations and between different cloud providers. They must provide multi-layer, integrated IP and optical capabilities with high performance, reliability and QoS, as well as multiple client interfaces such as Ethernet, Fibre Channel and InfiniBand, to accommodate legacy and future requirements.

• **Agile, dynamic provisioning:** Cloud interconnect solutions must support orchestration of network resources across cloud boundaries to ramp up resources when and where required (and then ramp them down again). That means they must provision bandwidth and orchestrate network resources dynamically, quickly and easily — between different locations, across multiple data centers and across different clouds and cloud providers.

The benefits of cloud interconnect

Enterprises are moving toward building a complete digital infrastructure – one that includes using a policy-based approach to orchestrating the use of compute, storage and applications. Cloud interconnect solutions have a role to play in helping enterprises dynamically match and execute workloads at the best location, based on cost, performance, security and other key business requirements.

Secure, high-speed cloud interconnect links between the enterprise and multiple cloud providers are critical to a successful cloud strategy. Enterprises are accustomed to using private connections to CSP and CNP hosting environments, but currently, these are not widely available or cost effective for connecting to public clouds. Instead, many ICPs offer public internet connections to their public clouds, limiting the attractiveness of their services to many large enterprises because of security and performance concerns. With cloud interconnect, enterprises can securely connect data centers in their private cloud to data center resources in CSP and CNP facilities. And with more ICPs also collocating their services in CNP facilities, cloud interconnect effectively facilitates a more secure, private environment that brings public cloud services closer to the enterprise, increasing performance and providing better quality of experience for users.

Cloud interconnect is particularly attractive to large enterprises, especially industry segments that need to share large data sets or exchange quantities of information. These segments include energy companies engaged in oil and gas exploration, media companies involved in movie production, financial services trading systems and various communities of vendors, suppliers and partners. As more large enterprises start to use CSP and CNP data center facilities, they can more easily share large data sets.

Large enterprises can gain the following benefits, when using dedicated cloud interconnect to link their private cloud to virtual private and hybrid cloud services provided by CSPs, CNPs and ICPs:

• **Security:** A dedicated cloud interconnect link offers a more secure transport connection than the public internet. When these links are combined with existing private WAN backbone and managed services, such as IP VPNs, multiple large sites, branch offices and remote locations can use cloud resources.
• **Cost**: A private cloud interconnect link can reduce costs, because traffic does not have to be routed over an ISP’s connection to the internet. Instead, it’s transported directly to the cloud provider. Cloud interconnect links based on managed wavelengths or carrier Ethernet generally offer much higher bandwidth and cost less to transport very large amounts of data, compared with public internet links.

• **Performance**: Bandwidth, latency, response time, QoS 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 could not be run over the public internet.

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

**Nokia cloud interconnect solutions for enterprise and public sector**

Nokia offers a choice of cloud interconnect solutions to meet the varying needs of enterprise and public sector customers, as shown in Figure 4. These cloud DCI solutions provide a scalable, high-performance and secure cloud interconnect architecture with the capacity, flexibility and agility needed to support different cloud types.

**Figure 4. Nokia cloud DCI solutions**
Nokia cloud DCI solutions include packet optical transport and IP/MPLS routing solutions covering metro, regional, national and international connectivity requirements, along with SDN solutions for both the data center and the WAN. The Nokia solutions support a choice of wavelength, Ethernet and IP options to provide the best cloud interconnect solutions to meet different business needs. By offering IP/optical management and automated and on-demand IP/optical networking with SDN solutions, Nokia can deliver agile, dynamic, flexible and cost-effective cloud DCI solutions for enterprise and public sector customers.

Nokia DCI solutions are used by many large enterprises in the financial, healthcare, consumer and industrial sectors for business-critical DCI applications such as business continuity and disaster recovery. They are widely deployed in the government, oil and gas, transportation and utility sectors for mission-critical DCI applications.

To find out more, please visit https://networks.nokia.com/portfolio/solutions/cloud-data-center-interconnect or see the relevant Nokia cloud interconnect solution white paper.

Acronyms

- BCDR: business continuity and disaster recovery
- CAPEX: capital expenditures
- CE: Carrier Ethernet
- CNP: carrier-neutral provider
- CRM: customer relationship management
- CSP: communications service provider
- DCI: data center interconnect
- ERP: enterprise resource planning
- GE: Gigabit Ethernet
- ICP: internet cloud provider/internet content provider
- MPLS: Multiprotocol Label Switching
- OPEX: operating expenditures
- QoS: Quality of Service
- SaaS: software as a service
- SDN: software-defined network
- SD-WAN: software-defined WAN
- SLA: service level agreement
- SSD: solid-state drive
- VPN: virtual private network
- WDM: wavelength division multiplexing
About Nokia

We create the technology to connect the world. Powered by the research and innovation of Nokia Bell Labs, we serve communications service providers, governments, large enterprises and consumers, with the industry's most complete, end-to-end portfolio of products, services and licensing.

From the enabling infrastructure for 5G and the Internet of Things, to emerging applications in digital health, we are shaping the future of technology to transform the human experience. networks.nokia.com

Nokia operates a policy of ongoing development and has made all reasonable efforts to ensure that the content of this document is adequate and free of material errors and omissions. Nokia assumes no responsibility for any inaccuracies in this document and reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

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.

© 2019 Nokia

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

Document code: SR1905035109EN (May) CID191151