Cloud data center interconnect for ICPs and CNPs

Web-scale and metro-scale data center interconnect

White paper

Although data center architectures vary depending on market segment, data centers operated by internet content providers (ICPs), communications service providers (CSPs) and carrier-neutral collocation providers (CNPs) host thousands of servers. Data center interconnect (DCI) solutions used to link and transport traffic between these web-scale data centers require terabits of optical transport capacity over metro, regional and long-haul distances.

With the continued growth of data centers across all market segments, DCI is the fastest growing optical transport application. However, cloud IT—or cloud computing—is driving an evolution from a centralized web-scale data center approach to a more distributed metro-scale data center approach. Deploying metro-scale data centers at the network edge offers significant business benefits and spawns new opportunities.

These changes mean that new cloud DCI solutions are needed that interconnect multiple hyper-scale data centers across metro, regional and long-haul distances, and automate and optimize network connections and bandwidth to make DCI networks as flexible and agile as cloud IT.
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>Opportunities and challenges driven by the evolution of cloud IT</td>
<td>4</td>
</tr>
<tr>
<td>Opportunities for ICPs</td>
<td>9</td>
</tr>
<tr>
<td>Opportunities for CNPs</td>
<td>11</td>
</tr>
<tr>
<td>The need for cloud DCI</td>
<td>13</td>
</tr>
<tr>
<td>Nokia cloud DCI solutions</td>
<td>14</td>
</tr>
<tr>
<td>Acronyms</td>
<td>16</td>
</tr>
</tbody>
</table>
Introduction

The move of IT to the cloud and the wide and rapid adoption of cloud services have created an ecosystem with different types of cloud, as shown in Figure 1.

With a public cloud, an internet cloud provider (ICP) offers cloud services to organizations to use on a pay-as-you-go basis, creating hyper-scale data centers and interconnecting them using terabit metro and long-haul private DCI networks. In a private cloud, a single organization—such as an enterprise, an industry body or a government agency—creates a private cloud, with on-premises data centers and a DCI network that interconnects them completely dedicated to and controlled by the organization.

An organization can also create a virtual private cloud by virtualizing its data centers, which allows it to include IT resources in off-premises data centers owned by other organizations in its private cloud. These off-premises data centers can include data centers operated by a communications service provider (CSP) or a carrier-neutral provider (CNP).

In a hybrid cloud, an organization combines public cloud services with its private and virtual public clouds, orchestrating resources and workloads across the private-public cloud boundary.

Figure 1. Cloud ecosystem participants and their roles

The different participants in the cloud ecosystem shown in Figure 1 have different roles and objectives. ICPs have built private, centralized, web-scale data centers, and many have built terabit DCI to assist their web-scale data center build-outs. They have interconnecting data centers on campuses, across metro areas and over regional, national and international long-haul distances.

CNPs have built large data center colocation facilities in large cities and metro areas that attract a wide range of tenants. These tenants include large enterprises, small to medium enterprises (SMEs), industries, industry groups, government and public-sector organizations.
The colocation facilities also attract CSPs looking to colocate with other CSPs to provide main cloud interconnect and exchange points for CNP tenants. CSPs also provide managed DCI and cloud interconnect services and are using their data center assets, points of presence (POPs) and repurposed central offices to provide virtual private cloud services.

Enterprises, industries and public-sector organizations are the main consumers of cloud services and are building private, virtual private and hybrid clouds. Using private DCI to build on-premises private clouds that offer control and security, they also expand off-premises using system integrator (SI), CNP colocation or CSP multi-tenant facilities, to implement virtual private clouds that offer more capacity at lower cost. These organizations also use ICP public cloud services to create hybrid clouds for greater agility and flexibility.

Opportunities and challenges driven by the evolution of cloud IT

From centralized to distributed cloud IT

Cloud IT is undergoing rapid change as multiple participants adapt their cloud IT services and operations to enhance customer experience, reduce operational costs and improve efficiency:

- ICPs are implementing a more distributed cloud IT model. They continue to deploy web-scale data centers but are also expanding into more metro areas and increasingly caching content in metro areas to reach new customers, improve content distribution, reduce latency and improve quality of Service (QoS).

- CNPs are expanding by building larger data center facilities in major cities and also expanding to smaller cities and metro areas. Many are expanding data centers between buildings on campuses and supporting metro data center build-outs by implementing metro DCI over dark fiber to extend inter-data center connectivity, capacity and reach.

- Mobile operators have deployed small cells in metro areas to increase coverage and optimize their networks for mobile video. They are implementing network functions virtualization (NFV) and software defined networking (SDN) to virtualize their networks, move to distributed cloud-based operational and service delivery models and prepare for the deployment of 5G.

- Fixed operators have invested heavily in metro networks to increase bandwidth and coverage, and are repurposing central offices (COs) as smart COs and mini data centers to bring services closer to customers. Fixed operators are also implementing NFV and SDN to automate the network and the delivery of cloud services.
This evolution of cloud IT to a more distributed model is driving the deployment of metro-scale colocation and multi-tenant data centers that move cloud IT to the network edge and facilitate more network interconnect and exchange points, as shown in Figure 2.

Figure 2. From centralized web-scale to distributed metro-scale data centers

**Metro-scale data centers and the move to the network edge**

ICPs and CNPs have already deployed very large metro-scale data centers in major cities worldwide. CNPs have emerged as key cloud infrastructure providers, and many are now expanding rapidly to large Tier 2 cities. They are also extending their data center build-outs to smaller Tier 3/4 cities to further expand their footprint and reach.

The emerging trend of metro-scale data centers at the network edge is captured by Gartner’s “The Edge Manifesto”¹, which outlines a distributed cloud model. This model moves data centers to the network edge and brings data processing as well as content delivery and collection closer to the sources and destinations of this information, thereby offering significant benefits:

- Spawns new opportunities and business models
- Better accommodates the continued rapid growth of data and information
- Is more able to support distributed data-intensive applications and technologies
- Provides better QoS for latency-sensitive applications and services
- Offers shared infrastructure to support smart cities and other socio-economic initiatives
- Is better suited to emerging technologies such as the Internet of Things (IoT), 5G, virtual reality (VR) and artificial intelligence (AI) applications.

Metro-scale data centers bring challenges from a network perspective. The cost of networking is on an upward trend relative to the cost of IT, which is on a downward trend driven by Moore’s Law and the economies of the cloud. Cloud IT also increases the ratio of networking to compute because it not only increases the amount of east-west traffic between servers in the same data center, it also increases east-west traffic between servers in different data centers. As the use of cloud IT increases, it also drives the growth of north-south traffic between data centers and end users, requiring new solutions to interconnect and access cloud-based, metro-scale data centers.

**OTT and the internet bypass private network model**

The internet has evolved over the years to support private peering as well as public peering, interconnection between thousands of internet service providers (ISPs), IP transit provided by global ISPs, and support for many over-the-top (OTT) service providers and applications. The internet has become the ubiquitous worldwide interconnect network.

However, the current internet is experiencing new commercialization pressures, with multilateral agreements already being replaced by private bilateral agreements. Traffic trends from major internet exchanges (IXs) worldwide show that traffic on the internet is not growing as fast as it has in the last few years. Also, the public peering model of multilateral agreements is giving way to a private peering model of multiple bilateral agreements and local peering that enables shorter direct paths between multiple cloud services.

An internet bypass private network model has also emerged that bypasses the public internet to support the cloud and mobile markets, as shown in Figure 3.

**Figure 3. The internet bypass private network model**

![Diagram of internet bypass private network model]
This internet bypass, or under-the-top (UTT), model is evolving to provide much higher bandwidth, better QoS and stricter SLAs than are possible with the OTT public internet model. For example:

- **Private CDN UTT:** Video content providers have exploited the internet OTT model but many have created a UTT direct-connect ecosystem to ensure access to users, performance and QoS. In this case, the UTT model is focused on the consumer market.

- **Cloud UTT:** ICPs have implemented direct-connect or cloud-connect services that exploit the internet OTT model. However, many larger ICPs are also building UTT direct-connect ecosystems to support the enterprise cloud IT market. In this case, the UTT model is focused on the enterprise market.

- **Global UTT:** Some Tier 1 CSPs have moved to fully commercialize the global internet. In some market verticals, direct-connect solutions have emerged that bypass segments of the internet.

- **Digital city UTT:** Shared infrastructure based on the UTT model will also become essential for smart city OTT applications and initiatives such as e-government, e-health and e-learning as well as the IoT and machine information age.

More recently, ICPs have continued to expand and deploy their own long-haul capacity while decreasing their dependence on IP transit and the internet. The largest ICPs operate private terrestrial networks based on dark fiber, providing affordable scaling and capacity to link their data centers and major interconnection points. Recently, they have also started to make major investments in subsea dark fiber, either as part of a consortium with CSPs or by building their own private ultra-long-haul submarine cable networks. This enables ICPs to connect their web-scale data centers over the shortest paths to minimize latency and improve performance.

A recent report by analyst TeleGeography\(^2\) showed that for private long-haul networks:

- Demand growth in North America already outstrips that of internet backbone providers, and private networks’ share of international bandwidth rose from 23 percent to 45 percent between 2011 and 2015

- Demand growth in Europe also outpaced that of internet backbone providers, and private networks’ share of used international bandwidth rose from 21 percent to 40 percent over the past five years.

Globally, private network growth has outpaced internet capacity growth, increasing 66 percent between 2010 and 2015, compared to 37 percent for international internet capacity.

ICPs are not the only organizations bypassing the internet; many large multinational enterprises are also building their own private networks to

---

\(^2\) “Executive Summary Global Bandwidth 2016”, TeleGeography.
provide network scaling, higher bandwidth, better QoS and lower latency. Private networks reduce latency, particularly on long-haul networks.

Latency is a major concern for many ICPs and enterprises in finance and banking, on-line gaming and content provision. Reducing latency enables real-time synchronous applications such as business continuity and disaster recovery. Reducing latency also improves click-throughs for ICPs, and profitability of trading for banks and finance companies. In addition, reducing latency improves responsiveness of on-line games and reduces jitter—which is becoming more important for HD video and VR. Very low latency is also required for emerging digital city UTT infrastructure supporting OTT applications such as IOT, automation, smart grids, digital imaging and automated transportation systems.

Cloud connect: High-speed Ethernet and wavelength services

The adoption of cloud IT and cloud services is driving a need for higher speed access to ICP public cloud services and CNP colocation facilities in metro areas. Enterprise, government and industry customers are rapidly migrating to 1G and 10G Ethernet as well as wavelength metro services. Best-effort internet connectivity does not offer the predictable performance, QoS or security that these organizations demand for access to public cloud services and colocation hosting facilities. Metro Ethernet and wavelength services with predictable performance, QoS and security are emerging as the preferred access method for data center and cloud connectivity.

While there is a rapidly emerging demand for 10G Ethernet and wavelength metro services, demand for 100G metro services is also emerging quickly, driven by enterprise access, aggregation and data center interconnect as well as the move to metro-scale data centers and distributed cloud services. This in turn will drive the need for national 100G Ethernet and wavelength services to support regional and long-haul cloud data center interconnect.

The Metro Ethernet Forum (MEF) is working on a standard set of service definitions for Layer 1 wavelength services, similar in scope to the existing Layer 2 MEF CE (Carrier Ethernet) 2.0 and emerging Layer 3 IP service definitions. The goal is to provide subscribers with consistent service offerings and to more easily compare service metrics such as performance, QoS and reliability. A standard definition of a Layer 1 External Network to Network Interface and associated operator services will enable certification of wavelength services as well as simplified and faster interconnection between different CSPs.

The standardization process for wavelength services is part of the MEF’s Third Network initiative to enable the evolution and transformation of network connectivity services and the networks used to deliver them3. The MEF has also defined Lifecycle Service Orchestration (LSO) specifications to enable standardized service orchestration of end-to-end connectivity services across one or more network service domains4.

4 Lifecycle Service Orchestration, MEF, March 2016.
LSO, in combination with SDN and NFV, is designed to enable the Third Network vision. Together, the Third Network and LSO service management will automate service ordering and configuration processes, enabling faster service delivery and lower operating costs through more agile, assured and orchestrated service management of Layer 1 wavelength services.

Secure data center interconnect

Security is a major concern for web-scale data centers as well as metro-scale colocation and multi-tenant data centers. All host multiple customers and thousands of servers supporting private and public cloud services—and many also store hundreds of terabytes of sensitive, confidential data. Providers have implemented sophisticated security measures to protect their data centers from a range of threats, physical intrusion and cyberattacks. Data centers, as the primary cloud IT resource for multiple participants in the cloud ecosystem, deserve this type of dedicated security effort.

There is a growing need to protect sensitive data in-flight when traversing the network between data centers as well as at rest on servers and storage in the data center. CSPs, ICPs and CNPs must secure their cloud DCI networks to protect in-flight data and guard against network intrusions and bulk data theft.

Opportunities for ICPs

Internet content providers (ICPs) include:

- Web-scale content providers such as Amazon, Apple, Baidu, TENCENT and Yahoo
- Cloud service providers with offerings such as Amazon Web Services, Google Compute Engine and Microsoft® Azure®
- Systems integrators such as IBM SoftLayer and HPE offering enterprise cloud services.

Many of these ICPs have built and continue to build hyper-scale data centers to host content and cloud services.

Many ICPs have built terabit DCI to assist their web-scale data center build-outs and to reach new markets. They have interconnecting web-scale data centers on campuses, across metro areas, and over regional, national and international long-haul distances. To build these networks, most ICPs have either leased dark fiber from fiber providers or leased bandwidth or wavelengths from CSPs. However, some have acquired dark fiber, particularly for campus or metro deployments.

In both cases, ICPs have tended to buy, deploy and operate their own optical DWDM equipment. However, unlike CSPs, ICPs take an IT-centric cloud view rather than a network- or telecom-centric view. This is largely because ICPs are not as restricted by regulatory requirements as CSPs and do not have a large installed base of legacy network equipment.
Some ICPs who have built and operate their own optical networks have used their software expertise to provision the network as well as cloud services. Most are innovative and at the forefront of deploying SDN and NFV to automate and provision the network and manage operations.

Many ICPs are also extending footprint and reach by building metro-scale data centers in Tier 1 cities at the network edge and by colocating in CNP facilities, particularly in Tier 2 and Tier 3 cities. This approach enables ICPs to expand local capacity, reach more customers and partners, and participate in main cloud interconnect and exchange points. This approach also gives both consumers and businesses better performance and lower latency when using public and hybrid cloud services. It also addresses data security and sovereignty concerns that some organizations may have when using public and hybrid cloud services.

Figure 4. Opportunities for ICPs

Opportunities for ICPs are shown in Figure 4 and include:

- Build metro-scale data centers at the network edge to support the growth of distributed cloud services, increase performance, reduce latency and offer better QoS
- Colocate in metro-scale CNP facilities to expand local capacity, reach more customers and partners, and participate in main cloud interconnect and exchange points
- Facilitate the adoption of cloud services by leveraging private DCI networks to offer private/public cloud interconnect using cost-effective Ethernet and wavelength services
- Deepen partnerships with CSPs by providing direct connection to public cloud services for CSP customers and a route to market for CSP value-added services
- Deploy SDN and NFV technologies to automate the provisioning and optimization of cloud DCI and cloud services.
As already noted, the largest web-scale ICPs have started to deploy metro-scale data centers and have bypassed the internet by building their own private networks that span the globe, including subsea ultra-long-haul networks. These ICPs continue to make investments to provide capacity, scale bandwidth, reduce latency and enhance application performance.

Opportunities for CNPs

Carrier-neutral providers (CNPs) cover a wide range of companies that operate multi-tenant data centers and colocation facilities. They have built these facilities in most large cities and metro areas worldwide and are expanding, particularly in smaller cities and metro areas, to extend their footprint and reach. These CNP facilities attract enterprises, industries, the public sector and other organizations as tenants wanting to host cloud IT, access public cloud services and collocate with similar organizations.

CNPs focus on providing space, power, cooling, colocation, and interconnect and exchange with other tenants within their facilities. Some CNPs also offer servers and storage, although most customers prefer to install their own servers as well as storage and network equipment. In most cases, CNPs do not offer DCI bandwidth to tenants. Typically, larger tenants lease or secure fiber from a fiber provider and purchase their own DCI equipment while others use managed DCI services from CSPs.

CNPs are building new metro-scale data centers in lower cost, fiber-rich areas or close to a CSP point of presence to encourage local fiber providers and CSPs to collocate and provide interconnect and exchange facilities. Many larger CSPs, particularly those with global reach, are choosing to collocate in CNP facilities to gain local presence and improve service delivery.

Fiber providers and CSPs bring bandwidth to CNP facilities at terabit scale, enabling CNPs to connect multiple buildings on a campus or in a metro area. They also help CNPs to provide terabit DCI between facilities, and enable tenants to connect to their own networks and data centers. Metro-scale data centers offering colocation and interconnect points also attract more ICPs wanting to extend footprint, reach more customers, and improve public cloud services and cloud application performance.
The opportunities for CNPs shown in Figure 5 include:

- Build metro-scale data centers at the network edge to attract more tenants, ICPs and CSPs to support the growth of the distributed cloud IT model
- Offer local facilities to help address data security and sovereignty concerns that many organizations may have when moving business-critical and sensitive data to the cloud
- Enable ICPs to offer better performance, lower latency and more attractive SLAs and key performance indicators (KPIs) to organizations accessing public and hybrid cloud services
- Leverage fiber presence to build private UTT networks to interconnect metro-scale data centers, achieving better economies of scale
- Leverage private UTT network to offer on-demand DCI to tenants between colocation facilities in different metro markets
- Create a bandwidth exchange service for CSP tenants to enable them to offer and bid for spare network capacity
- Offer low-cost, high-performance cloud connect solutions to smaller organizations and SMEs, leveraging UTT Ethernet and wavelength services as an alternative to the internet
- Attract mobile and fixed network operators looking for flexible and cost-effective ways to expand their operations and support emerging services such as 5G, IoT and VR
- Offer very high-performance, low-latency cloud DCI services to tenants as an alternative to leased fiber, private DCI solutions or managed DCI services from CSPs.

Metro-scale CNP facilities are extremely valuable assets when they house the largest number of tenants, have the highest density of fiber providers and CSPs offering interconnect and exchange, and offer the best options for DCI.
and cloud connect. CNPs continue to make investments in metro-scale data centers and are playing an increasingly important role in the cloud ecosystem and the emerging distributed cloud IT model.

## The need for cloud DCI

The evolution of cloud IT, the need to support distributed metro-scale data centers as well as centralized web-scale data centers, and the need for higher speed cloud connect services drive the need for specialist DCI solutions for the cloud (see Figure 6).

Distributed metro-scale data centers increase the amount of east-west and north-south traffic. This drives the need for both higher-capacity, lower-cost cloud DCI solutions and high-speed, low-cost cloud connect access solutions.

### Figure 6. The need for cloud DCI

<table>
<thead>
<tr>
<th>Enterprise data centers</th>
<th>Government data centers</th>
<th>CSP data centers</th>
<th>CNP data centers</th>
<th>ICP data centers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private cloud</td>
<td>Virtual private cloud</td>
<td>Hybrid cloud</td>
<td>Public cloud</td>
<td>Public internet</td>
</tr>
</tbody>
</table>

The internet bypass model requires both web-scale and metro-scale cloud DCI. This demands cloud DCI solutions with high interface densities, each supporting highly scalable bandwidth as well as flexible reach—from ultra-high-capacity, short-reach optical interfaces for metro connections to very-high-capacity, ultra-long-reach optical interfaces for subsea connections.

Metro-scale data centers at the network edge bring data processing as well as content delivery and collection closer to end users and help to reduce application latency. Cloud DCI solutions need to support very low latency as well as latency optimization to fine-tune application performance and delivery.

The work of the MEF on Layer 1 wavelength services and LSO means that cloud DCI solutions need to implement MEF-compliant wavelength services over point-to-point optical connections with support for multiple client interfaces, such as Ethernet, Fibre Channel and optical transport networks.
Increasing awareness about the need for security requires cloud DCI solutions that implement physical layer encryption at wire speed and with low latency, using strong symmetric encryption and centralized key management that are independently certified to comply with recognized security standards.

Cloud DCI solutions that support SDN are needed to enable multi-layer automation and optimization of network connections, and the provisioning of bandwidth dynamically, quickly and easily—between different locations and across multiple data centers. The solutions also need to support orchestration of network resources across private/public cloud boundaries to ramp up or turn down network resources when and where required. In addition, solutions need to support sophisticated optical intrusion detection at wavelength granularity to detect and locate physical tampering and ensure the integrity of network links.

**Nokia cloud DCI solutions**

Traditionally, DCI networks have focused on bandwidth and latency, but the move to cloud IT demands terabits of capacity, high interface density, very high performance and very low latency. Centralized web-scale data centers, distributed metro-scale data centers at the network edge and the dynamic nature of cloud services also create new demands and requirements. Cloud DCI provides some key capabilities to meet these requirements.

**Scalable bandwidth and flexible reach**

Cloud DCI delivers scalable, secure bandwidth as well as flexible reach—from ultra-high-capacity, short-reach metro connections to very-high-capacity, ultra-long-reach subsea connections. Cloud DCI also enables increases and decreases of bandwidth and reach as needed to meet the scalability, capacity and distance requirements for cloud service delivery from both centralized web-scale and distributed metro-scale data centers.

**Multi-technology, multi-site, multi-cloud**

Cloud DCI enables cloud services that share data, distribute applications and balance workloads across different cloud types, between multiple locations and between different cloud providers. Cloud DCI supports high-capacity optical wavelength and Ethernet capabilities and integrated IP/MPLS with high performance, reliability and QoS. Cloud DCI also supports multiple client interfaces such as Ethernet, Fibre Channel and InfiniBand, to accommodate legacy requirements.

**Agile, dynamic provisioning of network connections**

Cloud DCI supports orchestration of network resources across cloud boundaries to ramp up resources when and where required (and then ramp them down again). It can provision bandwidth and orchestrate network resources dynamically using SDN, quickly and easily—between different locations, across multiple data centers, and across different clouds and cloud providers.
**Secure optical transport**

Cloud DCI ensures that data in-flight between data centers is safe from theft and intrusion by using independently certified AES-256 encryption with strong, symmetric central key management complemented by intrusion detection and isolation mechanisms. Secure optical transport assures customers that their data is safe anywhere in the cloud.

Nokia offers a choice of cloud DCI solutions to enable ICPs and CNPs to build their own private DCI networks over metro, long-haul and ultra-long-haul subsea distances, as shown in Figure 7.

**Figure 7. Nokia cloud DCI solutions**

These solutions provide a scalable, high-performance and secure cloud DCI architecture with the capacity, flexibility and agility needed to support different cloud types. Solutions include packet optical transport and IP/MPLS routing products:

- Nokia 1830 Photonic Service Switch (PSS) family
- Nokia 1830 Photonic Service Interconnect (PSI)
- Nokia 1830 Photonic Service Demarcation (PSD)
- Nokia 7750 Service Router (SR) family
Nokia cloud DCI solutions support 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 MEF-compliant CE 2.0 and wavelength services as well as IP services to provide the best and most cost-effective cloud DCI solution to meet different business needs. By offering IP and optical management, as well as automated and on-demand IP and optical networking enabled by SDN, Nokia can deliver agile, dynamic, flexible and cost-effective cloud DCI solutions.

Nokia cloud DCI solutions are used by many CSPs, ICPs and CNPs to provide web-scale and metro-scale private DCI networks. They are used widely by large enterprises in the financial, healthcare, consumer and industrial sectors for business-critical DCI applications, such as business continuity and disaster recovery. They are also widely deployed in the government, oil and gas, transportation and utility sectors for mission-critical DCI applications.


**Acronyms**

<table>
<thead>
<tr>
<th>AI</th>
<th>artificial intelligence</th>
<th>LSO</th>
<th>Lifecycle Service Orchestration</th>
</tr>
</thead>
<tbody>
<tr>
<td>CNP</td>
<td>carrier-neutral provider</td>
<td>MEF</td>
<td>Metro Ethernet Forum</td>
</tr>
<tr>
<td>CSP</td>
<td>communications service provider</td>
<td>MPLS</td>
<td>multiprotocol label switching</td>
</tr>
<tr>
<td>DCI</td>
<td>data center interconnect</td>
<td>NFV</td>
<td>network functions virtualization</td>
</tr>
<tr>
<td>DWDM</td>
<td>dense wavelength division multiplexing</td>
<td>OTT</td>
<td>over-the-top</td>
</tr>
<tr>
<td>ICP</td>
<td>Internet cloud provider</td>
<td>POP</td>
<td>point of presence</td>
</tr>
<tr>
<td>HD</td>
<td>high definition</td>
<td>QoS</td>
<td>quality of service</td>
</tr>
<tr>
<td>ICP</td>
<td>Internet service provider</td>
<td>SDN</td>
<td>software-defined networking</td>
</tr>
<tr>
<td>IT</td>
<td>information technology</td>
<td>SI</td>
<td>system integrator</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
<td>SLA</td>
<td>Service Level Agreement</td>
</tr>
<tr>
<td>IX</td>
<td>internet exchange</td>
<td>SME</td>
<td>small to medium enterprise</td>
</tr>
<tr>
<td>IoT</td>
<td>Internet of Things</td>
<td>VR</td>
<td>virtual reality</td>
</tr>
<tr>
<td>KPI</td>
<td>Key performance indicator</td>
<td>WAN</td>
<td>wide area network</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: SR1612003673EN (March)