



Harness the power of a utility private OT cloud

With seamless IED-workload interconnect

White paper

As operational technology (OT) applications are moving to the cloud in the utility data center (private OT cloud), a new challenge is to provide the necessary communications between the intelligent electronic devices (IEDs) connected to the mission-critical network and the OT workloads connected to the data center fabric. This white paper explains how a fabric-WAN/FAN integration blueprint can provide seamless end-to-end communication paths to harness the full power of OT cloud.

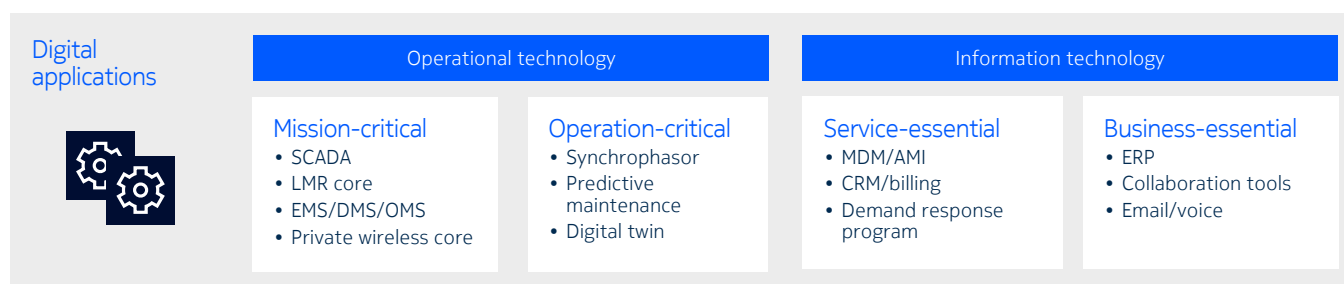
Contents

Evolving to a private OT cloud	3
Is the data center fabric ready for private OT cloud?	4
Essential data center fabric attributes for OT cloud	5
Support for IED-workload interconnect	5
Support for cloud-to-cloud interconnect	6
Evolve the data center fabric for private OT cloud	7
A data center fabric-WAN/FAN integration blueprint	7
Seamless control plane integration	7
Seamless data plane integration	8
Seamless service plane integration	8
Summary	8
Learn more	9
Abbreviations	9

Evolving to a private OT cloud

A confluence of energy technology innovations, regulatory changes and ambitious net-zero emission targets is reshaping the power utility landscape. In response, utilities are evolving the electric grid to a digitalized, decarbonized and decentralized system for a new energy future with better economies and more agile grid operations. Utilities are increasingly embracing digital applications and platforms to transform their grid and business operations (see Figure 1).

Figure 1. Common digital applications for utilities



Power utilities already deploy large-scale applications, particularly operational technology (OT) applications, to run their grids. They were early adopters of supervisory control and data acquisition (SCADA) systems for critical remote monitoring and control and private land mobile radio (LMR) systems for critical wireless communication with field crews.

As utilities modernize the grid to improve reliability and efficiency, they deploy OT applications on energy management systems (EMS), distribution management systems (DMS) and outage management systems (OMS). Utilities also deploy more comprehensive OT grid monitoring schemes such as synchrophasor measurement units and micro-sensors on grid assets for wide area monitoring and control, predictive maintenance and generating digital twin replicas. All of these new applications harness the latest information and communications technology advancements in industrial Internet of Things (IoT) and virtualized compute resources.

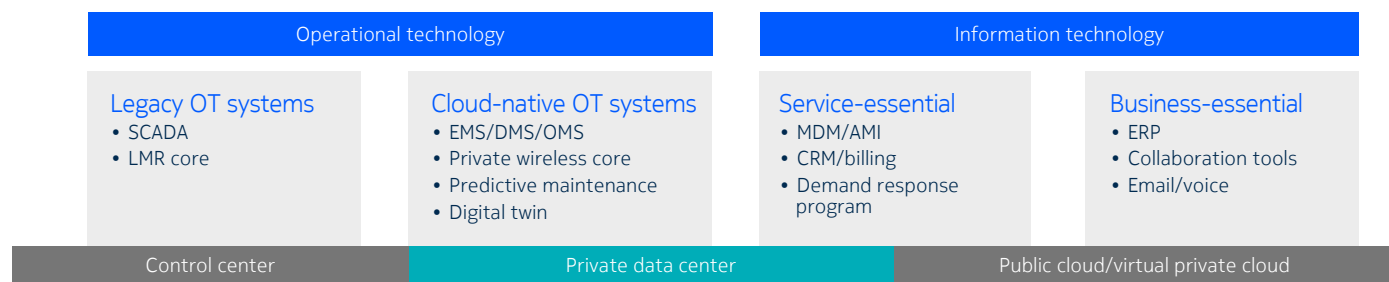
At the same time, utilities deploy information technology (IT) systems such as metering applications and customer care systems as well as other enterprise applications essential for business operations.

These developments in digital OT and IT applications have led to the adoption of cloud computing to meet the exponential increase in compute needs plus requirements for application agility and the capability to support elastic workload demand—all while keeping data center infrastructure costs under control.

Hybrid cloud adoption supports private cloud in utility-owned data centers for critical OT applications and migrates enterprise or service-related applications to public cloud services. Confidential information such as customer data is kept in utility data centers (see Figure 2).

In this hybrid cloud model, the majority of IT applications migrate to the public cloud. The private cloud is dominated by OT applications, becoming an OT cloud. This paper explores how private OT cloud impacts a utility's data center fabric.

Figure 2. A hybrid cloud model for utility digitalization

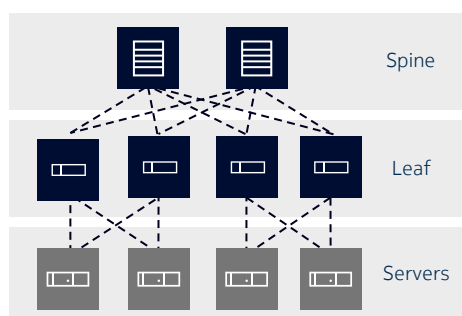


Is the data center fabric ready for private OT cloud?

A modern data center network is the communications foundation of a power utility's IT infrastructure. Optimized for cloud computing and scalability, the data center network is architected with a two-tiered leaf-spine topology (see Figure 3).

The data center network is referred as a fabric because every server-connected switch, the leaf switch, is connected to every spine switch, which is the fabric backbone. This topology provides fully meshed connectivity to all server endpoints, optimizing traffic flow (east-west traffic) between modules or microservices within an application.

Figure 3. Modern data center fabric topology



Essential data center fabric attributes for OT cloud

In a traditional OT deployment, many applications are siloed. Converting them to a cloud model allows support for more distributed traffic patterns, sharing of workstreams and scaling of OT application workflows. With OT applications running in the private cloud, the data center fabric is now part of the mission-critical network infrastructure and needs to support network essentials: strong resiliency, deterministic quality of service (QoS) and robust cyber security.

Strong resiliency

OT applications such as SCADA and synchrophasor provide continual oversight and control of the grid. Communication outages can have grave safety consequences.

With meshed leaf-spine connectivity and a server dual-homing configuration, the data center fabric has rich path diversity to deliver traffic reliably. Coupled with IP routing and the use of Ethernet VPN (EVPN), traffic can be redirected quickly for fast communication restoration. This approach allows data to move easily between any-clouds, data centers and other grid resources so that services can expand or contract seamlessly to meet evolving workloads.

Deterministic QoS

The data center fabric needs strong and flexible QoS capabilities to constantly meet QoS needs for each OT application. Differing performance requirements of applications can lead to great complexity.

Building different levels of QoS for utility applications or classes of users provides the following benefits:

- Establishes clear priorities to control heavy users or applications during peak or off-peak usage
- Protects the network from misconfigured or ill-behaved servers sending microburst data, causing congestion
- Ensures good application performance consistently
- Reduces potential scaling or congestion issues that could affect grid operations
- Classifies best practices for application key performance indicators (KPIs).

Robust cyber security

Because the data center fabric is part of the grid communication infrastructure, utilities need to evaluate their security needs based on utility-specific frameworks and guidelines such as IEC 62351 and the NERC CIP standard suite in addition to their standard IT security policy.

The use of a multi-layer security strategy is paramount. The strategy needs to include security for management and services as well as for the control, data and physical planes of any cloud or network. Examples such as end-to-end encryption at ingress and egress, use of access control lists and global or local firewall policies are all effective tools to stop illicit traffic flows.

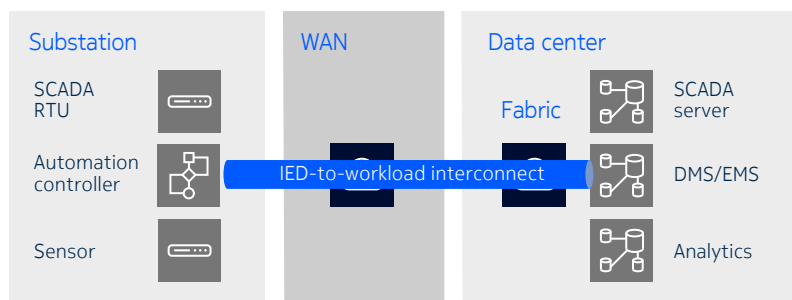
Support for IED-workload interconnect

In addition to the preceding essential attributes, the private OT cloud demands more from the data center fabric to support the evolving grid architecture. The data center fabric needs to support new use cases. The first use case is support for IED-workload interconnect.

Utilities capitalize on the capability of intelligent electronic devices (IEDs) in substations for grid automation, control and monitoring. The OT workloads in the data center need to constantly collect data from the IEDs and exchange control messages with them.

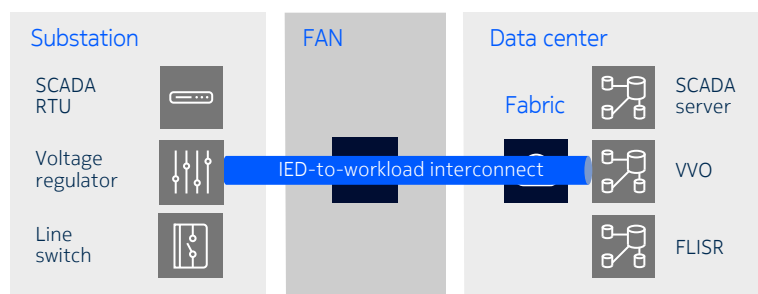
As utilities evaluate, trial and deploy new OT applications, they need to establish connections in the WAN through the data center fabric to link IEDs and OT workloads as needed (see Figure 4).

Figure 4. Data center fabric-WAN interconnect



Utilities are increasingly deploying incremental distribution automation, requiring large-scale IEDs to be deployed on utility poles or strategically in the grid assets, which can be reached only through the field area network (FAN) using wireless technology such as LTE. As a result, utilities need to establish connections in the FAN through the data center fabric to link IEDs and OT workloads as needed (see Figure 5).

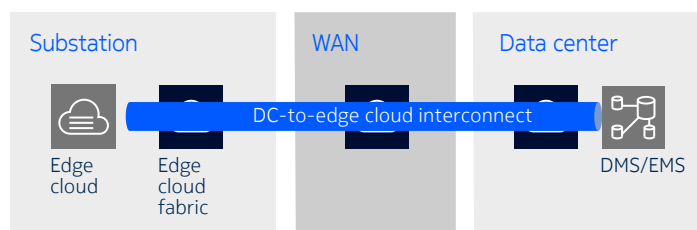
Figure 5. Data center fabric-FAN interconnect



Support for cloud-to-cloud interconnect

Utilities are looking ahead to grid intelligence decentralization for improved automation response speed and to edge computing for demand-side management that allows consumers more control of energy consumption. Deployment of edge cloud in substations can provide the required field computing capabilities. The second new use case is to seamlessly interconnect the workloads in the OT cloud in the data center and the edge cloud in the substation; this is called cloud-to-cloud interconnect (see Figure 6).

Figure 6. Cloud-to-cloud interconnect



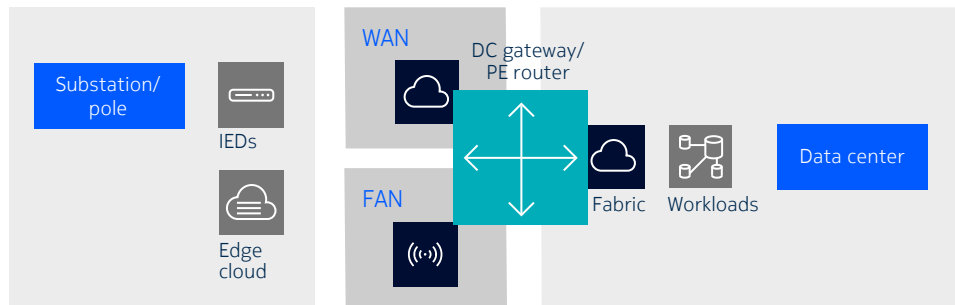
Evolve the data center fabric for private OT cloud

The data center fabric needs to support the new use cases introduced by the adoption of private OT cloud. However, networking technologies are a challenge.

The data center fabric uses a different networking technology than the WAN and the FAN. A legacy data center fabric typically uses Ethernet VLAN technology and is progressing to more flexible Virtual eXtensible LAN (VXLAN)/EVPN services to support cloud computing. By contrast, WANs and FANs tend to use IP/MPLS VPN for mission-critical grid communications.

A reliable and scalable approach to bridge the data center fabric and the network (WAN and FAN) domains is to introduce a data center gateway. A data center gateway that acts as the IP/MPLS provider edge (PE) router for the WAN and the FAN can integrate these two domains in the control, data and service planes (see Figure 7).

Figure 7. Data center gateway integrating the fabric with the WAN and the FAN



A data center fabric-WAN/FAN integration blueprint

Integrating the data center fabric with the WAN and the FAN requires interworking in the control plane, data plane and service plane. Figure 8 illustrates an integration blueprint comprising these three planes.

Seamless control plane integration

The data center gateway uses cloud-friendly Border Gateway Protocol (BGP) to peer with both the workload-connected leaf switch in the data center and the IED-connected substation router or field router in the WAN or the FAN.

The use of BGP provides full IP address advertisement for workload endpoints and IEDs across the two domains. This allows full automation of IED and workload deployment as well as mobility and migration. When the workloads migrate to another rack, pod or another facility, or when a new IED is deployed on the grid, the corresponding IP address is advertised by the leaf switch or the substation router throughout the WAN, FAN and the data center fabric. This full IP address advertisement ensures that routing information is always up to date everywhere.

BGP also plays an integral role in disaster recovery and operation continuity. When the active data center fails due to a major incident and workloads switch to the standby data center, end-to-end BGP can gracefully support the disaster recovery efforts through automated, reliable update of all routers in the WAN, FAN and the data center fabric. Workloads in the standby data center will now be able to communicate the IEDs for grid monitoring and control. In this way, BGP facilitates operations continuity.

Seamless data plane integration

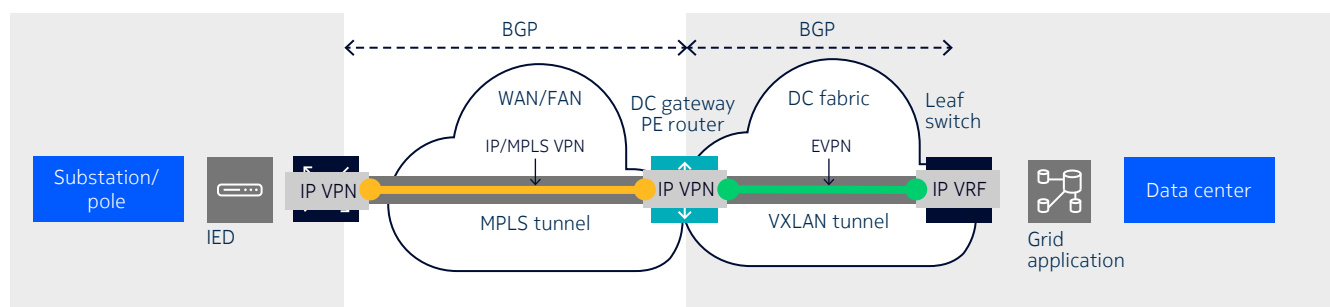
By supporting MPLS or IP tunnels on the WAN- or FAN-facing interface and VXLAN tunnel on the fabric-facing interface, the data center gateway provides seamless IED-to-workload data connections by switching traffic from one type of tunnel to another. The gateway also facilitates an end-to-end, deterministic and consistent QoS policy.

Furthermore, by harnessing the power and flexibility of an open network development kit (NDK) in the new generation of fabric switches, a utility can monitor the workload-to-IED connection to ensure consistent, high OT application performance.

Seamless service plane integration

Service plane integration enables IP/MPLS VPN services in the WAN/FAN and EVPN IP-VRF (virtual routing and forwarding) services for end-to-end IED-workload connections. This seamless service plane integration, together with control plane and data plane integration, allows IEDs and workloads to communicate with each other.

Figure 8. Data center fabric-WAN/FAN integration blueprint



Summary

As utilities modernize, they can harness the power of private OT cloud to digitalize their operations and transform the electric grid. Looking ahead, this transformation will also support adoption of larger scale IEDs and more cloud-based OT applications. The data center fabric-WAN/FAN integration blueprint can provide the reliable end-to-end communication paths to connect on-grid IEDs with OT in the cloud.

Nokia is at the forefront of cloud services development. Our solutions support any Layer 2 and Layer 3 WAN service type and connectivity model as well as VXLAN and EVPN technologies. We also offer flexible cloud-WAN service configuration models. And our solutions fully integrate into the data center for unrestricted data center networking across the WAN, FAN or any-cloud.

Our broad product portfolio spans data center fabric, IP/MPLS, packet optical and microwave transport as well as network automation, LTE/5G and security. Complemented by a full suite of professional services (network audit, design and engineering practices), Nokia has the unique capability and flexibility to help utilities build a cloud-optimized communications platform to thrive in the digital future.

Learn more

To learn more about Nokia solutions for utilities, data centers and IP/MPLS, visit our web pages:

- [Power utilities](#)
- [Data center solution](#)
- [IP/MPLS portfolio](#)

Abbreviations

AMI	advanced metering infrastructure	MP-BGP	Multiprotocol Border Gateway Protocol
CRM	customer relation management	MPLS	multiprotocol label switching
DC	data center	NERC CIP	North American Electric Reliability Corporation critical infrastructure protection
DMS	distribution management system		
EMS	energy management system	OMS	outage management system
ERP	enterprise resource planning	OT	operational technology
EVPN	Ethernet virtual private network	PE	provider edge
FAN	field area network	QoS	quality of service
FLISR	fault detection, location, isolation and service restoration	RTU	remote terminal unit
IED	intelligent electronic device	SCADA	supervisory control and data acquisition
IoT	Internet of Things	VLAN	virtual local area network
IP	Internet Protocol	VPN	virtual private network
IT	information technology	VVO	volt/VAR (volt-amps reactive) optimization
LMR	land mobile radio	VXLAN	Virtual eXtensible Local Area Network
LTE	long term evolution	WAN	wide area network
MDM	meter data management		

About Nokia

At Nokia, we create technology that helps the world act together.

As a B2B technology innovation leader, we are pioneering the future where networks meet cloud to realize the full potential of digital in every industry.

Through networks that sense, think and act, we work with our customers and partners to create the digital services and applications of the future.

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.

© 2023 Nokia

Nokia OYJ
Karakaari 7
02610 Espoo
Finland
Tel. +358 (0) 10 44 88 000

Document code: (February) CID210839