Enabling DER islanding protection—and more

Using a converged FAN for multiservice connections with resiliency, QoS and security

White paper

When interconnecting distributed energy resources (DERs) with electric grids, utilities need to deploy islanding protection schemes to make grid operations safe and to ensure power quality. One prevalent protection scheme is direct transfer trip (DTT)—but DTT alone is not enough. DTT needs a converged field area network (FAN) to provide multiservice connections with resiliency, QoS and security. This white paper explains how.

Contents

Safe DER interconnection with DTT

A confluence of energy technology innovations and government policy shift is placing immense strain on distribution grids. The continued drop in distributed energy resources (DERs) energy cost has propelled renewables to become the fastest growing source of new power capacity. Governments have increasingly committed to the ambitious goal of becoming climate neutral and in many cases have mandated aggressive adoption of green energy.

In response, utilities are striving to embrace DERs such as wind and solar for decarbonization. Utilities develop and source DERs and interconnect them with their grids. Due to the non-deterministic nature of DERs, they need continuous and intensive oversight of energy infeed at the interconnection point, the point of common coupling (PCC).

By deploying SCADA and synchrophasors at the PCC, utilities can monitor the infeed conditions (e.g., voltage, frequency, plus real and reactive power) in real time and use the information for power balancing and grid stability analysis.

In addition to grid stability, grid safety is another prime consideration. One top concern is the adverse impact brought by unintentional islanding.

Figure 1a shows a feeder circuit energized by a substation and a solar plant. If a fault occurs in Section 11, the adjacent recloser and the substation circuit breaker open to de-energize the circuit (see Figure 1b). Then, the solar plant energizes Section 12 through the PCC, creating unintentional islanding.

Unless special measures have been taken for islanded operation, this situation can cause hazards for the maintenance crew. In addition, out-of-range voltage and frequency can occur, damaging customer equipment in Section 12[1].

Figure 1a. A feeder circuit energized by DER

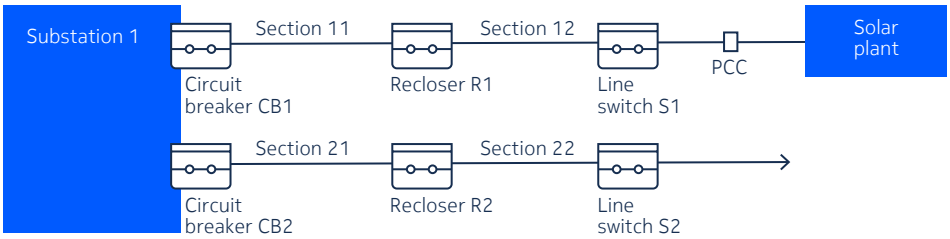
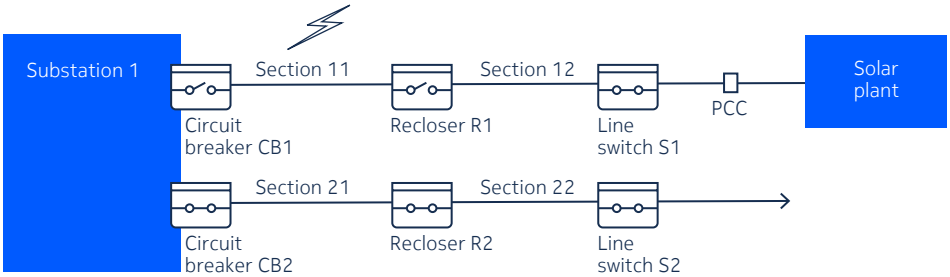


Figure 1b. A feeder circuit with fault in Section 11



To avoid these dangers, when interconnecting DERs in electric grids, utilities need to deploy islanding protection schemes to make grid operations safe and to ensure power quality. (Islanding protection is also commonly known as anti-islanding.) One prevalent protection scheme is direct transfer trip (DTT).

1 For a detailed discussion on islanding, read IEEE Standard 1547-2018.

DTT alone is not enough for islanding protection

DTT, a communication-based system protection application, was originally conceived for high-speed tripping of generator station equipment or transmission substation circuit breakers.

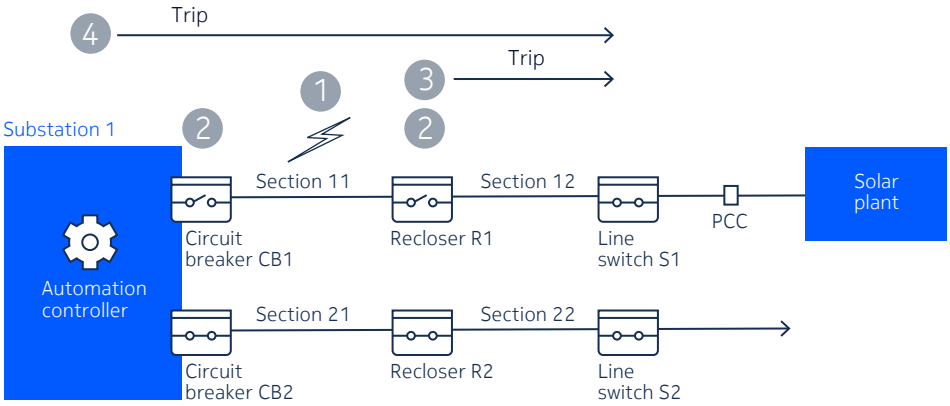
When a line fault occurs, the DTT relay sends a trip command through a communication channel to its remote counterpart to protect the generator or high-voltage transformer. To prevent damage, this type of high-voltage protection action needs to occur in the range of 5 – 50 ms.

Because DTT relies extensively on communications for fast protection, it is imperative that the communication channel can deliver trip messages reliably within the delay budget. The communication channel used to be a 2-wire/4-wire telephone circuit but has been successfully migrated to private IP/MPLS mission-critical networks.

DTT is a straightforward and effective islanding protection scheme that works as follows (see Figure 2):

1. A fault occurs in Section 11.
2. Upon detection, the adjacent circuit breaker and recloser open to clear the fault and to de-energize.
3. Recloser 1 (R1) then sends trip signals to the downstream line switch S1 at the PCC. S1 then become opens and the solar plant stops energizing the connected feeder.
4. Trip signals can alternatively be sent from an automation controller in the substation when the substation automation controller detects that a midline recloser is open.

Figure 2. Islanding protection by DTT



As shown in Figure 2, DTT is a communication-centric protection scheme requiring that trip signals be reliably delivered all the time. As a result, it is imperative that the field area network (FAN) that connects all the field IEDs provides resilient communications.

In addition, because of the hazards caused by unintentional islanding in which the DER energizes feeder circuits through the PCC, it is crucial to trip the breakers quickly (within 2 sec as specified in IEEE1547-2018). As a result, deterministic quality of service (QoS) is another important FAN attribute.

With the level of cyber threats rising, FAN security is also essential to protect DTT communications.

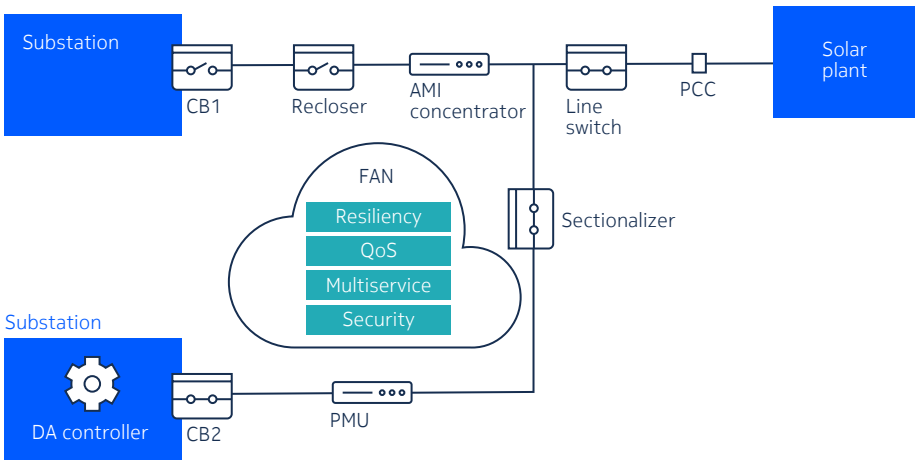
Finally, as utilities make the distribution grids smarter for better oversight, higher reliability and better power quality, they harness a range of distribution automation applications, including FLISR (fault location, isolation and service restoration) and synchrophasors. The FAN needs to support more than just DTT.

To address all of these needs, utilities need a converged FAN.

The converged FAN: Key to DTT and more

The rest of this paper provides an overview of the converged FAN architecture[2], then discusses its four essential attributes for DTT and other grid communications: strong multi-fault network resiliency, deterministic QoS, any-to-any multiservice, and network security (see Figure 3).

Figure 3. Essential attributes of a converged FAN



Overview of the converged FAN

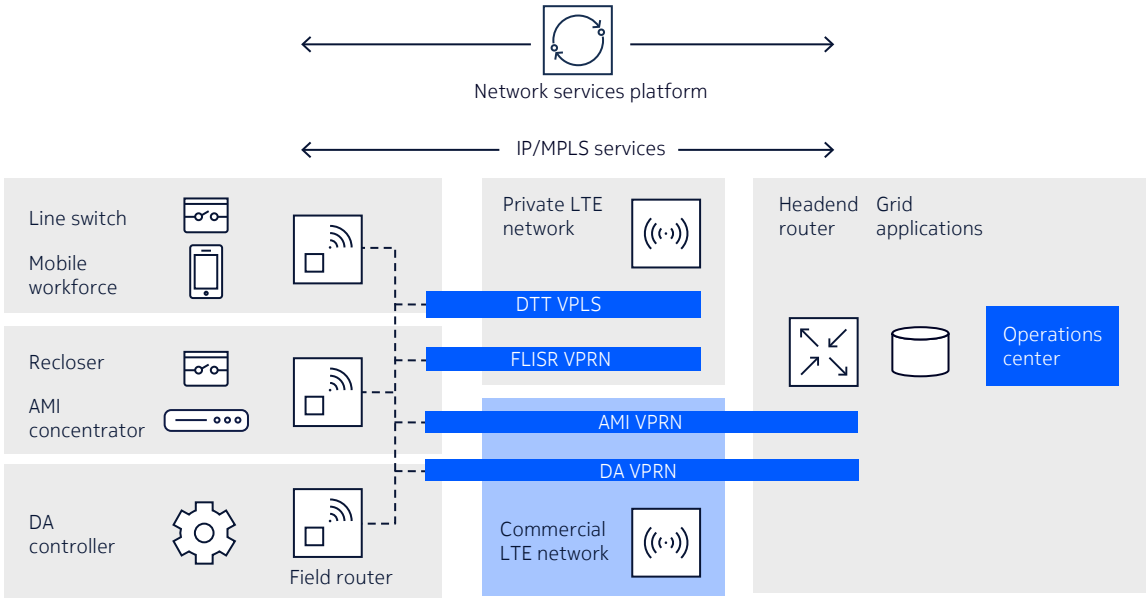
The converged FAN (see Figure 4) is grounded in standards-based LTE and IP/MPLS. Harnessing an IP/MPLS field router with an LTE interface, the FAN wirelessly brings the following capabilities out to utility poles, unfibered low-voltage substation and DER sites, and connect-grid intelligent electronic devices (IEDs):

- Ubiquitous IP/MPLS services connecting a vast and growing variety of IEDs, such as automation controllers, line switches, synchrophasors and Internet of Things sensors
- Advanced Layer-3 (IP) and Layer-2 (Ethernet) VPN services to support grid communications, including Distributed Network Protocol 3 (DNP3), GOOSE and serial interfaces
- Deterministic QoS for delay-sensitive applications such as DTT
- Enhanced any-to-any multipoint connectivity in the field for decentralized/distributed grid applications that require peer-to-peer[3] communications
- High mobility for assets and workers on the move
- Utmost resiliency to avoid disruptions, with fallback to commercial mobile data service
- Robust security to address a growing range of cyber-security threats.

2 For a full description of the Nokia converged FAN, read the white paper "Rethinking the FAN for grid automation."

3 Peer-to-peer communications are also known as machine-to-machine (M2M) or machine type communications (MTC).

Figure 4. Nokia converged FAN architecture supporting DTT and distribution automation (DA)



The converged FAN typically runs atop a private LTE (P-LTE) network deployed and operated by utilities using dedicated or shared spectrum. When P-LTE is not an option due to spectrum unavailability or other reasons, LTE service from commercial carriers is a viable alternative that provides the same functionality. However, utilities typically prefer P-LTE because it provides complete operational and maintenance control.

The converged FAN architecture can run over both P-LTE and carrier LTE service simultaneously.

Utmost end-to-end resiliency for reliable communications

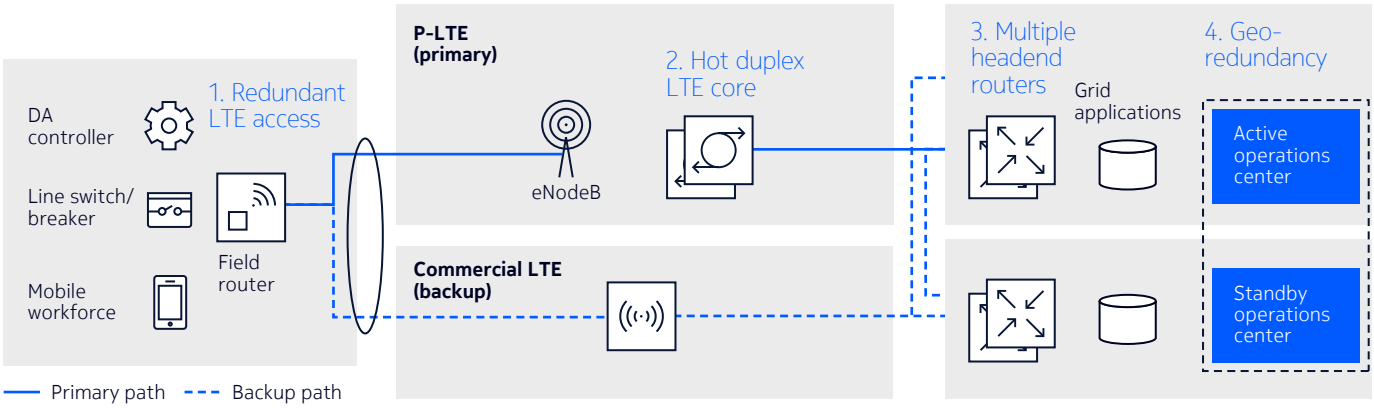
As seen in Figure 4, the scope of the FAN is more than just the LTE link between the field router and the base station (eNB). The FAN extends all the way to the headend router in the control center and data center, where operational technology (OT) applications such as Advanced Distribution Management Systems (ADMS) and grid analytics reside.

If there is a fault along the whole communication path, operators would lose oversight and control of the distribution grid and the DER status. Accordingly, the FAN needs to have full redundancy protection along the end-to-end communication path (see Figure 5).

The key protected elements in the converged FAN are:

1. Redundant LTE access
2. High availability (HA) and geo-redundant LTE packet core
3. Multiple redundant headend routers
4. Geo-redundant operations center

Figure 5. End-to-end FAN redundancy



Redundant LTE access

The field router connects with the LTE base station (called the eNB) of the private LTE network. If the eNB fails, grid communications in the area covered by the failed eNB stop completely. Therefore, it is necessary to have highly available LTE access.

Deploying a second eNB with overlapping wireless coverage as backup is technically feasible but often is not economical for a large service area. A cost-effective alternative is to use commercial LTE service as backup[4]. When the primary private LTE network fails, the field router resorts to the backup commercial LTE network.

HA and geo-redundant LTE packet core

The packet core is the central gateway for LTE radio traffic, forwarding packets to grid application servers in control centers/data centers or towards other IEDs in the field. Packet core equipment failure would render the whole LTE network inoperable, stopping all mission-critical traffic and other application traffic.

Consequently, it is necessary to deploy the packet core in HA mode, with an active core and a standby core. For further resiliency and to meet disaster recovery (DR) requirements, the packet core should be deployed in a geo-redundant mode.

A typical duplex-mode implementation needs to re-establish LTE sessions with all field routers during protection switching; this process disrupts all grid communications for minutes. Furthermore, with all IEDs trying to re-establish connections at the same time, there is a lot of signaling load on the packet core, causing potential instability.

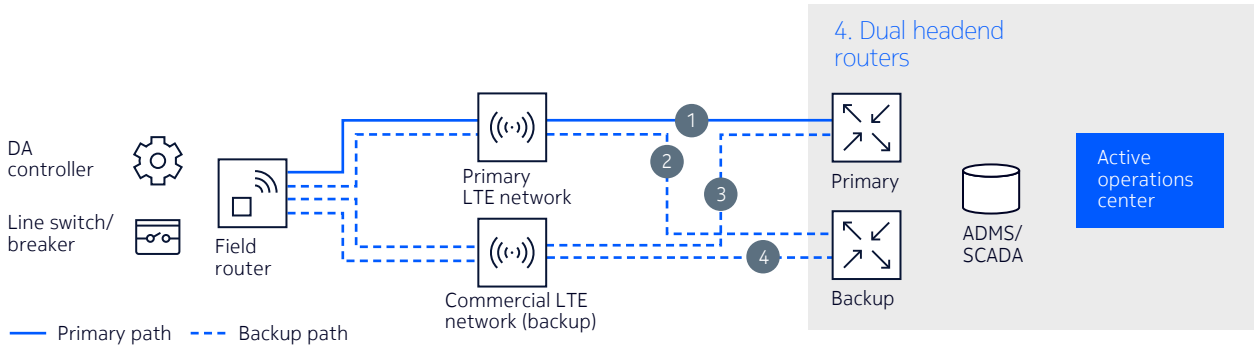
HA technology allows the active and standby cores to constantly synchronize the state information of all sessions, enabling graceful switching and eliminating any disruption to grid communications.

Multiple redundant headend routers

The headend router, located at the operations center, terminates IP/MPLS services for traffic destined to the centralized ADMS or SCADA server. It is imperative that the headend router be protected with nodal redundancy via backup headend routers located in the active operations center (see Figure 6) and in the standby operations center.

4 When considering commercial LTE service as a backup link, it is important to understand the SLA of and redundancy measures adopted by the commercial LTE operator.

Figure 6. Dual headend routers deployed in the active operations center



It is essential that the field router have the capability and scalability to establish multiple MP-BGP-4 (Multiprotocol Border Gateway Protocol-4) control sessions with the primary headend router and all backup headend routers via the primary or backup LTE networks.

The router monitors the operational status of the sessions. When the primary headend router fails, the router detects a status change of session and switches traffic from the primary path (Path 1 in Figure 6) to a backup path (Path 2 in Figure 6) to connect to the backup headend router.

The backup router maintains BGP routing information to the FAN routers so they can keep communicating with each other as needed for the DTT application.

If a second failure occurs in the primary LTE network, the router also detects the change of the control session with the backup headend router, then switches from Path 2 to Path 4.

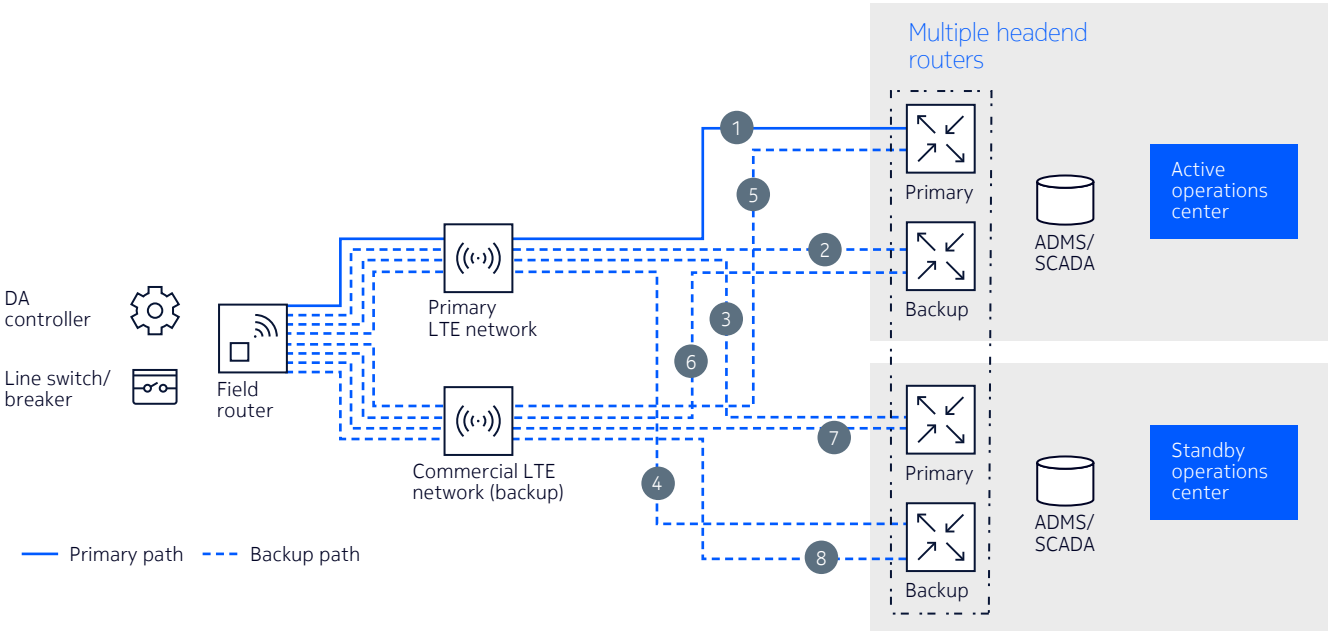
Geo-redundant operations center

The operations center is the nexus of grid operations where utilities monitor, control and analyze grid operating conditions and restore outages. Because extreme weather events such as hurricanes and severe flooding are becoming more intense and more frequent, even in urban areas, it is crucial for utilities to have a standby operations center equipped with an identical network and applications environment at a different location.

One key pillar of this geo-redundancy is to extend the multi-headend routers scheme by deploying another backup headend router pair in a standby operations center (see Figure 7). When the active operations center is damaged by major incidents, the field router detects the change in the control sessions with the headend router pair in the active operations center. It then switches traffic to Path 3 to reach the standby operations center.

If the primary LTE network is also struck by the weather event, the router can switch to Path 7 or Path 8 to restore connectivity.

Figure 7. Geo-redundant protection with multiple headend routers

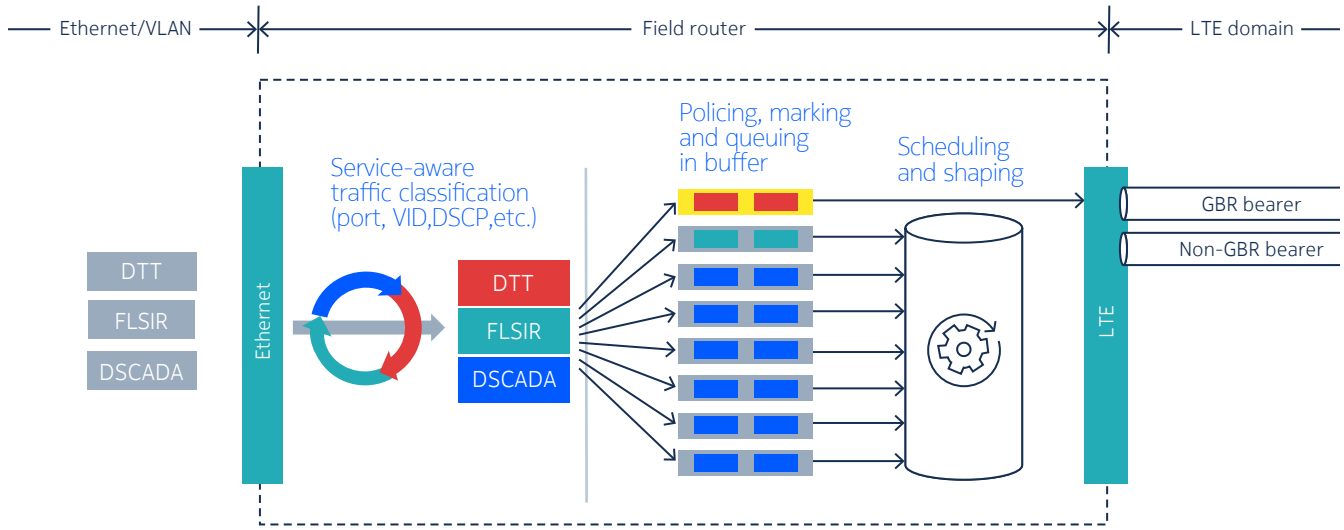


Deterministic QoS for assured data delivery

To ensure that DERs stop energizing within 2 sec after an island is formed requires prioritized network delivery of trip signals over other FAN applications such as FLISR, Advanced Metering Infrastructure (AMI) and workforce mobility.

The field router combines the use of Ethernet VLAN ID (802.1q), 802.1p tag, DiffServ, MPLS traffic class and LTE QoS Class Identifier (QCI) for advanced traffic classification, queuing, buffering and shaping to ensure that trip signals are consistently delivered within the delay budget (see Figure 8).

Figure 8. Deterministic QoS operations and mechanisms



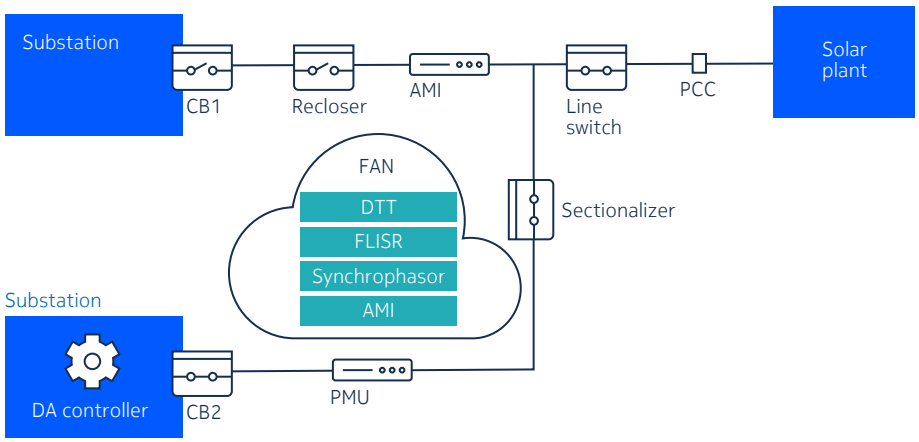
Any-to-any L2/L3 multiservice for efficient communications

Traditional grid applications adopt a model of centralized intelligence in which field devices communicate with centralized application systems such as an energy management system (EMS) or a distribution management system (DMS). As processors are now more powerful, intelligence is becoming distributed and residing in an automation controller and IEDs inside substations and on poles, resulting in faster responses unlocking more grid-edge innovations. Consequently, a converged FAN needs to support multipoint machine-to-machine communications in the field.

The traffic can contain control commands using IP-based DNP3 or Ethernet-based GOOSE messages. Moreover, when supporting GOOSE-based applications, it is important to segment the Ethernet domain into multiple virtual LAN (VLAN) domains to limit the scope of Ethernet broadcasting.

The converged FAN's full IP/MPLS multiservice capability can support virtual private LAN service (VPLS) for Layer 2 VLAN service, Ethernet pseudowires for point-to-point Ethernet service, and virtual private routed network VPRN for Layer 3 IP service, covering the whole range of service profiles (see Figure 9).

Figure 9. A multiservice converged FAN



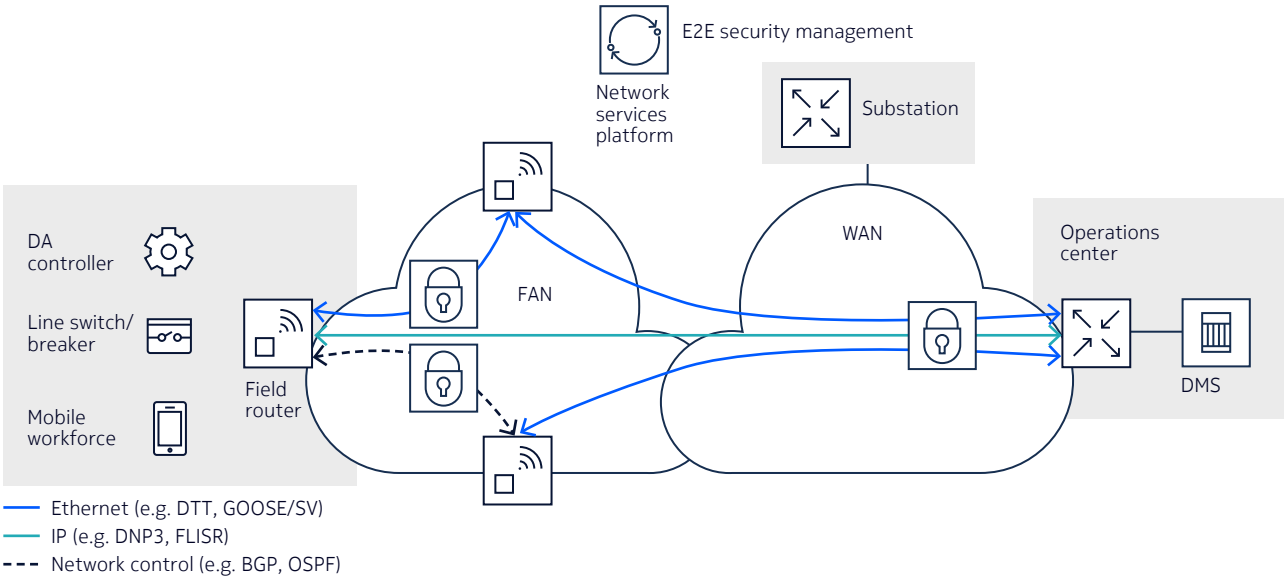
Robust network defense for secure communications

Today's encryption mechanisms are not robust enough to protect the any-to-any communications in the converged FAN because provisioning meshed point-to-point secure tunnels is operationally challenging. The encryption mechanisms are also not optimized for Layer 2 applications because they are designed for the IP protocol.

The converged FAN has a group-based encryption approach called Network Group Encryption (NGE) technology[5], to safeguard all traffic (including Layer 2, which is ideal to protect GOOSE traffic), Layer 3, and network control plane traffic) in the FAN as well as in the WAN (see Figure 10) on a per-application basis.

5 To learn more about NGE, read the Nokia white paper "Network Group Encryption."

Figure 10. NGE offers end-to-end protection



Summary

Utilities play an integral role in the world drive toward climate neutral. Decarbonizing the grid is an important step in the journey toward this goal.

DTT and other DA applications are pivotal for utilities to attain the goal of 100 percent clean energy while maintaining grid safety and improving power reliability. A highly resilient, QoS-enabled, service-centric and secure converged FAN is foundational to the green journey by providing the field communication foundation.

With a broad communications product portfolio spanning IP/MPLS, LTE/4G and 5G to packet microwave and packet optical transport, along with cyber security, Nokia has the unique capability and flexibility to help utilities transform their networks. This product portfolio is complemented by a full suite of professional services, including audit, design and engineering practices.

To learn more about Nokia for utilities, visit our Power utilities web page.

Abbreviations

ADMS	Advanced Distribution Management Systems
AMI	Advanced Metering Infrastructure
BGP	Border Gateway Protocol
CB	circuit breaker
DA	distribution automation
DER	distributed energy resource
DMS	distribution management system
DNP3	Distributed Network Protocol 3
DSCADA	distribution supervisory control and data acquisition

DSCP	Differentiated Services Code Point
DTT	direct transfer trip
EMS	energy management system
eNB	enhanced Node B
FAN	field area network
FLISR	fault location, isolation and service restoration
GBR	Guaranteed Bit Rate
IED	intelligent electronic device
IP	Internet Protocol
LTE	long term evolution
MP-BGP	Multiprotocol BGP
MPLS	multiprotocol label switching
NGE	Network Group Encryption
OSPF	Open Shortest Path First
PCC	Policy and Charging Control
P-LTE	private LTE
PMU	phasor measurement unit
QCI	QoS class identifier
QoS	quality of service
SCADA	supervisory control and data acquisition
SLA	Service Level Agreement
SV	Sampled Values
VLAN	virtual local area network
VPLS	virtual private LAN service
VPN	virtual private network
VPRN	virtual private routed network
WAN	wide area network

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

Document code: (February) CID210379