TÉCNICO LISBOA

Smart Grid Fundamentals

Smart Grid Architecture

António Grilo

A Communication Network Architecture for the Smart Grid

- Core-Edge Architecture:

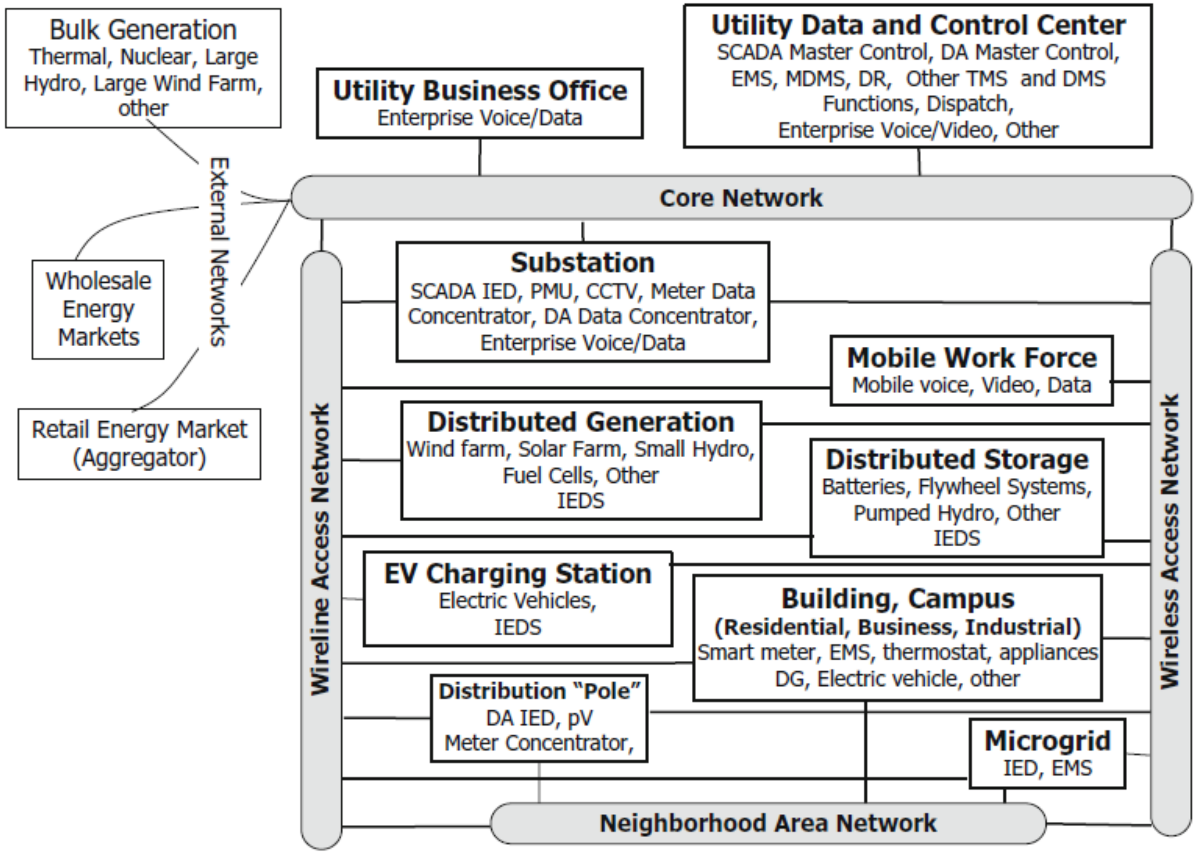


Fig. 6.1 Physical architecture framework for Smart Grid network

A Communication Network Architecture for the Smart Grid

- Physical architecture framework for Smart Grid network:

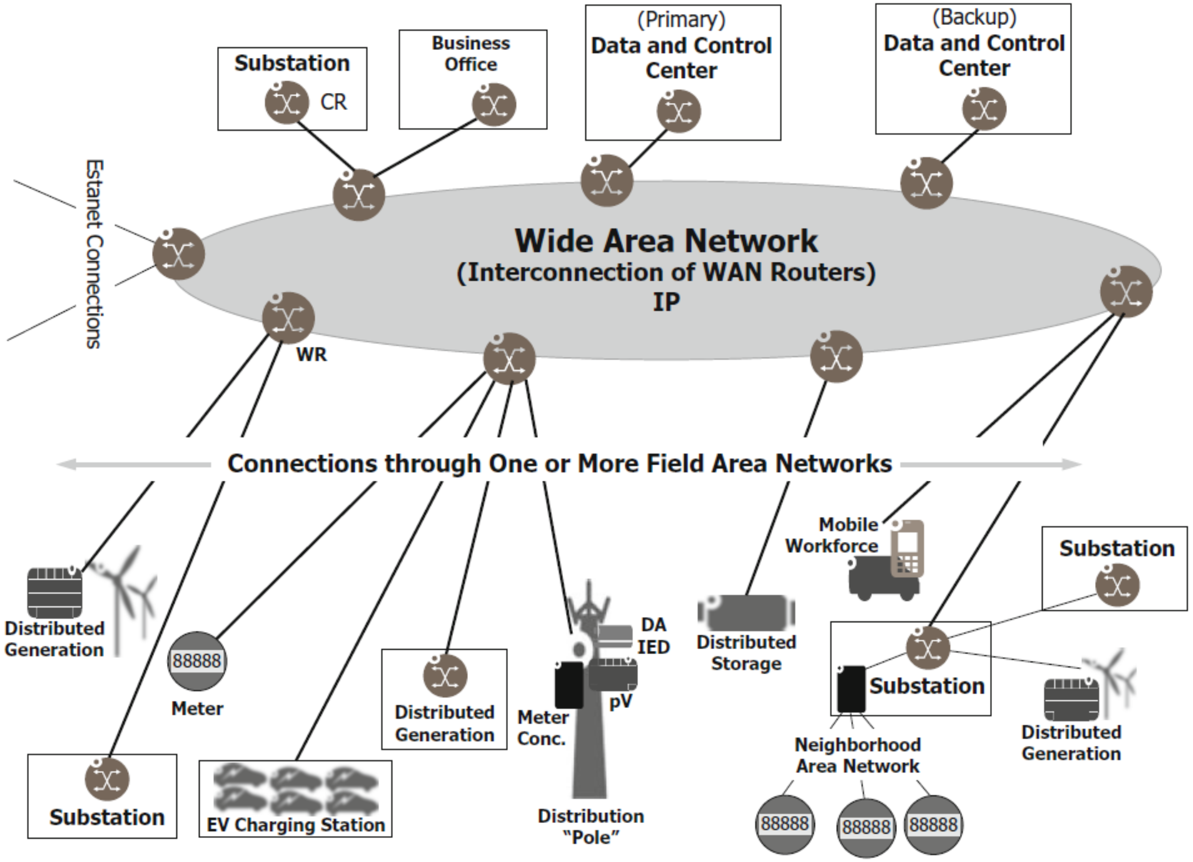


Fig. 6.10 Smart Grid communication network architecture illustration

A Communication Network Architecture for the Smart Grid

- Interior Routers (IRs) can bridge long distances between WAN Routers (WRs):

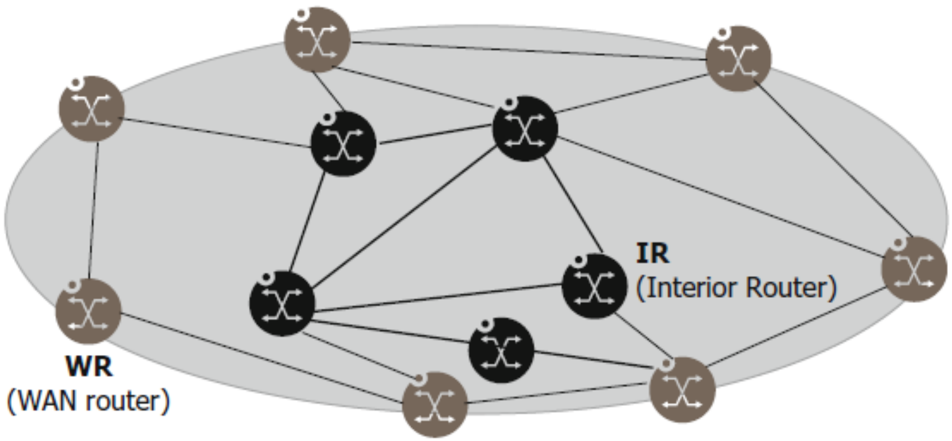


Fig. 6.3 Reliable WAN with at least two physical paths between every pair of WAN routers

A Communication Network Architecture for the Smart Grid

- Protocol layering:

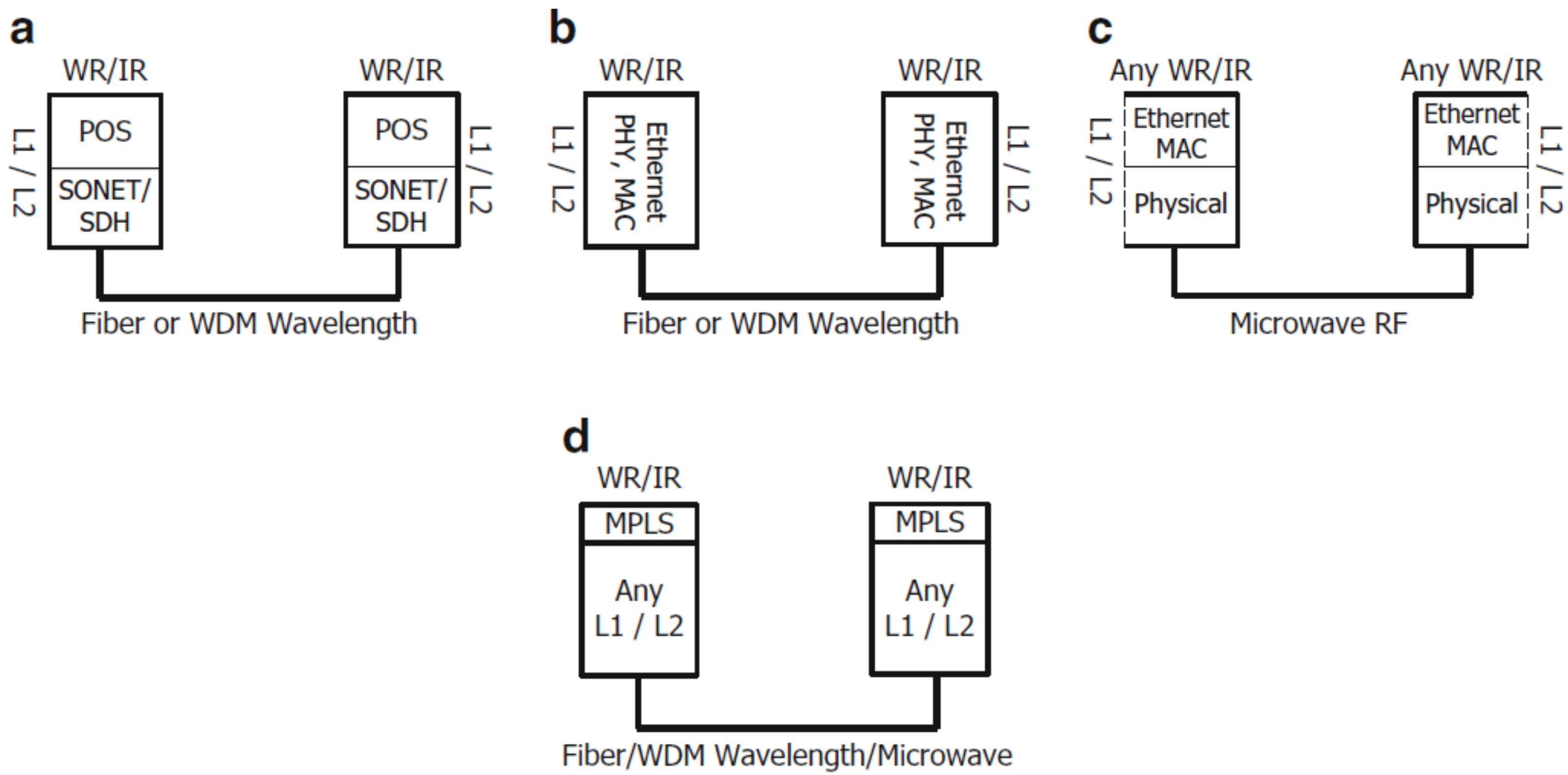


Fig. 6.4 Examples of protocol layering. (**a**) POS. (**b**) Ethernet. (**c**) Microwave. (**d**) MPLS

Traffic Aggregation

- Traffic aggregation:
  - Cost savings: fewer links need to be deployed: total cost of multiple links is larger than the cost of a single link carrying the same volume of traffic.
  - At WRs, where traffic from multiple endpoint locations is aggregated.
  - At the CRs located at substations and other locations. CR aggregates traffic generated at that location, but it may also aggregate traffic generated at nearby locations.

A Communication Network Architecture for the Smart Grid

A Communication Network Architecture for the Smart Grid
Network Design Process

- Local traffic aggregation at Cluster Routers (CRs):

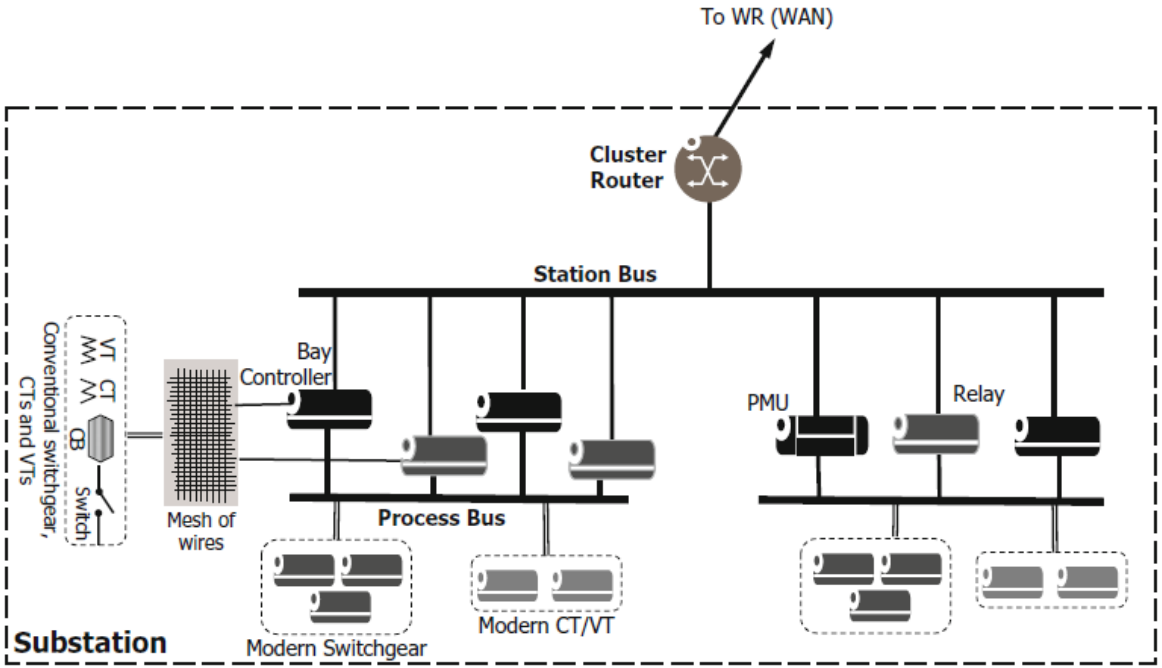


Fig. 6.6 Local traffic aggregation at a substation

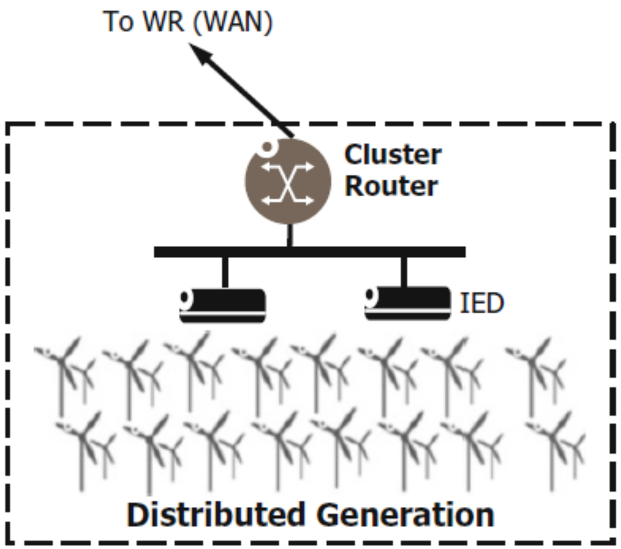


Fig. 6.7 Traffic aggregation at a distributed generation site

A Communication Network Architecture for the Smart Grid

- Local traffic aggregation at Cluster Routers (CRs):

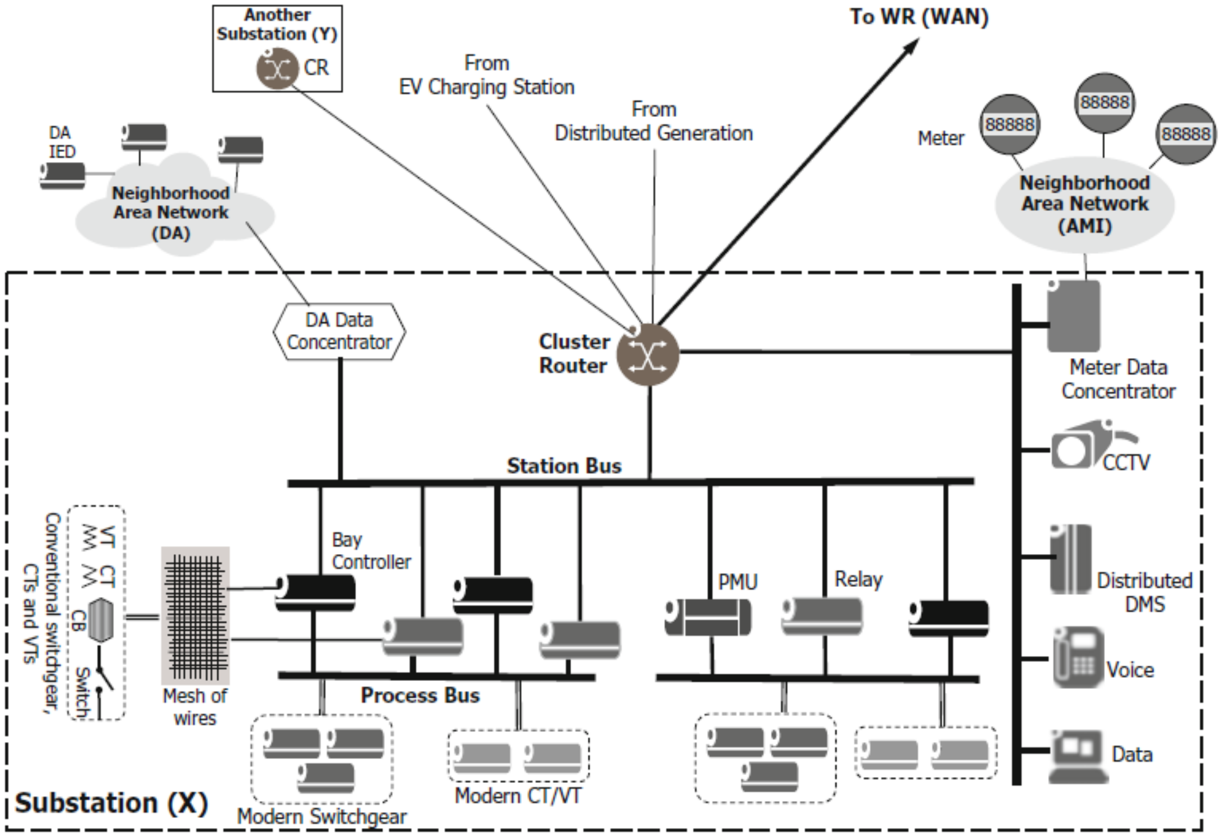


Fig. 6.9 CR at substation X aggregates traffic from nearby locations and local traffic at X

A Communication Network Architecture for the Smart Grid

- Local traffic aggregation at Cluster Routers (CRs):

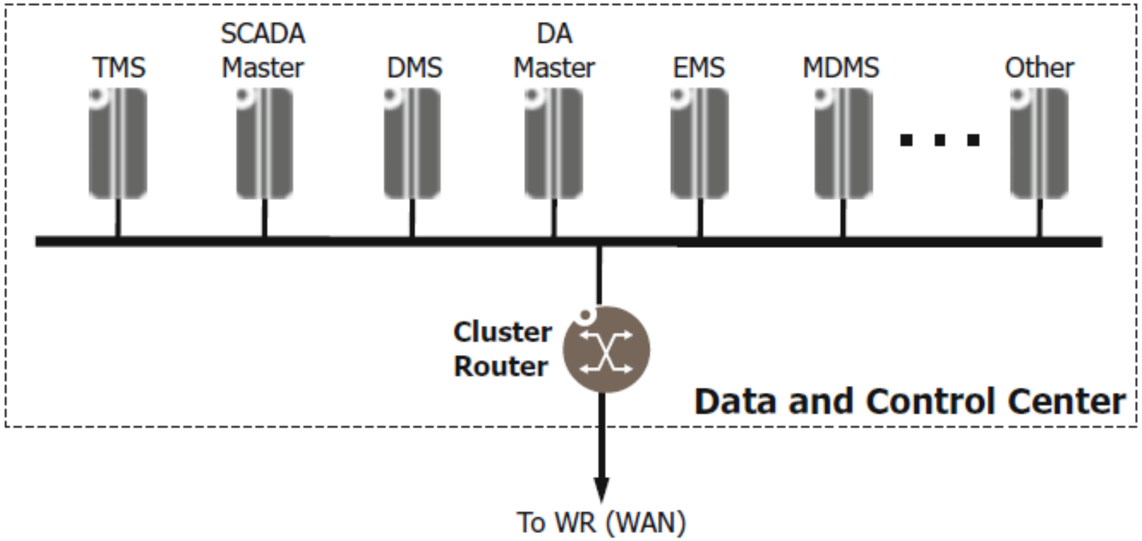


Fig. 6.8 Traffic aggregation at utility Data and Control Center

A Communication Network Architecture for the Smart Grid

Table 1
Comparison of communication technologies for the smart grid.

Technology	Standard/protocol	Max. theoretical data rate	Coverage range	Network		
				HAN/BAN/IAN	NAN/FAN	WAN
Wired communication technologies						
Fiber optic	PON	155 Mbps–2.5 Gbps	Up to 60 km			X
	WDM	40 Gbps	Up to 100 km			
	SONET/SDH	10 Gbps	Up to 100 km			
DSL	ADSL	1–8 Mbps	Up to 5 km		X	
	HDSL	2 Mbps	Up to 3.6 km			
	VDSL	15–100 Mbps	Up to 1.5 km			
Coaxial Cable	DOCSIS	172 Mbps	Up to 28 km		X	
PLC	HomePlug	14–200 Mbps	Up to 200 m	X		
	Narrowband	10–500 kbps	Up to 3 km		X	
Ethernet	802.3x	10 Mbps–10 Gbps	Up to 100 m	X	X	
Wireless communication technologies						
Z-Wave	Z-Wave	40 kbps	Up to 30 m	X		
Bluetooth	802.15.1	721 kbps	Up to 100 m	X		
ZigBee	ZigBee	250 kbps	Up to 100 m	X	X	
	ZigBee Pro	250 kbps	Up to 1600 m			
WiFi	802.11x	2–600 Mbps	Up to 100 m	X	X	
WiMAX	802.16	75 Mbps	Up to 50 km		X	X
Wireless Mesh	Various (e.g., RF mesh, 802.11, 802.15, 802.16)	Depending on selected protocols	Depending on deployment	X	X	
Cellular	2G	14.4 kbps	Up to 50 km		X	X
	2.5G	144 kbps				
	3G	2 Mbps				
	3.5G	14 Mbps				
	4G	100 Mbps				
Satellite	Satellite Internet	1 Mbps	100–6000 km			X

Murat Kuzlu, Manisa Pipattanasomporn, Saifur Rahman, Communication network requirements for major smart grid applications in HAN, NAN and WAN, Computer Networks, Volume 67, 2014, Pages 74-88, ISSN 1389-1286.

Network Design Process

- Networking requirements for the Smart Grid network differ in many critical respects from the networking requirements of NSPs:
  - NSP networks are primarily designed to support their customers' multimedia applications (including VoIP).
  - Smart Grid networks support mission-critical applications such as SCADA, teleprotection, and synchrophasors that have significantly more stringent requirements on reliability, security, and performance.
- Leads to different network design methods.

- MPLS infrastructure should be integrated in the network design process:
  - Implemented mainly at WAN level.
  - Provides traffic engineering and QoS support.

Network Design Process

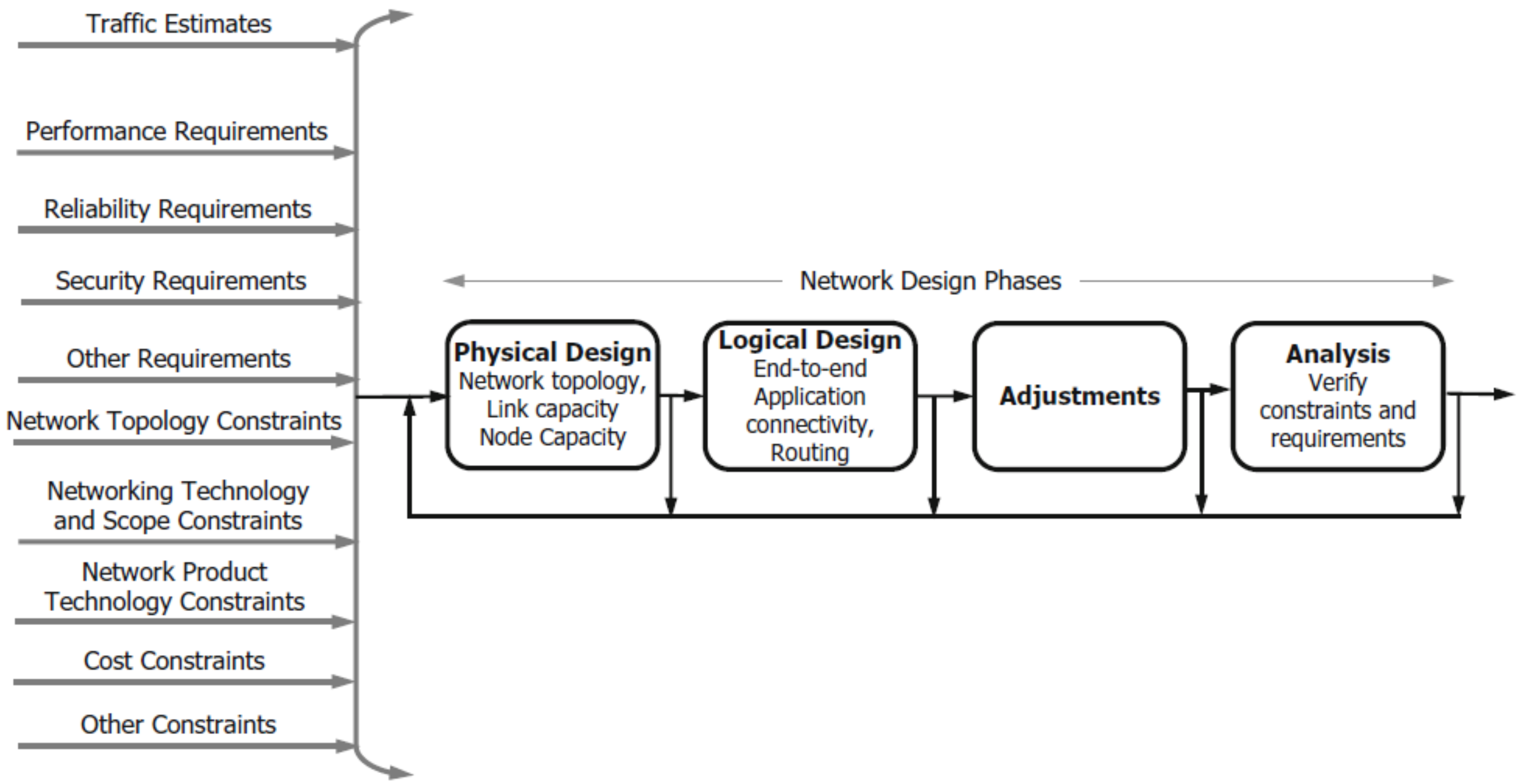


Fig. 7.1 Network design process – an overview

Estimating Network Traffic

- Computation of network traffic estimates:
  - Estimate the traffic matrix, i.e., traffic estimates between any pair of endpoints i and j:
    - d_{ij}
    - d_{ji}
  - Compute the data rate required in each link.
    - Depends on demand and routing.
    - Must account for link and node failures (redundancy).
      - Rerouted traffic must be estimated and added to nominal link traffic.
  - QoS requirements may help reduce required link capacities.
    - Traffic prioritization required when link capacity lower than peak demand.

Smart Grid Traffic Characterization

- Some specific SG traffic characteristics must be taken into account:

1. Traffic volume generated by most Smart Grid applications is small.

2. In most SG operations applications, traffic is asymmetric: traffic from the data center servers (e.g., from the SCADA and DA master control, WASA&C server, and MDMS) to the remote endpoints (to SCADA and DA IEDs, PMUs, and meters) is significantly less than the traffic from these remote endpoints.

3. For some applications, there may be additional requirements for traffic that must be carried during “critical” conditions, e.g.: power outage, security incident, etc.
   - For network design, greater between “normal” and “critical” traffic of each application should be considered.

Smart Grid Traffic Characterization

- Most traffic in the SG can be regarded as sensor **measurements** and **status** towards control and management system.
    - In some applications, sensors are polled.
    - In some applications, data is acknowledged.
    - In some applications, measurements are periodic (status can be piggybacked).
    - Some applications generate asynchronous traffic related with events (e.g., alarms): usually low average data rate, may have high peak data rate, requires high priority.

- Additional traffic required by SG operations (usually much smaller frequency, low average data rate, lager packets):
    - Protocol control messages (e.g., routing, network management, etc.);
    - Software and firmware upgrades;
    - File transfer of large reports;
    - Archiving.

Smart Grid Traffic Characterization

- Protocol header overheads must be taken into account in traffic estimates, e.g.:
  - Transport: TCP (20-28 bytes) or UDP (8 bytes)
  - Network: IPv4 (20 bytes) or IPv6 (40 bytes)
  - MPLS: 4 bytes
  - Data Link: PPP (6 bytes), or Frame Relay (4 bytes), or Ethernet (20 bytes)
  - PHY: varies widely with technology/protocol (e.g., 7 bytes for Ethernet)

Smart Grid Traffic Characterization

- Example:
  - Synchrophasor with 6 phasors (three voltages and three currents of 3-phase system):
    - Application: 3 bytes
    - UDP: 8 bytes
    - IPv4: 20 bytes
    - MPLS: 4 bytes
    - Ethernet DL: 20 bytes
    - Ethernet PHY: 7 bytes
    - A PMU message: 60 measurements per second
    - Throughput = (3+8+20+4+20+7) * 8 * 60 = 29760 bit/s

A Case Study: Smart Grid Bandwidth Requirement in an LTE Macrocell

- **Objective:** to determine total Smart Grid traffic that may need to be supported in an utility-owned LTE macrocell / eNB.
- **Worst case, but reasonable**, assumptions are made about the number of Smart Grid elements and the traffic requirements for each type of element.
- Total traffic that must be supported can be estimated.
- Current Smart Grid applications as well as those that may be deployed in the next several years are considered.

A Case Study: Smart Grid Bandwidth Requirement in an LTE Macrocell

A Communication Network Architecture for the Smart Grid

Network Design Process

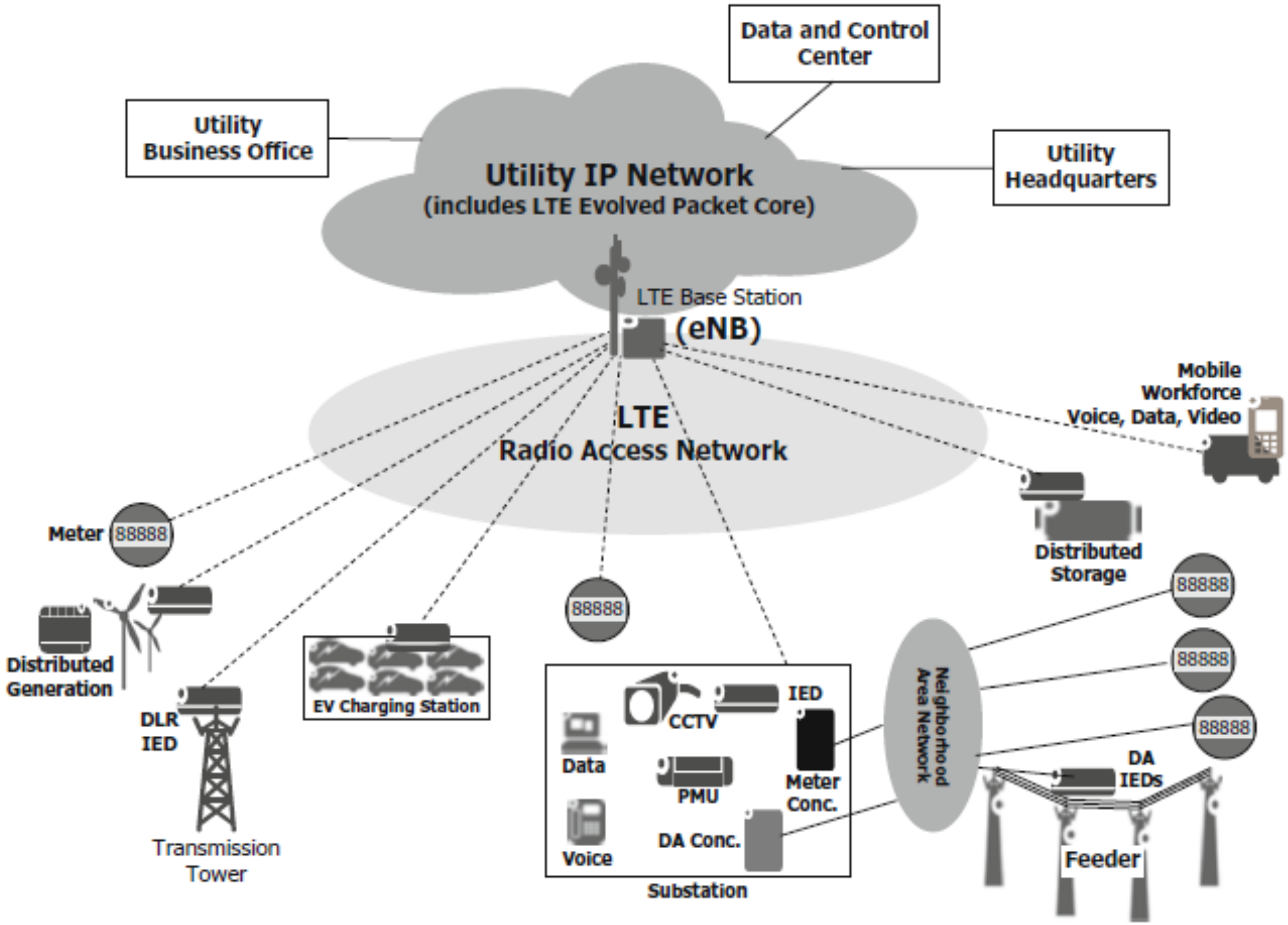


Fig. 7.2 Reference architecture for Smart Grid application endpoints in an LTE macrocell

A Case Study: Smart Grid Bandwidth Requirement in an LTE Macrocell

- Assumptions:
  1. Smart Grid elements deployed at substations, transmission lines, distribution feeders, DG sources, DS sites, and customer locations use LTE to support wide area IP connectivity. Same for MWF.
  2. For AMI, meters may be connected through meter data concentrator(s) at substation(s) over RF mesh NANs, or they may connect directly to the eNB, or both.
  3. DA IEDs are connected through DA data concentrator(s) at substation(s) over NANs.
  4. One or more PMUs are deployed at each transmission substation.
  5. Some transmission towers deployed in the cell may carry Dynamic Line Rating IEDs.
  6. IEDs at each DG and DS (and EV charging station) location are assumed to have the same traffic characteristics.
  7. For business voice and data, utility personnel in only the MWF and substation locations are considered.
  8. Only the uplink traffic is estimated, since uplink traffic (SG endpoint to ENB) is expected to be significantly more than downlink traffic.
  9. Traffic for both normal and critical operations conditions is computed.
  10. The substation corresponds in Europe to the secondary substation (MV/LV).
  11. All traffic in the LTE RAN is considered IP.

A Case Study: Smart Grid Bandwidth Requirement in an LTE Macrocell

- Considered scenario demographics:

Demographic type	Population density (per sq. km)	Coverage area of the LTE cell (sq. km)	Population in the macrocell coverage
Dense urban	29000	1,85	53760
Urban	14000	2,15	30100
Suburban	1900	11,70	22240
Rural	400	76,90	30760

A Case Study: Smart Grid Bandwidth Requirement in an LTE Macrocell

A Communication Network Architecture for the Smart Grid

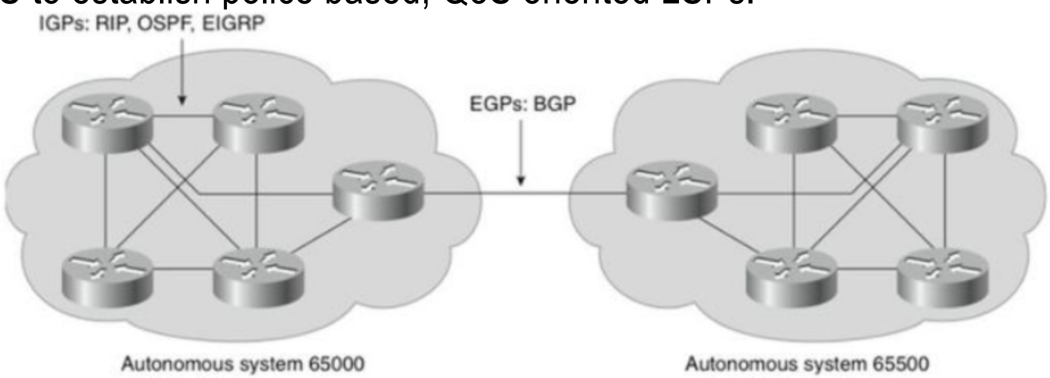
Network Design Process

Table 7.2 Summary of the data rate estimates in an LTE macrocell in 700 MHz spectrum

	Minimum required data rates (worst case) in kbps									
	Dense urban with AMI data concentrators		Dense urban *without* AMI data concentrators		Urban with AMI data concentrators		Suburban with AMI data concentrators		Rural *without* AMI data concentrators	
Application	Normal	Critical	Normal	Critical	Normal	Critical	Normal	Critical	Normal	Critical
SCADA and DA	165	138	165	138	95	79	140	116	236	197
DG, DS	80	67	80	67	97	80	129	107	161	134
Synchrophasors	213	178	213	178	213	178	213	178	426	355
AMI	165	165	210	279	83	83	83	83	120	160
CCTV	826	1,238	826	1,238	826	1,238	826	1,238	1,651	2,064
Mobile workforce push-to-talk voice	16	161	16	161	16	129	16	81	16	81
Mobile workforce live video	0	550	0	550	0	550	0	550	0	550
Person-to-person voice (MWF and substation personnel)	113	435	113	435	113	371	97	274	97	274
Business data (MWF and substation personnel)	124	554	124	554	124	459	96	287	105	296
Dynamic line rating	0	0	0	0	0	0	3	3	8	7
Total data rate	**1,703**	**3,487**	**1,747**	**3,601**	**1,566**	**3,167**	**1,601**	**2,917**	**2,820**	**4,118**
Total data only	748	1,102	793	1,216	612	879	663	773	1,056	1,149
Total video only	826	1,789	826	1,789	826	1,789	826	1,789	1,651	2,614
Total voice only	129	597	129	597	129	500	113	355	113	355

Routing Protocols

- Routing allows incoming traffic at the router to be dynamically routed to the destination over the optimal path.
- Routing protocols:
  - **Interior Gateway Protocols**
    - More relevant at Smart Grid level.
    - E.g., OSPF, IS-IS, RIP, EIGRP, etc.
  - Exterior Gateway Protocols
    - E.g., BGP
- Calculate optimal routes based on defined objective functions, e.g., hop distance, end-to-end delay, reliability (e.g. move from disrupted DCC to backup DCC).
- Results from the IGPs can be used to establish MPLS LSPs.
- RSVP-TE allows MPLS to establish police based, QoS oriented LSPs.



Network Performance and QoS Design

- Delay Requirements
  - Each application has its own requirement on the overall delay that can be tolerated from the time an event occurs to the time it's processing is finished (e.g., fault recovery), e.g.:
    - Teleprotection applications: delays between transmission line fault detection and the circuit breaker tripped must be lower than a few milliseconds.
    - Synchrophasor measurement delays a bit higher, but still low.
    - SCADA measurements require delays lower than hundred milliseconds.
    - Consumer meter measurements may tolerate delays of many seconds.

Delay and Priority Requirements

Table 7.3 Delay and priority requirements for Smart Grid applications

Application function	Delay allowance (minimum) ms	Priority 0 – max 100 – min	Application type
Delay ≤ 10 ms			
(High-speed) protection information	8, 10	2	Teleprotection (for 60 Hz, 50 Hz)
Load shedding for underfrequency	10	20	SCADA
10 ms < delay ≤ 20 ms			
Breaker reclosers	16	15	Teleprotection
Lockout functions	16	12	Teleprotection
Many transformer protection and control applications	16	12	Teleprotection
PMU measurements+status (class A) if used for protection function	20	12	Synchrophasors
20 ms < delay ≤ 100 ms			
PMU measurements+status (class A) for other than protection	60	10	Synchrophasors
SCADA periodic measurement+status, events, control	100	25	SCADA

Delay and Priority Requirements

Table 7.3 Delay and priority requirements for Smart Grid applications

Application function	Delay allowance (minimum) ms	Priority 0 – max 100 – min	Application type
DA periodic measurement+status, events, control	100	26	Distribution automation
DG/DS measurement+status, events, control	100	27	Distributed generation/ distributed storage
PTT signaling – critical	100	30	
PMU clock synchronization	100	20	Synchrophasors
100 ms < delay ≤ 250 ms			
VoIP bearer (including for PTT)	175	50	MWF, business voice
VoIP signaling (person-to-person)	200	60	Business voice
DLR measurements, status, events, control	200	28	Dynamic Line Rating
Real-time video (MWF)	200	55	MWF, CCTV
On demand CCTV video	200	55	CCTV
Critical grid operation data (e.g., DMS, TMS)	200	45	SCADA, DA, DG/DS, DLR, etc.
Critical business data	250	70	Business data
DMS and TMS applications (other than included above)	250	65	SCADA

TÉCNICO LISBOA

Delay and Priority Requirements

Table 7.3 (continued)

Application function	Delay allowance (minimum) ms	Priority 0 – max 100 – min	Application type
Noncritical operations data	500	80	SCADA, DA, DG/DS, DLR, etc.
Noncritical business data	500	80	Business data
1 s ≤ delay			
Image files	1,000	90	SCADA
Fault recorders	1,000	90	SCADA
(Medium-speed) Monitoring and control information	1,000	90	SCADA
(Low-speed) O and M information	1,000	90	SCADA
Fault isolation and service restoration	1,000	90	Protection
Distribution applications	1,000	90	Some distribution automation, some demand response
AMI – normal measurements+status, events, control	1,000	85	AMI
Text strings	1,000	90	SCADA
Audio and video data streams	1,000	78	SCADA
Fault recorders	1,000	90	SCADA
Best effort, default	2,000	100	Many

Per-Hop Behavior

A Communication Network Architecture for the Smart Grid

Network Design Process

- Bitrate is not enough to guarantee QoS:
  - Queueing delay of traffic mixes with different delay and criticality requirements.
  - High bandwidth links are expensive.
- Per-hop behavior of a router:
  - Priority enforcement at egress interface.
  - Packet discarding when queue is full (priority-based, may be probabilistic) .

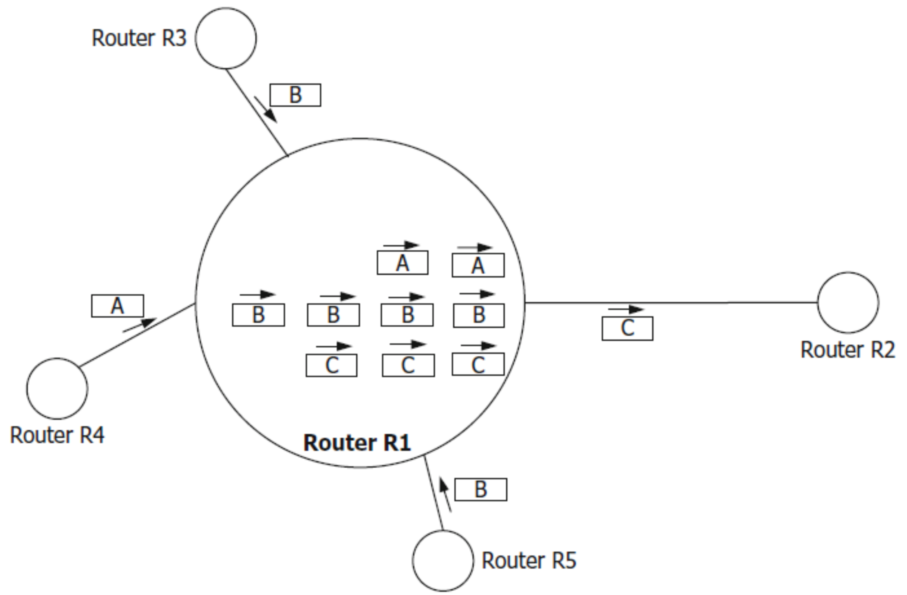


Fig. 7.3 Per-hop behavior

QoS Implementation in Current Data Networks

- Current IP data networks support a limited number of QoS classes:
  - Voice traffic (VoIP) assigned to higher priority QoS class.
  - For Smart Grid traffic, several applications must be aggregated in each class.
    - Aggregated applications may not have the very same requirements and criticality.
    - Support of delay-sensitive applications (e.g., protection) requires very high data rates.

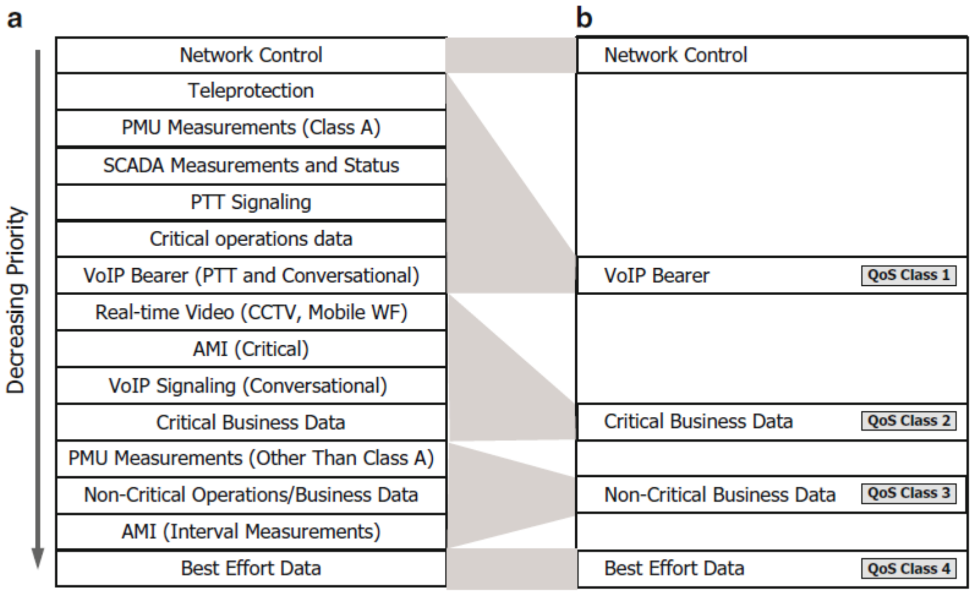
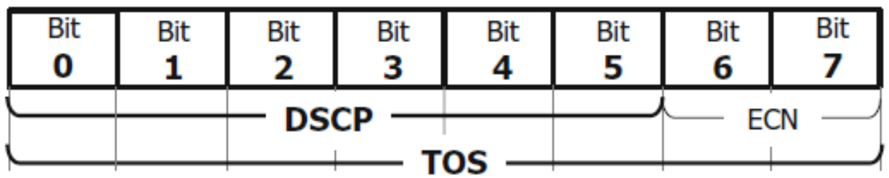


Fig. 7.4 An example of QoS implementation in Smart Grid network with just four QoS classes. (**a**) A few Smart Grid applications. (**b**) QoS classes in typical data network

QoS Classes and Differentiated Services

- Differentiated Services Code Points (DSCPs) defined in RFC 2474:
    - Encoded as first 6 bits of Type of Service (ToS) field in IP header.
    - Allows definition of 64 different QoS classes for IP traffic.
    - PHB defined for each configured QoS class.
    - Default DSCP value interpreted as best effort traffic.
- PHBs at each router set according to global QoS requirements.
- Some QoS classes already defined in standards:
    - Expedited Forwarding (EF) [RFC 3246]: highest priority applications such as VoIP.
    - Assured Forwarding (AF) [RFC 2597]: 12 QoS classes with different requirements on delay and packet loss.
    - Best Effort (BE): default.
- Unassigned DSCP codes may be needed in Smart Grids to support more QoS classes.

Fig. 7.5 DSCP field in the TOS byte of the IP packet header



QoS Classes and Differentiated Services

Table 7.4 Example DSCP for Smart Grid application functions

DSCP (Octal)	DSCP (bit 0–bit 5)	Example(s) of applications in this class including Smart Grid application functions	CS*n* (class selector *n*)
77	111 111		
76	111 110		
75	111 101		
74	111 100		
73	111 011		
72	111 010		
71	111 001		
70	111 000	**Network control (e.g., IP routing)**[a]	CS7
67	110 111	**Teleprotection**[a]	
66	110 110		
65	110 101		
64	110 100	**Synchrophasor measurements+status**[a]	
63	110 011		
62	110 010		
61	110 001		
60	110 000	Network control (e.g., IP routing)	CS6
57	101 111	**SCADA measurement+status, events, control**[a]	
56	101 110	**DA measurement+status, events, control**[a]	
55	101 101	**DG/DS measurement+status, events, control**[a]	
54	101 100	**PTT signaling – critical**[a]	
53	101 011	EF, VoIP bearer	
52	101 010		
51	101 001		

QoS Classes and Differentiated Services

A Communication Network Architecture for the Smart Grid

Network Design Process

Table 7.4 Example DSCP for Smart Grid application functions

DSCP (Octal)	DSCP (bit 0–bit 5)	Example(s) of applications in this class including Smart Grid application functions	CS*n* (class selector *n*)
50	101 000	Voice and video signaling (**including PTT signaling – normal**)	CS5
47	100 111	**DLR measurements+status, events, control**[a]	
46	100 110	AF43, interactive video, **on demand CCTV**[a]	
45	100 101		
44	100 100	AF42, interactive video	
43	100 011	**AMI – critical**[a]	
42	100 010	AF41, interactive video	
41	100 001		
40	100 000	Video conferencing, gaming	CS4
37	011 111		
36	011 110	AF33, critical apps, streaming	
35	011 101		
34	011 100	AF32, critical apps, streaming	
33	011 011		
32	011 010	AF31, critical apps, streaming, **CCTV stream – normal**[a]	

(continued)

QoS Classes and Differentiated Services

Table 7.4 (continued)

DSCP (Octal)	DSCP (bit 0–bit 5)	Example(s) of applications in this class including Smart Grid application functions	CS*n* (class selector *n*)
31	011 001		
30	011 000	Broadcast TV	CS3
27	010 111		
26	010 110	AF23, preferred (low-latency) data	
25	010 101	**AMI – priority**[a]	
24	010 100	AF22, preferred (low-latency) data	
23	010 011		
22	010 010	AF21, preferred (low-latency) data	
21	010 001		
20	010 000	OA&M	CS2
17	001 111		
16	001 110	AF13, other (store and forward) data	
15	001 101	**AMI – normal measurements+status, events, control**[a]	
14	001 100	AF12, other (store and forward) data	
13	001 011		
12	001 010	AF11, other (store and forward) data	
11	001 001		
10	001 000	Scavenger, no BW assurance	CS1
07	000 111	**Low-priority Smart Grid operation data**[a]	
06	000 110		
05	000 101		
04	000 100		
03	000 011		
02	000 010		
01	000 001		
00	000 000	BE, best effort, default	CS0

[a]**Possible DSCP values for some of the Smart Grid applications (in bold font)** – values not already proposed or assigned in standards and other documents

Multiprotocol Label Switching (MPLS)

- Convergence between datagrams and virtual circuits.
- Datagrams follow pre-established path as in a virtual circuit.
- Provider (P) routers aka Label Switching Routers (LSRs) forward datagrams based on **labels**:
  - A **label** is a short number that identifies the flow.
- Endpoints are Customer Edge (CE) routers.
- Provider Edge (PE) routers aka Label Edge Routers (LERs) interface with CE routers:
  - The traffic received from CEs is policed at ingress PE routers.
- Each P and PE router keeps a label switching table, which associates each configured label with the output port, leading to the next P or PE router.
- A path between CE routers passing through PE and P routers is called Label-Switched Path (LSP)

Multiprotocol Label Switching (MPLS)

A Communication Network Architecture for the Smart Grid

Network Design Process

- LSPs is formed by populating the label switching tables:
  - Label Distribution Protocol (LDP), based on routing table info (no QoS).
  - Resource Reservation Protocol (RSVP), for explicit QoS reservation with Traffic Engineering (TE).

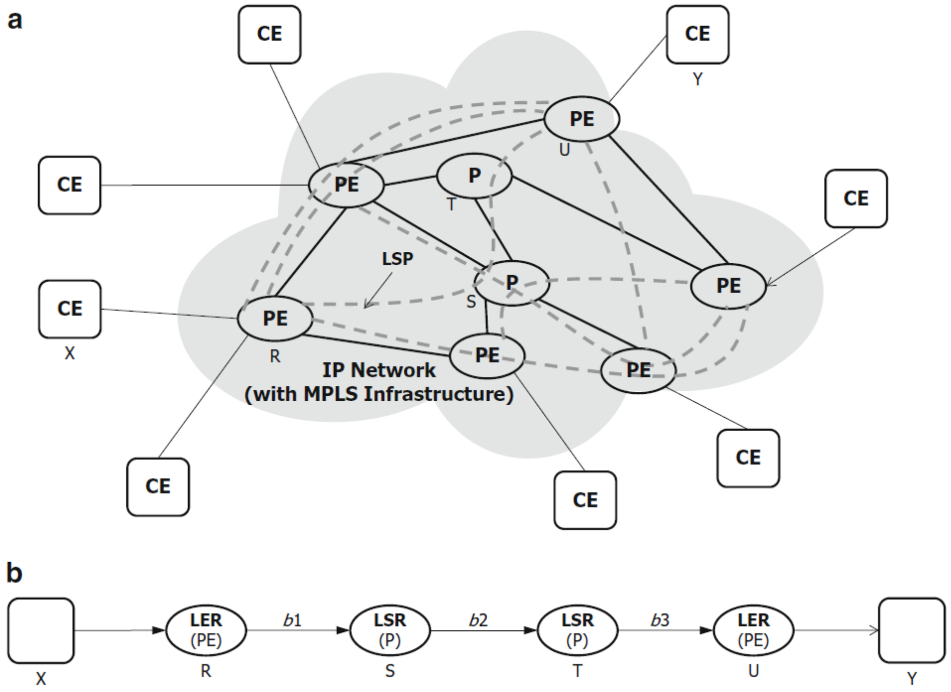


Fig. 3.12 Label-switched path. (**a**) LSPs. (**b**) Label management

Multiprotocol Label Switching (MPLS)

- MPLS header and label stacking:

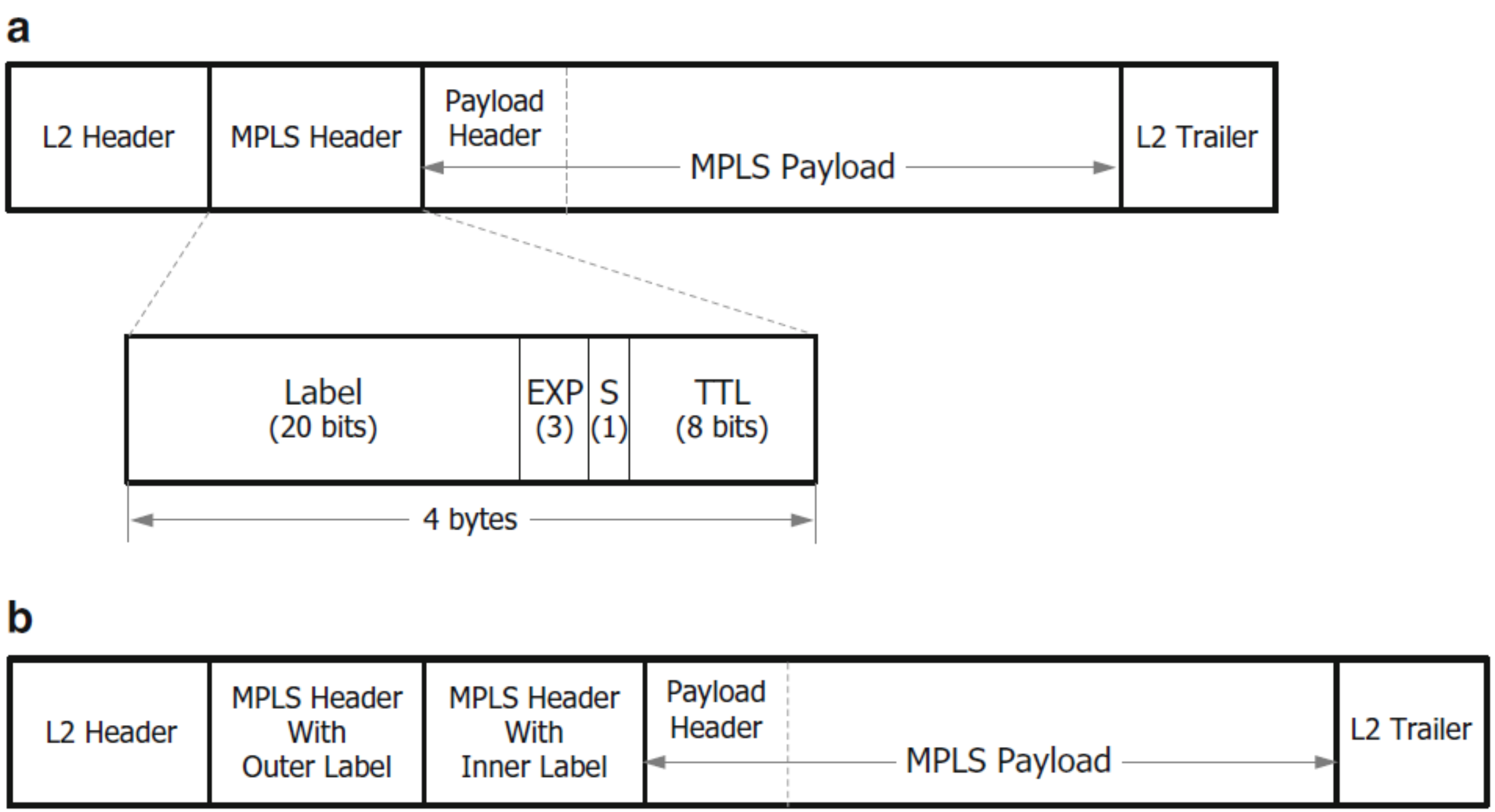
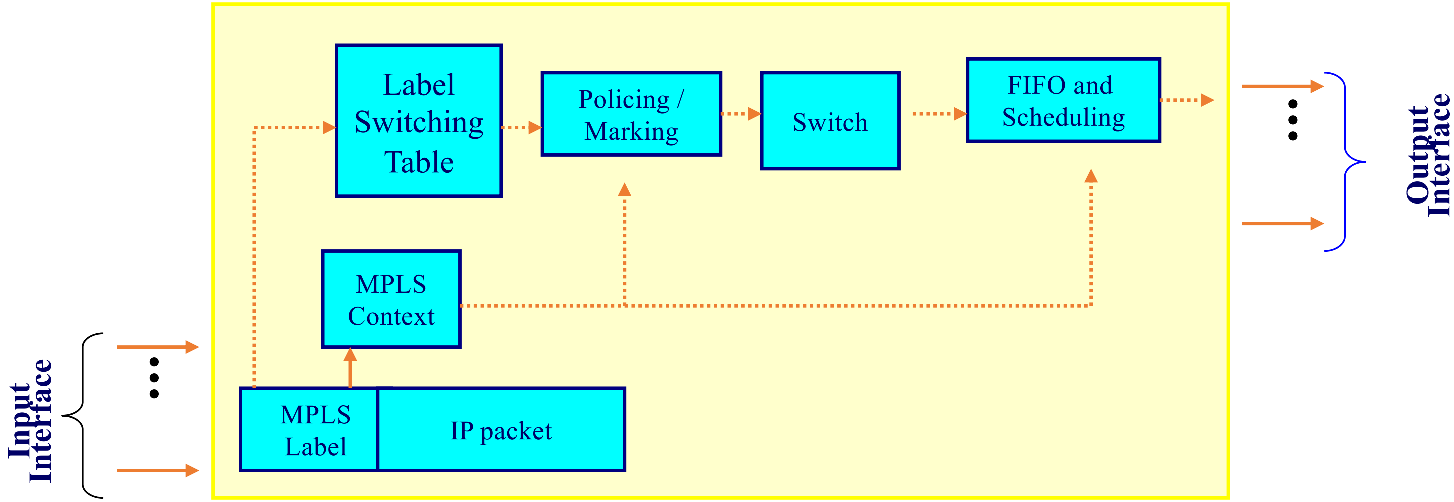


Fig. 3.13 MPLS headers. (**a**) MPLS header in a PDU. (**b**) Label stacking

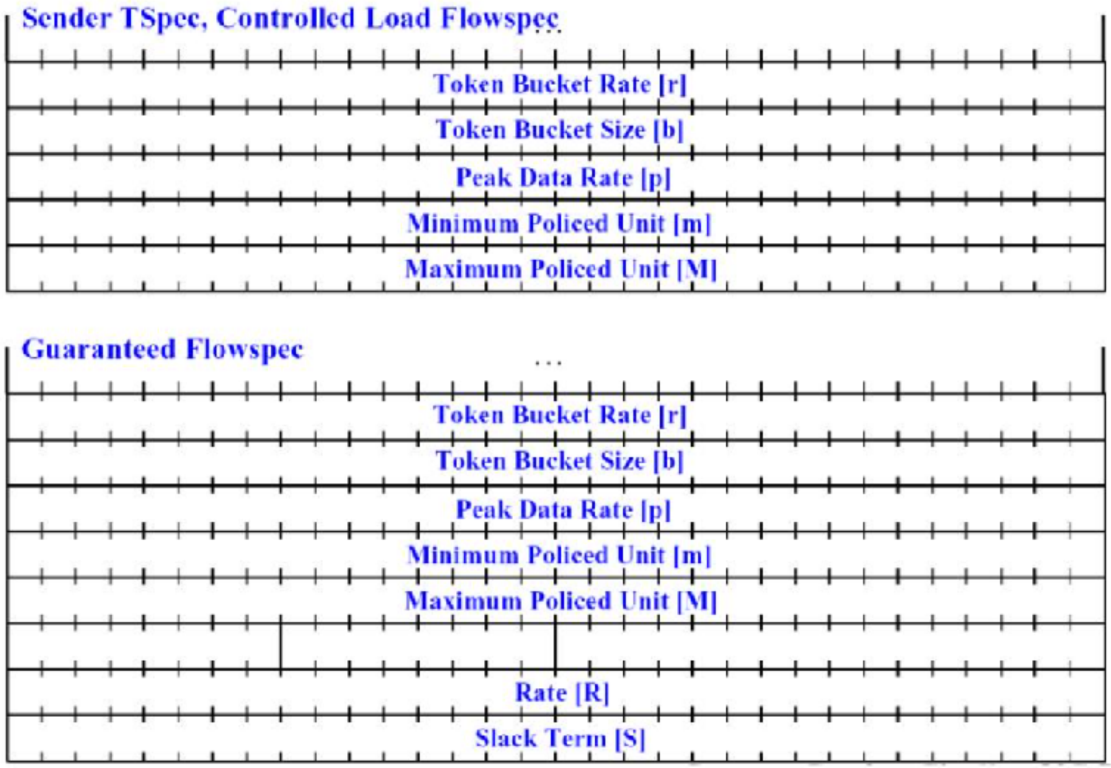
Multiprotocol Label Switching (MPLS)

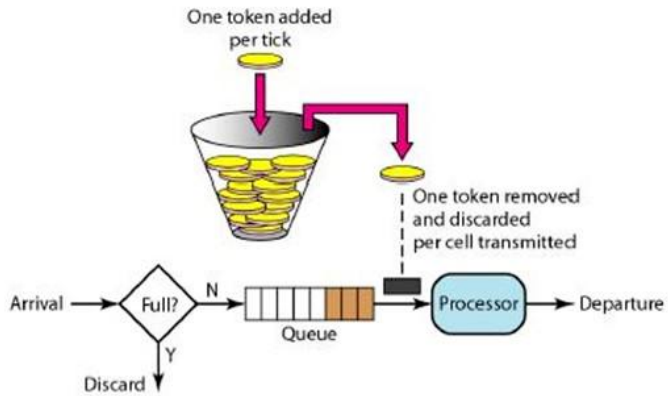
- Laber Switch Router (LSR) processing:



QoS with MPLS

- RSVP is the basis of the Integrated Services architecture:
  - Resources are reserved for a flow along the flow's path.
  - FLOWSPEC structures specify the resource reservation based on Token Bucket parameters.





QoS with MPLS

- IntServ reserves resources for each flow, DiffServ provides relative QoS treatment:
  - IntServ per-flow reservation gives more controlled QoS compared with DiffServ.
  - IntServ more expensive in terms of resources (aggregate QoS is simpler and cheaper).
- MPLS can integrate both when establishing LSPs:
  - Uses RSVP-TE to reserve resources for aggregate traffic in LSP.
  - Uses DiffServ PHB within each LSP.
- MPLS DiffServ implementation:
  - **E-LSP:** EXP field encoded as first 3 bits of TOS byte.
  - **L-LSP:** Label field used to provide label-specific PHB.
  - Can integrate both for finer granularity.

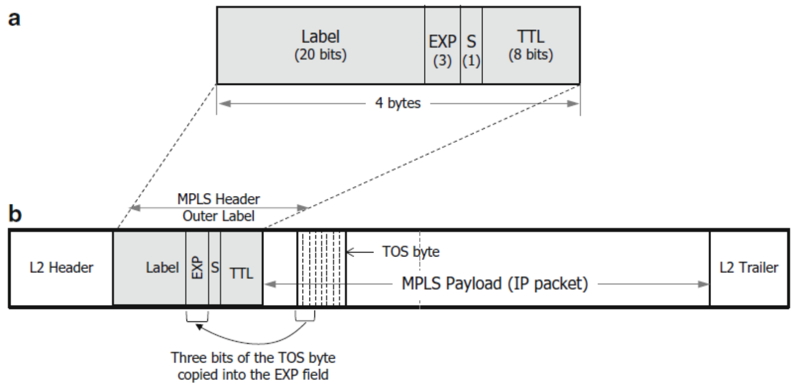


Fig. 7.6 MPLS header and diffServ QoS in MPLS with IP payload (an example). (**a**) MPLS label. (**b**) Mapping TOS in IP packet to EXP filed of the MPLS label

Network Reliability

- Network Availability: (probability of) availability of a network connection between endpoints. Depends on:
  - Mean Time Between Failure (MTBF): mean time between faulures of one component.
  - Failure in Thousand (FIT): Failure rate of a component.
  - Mean Time to Repair (MTTR): repair time, assuming that there is a failure.

- Network reliability can be improved by using redundancy:
  - Multiple physical paths as either parallel and separate links between adjacent network elements;
  - Two or more paths between two endpoints, each going over a separate set of intermediate network elements.

- Network redundancy mechanisms:
  - Link or Path Protection with SONET/SDH Rings;
  - Ethernet Link Aggregation;
  - Spanning Tree for Ethernet Network;
  - Routing Protocols;
  - MPLS Fast Reroute (FRR).

Network Reliability

- Reliable WAN:
  - At least two separate paths between every pair of WRs;
  - Connecting the CRs with each other directly (e.g., to support the delay requirement of less than 10 ms for teleprotection between substations);

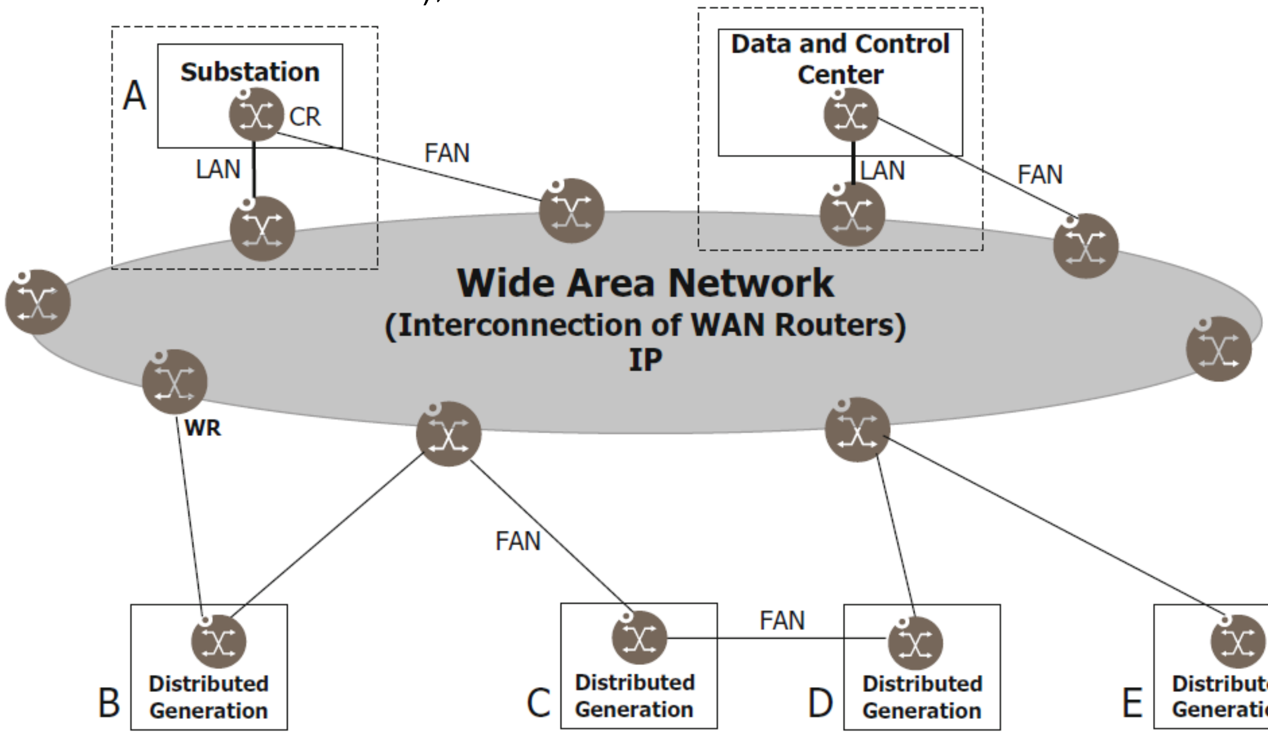


Fig. 7.7 Dual connections for reliability

Network Security

- Network Security elements:

  - Access Control Lists (ACLs) in routers:
    - Filter unwanted data traffic based on the IP headers in every packet entering the router.

  - Firewall (FW):
    - Integrated in routers or standalone. Monitors and controls incoming and outgoing network traffic based on predetermined security rules. Usually deployed at the border between trusted and untrusted network.

  - Intrusion Detection (IDS) and/or Intrusion Prevention (IPS) Systems: device or software application that monitors a network or systems for malicious activity or policy violations. IPSs are capable of performing countermeasures (e.g., reconfiguring a firewall, or changing the attack's content).

  - Unified Threat Management (UTM): integrates firewall, IDS and IPS.

Network Security

A Communication Network Architecture for the Smart Grid

Network Design Process

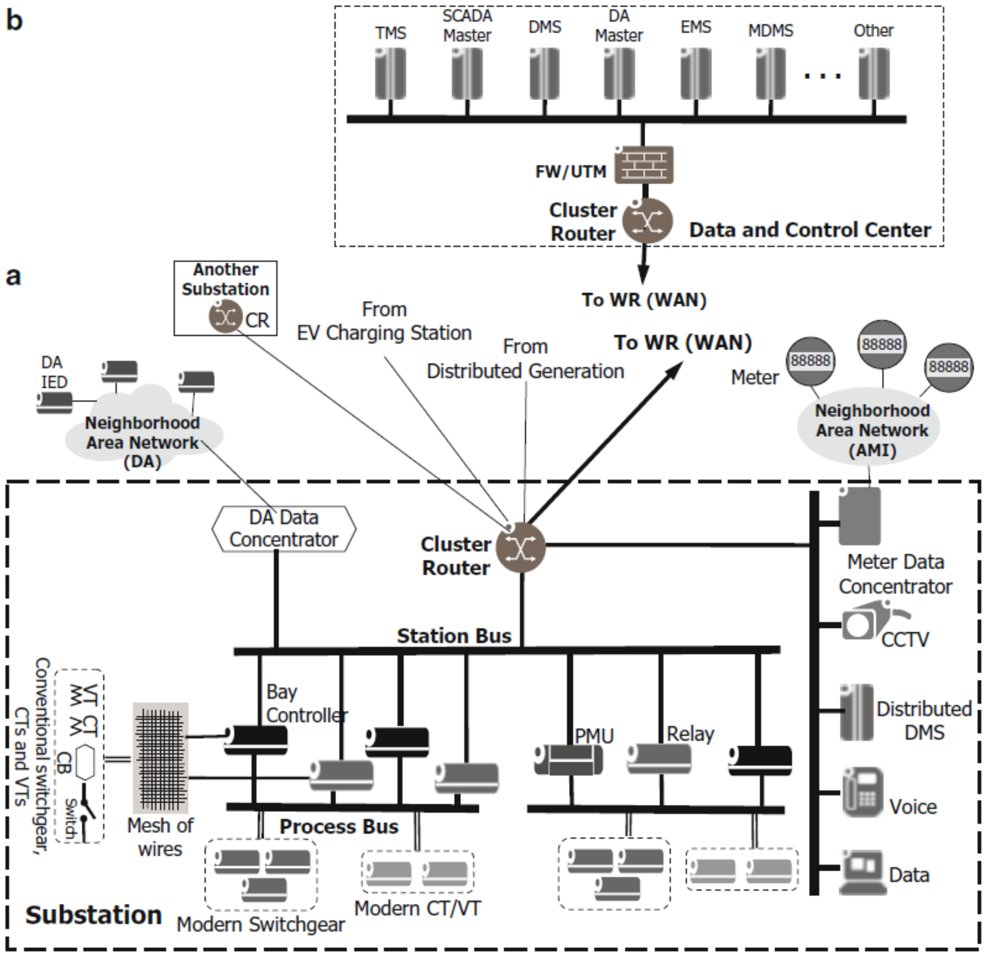


Fig. 7.8 Placement of firewall/UTM systems. (a) FW/UTM at substations. (b) FW/UTM at DCC