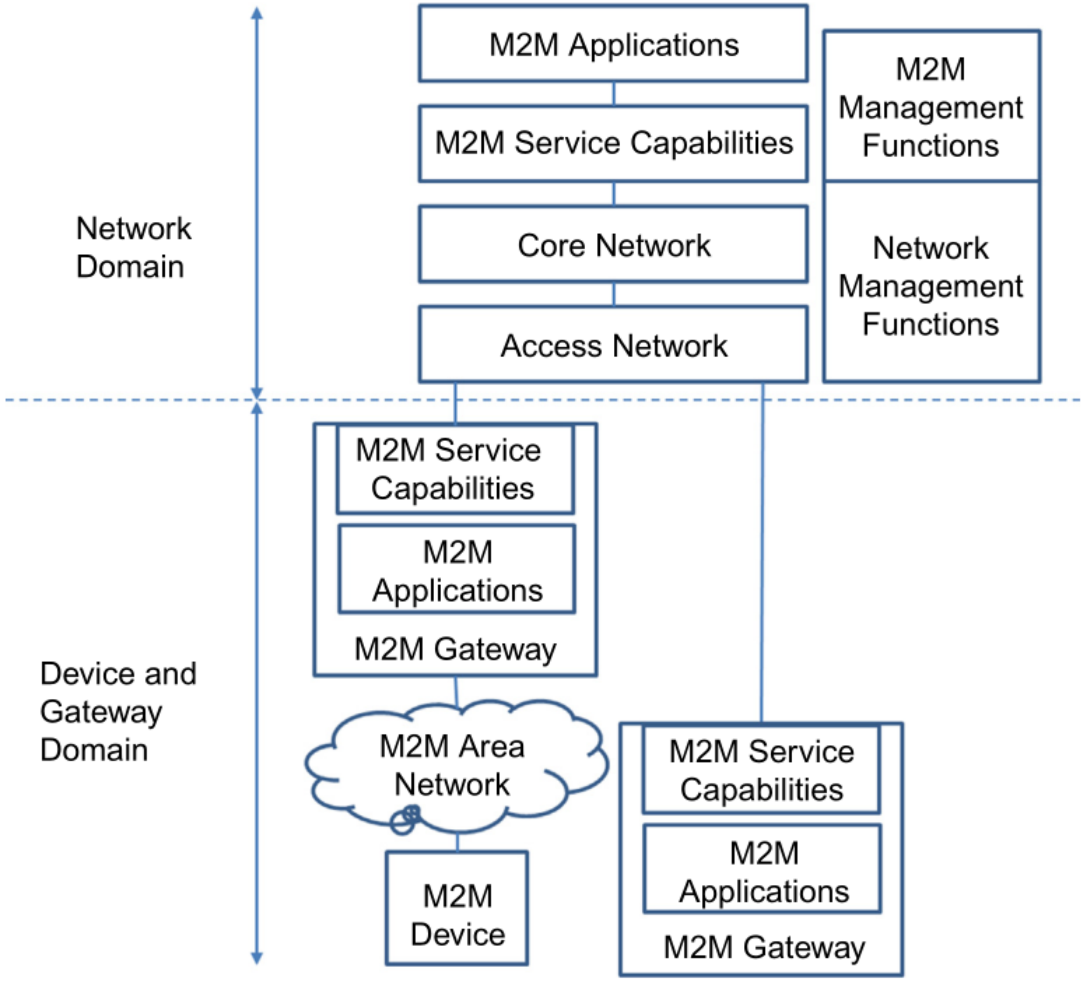
Unit 4 Review

IoT Architecture – State of the Art

- Introduction
- European Telecommunications Standards Institute
- International Telecommunication Union
- Internet Engineering Task Force architecture fragments

ETSI M2M high-level architecture



ETSI M2M High-Level Architecture.

ETSI M2M high-level architecture

- Figure shows the high-level ETSI M2M architecture.
- This high-level architecture is a combination of both a functional and topological view showing some functional groups (FG) clearly associated with pieces of physical infrastructure (e.g. M2M Devices, Gateways) while other functional groups lack specific topological placement.
- There are two main domains, a network domain and a device and gateway domain.
- The boundary between these conceptually separated domains is the topological border between the physical devices and gateways and the physical communication infrastructure (Access network).

The Device and Gateway Domain

- The Device and Gateway Domain contains the following functional/topological entities:
- **M2M Device:** This is the device of interest for an M2M scenario, for example, a device with a temperature sensor. An M2M Device contains M2M Applications and M2M Service Capabilities.
- An M2M device connects to the Network Domain either directly or through an M2M Gateway:
- ***Direct connection:*** The M2M Device is capable of performing registration, authentication, authorization, management, and provisioning to the Network Domain. Direct connection also means that the M2M device contains the appropriate physical layer to be able to communicate with the Access Network.
- ***Through one or more M2M Gateway:*** This is the case when the M2M device does not have the appropriate physical layer, compatible with the Access Network technology, and therefore it needs a network domain proxy.
- Moreover, a number of M2M devices may form their own local M2M Area Network that typically employs a different networking technology from the Access Network.
- The M2M Gateway acts as a proxy for the Network Domain and performs the procedures of authentication, authorization, management, and provisioning. An M2M Device could connect through multiple M2M Gateways.

The Device and Gateway Domain

- **M2M Area Network:** This is typically a local area network (LAN) or a Personal Area Network (PAN) and provides connectivity between M2M Devices and M2M Gateways.
- Typical networking technologies are IEEE 802.15.1 (Bluetooth), IEEE 802.15.4 (ZigBee, IETF 6LoWPAN/ROLL/CoRE), MBUS, KNX (wired or wireless) PLC, etc.
- **M2M Gateway:** The device that provides connectivity for M2M Devices in an M2M Area Network towards the Network Domain.
- The M2M Gateway contains M2M Applications and M2M Service Capabilities.
- The M2M Gateway may also provide services to other legacy devices that are not visible to the Network Domain.

The Network Domain

- The Network Domain contains the following functional/topological entities:
- **Access Network:** this is the network that allows the devices in the Device and Gateway Domain to communicate with the Core Network.
- Example Access Network Technologies are fixed (xDSL, HFC) and wireless (Satellite, GERAN, UTRAN, E-UTRAN W-LAN, WiMAX).
- **Core Network:** Examples of Core Networks are 3GPP Core Network and ETSI TISPAN Core Network.
- It provides the following functions:
  - ❖ IP connectivity.
  - ❖ Service and Network control.
  - ❖ Interconnection with other networks.
  - ❖ Roaming.

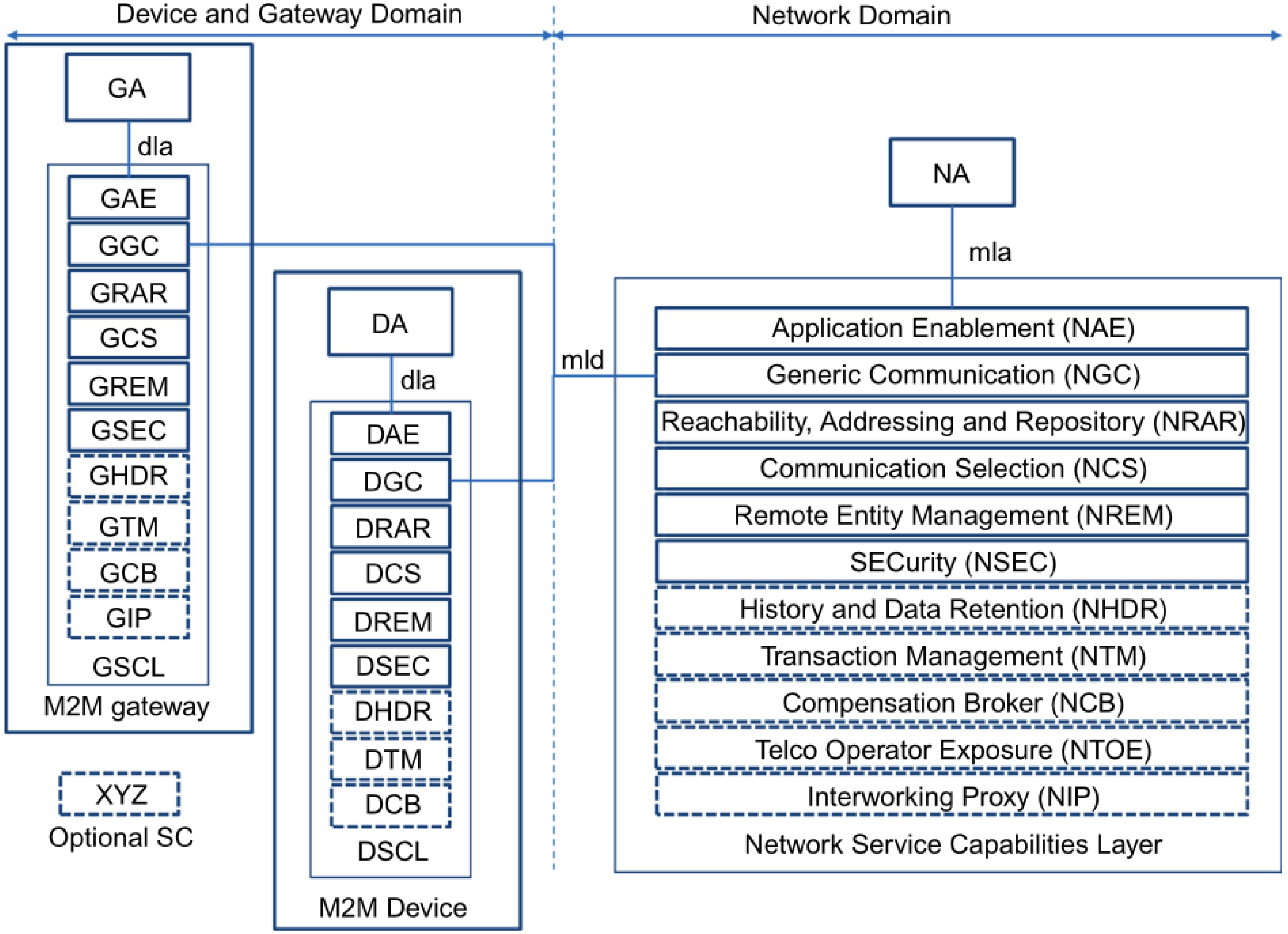
The Network Domain

- **M2M Service Capabilities:** These are functions exposed to different M2M Applications through a set of open interfaces.
- These functions use underlying Core Network functions, and their objective is to abstract the network functions for the sake of simpler applications.
- **M2M Applications:** These are the specific M2M applications (e.g. smart metering) that utilize the M2M Service Capabilities through the open interfaces.
- **Network Management Functions:** These are all the necessary functions to manage the Access and Core Network (e.g. Provisioning, Fault Management, etc.).

The Network Domain

- **M2M Management Functions:** These are the necessary functions required to manage the M2M Service Capabilities on the Network Domain while the management of an M2M Device or Gateway is performed by specific M2M Service Capabilities.
- There are two M2M Management functions:
- **M2M Service Bootstrap Function (MSBF):** The MSBF facilitates the bootstrapping of permanent M2M service layer security credentials in the M2M Device or Gateway and the M2M Service Capabilities in the Network Domain.
- In the Network Service Capabilities Layer, the Bootstrap procedures perform, among other procedures, provisioning of an M2M Root Key (secret key) to the M2M Device or Gateway and the M2M Authentication Server (MAS).
- **M2M Authentication Server (MAS):** This is the safe execution environment where permanent security credentials such as the M2M Root Key are stored.
- Any security credentials established on the M2M Device or Gateway are stored in a secure environment such as a trusted platform module.

ETSI M2M service capabilities


Device and Gateway Domain
Network Domain
GA
dIa
GAE
GGC
GRAR
GCS
GREM
GSEC
GHDR
GTM
GCB
GIP
GSCL
M2M gateway
XYZ
Optional SC
DA
dIa
DAE
DGC
DRAR
DCS
DREM
DSEC
DHDR
DTM
DCB
DSCL
M2M Device
mId
NA
mIa
Application Enablement (NAE)
Generic Communication (NGC)
Reachability, Addressing and Repository (NRAR)
Communication Selection (NCS)
Remote Entity Management (NREM)
SECurity (NSEC)
History and Data Retention (NHDR)
Transaction Management (NTM)
Compensation Broker (NCB)
Telco Operator Exposure (NTOE)
Interworking Proxy (NIP)
Network Service Capabilities Layer

M2M Capabilities for different M2M Nodes.

- An M2M Application is the main application logic that uses the Service Capabilities to achieve the M2M system requirements.
- The application logic can be deployed on a Device (Device Application, DA), Gateway (Gateway Application, GA) or Network (Network Application, NA).
- The SCL is a collection of functions that are exposed through the open
- interfaces or reference points mIa, dIa, and mId (ETSI M2M TC 2013b).
- Because the main topological entities that SCL can deploy are the Device, Gateway, and Network Domain, there are three types of SCL: DSCL (Device Service Capabilities Layer), GSCL (Gateway Service Capabilities Layer), and NSCL (Network Service Capabilities Layer).
- SCL functions utilize underlying networking capabilities through technology-specific interfaces. For example, an NSCL using a 3GPP type of access network uses 3GPP communication services interfaces.

ETSI M2M service capabilities

- All the possible Service Capabilities (where "x" is N(etwork), G(ateway), and D(evice)) are shown in Figure

1. Application Enablement (xAE).

- The xAE service capability is an application facing functionality and typically provides the implementation of the respective interface.
- In certain configurations xAE enables xAs to exchange messages to each other; for example, multiple Device Applications associated with the same M2M Gateway can exchange messages through the GAE.
- In certain configurations security operations such as authentication and authorization of applications is also performed by xAE.

ETSI M2M service capabilities

2.Generic Communication (xGC).

- The NGC is the single point of contact for communication towards the GSCL and DSCL.
- It provides transport session establishment and negotiation of security mechanisms, potentially secure transmission of messages, and reporting of errors such as transmission errors.
- The GSC/DSC is the single point of contact for communication with the NSCL, and they both perform similar operations to the NGC (e.g. secure message transmissions to NSCL).
- The GSC performs a few more functions such as relaying of messages to/from NSCL from/to other SCs in the GSCL, and handles name resolution for the requests within the M2M Area Network.

ETSI M2M service capabilities

3.**Reachability, Addressing, and Repository (xRAR).**

- This is one of the main service capabilities of the ETSI M2M architecture.
- The NRAR hosts mappings of M2M Device and Gateway names to reachability information (routable address information such as IP address and reachability status of the device such as up or down), and scheduling information relating to reachability, such as whether an M2M Device is reachable between 10 and 11 o'clock.
- It provides group management (creation/update/deletion) for groups of M2M Devices and Gateways, stores application (DA, GA, NA) data, and manages subscriptions to these data, stores registration information for NA, GSCL, and DSCL, and manages events (subscription notifications).
- The GRAR provides similar functionality to the NRAR, such as maintaining mappings of the names of M2M Devices or groups to reachability information (routable addresses, reachability status, and reachability scheduling), storing DA, GA, NSCL registration information, storing DA, GA, NA, GSCL, NSCL data and managing subscriptions about them, managing groups of M2M Devices, and managing events

ETSI M2M service capabilities

4. Communication Selection (xCS):

- This capability allows each xSCL to select the best possible communication network when there is more than one choice or when the current choice becomes unavailable due to communication errors.
- The NCS provides such a selection mechanism based on policies for reaching an M2M Device or Gateway, while the GCS/DCS provides a similar selection mechanism for reaching the NSCL.

5. Remote Entity Management (xREM).

- The NREM provides management capabilities such as Configuration Management (CM) for M2M Devices and Gateways (e.g. installs management objects in device and gateways), collects performance management (PM) and Fault Management (FM) data and provides them to NAs or M2M Management Functions, performs device management to M2M Devices and Gateways such as firmware and software (application, SCL software) updates, device configuration, and M2M Area Network configuration.
- The GREM acts as a management client for performing management operations to devices using the DREM and a remote proxy for NREM to perform management operations to M2M Devices in the M2M Area Network.
- Examples of proxy operations are mediation of NREM-initiated software updates, and handling management data flows from NREM to sleeping M2M Devices.
- The DREM provides the CM, PM, and FM counterpart on the device (e.g. start collecting radio link performance data) and provides the device-side software and firmware update support.

ETSI M2M service capabilities

6. SECurity (xSEC).

- These capabilities provide security mechanisms such as M2M Service Bootstrap, key management, mutual authentication, and key agreement (NSEC performs mutual authentication and key agreement while the GSEC and DESC initiate the procedures), and potential platform integrity mechanisms.

7. History and Data Retention (xHDR).

- The xHDR capabilities are optional capabilities, in other words, they are deployed when required by operator policies.
- These capabilities provide data retention support to other xSCL capabilities (which data to retain) as well as messages exchanged over the respective reference points.

8. Transaction Management (xTM).

- This set of capabilities is optional and provides support for atomic transactions of multiple operations.
- An atomic transaction involves three steps: (a) propagation of a request to a number of recipients, (b) collection of responses, and (c) commitment or roll back whether all the transactions successfully completed or not.

ETSI M2M service capabilities

9. Compensation Broker (xCB).

- This capability is optional and provides support for brokering M2M-related requests and compensation between a Customer and a Service Provider. In this context a Customer and a Service Provider is an M2M Application.

10. Telco Operator Exposure (NTOE).

- This is also an optional capability and provides exposure of the Core Network service offered by a Telecom Network Operator.

11. Interworking Proxy (xIP).

- This capability is an optional capability and provides mechanisms for connecting non-ETSI M2M Devices and Gateways to ETSI SCLs.
- NIP provides mechanisms for non-ETSI M2M Devices and Gateways to connect to NSCL while GIP provides the functionality for non-compliant M2M Devices to connect to GSCL via the reference point dIa, and the DIP provides the necessary mechanisms to connect non-compliant devices to DSCL via the dIa reference point.

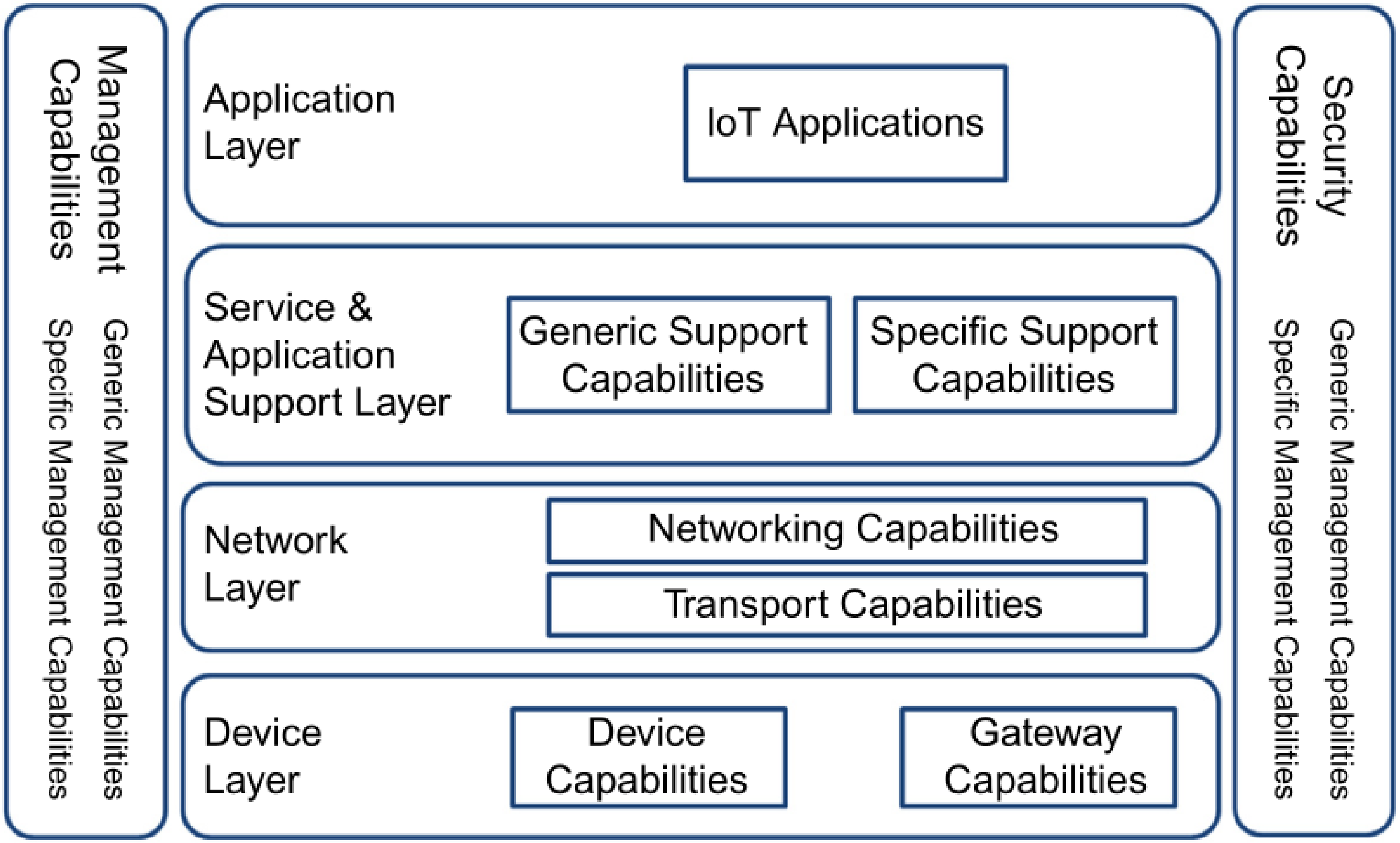
ETSI M2M interfaces

- The main interfaces mIa, dIa, and mId (ETSI M2M TC 2013b) can be briefly described as follows:
- **mIa:** This is the interface between a Network Application and the Network Service Capabilities Layer (NSCL).
- The procedures supported by this interface are (among others) registration of a Network Application to the NSCL, request to read/write information to NSCL, GSCL, or DSCL, request for device management actions (e.g. software updates), subscription and notification of specific events.
- **dIa:** This is the interface between a Device Application and (D/G)SCL or a Gateway Application and the GSCL.
- The procedures supported by this interface are (among others) registration of a Device/Gateway Application to the GSCL, registration of a Device Application to the DSCL, request to read/write information to NSCL, GSCL, or DSCL, subscription and notification of specific events.
- **mId:** This is the interface between the Network Service Capabilities Layer (NSCL) and the GSCL or the DSCL.
- The procedures supported by this interface are (among others) registration of a Device/Gateway SCL to the NSCL, request to read/write information to NSCL, GSCL, or DSCL, subscription and notification of specific events.

International Telecommunication Union – Telecommunication Sector View

- The ITU-T IoT domain model includes a set of physical devices that connect directly or through gateway devices to a communication network that allows them to exchange information with other devices, services, and applications.
- The physical world of things is reflected by an information world of virtual things that are digital representations of the physical things (not necessarily a one-to-one mapping because multiple virtual things can represent one physical thing).
- The devices in this model include mandatory communication capabilities and optional sensing, actuation, and processing capabilities in order to capture and transport information about the things.

ITU-T IoT Reference Model


Management Capabilities
Generic Management Capabilities
Specific Management Capabilities
Application Layer
IoT Applications
Service & Application Support Layer
Generic Support Capabilities
Specific Support Capabilities
Network Layer
Networking Capabilities
Transport Capabilities
Device Layer
Device Capabilities
Gateway Capabilities
Security Capabilities
Generic Management Capabilities
Specific Management Capabilities

ITU-T IoT Reference Model.

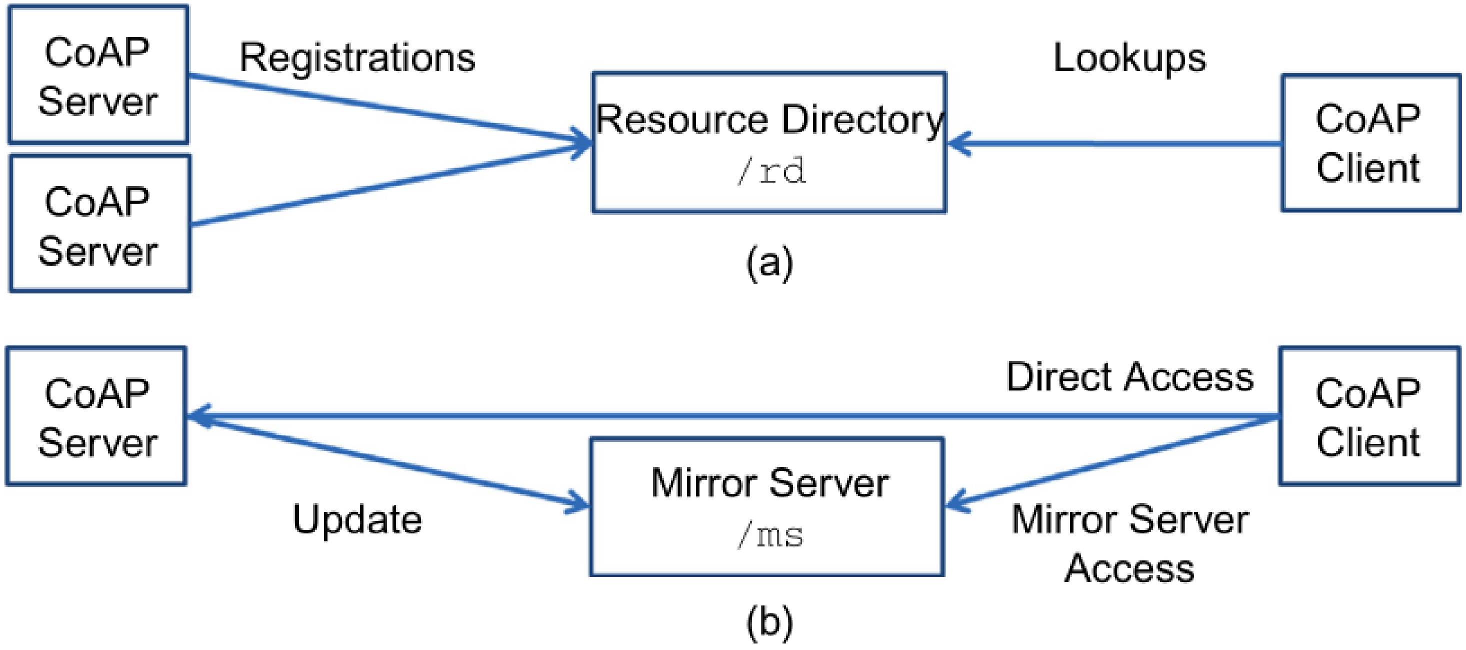
ITU-T IoT Reference Model

- Regarding the Service Capabilities, starting from the Application Layer the ITU-T IoT model considers this layer as the host of specific IoT applications (e.g. remote patient monitoring).
- The Service & Application Support Layer (otherwise known as Service Support and Application Support Layer) consists of generic service capabilities used by all IoT applications, such as data processing and data storage, and specific service capabilities tailored to specific application domains, such as e-health or telematics.
- The Network Layer provides networking capabilities such as Mobility Management, Authentication, Authorization, and Accounting (AAA), and Transport Capabilities such as connectivity for IoT service data.
- The Device Layer includes Device Capabilities and Gateway Capabilities. The Device Capabilities include, among others, the direct device interaction with the communication network and therefore the Network Layer Capabilities, the indirect interaction with the Network Layer Capabilities through Gateway Devices, any ad hoc networking capabilities, as well as low-power operation capabilities (e.g. capability to sleep and wakeup) that affect communications.

ITU-T IoT Reference Model

- The Gateway Device Capabilities include multiple protocol support and protocol conversion in order to bridge the Network Layer capabilities and the device communication capabilities.
- In terms of Management Capabilities, these include the typical FCAPS (Fault, Configuration, Accounting, provisioning, software updates, activation/deactivation), network topology management (e.g. for local and short range networks), and traffic management.
- Specific management functionality related to a specific application domain is also included among the Management Capabilities.
- With respect to the Security Capabilities, this layer represents a grouping of different Security Capabilities required by other layers. The capabilities are grouped generically, such as AAA and message integrity/confidentiality support, and specifically, such as ones that are tailored to the specific application, e.g. mobile payment.

Internet Engineering Task Force architecture fragments



IETF CoRE Functional Components: (a) Resource Directory, (b) Mirror Server.

IETF CoRE Functional Components

- The IETF CoRE working group has also produced a draft specification for a Resource Directory
- A Resource Directory is a CoAP server resource (/rd) that maintains a list of resources, their corresponding server contact information (e.g. IP addresses or fully qualified domain name, or FQDN), their type, interface, and other information similar to the information that the CoRE Link Format document specifies (Figure (a)).
- An RD plays the role for devices to publish the descriptions of the available resources and for CoAP clients to locate resources that satisfy certain criteria such as specific resource types (e.g. temperature sensor resource type).

IETF CoRE Functional Components

- While the Resource Directory is a rendezvous mechanism for CoAP Server resource descriptions, a Mirror Server (Vial 2012) is a rendezvous mechanism for CoAP Server resource presentations.
- A Mirror Server is a CoAP Server resource (/ms) that maintains a list of resources and their cached representations (Figure (b)).
- A CoAP Server registers its resources to the Mirror Server, and upon registration a new mirror server resource is created on the Mirror Server with a container (mirror representation) for the original server representation.
- The original CoAP Server updates the mirror representation either periodically or when the representation changes.
- A CoAP Client that retrieves the mirror representation receives the latest updated representation from the original CoAP Server.
- The Mirror Server is useful when the CoAP Server is not always available for direct access.
- An example of such a CoAP Server is one that resides on a real device whose communication capabilities are turned off in order to preserve energy, e.g. battery-powered radio devices whose radio and/or processor goes to sleep mode. Typically, a Mirror Server is hosted on a device or machine that is always available

Open Geospatial Consortium architecture

- The Open Geospatial Consortium (OGC 2013) is an international industry consortium of a few hundred companies, government agencies, and universities that develops publicly available standards that provide geographical information support to the Web, and wireless and location-based services.
- OGC includes, among other working groups, the Sensor Web Enablement (SWE) (OGC SWE 2013) domain working group, which develops standards for sensor system models (e.g. Sensor Model Language, or SensorML), sensor information models (Observations & Measurements, or O&M), and sensor services that follow the Service-Oriented Architecture (SOA) paradigm, as is the case for all OGC-standardized services.

Open Geospatial Consortium architecture

- The functionality that is targeted by OGC SWE includes:
- Discovery of sensor systems and observations that meet an application’s criteria.
- Discovery of a sensor’s capabilities and quality of measurements.
- Retrieval of real-time or time-series observations in standard encodings.
- Tasking of sensors to acquire observations.
- Subscription to, and publishing of, alerts to be issued by sensors or sensor services based upon certain criteria.

Open Geospatial Consortium architecture

- OGC SWE includes the following standards:
- **SensorML and Transducer Model Language (TML),** which include a model and an XML schema for describing sensor and actuator systems and processes; for example, a system that contains a temperature sensor measuring temperature in Celsius, which also involves a process for converting this measurement to a measurement with Fahrenheit units.
- **Observations and Measurements (O&M),** which is a model and an XML schema for describing the observations and measurements for a sensor (Observations and Measurements, O&M).

Open Geospatial Consortium architecture

- **SWE Common Data model** for describing low-level data models (e.g. serialization in XML) in the messages exchanged between OGC SWE functional entities.
- **Sensor Observation Service (SOS),** which is a service for requesting, filtering, and retrieving observations and sensor system information.
- This is the intermediary between a client and an observation repository or near real-time sensor channel.
- **Sensor Planning Service (SPS),** which is a service for applications requesting a user-defined sensor observations and measurements acquisition.
- This is the intermediary between the application and a sensor collection system.
- **PUCK,** which defines a protocol for retrieving sensor metadata for serial port (RS232) or Ethernet-enabled sensor devices.