universidade de aveiro

Gestão/Management

Management of Local and Global Networks

Concepts and Protocols

Why Networks and Systems Management?

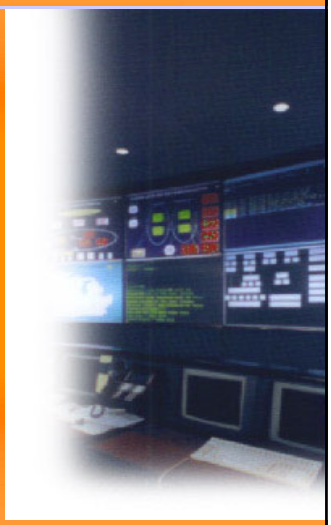
- Lower Cost – Manual management is costly
- More efficient – Automatic systems allow an efficient planning, and mechanisms to predict the utilization trends: lower errors and faster actuation
- Better service – The manager is informed at the same time the (client) is, and can make an automatic check of the situation
- Greater knowledge – more information exists about the network, allowing better decisions and planning
- Why not human intervention?
  - **Difficult to describe responsabilities**
  - **Technology rapidly evolves**
  - **Mangement systems rapidly evolve**
  - **Lack of technical resources**

universidade de aveiro

5

Commercial perspective

- Problems need to be quickly solved
- Management systems simplify the work of multi-functional networks (e.g. VoIP in multiple networks)
- Persons better used – they do not need to perform repetitive tasks
- Companies need to optimze their structures, and network management allow resources optimization

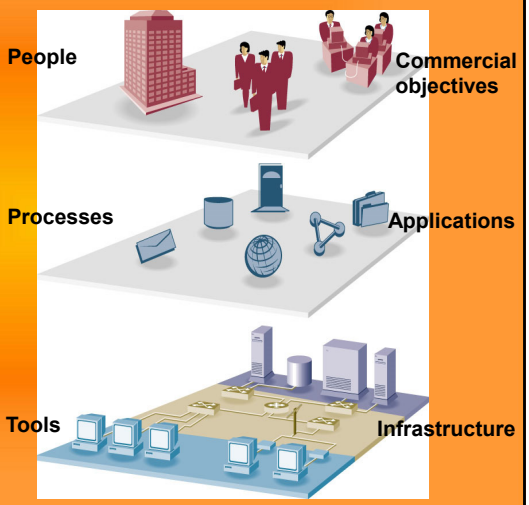


universidade de aveiro

6

Network management is:

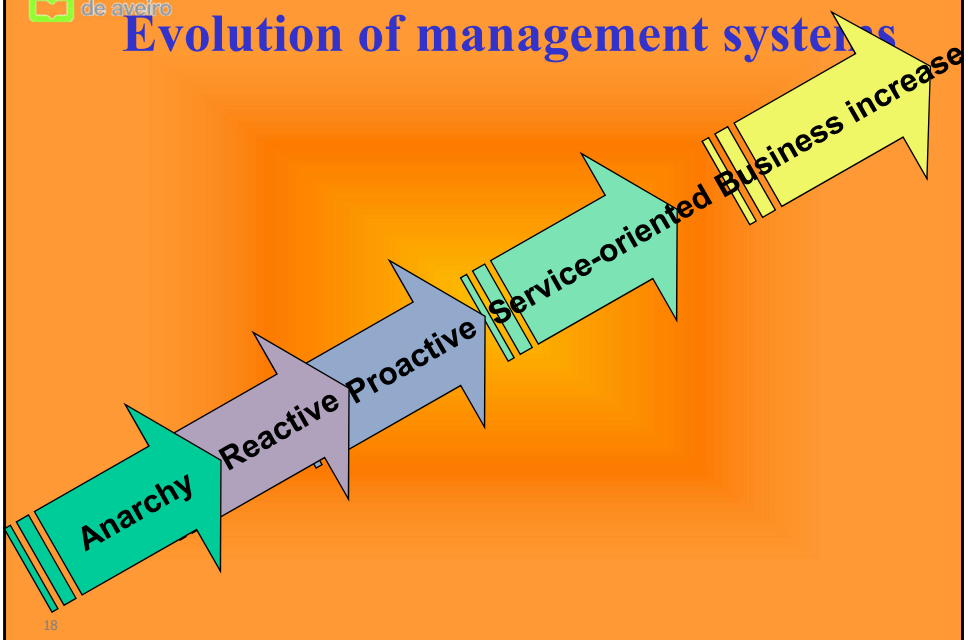
Implement, integrate and coordinate resources (HW, SW and people) to plan, operate, manage, analize, test, evaluate, design and expand the system to guarantee the service objectives (temporal, performance), with a reasonable cost and capacity.



universidade de aveiro

7

Evolution of management systems



18

universidade de aveiro

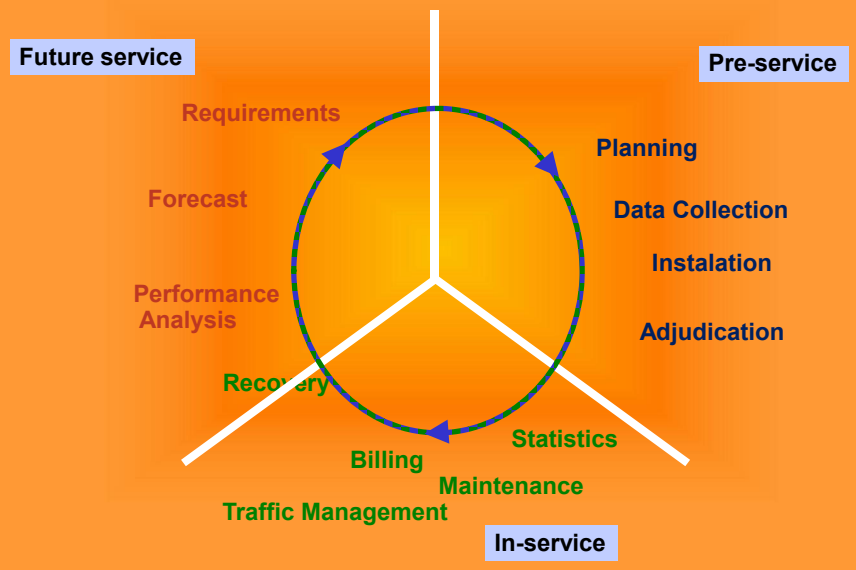
8

Aspects of Network Management

- **What to manage?**
  - Network, equipment, systems, users, services, applications
- **How to manage?**
  - Interfaces, actions, abstractions
- **What protocol(s) format(s)?**
  - Protocol abstraction, formats, messages
- **What information format(s)?**
  - Information type

Standards for all this – including global frameworks

Management Life Cycle



Management alternatives

- Systems management – Covers all company aspects
- Networks management – Covers mainly network aspects and communications systems and equipments

- Dedicated protocols – dedicated for networks
- Web based systems – resort to HTTP models, recently common

- Centralized models – Agent-manager model
- Distributed models – Share of the management responsabilities
- Hierarchical models – Hierarchic structure with centralized information in the root

Current structures very complex, with several operational models

universidade de aveiro

11

Management protocols

- **Methods to monitor and configure network equipments**
- **Do not describe how to achieve management objectives**

Simple protocols ⇒ common data and parameters formats allowing easy information transfer

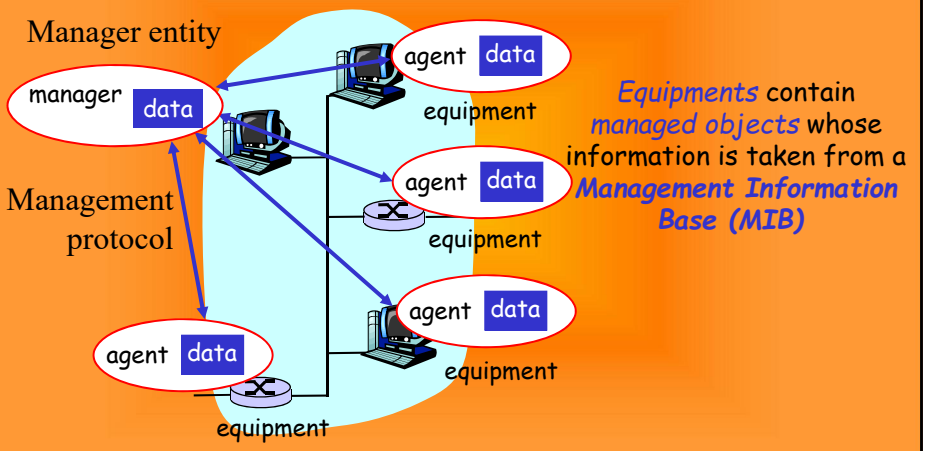
Complex protocols ⇒ add flexibility and security capacity

Advanced protocols ⇒ remotely execute network management tasks, without depending on specific protocol layers

universidade de aveiro

12

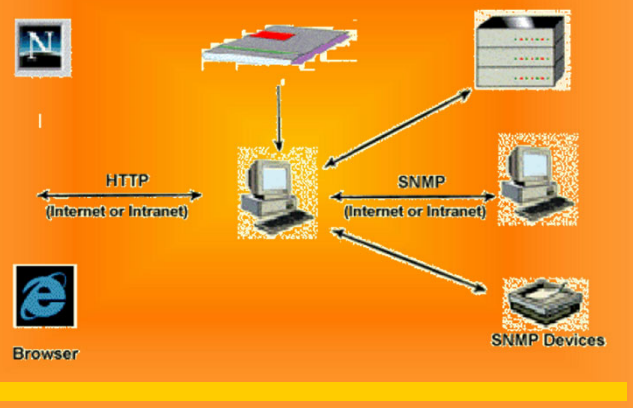
Basic Model for Network Management



13

universidade de aveiro

WEB-based management

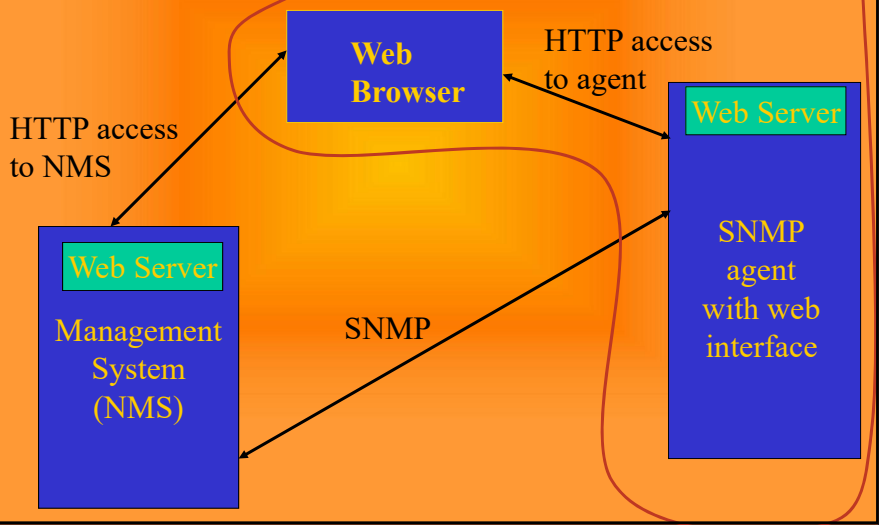


Very common:
Network and device management via web interfaces

universidade de aveiro

Web-based management concept

14



universidade de aveiro

15

Network management

- ISO defined five areas for network management
  - Fault management – detection, isolation, and correction of anomaly behaviors

Fault

  - Configuration management – control data for the network elements / colect data from network elements

Configuration

  - Accounting management – measure network utilization and determine network costs and user accountings

Accounting

  - Performance management – evaluate/report network equipment behavior/efficiency

Performance

  - Security management– support communications network secure management

Security

universidade de aveiro

16

Fault management

- Location of problems (or faults) in the communications network:
  - Fault detection
  - Fault isolation
  - Fault correction
- Faults can be:
  - Transients
  - Persistents
- Fault management includes functions to:
  - Mantain and examine error logs
  - Create and act in error notifications
  - Search, identify and correct faults
  - Perform diagnosis test sequences

universidade de aveiro

Accounting management

- Detect resource usage and its administration to assure its availability for the users
- Access control per user
- Allow costs per resource usage and association to tariffs
- It includes functions to
  - Inform users about costs and used resources
  - Establish utilization limits
  - Combine costs from multiple resources used to create the communication system

universidade de aveiro

Configuration management

- The configuration of critical elements controls the network behavior
  - The configuration management resides through these critical elements
- Configuration management identifies, acts, merges data and provides commands to systems to initialize, start, maintain in continuous operation, and terminate connections
- It includes functions to
  - Define parameters that control the system operation
  - Merge information about the actual system conditions
  - Modify the system configuration

universidade de aveiro

Performance management

- Measure the network performance (HW, SW). E.g.
  - Usage percentage, error rates, answer time, throughput
- Performance management supports the evaluation of system actions
- It includes functions to
  - Obtain statistical information
  - Maintain and examine logs of system state
  - Determine the system performance in normal and artificial conditions
  - Change working modes to perform management and performance functions

universidade de aveiro

Security management

- Access control mechanism to network information
- Monitors access points, periodically stores information and creates *logs* and alarms for security reasons
- Supports the appliance of security policies through functions to:
  - Create, remove and control of services and security mechanisms
  - Distribute information related to security
  - Report events associated to security

universidade de aveiro

21

Network management

- ISO defined five areas for network management
  - Fault management – detection, isolation, and correction of anomaly behaviors

Fault

  - Configuration management – configure network elements / colect data from network elements

Configuration

  - Accounting management – measure network utilization and detect network overload

Accounting

  - Performance management – evaluate/report network equipment behavior/efficiency

Performance

  - Security management– support communications network secure management

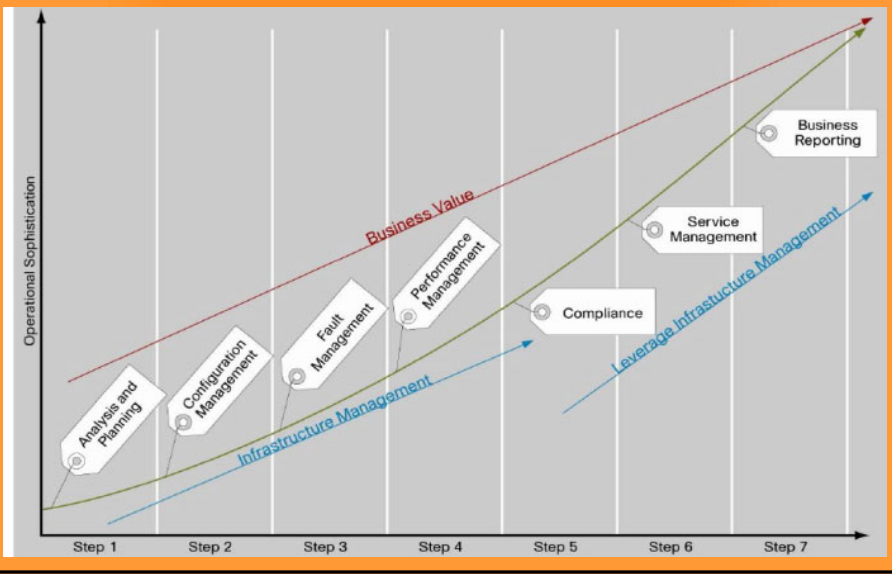
Security

Isolating the management problems in distinct areas, ISO model allows conceptual solutions optimized to specific problems in each functional area

universidade de aveiro

22

Implementation plans



universidade de aveiro

23

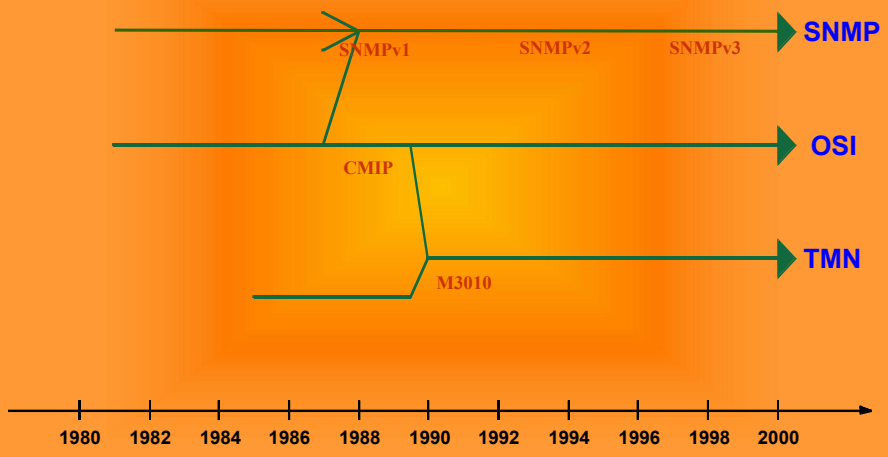
Network management: standardization

- **Internet Engineering Task Force (IETF)**
  - **Simple Network Management Protocol**
    - SNMP, disman
    - *Operations and Management Area*
- **International Telecommunications Union (ITU-T)**
  - **Telecommunications Management Network**
    - *SG IV*
- **International Standard Organization (ISO)**
  - **OSI, CMIP-CSIS**
    - *ISO-IEC/JTC 1/WG 4*
- **Others**
  - **DMTF, TM FORUM, OMG, IEEE, …**

universidade de aveiro

24

Cronology



universidade de aveiro

SNMP
(short review)

Simple Network Management Protocol

universidade de aveiro

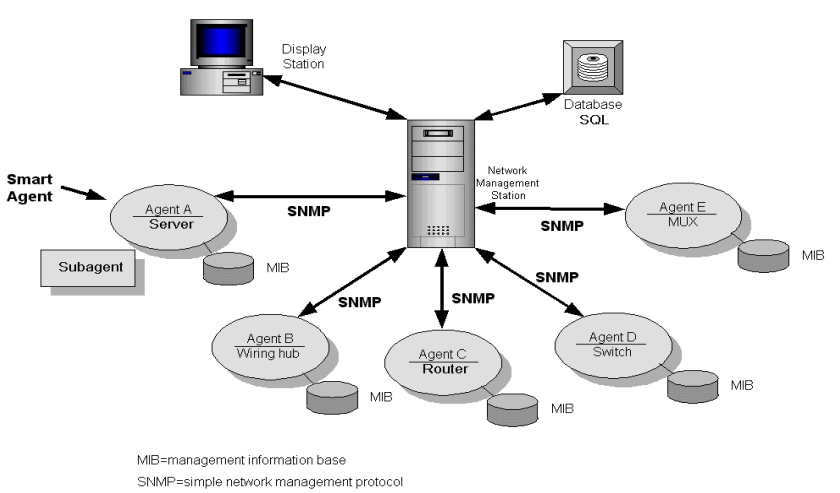
Manager/Agent Paradigm

- **Manager/agent: common in all NMS (especially in SNMP/CMIP)**
- **Idea of a client/server, but many clients and only some servers**
  - **(manager ↔client; agent ↔server)**
- **The agent operates with the equipment**
  - **Reports problems to the manager, to control all the equipment information**
- **The manager contains the intelligence to decide what the agents should do, and gives instructions to them**
  - **It controls the agents and manages their interworking**

universidade de aveiro

27

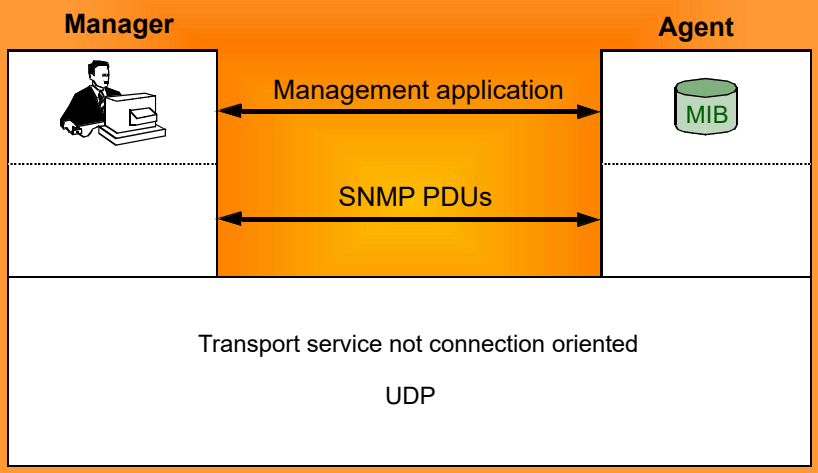
Structure of SNMP management



universidade de aveiro

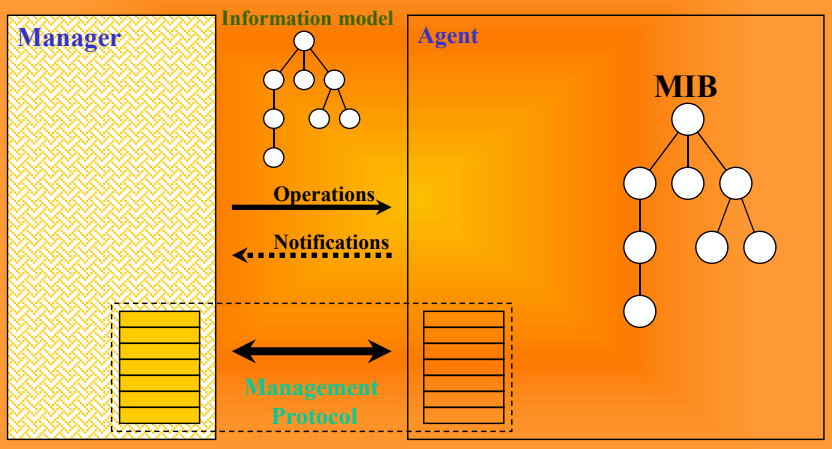
28

SNMP Structure



universidade de aveiro

Manager/Agent model



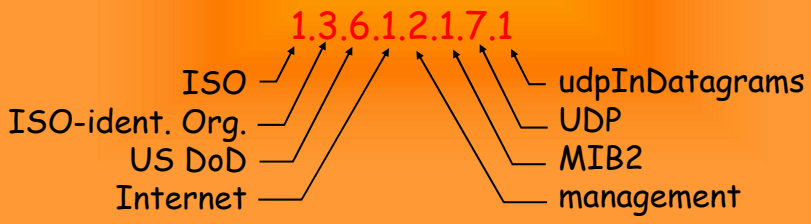
universidade de aveiro

Names (numbers) SNMP

Problem: **How to name all possible objects (protocols, data, etc..) in all possible protocols??**

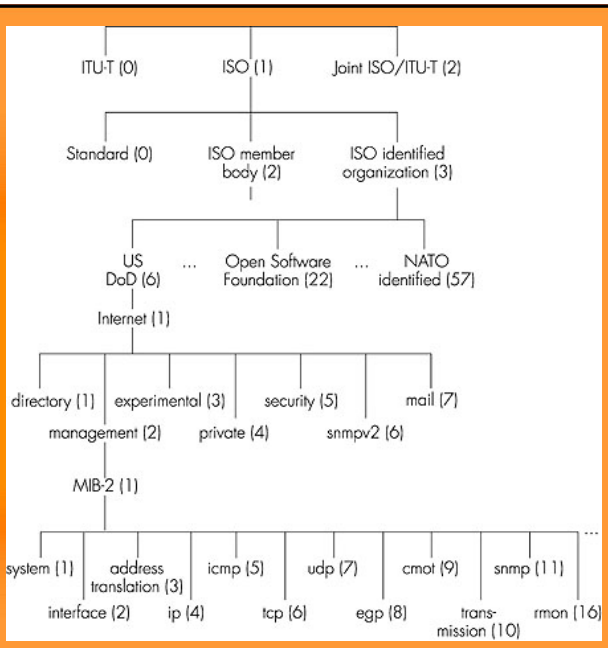
Answer: ***ISO Object Identifier tree:***

- **Hierarchical naming for objects**
- **Each node has a name and a number**



31

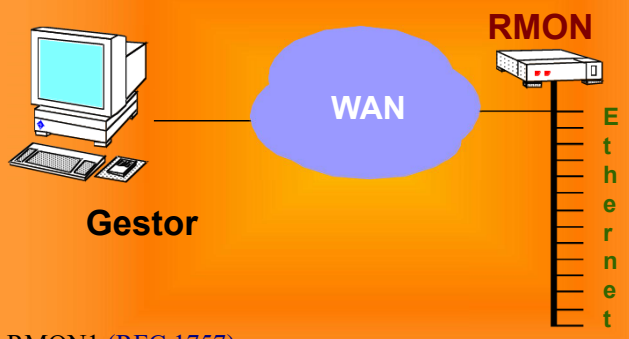
OSI Object Identifier Tree



www.alvestrand.no/harald/objectid/top.html

32

REMOTE MONITORING



- RMON1 (RFC 1757)
- Token Ring extensions to RMON (RFC 1513)
- RMON2 (RFC 2021)
- SMON (RFC 2613)

33 universidade de aveiro

RMON

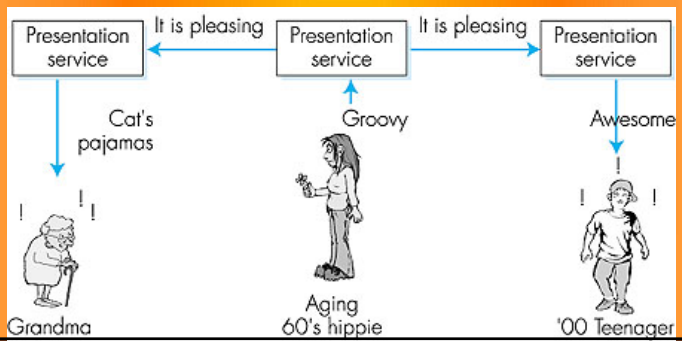
- Remote monitoring MIB – measure network traffic
  - Agents – management interface
  - Probes – equipment for network analysis (promiscuous); usually configured to specific data types.
- Off-line operation (separated from the network)
- Preemptive monitoring, providing multiple information in the network.
- Support multiple managers and probes
- Detection and report of problems
- RMON has 9 groups:

  Statistics, History, Alarm, Host, HostTopN, Matrix, Filter, Packet Capture, and Event

34 universidade de aveiro

The presentation problem?

1. Translate the local format to a host-independente format.
2. Transmit the data in a host independente format
3. Translate the host-independente format in a format adequate to the new machine adequado à nova máquina.



35 universidade de aveiro

ASN.1

- ISO X.680 standard
  - Formal language to describe SMI
  - Frequent in Internet
  - "Heavy", but essential for heterogenous environments.
- Data types, object constructors
  - As in SMI
- BER: Basic Encoding Rules
  - Specified the format as ASN.1 data should be transmitted.
  - Each transmitted object has a coding Type, Length, Value (TLV) encoding

36 universidade de aveiro

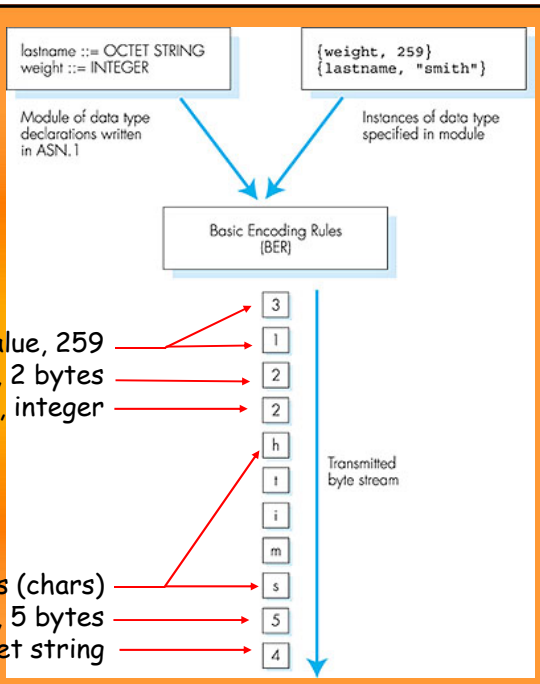
TLV Coding

Idea: Data must be auto-identified
- T: data type, (ASN.1-defined)
- L: data lenght in bytes
- V: data, coded according with ASN.1 syntax.

Valor Tag	Tipo
1	Boolean
2	Integer
3	Bitstring
4	Octet string
5	Null
6	Object Identifier
9	Real

universidade de aveiro

TLV coding example



universidade de aveiro

SNMP: Pros and Cons

- Agents widely used/known
- Simple to implement
- Robust e extensible
- Polling approach adequate to LAN objects

Critical requirement satisfied: available to be developed in the right time

- Very simple: does not scale
- Specifc semantics make its integration with other approaches difficult
- Large communication overhead due to polling
- Many specific implementations (private MIBs)
- In several management systems, small agents may be inadequate

Note that SNMP became a misnomer, referring both to the management protocol and the management framework. These are different things.

universidade de aveiro

PBM and COPS

Policy Based Management

Common Open Policy Service

universidade de aveiro

Policies - Example

- **Network with multiple services support**
  - **Differentiated QoS**
  - **Additional requirements in AAA functions**
    - Different levels
      - User
      - Service
      - QoS
- **Service authorized**
  - **only to some users**
  - **between authorized network points**
  - **with specific QoS requirements**
  - **between specific time intervals**
- **User also needs to be charged according to the service characteristics being received**

Management based on Policies

- **Objective: globally manage the network and not its elements.**
- **Mechanism:**
  - **Define policies (rules) to inform the network of what to do – e.g:**
    - Operation center should have access to all routers
    - Charging department has priority in the last 3 months of each year
    - In the maximum, only 10% of each link can transport video.
  - **The policy rules are translated in equipment configuration changes**

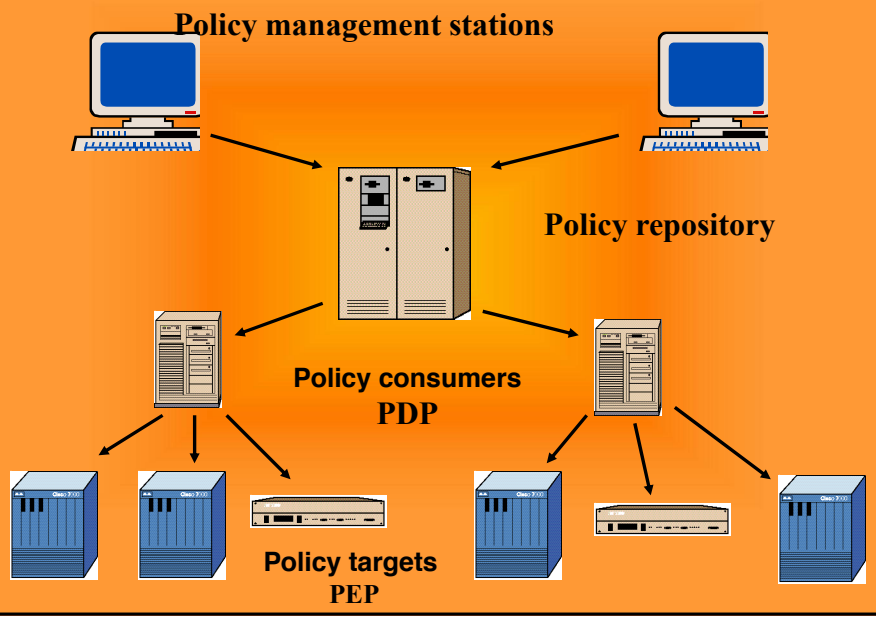
Elements of systems based on policies

Conceptual parts:

- **Management policy tools:**
  - Used to create the policy rules
- **Policies repository**
  - Store the policy rules
- **Policy consumers – *policy decision points*, PDP**
  - Make decisions and transfer the policy rules (eventually translated) to the policy targets.
- **Policy targets, *policy enforcement points*, PEP**
  - Functional elements affected by the policy rules.

43

Policy management system - example



44

Processing rules - sequence

- **Rules definition**
  - Verify internal conflicts
  - Include in a repository (e.g. with LDAP)
- **Get policies from policy consumers**
  - Take decisions based on policies
  - Processed to create configurations in policy targets
  - May use temporal restrictions
- **Send policies to policy targets**
  - Can be “pushed” or “pulled” (e.g. by COPS or SNMP)
- **Policy targets**
  - Instal configurations

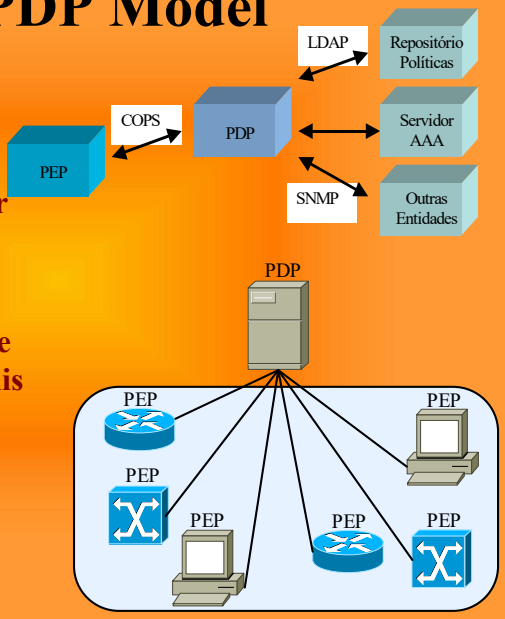
universidade de aveiro

45

PEP-PDP Model

- Model uses (may use) different protocols
  - Abstraction levels differ
- Increasing trend
  - Software defined netwoking (SDN) can be seen as a variation of this concept

(OpenFlow is a protocol for SDN, replacing COPS in this context)



universidade de aveiro

46

COPS – Common Open Policy Service

- Question/answer protocol to PDP-PEP interaction
- Based on TCP
- Maintains state synchronization
  - Recovers from fault
  - State maintenance with keep-alive
- PDP can send notifications to PEP
- PDP can receive policies through LDAP and SNMP
- Supports two types of clients
  - RSVP, outsourcing model
  - Diff-serv, configuration model

universidade de aveiro

47

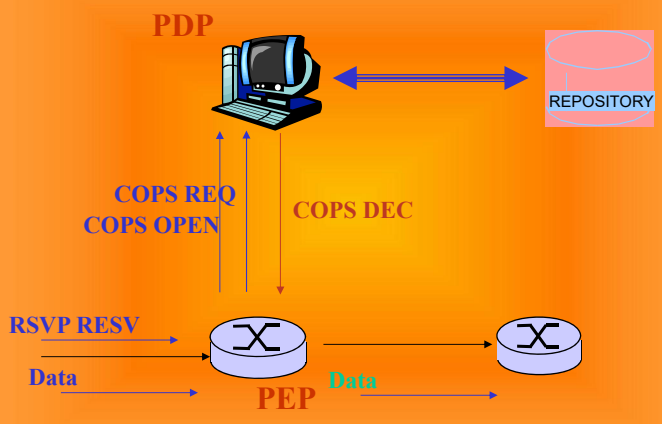
PDP-PEP Interactions

- Outsourcing (RSVP)
  - PEP contacts PDP when a decision is needed
  - Request contains relevant elements for the policy, and admission control information (e.g. flowspec)
- Configuration requests (Diffserv)
  - PDP configures PEP with specific equipment information
  - Considers a PIB (policy information base) that maintains provisioning information

universidade de aveiro

50

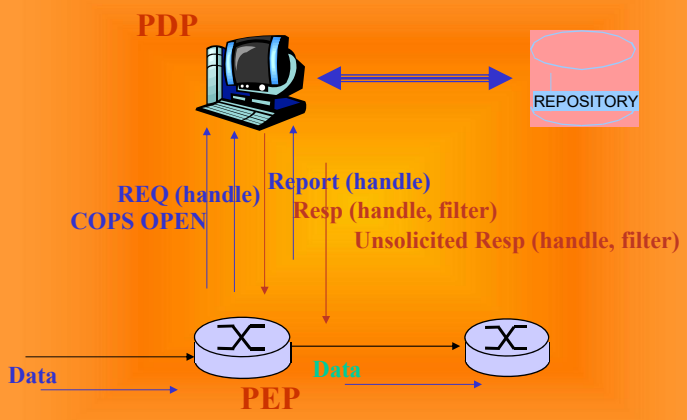
COPS with RSVP



universidade de aveiro

51

COPS with DiffServ



It is not required end-to-end signalling
It configures routers with packets lists and actions

universidade de aveiro

CMIS/CMIP

Common Management Information Services/Protocol

53

Management protocolos (LAN-based)

OSI CMIP

- Common Management Information Protocol
- Designed in 1980's: *the* unifying protocol ("advanced") to network management
- Implemented very slowly

SNMP: Simple Network Management Protocol

- Internet based (SGMP)
- Very simple in the beginning
- Rapidly spreaded
- It grew in largeness and complexity
- actual: SNMPv3
- Management protocol *de facto*

54

OSI Management architecture

ITU-T	Acronym	Title
X.701		*System Management Overview*
X.710	CMIS	*Common Management Information Service*
X.711	CMIP	*Common Management Information Protocol*
X.712	CMIP-PICS	*CMIP Protocol Implementation Conformance State Proforma*
X.720	MIM	*Management Information Model (defines fundamental concepts of the objects)*
X.721	DMI	*Definition of Management Information*
X.722	GDMO	*Guideline for Definition of Management Objects (techniques for specification of objects)*

universidade de aveiro

55

CMIS/CMIP

- Approach object-oriented - objects
  - Have attributes
  - Generate events/notifications (reliably)
  - Execute operations
- Objects with same attributes, notifications and operations belong to the same class
- Objects inserted in multiples hierarchies, with different inherits and containers
- Intelligent agents
  - Can use rules or policies defined by the manager
  - Can be changed on-line
- Actions (verbs)
  GET, SET, CREATE, DELETE, ACTION, NOTIFICATION, CANCEL_GET
- Capacity of CMIP actions is related to scoping and filtering capacities - through GDMOs

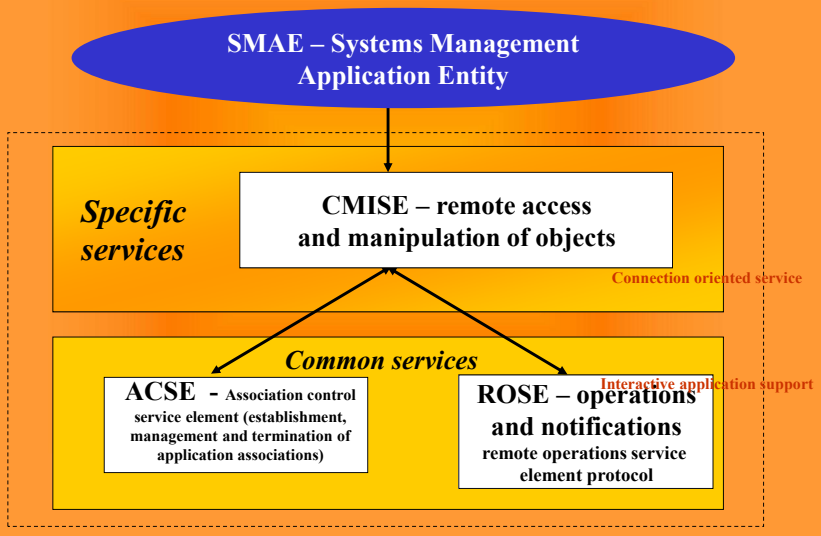
universidade de aveiro

56

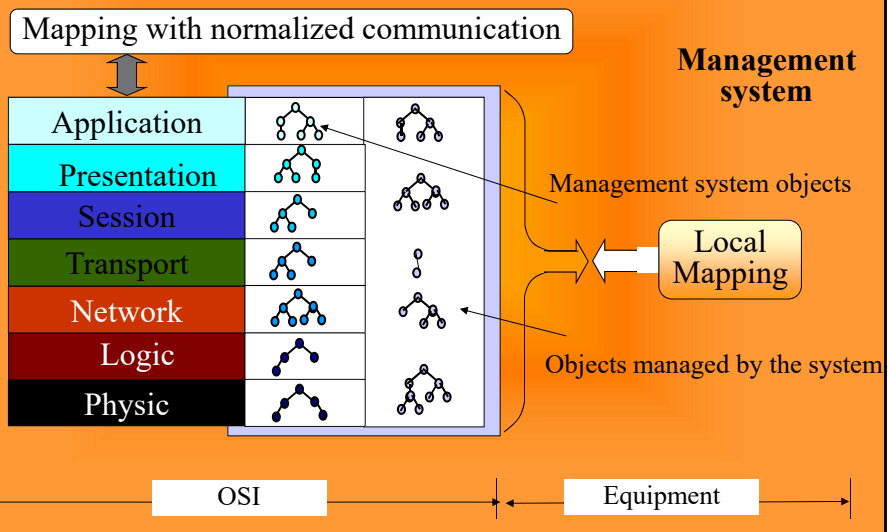
CMIP - GDMOs

- Guideline for the Definition of Managed Objects
  - The equipment through which the agent operates
- Model objects inside the equipment
  - Instantiation of GDMOs is called MIB
- Do not have well-defined behaviors, with large implementation freedom
  - Flexibility
  - Problem (complexity)
- CMIP is not polling oriented
  - Better scalability is achieved
- There are not so many defined GDMOs as MIBs

Common Management Information Service (CMIS)



OSI management architecture



61

CMIP: pros and cons

- CMIP advantages
  - Object-oriented approach is flexible and extensible
  - Support from telecommunications industry and international vendors
  - Support of manager-manager interaction
  - Support of automation environments
  - Imposed in some industrial areas
- CMIP disadvantages
  - Complex and multi-layer
  - Large management overhead
  - Few management systems based on CMIP
  - Few CMIP agents in use
  - Generally rejected in the Internet.

62

Frameworks: SNMP and CMIS

SNMP	CMIS
• Static MIBs • Concepts of limited models • Non-connection oriented protocol • Polling model • Implementation-oriented • Ligth • Limited functionalities • Bulk capcacity only in new versions • Completely dominating the market • Many SNMP-based products	• Dynamic MIBs • Object-oriented models • Connection-oriented protocol • Event-oriented model • Specification-oriented • Heavy • Functionalities until the system management level • Bulk capacity with scope and filtering • Some relevance in the telecommunications market • Some CMIP-based products in the market

universidade de aveiro

TMN

Telecomunications Management Network

universidade de aveiro

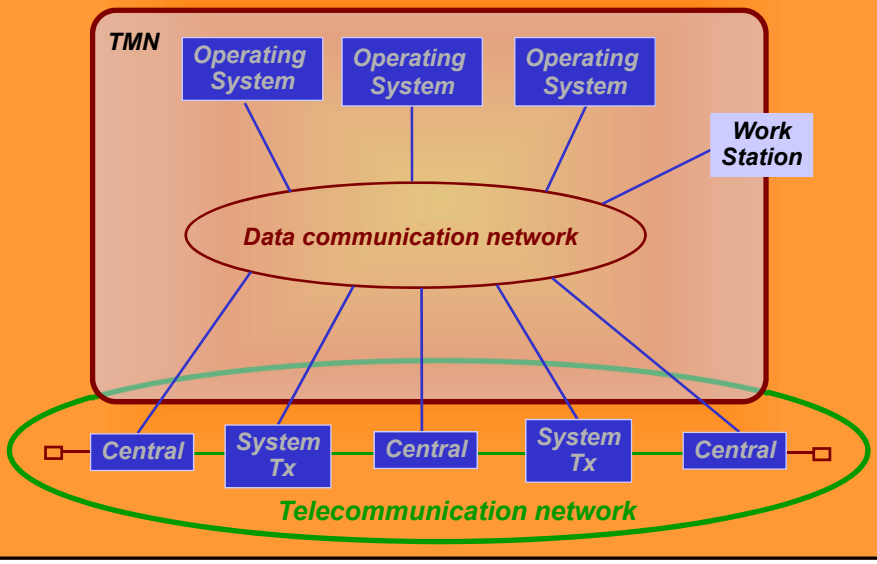
What is TMN ?

- **Defined in CCITT recommendation M.3010 and elaborated in the M.3xxx recommendations.**
  - **builds above the OSI- SM standards.**
- ***Objective***
  - **Support the management of the telecommunication networks and services**
- ***Concept***
  - **Create an organized structure to allow the interconnection of several operating systems and telecommunications equipments, using a well-defined architecture, with normalized protocols and interfaces**

universidade de aveiro

65

TMN and the communications network



universidade de aveiro

66

TMN

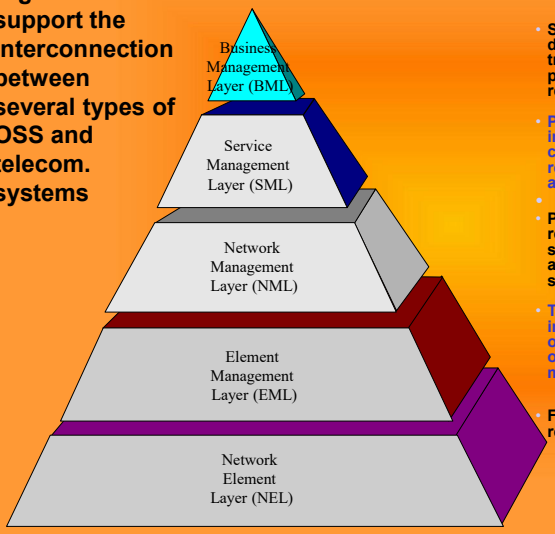
- **TMN is the telecommunications management network.**
  - **Relies on other management protocols and concepts.**
  - **Operations systems are where the main management functionality resides**
    - Now also known as OSS operational support systems
  - **The data communications network is where the management information flows**
  - **The TMN boundary intersects NEs (network elements) as they include some CM functionality.**
  - **Workstations provides user access to management functionality.**
    - The workstation glass interface is outside the bounds of standardisation.

universidade de aveiro

67

Multi-layer model

Architecture organized to support the interconnection between several types of OSS and telecom. systems

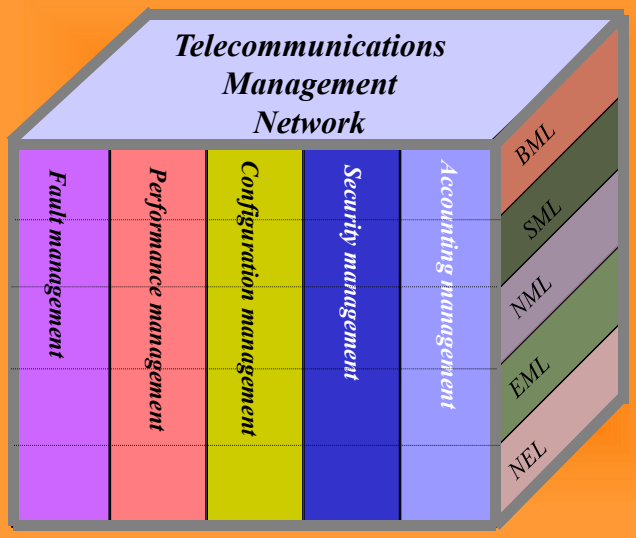


- Service levels, contact point for client reports, definition of policies for fault support, analyzes trends and quality issues, for example, or to provide a basis for billing and other financial reports
- Performs functions for the handling of services in the network: definition, administration and charging of services, scalability policies, service restore, monitoring and report of SLAs availability.
- Performs functions for distribution of network resources: configuration, control and supervision of the network, correlation of events and filtering, fault location, problem isolation, syslog management and monitor.
- This includes alarm management, handling of information, backup, logging, and maintenance of hardware and software, automatic correction of faults, polling of network elements, event management.
- Fault detection, trap generation, restoration/substitution procedures.

universidade de aveiro

68

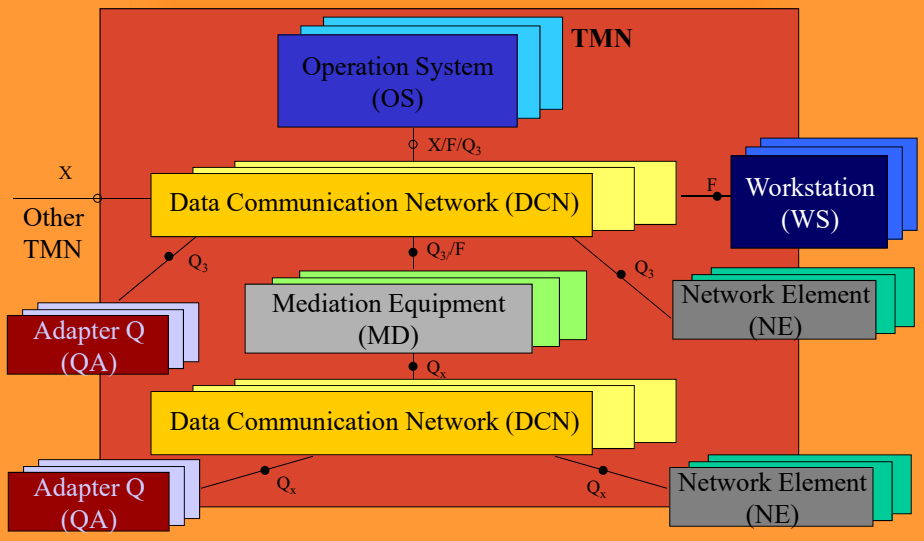
TMN Matrix



Depicts the FCAPS functionality along the TMN layers

universidade de aveiro

TMN Physical architecture



Reference points are exposed as interfaces (message and protocol parts) Notation - reference point lower case, interfaces upper case.

universidade de aveiro

Physical Architecture

Standard interfaces

- Interface Q_3
  - Operation System ↔ TMN elements connected to it
- Interface Q_x
  - Mediation Element ↔ Network element/adapter
- Interface F
  - Workstation ↔ Operation system / mediator (through a DCN)
- Interface X
  - TMN network ↔ TMN network / network with *interface* to TMN.

- **Communication protocols**
  - For each interface, the choice depends on the physical implementation.
  - It is normal to use CMIP protocol in the Q_3 interface.

universidade de aveiro

72

TMN Information model

Similar to OSI Information Model :

- Re-using of classes and templates
- Classes definition of generic objects.

Generic Network Information Model (GNIM)

- **Object classes defined by GNIM, relative to transport networks:**
  - Network fragment
  - Fragment of managed element
  - Fragment of termination point
  - Fragment of transmission
  - Fragment of *Cross-Connection*
  - Fragment of functional area
- **There are also object classes for other technologies (RDIS, SDH, ATM and mobile networks)**

universidade de aveiro

73

TMN and OSI

- TMN adds-on to OSI management

- **Information model – new network**
- **Organization model – extension through the concept of functional block**
- **Communication model – Correspondence between interface - protocol**
- **Functional model – new management functions (network)**

- Interworking TMN with other OSI systems

- **Atenuate differences between protocols**
- **Services functionalities and complementaring functions**
- **Increase the OSI management potentialities or restrict the TMN management potentialities**

universidade de aveiro

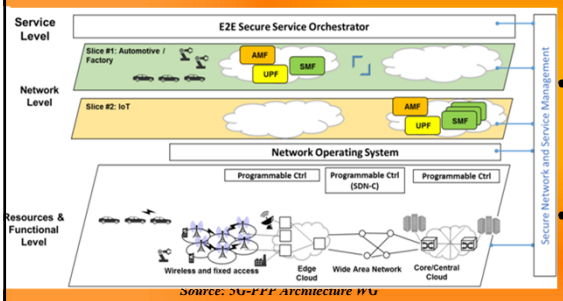
New network challenges

Bringing IT to networking

universidade de aveiro

Future networks
Emerging Architecture and Enabling Technologies

Architecture Themes:
Flexibility, Scalability



Source: 5G-PPP Architecture WG View on 5G Architecture (Version 2.0)

- **Network Function Virtualization**
  - **Network realized in software: Core and RAN**
  - **Cloud resources throughout the network**
- **Programmable Network**
  - **Flexible orchestration of network resources and infrastructure: RAN, core, transport, etc.**
- **Network Slicing**
  - **Self-contained, independent network partition including all segments: radio, core, transport, and edge.**
  - **Multi-domain, multi-tenant**

75

universidade de aveiro

76

Cloud computing

"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources […] that can be rapidly provisioned and released with minimal management effort or service provider interaction."

— NIST

universidade de aveiro

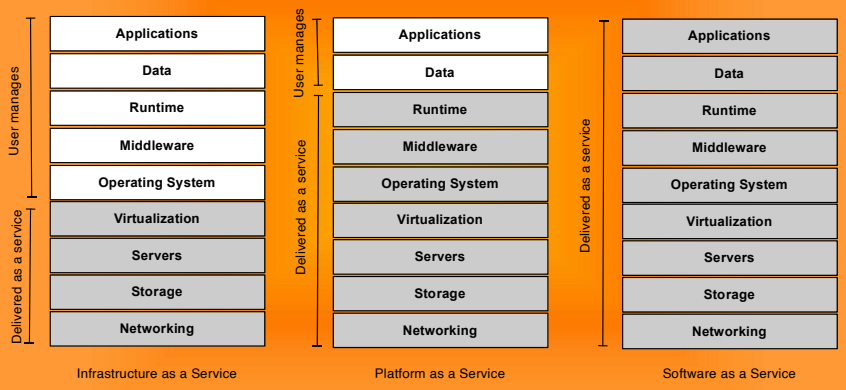
77

CC Essential characteristics

1. **On-demand self-service**
   - Dynamic usage of services, on-demand.
2. **Rapid elasticity**
   - Add and remove computational capability easily
3. **Ubiquitous network access**
   - Services (usually) accessible from the Internet
4. **Resource pooling**
   - Multiple customers can access the same resources
5. **Measured service**
   - Service usage is measured and reported, with cost usually in as pay-as-you-go

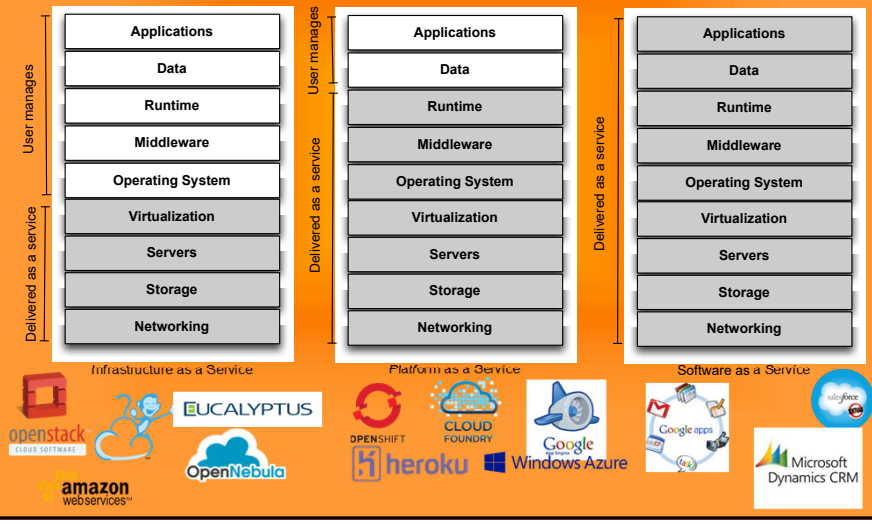
universidade de aveiro

Delivery models



universidade de aveiro

Delivery models



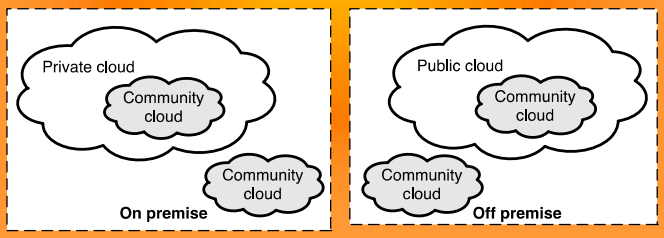
universidade de aveiro

82

Deployment models

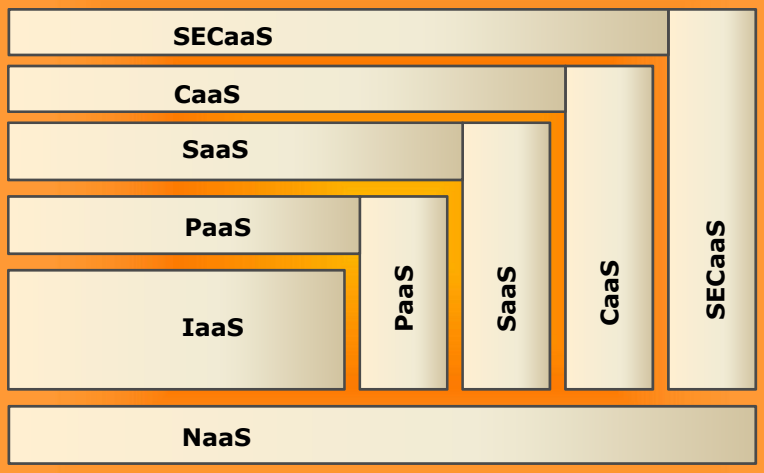
- Public cloud
- Private cloud
- Community cloud
- Hybrid cloud

- On-premises
- Off-premises



universidade de aveiro

Overall: Cloud Services

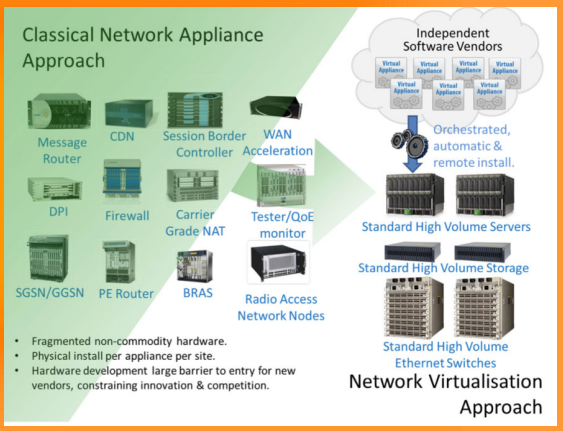


Network as as service relies on SDN – software defined networking – and NVF – network function virtualisation

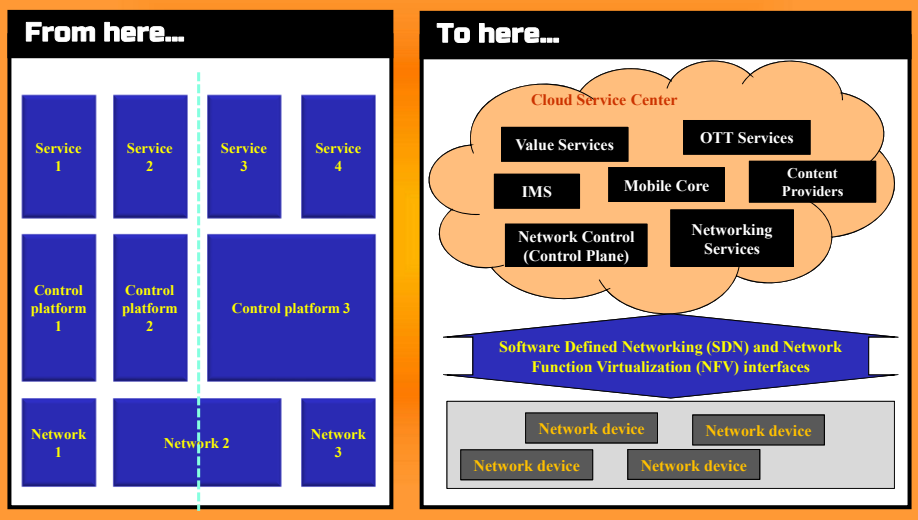
Networks require (complex) infrastructure

–Current infrastructure.
- Current network equipment designed for special use case

–Software Defined Networking and Network function Virtualization:
- Special use cases as software release running on top of standard hardware
- Virtualization will become a key issue to reduce OPEX and CAPEX



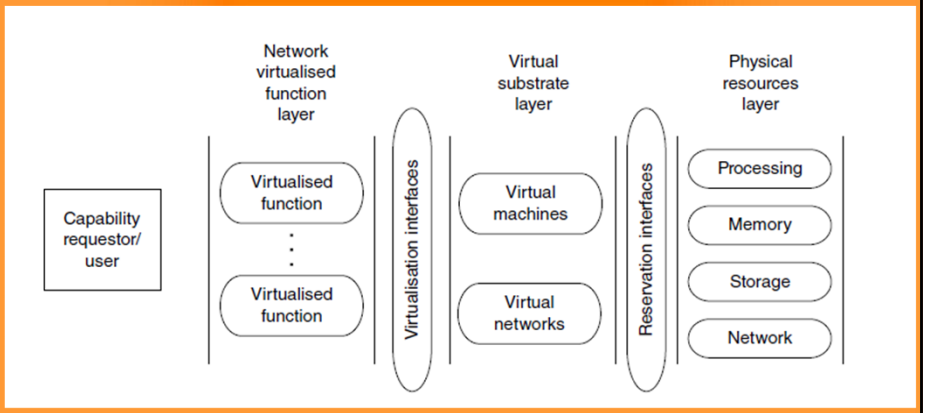
Evolving complex infrastructure



universidade de aveiro

86

The NFV concept



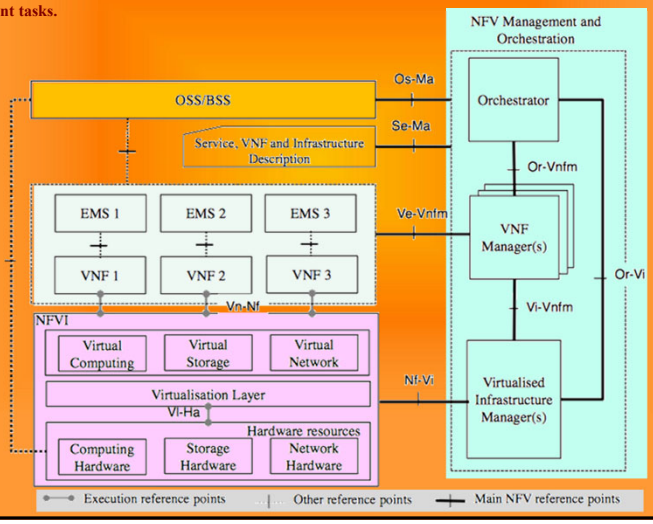
universidade de aveiro

87

ETSI NFV

High-level functional architecture for virtualised network functions and the underlying virtualisation infrastructure.

NVF M&O: orchestration and lifecycle management of physical and/or software resources that support the infrastructure virtualisation and lifecycle management of VNFs. Focused on the virtualisation-specific management tasks.

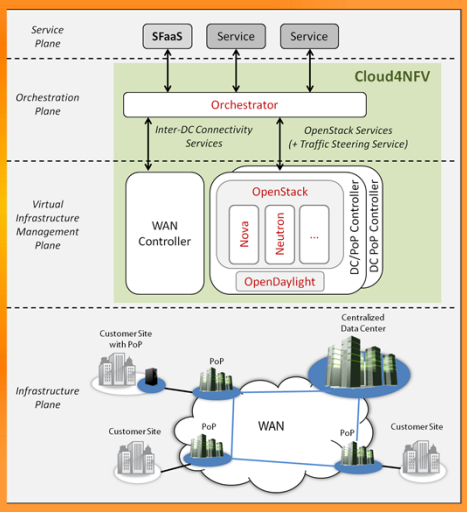


Source: ETSI

Cloud4NFV

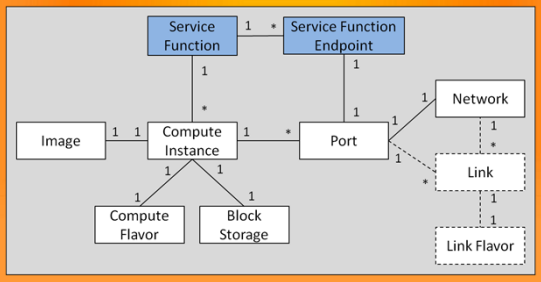
Platform built to allow Service Functions to be managed in *a as-a-Service* basis

- **Automated deployment, configuration and lifecycle management**
- **Federated management and optimization of WAN and cloud resources for accommodating SFs**
- **Supports composition of SFs through Service Function Chaining**



Virtualised Network Function

- **VNF - Software implementation of a network function capable of running over the NFV Infrastructure**
  - **Pure software free from hardware dependency**
  - **Service Function: represents an instance of a functional block responsible for a specific treatment of received packets that has well-defined external interfaces – *Service Function Endpoints* (SFEs).**
  - **Service Function Endpoint (SFE): represents an external interface of one SF instance that is always associated to a SF. Each SFE can have associated information regarding layer 1 (e.g. physical/virtual interface), layer 2 (e.g. MAC address) and/or layer 3 (e.g. IP address), or even regarding higher layers (e.g. HTTP).**



SF data model towards a Cloud infrastructure

Service Function Chaining

SFC

- ***An ordered set of Service Functions that must be applied to packets and/or frames selected as a result of classification***
- ***Defined by an orchestrator***
- ***Based on service requirements***
- ***Reliant on existing VNF***

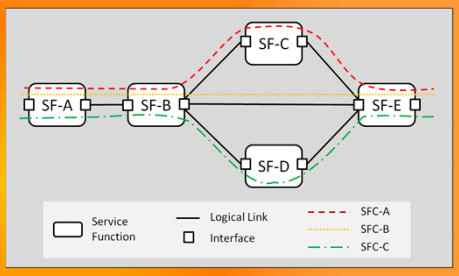
Service Function Chaining

In SFC two aspects are vital:

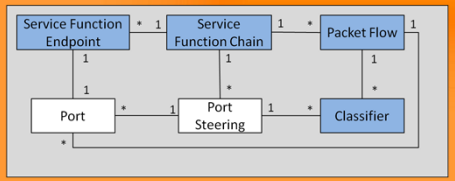
- **Classification**
- **Traffic Steering**

Combination of classification and traffic steering can be done in two ways:

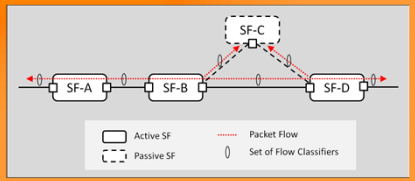
- **Tagged packet approach**
- **Non-tagged packet approach**



SF composition example



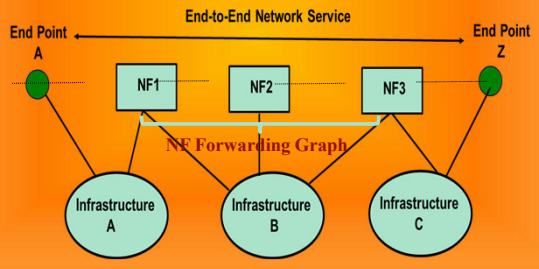
Service Function Chain data model towards a Cloud Infrastructure



Non-tagged packet approach; Active and Passive SFs

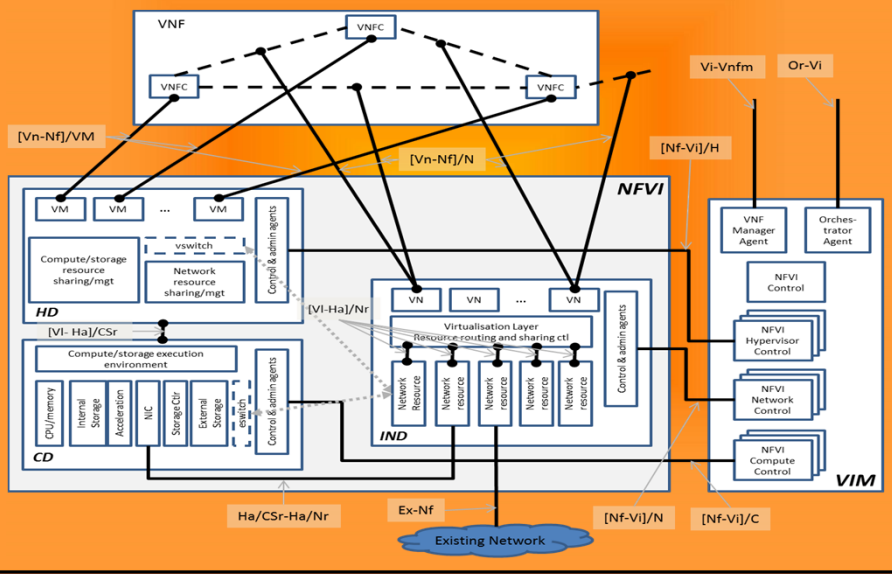
ETSI GS NFV 002 v1.1.1

- NFs are connected by logical links
- End points are connected to NFs via infrastructure resulting in a logical interface between end points and NFs



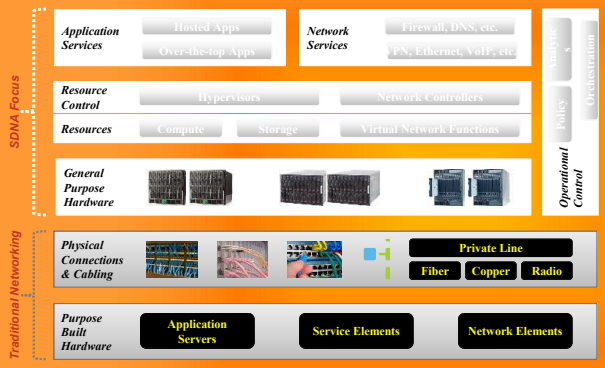
NFV Reference Architectural Framework

(ETSI GS NFV-INF 004 V1.1.1 (2015-01))



universidade de aveiro

Traditional Network vs. SDN/NFV Network



Virtualized Networks

- General purpose cloud-based hardware components
- Software-based virtual network components and services
- Dynamic real-time configuration to support internal or customer activity
- Programmable network management
  - Software Defined Network controls
  - Real-time analytics and policy driven orchestration of service, network and capacity requests

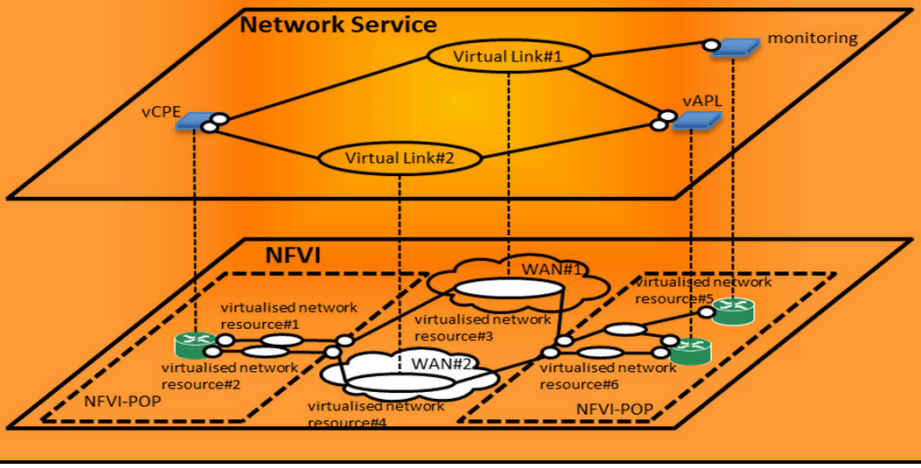
Traditional Networks

- Built using purpose-built hardware coupled with physical connectivity
- Control logic largely coordinated and implemented by layers of OSSs
- Control, Forward and Data Planes are tightly integrated in Network Elements
  - OA&M, inventory views and operational controls managed in OSSs to avoid negative impact to service performance

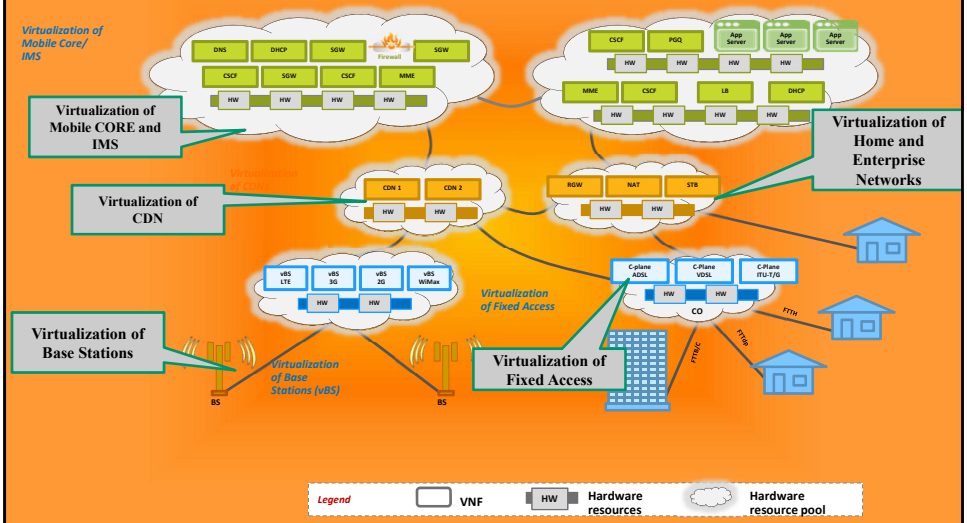
universidade de aveiro

Connectivity overview

enabling End-to-End Network Service across two WANs

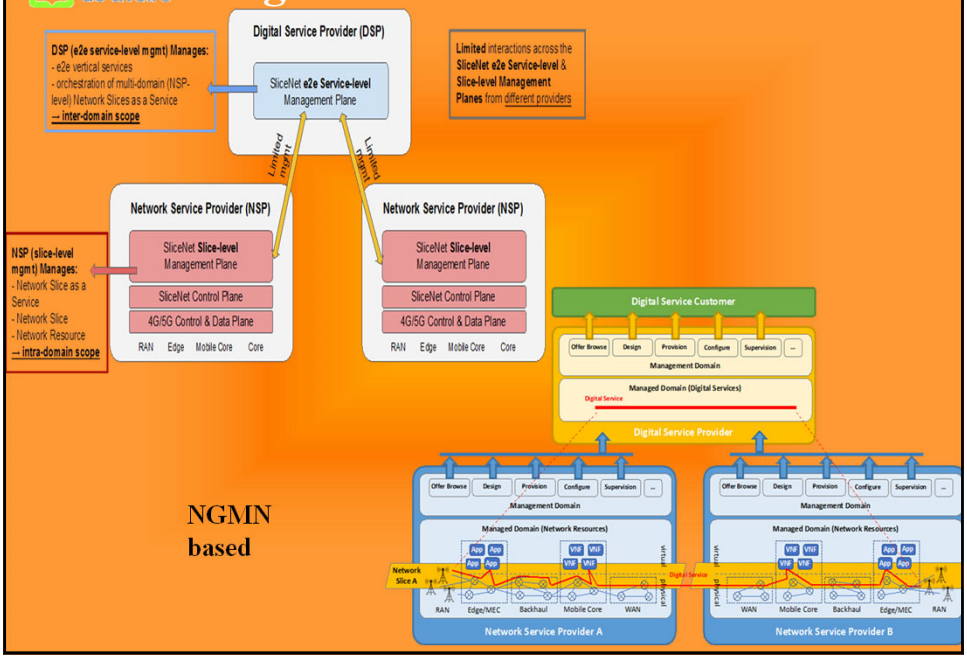


Overview of NFV (Network Function Virtualization) Sample Use cases



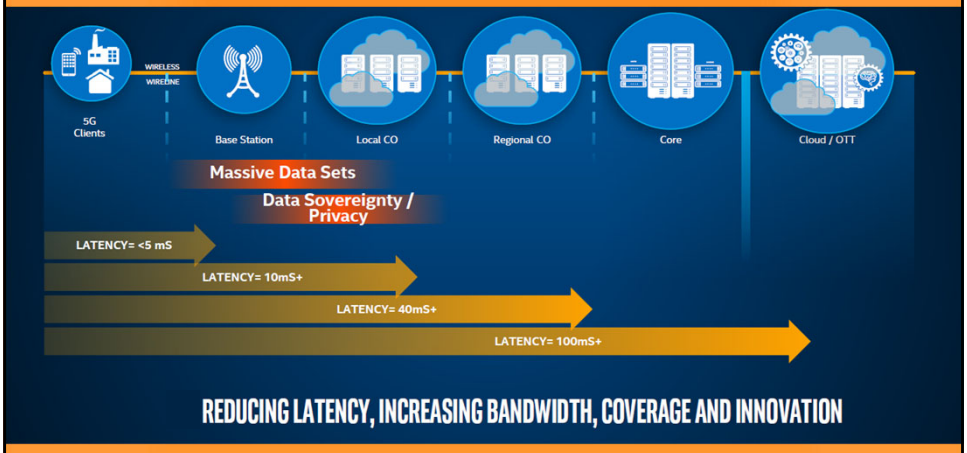
Management architectures and roles

99



universidade de aveiro

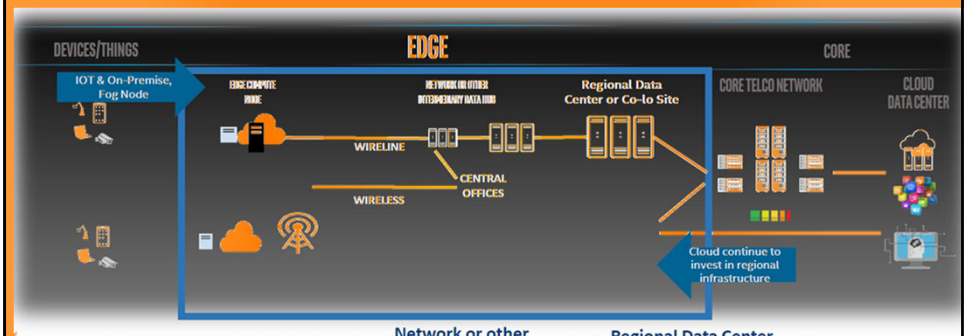
Network as a set of distributed datacenters



100

universidade de aveiro

The role of "edge"



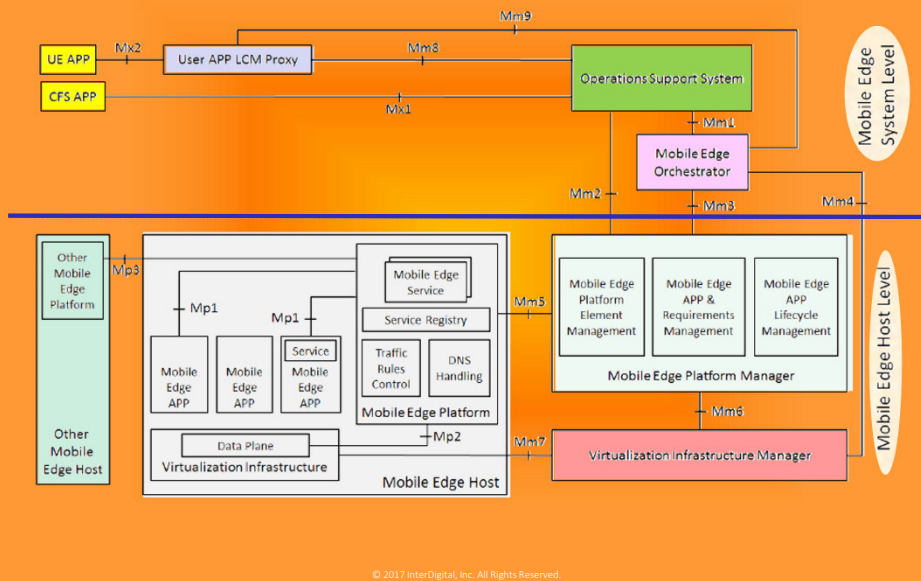
Edge Compute Nodes
Millions of on-premise sites; Typically virtualized servers, gateways, and traditional Routers/Switches/Appliances

Network or other Intermediary Data Hub
Access points & traditional network infra; transitioning to virtualized servers providing infra. & compute (NGCO)

Regional Data Center or Co-lo Site
Typically virtualized servers

101

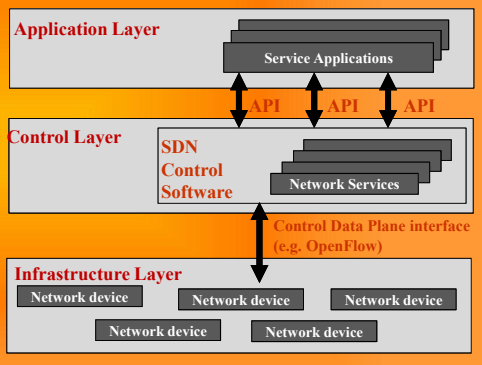
The (limited) ETSI view on MEC



The "new" purpose of SDN and NFV

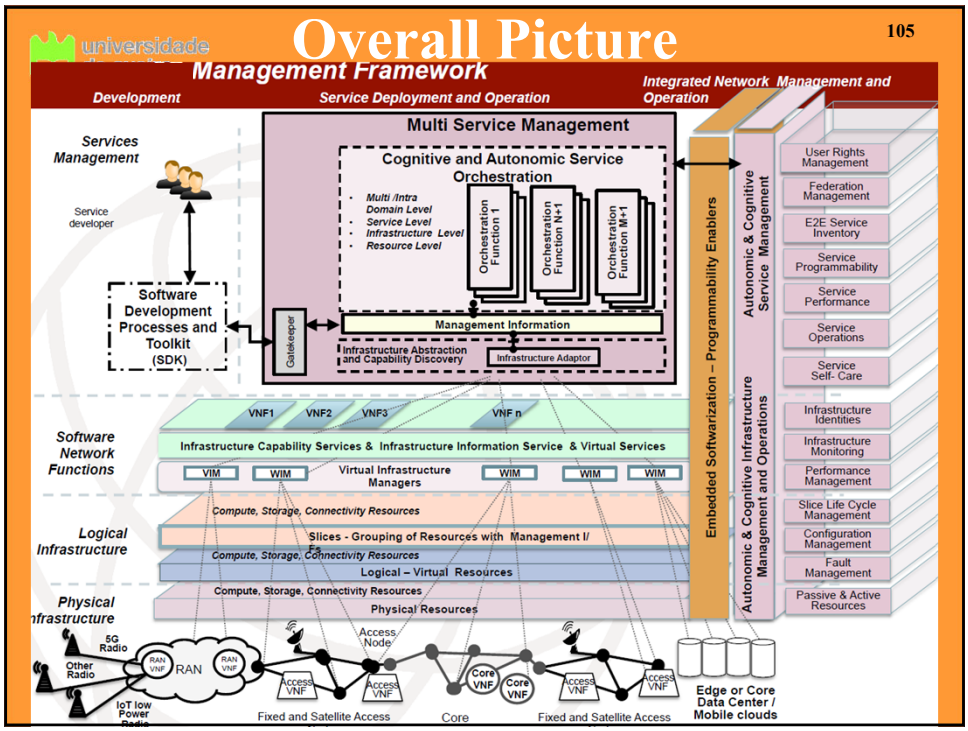
Split of the control plane from the user/data plane

- User/data plane implemented by standard (low-cost) equipment
  - Reduction on the HW cost
- Control plane implemented in the cloud – Network Function Virtualization – with standardized and open interfaces to services/business applications
  - Easy service development
- Software maintained by the operator
  - Change on the value and revenue model



Source: ONF (Open Network Foundation)

Overall Picture



Open Source Networking Landscape

[source: Linux Foundation – Arpit Joshipura]