Future Internet Trends: Networked Media, Content and Services Orientation

Eugen Borcoci,
University POLITEHNICA Bucharest,
Eugen.Borcoci@elcom.pub.ro

Daniel Negru,
CNRS-LaBRI Lab. University of Bordeaux, France

Christian Timmerer,
Dept. of Information Technology (ITEC) Klagenfurt University, Austria

INFOWARE 2011 Conference, June 19-24, 2011 Luxembourg

Acknowledgement

The **overview (State of the Art) part is compiled**, based on several public documents and authors' work: FI conferences public material, research papers, overviews, tutorials, etc.: (see Reference list)

The **ALICANTE –project case study** as an example of content/media –oriented architecture is resulted and presented with permission of the ALICANTE Consortium.

This work is supported by **ALICANTE FP7 IP Project 248652: "MediA Ecosystem Deployment Through Ubiquitous Content-Aware Network Environments".**

Note: Additional slides – may be skipped

CONTENTS

1. Future Internet : Trends and Challenges
2. Networked Media
3. Content and Services Oriented Networking
4. Content Aware Networking Architecture examples: ALICANTE project
5. Conclusions

CONTENTS

.

Future Internet

- Internet : major impact on *all socio-economic and life aspects* of the global society
- Current internet :
  - many limitations
  - not designed for a global scale and integrated services
  - ossification
  - …..

- Large efforts to revisit/re-define the future directions of Internet
  - points of view: technical, economical, social, evolution, etc.
- Entities involved: Research groups, Academia, Industry, Standardization organizations, Governments, Users, ..
- Still – there are many open FI issues, including discussion/revision of the basic concepts

1. Future Internet: Trends and Challenges

- **Future Internet**
  - **Partial list of FI initiatives/projects/…**

  - GENI Global Environment for Network Innovations, NSF
  - FIRE Future Internet Research and Experimentation - European program
  - European Future Internet Portal
  - FIA - Future Internet Assembly
  - EU ICT FP7 Future Internet projects
  - FIND - Future Internet network design
  - Clean Slate Research Program - Stanford University
  - TARIFA - The Atomic Redesign of the Internet Future Architecture
  - ITU-T Study Group 13 (SG13) on Future Networks , mobile and NGN, focus group FG-FN, Q21/13
  - ITFAN Inter-Agency Task Force for Advanced Networking (USA)
  - it839/u-it839 (Korea)
  - it839/u-it839 and FIF (FIForum) funded by MIC (Korea) http://www.fif.kr/
  - NICTA (Australia)
  - ANR (France)
  - ICT SHOK (Finland)

1. Future Internet: Trends and Challenges

- **Future Internet**
-
  - Partial list of FI initiatives/projects/…

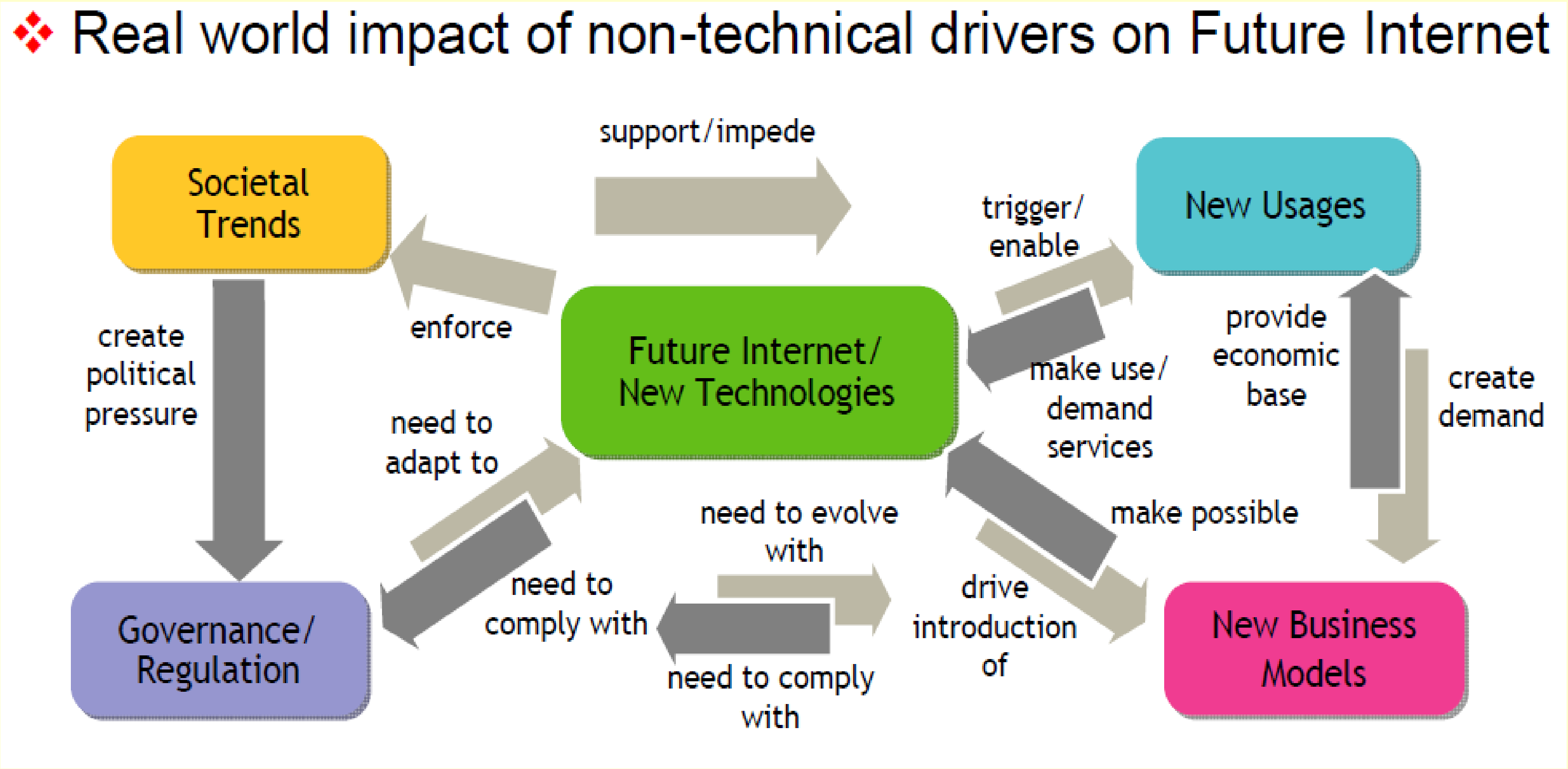
- (Japan)
- Super Janet funded by EPSRC (UK)
- Internet del Futuro (Spain)
- Ambient Sweden
- Belgium, Luxembourg, Italy, Netherlands, Ireland, UK
- United Kingdom FISG
- Finland - Finnish ICT SHOK research programme [www.futureinternet.fi]
- Spain - Internet del Futuro [www.internetdelfuturo.es]
- Germany -
- France - Groupe de Reflexion Internet du Futur - GRIF
- Euro-NF / Anticipating the Network of the Future - From Theory to Design

- Autonomic Internet Project
- Reservoir -Cloud Computing Project

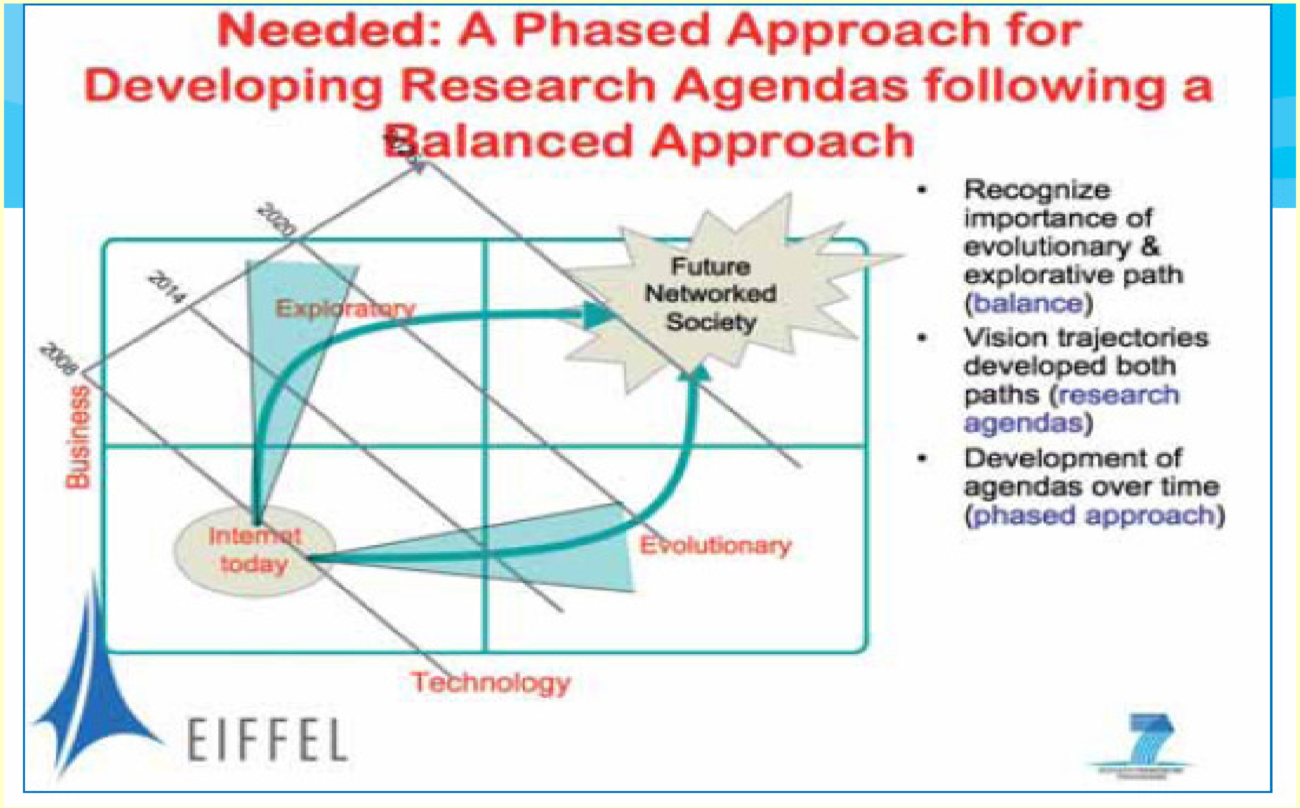
- **European EC events: Bled 2008, Prague, Lulea 2009, Valencia 2010, …..**

FI - Social, Economic and Environmental Challenges

- Source: Future Internet – Towards Research Challenges – 07 APRIL 2009, http://www.future-internet.eu/fileadmin/documents/prague_documents/FI



- **Approach?**
  - **evolution? clean slate approach? Middle way ?**
  - **Source:** Petri Mahönen, Project Coordinator, EIFFEL, RWTH Aachen University**" Evolved Internet Future for European Leadership (EIFFEL)", FI Conference, Bled, 2008**



1. Future Internet : Trends and Challenges

- **Usage trends versus Current Internet (CI) limitations**

Usage Trend	Current Internet limitations
Very high rate throughput, E2E	Many protocols not designed for ultra broadband scenarios
Ubiquitous good quality and cheap network access	Limited availability of high-quality optical wired networks; not enough bandwidths&QoS in wireless
Increasing mobility needs (micro, macro, terminal/ session, user, network mobility)	Initial Internet support has been conceived for fixed usages
Need for more *security*, and *trust, privacy* and *anonymity*	Security and trust natively supported in service and network infrastructures. Currently: privacy by design.
New/media oriented services: VoIP, P2P, IPTV	Not enough and effective networking support, including QoS

1. Future Internet: Trends and Challenges

- ## Current trends versus limitations

Usage Trend	Ccurrent Internet limitations
User generated content and services	Service architecture enabling service compositions and mashups- starting phase. No business models enough flexible
Novel human-computer interaction techniques	Reduced availability of cheap and compact sensor technology and advanced display technologies Basic Human-computer interaction
Universal connectivity,of devices, coupling of virtual world data with physical world information (RFID, sensors)	Network architecture itself scalability Non existing protocols for an optimal support device generated traffic Basic-only service architectures Not enough capability for service discovery
3D becoming mainstream	Imposes resource intensive usage of computing and networking platforms and standards - only partially available today
Negotiated management and control of resources, negotiated SLA's	Dynamic and predictive network management, infrastructure observability and controllability- objectives partially fulfilled

1. Future Internet: Trends and Challenges

- **Current trends versus limitations**

Usage Trend	Current Internet limitations
User is mainly interested in services and content- not in location	Need for content/service awareness, need for content oriented/centric Internet
Personalized services will become widespread on the FI.	Limited context awareness, lack of personalization tools, basic search capabilities
Computing and software as a network-centric service.	Currently many PCs exist, having installed a large number of different applications.
More need for *Availability*, *reliability*, and *dependability*	Limited: various degree of offering these, depending on provider.

1. Future Internet: Trends and Challenges

- **Source: Fundamental Limitations of current Internet and the path to Future Internet** EC FIArch Group2, Release Date: 1 March 2011
- http://ec.europa.eu/information_society/activities/foi/docs/current_internet_limitations_v9.pdf

- *Processing/handling of "data":*
  - no possibility for hosts to diagnose potential network problems and low feedback from the network;
  - lack of data and service identity;
  - lack of methods for dependable, trustworthy processing and handling of network and systems;
  - lack of data integrity, reliability, provenance, and trust.

- *Transmission of "data":* lack of efficient transmission of content-oriented traffic.

- *Control of processing, storage, transmission of systems and functions:*
  - lack of flexibility and adaptive control;
  - lack of reference architecture of the IP control plane (numerous control components added to the original IP simple data plane);
  - lack of efficient congestion control.

- *Multi-category limitations*:
  - traffic growth versus heterogeneity in capacity distribution;
  - the current inter-domain routing system is reaching fundamental limits
  - low security

1. Future Internet: Trends and Challenges

- **Source: Management and Service-aware Networking Architectures (MANA) Group :**
- A. Galis et. al., “Management and Service-aware Networking Architectures (MANA) for Future Internet Position Paper: System Functions, Capabilities and Requirements”, http://www.future-internet.eu/home/future-internet-assembly/prague-may-2009
- **CI Problems not (fully) solved:**
  - Guaranteeing availability of service according to Service Level Agreements (SLAs) and high-level objectives ; facilities to support Quality of Service (QoS)
  - Mobility of services
  - Inherent network mgmt. functionality, self-management functionality
  - Reducing the management overhead (critical part of lifecycle costs)
  - Facilities for the large scale provisioning and deployment of both services and management
  - Support for higher integration between services and networks.
  - Facilities for the addition of new functionality, capability for activating a new service on-demand, network functionality, or protocol (i.e. addressing the ossification bottleneck).
  - Support of security, reliability, robustness, context, service support, orchestration and management for communication and services’ resources.

CONTENTS

2. Networked Media

- Source: D.Kennedy, Networks + Content, Eurescom, FI Conference, Bled 2008 + others
- **Content/Media orientation- main trend in near/mid future**
- Trends in media oriented communications
  - combined services, high volume, high speed, high interactivity, spanning any geographic distances
- The Future of Content delivery
  - Ability to aggregate/bundle and manage content
  - Need for
    - a closer relationship : content producers/providers/networking
    - flexibility, extensibility and capability to evolve
    - distributed control and management (including autonomic)
  - Knowledge at network level on content (new concept) seems to be necessary (less separation between layers)
  - The challenge: “can we efficiently cross the old layers”?

2. Networked Media

- **Source: Future Media Internet Architecture Reference Model**
  - www.fi-nextmedia.eu /

  - *Improvement proposed by FMIA group*

    - ***Dynamic caching*** Content delivery efficiency increase by (In the network): network nodes capable to store content could be (routers, servers, nodes, data centres) – closer to the users

    - ***Content Identification:*** routers could identify/analyse *content_type* and/or *content_objects* flowing through them and replicate it efficiently: the search engines would gain better knowledge of the content popularity and provide information - even for "live" video streams.

    - ***Network topology & traffic knowledge:*** the current best/better E2E path could be selected for data delivery, if knowledge about the network topology /traffic per link were known, by some other entities than the network ones only

    - ***Content Centric Delivery***: more efficient content-aware delivery - based on the content name, if the content caching location, the network topology and traffic were known, rather than initial location of the content only

    - ***Dynamic Content Adaptation & Enrichment*****:** based on user preferences and user/network context

2. Networked Media

- **Future Media Internet Architecture Reference Model**

  - **FI Design principles (valid also for FMIA)**
  - Support flexible business models
    - multiple stakeholders can participate in an open environment that supports
    - encourages innovation and participation without barriers.
  - Open architectures and protocols
    - enable increased competition between providers(NP, SP, ..)
  - Users should be "prosumers"
  - Support of a greater participation of individuals, communities and small businesses + and more established organizations

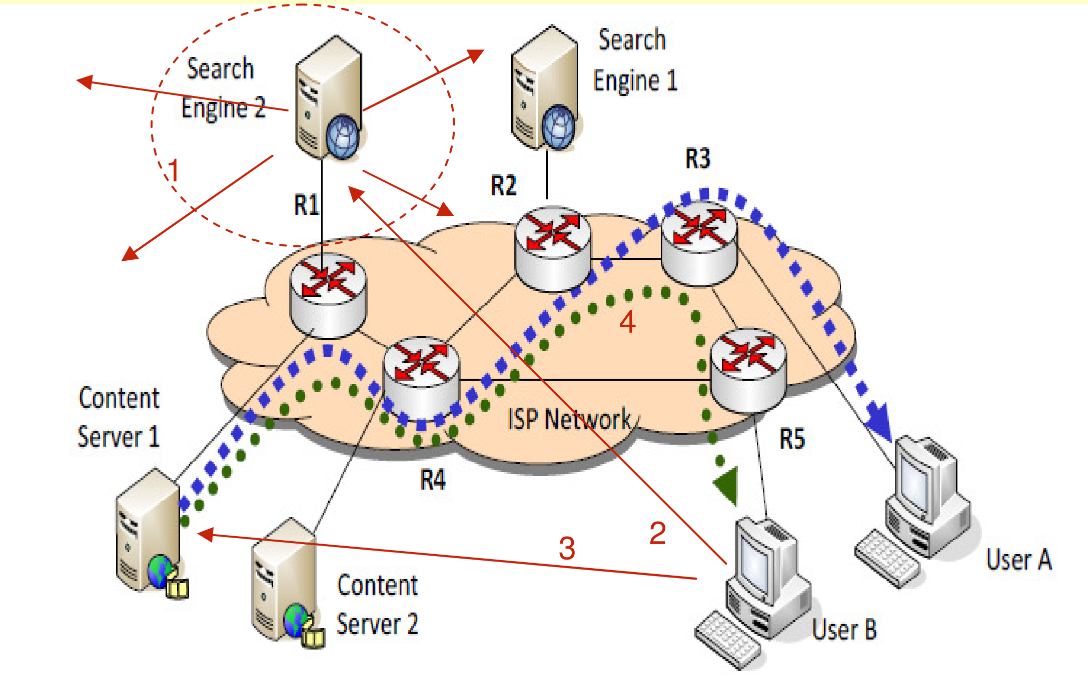
  - Offer incentives for all providers of content/services to receive appropriate benefits for their contribution
  - FI should be sustainable network , flexible enough to evolve, develop and extend in response to market needs
    - ability to be scalable, available and reliable in a resource- and cost efficient manner

2. Networked Media

- **Source: Future Media Internet Architecture Reference Model**
  - www.fi-nextmedia.eu /
  - http://initiative.future-internet.eu/news/view/article/future-media-internet-architecture-reference-model-white-paper.html- 2011

- **Current Internet limitations- related to content delivery**
  - *Components*
    - *Content Servers* or *Content Caches* (Content Provider or user generated content and services),
    - *Search Engines* (centralised or clustered)
    - *Network Nodes (Routers -* edge *and* core and, *Residential Gateways)*
    - *User terminals*

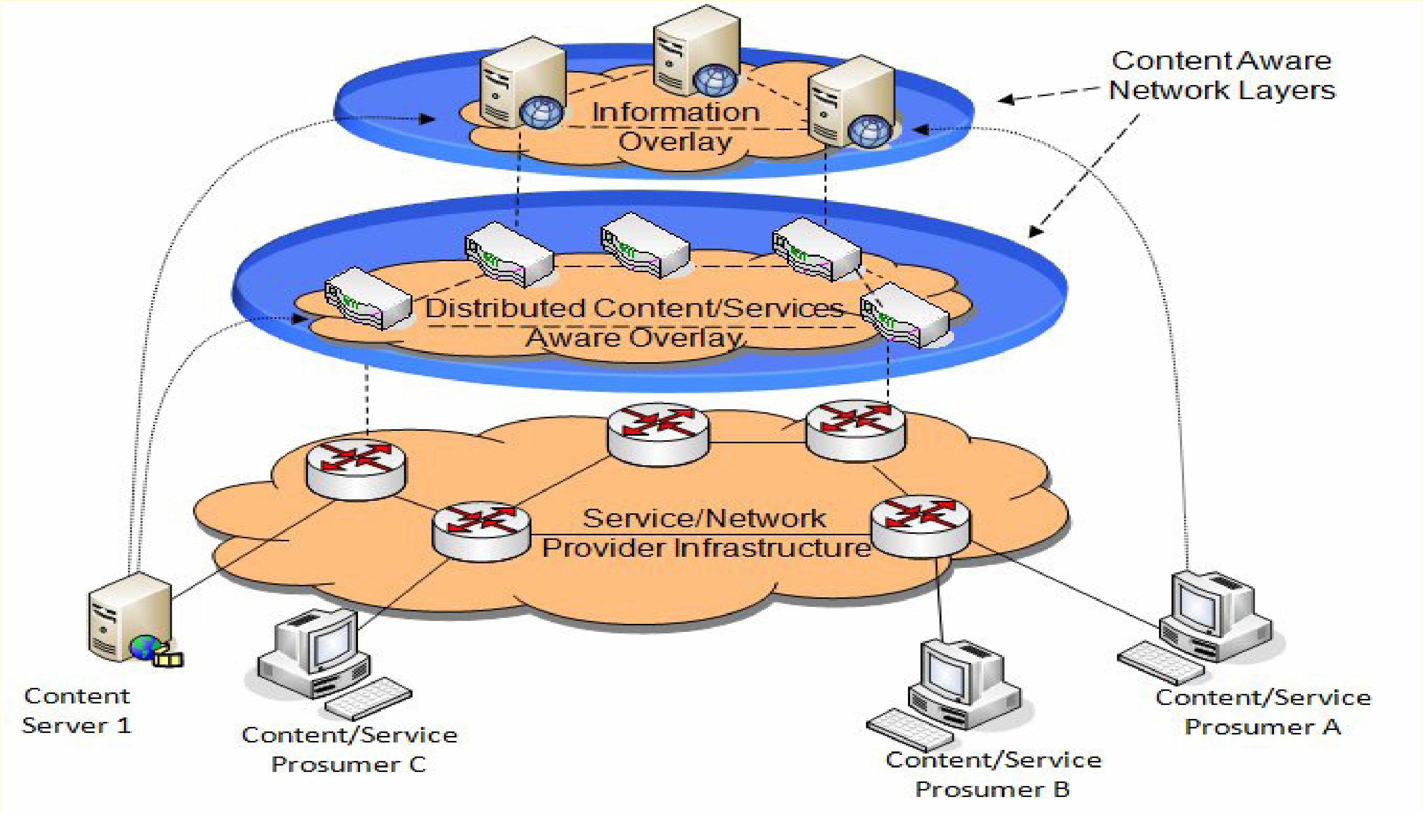
    - *Phases: 1-4 to get content*



Source: http://initiative.future-internet.eu/news/view/article/future-media-internet-architecture-reference-model-white-paper.html- 2011

2. Networked Media

- **Source: Future Media Internet Architecture Reference Model**
  - www.fi-nextmedia.eu /
  - **High –level FMI Network Architecture**



- **Source: Future Media Internet Architecture Reference Model**
  - www.fi-nextmedia.eu /

- **High –level FMI Network Architecture (cont'd)**
- nodes may belong to more than one layer

- FMI deployment is expected to be incremental
  - legacy network nodes will remain for a number of years;
  - the proposed architecture should be backward compatible with current Internet deployment

  - ***Service/Network Provider Infrastructure***
    - lower layer
    - Users are considered as Content Producers (user generated content) and Consumers ("Prosumers")
    - Usually the owner is ISP/network provider
    - Limited functionality and intelligence nodes
    - Content will be routed, assuming basic quality requirements and if possible and needed cached in this layer.

2. Networked Media

- **Source: Future Media Internet Architecture Reference Model**
  - www.fi-nextmedia.eu /
  - **High –level FMI Network Architecture (cont'd)**
  - ***Distributed Content/Services Aware Overlay***
    - Content-Aware Network Nodes (edge routers, home gateways, terminals devices)
    - *Intelligent nodes* can filter content and Web services flowing through (e.g. via DPI, signalling processing),
    - identify streaming sessions and traffic (via signalling analysis) and provide qualification of the content.
    - information reported to the *Information Overlay*
    - *Virtual overlays* (not shown) are statically/dynamically constructed at this layer.
      - overlays can target specific purposes: e.g. content caching, content classification, indexing, network monitoring, content adaptation, optimal delivery/streaming
    - Content delivery modes; hybrid client-server and/or P2P
    - Nodes have information on the content and the content type/context that they deliver ➔ hybrid topologies may be constructed, customised for streaming complex media

Scalable Video Coding (SVC), Multi-view Video Coding (MVC).

2. Networked Media

- **Source: Future Media Internet Architecture Reference Model**
  - www.fi-nextmedia.eu /

- **High –level FMI Network Architecture (cont'd)**

- ***Information Overlay***
- intelligent nodes/servers having distributed knowledge of
  - content/web-service location/caching
  - (mobile) network instantiation/ conditions (limited)

- Types of nodes:
  - unreliable peers in a P2P topology
  - secure corporate routers
  - Data Centres in a distributed carrier-grade cloud network
- Factors determining variation: actual network deployment and instantiation, the service scenario/requirements, service quality agreements

- Content stored/cached : at the *Information Overlay* or at lower hierarchy layers.

- *Information Overlay allows* awareness of the content/services location/caching and the network information
  - decision can be made on the way that content will be optimally retrieved and delivered to the subscribers or inquiring users or services

2. Networked Media

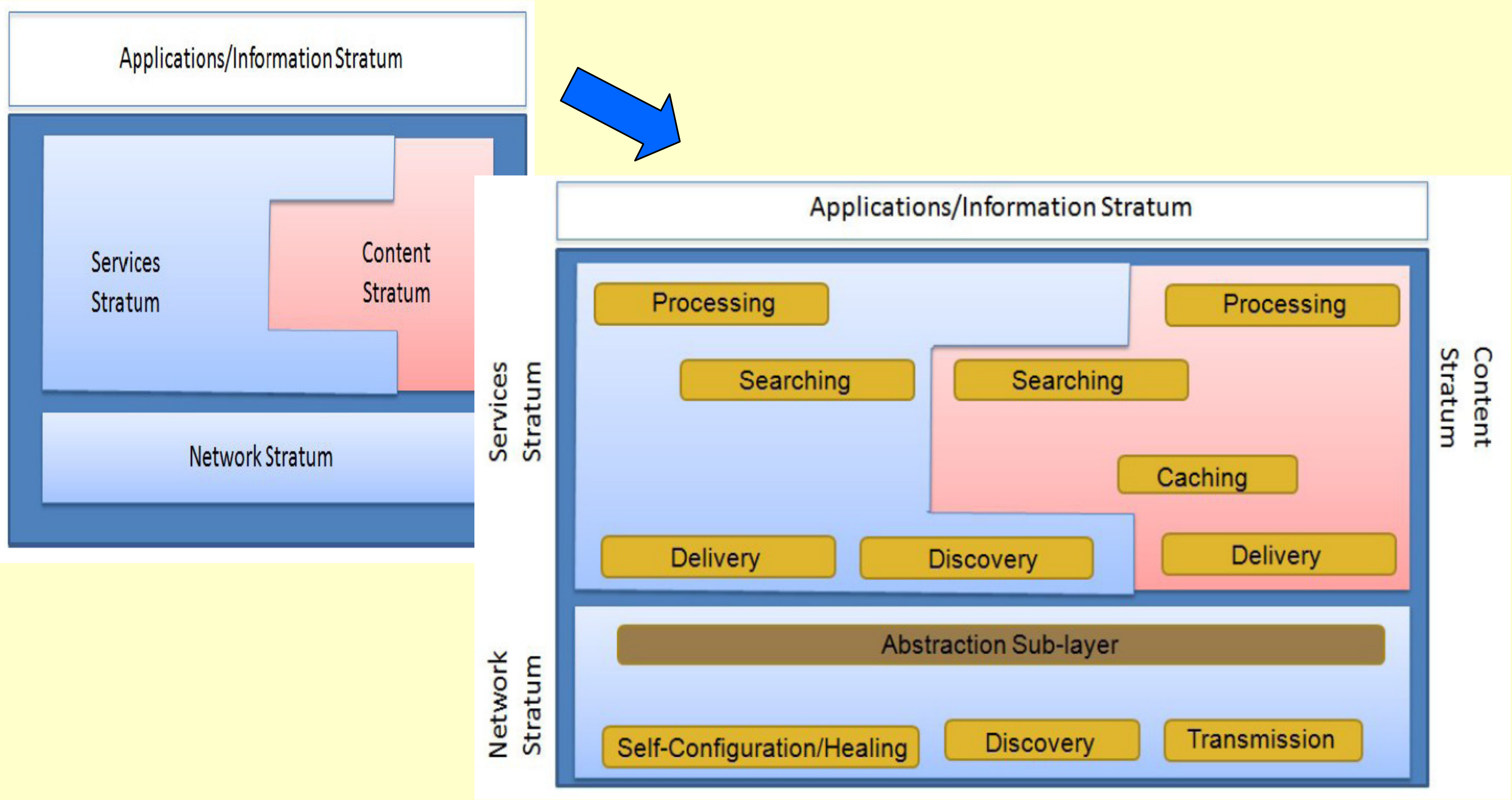
- Source: Future Media Internet Architecture Reference Model

Actions in the content production and delivery workflow

- **Content production**:
  - generation and store in a server
    - associated metadata (created manually/ automatically)
- **Publishing** inside the FMI network (manual publishing procedure or automatic content discovery and identification procedure)
- **Search by the CC** using a search engine.
  - A user can directly consume content utilizing the FMI network if he/she knows exactly the content item he/she is looking for.
- **Caching** by different cache nodes - as the content is delivered in the FMI overlay network (different criteria and policies)
- **Content** consumption by the CC
- **Network**
  - may also analyze the content being requested to be transported through it. (this information could be used by the search engine)
  - monitor its own state, as for example the connectivity between nodes, in order to report it to various components.

2. Networked Media

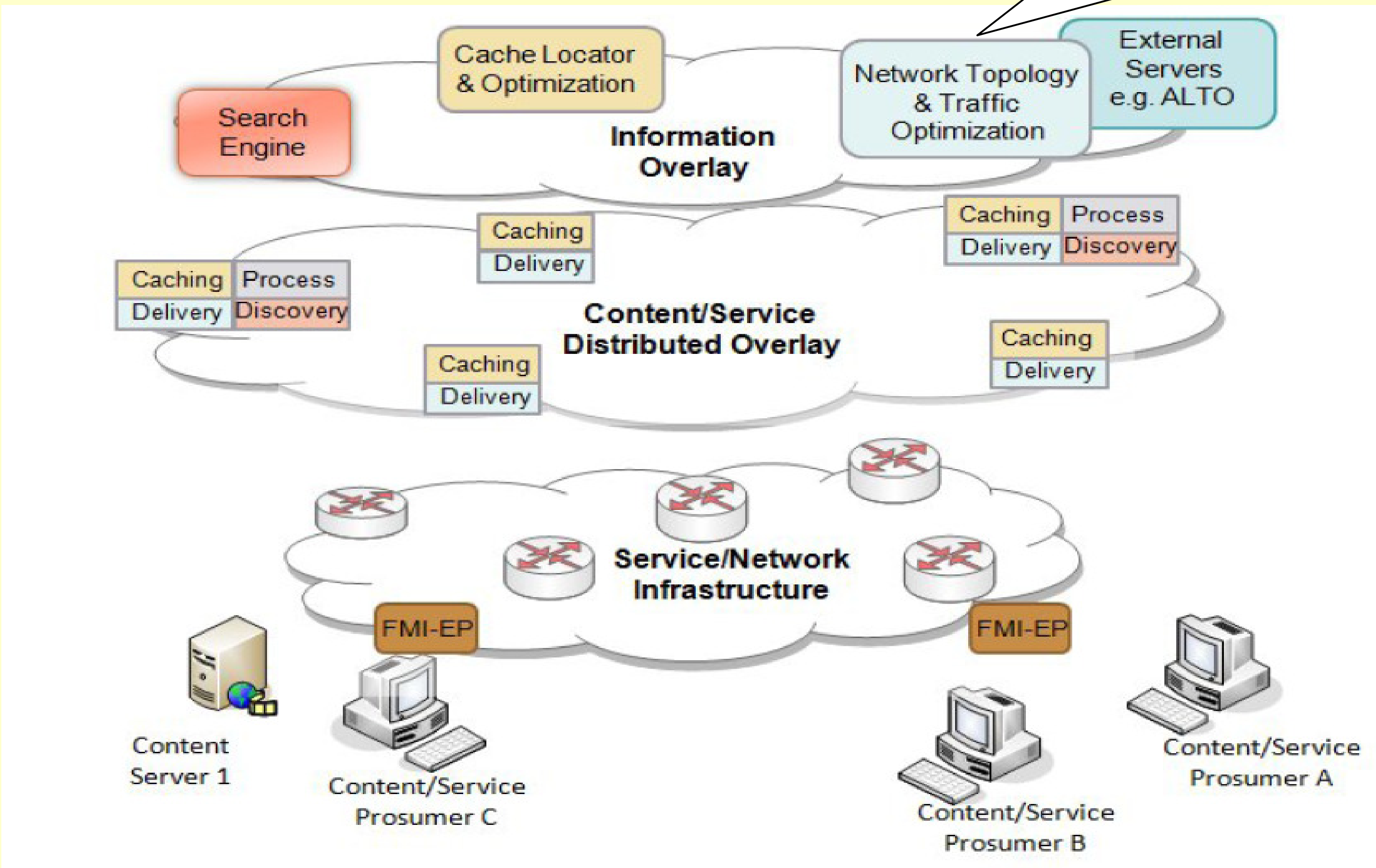
- Source: Future Media Internet Architecture Reference Model
- FMIA proposed protocol stack



2. Networked Media

- Source: Future Media Internet Architecture Reference Model
- FMIA Network Architecture- example

Limited rights (NP independence)



CONTENTS

Terminology

- Not standardised, different (overlapping) semantics…
  - **CAN- Content Aware Networking**
  - **CON - Content Oriented Networking**
  - **CCN - Content Aware Networking**
  - **SON – Service Oriented Networking**
  - **NAA- Network Aware Applications**

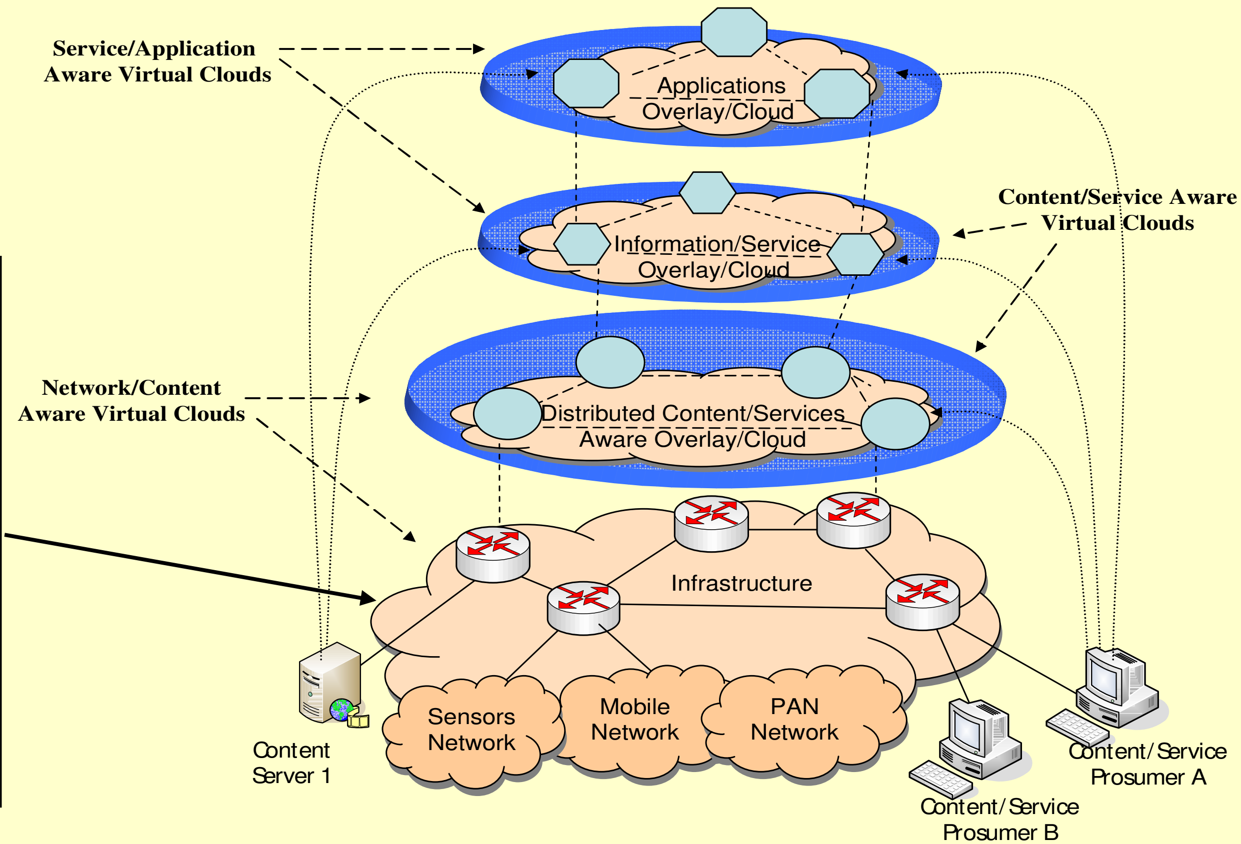
- This text approach:
  - CAN – is seen as having a more general scope
    Awareness of content type and /or
    Awareness of content object
  - CON: basic meaning: dealing with *content objects*: *naming, locating/routing, deliver/disseminate, caching in-network*
    CCN – particular case of CON

3. Content and Services Oriented Networking

- Source: Future Media Internet Architecture reference model outline
- www.fi-nextmedia.eu / http://www.gatv.ssr.upm.es/nextmedia/index.php?option=com_content&view=article&id=34&Itemid=40

- Evolutionary Content –centric Internet Architecture

- Current ISP and network provider network infrastructure
- Nodes with limited functionality and intelligence.
- Users : Prosumers
-
- Content : routed, QoS, possible caching



3. Content and Services Oriented Networking

- Evolutionary Content–centric Internet Architecture **(cont'd)**
  - **Service/Network infrastructure tasks :**
    - Perform content aware operations
      - Deal with active content objects
      - And unstructured bitstreams whose type is known
    - Transport, congestion-control, policy, signalling and processing protocols in a distributed manner
    - Quality of Service (QoS) and Service Level Agreements (SLA).
    - Mobility of terminals services, users and portability of content
    - Virtualisation and self-organisation/self-management
    - Inter-domain connectivity and interworking
    - Classic (FCAPS) functionality
    - Monitor and control network resources
    - Security and privacy of the infrastructure
    - Assure robustness, stability, and survivability
    - Hide network complexity to the higher layers (provide limited information)

3. Content and Services Oriented Networking

- Evolutionary Content –centric Internet Architecture (cont'd)

  - Distributed Content/Services Aware Overlay
  - Contains CAN Nodes (e.g. core routers, edge routers, home gateways, terminal devices)
  - CAN nodes have the intelligence
    - recognise and qualify the content
      - Part of this information may be stored locally and/or reported to the higher layer (Information Overlay).
    - filter the content and Web services flowing through
      - via DPI
      - identify streaming sessions and traffic via signalling
    - Other view:
      - Content = *information objects* = first order elements in the network, identifiable by the network nodes.

3. Content and Services Oriented Networking

- Evolutionary Content –centric Internet Architecture (cont'd)

  - Distributed Content/Services Aware Overlay provides: (cont'd)
    - content (media and services) awareness (inspection, crawling, recognition, categorisation, indexing)
    - content (media and services) adaptation and personalisation
    - content caching and "findability"
    - mechanisms for content (media and services) extraction, combination, creation, orchestration
    - name resolution, *route by name* and *route by type* capabilities
    - mechanisms for accountability and billing of content (media and services)
    - mechanisms for protection of content (including beyond DRM, lightweight management of the content)

3. Content and Services Oriented Networking

- Evolutionary Content –centric Internet Architecture (cont'd)

  - **Information Overlay (IO)**

  - Intelligent nodes/servers knowing
    - content/web-service location/ caching
    - (NAA-capabilities info on network instantiation/conditions)
  - Node types range: ordinary P2P peers …..secure corporate routers, data centers in distributed carrier-grade cloud networks

  - IO is aware of the content/services location/caching and the network information
    - However the content may be stored/ cached at IO level or lower

  - IO decide on the way that content will be optimally retrieved and delivered to the subscribers or inquiring users or services

3. Content and Services Oriented Networking

- Evolutionary Content –centric Internet Architecture (cont'd)

  - **Information Overlay (IO)** provides mechanisms for:
    - control the content and service "findability", construction, orchestration, representation and deployment.
    - supervise the *content/services location/ caching/ deployment* and the network resources information.
    - *services/ content/media publishing/ subscription*, pushing
    - accountability and billing of services / content /media
    - supporting *networking tussle* and new business models

  - **Applications layer**
    - Applications use
      - Services
      - information and the media/content

CAN- versus Content Delivery Networks (CDN)

- Source: wikipedia
  - (**CDN**) **delivery/distribution network** : system of computers containing copies of data, placed at various points in a network so as to maximize bandwidth for clients access to the data throughout the network
  - A client
    - accesses a copy of the data near to its location
    - opposed to all clients accessing the same central server, (avoid single server bottleneck)
  - *Content types :* web objects, downloadable objects (media files, software, documents), applications, real time media streams, and other components of internet delivery (DNS, routes, and database queries)

3. Content and Services Oriented Networking

- **CAN- versus Content Delivery Networks (CDN)**

- CDN

- The servers aggregate capacity is higher than the network backbone capacity -> impressive increase in the number of concurrent users

- Edge servers should be strategically placed -> decrease the load on interconnects, public peers, private peers and backbones

- CDN can optimally redirect the traffic to edge servers (optimize capacity per customer, provide views of real-time load and statistics, reveal which assets are popular, show active regions and report exact viewing details to the customers)

- **CDNs generally deliver content over traditional TCP/ UDP (no content awareness is supposed to exist in the network nodes)**
  - TCP throughput : impacted by latency , loss, ... -> need that CDNs place servers as close to the edge networks where users are

3. Content and Services Oriented Networking

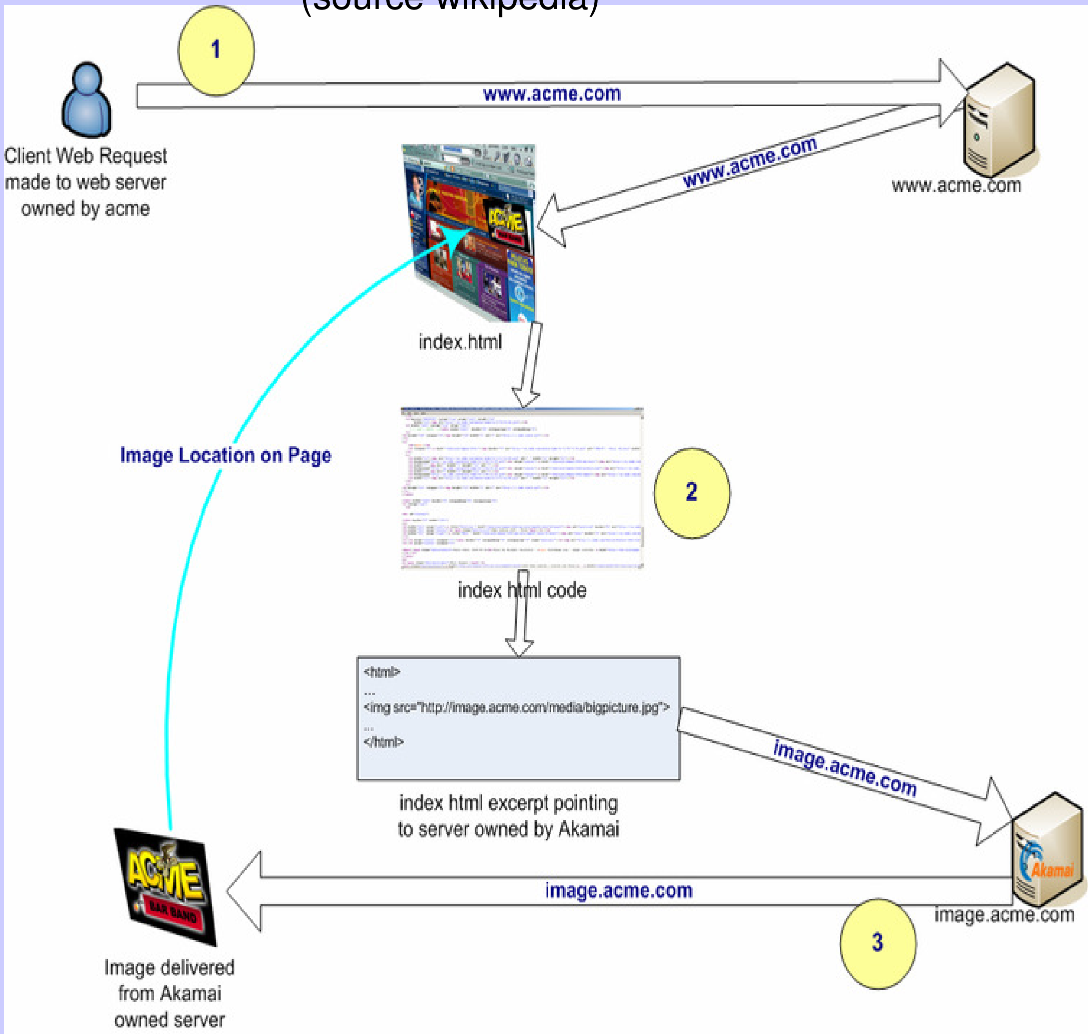
- **CAN- versus Content Delivery Networks (CDN)**
- CDN
- CDN increased reliability: deliver HD quality content with high QoS , low costs and low network load
- CDNs can dynamically distribute assets to strategically placed redundant core, fallback and edge servers
- CDNs can have automatic server availability sensing with instant user redirection
- A CDN can offer 100% availability, even with large power, network or hardware outages
- CDN must provide usage details
  - since the usage logs are no longer available at the content source server after it has been plugged into the CDN
  - the connections of end-users are now served by the CDN edges instead of the content source

3. Content and Services Oriented Networking

- **CAN- versus Content Delivery Networks (CDN)**
- CDN Examples:
- **Free CDNs:**
  - Coral CDN,coBlitz (a subproject of CoDeeN), FreeCast, MediaBlog, PeerCast PPLive, PPStream, QQLive
- **Commercial CDNs:**
  - Akamai Technologies, Amazon CloudFront, CacheFly, CDNetworks (PantherExpress), Chinacache, Cotendo, EdgeCast Networks, Highwinds Network Group, Internap, Level 3 Communications, Limelight Networks, PEER 1, Windows Azure
- **Commercial CDNs using P2P for delivery**
  - BitTorrent, Inc., Internap, Octoshape, Pando, Rawflow, AT&T

Example : AKAMAI access

(source wikipedia)



3. Content and Services Oriented Networking

- CAN + NAA Concepts

  - **Content access is the dominant service requested by the users in today's and FI**

  - Current network layer (routing, transport) do not meet the needs of the content related services.
    - Network services are address-location based : traditional routing and forwarding (OSPF, BGP, ..)
    - The network – is neutral: it has no knowledge related to the content-type which it transport and about some optimisation possibilities

  - Examples:
    - 1. For a portal which may be served by several servers, the DNS may return IP addresses, of multiple servers with same domain name, in a round robin scheme,
    - Neither DNS nor network do not know which server (IP address) is closer and maybe less loaded , given a particular user request
    - **CAN could solve such problems**

    - 2. Content based routing and forwarding: the network
      - can route and forward different type of contents among different routes
      - and can reserve resources without the user or application level signaling

3. Content and Services Oriented Networking

- **CAN + NAA Concepts**
  - CAN overlays existing IP infrastructure
  - It does : filter, forward and transform inter-application messages/data based on their content
  - It moves (partially) application logic and business rules into the network
  - This helps customers to build a more intelligent infrastructure (one that identifies content) routes it efficiently and reduces latency.

  - **Service Provider (SP) Role**
    - Many enterprises may build their own CANs,
    - Others focus on their core businesses and engage SPs to provide and manage them.
    - Content-aware, application-enabled networks are helping SP to reach this objective
    - With moderate capital investment, the networks offer the application-layer services their clients

CAN + NAA Concepts (cont'd)

- Business model entities possible in a Content-based Internet **:**
- basic split:
  - **Content-Based Service Provider (CSP)**
    - locating a content, searching static contents to build a dynamic content, charging information, and content negotiation
    - CSP: e.g. Yahoo, AOL, etc.
  - **Content Provider** - actual creator or owner of the content
  - **Content Consumer**

- **Entity similar to CSP**
  - **(High level) - Service Provider (HLSP)** which offer and manages high level services but uses the content-based transport services from another entity (e.g Content Aware Network Provider - CANP)
  - HLSP and CSP roles can be merged

CAN + NAA Concepts (cont'd)

- **Content Request Distribution**
  - Distributing the requests among servers (further than round robin scheme)
- *Centralised solution:*
  - front end unit to distribute the load
  - requires as much networking resources as collectively required by all nodes, (network bottleneck)
  - Commercial products: Cisco's LocalDirector, Connect-Control by Check Point, Locality Aware Request Distribution (LARD) scheme
-
- *Distributed solutions:*
  - an incoming content request can be received by any server in the cluster
  - servers have new inter-communication protocol to learn the status of other servers
  - each server will determine which other server is suitable (load, content type)
  - no bottleneck (front-end) but horizontal protocol overhead

CAN + NAA Concepts (cont'd)

- **Content delivery /distribution**
- *Multicast content delivery examples*
  - Problem : to serve a static content to a group of users whose requests are received at different times at a content server.
  - Time slot multicast:
    - All users whose requests, for the same content, are received in the same time slot are served in a group
    - The server can create a multicast group and instruct them to join a new multicast group.
    - All users always receive the content from the beginning.
    - Trade-off is needed for selection of the length of the time-slot: waiting-time seen by users versus mcast efficiency
    - CAN approach can support such a service including offering of QoS customised CANs
- *Reliable multicast content distribution*
  - CANs for reliable multicast can be constructed to distribute contents between CSs within the domain of a web portal.
  - Reliable multicast can be used
    - - to push the content from the main server to all other edge servers
    - - to deliver any reliable content to a group of users

CAN + NAA Concepts (cont'd)

Content aware routing and forwarding

- Content-based routing can be used to to direct the request to the most appropriate server (among several distributed at different IP addresses) with intelligence closer to the client.
  - Current DNS mapping based systems do not proceed like this
  - The server distribution may be non-overlapping or it may be complete duplication (often referred to as mirroring).
  - Variants:
    - routes are computed in traditional way but forwarding is choosing the most appropriate one based on content type analysis
    - the routes themselves are computed in a content-based style

CAN + NAA Concepts (cont'd)

- **Location aware content services (LACS)**
  - They offer information about sites/environment "content" based on their location
  - The use of clients location is also helpful for content routing,
    - the I/F to a content aware DNS respond with the IP address of one of the distributed servers closest to the client
  - LACS are useful for a CSP to push contents to customers.
    - e.g. provide up to date info about a customer's environment (e.g traffic data in the visited zone)
  - Problems with providing LACS: no association of IP addresses with the physical location of the content
  - Solution:
    - use of GPS or some other device and this location information is transmitted to the CSP.
    - CSP then processes the location information along with the requested content
    - contacts the content provider (CP) to retrieve the desired content
    - delivers it to the client, or redirects the client to the desired content

CAN + NAA Concepts (cont'd)

- *Security aspects and CAN*
  - IP Security define ways to encrypt data between peer entities thus protecting integrity and privacy of the data
  - The use of IPSec is becoming popular in VPN based services
  - If IPSec is used between peer nodes, intermediate networking nodes no longer have access to the content carried inside an IP packet.
  - This is one of the reasons why CAN cannot be so easy feasible in the core of the Internet
  - However we can solve security issues in a CSP domain such as portal sites.
    - Content distribution involves Front End Servers (FES) and Back End servers (BES) where FES handles all the incoming content requests
  - Possible solution:
    - if CSPs want to use CAN techniques with IPSec, it is advisable that IPSec is terminated at the FES
    - Once FES decrypts and analyzes the content, it is easier to use CAN techniques to route, reserve and charge accordingly

Content-oriented concepts

- Source: J.Choi, Jinyoung Han, E.Cho, Ted Kwon, and Y.Choi,A Survey on Content-Oriented Networking for Efficient Content Delivery, IEEE Communications Magazine • March 2011
- CON node performs ***routing by content names***, not by (host) locators.
  - Identifying hosts is replaced by identifying contents.
  - The location of a content file is independent of its name
- CON has location independence in *content naming* and *routing*
  - and is free from mobility and multi-homing problems
- **Publish/subscribe** is the main communication model in CON:
  - A content source announces (or *publishes*) a content file
  - An user requests (or *subscribes* to) the content file.
  - P/S ***decouples the content generation and consumption*** in time and space, so contents are delivered efficiently and scalably (e.g., multicast/anycast).

- **Content-oriented concepts (cont'd)**
  - **Content naming**
  - **Hierarchical Naming**
  - CCN and others: introduce a hierarchical structure to name a content file.
  - A content file is often named by an identifier like a web URL (e.g. /www.acme.com/main/logo.jpg),
  - → the naming mechanism can be compatible with the current URLbased applications/services, (lower lower deployment hurdle)
  - Hierarchy can help routing scalability (routing entries for contents might
  - be aggregated)
  - Limitation:
    - if content files are replicated at multiple places, the degree of aggregation decreases.
    - components in a hierarchical name have semantics, which does not allow *persistent* naming
      - Persistence : once a content name is given, people would like to access the content file with the same name as long as possible.

CCN: Van Jacobson Diana K. Smetters James D. Thornton Michael F. Plass, Nicholas H. Briggs Rebecca L. Braynard, Networking Named Content, Palo Alto Research Center, Palo Alto, CA, October 2009

3. Content and Services Oriented Networking

- **Content-oriented concepts (cont'd)**
  - **Content naming**
  - **Flat names (DONA, PSIRP)**
    - flat and self-certifying names - by defining a content identifier as a cryptographic hash of a public key.
    - Flatness (a name is a random looking series of bits with no semantics) → persistence and uniqueness are achieved.
    - Limitation:
      - flat naming aggravates the routing scalability problem due to no possibility of aggregation.
      - flat names are not human-readable,--> additional "resolution" between (application-level) human-readable names and content names may be needed.

- *DONA: T. Koponen et al., "A Data-Oriented (and Beyond) Network Architecture," SIGCOMM '07, 2007, pp. 181–92*
- *PSIRP : K. Visala et al., "An Inter-Domain Data-Oriented Routing Architecture," ReArch '09: Proc. 2009 Wksp. Rearchitecting the internet, New York, NY, 2009, pp. 55–60.*

3. Content and Services Oriented Networking

- **Content-oriented concepts (cont'd)**
  - **Content naming**
  - ***Attribute-Based Naming* — CBCB**
  - Identifies contents with a set of attribute-value pairs (AVPs).
  - Since a user specifies her interests with a conjunction and disjunction of AVPs, a CONnode can locate eligible contents by comparing the interest with advertised AVPs from content sources.
  - It can facilitate *in-network searching* (and routing), which is performed by external searching engines in the current Internet.
  - Limitations
    - An AVP may not be unique or well defined.
    - The semantics of AVPs may be ambiguous.
    - The number of possible AVPs can be huge.

- CBCB : A.Carzaniga, M. J. Rutherford, A. L. Wolf, A Routing Scheme for Content-Based Networking, http://www.inf.usi.ch/carzaniga/papers/crw_infocom04.pdf

3. Content and Services Oriented Networking

- **Content-oriented concepts (cont'd)**
  - **Name based routing**
  - CON locate a content file based on its name = *name-based routing*

  - ***Unstructured Routing***
  - Similar to IP routing : assumes no structure to maintain routing tables
  - the routing advertisement (for contents) is mainly performed based on flooding.
    - Example: CCN; it has IP compatibility to a certain degree.
    - CCN might be deployed incrementally with current IP networking.
    - CCN just replaces network prefixes (in IP routing) with content identifiers,
    - (modification of IP routing protocols may not be significant).

  - Network prefixes are aggregatable in IP routing ~ so are hierarchical content identifiers in CCN routing.
  - Limitation:
    - If content file is increasingly replicated or moved, the level of aggregation diminishes.
    - High control traffic overhead (announcement messages if a content file is created, replicated, or deleted)

3. Content and Services Oriented Networking

- **Content-oriented concepts (cont'd)**
  - **Name based routing**

  - ***Structured Routing***
  - **Solutions: tree and a distributed hash table (DHT).**

  - **Tree-based routing scheme (E.g. DONA)**
    - Routers form a hierarchical tree, and each router maintains the routing information of all the contents published in its descendant routers.
    - When a content file is newly published, replicated, or removed, the announcement will be propagated up along the tree until it encounters a router with the corresponding routing entry.
    - Limitation:
      - increasing routing burden as the level of a router becomes higher.
      - the root router should have the routing information of all the contents in the network.
      - Since DONA employs flat content names → scability problem

3. Content and Services Oriented Networking

- **Content-oriented concepts (cont'd)**
  - **Name based routing**

  - ***Structured Routing (cont'd)***
  - **Hierarchical Distributed Hash Tables (PSIRP)**

  - The flatness of a DHT imposes an equal and scalable routing burden among routers.
  - If the number of contents is *C*, each router should have log(*C*) routing entries

  - Limitations:
    - the DHT is constructed by random and uniform placement of routers, and → longer paths than a tree (the latter can exploit the information of network topology).
    - the flatness of a DHT often requires forwarding traffic in a direction that violates the provider-customer relation among ISPs

3. Content and Services Oriented Networking

- **Content-oriented concepts (cont'd)**
  - **Comparison**
  - **Source:** J.Choi, Jinyoung Han, E.Cho, Ted Kwon, and Y.Choi,A Survey on Content-Oriented Networking for Efficient Content Delivery, IEEE Communications Magazine • March 2011

	Naming	Naming advantages	Routing structure	Routing scalability	Control overheads
CCN	Hierarchical	Aggregatable, IP compatible	Unstructured	*N* (best) C (worst)	High
DONA	Flat	Persistent	Structured (tree)	*C*	Low
PSIRP	Flat	Persistent	Structured (hierarchical DHT)	*logC*	Low
TRIAD	Hierarchical	Aggregatable, IP compatible	Unstructured	*N*	High
CBCB	(attribute, value) pairs	In-network searching	Source-based multicast tree	2^A	High

  - N*, C, and* A *are the numbers of publisher nodes, contents, and attributes in the entire network, respectively*

Content-Aware Network: Example 1

- Content Routing Mechanism based on content tagging
  - Source: A. Mitra, M.Maheswaran, Wide-Area Content-based Routing Mechanism, International Parallel and Distributed Processing Symposium (IPDPS'03)

  - Wide area network environment
  - Content Clients, Content Servers distributed at the edge of a network

  - Clients are requesting content

  - The requests for content are steered by *content routers* (examining dest but also also *content descriptors – e.g.* such as URLs and cookies
  - In the current CDN, content routing is confined to selecting the most appropriate back-end server in virtualized web server clusters

  - The architecture: based on tagging the requests at ingress points
    - The tags incorporate several different content attributes and are used in the in the routing process.

3. Content and Services Oriented Networking

- Content-Aware Network: Example 1
- Content Routing Mechanism based on content tagging
- Wide-Area Content-based Routing Mechanism (cont'd)

  - Content-based routing architecture: *protocol independent content switching* (PICS).
  - Client and server sites – linked through an overlay -*virtual content network* (VCN)
  - The client and server sites connect to the VCN using GWs (called content-based routers).
    - *content edge routers* (CERs).-placed at the outer edge of the VCN first examine the content
    - VCN interior : *content-based switching routers* (CSRs)

    - the client or server sites can connect to the VCN, via multiple CERs (load balancing + preventing single-point failures)
    - CERs
      - are responsible for characterization and classification of content
      - encapsulate the incoming packets using a content header containing a content derived tag uniquely identifying a content within the VCN
    - The CSRs at the VCN's core steer the content requests from the ingress CER to the egress CER based on the tags in the content header
      - CSRs are Tag based switches that support a single forwarding component (i.e., algorithm for tag-based forwarding)

3. Content and Services Oriented Networking

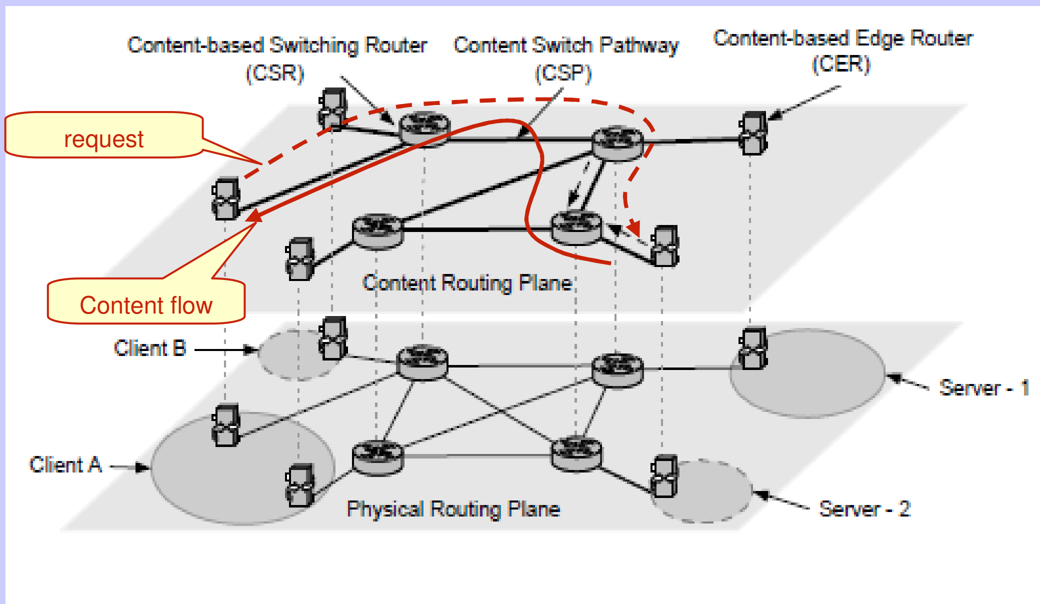
- Wide-Area Content-based Routing Mechanism (cont'd)
- Virtual content network
  - A content request arrives to a ingress CER
  - Ingress CER identifies the content and tag it

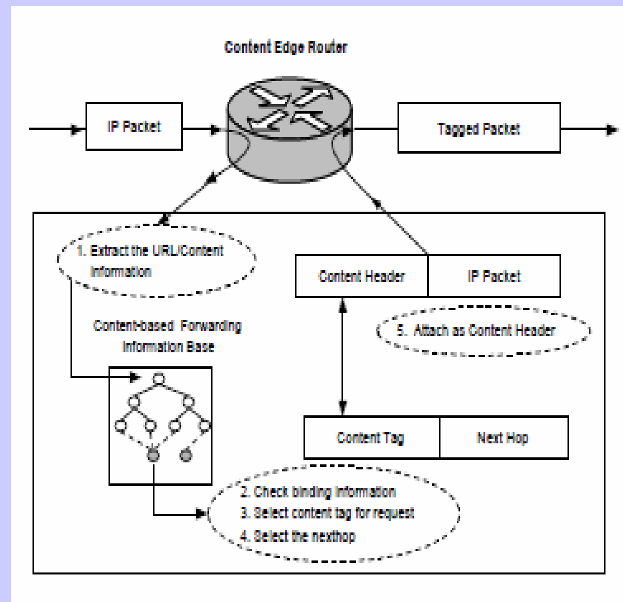
  - The CERs extract the content descriptors (e.g URLs, cookies, etc.) from the requests and use a *content-based forwarding information base* (CFIB) to determine the corresponding content derived tag, (content-to-tag bindings)
    - The tag is generated by a combination of content and policy information
    - CFIB is organized hierarchically based on the popularity of the content to enhance the scalability
    - The CFIB is reorganized periodically by the *content classification* process to reflect additions and deletions in content subscriptions

  - The content classification process leverages the properties of the content identified by the *content characterization* process
  - The content classification process uses the content attributes
  - to create *content equivalence classes* (CECs)
  - The IP packet is encapsulated with a content header at the ingress CER
  - and is restored by the egress CER

3. Content and Services Oriented Networking

- Wide-Area Content-based Routing Mechanism
- Virtual content network topology example
  - CSRs
    - maintain content based forwarding tables
    - do not have any content-to-tag binding information (they are tag switches)
    - assume that the appropriate tags are already created by the CERs.
    - use the content-based forwarding tables to steer the requests toward the appropriate server side CER.
- Note: the proposed technique is similar to MPLS where the LSP is replacing CSP





Source: A. Mitra, M.Maheswaran, Wide-Area Content-based Routing Mechanism, International Parallel and Distributed Processing Symposium (IPDPS'03)

3. Content and Services Oriented Networking

- Wide-Area Content-based Routing Mechanism
- Virtual content network topology example

  - Content characterisation
    - Process that identifies the content key attributes
    - Used to to generate content description and its resource reqs
    - A content profile is defined *a priori* to the routing process.
    - used to locate the content and also allows the routing protocol to infer those characteristics that directly affects the content delivery mechanism (e.g., bandwidth required for delivery, client QoS reqs.etc.).

  - Possible two distinct classes of attributes:
    - Structural class : their values are known prior to the routing process and can be used to create content description, a priori, which is then used to discover content on a network.
    - Semantic class: are initialized only at the time a request for the content is submitted and is used for accessing the content.
  - A combination of them decides the network resources to be allocated for a request

3. Content and Services Oriented Networking

- Wide-Area Content-based Routing Mechanism (con'd)
- Virtual content network topology example

  - Content characterisation:
  - **Physical:** size, version, modification date, ownership permissions, copyrights, author
  - **Name-based** filename, location name, URL, origin server name
  - **End data type:** HTML, cookies, scripts, audio/video
  - clips, text
  - **Popularity** temporal, spatial

  - **Access :** duration, streaming, non-streaming,
  - variable-bit rate, constant-bit rate,
  - adaptive-bit rate
  - **Quality of service** bandwidth, delay,
  - loss tolerance
  - **Document Type** static, dynamic

Content-Aware Network: Example 2

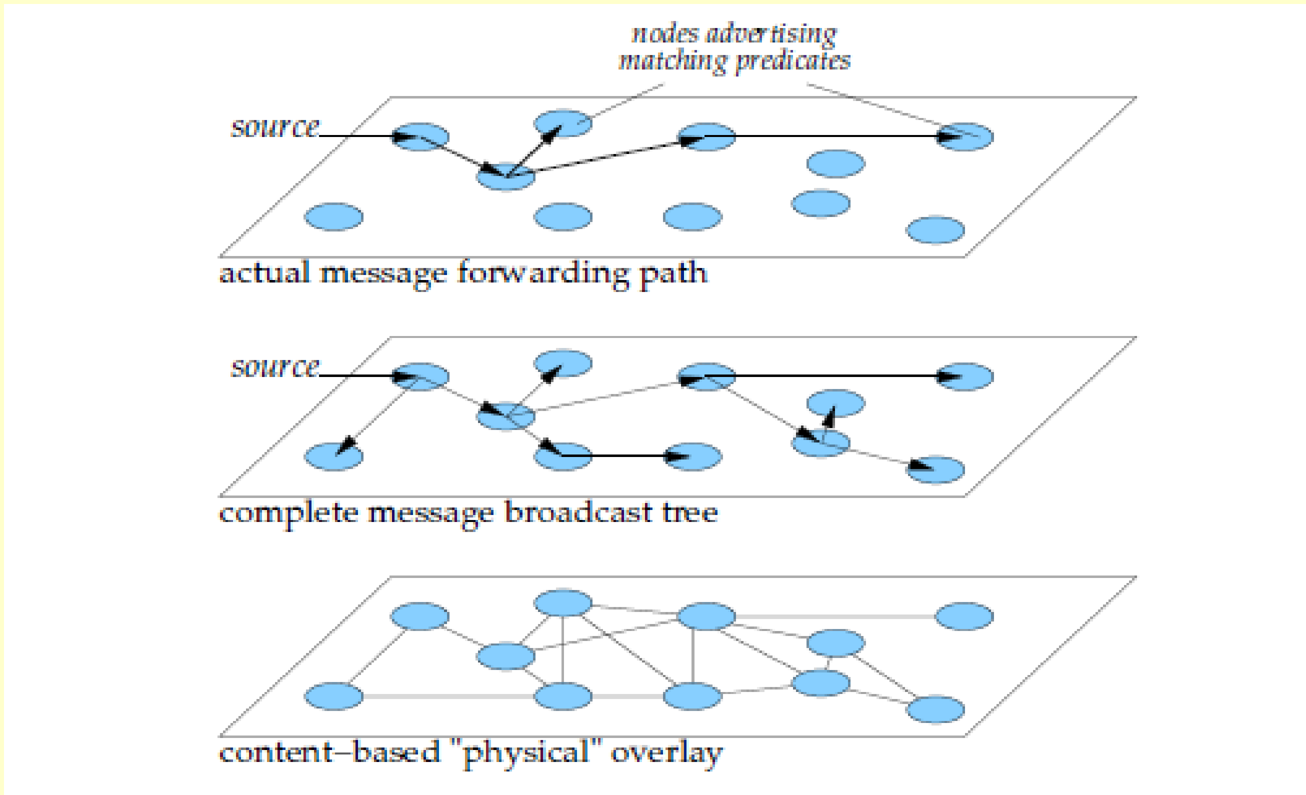
- Source: A.Carzaniga, M. J. Rutherford, A. L. Wolf, A Routing Scheme for Content-Based Networking, http://www.inf.usi.ch/carzaniga/papers/crw_infocom04.pdf

- Content-based communication service example: datagram, connectionless service, through a *content-based network*
- content-based network as an overlay point-to-point network.
- Routing in a content-based network
  - synthesizing distribution paths throughout the network
  - forwarding : determining at each router the set of next-hop destinations of a message

- Solution: ***combined broadcast and content-based (CBCB)*** routing scheme.
  - content-based layer over a traditional broadcast layer
  - The broadcast layer handles each message as a broadcast message
  - the content-based layer prunes the broadcast distribution paths, limiting the propagation of each message to only those nodes that advertised predicates matching the message

Content-Aware Network: Example 2 (cont'd)

- Network Overlay and High-Level Routing Scheme



- Source: A.Carzaniga, M. J. Rutherford, A. L. Wolf, A Routing Scheme
- for Content-Based Networking,
- http://www.inf.usi.ch/carzaniga/papers/crw_infocom04.pdf

- **Content-Aware Network: Example 2 (cont'd)**

- A router runs two protocols :
  - a *broadcast routing* protocol
  - a *content-based routing* protocol.
-
- The broadcast protocol
  - creates a broadcast tree:
    - processes topological information
    - maintains the forwarding state necessary to send a message from each node to every other node.
  - There is a broadcast layer to execute broadcast tree construction
    - common broadcast schemes can be used maybe slightly modified
    - Implementation : global spanning tree protocol, per-source minimal-paths spanning trees, or reverse-path broadcasting.

- **Content-Aware Network: Example 2 (cont'd)**
- The content-based protocol
  - processes *predicates advertised by nodes*,
  - maintains the forwarding state - to decide, for each router I/F whether a message matches the predicates advertised by any downstream node reachable through that interface.
- is based on a *dual push/pull* mechanism that guarantees robust and timely propagation of CB routing information

- **Message content**: structured as a set of attribute/value pairs, and a selection logical predicate (disjunction of conjunctions) of elementary constraints over the values of individual attributes
- Example: a message might have the following content
  - [class=alert, severity=6, device-type=web-server, alert-type=hardware failure]
- This content matches a selection predicate e.g. :
  - [alert-type=intrusion ^ severity>2 U class=alert ^ device-type=web-server]

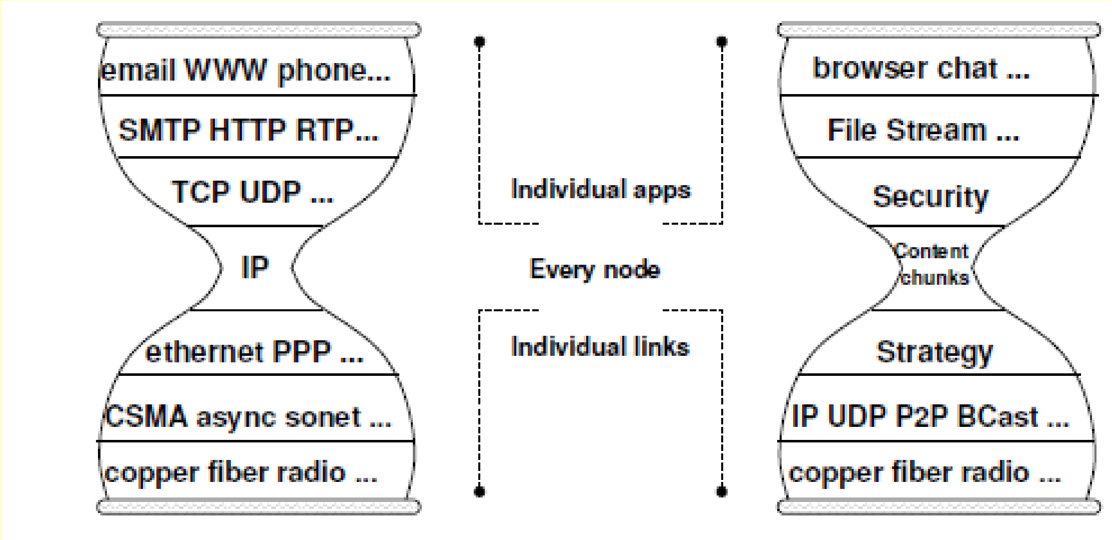
3. Content and Services Oriented Networking

- Content Centric Networking
- Source: Van Jacobson Diana K. Smetters James D. Thornton Michael F. Plass, Nicholas H. Briggs Rebecca L. Braynard, Networking Named Content, Palo Alto Research Center, Palo Alto, CA, October 2009

- **CCN Concepts**
  - Current network evolve mainly to content distribution and retrieval
  - Traditional networking technology still uses connections based on hosts locations
  - Accessing content and services requires mapping from the *what* that users care about to the network's *where.*
  - CCN proposes to treats content as a primitive – *decoupling location from identity, security and access, and retrieving content by name*
  - *Routing named content*, (derived from IP), allows to achieve scalability, security and performance
  - New architectures are proposed to demonstrate new features of the CCN

CCN concepts (cont'd) Example 1

CCN transformation of the traditional network stack from IP to chunks of named content



Traditional TCP/IP stack → CCN

Source: Van Jacobson Diana K. Smetters James D. Thornton Michael F. Plass, Nicholas H. Briggs Rebecca L. Braynard, Networking Named Content, Palo Alto Research Center, Palo Alto, CA, October 2009

- **CCN Concepts** (cont'd)
  - Most layers of the traditional stack horizontal bilateral agreements/protocols (Node to node, end to end)
  - Network layer : the only one requiring universal agreement
  - IP's success:
    - It is simple (thin 'waist' of the stack)
    - flexible (dynamic routing)
    - Low demand from layer 2: stateless, unreliable, unordered, best-effort delivery.
  - **CCN's network layer is similar to IP**
    - it makes fewer demands on layer 2, giving it many of the same attractive properties.
    - (+): CCN *can be layered over anything,* including IP itself.

3. Content and Services Oriented Networking

- **CCN Concepts (cont'd)**
  - CCN specific features- different from IP
  - Strategy and security: new layers
  - CCN
    - can use multiple simultaneous connectivity (e.g., Eth., 3G, 802.11, 802.16, etc.) due to its simpler relationship with layer 2.
  - The strategy layer
    - *makes the fine-grained, dynamic optimization* choices needed to best exploit multiple connectivity under changing conditions
  - CCN
    - *secures content itself* rather than the connections over which it travels
    - thereby avoiding many of the host-based vulnerabilities that exist in IP networking

- **CCN Concepts (cont'd)**
  - CCN node model
    - CCN communication is driven by the data consumers
    - CCN packet types
      - Interest packet (InP) ("Querry" for content)
      - Data (DP) (carry the actual content)
    - **CCN high level description)**
      - The consumers broadcast their interest for some content
      - Any node hearing the *Interest* and having the required content can respond with *Data* packet
      - *Data* are transmitted as a response only to an interest and consumes this *interest (1-to- 1 relationship Interest-data)*

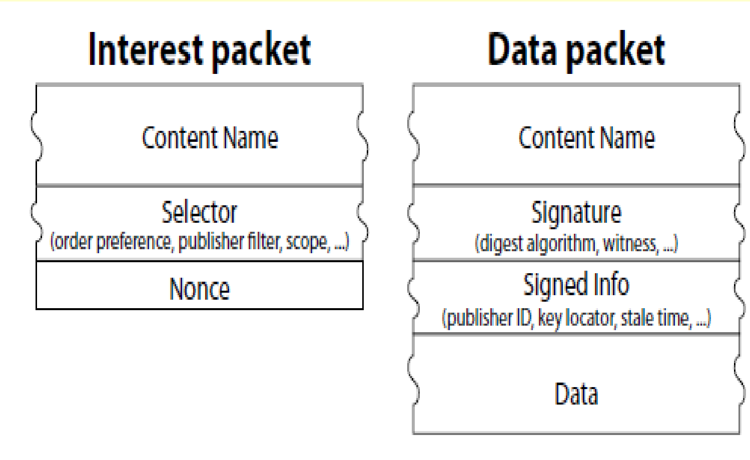
CCN node model (cont'd)

- Multiple nodes interested in the same content may share the Data packets: CCN is naturally multicast enabled

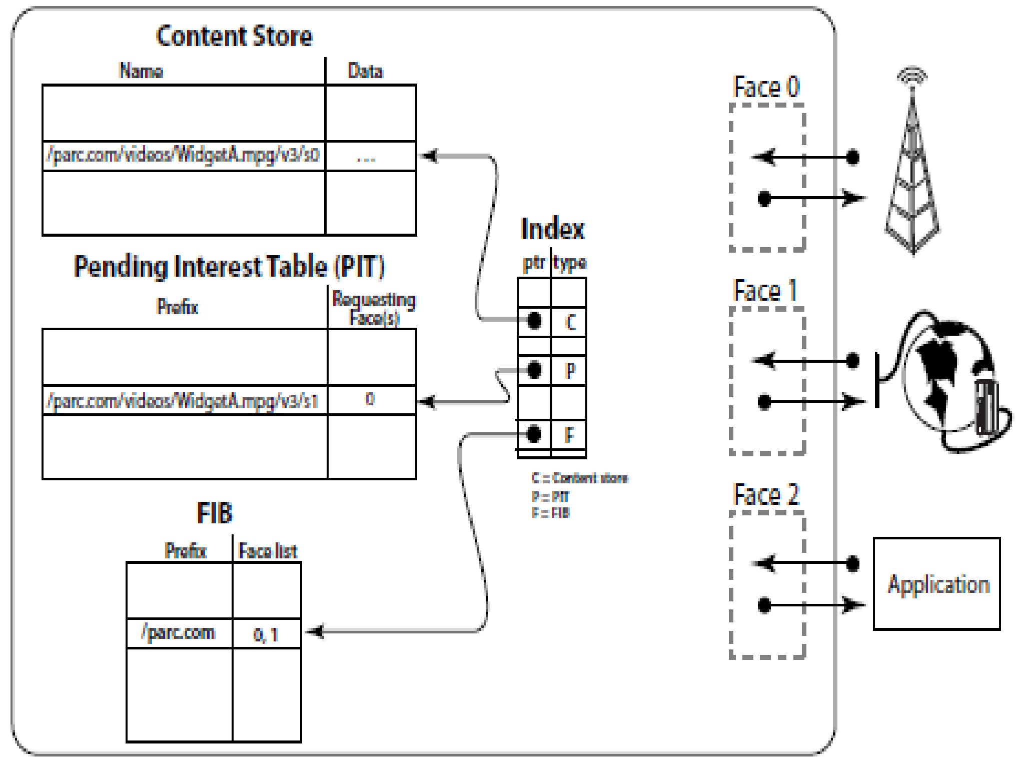
- Content characterisation:
  - Data 'satisfies' an Interest if the *ContentName* in the InP is a prefix of the *ContentName* in the DP
  - CCN names :opaque, binary objects composed of an (explicitly specified) number of components
  - Hierarchical structure of names => the above prefix match is equivalent to : the DP is in the *name subtree* specified by the InP
  - Similarity wit hierarchical structure of IP addresses ((net, subnet, ..)
  - Name prefixes can be context dependent (e.g. *"This building/this_room*")

3. Content and Services Oriented Networking

- **CCN node model (cont'd)**



CCN Packet types



CCN Forwarding Engine Model

Source: Van Jacobson Diana K. Smetters James D. Thornton Michael F. Plass, Nicholas H. Briggs Rebecca L. Braynard, Networking Named Content, Palo Alto Research Center, Palo Alto, CA, October 2009

- CCN node model (cont'd)

- CCN Forwarding engine
  - FIB (Forwarding Information Base)
  - CS (Content Store – i.e. buffer memory)
  - PIT (Pending Interest Table)
  - FIB
    - used to forward an InP towards potential (sources)
    - Similar to IP FIB
    - But admits several I/Fs
      - multiple sources that can act in parallel
      - CCN is not limited to the spanning tree as in IP routing
  - CS
    - Same as buffer memory in IP router
    - stores the DPs to be used in the future by other recipients (difference from IP router which forgets a packet after it has been forwarded)
    - It has a different replacement policy
    - Allows "caching" at every node – depending on its capabilities
    - Content delivery performance is increased

- **CCN node model (cont'd)**

- **CCN Forwarding engine**
- Pending Interest Table (PIT)
  - Stores the pending requests for content, i.e
  - It keeps track of InP forwarded upstream toward content source(s) so that returned Data can be sent downstream to its requester(s)
  - In CCN the routes are computed for InP packets only, (when they propagates upstream towards the data sources)
  - Each unsolved InP is stored in PIT, so the DPs will be forwarded on the reverse (towards the requester(s) path when they come
  - Basic operation at a CCN node-
    - similar to IP node (router) done performing forwarding phase
  - Packet arrives on an I/F (InP or DP)
    - (note that in original source) these are named *faces* – as to emphasize their logical roles – an I/F can be in the same machine towards an application
    - Longest match look-up is performed based on its *ContentName*
    - Appropriate actions are done based on the result

3. Content and Services Oriented Networking

- **CCN node model (cont'd)**
- **Basic operation at a CCN node**
- **InP packet arrives**
  - Longest match lookup is done based on its ContentName
  - **Priorities of the search: CS, PIT, FIB**
  - If there is a DP in the Content Store that matches the InP
    - Then it will be sent in the reverse direction on the I/F the InP arrived
    - Discard the InP (solved)
  - Otherwise: If there is an exact match to to PIT,
    - then a new I/F is added to the pending list
    - And the InP is discarded (similar to IGMP working in multicast)
  - Otherwise: If a FIB matching is found
    - then the request (InP) is sent upstream towards the data source(s)
    - On all I/Fs except the input I/F
  - If no match for InP then discard

- **CCN node model (cont'd)**
- **Basic operation at a CCN node**
- **Data packet arrives**
  - DPgenerally follows the route back conforming the PIT information
  - Longest-match lookup is done at DP arrival on its Content Name
  - CS match => DP is a duplicate, discard
  - PIT match (there can be more that one) =>
    - Data validation (security)
    - Data are added to the CS (caching)
    - Data are sent towards the pending entities (list in PIT)
    - The PiT- corresponding pending requests are solved (erased)
  - In CCN each new packet of data is sent only after a new interest is expressed
    - This approach is similar to TCP ACKs(giving a new window to the transmitter) + Data packets
    - Senders are stateless, so retransmission if necessary is requested by the application (the strategy level has the task to determine the policies)
    - CCN has in such a way a flow control mechanism

- CAN/CCN and Virtualisation
- **Network Virtualisation- Example 1**
  - **Source : N. M. Mosharaf Kabir Chowdhury and Raouf Boutaba “Network Virtualization:State of the Art and Research Challenges”, IEEE Commm Magazine, July 2009**

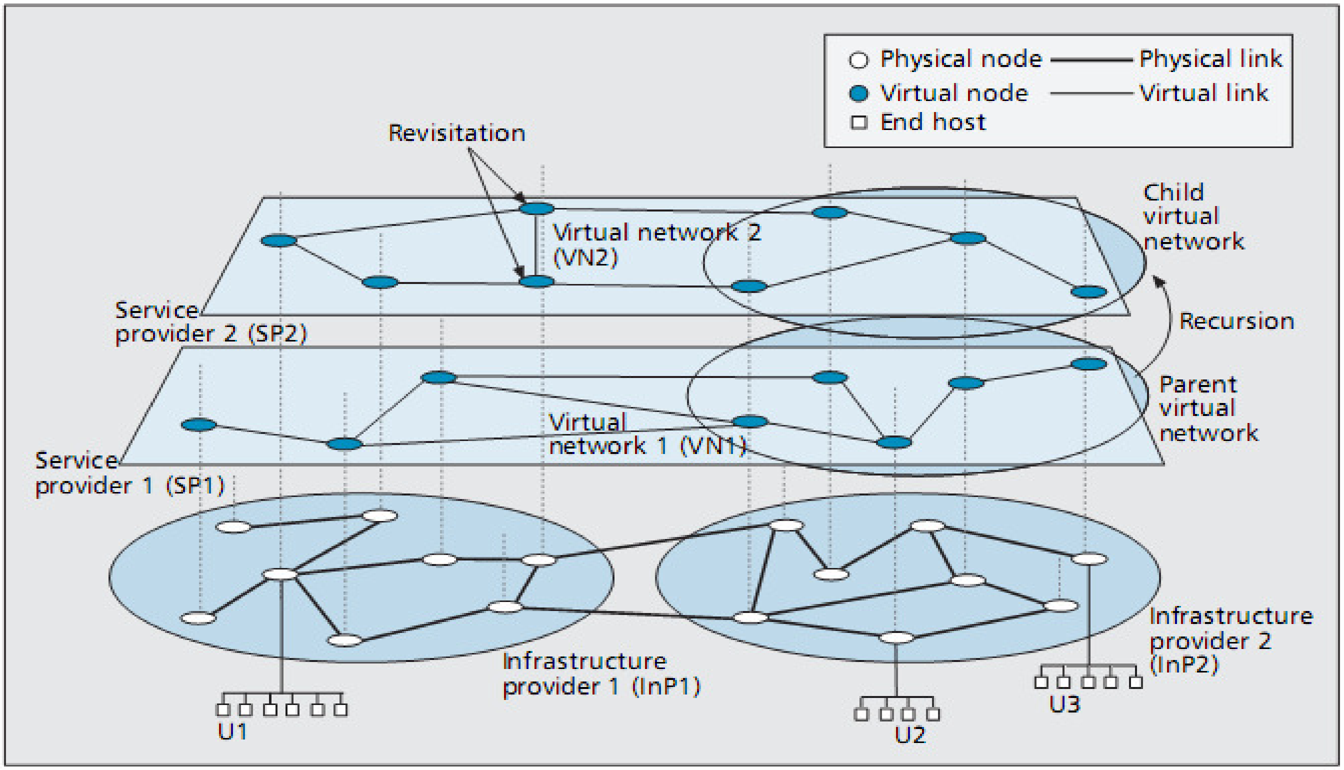
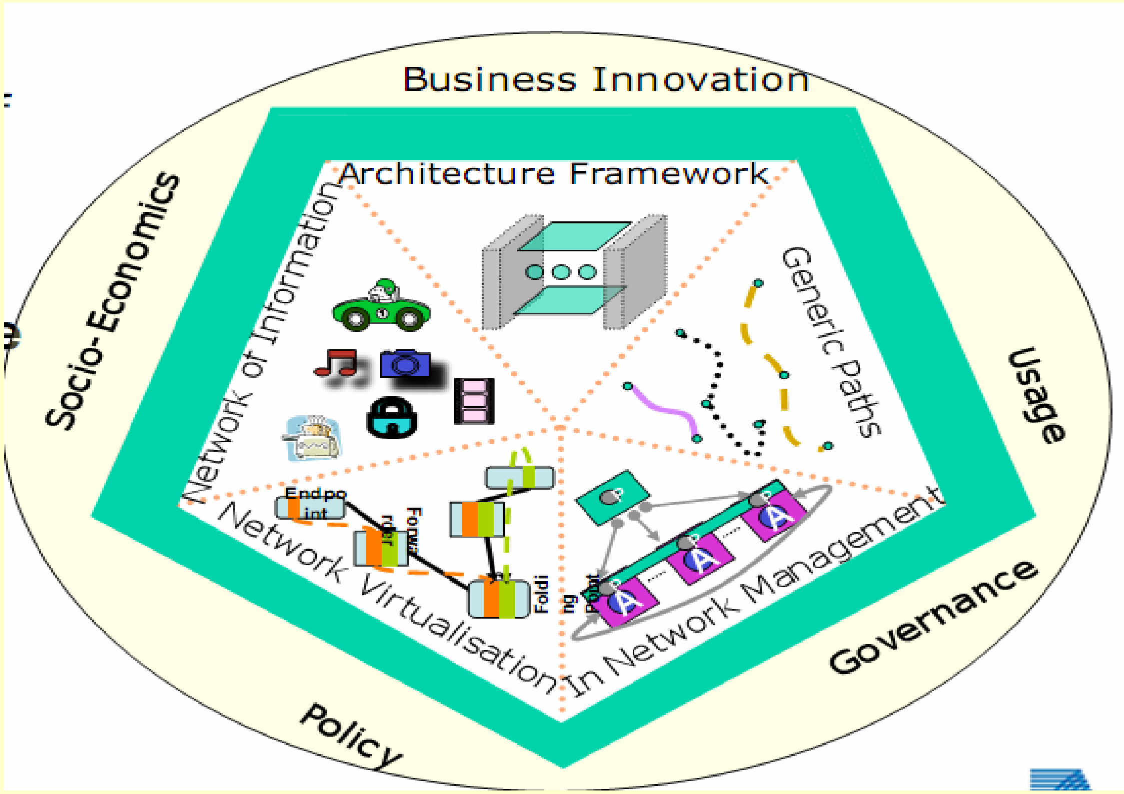


Figure 1. *Network virtualization environment.*

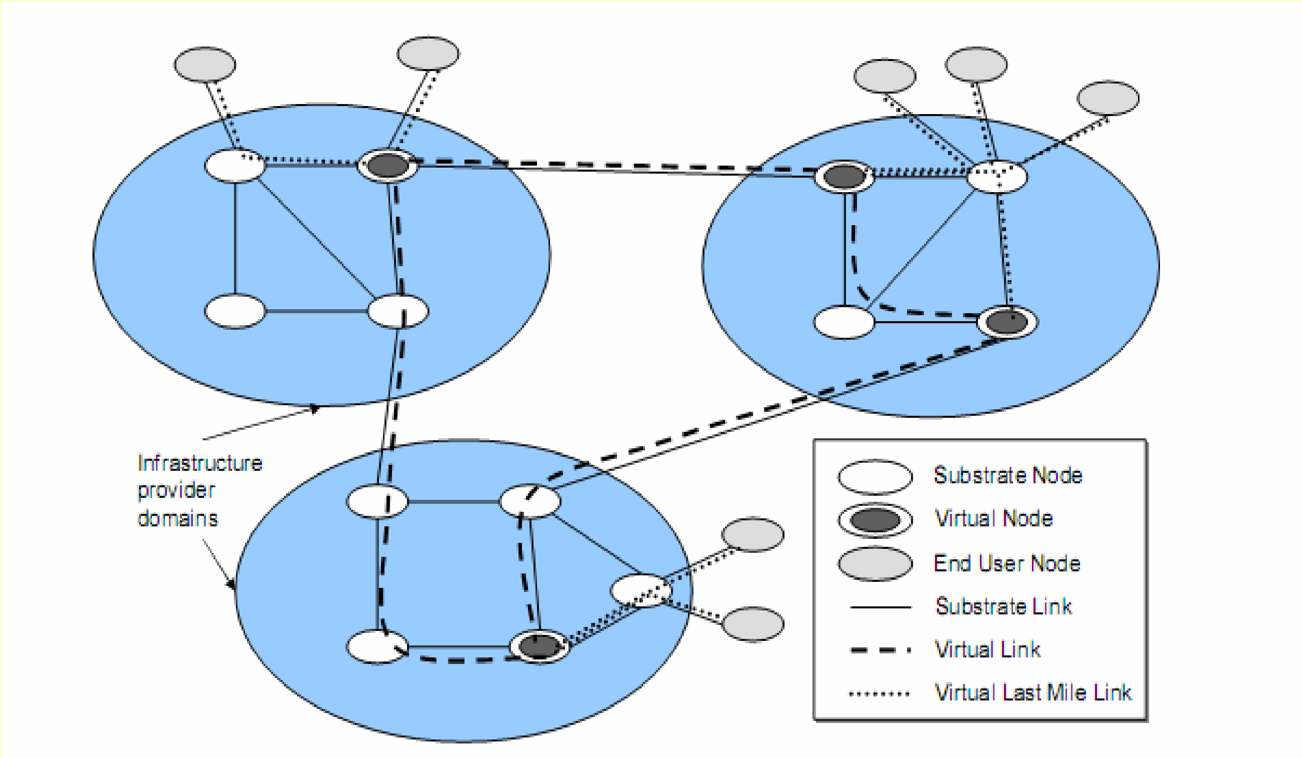
3. Content and Services Oriented Networking

- **CAN/CCN and Virtualisation**
- Example of an European project using full virtualisation (Data Control and Management Plane):
- 4WARD A clean slate approach for Future Internet, FP7 IP Project (2008-2009)



Source: …Abramowicz,H. Introduction to BIRD WS, http://www.4ward-project.eu

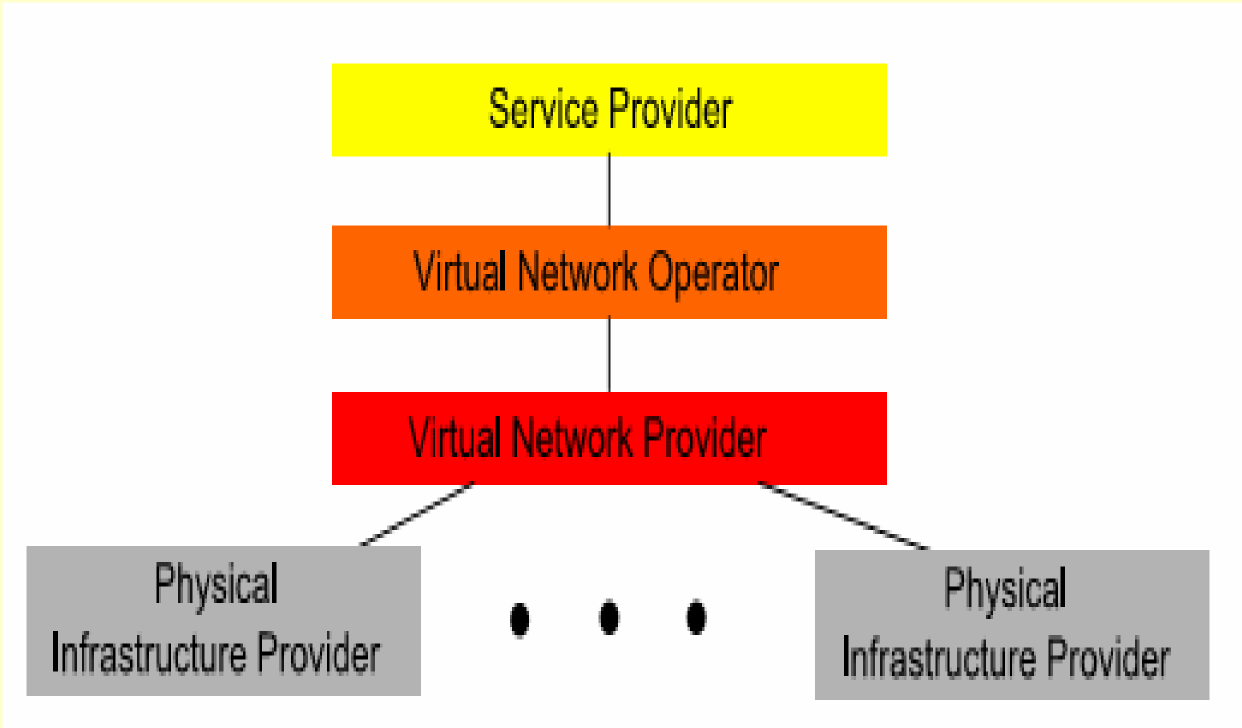
- **CAN/CCN and Virtualisation**
- **Example of full virtualisation**
- Overview of a virtual network topology and substrate networks



R.Bless, C.Werle, Control Plane Issues in the 4WARD Network Virtualization Architecture, Electronic Communications of the EASST Volume 17 (2009)

3. Content and Services Oriented Networking

- 4WARD Main approach : virtualisation
- New business entities needed:

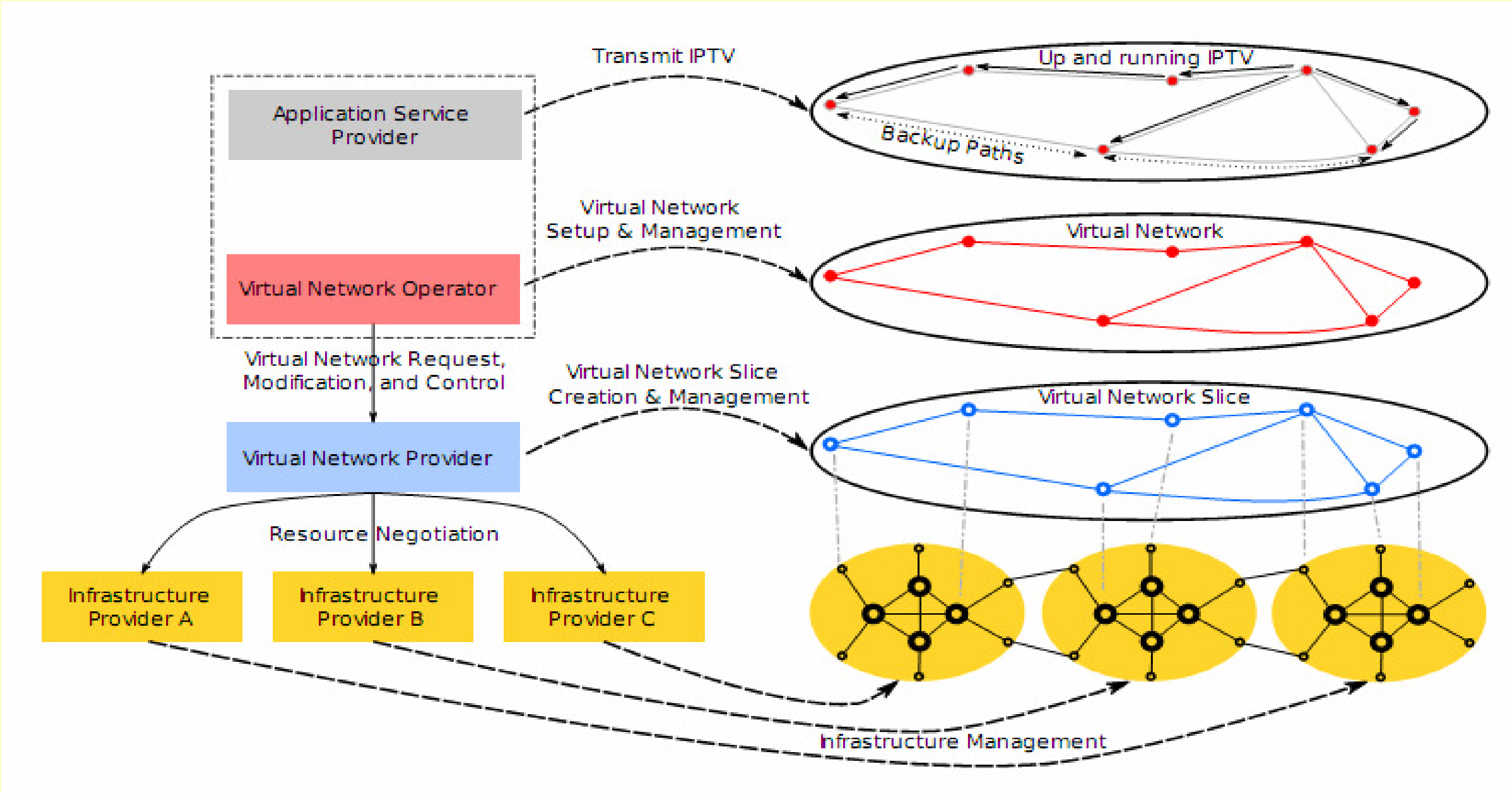


Source: L.M. Correia and L.Lundgren-editors, *Going 4WARD Newsletter,* 4WARD- Architecture and Design for the Future Internet May 2009, Issue No. 4

3. Content and Services Oriented Networking

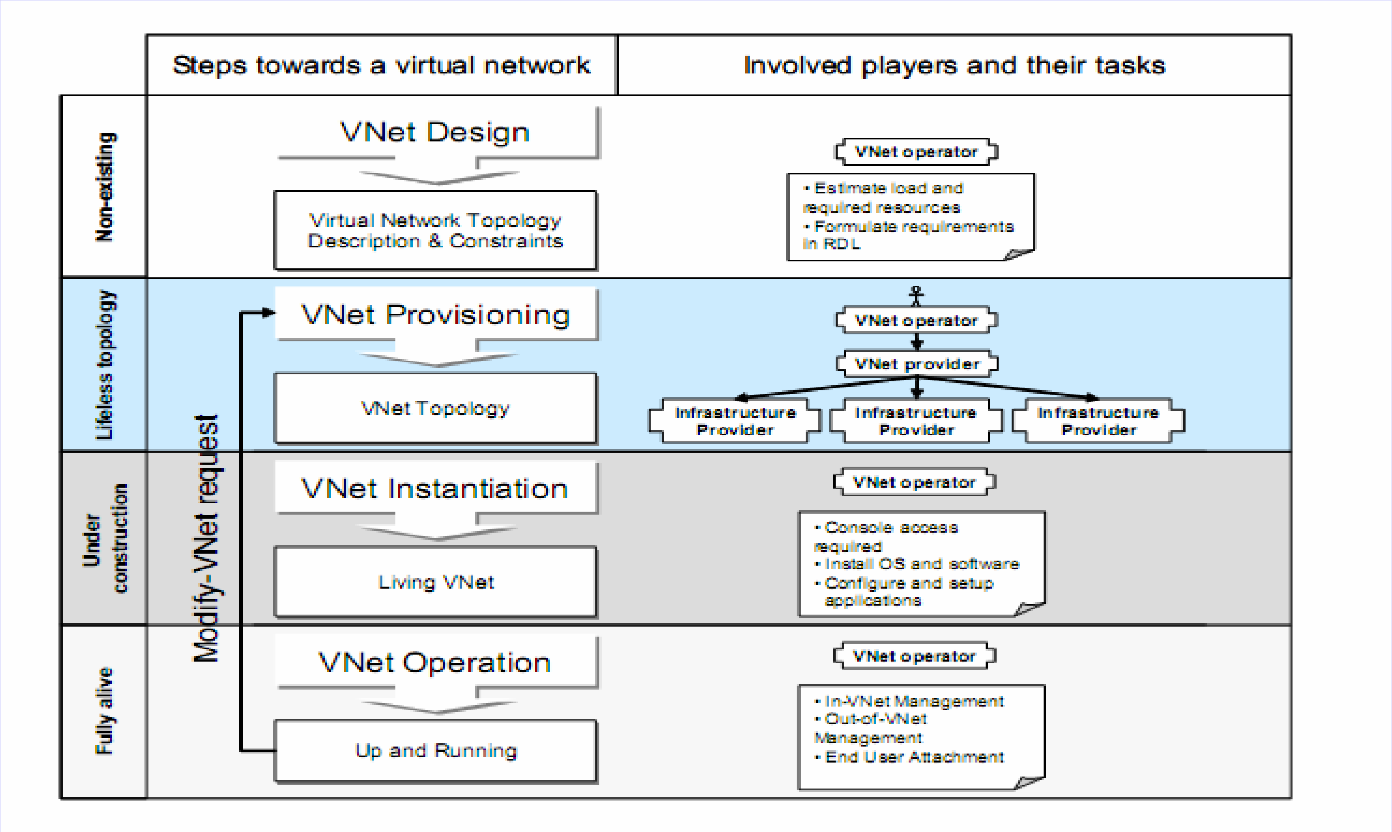
- 4WARD- Business entities
- **Physical Infrastructure Provider (PIP)** : owns and manages the PHY infrastructure (the substrate), and provides wholesale of raw bit and processing services (also known as slices), which support network virtualisation
- **Virtual Network Provider (VNP):** assembles virtual resources from one or multiple PIPs into a virtual topology
- **Virtual Network Operator (VNO)** initiate installation and then performs operation of a VNet over the virtual topology provided by the VNP according to the needs of the SP (realises a tailored connectivity service)
- **Service Provider (SP):** constructs, advertises and offers high level services to the customers/users

- 4WARD- Business entities (cont'd)
- Service Providers (SP) use the VNets to offer their services
  - value-added services (SPs act as ASP)
  - or transport services (SPs act as NSP)
- VNP : new business role (it does not exist in today's economic structure)
  - enable the layer of indirection that virtualisation is providing.
  - Notes: The above roles must be understood as a technical concept, while:
    - a single business entity could perform more than one task, e.g., one company can be PIP and VNP at the same time
    - or VNP and VNO could coincide
  - The 4WARD separation concept allows VNets to have properties and guarantees not currently available in today's Internet.

- 4WARD- Business entities (cont'd)
- 

Source: R.Bless, C.Werle, Control Plane Issues in the 4WARD Network Virtualization Architecture, Electronic Communications of the EASST Volume 17 (2009)

- 4WARD- Business entities (cont'd)
  - VNet Lyfe cycle overview



Source: R.Bless, C.Werle, Control Plane Issues in the 4WARD Network Virtualization Architecture, Electronic Communications of the EASST Volume 17 (2009)

CONTENTS

.

4. CAN Architecture example

- **ALICANTE**, 2010-2013, Integrated Project (IP): MediA Ecosystem Deployment Through Ubiquitous Content-Aware Network Environment- *FI oriented project*
- *http://www.ict-alicante.eu/*
- *19 European partners*
  - *Industry, SME*
  - *Operators*
  - *Universities*
  - *Research groups*

4. CAN Architecture example

- Applying new concepts (Future Internet – oriented):
  - **Networked Media**
  - **Content Aware Networking & Network Aware Application**
  - **Evolutionary architecture** for networked media systems

- Media services management and network resources management
- Novel virtual *Content-Aware Network (CAN)* layer
  - Content-Awareness delivered to Network Environment
  - Network- and User Context-Awareness to Service Environment
  - Assuring Quality of Services (QoS), security, etc. for media-oriented services

- **ALICANTE general objectives:**
  - End users
    - efficiently access multimedia services in various contexts
    - consume, share, generate audiovisual content
  - Providers (high level services, connectivity services)
    - extend their range of services
    - service large number of users
    - efficiently manage their high level services and /or network resources
  - Flexible cooperation between providers, operators and end-users

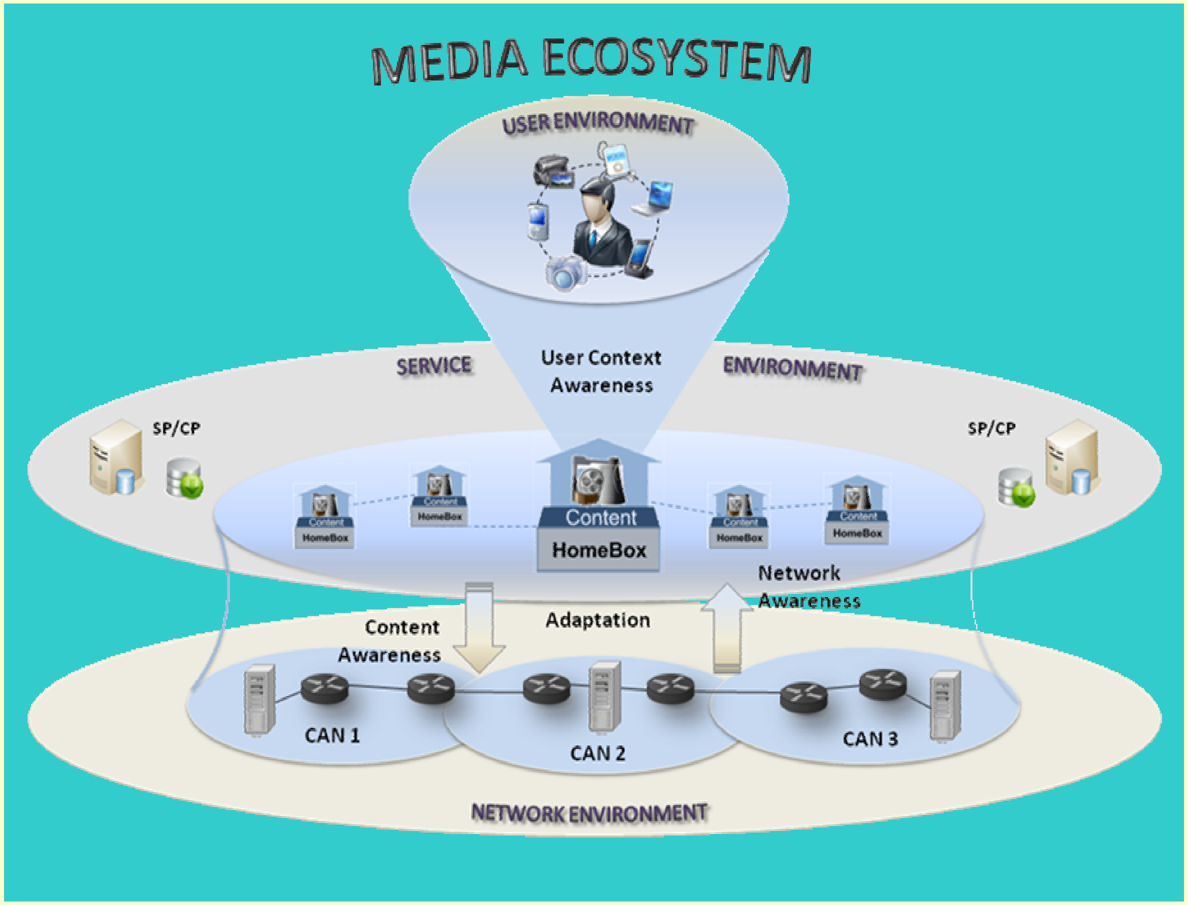
- This presentation :
  - concepts and architecture: emphasis on virtual network layer (i.e., CAN)
  - exposing its role and interfaces among overall system layers.

4. CAN Architecture example:

▪ **ALICANTE-** High level architectural view

- **Environments:**
- *User (UE)* : End-Users terminals
- *Service (SE):* Service and Content Providers
- *Network (NE)*, CAN Providers, Network Providers

"Environment ": groups of functions defined around the same functional goal and possibly spanning, vertically, one or more several architectural (sub-) layers.



4. CAN Architecture example

- **ALICANTE specific objectives:**

- Business Model (BM):
- *flexible and open business model* (BM), FI oriented, supporting single or multiple roles of the business actors
- *rich set of (high) level services* (single or composite), mainly *media and content-oriented*
  - various modes of communication (unicast, multicast, broadcast, P2P and combinations, synchronous/asynchronous)
  - different levels of QoS/QoE, availability, security, etc.
  - *Service mobility* is also a target

- Flexible BM:
  - EU may act as content consumers/providers
  - May benefit from a friendly and flexible *User environment* seamlessly interacting with the underlying layers
  - *preserve the independency of business actors*
    - in terms of managing their resources and protect the ownership,
    - while offering a framework for their cooperation

4. CAN Architecture example:

ALICANTE specific objectives (Cont'd) :

- Architectural:
- *middle-way architecture* : *CAN/NAA* coupling, extendable both at service level and network/ transport level
- support integration
  - *vertical* (based on CAN/NAA) of high level services and connectivity ones,
  - *horizontal integration* on top of single or multiple-domain IP networks.
- network virtualization techniques is applied
  - to create parallel *content-aware virtual planes*
    - enriched in terms of functionality (due to content –awareness)
    - represented by *Virtual Content Aware Networks (VCAN)*
    - spanning single or multiple IP domains

4. CAN Architecture example:

ALICANTE specific objectives (Cont'd) :

- Architectural (cont'd):
- *open architecture,* to support cooperation
  - at high level services : with other existing / future systems (IMS, CDN, etc.)
  - at connectivity services level with traditional core and access network providers

- introduce *distributed intelligence in network nodes*
  - (unlike the traditional TCP/IP architecture)
  - by developping CA features
    - in *new core network elements* (new routers)
    - and *Home Boxes* (peripheral gateways)
  - while preserving the compatibility of inter-working with traditional network elements.

4. CAN Architecture example

- ALICANTE specific objectives (Cont'd) :
- Service and Network Management and Control:
- a management and control system
  - orchestrating a multi-domain and multi-provider assembly
  - while cooperating with traditional service and network managers of ISPs
  - however the system is a distributed one

- powerful and *efficient resource management* system
  - *clearly delimitate the roles and responsibilities* of different cooperating actors, by defining dynamic Service Level Agreement-type interactions between entities
  - monitoring in real time the fulfillment of these SLAs
  - combining statically/dynamically
    - resource *provisioning* techniques
    - with new *media flows adaptation* techniques

4. CAN Architecture example

ALICANTE specific objectives (Cont'd) :

- Service and Network Management and Control (cont'd):

- offer *guarantees and satisfaction to the EU/providers*
  - and deliver to EU info on status of his/her communication session and possibilities to measure the QoS/QoE
  - these will be supported by a *hierarchical monitoring system* at service and network level

- take benefit at network level from mature network level technologies
  - e.g. MPLS,, DiffServ, routing, multicast, etc.
  - to solve the network level tasks, under control of the ALICANTE management and control sysyem

4. CAN Architecture example:

Business Model

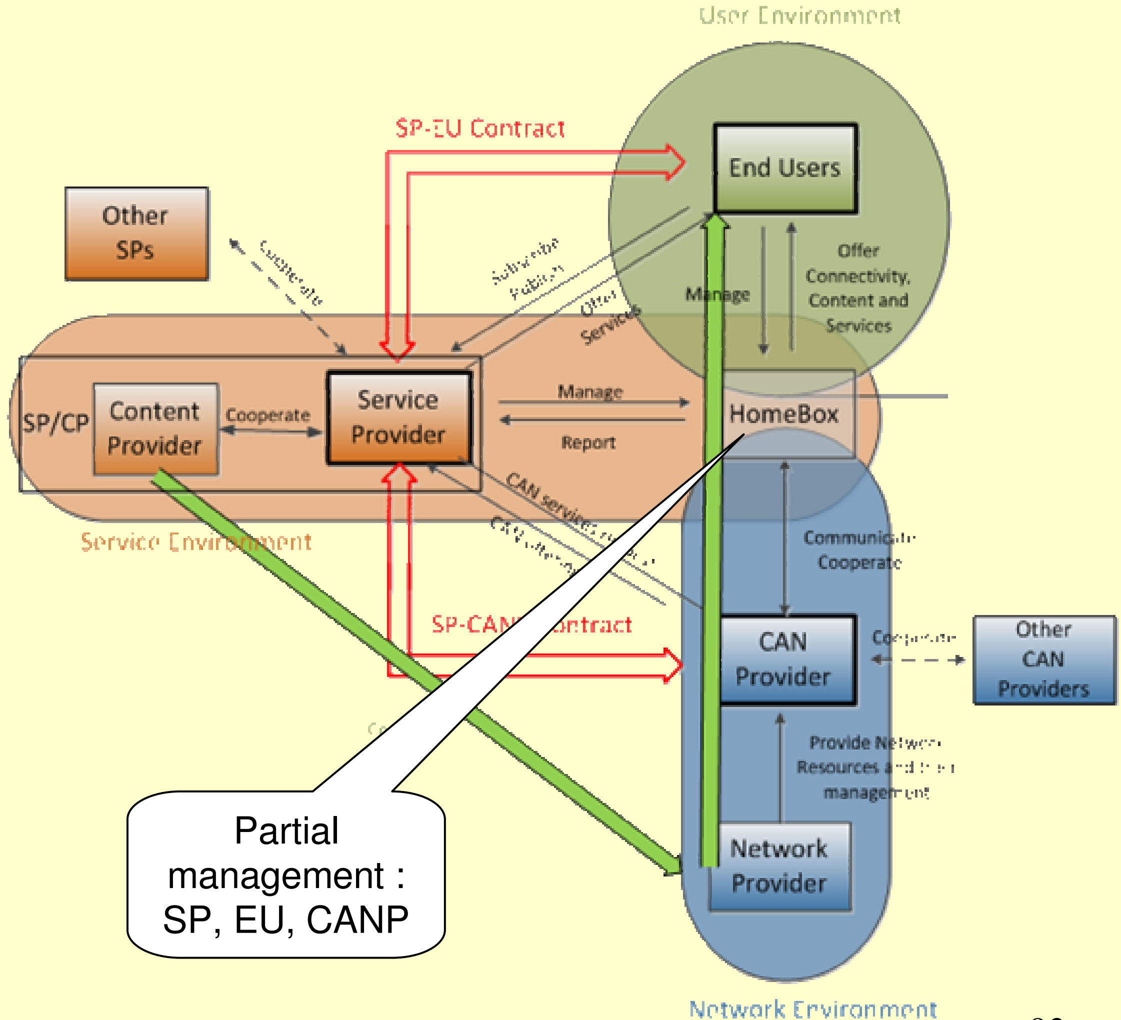
Business Actors:

- *End-User (EU)*
- *Content Provider* (CP)
- *Service Provider* (SP)
- *Network Provider* (NP)
- *CAN Provider (CANP) (new)*

Cooperation, interaction:

- Single roles or aggregated roles of SP, CP, NP, ANP, C/SCs, including incentive given to CCs in P2P Service Provider driven cases
- Cooperation, via appropriate static and/or dynamic SLAs
- Distributed management and independency of each actor in terms of managing its own resources

Flexible Business Model : B2C, B2B, C2C and to consider new CAN features and service environment new capabilities



4. CAN Architecture example

ALICANTE services (1)

- **Various exploitation models possible - based on ALICANTE's new business models**
  - VoD distribution offered by CAN Provider with QoS guarantees through adaptation in MANE according to the overall User Context
  - IPTV Hybrid multi-domain multicast distribution offered by CAN Provider
  - ALICANTE's enhanced service personalization
  - Watch TV Anywhere at Any Time

  Service Types

  Push Content: Big, Middle, small size
  User Interaction
  Web based services: HTTP Streams, Instant Msg. Data transfer, Content Down/Upload
  LIVE TV : 3D, HD, SD; *VOD* : 3D, HD, SD
  Video Conference : HD, SD
  Content download: Big , middle, small size

- Levels of guarantees: Fully / Partially/ Unmanaged Managed Services
  - This split captures two point of views
    - Services: (degree) how strict the QoS requirements are
    - CANP: shows the degree of the CAN layer freedom to perform autonomic actions

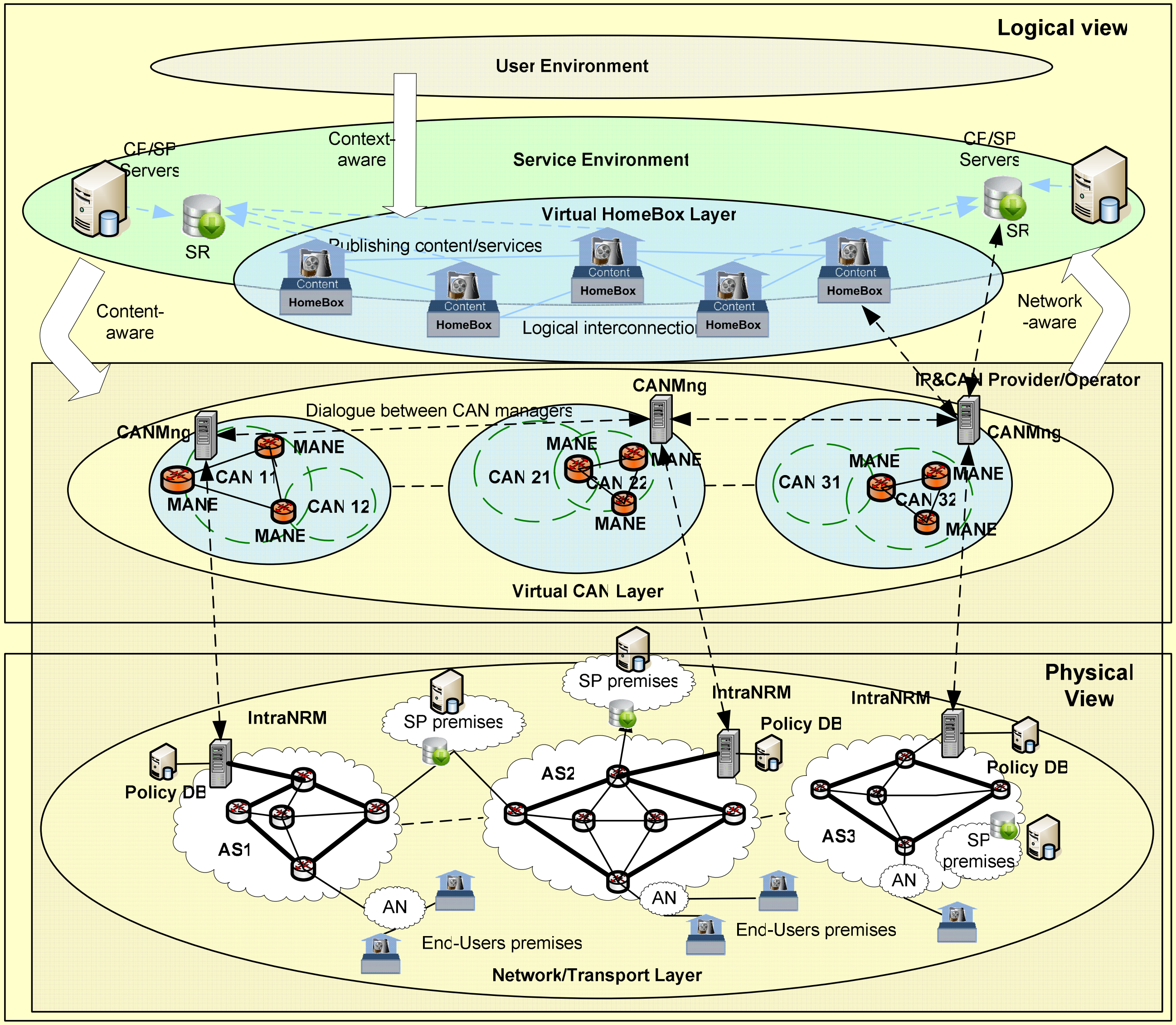
4. CAN Architecture example

- ALICANTE architectural solution:
- Two virtual layers,
  - CAN layer for virtual connectivity services on top of the the core IP network
  - Home-Box layer- content delivery
- On top of the traditional IP Network layer, virtualising the network nodes in
- User Environment, seamlessly interacting with the underlying layers
- Service Environment, based on cooperation between the traditional SPs and End-Users (through their HBs)
- Combine resource provisioning at CAN layer with two level solution adaptation for the multimedia flow delivery over multi-domains
- Hierarchical Multi-layered monitoring sub-system at all defined levels: User, Service, Home-Box, CAN, Underlying network

4.CAN Architecture example

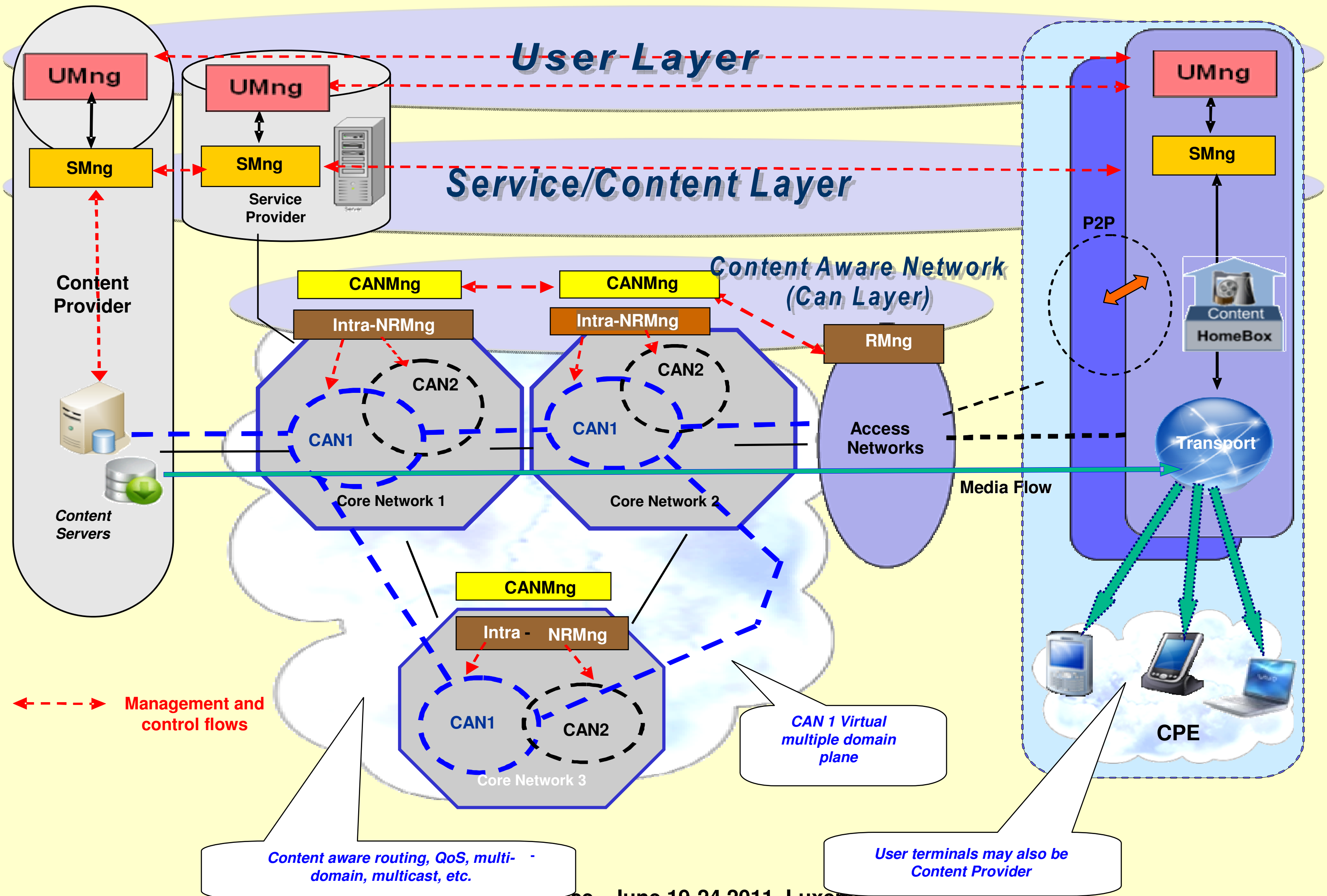
- **Overall Architecture View (1)**

- User Env
- Service Env
- HB-layer
- Net Env
  - CAN layer
  - Infrastructure layer



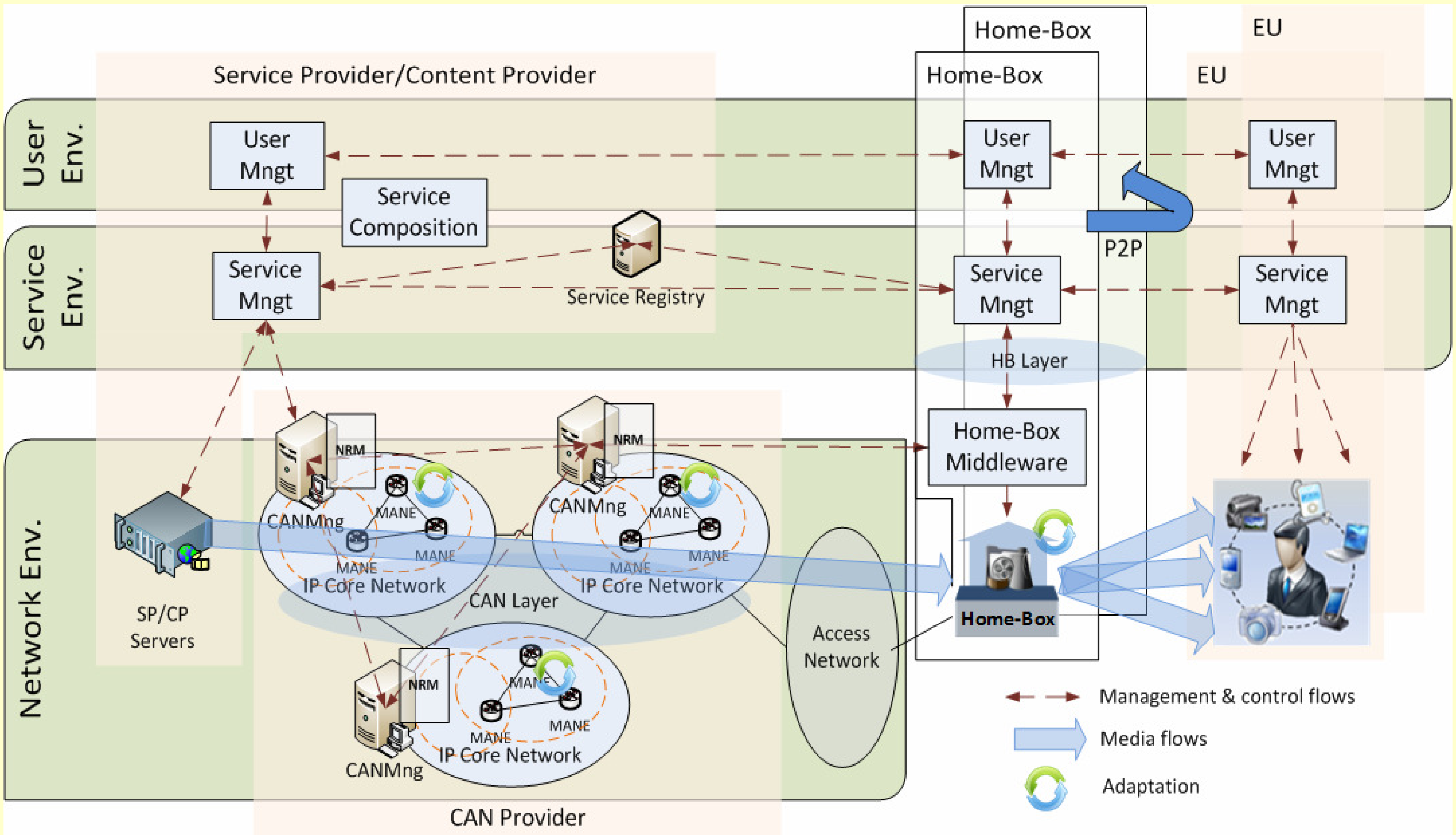
4. CAN Architecture example

Overall Architecture view (2): layers



4. CAN Architecture example

Overall Architecture view (3): splitting of functions



Architectural model- design principles

- **Separation in planes: traditional MPI, CPI, DPI**
- **Scalability : important objective seen on several dimensions/ levels**

  - **User and Service-Content layer:**
    - M&CPI : Distributed per/entity; Aggregated and/or individual signalling
    - DPI: P2P scalable overlay; HBs may act in adaptation (per class or individual) and distribution of content to other HBs

  - **CAN and network layer:**
    - M&CPI : distributed per/domain or per/entity; Aggregated and/or individual resource allocation
    - DPI: Still push complexity at the edges (MANE); Network QoS procedures applied first and then adaptation if necessary

  - **Per/node entity model (e.g MANE):**
    - High perf. algorithms for MANE (w.r.t packet inspection and fwd)
    - reduce the amount of analysis task of packets (first packet of a flow- deep analysis, the rest- summarised processing)
    - Help MANE with control information to recognise flows

  - PBM approach are investigated for CAN configuration:
    - For better flexibility
    - To reduce the amount of processing tasks in the data plane

- **Cross-layer optimisation** : via CANP-SP, CAN – HB -interactions

4. CAN Architecture example

Vertical and Horizontal Layering and functional splitting

- ***User Environment***
  - Data Plane
    - users can consume and/or generate content and exploit services delivered by components of the SE or by other users (Via HB)
  - *M&C Plane*
    - *adding new dimensions* user may have several roles: Content and Service Consumer; Content and Service Provider; Content and Service Manager
    - *elaborating a User Profile* : static and dynamic parameters of the user and his context
    - *permitting any user* to access/deliver/manage any service/content on any device from anywhere and at any time
    - *achieving efficient collaboration* with the SE, enabling user context-awareness
    - SLAs may be established by the EU/HB with SP for guaranteed services

4. CAN Architecture example

- Vertical and Horizontal Layering and functional splitting

- ***Service Environment***
  - full service management (creation, provisioning, offering, delivery, control)
  - composition of services and the delivery of content to End-Users throughout the network.
  - Divided in two parts: *SP/CP-based*; Virtual *Home-Box* layer part

  - SE
    - provides components
      - SP/CP servers, incorporating novel components and functionalities
      - Service Registry
    - uses the VCAN connectivity services
    - involved in the process for efficient adaptation of the services/content according to the End-Users' context
    - Other functions:
      - User mobility features
      - content producer features
      - security and privacy
    - SE Components
      - SP/CP servers
      - Service composition
      - Service Management
      - Service Registry
      - Service monitoring

4. CAN Architecture example

Vertical and Horizontal Layering and functional splitting

- ***Service Environment (cont'd)***
- *Data Plane*
  - Content server – media/content flows generation
  - Compose media flows in composite services

- *M&C Plane*
  - *Service*
    - *discovery* - new type of component :*Service Registry (SR)*
    - *advertisment – to external parties*
    - *delivery* - through the servers or HBs, in various modes;
    - *Management*
      - *Creation, offering, session control*
      - *SLA contracts with EU/HB*
      - SLA with CAN layer to contract VCANs
    - *composition* - Service Composition Engine for streaming media applications
  - *collaboration* with the User Environment and with the CAN layer

4. CAN Architecture example

- ***Vertical and Horizontal Layering***

- ***Virtual Home-Box Layer (HB layer)***
- allows SPs to supply EUs with advanced context-aware multimedia services in a consistent and interoperable way
- enables uniform access for heterogeneous terminals and supports enhanced Quality of Experience (QoE)
- advanced user context management and monitoring functions provides real-time information on user context and network conditions, allowing
  - control over multimedia delivery
  - intelligent adaptation, service mobility, security

- context management, monitoring and adaptation : key features enabling the support of user mobility using a Connectivity Engine in secure manner.

- HB layer : logical interconnection (in P2P or distributed modes) of deployed HBs (it has a Connectivity Engine),
- uses CAN services and network-aware info delivered by the CAN layer

4. CAN Architecture example

- ***Vertical and Horizontal Layering***

- ***Virtual Home-Box Layer (HB layer)***
- HB :
  - can be seen as the evolution of today's Home Gateways (HGs)
  - physical entity deployed inside each user's home
  - cooperates with User, Service, and Network Environments for :
    - Elaboration of network and context-aware appl. and deliver the necessary inputs to create CANs
    - overall management of services and content are assured at this layer- in the CPE premises

4. CAN Architecture example

- ***Vertical and Horizontal Layering and functional splitting***
- ***Virtual Content-Aware Network (V)CAN* - layer**
  - Works on top of traditional IP network/transport layer
  - *Data Plane*
    - enhanced support for packet payload inspection, processing and caching in network equipment
    - improves media flows transport by applying customised processing depending on *content, service application*
    - improves QoS assurance via content-aware forwarding/routing
    - increases network security level via content-based monitoring and filtering
    - 1:1, 1:n, n:m communications, P2P
  - *M&C Plane*
    - Distributed M&C: per domain CANMgr
    - Establish SLA/SLS between CANP and other business entities
    - Plan, provisioning, modifying VCANs in the form of parallel planes
  - The specific components of VCAN are the
    - Media-Aware Network Elements (MANE), i.e., the new CAN routers
    - CAN managers.

4. CAN Architecture example

- ***Vertical and Horizontal Layering and functional splitting (cont'd)***

- ***Intra-domain Network Layer***
  - Traditional network TCP/IP layer
  - Data Plane
    - Implements VCANs by process data flows in CA style in MANE
    - Makes use of traditional network technologies to assure QoS, availability of paths
      - MPLS, Diffserv, etc.
    - IP multicast
  - M&C Plane
    - Managed by the Intra-domain Network Resource Manager (IntraNRM)
      - Having full authority on the network nodes and domain configuration
      - Cooperating with CANMgr in order to negotiate and install VCANs
    - IntraNRM
      - establish Network Interconnection Agreements with other IntraNRMs
      - Establish SLA with CAN Manager

4. CAN Architecture example

Summary of functions

➢ User Environment functional components:

•User Profile modelling and context management framework

•QoS/QoE monitoring tool & manager

•User/Service widget-based interface and management framework

➢ Service Environment functional components:

•SP/CP servers with content-awareness and adaptation features

•Service manager and monitoring manager

•Service composition tool suite and distributed pipeline framework

•Distributed service registries

Home-Box Layer

➢ Network Environment functional components:

•CAN Manager

•Intra Network Resource and Monitoring Manager

•**NEW network component: MANE**

- Policies
- Multi-domain VCAN creation, exploitation & termination
- CA processing and routing/forwarding
- QoS assurance
- QoS mapping on MPLS/Diffserv
- Hybrid multicast
- Flow adaptation
- Hierarchical monitoring
- Security

CAN Layer

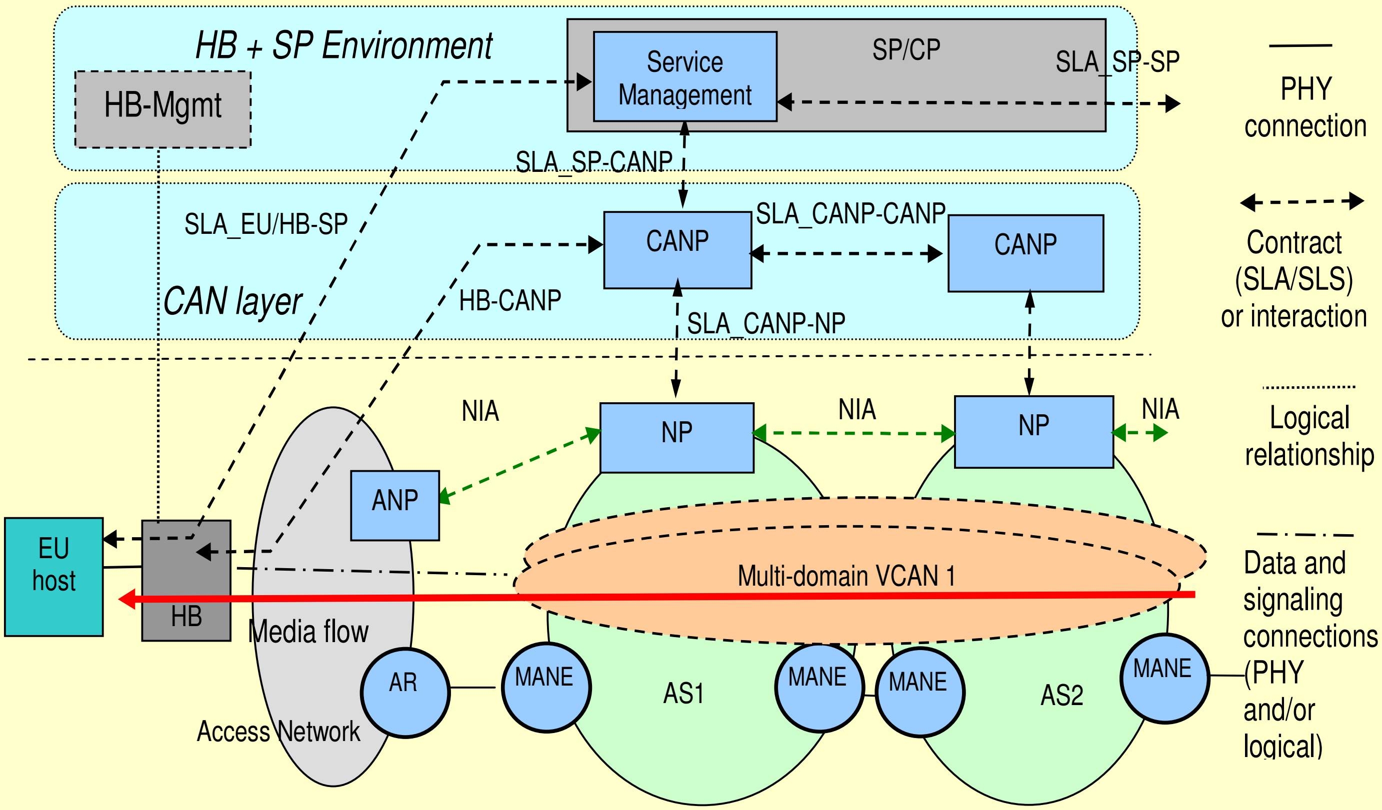
➢ **Home-Box component:**

- Context-aware management (user, service, session, ressources, mobility, security…)
- Service delivery
- Network-aware monitoring & adaptation

4. CAN Architecture Example

- ALICANTE Environments: contracts/interactions between BM actors

CANP – CAN Provider; SP/CP Service/Content Provider; CP – Content Provider; (A)NP – (Access) Network Provider; VCAN Virtual Content Aware Network; MANE Media Aware Network Element; HB – Home Box; AS – Autonomous System; AR – Access Router; EU- End User (terminal)



4. CAN Architecture example

- ALICANTE Environments: contracts/interactions between BM actors

- Main possible contracts established in the MPI /CPI

  - ***SLA_SP-CANP-*** through which an SP requests and receives VCAN resources from CANP,

  - ***SLA_CANP-CANP*** –to extend VCAN upon several NP domains,

  - ***SLA_CANP-NP*** - through which the NP commits to offer connectivity resources to CANP,

  - ***SLA_EU/HB-SP***- individual contracts to give access for EUs to SP services, or to give rights for SPs to distribute content provided by EUs.

  - ***NIA*** - network interconnection agreements between the NPs or (NPs and ANPs) to establish inter-domain connectivity services,

4. CAN Architecture example

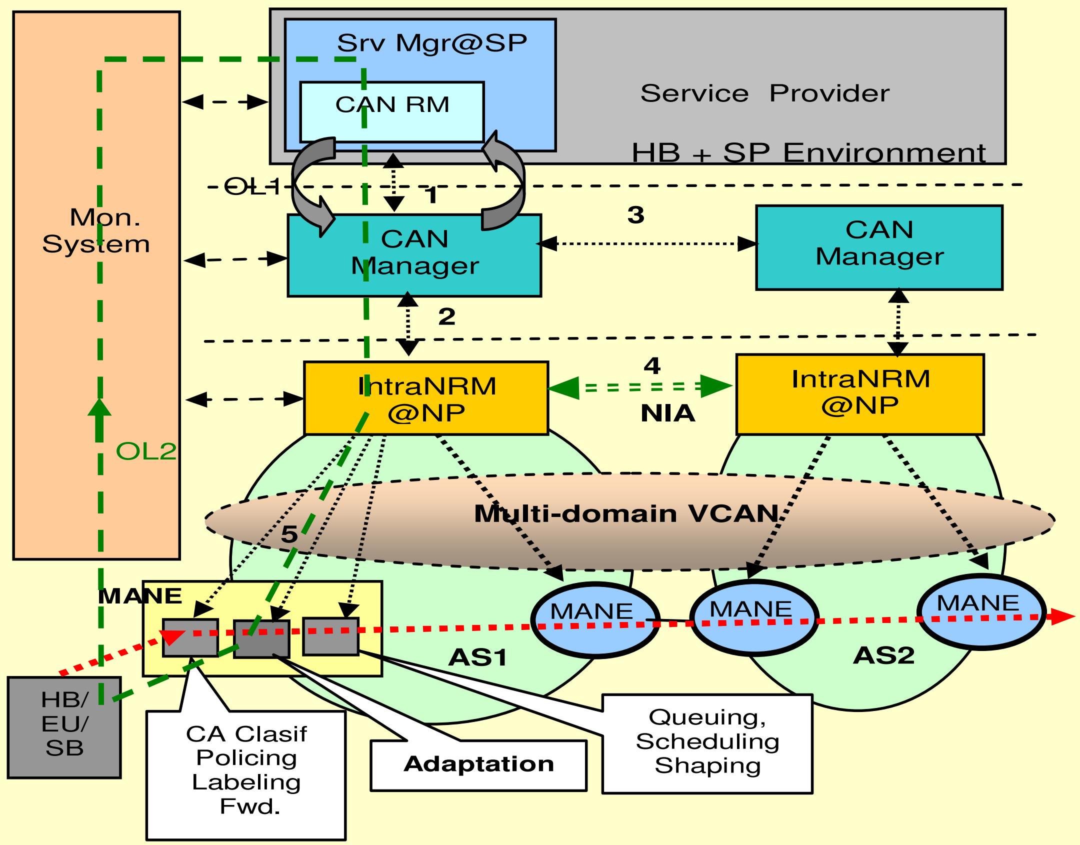
- ALICANTE Environments: contracts/interactions between BM actors

- Other possible interactions established in the MPI /CPI
-
  - ***SLA_ SP-SP*** – concluded if SPs want to cooperate in offering services
  - ***SLA_SP-CP*** - to allow SP to *advertise, offer, negotiate and distribute* content produced by CP (traditional one or EU), through high level services (not mandatory in ALICANTE)
  - ***EU-SP -*** ad-hoc interaction through which the EU try to consume content if currently available
  - ***HB- HB*** for inter-HB communication in client server mode or P2P style
  -
  - ***HB-CANP*** - through which the HB could ask special CAN services directly from CANP (without intermediation of SP - for instance in order to find distances between HBs)

4. CAN Architecture example

- Content and context aware architecture at network layer

- Two main optimisation loops
- *provisioning loop* (OL1)
  - CAN/NAA
    - SP, CANP, (NP)
- *adaptation loop* (OL2)
  - Network
  - HB, terminals
  - monitoring system
    - QoS, QoE probes
  - Adptation Decision Taking Engine (ADTF)



4. CAN Architecture example

CAN Layer Development Objectives

- Overlay VCAN infrastructure
  - multiple-domain, multiple providers, VCAN
  - preserve the Network Providers independency in terms of resource management
- Media Aware Network Element (MANE) as a main CAN entity
  - Content aware & context aware packet flow processing
- Resource Management and Control, QoS assurance- several levels of guarantees
  - VCAN provisioning, VCAN-style autonomic processing
  - Map VCANs onto MPLS and Diffserv support
  - Integration of flow adaptation
- CAN layer monitoring – hierarchical solution
- Inter and intra-domain multicast services
  - IP layer intra-domain multicast –cooperation with inter-domain overlay multicast
- CAN layer Security functionalities

4. CAN Architecture example

- **CAN Layer: Key innovations**
- **Content and context aware architecture at network layer**
  - CA media flow processing (for QoS multi-level guarantees)
    - Cooperation of several functionalities
      - CA-classification, CA-forwarding, CA-adaptation
      - MPLS, Diffserv, IP multicast, IP layer security
- Multi-domain, multi provider VCANs – parallel customisable overlays
  - Multi-domain, multi-layer, multi-provider VCAN (resource) management system
- **Development of MANE – new network element (CA-router) + MPLS-Diffserv**
  - Cross-layer optimisation SP-CANP-NP
  - Advanced, hierarchical, layered monitoring system
  - Integrated solution : CA + unicast, multicast, P2P
  - Incremental possibility of VCAN deployment

4. CAN Architecture example

- CAN Layer :Management Level of services
  - **Fully Managed Services (FM)**
  - **Partially managed Services (PM)**
  - **Unmanaged Services**
  - This split captures two point of views
    - Services: (degree) how strict the QoS requirements are
    - CANP: shows the degree of the CAN layer freedom to perform autonomic actions
- **Fully Managed Services**
  - High priority services in ALICANTE: delivered by the SP and the in some cases EU's HB
  - **SLAs exists agreed between SP and CANP**
    - Services requirements: Guaranteed: (low) packet delay; bandwidth; (low) packet loss; possible secure, private connectivity
    - VCANs provisioned by the CANP to answer the requirements
      - Different levels of guarantees are possible
  - Services adaptation may be performed - if necessary- at HB and MANE level- but in the limits of the SLA

4. CAN Architecture example

- CAN Layer: Management Level of services (cont'd)
  - **Partially managed Services (PM)**
    - The CAN layer has more freedom (to act upon flows) than in FM case
    - Still one may have a contract SP-CANP specifying:
      - PM1: some minimum QoS guarantees (quantitative) – plus some extra, or
      - PM2: only statistical/qualitative (weak) guarantees
    - CAN layer may apply adaptation if necessary:
      - PM1 case: not to violate the contract (in normal network operation cases)
      - PM2 case: any adaptation operation in the network is allowed to CAN layer in order to do "its best"
  - **Unmanaged Services:**
    - No contract SP – CANP
    - CAN layer
      - Still may offer some QoS
      - Is totally free to treat the traffic conforming the NP policy

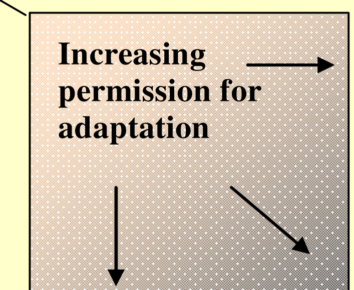
4. CAN Architecture example

- **Type of services guarantees supported by VCANs**
  - Hard Guarantees – HG
  - Statistical Quantitative Guarantees- SQnG
  - Statistical Qualtitative Guarantees – SQlG
  - No guarantees (Best Effort) – BE
- **Notations:**
- BQ1, BQ2, .. Different sets of Bandwidth reqs.
- (decreasing QoS order)
- DLJ-Q1, 2, ..- different sets of DJL reqs (decreasing QoS order)
- QoS classes
  - Well known-int'l(MQC)
  - Local (LQC) composition

Delay, Jitter, Loss \ Bandwidth assurance degree		HG	SQnG		SQlG	BE
		BQ1	BQ2	BQ3	BQ4	NA
HG	DJL-Q1					
	DJL-Q2	FM				
	DJL-Q3					
SQnG	DJL-Q4		PM1			
	DJL-Q5			PM1		
SQlG	DJL-Q5				PM2	
BE	NA					UM

Lower limit guaranteed plus some chances for more resources

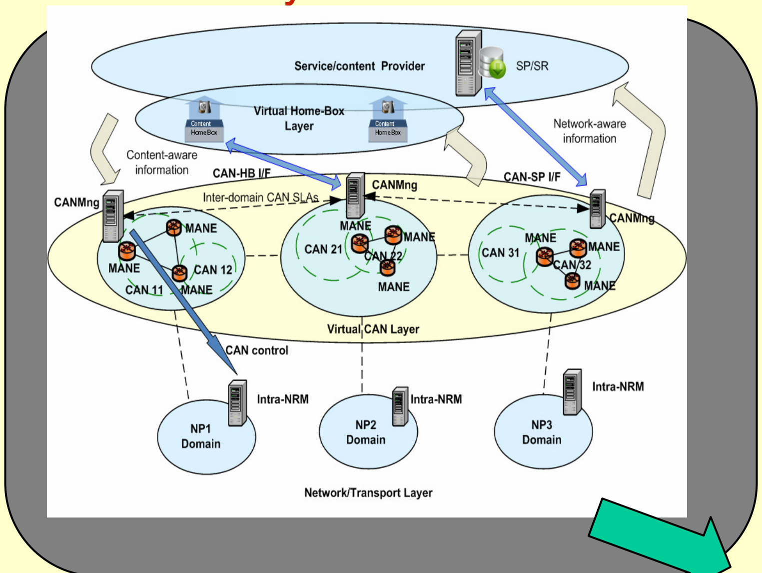
Only statistical values guaranteed



Adaptation view

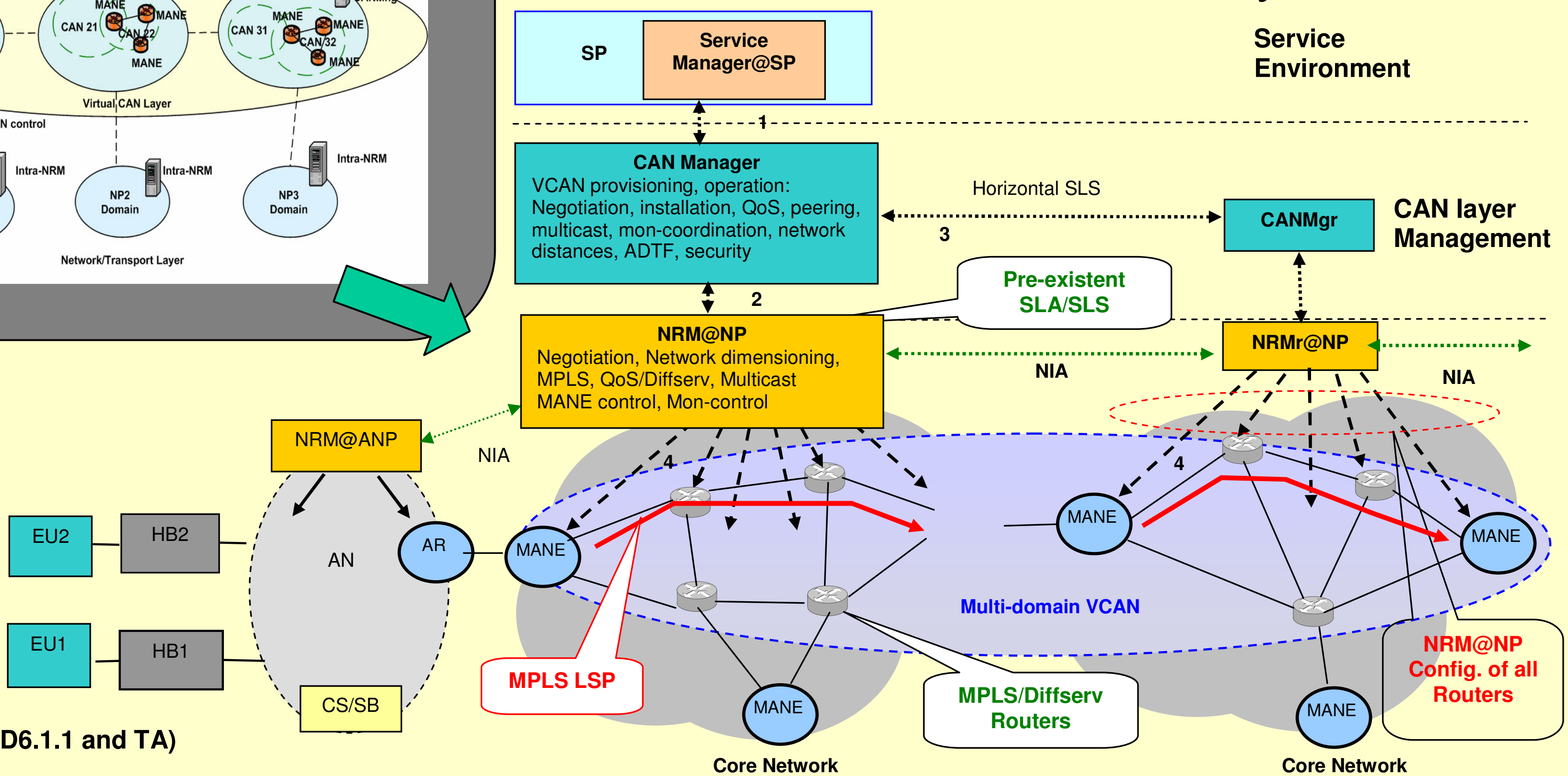
4. CAN Architecture example

CAN Layer Architecture



Technical Annex

- Content and context aware architecture at network layer



(See D2.1, D6.1.1 and TA)

4. CAN Architecture example

- CAN Layer:
- MANE/Content-Aware Network Router (CANR)
  - Intelligent network node.
  - Consider the content type in order to perform
    - appropriate processing (filtering, routing, adaptation, security operations, etc.)
    - according to the content properties (metadata, protocol field analysis) and also depending on network properties and its current status.
- MANE basic set of functions :
  - *Content-aware intelligent routing and forwarding*: based on results extracted from packet fields' analysis or content description metadata
  - *Content-aware QoS and resource allocation*
  - *Flow adaptation : e.g considering SVC codes*
  - *Specific Security processing*
    - Keep the traditional security procedures- plus specific treatment based on content type

4. CAN Architecture example

- CAN Layer:
- MANE/Content-Aware Network Router (CANR)
- Basic set of functions : (cont'd)

  - *Content-aware QoS and resource allocation:*
    - appropriate instances of CAN will be assigned to flows depending on the level of QoS guarantees and network status
    - the MANEs deduce the QoS requirements of different flows based on the flows content
    - MANE will assign the flows to the appropriate CANs
    - The CAN layer will monitor the current load CANs
    - The MANE will maintain an aggregated image of flows that they forward
    - Efficient resource allocation and/or load balancing –possible

4. CAN Architecture example

CAN Layer: Content Awareness (1/3)

- MANE : Traffic Classification Mechanisms
  - Exact matching (Port Number to Service mapping)
  - Prefix matching (specific patterns inside headers)
  - Deep Packet Inspection (heuristics, pattern matching)
    - MANE is instructed via Control plane about some headers relevant in the data flow packets
    - Only initial packets of a flow will be fully analysed
    - MANE will identify the incoming flows, applying a hash id on each calculated by the 5-tuple (Layer3-4)
    - *Automaton*, *Heuristics* and *Filtering-based* approaches will be exploited in order to provide Content Awareness
    - When the content is identified the corresponding Flow Table entry is updated

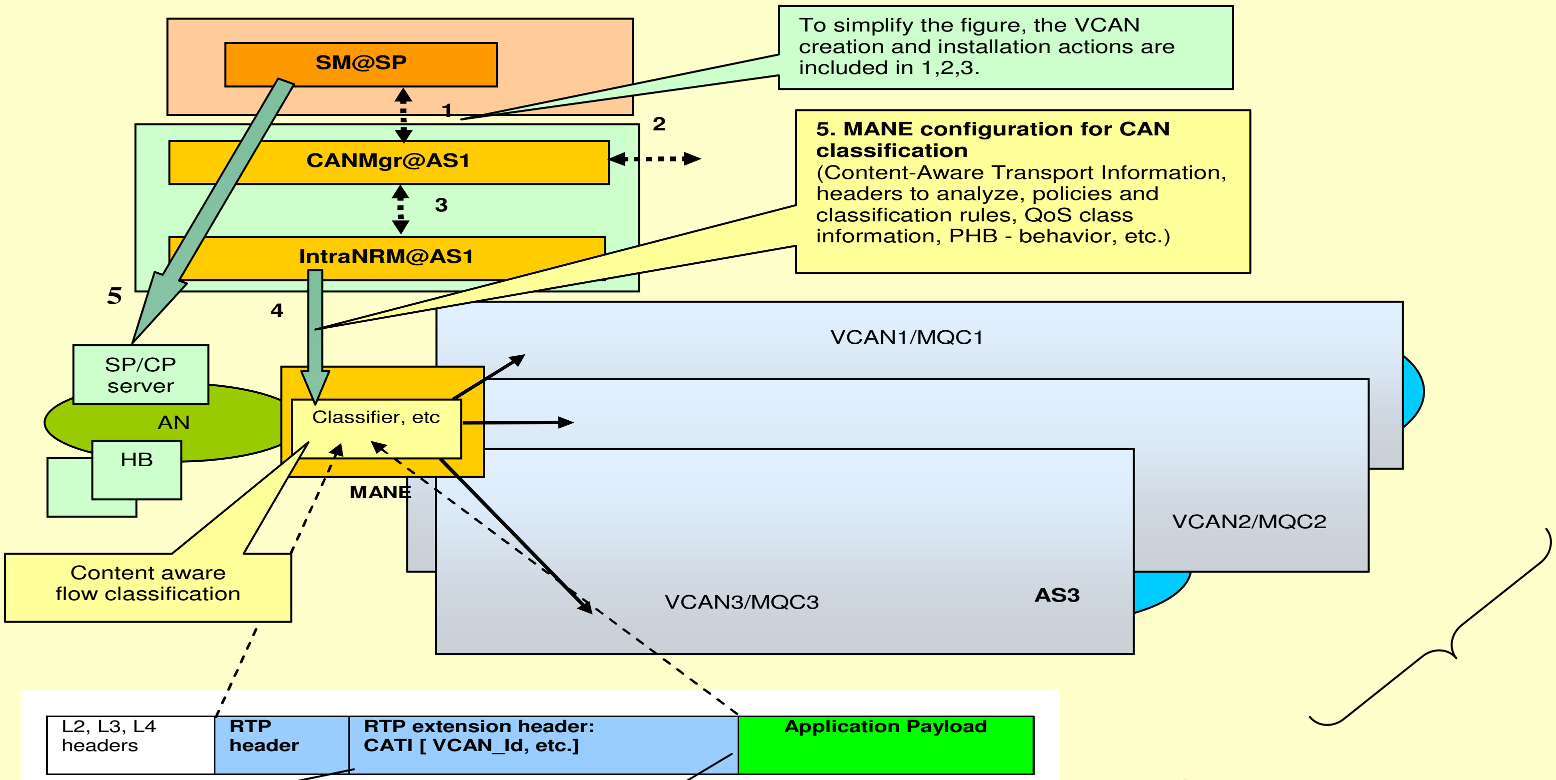
4. CAN Architecture example

CAN Layer: Content Awareness (2/3)

- MANE : Traffic Classification Mechanisms (cont'd)
  - Statistical methods (based on machine learning algorithms)
    - Useful for classification of encrypted traffic flows where DPI is inappropriate
    - Correlation exists between the behavioral characteristics of a flow and the service that generate it
    - Machine learning algorithms exploit the behavioral characteristics observed through the statistical analysis of the flow
- ***Content Aware Transport Information (CATI): Simplify the MANE analysis***
  - **Operational Cases**
    - A. SLA SP-CANP for VCAN(s) construction; CS insert CATI in data packets
    - B. SLA SP-CANP for VCAN(s) construction; No CATI, but DPI
    - C. no SLA SP-CANP; No CATI; DPI possible or BE.

4. CAN Architecture example

Content Awareness (3/3)



VCAN Parallel Planes

	CATI
Bits	Definition
1	Unicast or multicast mode
2	Extension header presence
3	Adaptability of the service
4 -7	Service type
8-10	Service Sub-Type
11-12	Service priority
13-18	VCAN label
19-26	Extension purposes

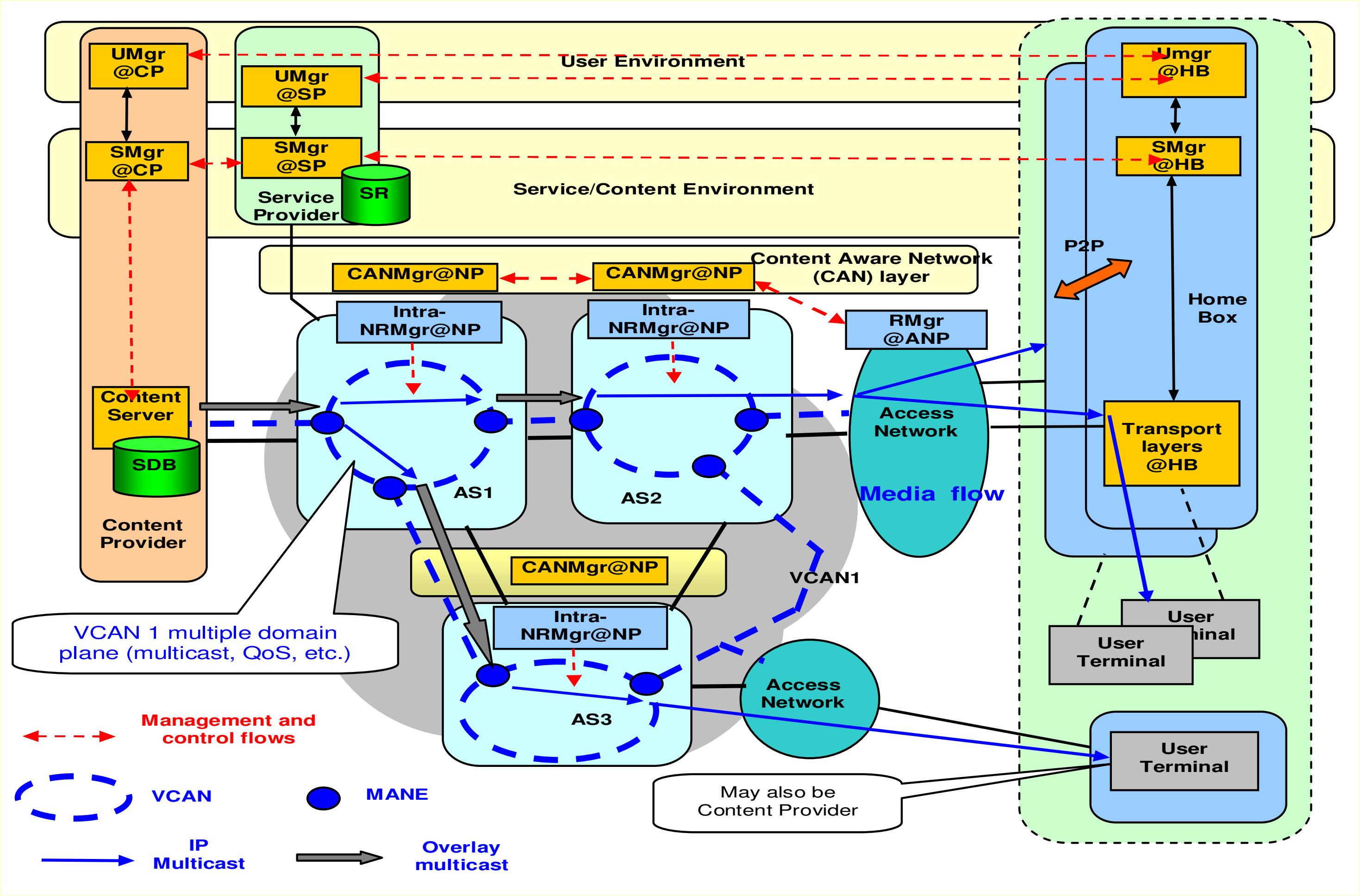
4. CAN Architecture example

- **Summary of the Main challenges at CAN Layer**

  - Offer all above capabilities – content aware related
    - QoS, routing/forwarding, adaptation, security, caching,
  - While:
    - Keep the amount of per/packet processing as low as possible in order tu function at high line rate
      - E.g.:First packet deep analysis plus hash table techniques
    - Allow seamless development in the network
      - Primarily – they will be installed at core domain edges
    - Preserve the Intra-domain independency combined to offering capability to extend VCAN over multiple domains
    - Taking into account network dimensioning information provided by the IntraNRM when designing CANs

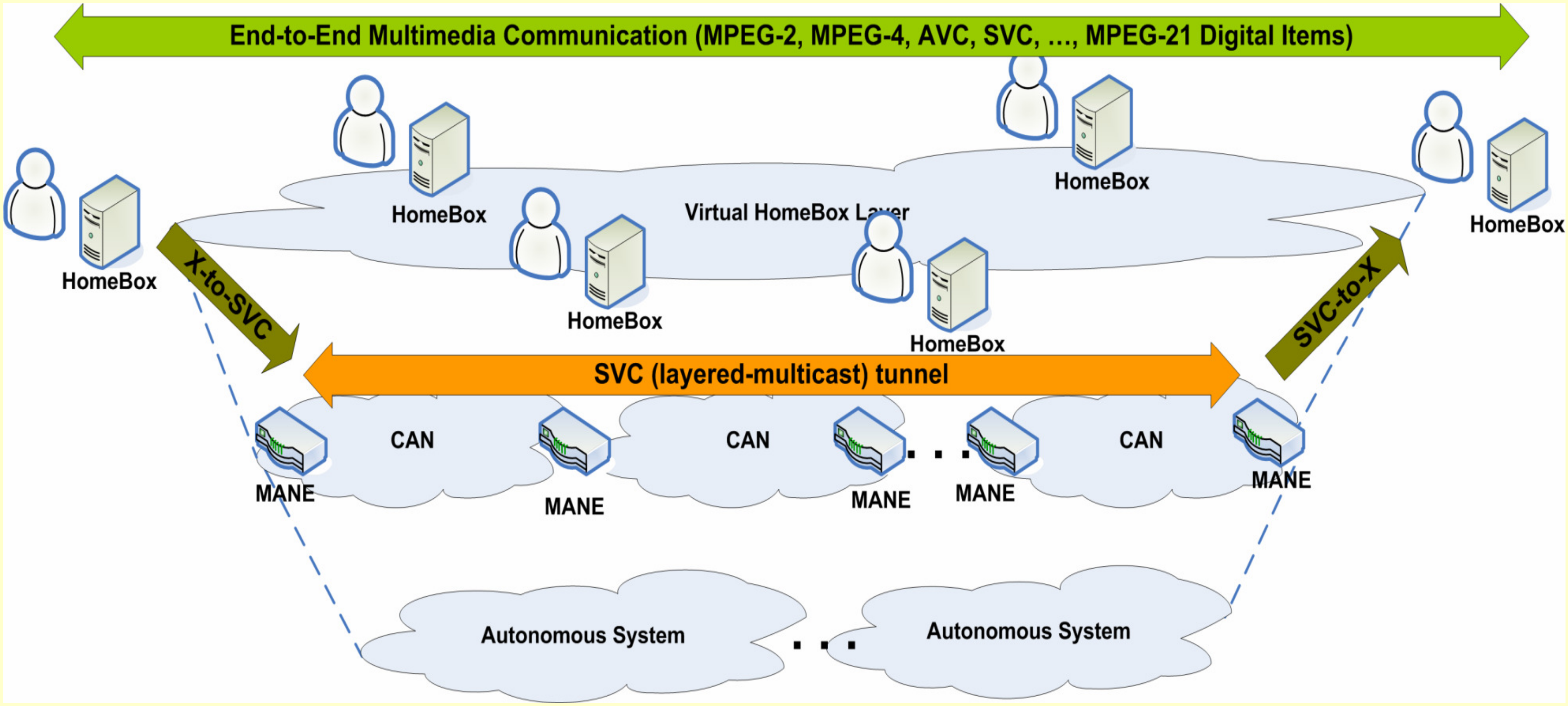
4. CAN Architecture example

- **Multicast Services**
- **Hybrid solution: IP multicast-intra-domain; Overlay Multicast –inter-domain; QoS enabled tree**

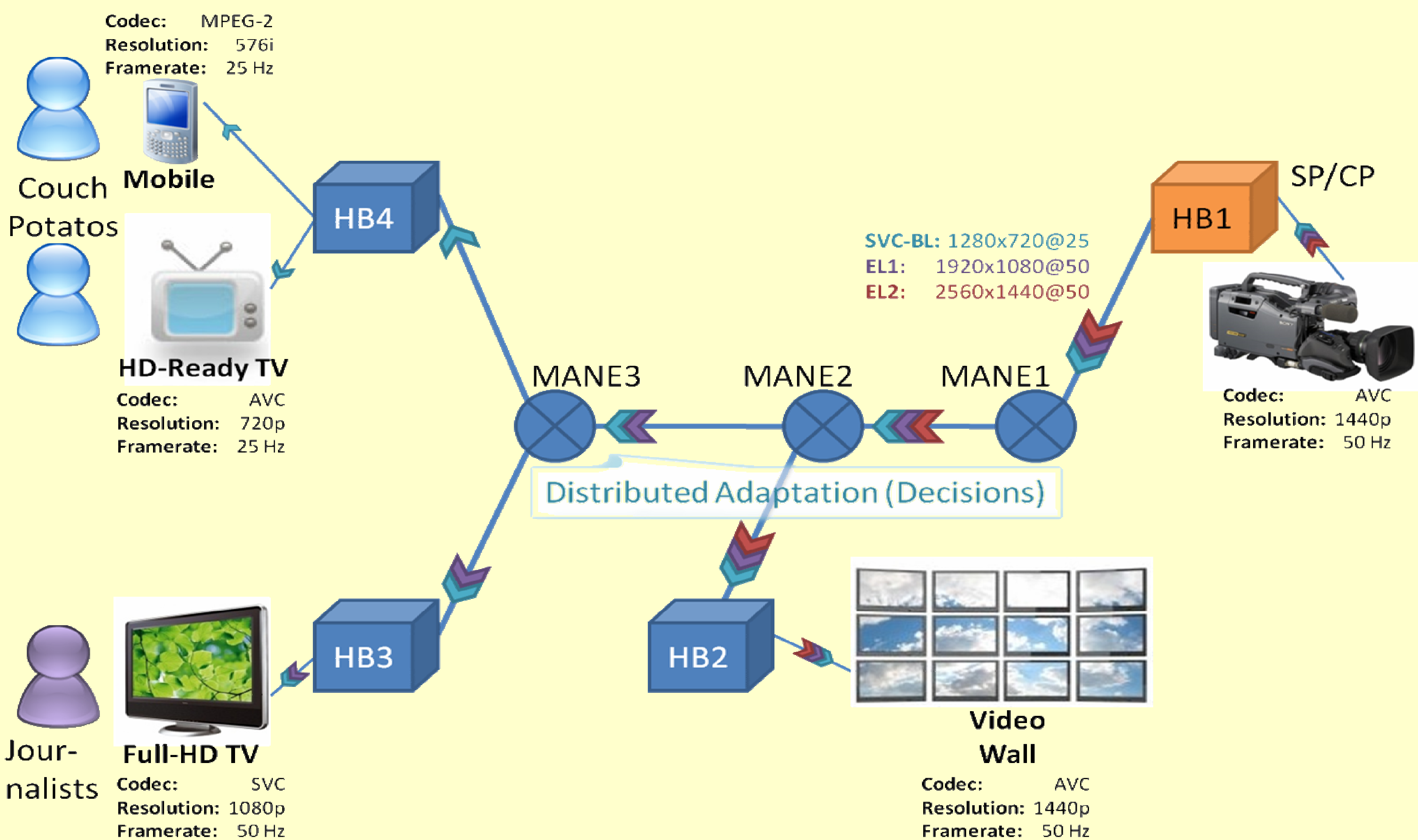


4. CAN Architecture example

- **Adaptation**: Key innovation in Alicante
- SVC tunnel with in-network adaptation
  - Better network resource utilization
  - Maintaining a satisfactory Quality of Experience for the end user

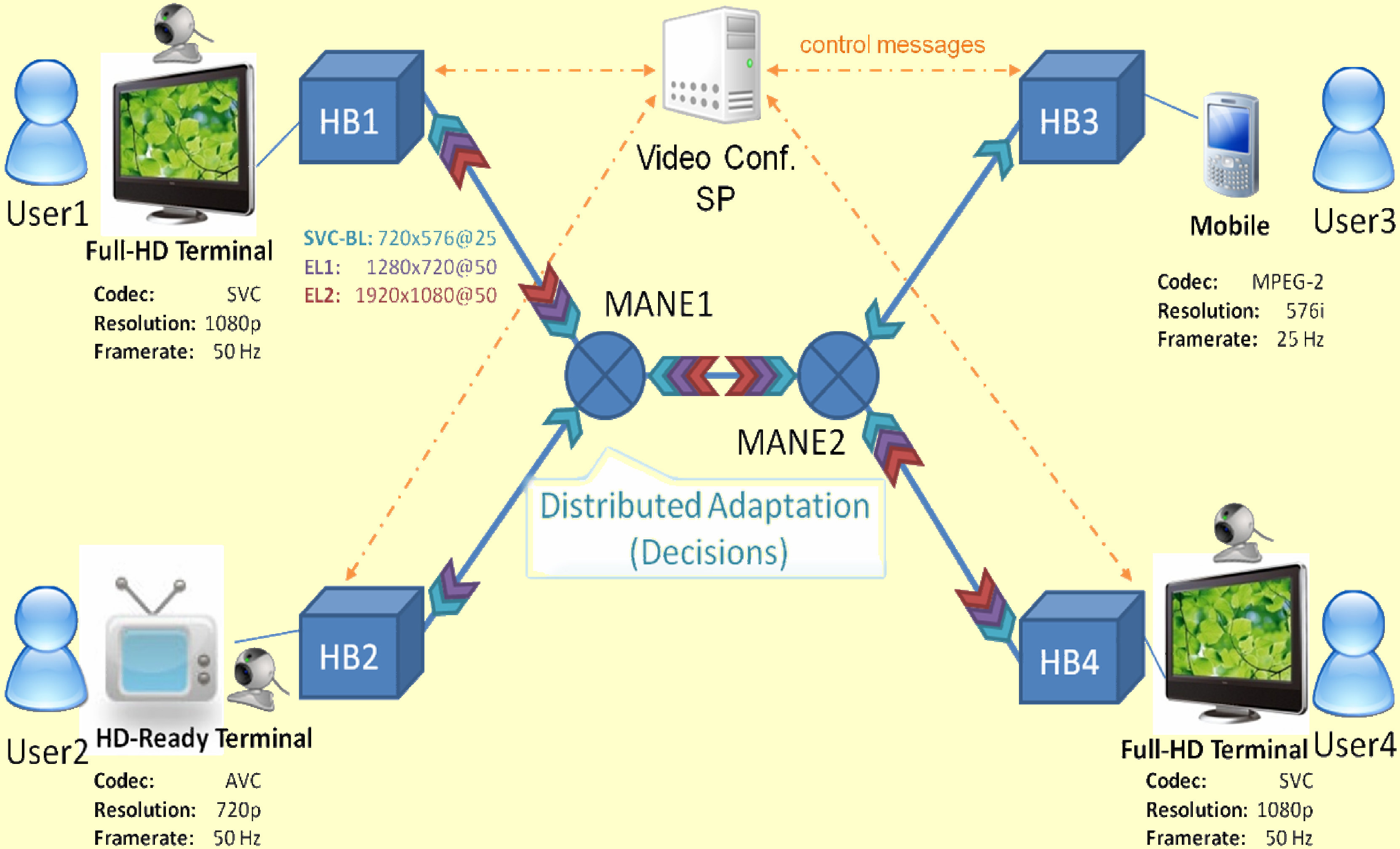


Use Case: Multicast Streaming



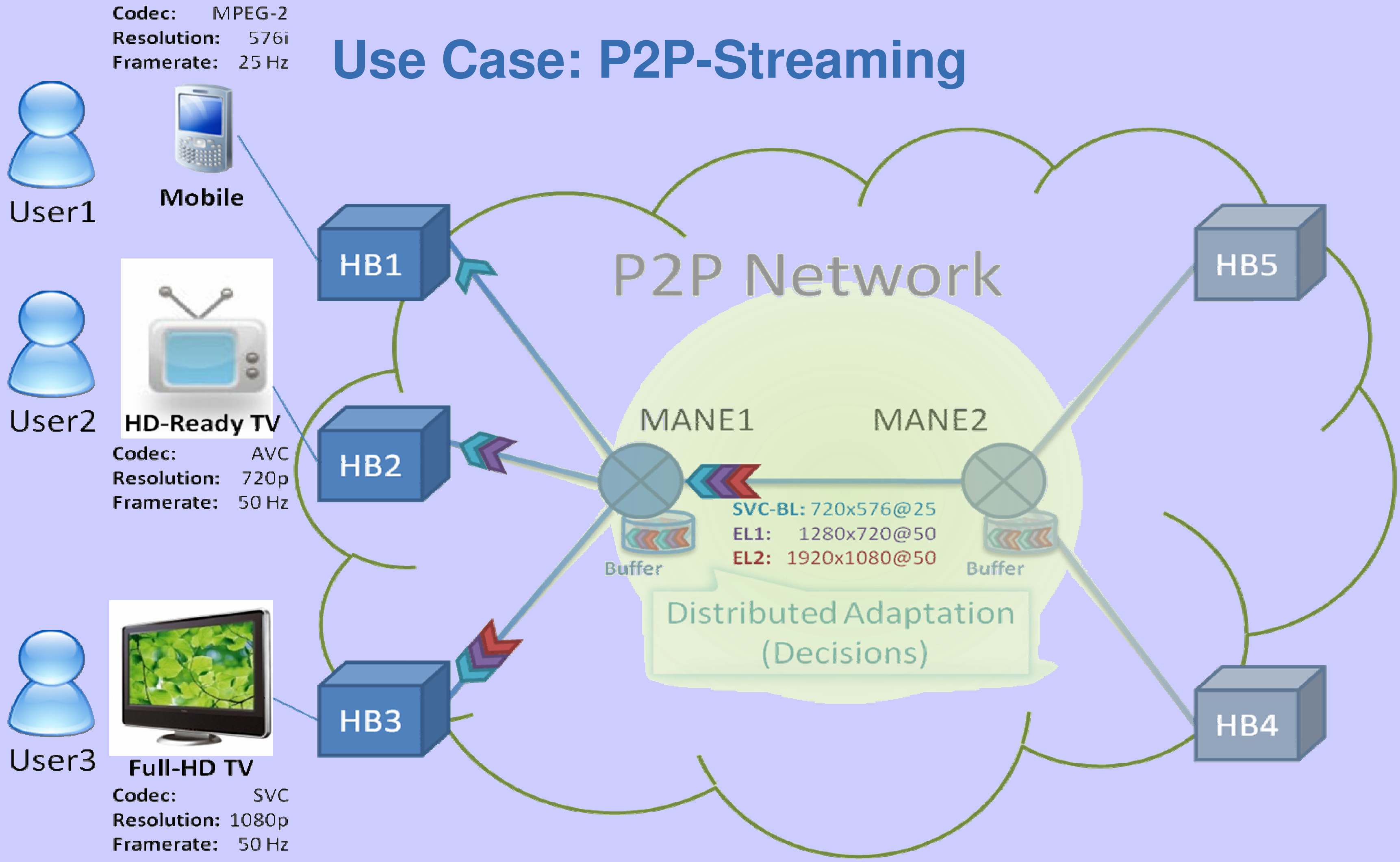
4. CAN Architecture example

Use Case: Video Conference



4. CAN Architecture example

Use Case: P2P-Streaming



4. CAN Architecture example

Adaptation: Generic Architecture (cont'd)

- Adaptation at the CAN layer (online)
  - MANEs only at edges of AS
  - CAN Monitoring available only in aggregated form
  - SVC scalability
    - Spatial: Multiple resolutions in ELs
    - Temporal: Multiple frame rates
    - SNR (Quality): Multiple bitrates

- Adaptation at the HB layer
  - X-to-SVC and SVC-to-X transcoding
    - SVC encoder/decoder, SVC-to-AVC & AVC-to-SVC
  - All scalability dimensions supported
  - Offline and real-time adaptation possible (at the SP/CP side)

CONTENTS

5. Conclusions

- Conclusions ALICANTE
  - New architecture oriented to
    - Content aware networking
    - and Network aware applications
  - Environment/layers: User, Service, Home-box, CAN
  - Horizontal and vertical cooperation between the CAN layer and upper layer
  - Combines the networking technology with adaptation methods
  - Allows multimedia oriented services to be developed in a flexible way
  - Multi-domain
  - Users as consumer and producers of content

5. Conclusions

- **General open issues :**
  - How much to preserve the current network neutrality?
  - Content Aware Networking- Network Aware Applications
    - evolutionary approach: in the data plane mainly
    - traditional protocol stack modifications
  - Content Centric Networking/Content oriented networking –
    - Revolutionary approach
    - new paradigm for IP networking
  - Applications/services exist which
    - Are not primarily driven by content but by identity/location - VoIP, VC, etc.→ combined solutions should be considered
  - Virtualisation – strong tool helping also CAN , CCN – still open to research
  - New business models are needed
  - Scalability, cost, backward compatibility?
  - Acceptance by the vendors, providers, operators of these new approaches ?

- Thank you !
- Questions?

References

- **References (partial list)**

1. Report from the National ICT Research Directors Working Group on Future Internet (FI) of the EC on Information Society and Media- Nov. 2008)
2. A.Peltomäki, Stimulating an Innovation Ecosystem for Future Internet Technologies, EC Information Society and Media Directorate-General, Lulea, Sweden June 2009
3. Schönwälder ,j. et al. , Future Internet = Content + Services + Management, IEEE Communications Magazine, July 2009
4. FUTURE INTERNET ASSEMBLY, Madrid, Spain, 9th – 10th December 2008, MEETING REPORT, December 2008
5. DG Information Society and Media Directorate, for Converged Networks and ServiceFuture Internet 2020, VISIONS OF AN INDUSTRY EXPERT GROUP, May 2009
6. G. Tselentis et al. (Eds.), Towards the Future Internet, IOS Press, 2009
7. Future Internet – Towards Research Challenges – 07 APR 2009, http://www.future-internet.eu/fileadmin/documents/prague_documents/FI_-_From_Functionalities2Challenges-09_04_08.pdf
8. Future Internet Initiatives, http://www.nessi-europe.com/Nessi/ (Networked European Software and sevices initiative)
9. Pavlou G., Towards a Service-aware Future Internet Architecture, Future Internet Assembly – Madrid, Dec 2008
10. The FP7 4WARD Project , http://www.4ward-project.eu/
11. Luis M. Correia, An Academic View on Business and Regulatory Issues on the Future Internet, http://www.4ward-project.eu/
12. Abramowicz,H. Introduction to BIRD WS, http://www.4ward-project.eu

References

- **References (partial list)**

13. The Content-Aware Network, Solace Systems, www.solacesystems.com
14. D.Kennedy, Networks + Content, Eurescom, Bled 2008
15. Van Jacobson, D.K. Smetters, J.D. Thornton, M. F. Plass, NH. Briggs, R.L. Braynard, Networking Named Content, Palo Alto Research Center, Palo Alto, CA, October 2009
16. A. Mitra, M.Maheswaran, Wide-Area Content-based Routing Mechanism, International Parallel and Distributed Processing Symposium (IPDPS'03), http://www.computer.org/portal/web/csdl/doi/10.1109/IPDPS.2003.1213447
17. Barani Subbiah Zartash Afzal Uzmi Content Aware Networking in the Internet: Issues and Challenges, suraj.lums.edu.pk/~zartash/publications/2001-06-ICC-Content.pdf
18. A.Carzaniga, A. L. Wolf, Forwarding in a Content-Based Network, www.inf.usi.ch/carzaniga/papers/cw_sigcomm03.pdf
19. R.Bless, C.Werle, Control Plane Issues in the 4WARD Network Virtualization Architecture, Electronic Communications of the EASST Volume 17 (2009)
20. Editors: L.M. Correia and L.Lundgren, *Going 4WARD Newsletter,* 4WARD- Architecture and Design for the Future Internet May 2009, Issue No. 4
21. Future Media Internet Architecture Reference Model, www.fi-nextmedia.eu /http://initiative.future-internet.eu/news/view/article/future-media-internet-architecture-reference-model-white-paper.html- 2011
22. Subharthi Paul, Jianli Pan, and Raj Jain, Architectures for the Future Networks and the Next Generation Internet: A Survey
23. J.Choi, Jinyoung Han, E.Cho, Ted Kwon, and Y.Choi,A Survey on Content-Oriented Networking for Efficient Content Delivery, IEEE Communications Magazine • March 2011
24. T. Koponen *et al.*, “A Data-Oriented (and Beyond) Network Architecture,” *SIGCOMM ’07*, 2007, pp. 181–92
25. K. Visala *et al.*, “An Inter-Domain Data-Oriented Routing Architecture,” *ReArch ’09: Proc. 2009 Wksp. Rearchitecting the internet*, New York, NY, 2009, pp. 55–60
26. http://www.ict-alicante.eu/