Orchestrating a brighter world

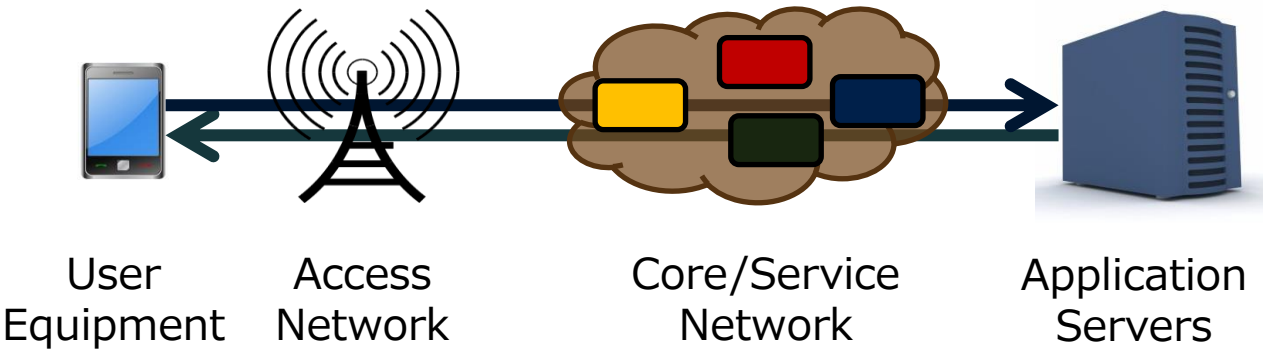
NEC

Security & Transport Performance in 5G

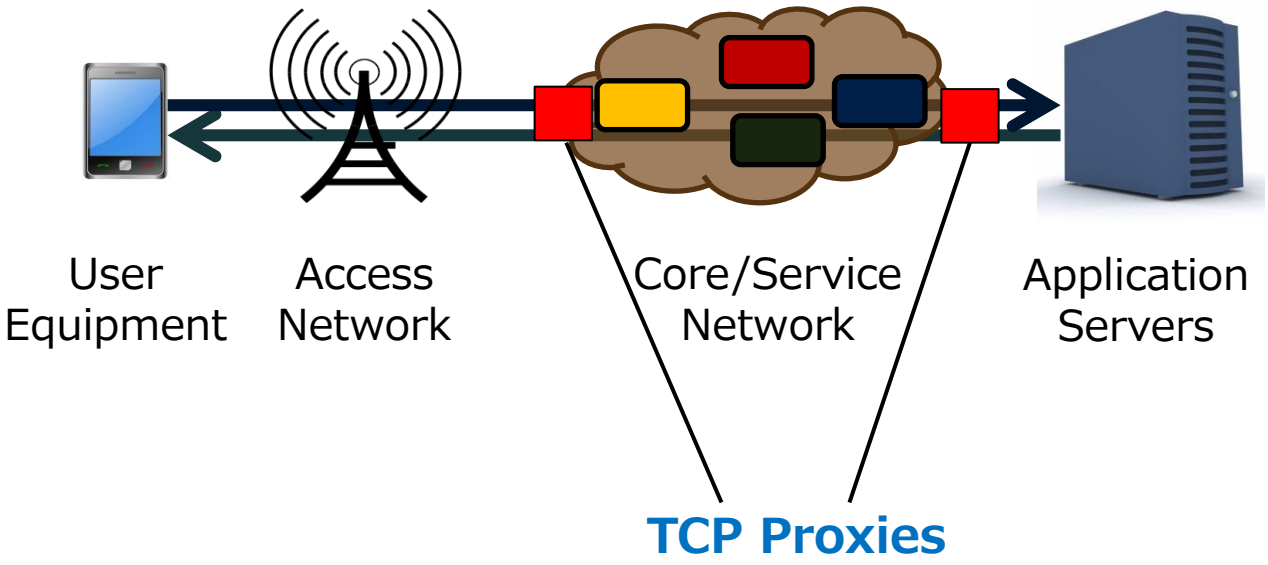
Dr.-Ing. Dirk Kutscher
Chief Researcher Networking

NEC Laboratories Europe

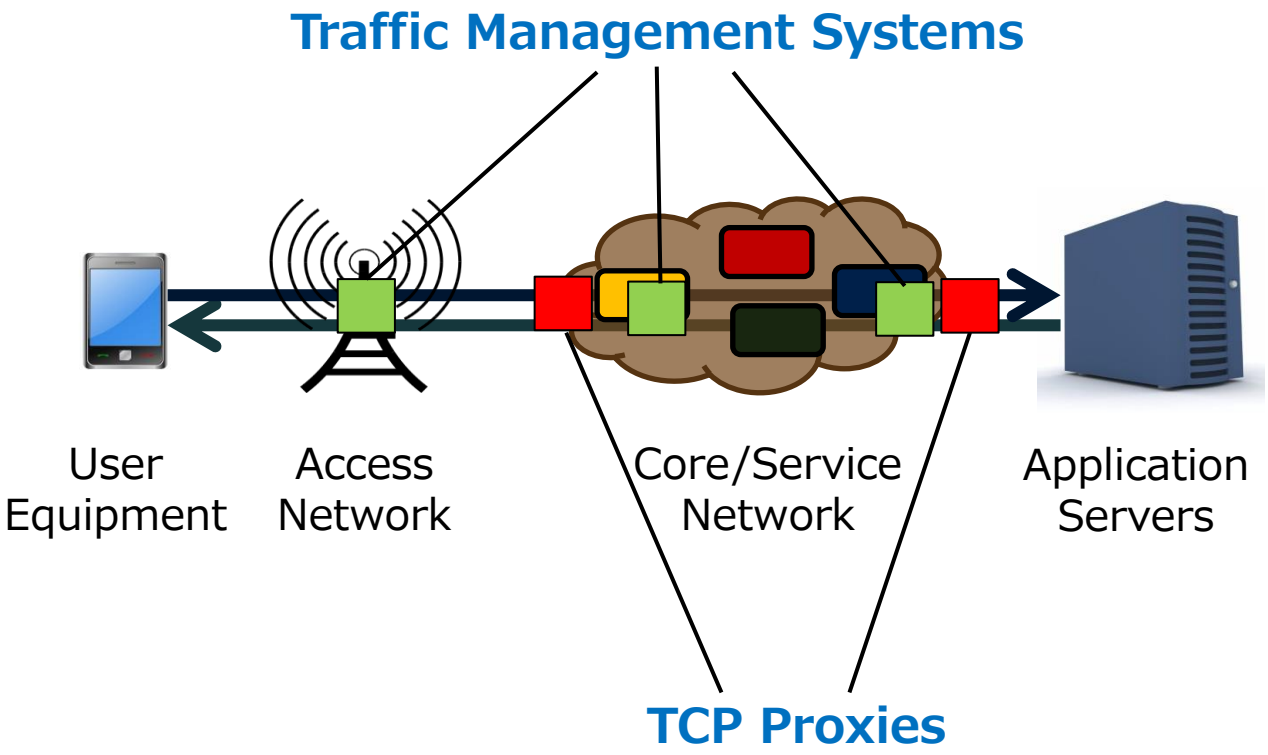
Performance and Security Today



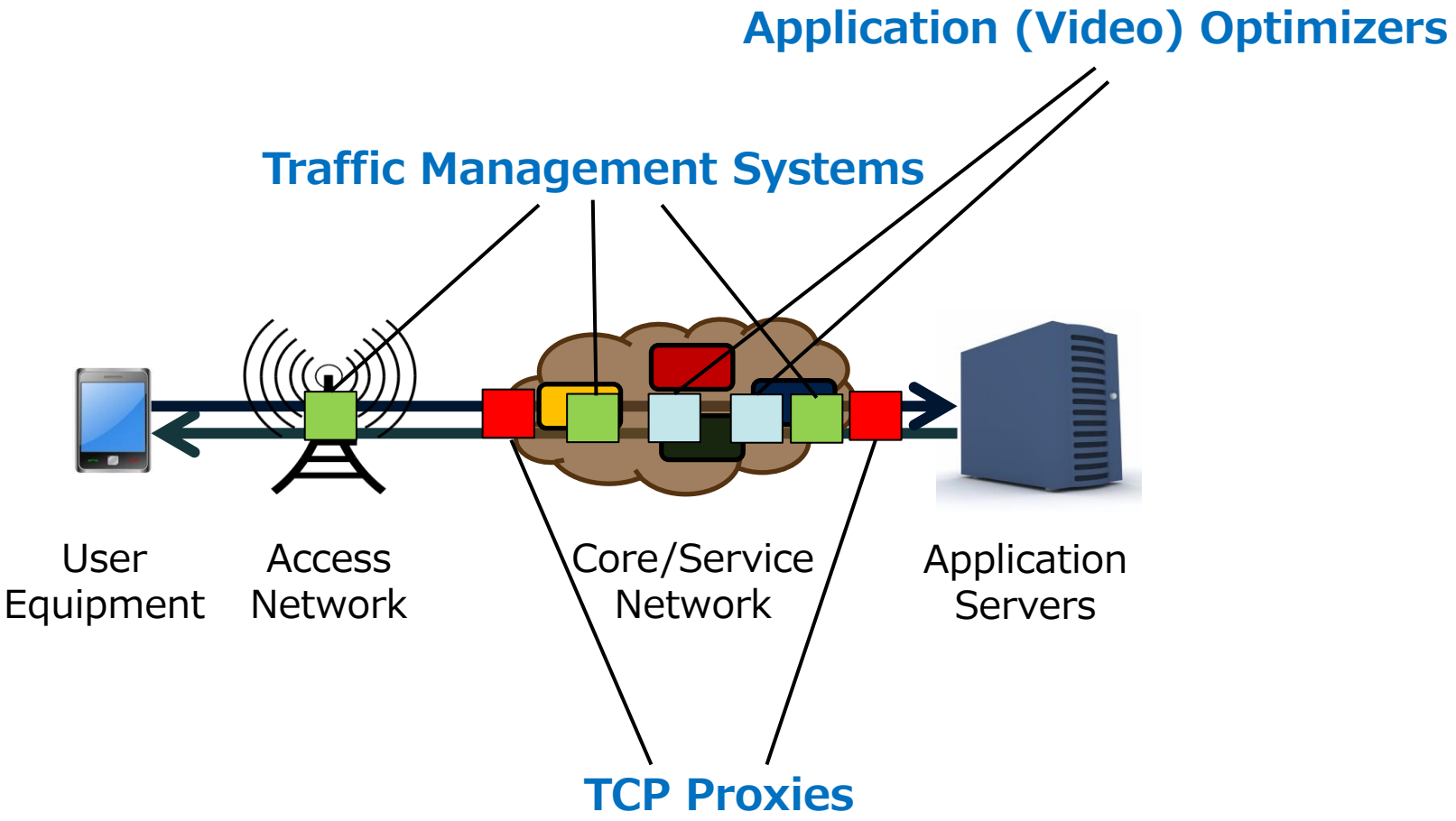
Performance and Security Today



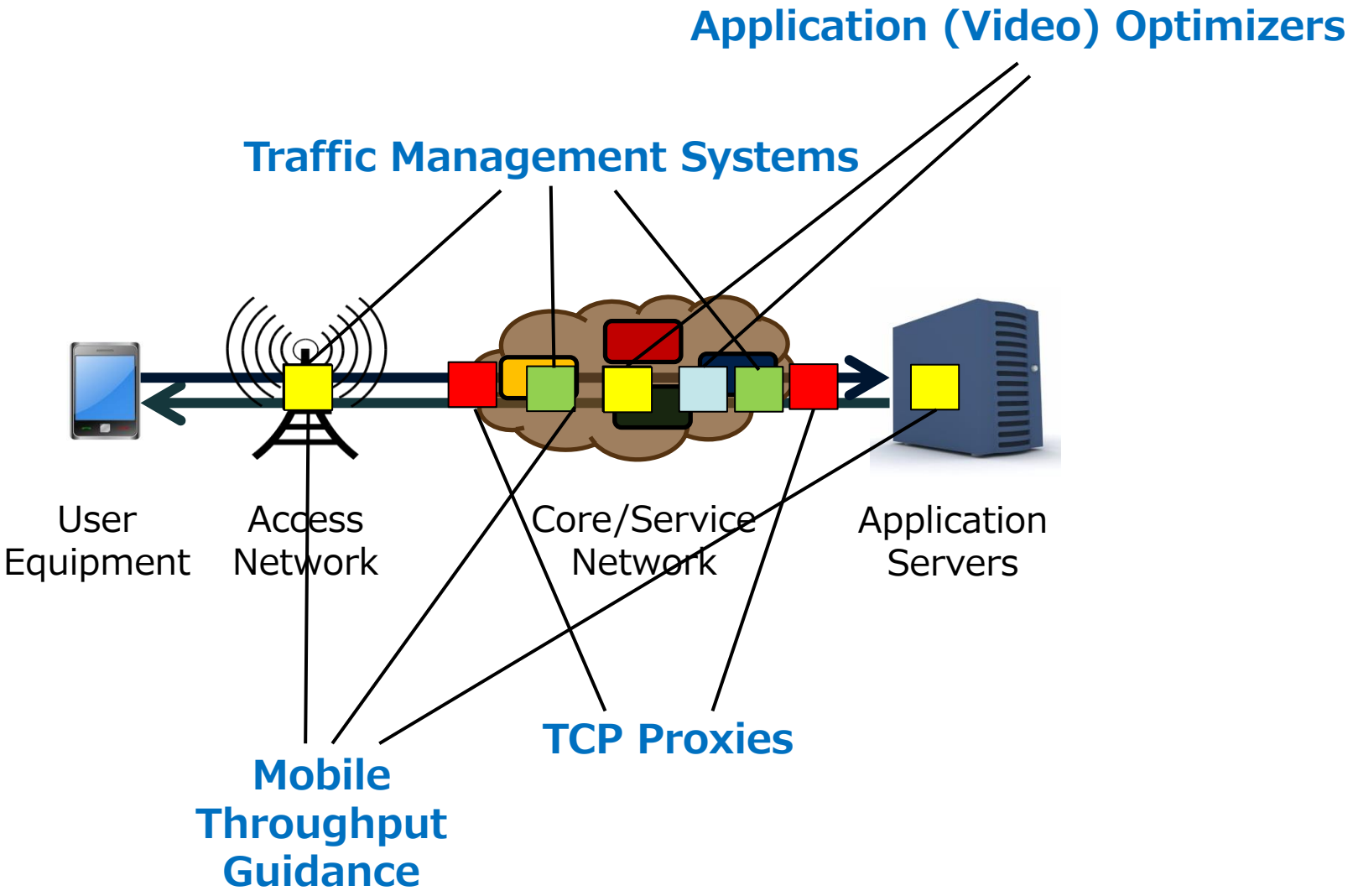
Performance and Security Today



Performance and Security Today



Performance and Security Today



Motivation

TCP proxies

- Lack of AQM and ECN deployment
- Sub-optimal performance: e2e control loop over heterogenous networks

Traffic management systems

- Lack of AQM and ECN deployment
- Lack of incentives for adaptive applications
- Perceived need for policing applications depending on access network conditions

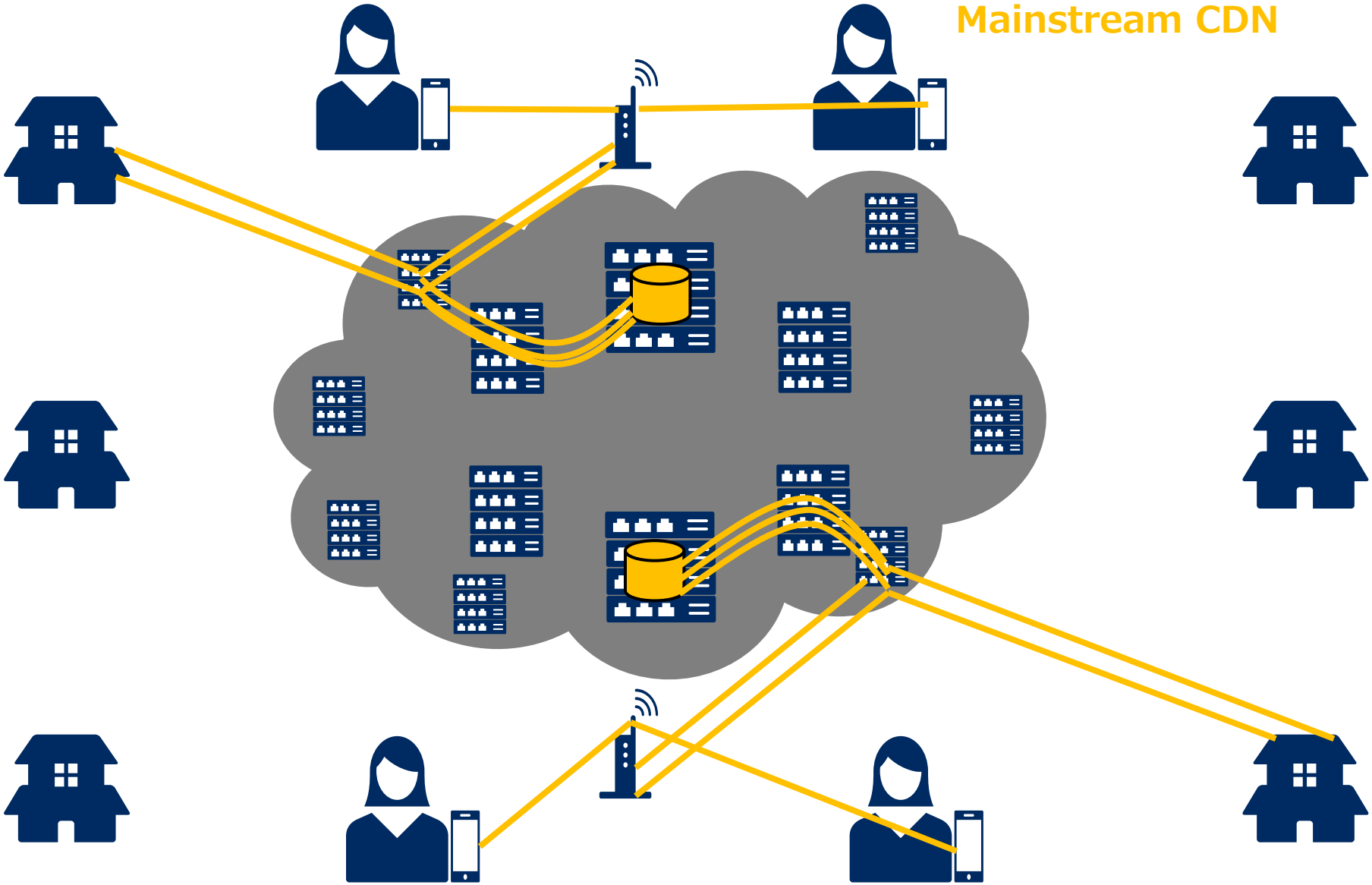
Application optimizers

- Operator resource conservation and performance concerns
- Access to user data for analytics

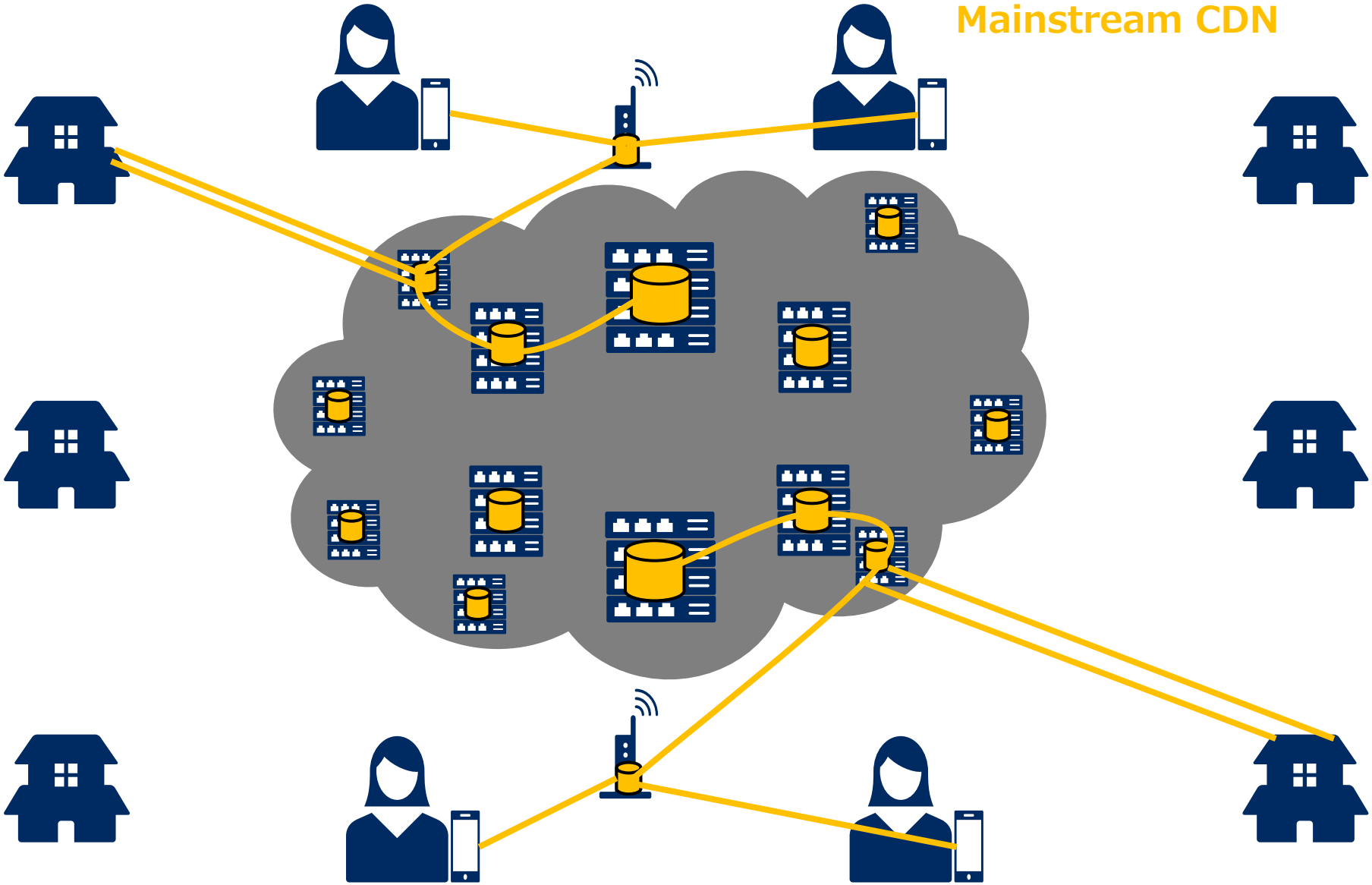
Mobile Throughput Guidance

- All of the above

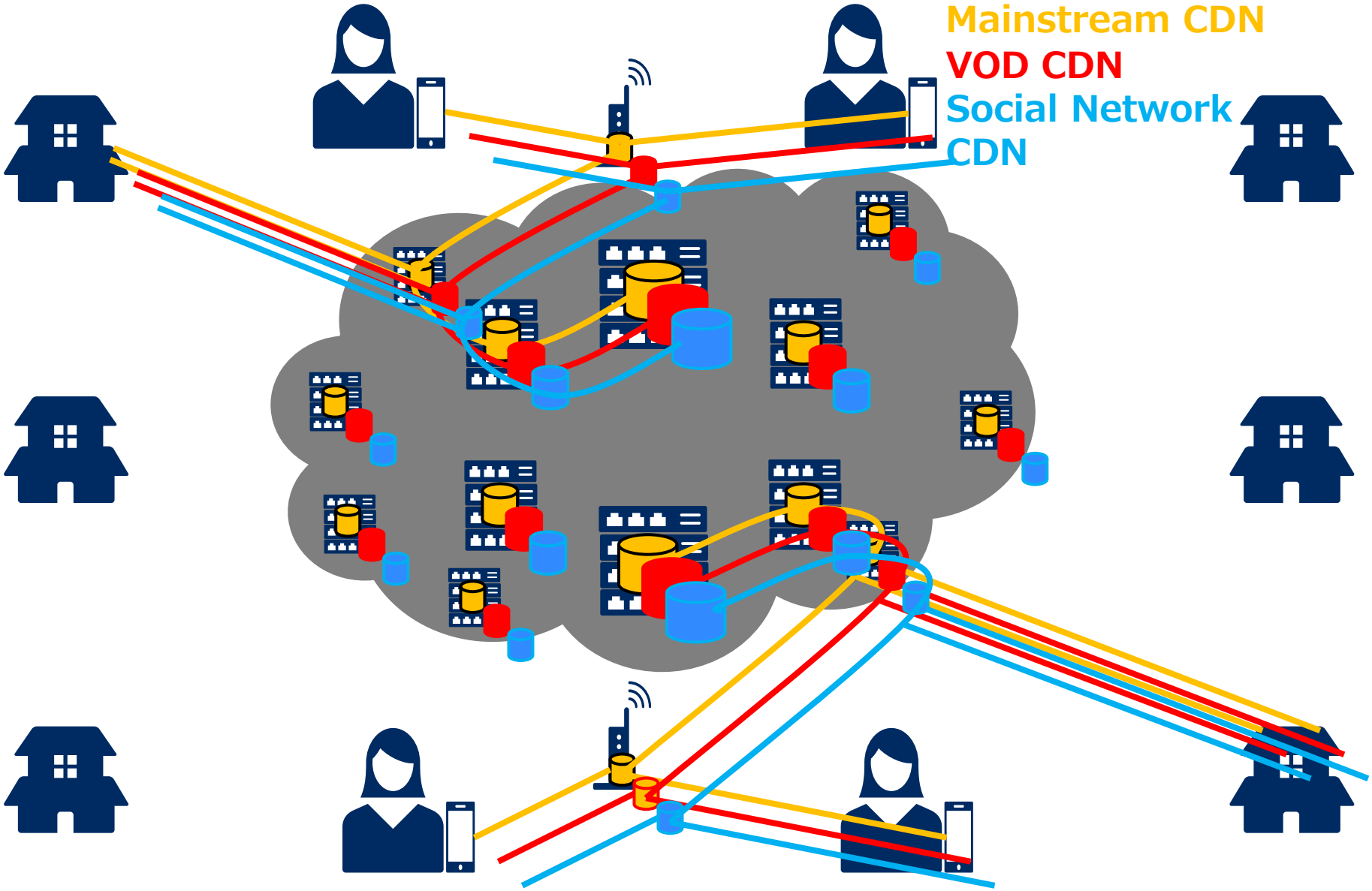
CDN Today



CDN Tomorrow



CDN Tomorrow: Silo Danger



Motivation

TCP proxies
- Lack of AQM and ECN deployment
- Sub-optimal performance: e2e control loop over heterogenous networks

Traffic management systems
- Lack of AQM and ECN deployment
- Lack of incentives for adaptive applications
- Perceived need for policing applications depending on access network conditions

Application optimizers
- Operator resource conservation and performance concerns
- Access to user data for analytics

Mobile Throughput Guidance
- All of the above

CDN
- Network offloading
- QoE improvement through latency reduction
- Moving data and computation closer to the edge
- Application-layer request/content routing policies

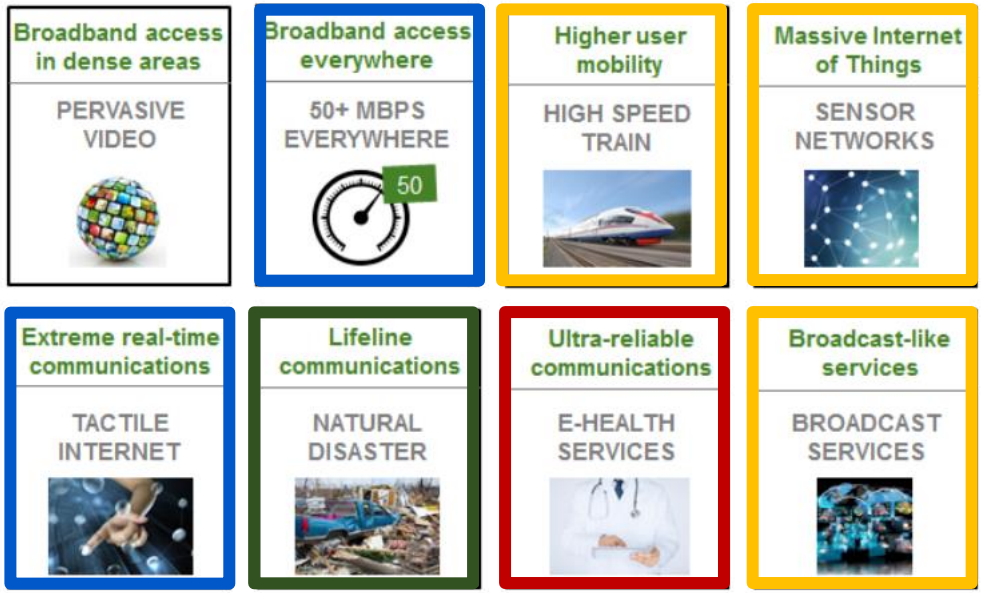
Observations

- Significant infrastructure required to make things „only work“ today
  - Overcoming TCP e2e performance issues in heterogenous networks
- Caching deemed important for scalable, low-latency data access
  - Deployment likely going to increase in next generation networks (edge caching)
  - General CDN and application-specific CDN deployments (new OTT services)
  - How many different CDN-like overlays will you have to run as an ISP?
- What does that mean for 5G networks?

NGMN 5G Use Cases

**Low latency,
local loop communication**

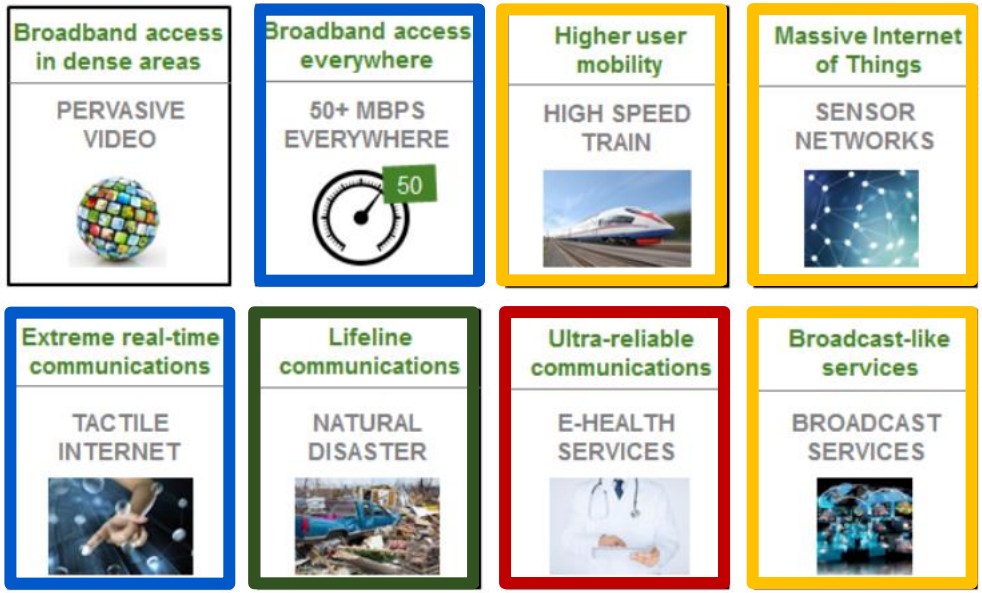
**Optimized Forwarding
for Heterogenous Access**



**Decentralized
Communication**

**Security,
User Privacy**

NGMN 5G Use Cases



Security,
User Privacy

Security & User Privacy

HTTP/2 is here to stay

- Connection-based encryption on transport layer (TLS)
  - Encrypt connection (and authenticate endpoints)
  - Encrypted channel for all communication
- De-facto ubiquitous (client implementations...)
- No (easy) way for traffic management (based on flow/application information)

Major concerns with network operators

- See recent GSMA/IAB workshop on Managing Radio Networks in an Encrypted World (MaRNEW)
- Many of the previously mentioned optimization become difficult/expensive/impossible

TLS and Future Deep CDN

CDN and TLS

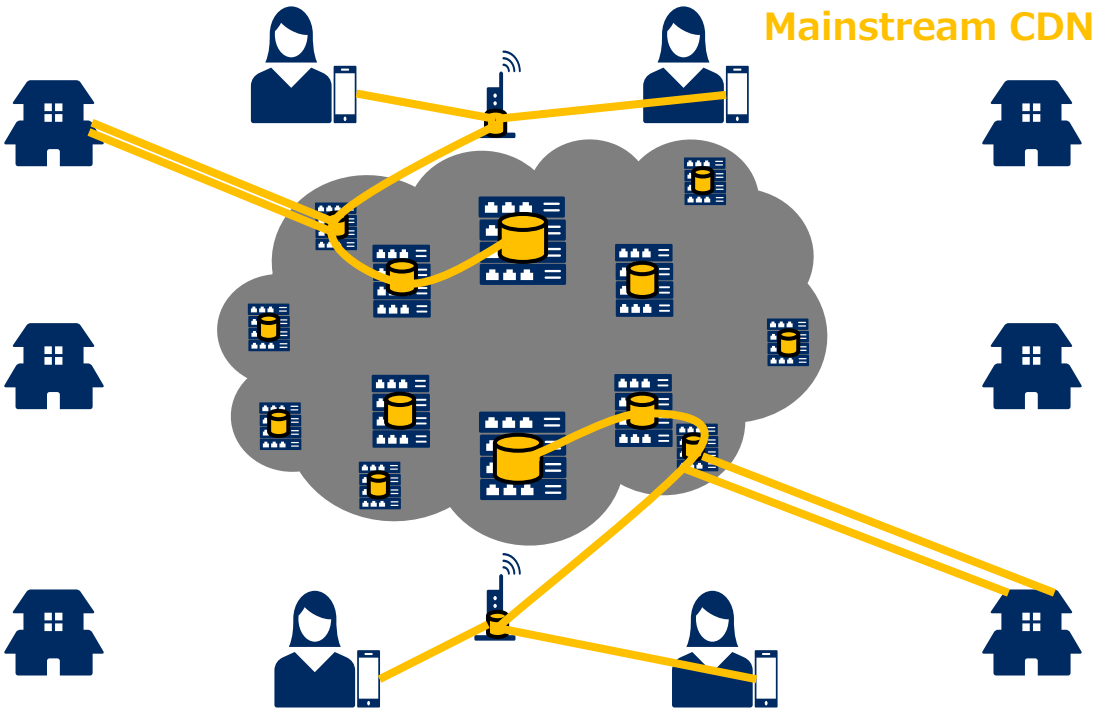
- CDN nodes maintain certificates on keying material on behalf of publishers
- Managing those certificates/keys is an important function of any CDN
- Protecting those certificates/keys is an important security requirement

Scaling CDNs

- More attack surfaces
- More challenges to certificate/key management
- User-privacy only guaranteed for connection to CDN proxy

Are there better ways?

- Object-based security
- Generic object caching & forwarding infrastructure



Optimized Forwarding for Heterogenous Access

Broadband access in dense areas

PERVASIVE VIDEO

Massive Internet of Things

SENSOR NETWORKS

Broadcast-like services

BROADCAST SERVICES

Higher user mobility

HIGH SPEED TRAIN

Low latency, high-bandwidth

- Fiber, new radios

Slow, ad-hoc, unpredictable

- Low-power radios, sleep/duty cycles
- Constrained devices

Massively scalable distribution

- Server-push or pub/sub style
- Possibly in-network adaptation

Variable performance

- Dynamically changing network conditions
- Disruptions and delays
- On-board caching for all applications & protocols

Optimized Forwarding for Heterogenous Access

Broadband access in dense areas

PERVASIVE VIDEO

Massive Internet of Things

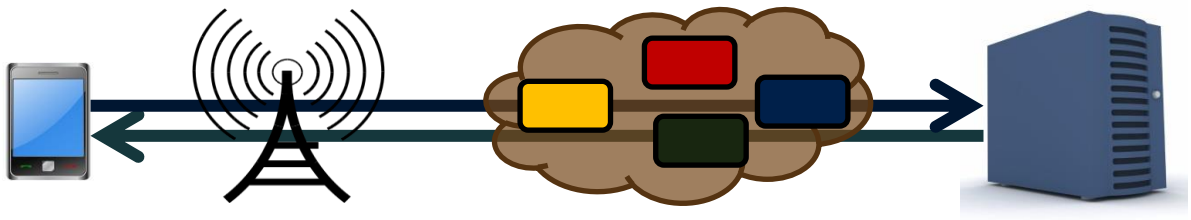
SENSOR NETWORKS

Broadcast-like services

BROADCAST SERVICES

Higher user mobility

HIGH SPEED TRAIN



- Will be difficult to implement with TCP as is
- Remember: reduced deployment options for application-layer gateways
- Network of TCP proxies does not sound convincing

- **Need more powerful forwarding layer and transport services**
  - Potential for hop-by-hop forwarding strategies
  - Caching for local retransmissions

Information-Centric Networking

Accessing Named Data Objects (NDOs) in the network

- ADUs, chunks, fragments

Data-centric security approach

- Disentangled means for name-content binding validation, publisher authentication, confidentiality

Name-Content binding validation:

- Public-Key and hash-based schemes

Publisher authentication

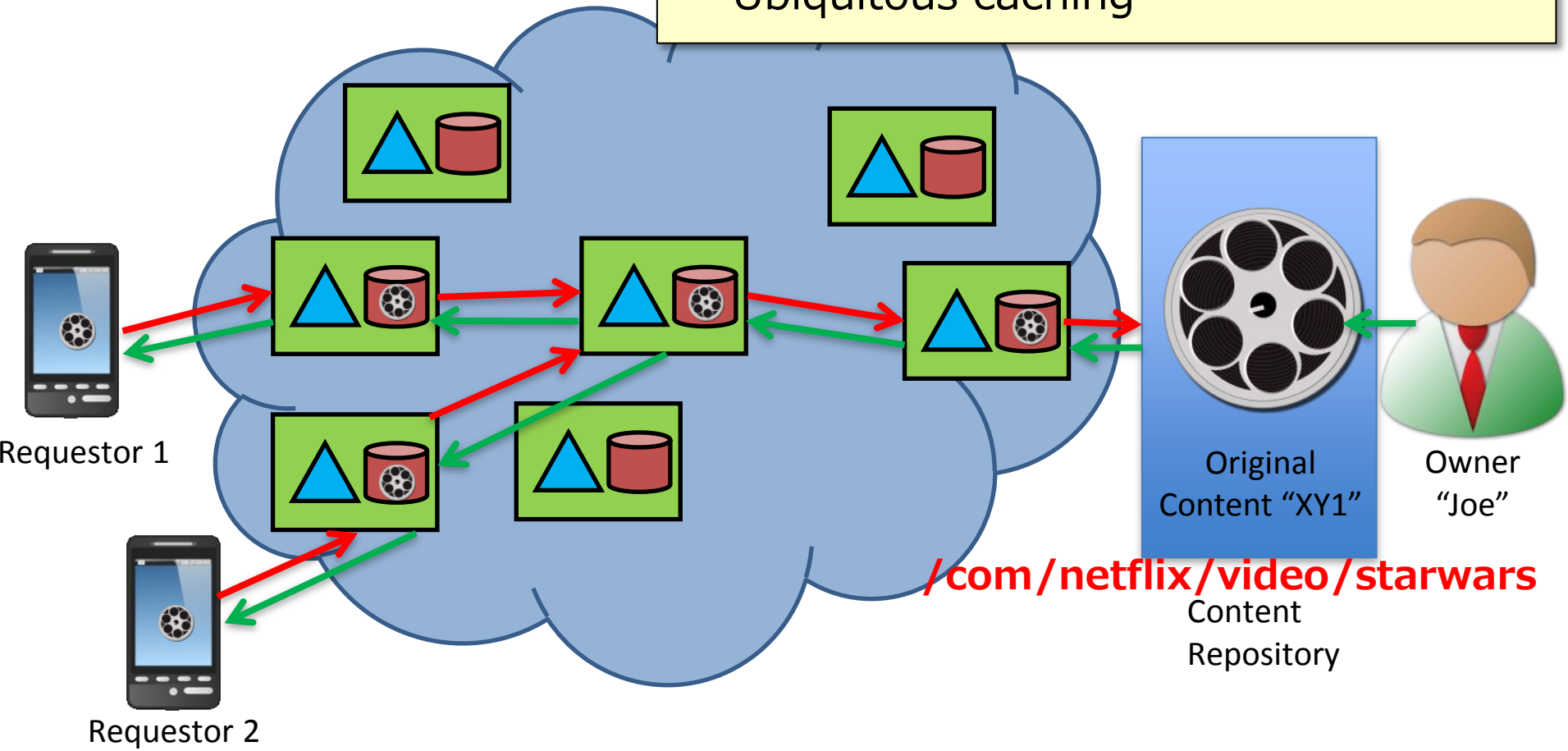
- One approach: publishers to sign NDOs, signature part of NDO meta data; trust model a la PKI

Confidentiality and access control

- Payload encryption

ICN Overview

- Request Response, Receiver-driven
- Pending Interesting Tables
- Forward-by-name (prefix)
- Per-node forwarding strategies
- Object-based security
- Ubiquitous caching



ICN Performance and Resource Management

Key ICN properties

- Requesting individual Named Data Objects
- Ubiquituous Caching

Implicit caching

- Every router can store NDO – depending on configuration, policy etc.
- Even with encrypted traffic, caching can help with local retransmissions, media re-play etc.

Simplified mobility management

- Request/Response model – eliminates need for tunnels

Flexible multipath communication

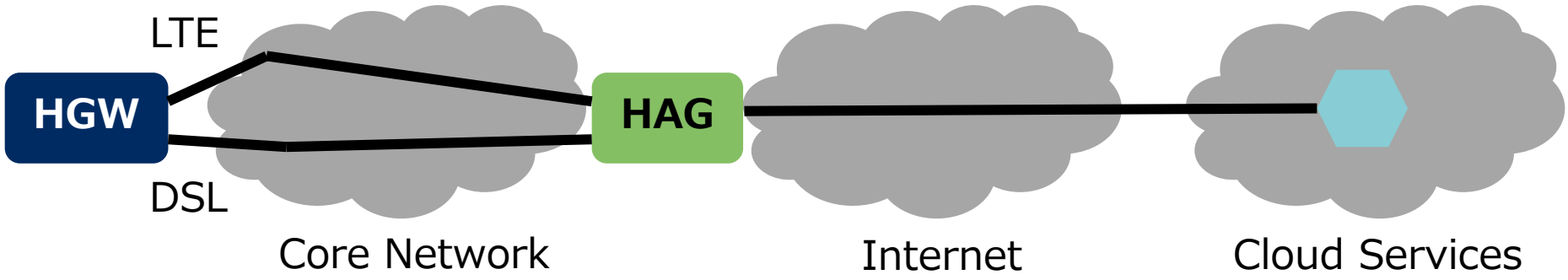
- **Powerful forwarding layer**
- Every router can make forwarding decisions depending on strategy, network characteristics, name prefix, policy

Easy policing and filtering

- Requestors, publishers and requestors see ICN requests and responses
- Policing without DPI
- Enabling other optimizations: in-network pre-fetching etc.

Proof-of-Concept

ICN for managing multi-path connectivity in Hybrid Access scenarios

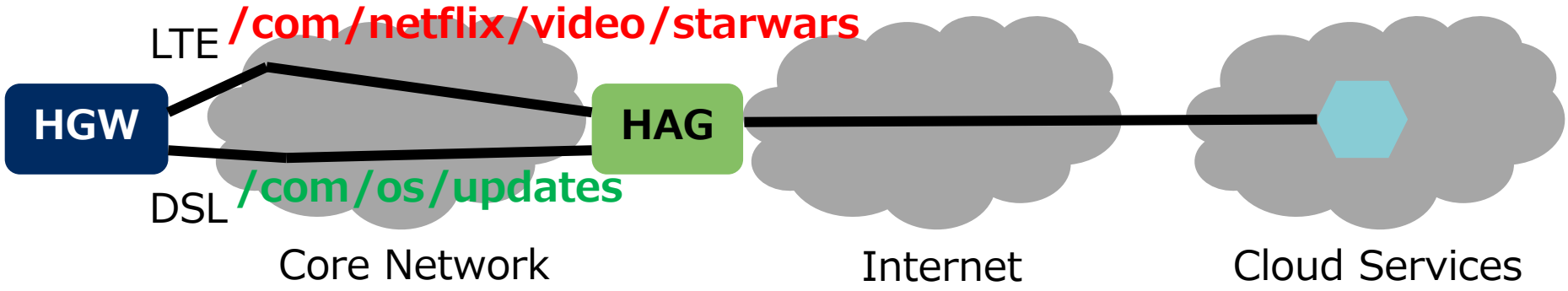


State of the art

- Connection Bundling over IP tunnels (GRE): poor performance with transport protocols
- MPTCP: better from transport perspective, but problematic interaction with CDN (DNS redirection per interface) and lack of policy control

Proof-of-Concept

ICN for managing multi-path connectivity in Hybrid Access scenarios



ICN approach

- **Routers have better visibility of interface performance** (can continously measure latency between requests and responses on a name-prefix basis)
- Easy to implement **policy based on request prefixes**
- Our implementation: **prioritizing critical applications** by constantly assessing interface performance and by assigning best interfaces to prioritized applications
- Works with **high degree of dynamicity** (mobile networks)

First results

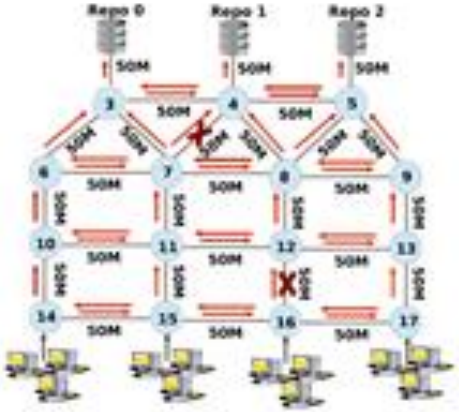
- Extremely fast response to congestion – on all nodes of a heterogenous path
- Constantly high capacity utilization
- Effective prioritization

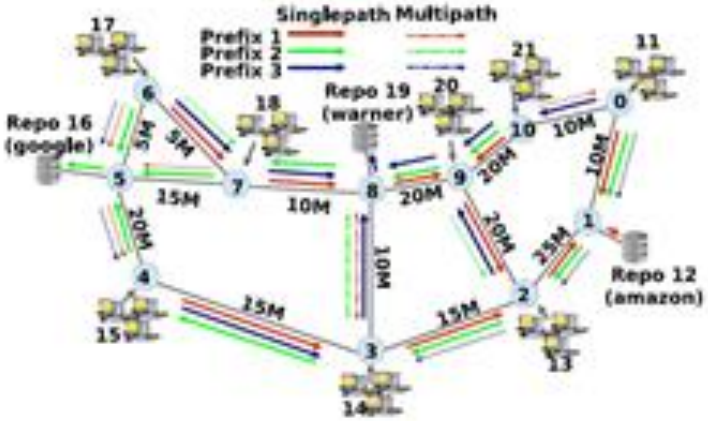
Other Recent Results

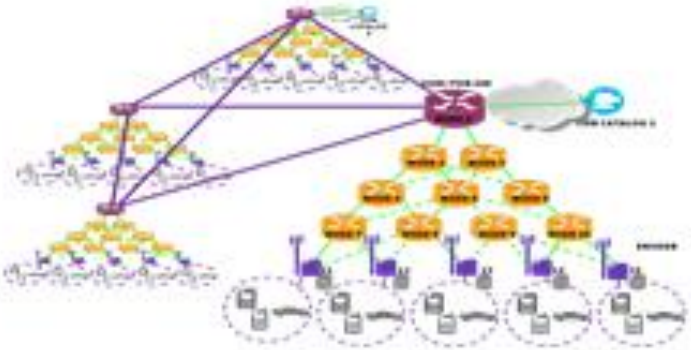
SystemX

Experiments

- **Large topologies**
  - Up to 100 physical nodes
  - More than 200 links
- **Realistic scenarios**
  - Mobile Backhaul







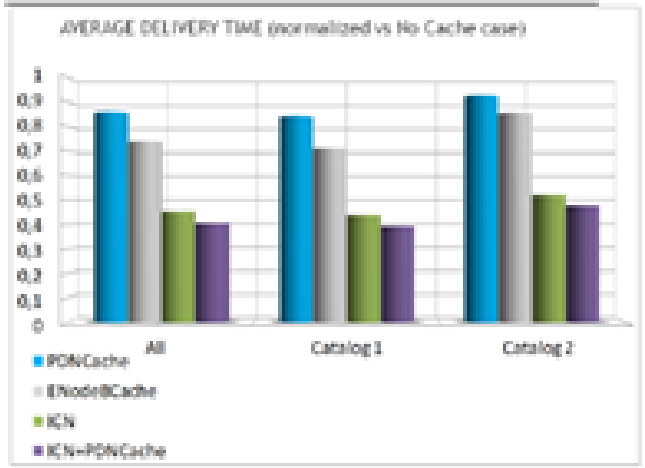
Alcatel-Lucent

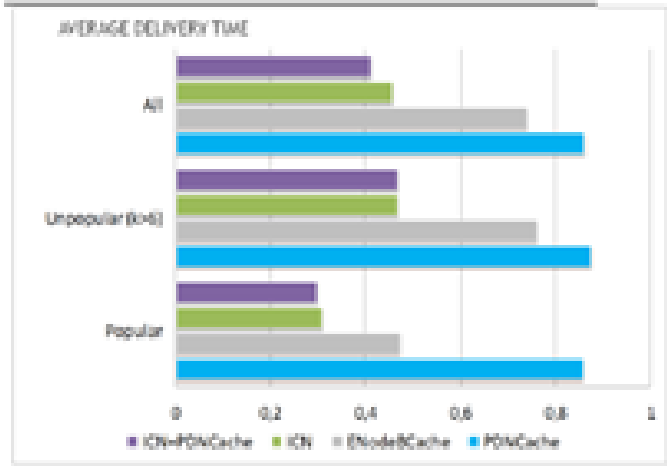
http://www.ietf.org/proceedings/interim/2014/09/27/icnrg/proceedings.html

Orange/ALU/SystemX Testbed Measurement Results

results – latency reduction

- ICN shows the better QoE in terms of delivery time
- Improved user QoE due to:
  - *in-network caching.*
  - *dynamic multipath transfer.*





– a factor 3 reduction in average delivery time

http://www.ietf.org/proceedings/interim/2014/09/27/icnrg/proceedings.html

5G Blueprint

Baseline IP e2e applications

M2M applications

In-network processing

IM, server applications

Interactive real-time

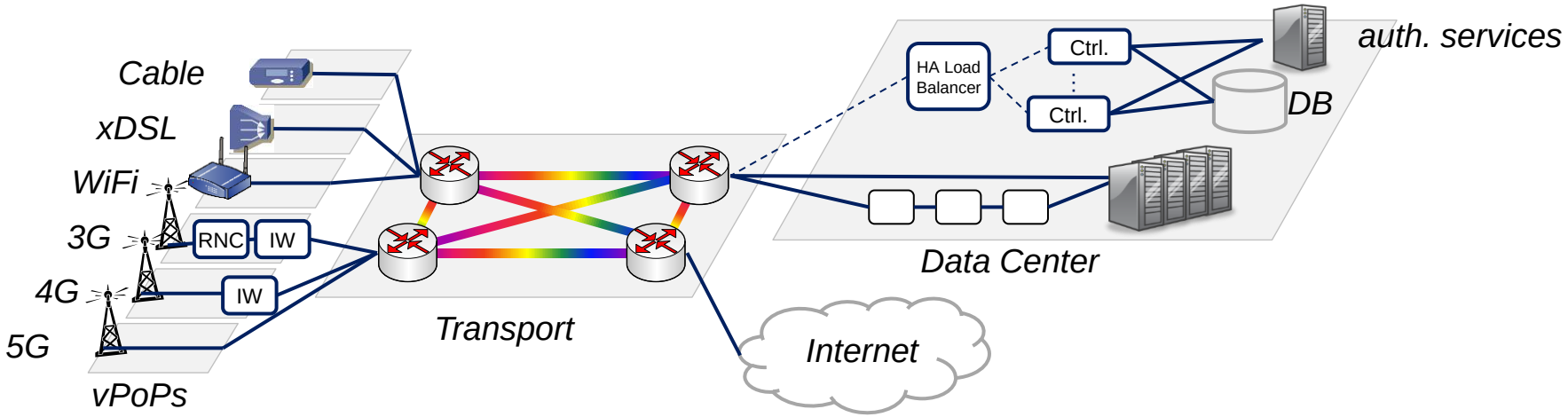
Video streaming, VOD

Caching, multicast

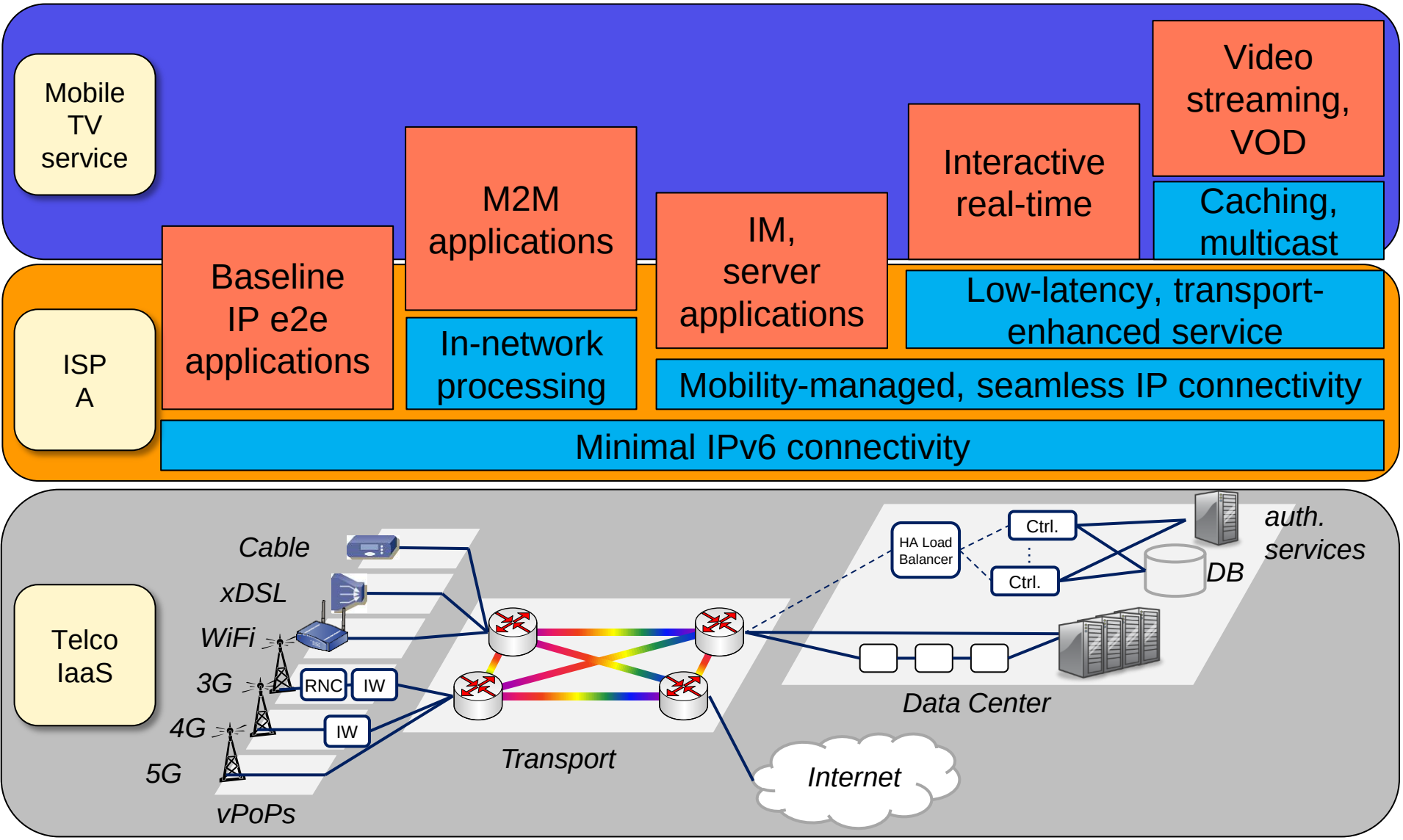
Low-latency, transport-enhanced service

Mobility-managed, seamless IP connectivity

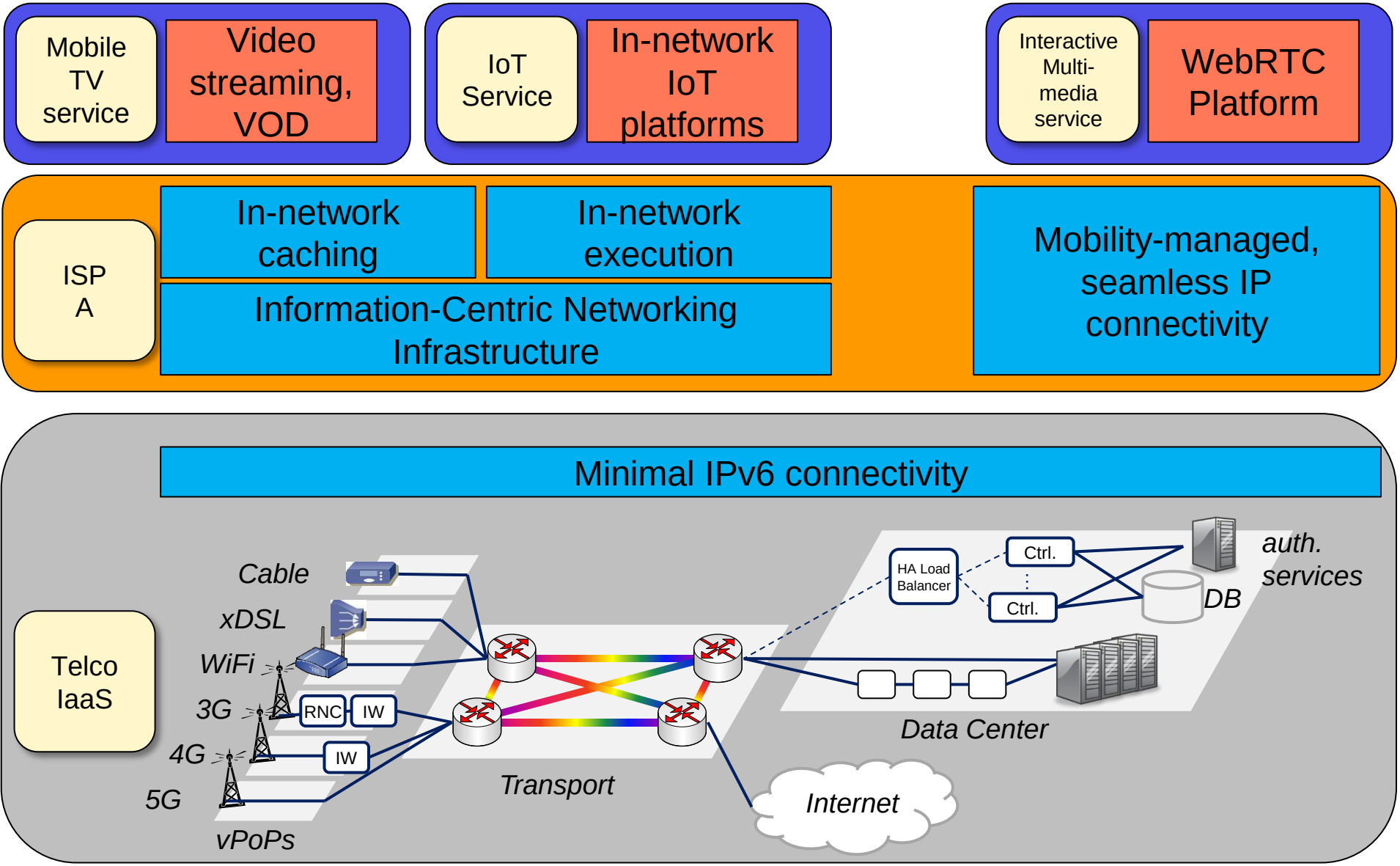
Minimal IPv6 connectivity



5G Multitenancy



Possible 5G ICN Deployment Option



Conclusions: 5G has challenges beyond SDN/NFV

Security

- User-privacy concerns one of the drivers for HTTP/2 (TLS) adoption
- Will reduce leverage for operators for „value-added service“, application-layer optimizations etc.
- Security challenges for TLS and (Deep) CDN

Performance

- 5G has potential for better performance due to new link layers and backhaul architectures
- But: heterogenous access and diverse use cases also imply new challenges

Information-Centric Networking

- **Data-centric communication** approach more suitable for secure and efficient communication
- **Powerful forwarding layer**: node-specific forwarding strategies thanks to better visibility of forwarding performance
- **Common infrastructure** for different types of applications: enabling efficient multi-tenancy operation without silos

IRTF ICNRG

Cross-project research community

- Not limited to a specific funding authority, project, protocol
- Sharing of research results, new ideas
- Documenting ICN scenarios, challenges, state-of-the-art solutions, gaps
- Specifying protocols and semantics for ICN
- Sharing implementation, experience from experiments

ICNRG and standards

- Not setting standards...
- But: helping to understand what needs to be standardized
- And: working on specifications

ICNRG Administrivia

- Web: http://irtf.org/icnrg
- Chairs
  - Börje Ohlman (Ericsson Research)
  - Dave Oran (Cisco Systems)
  - Dirk Kutscher (NEC Laboratories)

ICNRG Work Items

Scenarios, use cases

- Baseline scenarios (RFC 7476)
- Video distribution
- IoT
- Challenged networks and disaster scenarios

Challenges, evaluation

- Research challenges
- Evaluation Methodology

Protocol specifications

- CCNx Messages in TLV format
- CCNx Semantics

Newly proposed topics

- Manifests, chunking, fragmentation, versioning
- User privacy, access control
- Name resolution
- Named function networking

Documenting use cases & opportunities

Evolving research agenda & evaluation approaches

Creating interoperable platforms for experimentation

Evolving ICN concepts and technologies

Running Code

CCNx-1.0 (PARC)

- PARC license
- Developed by PARC
- Implements ccnx-messages and ccnx-semantics

CCN-lite (University of Basel)

- Open Source, free to use without restrictions
- Implements ccnx protocol
- Used by RIOT project

NDN NFD (NDN project)

- GPL-3.0
- Maintained by NDN project
- Implemented NDN protocol

Orchestrating a brighter world

未来に向かい、人が生きる、豊かに生きるために欠かせないもの。
それは「安全」「安心」「効率」「公平」という価値が実現された社会です。

NECは、ネットワーク技術とコンピューティング技術をあわせ持つ
類のないインテグレーターとしてリーダーシップを発揮し、
卓越した技術とさまざまな知見やアイデアを融合することで、
世界の国々や地域の人々と協奏しながら、
明るく希望に満ちた暮らしと社会を実現し、未来につなげていきます。


Orchestrating a brighter world
NEC