Authors: Prakash Suthar   Milan Stolic
         Google Inc.   Cisco Systems Inc.
         Anil Jangam, Ed.   Dirk Trossen
         Cisco Systems Inc.   Huawei Technologies
         Ravi Ravindran
         F5 Networks

Experimental Scenarios of ICN Integration in 4G Mobile Networks

Abstract

   4G mobile network uses IP-based transport for the control plane to
   establish the data session at the user plane for the actual data
   delivery. In the existing architecture, IP-based unicast is used for
   the delivery of multimedia content to a mobile terminal, where each
   user is receiving a separate stream from the server. From a
   bandwidth and routing perspective, this approach is inefficient.
   Evolved multimedia broadcast and multicast service (eMBMS) provides
   capabilities for delivering contents to multiple users
   simultaneously, but its deployment is very limited or at an
   experimental stage due to numerous challenges. The focus of this
   draft is to list the options for use of Information centric
   technology (ICN) in 4G mobile networks and elaborate the
   experimental setups for its further evaluation. The experimental
   setups discussed provide for using ICN either natively or with
   existing mobility protocol stack. With further investigations based
   on the listed experiments, ICN with its inherent capabilities such
   as, network-layer multicast, anchorless mobility, security, and
   optimized data delivery using local caching at the edge may provide
   a viable alternative to IP transport in 4G mobile networks.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

4G mobile technology is built as an all-IP network using routing
protocols (OSPF, ISIS, BGP, etc.) to establish network routes.
Stickiness of an IP address to a device is the key to get connected
to a mobile network. The same IP address is maintained through the
session until the device gets detached or moves to another network.

Key protocols used in 4G networks are GPRS Tunneling protocol (GTP),
DIAMETER, and other protocols that are built on top of IP. One of
the biggest challenges with IP-based routing in 4G is that it is not
optimized for data transport. As an alternative to IP routing, this
draft presents and list the possible options for integration of
Information Centric Networking (ICN) in 3GPP 4G mobile network,
offering an opportunity to leverage inherent ICN capabilities such
as in-network caching, multicast, anchorless mobility management,
and authentication. This draft also discuss how those options affect
mobile providers and end users.

The goal of the proposed experiments is to present possibilities to
create simulated environments for evaluation of the benefits of ICN
protocol deployment in a 4G mobile network in different scenarios
that have been analyzed in this document. The consensus of the
Information-Centric Networking Research Group (ICNRG) is to publish
this document in order to facilitate experiments to show deployment
options and qualitative and quantitative benefits of ICN protocol
deployment in 4G mobile networks.

2. 3GPP Terminology and Concepts

   1. Access Point Name

      The Access Point Name (APN) is a Fully Qualified Domain Name
      (FQDN) and resolves to a set of gateways in an operator's
      network. APN identifies the packet data network (PDN) with
      which a mobile data user wants to communicate. In addition to
      identifying a PDN, an APN may also be used to define the type
      of service, QoS, and other logical entities inside GGSN, PGW.

   2. Control Plane

      The control plane carries signaling traffic and is responsible
      for routing between eNodeB and MME, MME and HSS, MME and SGW,
      SGW and PGW, etc. Control plane signaling is required to
      authenticate and authorize the mobile terminal and establish a

mobility session with mobile gateways (SGW/PGW). Control plane functions also include system configuration and management.

3. Dual Address PDN/PDP Type

   The dual address Packet Data Network/Packet Data Protocol (PDN/PDP) Type (IPv4v6) is used in 3GPP context, in many cases as a synonym for dual stack, i.e., a connection type capable of serving IPv4 and IPv6 simultaneously.

4. eNodeB

   The eNodeB is a base station entity that supports the Long-Term Evolution (LTE) air interface.

5. Evolved Packet Core

   The Evolved Packet Core (EPC) is an evolution of the 3GPP GPRS system characterized by a higher-data-rate, lower-latency, packet-optimized system. The EPC comprises some sub components of the EPS core such as Mobility Management Entity (MME), Serving Gateway (SGW), Packet Data Network Gateway (PDN-GW), and Home Subscriber Server (HSS).

6. Evolved Packet System

   The Evolved Packet System (EPS) is an evolution of the 3GPP GPRS system characterized by a higher-data-rate, lower-latency, packet-optimized system that supports multiple Radio Access Technologies (RATs). The EPS comprises the EPC together with the Evolved Universal Terrestrial Radio Access (E-UTRA) and the Evolved Universal Terrestrial Radio Access Network (E-UTRAN).

7. Evolved UTRAN

   The E-UTRAN is a communications network sometimes referred to as 4G, and consists of eNodeB (4G base stations). The E-UTRAN allows connectivity between the User Equipment and the core network.

8. GPRS Tunneling Protocol

   The GPRS Tunneling Protocol (GTP) [TS29.060] [TS29.274] [TS29.281] is a tunneling protocol defined by 3GPP. It is a network-based mobility protocol, working similar to Proxy Mobile IPv6 (PMIPv6). However, GTP also provides functionality beyond mobility, such as in-band signaling related to QoS and charging, among others.

9. Gateway GPRS Support Node

The Gateway GPRS Support Node (GGSN) is a gateway function in
the GPRS and 3G network that provides connectivity to the
Internet or other PDNs. The host attaches to a GGSN identified
by an APN assigned to it by an operator. The GGSN also serves
as the topological anchor for addresses/prefixes assigned to
the User Equipment.

10. General Packet Radio Service

The General Packet Radio Service (GPRS) is a packet-oriented
mobile data service available to users of the 2G and 3G
cellular communication systems--the GSM--specified by 3GPP.

11. Home Subscriber Server

The Home Subscriber Server (HSS) is a database for a given
subscriber and was introduced in 3GPP Release-5. It is the
entity containing subscription-related information to support
the network entities that handle calls/sessions.

12. Mobility Management Entity

The Mobility Management Entity (MME) is a network element
responsible for control plane functionalities, including
authentication, authorization, bearer management, layer-2
mobility, and so on. The MME is essentially the control plane
part of the SGSN in the GPRS. The user plane traffic bypasses
the MME.

13. Public Land Mobile Network

The Public Land Mobile Network (PLMN) is a network operated by
a single administration. A PLMN (and, therefore, also an
operator) is identified by the Mobile Country Code (MCC) and
the Mobile Network Code (MNC). Each (telecommunications)
operator providing mobile services has its own PLMN.

14. Policy and Charging Control

The Policy and Charging Control (PCC) framework is used for QoS
policy and charging control. It has two main functions: flow-
based charging (including online credit control), and policy
control (for example, gating control, QoS control, and QoS
signaling). It is optional to 3GPP EPS but needed if dynamic
policy and charging control by means of PCC rules based on user
and services are desired.

15. Packet Data Network

The Packet Data Network (PDN) is a packet-based network that
either belongs to the operator or is an external network such
as the Internet or a corporate intranet. The user eventually
accesses services in one or more PDNs. The operator's packet
core networks are separated from packet data networks either by
GGSNs or PDN Gateways (PGWs).

16. Serving Gateway

The Serving Gateway (SGW) is a gateway function in the EPS,
which terminates the interface towards the E-UTRAN. The SGW is
the Mobility Anchor point for layer-2 mobility (inter-eNodeB
handovers). For each mobile terminal connected with the EPS,
there is only one SGW at any given point in time. The SGW is
essentially the user plane part of the GPRS's SGSN.

17. Packet Data Network Gateway

The Packet Data Network Gateway (PGW) is a gateway function in
the Evolved Packet System (EPS), which provides connectivity to
the Internet or other PDNs. The host attaches to a PGW
identified by an APN assigned to it by an operator. The PGW
also serves as the topological anchor for addresses/prefixes
assigned to the User Equipment.

18. Packet Data Protocol Context

A Packet Data Protocol (PDP) context is the equivalent of a
virtual connection between the mobile terminal (MT) and a PDN
using a specific gateway.

19. Packet Data Protocol Type

A Packet Data Protocol Type (PDP Type) identifies the used/
allowed protocols within the PDP context. Examples are IPv4,
IPv6, and IPv4v6 (dual-stack).

20. Serving GPRS Support Node

The Serving GPRS Support Node (SGSN) is a network element
located between the radio access network (RAN) and the gateway
(GGSN). A per-MT point-to-point (p2p) tunnel between the GGSN
and SGSN transports the packets between the mobile terminal and
the gateway.

21. Mobile Terminal/User Equipment

The terms User Equipment (UE), Mobile Station (MS), Mobile Node
(MN), and mobile refer to the devices that are hosts with the
ability to obtain Internet connectivity via a 3GPP network. An

MS comprises the Terminal Equipment (TE) and a Mobile Terminal
(MT). The terms MT, MS, MN, and mobile are used interchangeably
within this document.

22. User Plane

The user plane refers to data traffic and the required bearers
for the data traffic. In practice, IP is the only data traffic
protocol used in the user plane.

3. 4G Mobile Network Architecture

This section provide a high-level overview of typical 4G mobile
network architecture and their key functions related to a
possibility of using of ICN technology.

3.1. Network Overview

4G mobile networks are designed to use IP transport for
communication among different elements such as eNodeB, MME, SGW/PGW,
HSS, PCRF, etc. [GRAYSON]. For backward compatibility with 3G, it
has support for legacy Circuit Switch features such as voice and SMS
through transitional CS fallback and flexible IMS deployment. For
each mobile device attached to the radio (eNodeB), there is a
separate overlay tunnel (GPRS Tunneling Protocol, GTP) between
eNodeB and Mobile gateways (i.e., SGW, PGW).

When any mobile terminal is powered up, it attaches to a mobile
network based on its configuration and subscription. After a
successful attachment procedure, the mobile terminal registers with
the mobile core network using IPv4 and/or IPv6 address based on
request and capabilities offered by mobile gateways.

The GTP tunnel is used to carry user traffic between gateways and
mobile terminal, therefore using the unicast delivery for any data
transfer. It is also important to understand the overhead of GTP and
IPSec protocols. All mobile backhaul traffic is encapsulated using a
GTP tunnel, which has overhead of 8 bytes on top of IP and UDP
[NGMN]. Additionally, if IPSec is used for security (which is often
required if the Service Provider is using a shared backhaul), it
adds overhead based on the IPSec tunneling model (tunnel or
transport) as well as the encryption and authentication header
algorithm used. If we consider as an example an Advanced Encryption
Standard (AES) encryption, the overhead can be significant
[OLTEANU], particularly for smaller payloads.

```
                                    +-------+  Diameter  +-------+
                                    |  HSS  |------------|  SPR  |
                                    +-------+            +-------+
                                        |                    |
           +------+   +------+    S4     |                +-------+
           |  3G  |---| SGSN |----------------|------+  +------|  PCRF |
       ^   |NodeB |   |      |---------+  +---+      |  |      +-------+
    +-+ |  +------+   +------+  S3     |  | S6a      |  |Gxc       |
    | | |                      +-------+           |  |         |Gx
    +-+ |      +------------------|  MME  |------+  |  |          |
    MT  v      |       S1MME      +-------+  S11 |  |  |          |
        +----+-+                            +-------+     +-------+
        |4G/LTE|----------------------------|  SGW  |-----|  PGW  |
        |eNodeB|            S1U             +-------+  +--|       |
        +------+                                        |  +-------+
                            +--------------------+    |  |
      S1U GTP Tunnel traffic         |              +-------+        |  |
      S2a GRE Tunnel traffic         |S2A           | ePDG  |-------+  |
      S2b GRE Tunnel traffic         |              +-------+  S2B     |SGi
      SGi IP traffic                 |                 |                |
                            +---------+   +---------+      +-----+
                            | Trusted |   |Untrusted|      | CDN |
                            |non-3GPP |   |non-3GPP |      +-----+
                            +---------+   +---------+
                                 |             |
                                +-+           +-+
                                | |           | |
                                +-+           +-+
                                MT            MT
```

Figure 1: 4G Mobile Network Overview

   If we consider the combined impact of GTP, IPSec and unicast
   traffic, the data delivery is not efficient because of overhead. The
   IETF has developed various header compression algorithms to reduce
   the overhead associated with IP packets. Some techniques are robust
   header compression (ROHC) and enhanced compression of the real-time
   transport protocol (ECRTP) so that the impact of overhead created by
   GTP, IPsec, etc., is reduced to some extent [BROWER]. For commercial
   mobile networks, 3GPP has adopted different mechanisms for header
   compression to achieve efficiency in data delivery [TS25.323]; those
   solutions can be adapted to other data protocols, such as ICN, too
   [ICNLOWPAN] [TLVCOMP].

3.2. Mobile Network Quality of Service

   During the mobile terminal attachment procedure, a default bearer is
   created for each mobile terminal and it is assigned to the default
```

Access Point Name (APN), which provides the default transport. For
any QoS-aware application, one or more new dedicated bearers are
established between eNodeB and Mobile Gateway. Dedicated bearer can
be requested either by mobile terminal or mobile gateway based on
direction of first data flow. There are many bearers (logical paths)
established between eNodeB and mobile gateway for each mobile
terminal catering to different data flow simultaneously.

While all traffic within a certain bearer receives the same
treatment, QoS parameters supporting these requirements can be very
granular in different bearers. These values vary for the control,
management and user traffic, and can be very different depending on
application key parameters such as latency, jitter (important for
voice and other real-time applications), packet loss, and queuing
mechanism (strict priority, low-latency, fair, and so on).

Implementation of QoS for mobile networks is done at two stages: at
content prioritization/marking and transport marking, and congestion
management. From the transport perspective, QoS is defined at layer
2 as class of service (CoS) and at layer 3 as Differentiated
Services (DS). The mapping of DSCP to CoS takes place at layer 2/3
switching and routing elements. 3GPP has a specified a QoS Class
Identifier (QCI), which represents different types of content and
equivalent mappings to the DSCP at transport layer [TS23.401].
However, this requires manual configuration at different elements
and is therefore prone to possible misconfigurations.

In summary, QoS configuration in mobile networks for user plane
traffic requires synchronization of parameters among different
platforms. Normally, QoS in IP is implemented using DiffServ, which
uses hop-by-hop QoS configuration at each router. Any inconsistency
in IP QoS configuration at routers in the forwarding path can result
in a poor subscriber experience (e.g., packet classified as high
priority can go to a lower priority queue). By deploying ICN, we
intend to enhance the subscriber experience using policy-based
configuration, which can be associated with the named contents
[ICNQoS] at the ICN forwarder. Further investigation is underway to
understand how QoS in ICN [I-D.anilj-icnrg-dnc-qos-icn] can be
implemented with reference to the ICN QoS guidelines [RFC9064] to
meet the QoS requirements [RFC4594].

### 3.3.  Data Transport Using IP

The data delivered to mobile devices is sent in unicast semantic
inside the GTP tunnel from an eNodeB to a PDN gateway (PGW), as
described in 3GPP specifications [TS23.401]. While the technology
exists to address the issue of possible multicast delivery, there
are many difficulties related to multicast protocol implementations
on the RAN side of the network. By using eMBMS [EMBMS], multicast

routing can be enabled in mobile backhaul between eNodeB and Mobile
Gateways (SGW) however for radio interface it requires broadcast
which implies that we need dedicated radio channel. Implementation
of eMBMS in RAN is still lagging behind due to complexities related
to client mobility, handovers, and the fact that the potential gain
to Service Providers may not justify the investment, which explains
the prevalence of unicast delivery in mobile networks. Techniques to
handle multicast (such as LTE-B or eMBMS) have been designed to
handle pre-planned content delivery, such as live content, which
contrasts user behavior today, largely based on content (or video)
on demand model.

To ease the burden on the bandwidth of the SGi interface, caching is
introduced in a similar manner as with many Enterprises. In mobile
networks, whenever possible, cached data is delivered. Caching
servers are placed at a centralized location, typically in the
Service Provider's Data Center, or in some cases lightly distributed
in Packet Core locations with the PGW nodes close to the Internet
and IP services access (SGi interface). This is a very inefficient
concept because traffic must traverse the entire backhaul path for
the data to be delivered to the end user. Other issues, such as out-
of-order delivery, contribute to this complexity and inefficiency,
which needs to be addressed at the application level.

## 3.4.  Virtualized Mobile Networks

The Mobile gateways deployed in a major Service Provider network are
either based on dedicated hardware or, commercially off the shelf
(COTS) based x86 technology. With the adoption of Mobile Virtual
Network Operators (MVNO), public safety networks, and enterprise
mobility networks, elastic mobile core architecture are needed. By
deploying the mobile packet core on COTS platform, using a
virtualized infrastructure (NFVI) framework and end-to-end
orchestration, new deployments can be simplified to provide
optimized total cost of ownership (TCO).

While virtualization is growing, and many mobile providers use a
hybrid architecture that consists of dedicated and virtualized
infrastructures, the control, and data planes are still the same.
There is also work under way to separate the control and user plane
for the network to scale better. Virtualized mobile networks and
network slicing with control and user plane separation provide a
mechanism to evolve the GTP-based architecture towards an OpenFlow
SDN-based signaling for 4G and proposed 5G core. Some early
architecture work for 5G mobile technologies provides a mechanism
for control and user plane separation and simplifies the mobility
call flow by introducing OpenFlow-based signaling [ICN5G]. This has
been considered by 3GPP [EPCCUPS] and is also described in [SDN5G].

## 4.  Data Transport Using ICN

For mobile devices, the edge connectivity is between mobile terminal
and a router or mobile edge computing (MEC) [MECSPEC] element. Edge
computing has the capability of processing client requests and
segregating control and user traffic at the edge of radio, rather
than sending all requests to the mobile gateway.

```
    +----------+
    | Content  +-----------------------------------------+
    | Publisher|                                         |
    +---+---+--+                                         |
        |   |    +--+              +--+            +--+   |
        |   +--->|R1|------------->|R2|----------->|R4|   |
        |        +--+              +--+            +--+   |
        |                           |    Cached          |
        |                           v    content         |
        |                          +--+  at R3            |
        |              +========|R3|---+               |
        |              #         +--+   |                |
        |              #                |                |
        |              v                v                |
        |             +-+              +-+               |
    +---------------| |-------------| |-------------+
                     +-+              +-+
               Consumer-1       Consumer-2
              Mobile Terminal  Mobile Terminal
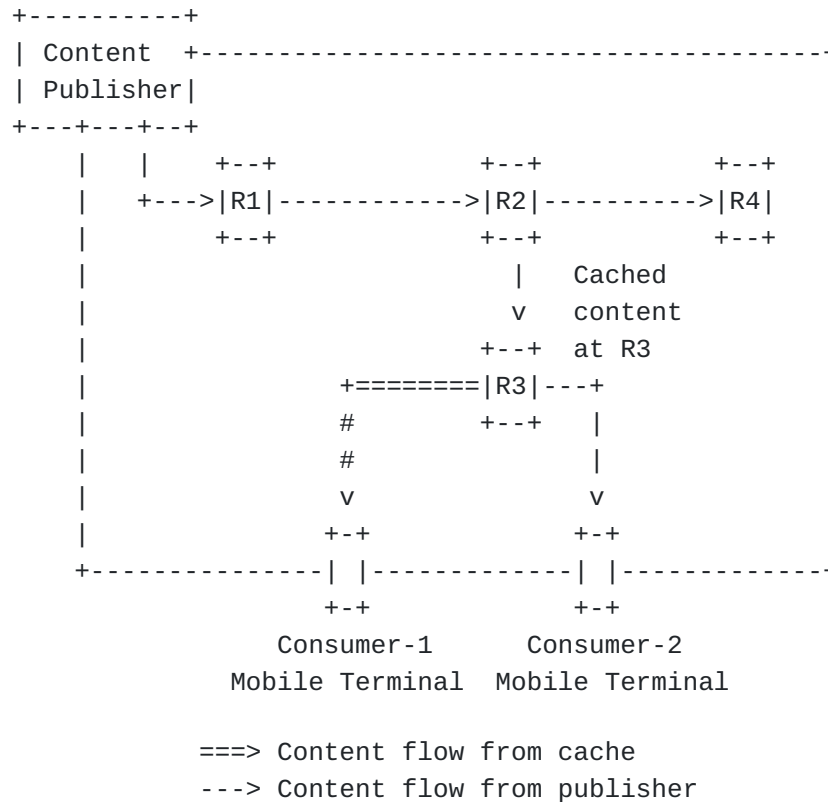
            ===> Content flow from cache
            ---> Content flow from publisher
```

Figure 2: ICN Architecture

Edge computing transforms radio access network into an intelligent
service edge capable of delivering services directly from the edge
of the network, while providing the best possible performance to the
client. Edge computing can be an ideal candidate for implementing
ICN forwarders in addition to its usual function of managing mobile
termination. In addition to edge computing, other transport
elements, such as routers, can work as ICN forwarders.

Data transport using ICN is different to IP-based transport by
introducing uniquely named-data as a core design principle.
Communication in ICN takes place between the content provider
(producer) and the end user (consumer), as described in Figure 2.

Every node in a physical path between a client and a content
provider is called the ICN forwarder or router. It can route the

request intelligently and cache content so it can be delivered
locally for subsequent requests from any other client. For mobile
networks, transport between a client and a content provider consists
of radio network + mobile backhaul and IP core transport + Mobile
Gateways + Internet + content data network (CDN).

To understand the suitability of ICN for mobile networks, we will
discuss the ICN framework by describing its protocols architecture
and different types of messages to then consider how we can use this
in mobile networks for delivering content more efficiently. ICN uses
two types of packets called "interest packet" and "data packet" as
described in Figure 3.

```
                  +------------------------------------+
        Interest | +------+     +------+     +------+ |         +-----+
+-+         ---->|  CS  |---->| PIT  |---->| FIB  |--------->| CDN |
| |              | +------+     +------+     +------+ |         +-----+
+-+              |      |    Add  |       Drop  |     | Forward
MT              <--------+    Intf v       Nack v     |
        Data  |                                       |
                  +------------------------------------+
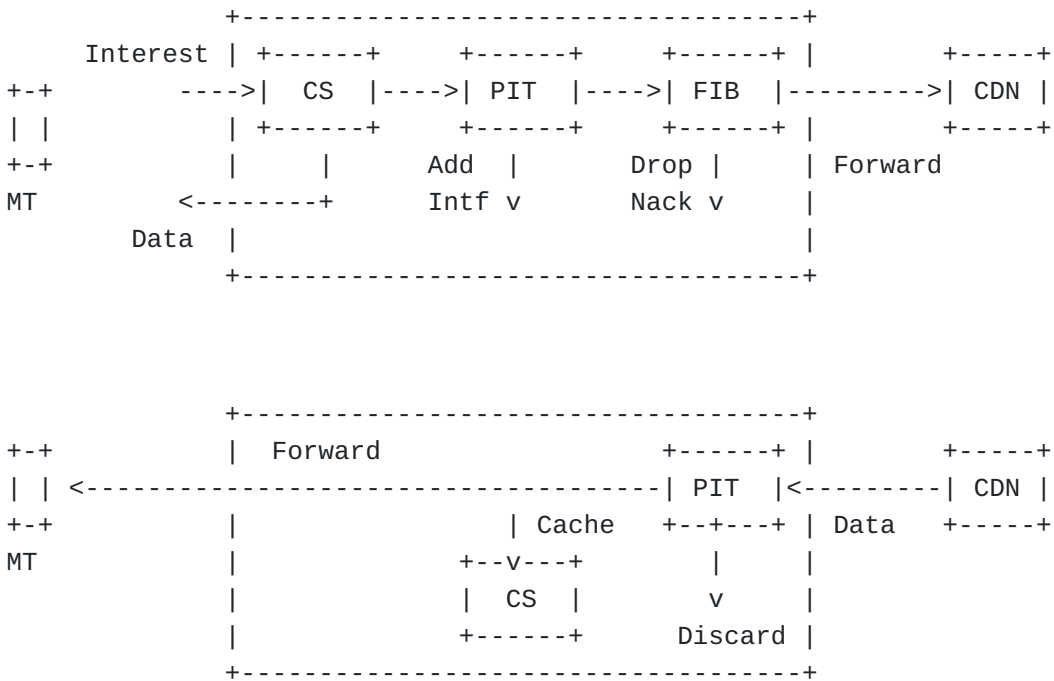


                  +------------------------------------+
+-+               | Forward                   +------+ |         +-----+
| | <------------------------------------| PIT  |<---------| CDN |
+-+               |                   | Cache  +--+---+ | Data    +-----+
MT               |            +--v---+       |    |
                 |            | CS  |        v    |
                 |            +------+      Discard |
                  +------------------------------------+
```

              Figure 3: ICN Interest, Data Packet and Forwarder

In an 4G network, when a mobile device wants to receive certain
content, it will send an Interest message to the closest eNodeB.
Interest packets follow the TLV format [RFC8609] and contain
mandatory fields, such as name of the content and content matching
restrictions (KeyIdRestr and ContentObjectHashRestr), expressed as a
tuple [RFC8569]. The content matching tuple uniquely identifies the
matching data packet for the given Interest packet. Another
attribute called HopLimit is used to detect looping Interest
messages.

An ICN router will receive an Interest packet and lookup if a
request for such content has arrived earlier from another client. If
so, it may be served from the local cache; otherwise, the request is

forwarded to the next-hop ICN router. Each ICN router maintains
three data structures: Pending Interest Table (PIT), Forwarding
Information Base (FIB), and Content Store (CS). The Interest packet
travels hop-by-hop towards the content provider. Once the Interest
packet reaches the content provider, it will return a Data packet
containing information such as content name, signature, and the
actual data.

The data packet travels in reverse direction following the same path
taken by the Interest packet, maintaining routing symmetry. Details
about algorithms used in PIT, FIB, CS, and security trust models are
described in various resources [CCN]; here, we have explained the
concept and its applicability to the 4G network.

5. Experimental Scenarios for ICN Deployment

In 4G mobile networks, both user and control plane traffic have to
be transported from the edge to the mobile packet core via IP
transport. The evolution of the existing mobile packet core using
Control and User Plane Separation (CUPS) [TS23.714] enables flexible
network and operations by distributed deployment and the independent
scaling of control plane and user plane functions - while not
affecting the functionality of existing nodes subject to this split.

In this section, we analyze the potential impact of ICN on control
and user plane traffic for centralized and disaggregated CUPS-based
mobile network architecture. We list various experimental options
and opportunities to study the feasibility of the deployment of ICN
in 4G networks. The proposed experiments would help the network and
OEM designers to understand various issues, optimizations, and
advantages of deployment of ICN in 4G networks.

5.1. General Considerations

In the CUPS architecture, there is an opportunity to shorten the
path for user plane traffic by deploying offload nodes closer to the
edge [OFFLOAD]. With this major architecture change, a User Plane
Function (UPF) node is placed close to the edge so traffic no longer
needs to traverse the entire backhaul path to reach the EPC. In many
cases, where feasible, the UPF can be collocated with the eNodeB,
which is also a business decision based on user demand. Placing a
Publisher close to the offload site, or at the offload site,
provides for a significant improvement in user experience,
especially with latency-sensitive applications. This capability
allows for the introduction of ICN and amplifies its advantages.

5.2. Scenarios of ICN Integration

The integration of ICN provides an opportunity to further optimize
the existing data transport in 4G mobile networks. The various

opportunities from the coexistence of ICN and IP transport in the
mobile network are somewhat analogous to the deployment scenarios
when IPv6 was introduced to interoperate with IPv4 except, with ICN,
the whole IP stack can be replaced. We have reviewed [RFC6459] and
analyzed the impact of ICN on control plane signaling and user plane
data delivery. In general, ICN can be used natively by replacing IP
transport (IPv4 and IPv6) or as an overlay protocol. Figure 4
describes a proposal to modify the existing transport protocol stack
to support ICN in 4G mobile network.

```
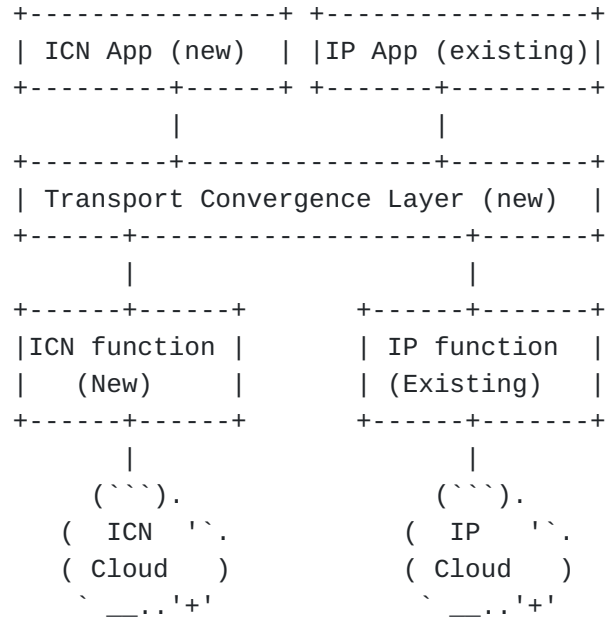          +----------------+ +----------------+
          | ICN App (new)  | |IP App (existing)|
          +---------+------+ +-------+---------+
                    |                |
          +---------+----------------+---------+
          | Transport Convergence Layer (new)  |
          +------+---------------------+-------+
                 |                     |
          +------+------+       +------+-------+
          |ICN function |       | IP function  |
          |   (New)     |       | (Existing)   |
          +------+------+       +------+-------+
                 |                     |
             (```).                 (```).
            (   ICN   '`.          (   IP    '`.
            ( Cloud    )          ( Cloud    )
             ` __..'+'              ` __..'+'
```

Figure 4: IP/ICN Convergence Scenarios

As shown in Figure 4, for applications - running either in the
mobile terminal or in the content provider system - to use the ICN
transport option, we propose a new transport convergence layer
(TCL). The TCL helps determine the type of transport (such as ICN or
IP), as well as the type of radio interface (LTE or WiFi or both)
used to send and receive traffic based on preference (e.g., content
location, content type, content publisher, congestion, cost, QoS).
It helps configure and determine the type of connection (native IP
or ICN) or the overlay mode (ICNoIP or IPoICN) between application
and the protocol stack (IP or ICN).

Combined with the existing IP function, the ICN function provides
support for either native ICN and/or the dual transport (ICN/IP)
transport functionality. See Section 5.4.1 for elaborate
descriptions of these functional layers.

The TCL can use several mechanisms for transport selection. It can use a per-application configuration through a management interface, possibly a user-facing setting realized through a user interface, like those used to select cellular over WiFi. In another option, it might use a software API, which an adapted IP application could use to specify the type of transport option (such as ICN) to take advantage of its benefits.

Another potential application of TCL is in implementation of network slicing, with a slice management capability locally or through an interface to an external slice manager via an API [GALIS]. This solution can enable network slicing for IP and ICN transport selection from the mobile terminal itself. The TCL could apply slice settings to direct certain applications traffic over one slice and others over another slice, determined by some form of 'slicing policy'. Slicing policy can be obtained externally from the slice manager or configured locally on the mobile terminal.

From the perspective of applications either on the mobile terminal or at a content provider, the following options are possible for potential use of ICN natively and/or with IP.

1. IP over IP

   In this scenario, the mobile terminal applications are tightly integrated with the existing IP transport infrastructure. The TCL has no additional function because packets are forwarded directly using an IP protocol stack, which sends packets over the IP transport.

2. ICN over ICN

   Similar to case 1, ICN applications tightly integrate with the ICN transport infrastructure. The TCL has no additional responsibility because packets are forwarded directly using the native ICN protocol stack, which sends packets over the ICN transport.

3. ICN over IP (ICNoIP)

   In this scenario, the underlying IP transport infrastructure is not impacted (that is, ICN is implemented as an IP overlay between mobile terminal and content provider). IP routing is used from the Radio Access Network (eNodeB) to the mobile backhaul, the IP core, and the Mobile Gateway (SGW/PGW). The mobile terminal attaches to the Mobile Gateway (SGW/PGW) using an IP address. Also, the data transport between Mobile Gateway (SGW/PGW) and content publisher uses IP. The content provider can serve content either using IP or ICN, based on the mobile terminal request.

One of the approaches to implement ICN in mobile backhaul
networks is described in [MBICN]. It implements a GTP-U
extension header option to encapsulate ICN payload in a GTP
tunnel. However, as this design runs ICN as an IP overlay, the
mobile backhaul can be deployed using native IP. The proposal
describes a mechanism where the GTP-U tunnel can be terminated
by hairpinning the packet before it reaches SGW, if an ICN-
enabled node is deployed in the mobile backhaul (that is,
between eNodeB and SGW). This could be useful when an ICN data
packet is stored in the ICN node (such as repositories, caches)
in the tunnel path so that the ICN node can reply without going
all the way through the mobile core. While a GTP-U extension
header is used to carry mobile terminal specific ICN payload,
they are not visible to the transport, including SGW. On the
other hand, the PGW can use the mobile terminal-specific ICN
header extension and ICN payload to set up an uplink transport
towards a content provider in the Internet. In addition, the
design assumes a proxy function at the edge, to perform ICN
data retrieval on behalf of a non-ICN end device.

4. IP over ICN (IPoICN)

   [IPoICN] provides an architectural framework for running IP as
   an overlay over ICN protocol. Implementing IP services over ICN
   provides an opportunity to leverage the benefits of ICN in the
   transport infrastructure while there is no impact on end
   devices (MT and access network) as they continue to use IP.
   IPoICN however, will require an inter-working function (IWF/
   Border Gateway) to translate various transport primitives. The
   IWF function will provide a mechanism for protocol translation
   between IPoICN and the native IP. After reviewing [IPoICN], we
   understand and interpret that ICN is implemented in the
   transport natively, however, IP is implemented in MT, eNodeB,
   and Mobile gateway (SGW/PGW), which is also called as a network
   attach point (NAP).

   For this, said NAP receives an incoming IP or HTTP packet (the
   latter through TCP connection termination) and publishes the
   packet under a suitable ICN name (i.e., the hash over the
   destination IP address for an IP packet or the hash over the
   FQDN of the HTTP request for an HTTP packet) to the ICN
   network. In the HTTP case, the NAP maintains a pending request
   mapping table to map returning responses to the terminated TCP
   connection.

5. Hybrid ICN (hICN)

   An alternative approach to implement ICN over IP is provided in
   Hybrid ICN [HICN]. It describes a novel approach to integrate

ICN into IPv6 without creating overlays with a new packet
format as an encapsulation. hICN addresses the content by
encoding a location-independent name in an IPv6 address. It
uses two name components--name prefix and name suffix--that
identify the source of data and the data segment within the
scope of the name prefix, respectively.

At application layer, hICN maps the name into an IPv6 prefix
and, thus, uses IP as transport. As long as the name prefixes,
which are routable IP prefixes, point towards a mobile GW (PGW
or local breakout, such as CUPS), there are potentially no
updates required to any of the mobile core gateways (for
example, SGW/PGW). The IPv6 backhaul routes the packets within
the mobile core. hICN can run in the mobile terminal, in the
eNodeB, in the mobile backhaul, or in the mobile core. Finally,
as hICN itself uses IPv6, it cannot be considered as an
alternative transport layer.

5.3. Integration of ICN in 4G Control Plane

In this section, we analyze signaling messages that are required for
different procedures, such as attach, handover, tracking area
update, and so on. The goal of this analysis is to see if there are
any benefits to replacing IP-based protocols with ICN for 4G
signaling in the current architecture. It is important to understand
the concept of point of attachment (POA). When mobile terminal
connects to a network, it has the following POAs:

1. eNodeB managing location or physical POA

2. Authentication and Authorization (MME, HSS) managing identity
   or authentication POA

3. Mobile Gateways (SGW, PGW) managing logical or session
   management POA

In the current architecture, IP transport is used for all messages
associated with the control plane for mobility and session
management. IP is embedded very deeply into these messages utilizing
TLV syntax for carrying additional attributes such as a layer 3
transport. The physical POA in the eNodeB handles both mobility and
session management for any mobile terminal attached to 4G network.
The number of mobility management messages between different nodes
in an 4G network per signaling procedure is shown in Table 1.

Normally, two types of mobile terminals attach to the 4G network:
SIM based (need 3GPP mobility protocol for authentication) or non-
SIM based (which connect to WiFi network). Both device types require
authentication. For non-SIM based devices, AAA is used for
authentication. We do not propose to change mobile terminal

authentication or mobility management messaging for user data transport using ICN. A separate study would be required to analyze the impact of ICN on mobility management messages structures and flows. We are merely analyzing the viability of implementing ICN as a transport for control plane messages.

It is important to note that if MME and HSS do not support ICN transport, they still need to support mobile terminal capable of dual transport or native ICN. When mobile terminal initiates an attach request using the identity as ICN, MME must be able to parse that message and create a session. MME forwards mobile terminal authentication to HSS, so HSS must be able to authenticate an ICN-capable mobile terminal and authorize create session [TS23.401].

4G Signaling Procedures	MME	HSS	SGW	PGW	PCRF
Attach	10	2	3	2	1
Additional default bearer	4	0	3	2	1
Dedicated bearer	2	0	2	2	0
Idle-to-connect	3	0	1	0	0
Connect-to-Idle	3	0	1	0	0
X2 handover	2	0	1	0	0
S1 handover	8	0	3	0	0
Tracking area update	2	2	0	0	0
Total	34	2	14	6	3

Table 1: Signaling Messages in 4G Gateways

Anchorless mobility [ALM] provides a fully decentralized, control-plane agnostic solution to handle producer mobility in ICN. Mobility management at layer-3 level makes it access agnostic and transparent to the end device or the application. The solution discusses handling mobility without having to depend on core network functions (e.g. MME); however, a location update to the core network may still be required to support legal compliance requirements such as lawful intercept and emergency services. These aspects are open for further study.

One of the advantages of ICN is in the caching and reusing of the content, which does not apply to the transactional signaling exchange. After analyzing 4G signaling call flows [TS23.401] and messages inter-dependencies (see Table 1), our recommendation is that it is not beneficial to use ICN for control plane and mobility management functions. Among the features of ICN design, Interest aggregation and content caching are not applicable to control plane signaling messages. Control plane messages are originated and consumed by the applications and they cannot be shared.

5.4. Integration of ICN in 4G User Plane

We will consider Figure 1 to discuss different mechanisms to integrate ICN in mobile networks. In Section 5.2, we discussed generic experimental setups of ICN integration. In this section, we discuss the specific options of possible use of native ICN in 4G user plane. We consider the following options:

1. Dual transport (IP/ICN) mode in Mobile Terminal

2. Using ICN in Mobile Terminal

3. Using ICN in eNodeB

4. Using ICN in mobile gateways (SGW/PGW)

5.4.1. Dual Transport (IP/ICN) Mode in Mobile Terminal

The control and user plane communications in 4G mobile networks are specified in 3GPP documents [TS23.203] and [TS23.401]. It is important to understand that mobile terminal can be either consumer (receiving content) or publisher (pushing content for other clients). The protocol stack inside the mobile terminal (MT) is complex because it must support multiple radio connectivity access to eNodeB(s).

Figure 5 provides a high-level description of a protocol stack, where IP is used at two layers: (1) user plane communication and (2) UDP encapsulation. User plane communication takes place between Packet Data Convergence Protocol (PDCP) and Application layer, whereas UDP encapsulation is at GTP protocol stack.

The protocol interactions and impact of supporting tunneling of ICN packet into IP or to support ICN natively are described in Figure 5 and Figure 6, respectively.

```
+--------+                                        +--------+
|  App   |                                        |  CDN   |
+--------+                                        +--------+
|Transp. | |            |            |            |Transp. |
|Converg.|.|............|............|...........|.|Converge|
+--------+ |            |            | +--------+ | +--------+
|        |.|............|............|.|        |.|.|        |
| ICN/IP | |            |            | | ICN/IP | | | ICN/IP|
|        | |            |            | |        | | |        |
+--------+ | +----+-----+ | +-----+-----+ | +-----+--+ | +--------+
|        |.|.|    |     |.|.|     |     |.|.|     |  | | | |        |
|  PDCP  | | |PDCP|GTP-U| | |GTP-U|GTP-U| | |GTP-U|  | | |  L2    |
+--------+ | +----------+ | +-----------+ | +-----+  | | |        |
|  RLC   |.|.|RLC | UDP |.|.| UDP | UDP |.|.|UDP  |L2|.|.|        |
+--------+ | +----------+ | +-----------+ | +-----+  | | |        |
|  MAC   |.|.| MAC|  L2 |.|.| L2  | L2  |.|.| L2  |  | | |        |
+--------+ | +----------+ | +-----------+ | +--------+ | +--------+
|  L1    |.|.| L1 |  L1 |.|.| L1  | L1  |.|.| L1  |L1|.|.|  L1    |
+--------+ | +----+-----+ | +-----+-----+ | +-----+--+ | +--------+
    MT     |  BS(eNodeB)  |     SGW       |     PGW     |
         Uu             S1U            S5/S8          SGi
```

              Figure 5: Dual Transport (IP/ICN) mode in Mobile Terminal

The protocols and software stack used inside 4G capable mobile
terminal support both 3G and 4G software interworking and handover.
3GPP Rel.13 onward specifications describe the use of IP and non-IP
protocols to establish logical/session connectivity. We can leverage
the non-IP protocol-based mechanism to deploy ICN protocol stack in
the mobile terminal, as well as in eNodeB and mobile gateways (SGW,
PGW). The following paragraphs describe per-layer considerations of
supporting tunneling of ICN packet into IP or to support ICN
natively.

   1. An existing application layer can be modified to provide
      options for a new ICN-based application and existing IP-based
      applications. The mobile terminal can continue to support
      existing IP-based applications or can develop new applications
      to support native ICN, ICNoIP, or IPoICN-based transport. The
      application layer can be provided with an option of selecting
      either ICN or IP transport, as well as radio interface, to send
      and receive data traffic.

      Our proposal is to provide an Application Programming Interface
      (API) to the application developers so they can choose either
      ICN or IP transport for exchanging the traffic with the
      network. As mentioned in Section 5.2, the transport convergence
```

layer (TCL) function handles the interaction of applications with multiple transport options.

2. The transport convergence layer helps determine the type of transport (such as ICN, hICN, or IP) and type of radio interface (LTE or WiFi, or both) used to send and receive traffic. Application layer can make the decision to select a specific transport based on preference, such as content location, content type, content publisher, congestion, cost, QoS, and so on. There can be an Application Programming Interface (API) to exchange parameters required for transport selection. Southbound interactions of Transport Convergence Layer (TCL) will be either to IP or ICN at the network layer.

   When selecting the IPoICN mode, the TCL is responsible for receiving an incoming IP or HTTP packet and publishing the packet to the ICN network under a suitable ICN name (that is, the hash over the destination IP address for an IP packet, or the hash over the FQDN of the HTTP request for an HTTP packet).

   In the HTTP case, the TCL can maintain a pending request mapping table to map returning responses to the originating HTTP request. The common API will provide a 'connection' abstraction for this HTTP mode of operation, returning the response over said connection abstraction, akin to the TCP socket interface, while implementing a reliable transport connection semantic over the ICN from the mobile terminal to the receiving mobile terminal or the PGW. If the HTTP protocol stack remains unchanged, therefore utilizing the TCP protocol for transfer, the TCL operates in local TCP termination mode, retrieving the HTTP packet through said local termination.
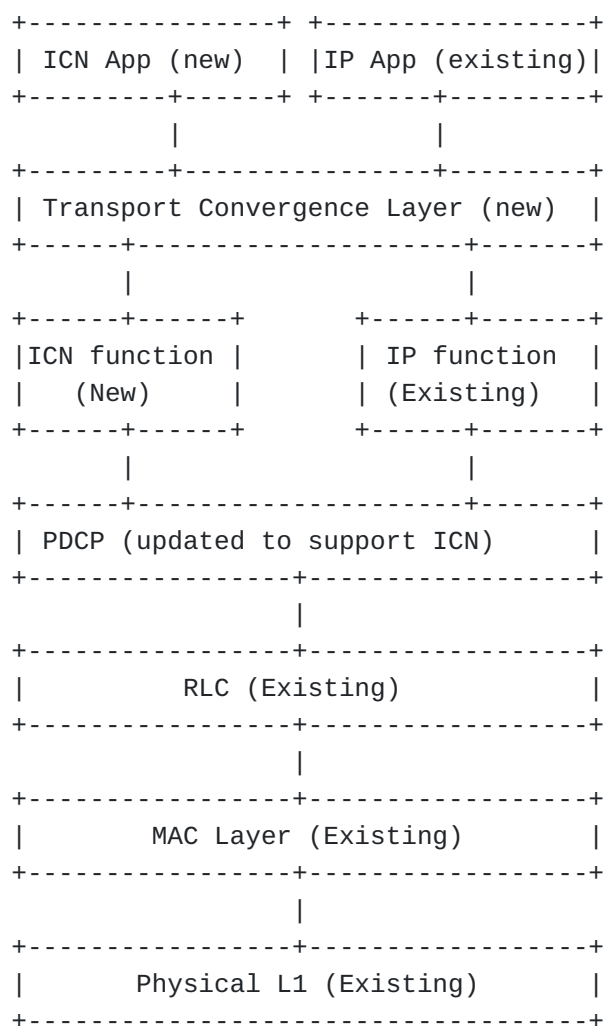
```
            +----------------+ +-----------------+
            | ICN App (new)  | |IP App (existing)|
            +---------+------+ +-------+---------+
                      |                |
            +---------+----------------+---------+
            | Transport Convergence Layer (new)  |
            +------+--------------------+-------+
                   |                    |
            +------+------+      +------+-------+
            |ICN function |      | IP function  |
            |   (New)     |      | (Existing)   |
            +------+------+      +------+-------+
                   |                    |
            +------+--------------------+-------+
            | PDCP (updated to support ICN)     |
            +----------------+-----------------+
                             |
            +----------------+-----------------+
            |         RLC (Existing)           |
            +----------------+-----------------+
                             |
            +----------------+-----------------+
            |        MAC Layer (Existing)      |
            +----------------+-----------------+
                             |
            +----------------+-----------------+
            |       Physical L1 (Existing)     |
            +----------------------------------+
```

            Figure 6: Dual Stack ICN Protocol Interactions

3. The ICN function (forwarder) is proposed to run in parallel to
   the existing IP layer. The ICN forwarder forwards the ICN
   packets, such as an Interest packet to eNodeB or a response
   "data packet" from eNodeB to the application.

4. For the dual-transport scenario, when mobile terminal is not
   supporting ICN as transport, the TCL can use the IP underlay to
   tunnel the ICN packets. The ICN function can use the IP
   interface to send Interest and Data packets for fetching or
   sending data respectively. This interface can use the ICN
   overlay over IP.

5. To support ICN at network layer in mobile terminal, the PDCP
   layer should be aware of ICN capabilities and parameters. PDCP
   is located in the Radio Protocol Stack in the LTE Air

interface, between IP (Network layer) and Radio Link Control
Layer (RLC). PDCP performs the following functions [TS36.323]:

1. Data transport by listening to upper layer, formatting and
   pushing down to Radio Link Layer (RLC)

2. Header compression and decompression using Robust Header
   Compression (ROHC)

3. Security protections such as ciphering, deciphering, and
   integrity protection

4. Radio layer messages associated with sequencing, packet
   drop detection and re-transmission, and so on.

6. No changes are required for lower layer such as RLC, MAC, and
   Physical (L1) as they are not IP aware.

One key point to understand in this scenario is that ICN is deployed
as an overlay on top of IP.

5.4.2. Using ICN in Mobile Terminal

We can implement ICN natively in mobile terminal by modifying the
PDCP layer in 3GPP protocols. Figure 7 provides a high-level
protocol stack description where ICN can be used at the following
different layers:

1. User plane communication

2. Transport layer

ICN transport would be a substitute of the GTP protocol. The removal
of the GTP protocol stack is a significant change in the mobile
architecture and requires a thorough study mainly because it is used
not just for routing but for mobility management functions, such as
billing, mediation, and policy enforcement.

The implementation of ICN natively in the mobile terminal leads to a
changed communication model between mobile terminal and eNodeB.
Also, we can avoid tunneling the user plane traffic from eNodeB to
the mobile packet core (SGW, PGW) through a GTP tunnel.

For native ICN use, an application can be configured to use ICN
forwarder and it does not need the TCL layer. Also, to support ICN
at the network layer, the existing PDCP layer may need to be changed
to be aware of ICN capabilities and parameters.

The native implementation can provide new opportunities to develop
new use cases leveraging ICN capabilities, such as seamless

mobility, mobile terminal to mobile terminal content delivery using
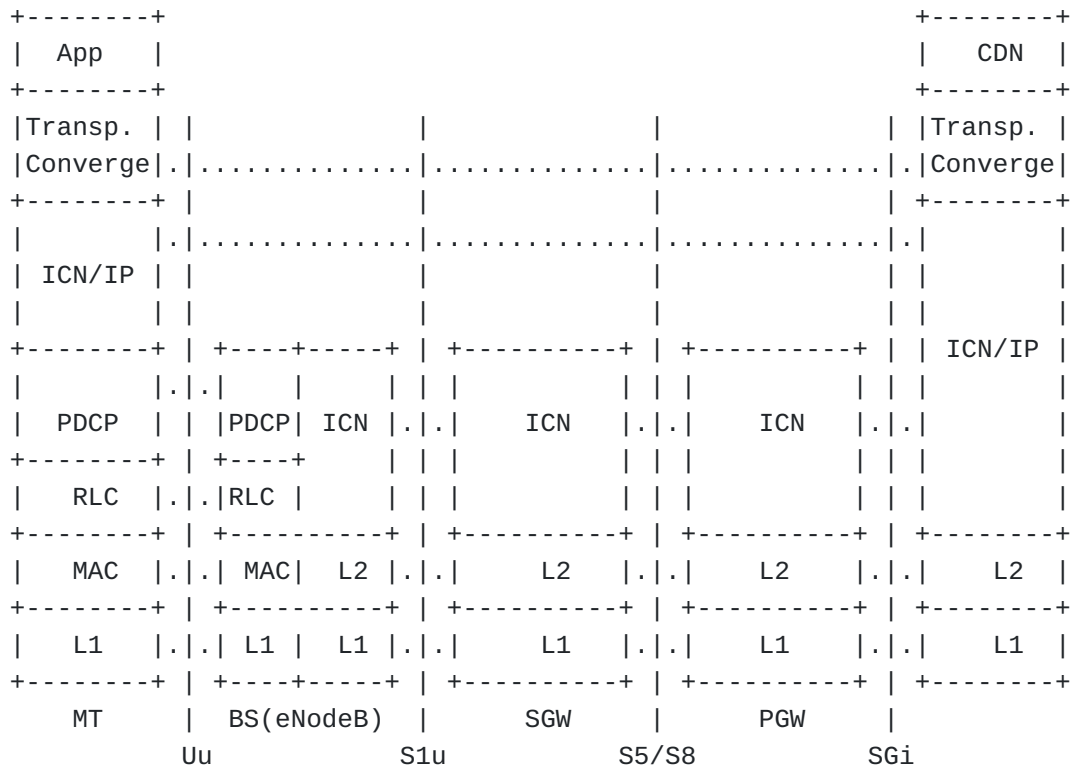radio network without traversing the mobile gateways, and more.

```
+--------+                                                   +--------+
|  App   |                                                   |  CDN   |
+--------+                                                   +--------+
|Transp. | |                |              |              | |Transp. |
|Converge|.|..............|..............|..............|.|Converge|
+--------+ |                |              |              | +--------+
|        |.|..............|..............|..............|.|        |
| ICN/IP | |                |              |              | |        |
|        | | |              |              |              | |        |
+--------+ | +----+-----+ | +----------+ | +----------+ | | ICN/IP |
|        |.|.|    |     | | |          | | |          | | | |        |
|  PDCP  | | |PDCP| ICN |.|.|   ICN    |.|.|   ICN    |.|.|        |
+--------+ | +----+     | | |          | | |          | | | |        |
|  RLC   |.|.|RLC |     | | |          | | |          | | | |        |
+--------+ | +----------+ | +----------+ | +----------+ | +--------+
|  MAC   |.|.| MAC| L2  |.|.|    L2    |.|.|    L2    |.|.|   L2   |
+--------+ | +----------+ | +----------+ | +----------+ | +--------+
|  L1    |.|.| L1 | L1  |.|.|    L1    |.|.|    L1    |.|.|   L1   |
+--------+ | +----+-----+ | +----------+ | +----------+ | +--------+
    MT     |  BS(eNodeB)  |     SGW      |     PGW      |
          Uu            S1u          S5/S8          SGi
```

Figure 7: Using Native ICN in Mobile Terminal

5.4.3. Using ICN in eNodeB

The eNodeB is a physical point of attachment for the mobile
terminal, where radio protocols are converted into IP transport
protocol for dual transport/overlay and native ICN, respectively
(see Figure 6 and Figure 7). When a mobile terminal performs an
attach procedure, it would be assigned an identity either as IP or
dual transport (IP and ICN), or ICN endpoint. Mobile terminal can
initiate data traffic using any of the following options:

   1. Native IP (IPv4 or IPv6)

   2. Native ICN

   3. Dual transport IP (IPv4/IPv6) and ICN

The mobile terminal encapsulates a user data transport request into
PDCP layer and sends the information on the air interface to eNodeB,
which in turn receives the information and, using PDCP [TS36.323],
de-encapsulates the air-interface messages and converts them to
forward to core mobile gateways (SGW, PGW). As shown in Figure 8, to

support ICN natively in eNodeB, it is proposed to provide transport
convergence layer (TCL) capabilities in eNodeB (similar to as
provided in MT), which provides the following functions:

1. It decides the forwarding strategy for a user data request
   coming from mobile terminal. The strategy can decide based on
   preference indicated by the application, such as congestion,
   cost, QoS, and so on.

2. eNodeB to provide open Application Programming Interface (API)
   to external management systems, to provide capability to eNodeB
   to program the forwarding strategies.

```
                  +---------------+  |
                  | MT request    |  |    ICN          +---------+
           +----->| content using |--+--- transport -->|         |
           |      |ICN protocol   |  |                  |         |
           |      +---------------+  |                  |         |
           |                         |                  |         |
           |      +---------------+  |                  |         |
     +-+ |        | MT request    |  |    IP            |To mobile|
     | |-+----->| content using |--+--- transport -->|   GW    |
     +-+ |        | IP protocol   |  |                  |(SGW,PGW)|
     MT  |        +---------------+  |                  |         |
         |                          |                  |         |
         |       +---------------+  |                  |         |
         |       | MT request    |  |    Dual stack    |         |
         +----->| content using |--+--- IP+ICN    -->|         |
                 |IP/ICN protocol|  |    transport     +---------+
                 +---------------+  |
                     eNodeB         S1u
```
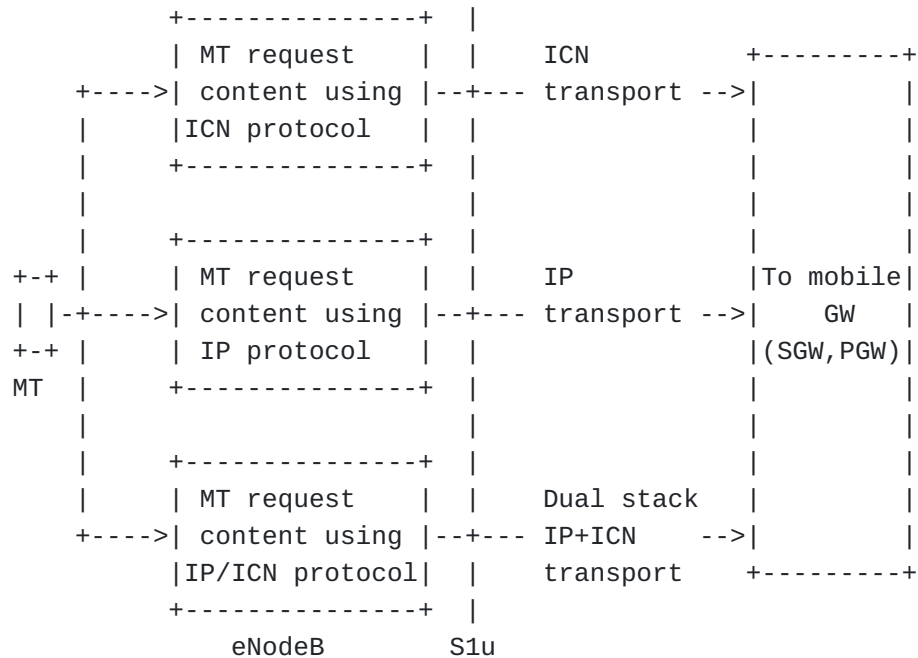
                Figure 8: Integration of Native ICN in eNodeB

3. eNodeB can be upgraded to support three different types of
   transport: IP, ICN, and dual transport IP+ICN towards mobile
   gateways, as depicted in Figure 8. It is also proposed to
   deploy IP and/or ICN forwarding capabilities into eNodeB, for
   efficient transfer of data between eNodeB and mobile gateways.
   Following are choices for forwarding a data request towards
   mobile gateways:

   1. Assuming eNodeB is IP enabled and the MT requests an IP
      transfer, eNodeB forwards data over IP.

   2. Assuming eNodeB is ICN enabled and the MT requests an ICN
      transfer, eNodeB forwards data over ICN.

3. Assuming eNodeB is IP enabled and the MT requests an ICN
    transfer, eNodeB overlays ICN on IP and forwards user
    plane traffic over IP.

4. Assuming eNodeB is ICN enabled and the MT requests an IP
    transfer, eNodeB overlays IP on ICN and forwards user
    plane traffic over ICN [IPoICN].

5.4.4. Using ICN in Packet Core (SGW, PGW) Gateways

Mobile gateways (a.k.a. Evolved Packet Core (EPC)) include SGW, PGW,
which perform session management for MT from the initial attach to
disconnection. When MT is powered on, it performs NAS signaling and
attaches to PGW after successful authentication. PGW is an anchoring
point for MT and responsible for service creations, authorization,
maintenance, and so on. The Entire functionality is managed using IP
address(es) for MT.

To implement ICN in EPC, the following functions are proposed:

1. Insert ICN attributes in session management layer as additional
    functionality with IP stack. Session management layer is used
    for performing attach procedures and assigning logical identity
    to user. After successful authentication by HSS, MME sends a
    create session request (CSR) to SGW and SGW to PGW.

2. When MME sends Create Session Request message (Step 12 in
    [TS23.401]) to SGW or PGW, it includes a Protocol Configuration
    Option Information Element (PCO IE) containing MT capabilities.
    We can use PCO IE to carry ICN-related capabilities information
    from MT to PGW. This information is received from MT during the
    initial attach request in MME. Details of available TLV, which
    can be used for ICN, are given in subsequent sections. MT can
    support either native IP, ICN+IP, or native ICN. IP is referred
    to as both IPv4 and IPv6 protocols.

3. For ICN+IP-capable MT, PGW assigns the MT both an IP address
    and ICN identity. MT selects either of the identities during
    the initial attach procedures and registers with the network
    for session management. For ICN-capable MT, it will provide
    only ICN attachment. For native IP-capable MT, there is no
    change.

4. To support ICN-capable attach procedures and use ICN for user
    plane traffic, PGW needs to have full ICN protocol stack
    functionalities. Typical ICN capabilities include functions
    such as content store (CS), Pending Interest Table (PIT),
    Forwarding Information Base (FIB) capabilities, and so on. If
    MT requests ICN in PCO IE, then PGW registers MT with ICN

names. For ICN forwarding, PGW caches content locally using CS functionality.

5. PCO IE described in [TS24.008] (see Figure 10.5.136 on page 598) and [TS24.008] (see Table 10.5.154 on page 599) provide details for different fields.

   1. Octet 3 (configuration protocols define PDN types), which contains details about IPv4, IPv6, both or ICN.

   2. Any combination of Octet 4 to Z can be used to provide additional information related to ICN capability. It is most important that PCO IE parameters are matched between MT and mobile gateways (SGW, PGW) so they can be interpreted properly and the MT can attach successfully.

6. The ICN functionalities in SGW and PGW should be matched with MT and eNodeB because they will exchange ICN protocols and parameters.

7. Mobile gateways SGW, PGW will also need ICN forwarding and caching capability. This is especially important if CUPS is implemented. User Plane Function (UPF), comprising the SGW and PGW user plane, will be located at the edge of the network and close to the end user. ICN-enabled gateway means that this UPF would serve as a forwarder and should be capable of caching, as is the case with any other ICN-enabled node.

8. The transport between PGW and CDN provider can be either IP or ICN. When MT is attached to PGW with ICN identity and communicates with an ICN-enabled CDN provider, it will use ICN primitives to fetch the data. On the other hand, for a MT attached with an ICN identity, if PGW must communicate with an IP enabled CDN provider, it will have to use an ICN-IP interworking gateway to perform conversion between ICN and IP primitives for data retrieval. In the case of CUPS implementation with an offload close to the edge, this interworking gateway can be collocated with the UPF at the offload site to maximize the path optimization. Further study is required to understand how this ICN-to-IP (and vice versa) interworking gateway would function.

5.5. An Experimental Test Setup

This section proposes an experimental lab setup and discusses the open issues and questions that use of ICN protocol is intended to address. To further test the modifications proposed in different scenarios, a simple lab can be set up, as shown in Figure 9.

```
+--------------------------------------------+
| +-----+   +------+   (```).     +------+ |   (````).    +-----+
| | SUB |-->| EMU  |--(x-haul'.-->| EPC  |--->(  PDN ).-->| CDN |
| +-----+   +------+   `__..''    +------+ |   `__...'    +-----+
+--------------------------------------------+
              4G Mobile Network Functions
```
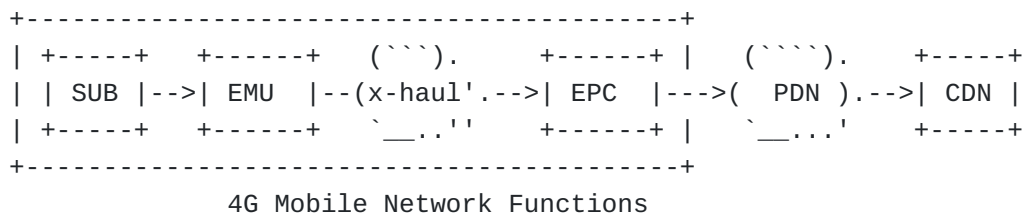
Figure 9: Native ICN Deployment Lab Setup

The following test scenarios can be set up with VM-based deployment:

1. SUB: ICN simulated client (using ndnSIM), a client application
   on workstation requesting content.

2. EMU: test unit emulating eNodeB. This will be a test node
   allowing for UE attachment and routing traffic subsequently
   from the Subscriber to the Publisher.

3. EPC: Evolved Packet Core in a single instance (such as
   5GOpenCore [Open5GCore]).

4. CDN: content delivery by a Publisher server.

For the purpose of this testing, ICN emulating code can be inserted
in the test code in EMU to emulate ICN-capable eNodeB. An example of
the code to be used is NS3 in its LTE model. Effect of such traffic
on EPC and CDN can be observed and documented. In a subsequent
phase, EPC code supporting ICN can be tested when available.

Another option is to simulate the UE/eNodeB and EPC functions using
NS3's LTE [NS3LTE] and EPC [NS3EPC] models respectively. LTE model
includes the LTE Radio Protocol stack, which resides entirely within
the UE and the eNodeB nodes. This capability provides the simulation
of UE and eNodeB deployment use cases. Similarly, EPC model includes
core network interfaces, protocols, and entities, which reside
within the SGW, PGW and MME nodes, and partially within the eNodeB
nodes.

Even with its current limitations (such as IPv4 only, lack of
integration with ndnSIM, no support for UE idle state), LTE
simulation may be a very useful tool. In any case, both control and
user plane traffic should be tested independently according to the
deployment model discussed in Section 5.4.

6. **Expected Outcomes from Experimentation**

The experimentations explained in [Section 5](#) can be categorized in three broader scopes as follows. Note that, a further research and study is required to fully understand and document the impact.

1. Architecture scope: to study the aspect of use of ICN at user plane to reduce the complexities in current transport protocols, while also evaluating its use in the control plane.

2. Performance scope: to evaluate the gains through multicast, caching, and other ICN features.

3. Deployment scope: to check the viability of the ICN inclusion in 3GPP protocol stack and its viability in real-world deployments.

6.1. **Feeding into ICN Research**

Specifically, we have identified the following open questions, from the architectural and performance perspective, that the proposed experiments with ICN implementation scenarios in 4G mobile networks could address in further research:

1. Efficiency gains in terms of the amount of traffic in multicast scenarios (i.e., quantify the possible gains along different use cases) and the efficiency gained in terms of latency for cached content, mainly in the CDN use case.

2. How the new transport would coexist or replace the legacy transport protocols (e.g., IPv4, IPv6, MPLS, RSVP, etc.) and related services (e.g., bandwidth management, QoS handling, etc.).

3. To what extent the simplification in the IP-based transport protocols will be achieved. The multiple overlays (e.g., the MPLS, VPN, VPLS, Ethernet VPN, etc.) of services in the current IP-based transport adds to the complexity on top of basic IP transport. This makes the troubleshooting extremely challenging.

4. How the new transport can become service-aware such that it brings in more simplicity in the system.

5. Confirm how (in)adequate would be ICN implementation in control plane (which this draft discourages). Given that the 5G system, as specified in [TS23.501] (Appendix G.4), encourages the use of name-based routing in (5G) control plane for realizing the 5G-specific service-based architecture for control plane services (so-called network function service), it would be

worthwhile to investigate whether the 4G control plane would
benefit similarly from such use or whether specific 4G
architectural constraints would prevent ICN from providing any
notable benefit.

6.2. Use of Results Beyond Research

With the experiments and their outcomes outlined in this draft, we
believe that this technology is ready for a wider use and adoption,
providing additional insights. Specifically, we expect to study the
following:

1. Viability of ICN inclusion in the 3GPP protocol stack, i.e.,
   investigate how realistic it would be to modify the stack,
   considering the scenarios explained in Section 5.4, and
   complete the user session without feature degradation?

2. Viability of utilizing solutions in greenfield deployments,
   i.e., deploying the ICN-based extensions and solutions proposed
   in this draft in greenfield 4G deployments in order to assess
   real-world benefits when doing so.

7. Security and Privacy Considerations

This section will cover some security and privacy considerations in
mobile and 4G network because of introduction of ICN.

7.1. Security Considerations

To ensure only authenticated mobile terminals are connected to the
network, 4G mobile network implements various security mechanisms.
From the perspective of using ICN in the user plane, it needs to
take care of the following security aspects:

1. MT authentication and authorization

2. Radio or air interface security

3. Denial of service attacks on the mobile gateway, services
   either by the MT or by external entities in the Internet

4. Content poisoning either in transport or servers

5. Content cache pollution attacks

6. Secure naming, routing, and forwarding

7. Application security

Security over the LTE air interface is provided through
cryptographic techniques. When MT is powered up, it performs a key
exchange between MT's USIM and HSS/Authentication Center using NAS
messages, including ciphering and integrity protections between MT
and MME. Details for secure MT authentication, key exchange,
ciphering, and integrity protections messages are given in the 3GPP
call flow [TS23.401]. With ICN we are modifying protocol stack for
user plane and not control plane. The NAS signaling is exchanged
between MT and mobile gateways e.g. MME, using control plane,
therefore there is no adverse impact of ICN on MT.

4G uses IP transport in its mobile backhaul (between eNodeB and core
network). In case of provider-owned backhaul, service provider may
require implementing a security mechanism in the backhaul network.
The native IP transport continues to leverage security mechanism
such as Internet key exchange (IKE) and the IP security protocol
(IPsec). More details of mobile backhaul security are provided in
3GPP network security specifications [TS33.310] and [TS33.320]. When
mobile backhaul is upgraded to support dual transport (IP+ICN) or
native ICN, it is required to implement security techniques that are
deployed in the mobile backhaul. When ICN forwarding is enabled on
mobile transport routers, we need to deploy security practices based
on [RFC7476] and [RFC7927].

4G mobile gateways (SGW, PGW) perform some of key functions such as
content based online/offline billing and accounting, deep packet
inspection (DPI), and lawful interception (LI). When ICN is deployed
in user plane , we need to integrate ICN security for sessions
between MT and gateway. If we encrypt user plane payload metadata
then it might be difficult to perform routing based on contents and
it may not work because we need decryption keys at every forwarder
to route the content. The content itself can be encrypted between
publisher and consumer to ensure privacy. Only the user with right
decryption key shall be able to access the content. We need further
research for ICN impact on LI, online/offline charging and
accounting.

7.2. Privacy Considerations

In 4G networks, two main privacy issues are [MUTHANA]

1. User Identity Privacy Issues. The main privacy issue within the
   4G is the exposure of the IMSI. The IMSI can be intercepted by
   adversaries. Such attacks are commonly referred to as "IMSI
   catching".

2. Location Privacy Issues. IMSI Catching is closely related to
   the issue of location privacy. Knowing IMSI of user allows the

attacker to track the user's movements and create profile about the user and thus breaches the user's location privacy.

In any network, caching implies a trade-off between network efficiency and privacy. The activity of users is exposed to the scrutiny of cache owners with whom they may not have any relationship. By monitoring the cache transactions, an attacker could obtain significant information related to the objects accessed, topology and timing of the requests [RFC7945]. Privacy concerns are amplified by the introduction of new network functions such as Information lookup and Network storage, and different forms of communication [FOTIOU]. Privacy risks in ICN can be broadly divided in the following categories [TOURANI]:

1. Timing attack

2. Communication monitoring attack

3. Censorship and anonymity attack

4. Protocol attack

5. Naming-signature privacy

Introduction of TCL effectively enables ICN at the application and/ or transport layer, depending on the scenario described in section 5. Enabling ICN in 4G networks is expected to increase efficiency by taking advantage of ICN's inherent characteristics. This approach would potentially leave some of the above-mentioned privacy concerns open as a consequence of using ICN transport and ICN inherent privacy vulnerabilities.

1. IPoIP Section 5.2 would not be affected as TCL has no role in it and ICN does not apply

2. ICNoICN scenario Section 5.2 has increased risk of a privacy attack, and that risk is applicable to ICN protocol in general rather than specifically to the 4G implementation. Since this scenario describes communication over ICN transport, every forwarder in the path could be a potential risk for privacy attack

3. ICNoIP scenario Section 5.2 uses IP for transport, so the only additional ICN-related potential privacy risk areas are the endpoints (consumer and publisher) where, at the application layer, content is being served

4. IPoICN scenario Section 5.2 could have potentially increased risk due to possible vulnerability of the forwarders in the path of ICN transport

Privacy issues already identified in 4G remain a concern if ICN is introduced in any of the scenarios described earlier and compound to the new, ICN-related privacy issues. Many research papers have been published proposing solutions to the privacy issues listed above. For LTE-specific privacy issues, some of the proposed solutions [MUTHANA] are IMSI encryption by a MT, mutual authentication, concealing the real IMSI within a random bit stream of certain size where only the subscriber and HSS could extract the respective IMSI, IMSI replacement with a changing pseudonym that only the HSS server can map it the UE's IMSI, and others. Similarly, some of the proposed ICN-specific privacy concerns mitigation methods, applicable where ICN transport is introduced as specified earlier in this section, include [FOTIOU]:

  *Delay for the first, or first k interests on edge routers (timing attack)

  *Creating a secure tunnel or clients flagging the requests as non-cacheable for privacy (communication monitoring attack)

  *Encoding interest by mixing content and cover file or using hierarchical DNS-based brokering model (censorship and anonymity attack)

  *Use of rate-limiting requests for a specific namespace (protocol attack)

  *Cryptographic content hash-based naming or digital identity in an overlay network (naming-signature privacy)

Further research in this area is needed. Detailed discussion of privacy is beyond the scope of this document.

8. Summary

In this draft, we have discussed the 4G networks and the experimental setups to study the advantages of potential use of ICN for efficient delivery of contents to mobile terminals. We have discussed different options to try and test the ICN and dependencies such as ICN functionalities and changes required in different 4G network elements. In order to further explore potential use of ICN one can devise an experimental set-up consisting of 4G network elements and deploy ICN data transport in user plane. Different options can be either overlay, dual transport (IP + ICN), hICN, or natively (by integrating ICN with CDN, eNodeB, SGW, PGW and transport network). Note that, for the scenarios discussed above, additional study is required for lawful interception, billing/ mediation, network slicing, and provisioning APIs.

Edge Computing [CHENG] provides capabilities to deploy
functionalities such as Content Delivery Network (CDN) caching and
mobile user plane functions (UPF) [TS23.501]. Recent research for
delivering real-time video content [MPVCICN] using ICN has also been
proven to be efficient [NDNRTC] and can be used towards realizing
the benefits of using ICN in eNodeB, edge computing, mobile gateways
(SGW, PGW) and CDN. The key aspect for ICN is in its seamless
integration in 4G and 5G networks with tangible benefits so we can
optimize content delivery using a simple and scalable architecture.
The authors will continue to explore how ICN forwarding in edge
computing could be used for efficient data delivery from the mobile
edge.

Based on our study of control plane signaling, it is not beneficial
to deploy ICN with existing protocols unless further changes are
introduced in the control protocol stack itself.

As a starting step towards use of ICN in user plane, it is proposed
to incorporate protocol changes in MT, eNodeB, SGW/PGW for data
transport. ICN has inherent capabilities for mobility and content
caching, which can improve the efficiency of data transport for
unicast and multicast delivery. The authors welcome contributions
and suggestions, including those related to further validations of
the principles by implementing prototype and/or proof of concept in
the lab and in the production environment.

9. Acknowledgements

10. References

10.1. Normative References

[TS24.008] 3GPP, "Mobile radio interface Layer 3 specification; Core
            network protocols; Stage 3", 3GPP TS 24.008 3.20.0, 15
            December 2005, <http://www.3gpp.org/ftp/Specs/html-info/
            24008.htm>.

[TS25.323] 3GPP, "Packet Data Convergence Protocol (PDCP)
            specification", 3GPP TS 25.323 3.10.0, 18 September 2002,
            <http://www.3gpp.org/ftp/Specs/html-info/25323.htm>.

[TS29.274]
3GPP, "3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunneling Protocol for Control plane (GTPv2-C); Stage 3", 3GPP TS 29.274 10.11.0, 25 June 2013, <http://www.3gpp.org/ftp/Specs/html-info/29274.htm>.

[TS29.281] 3GPP, "General Packet Radio System (GPRS) Tunneling Protocol User Plane (GTPv1-U)", 3GPP TS 29.281 10.3.0, 26 September 2011, <http://www.3gpp.org/ftp/Specs/html-info/29281.htm>.

[TS36.323] 3GPP, "Evolved Universal Terrestrial Radio Access (E-UTRA); Packet Data Convergence Protocol (PDCP) specification", 3GPP TS 36.323 10.2.0, 3 January 2013, <http://www.3gpp.org/ftp/Specs/html-info/36323.htm>.

10.2. Informative References

[ALM]
Augé, J., Carofiglio, G., Grassi, G., Muscariello, L., Pau, G., and X. Zeng, "Anchor-Less Producer Mobility in ICN", Proceedings of the 2Nd ACM Conference on Information-Centric Networking, ACM-ICN'15, ACM DL, pp. 189-190, 30 September 2013, <https://dl.acm.org/citation.cfm?id=2812601>.

[BROWER]
Brower, E., Jeffress, L., Pezeshki, J., Jasani, R., and E. Ertekin, "Integrating Header Compression with IPsec", MILCOM 2006 - 2006 IEEE Military Communications conference IEEE Xplore DL, pp.1-6, 23 October 2006, <https://ieeexplore.ieee.org/document/4086687>.

[CCN]
"Content Centric Networking", <http://www.ccnx.org>.

[CHENG]
Liang, C., Yu, R., and X. Zhang, "Information-centric network function virtualization over 5g mobile wireless networks", IEEE Network Journal vol. 29, number 3, pp. 68-74, 1 June 2015, <https://ieeexplore.ieee.org/document/7113228>.

[EMBMS]
Zahoor, K., Bilal, K., Erbad, A., and A. Mohamed, "Service-Less Video Multicast in 5G: Enablers and Challenges", IEEE Network vol. 34, no. 3, pp. 270-276, May 2020, <https://ieeexplore.ieee.org/document/9105941>.

[EPCCUPS] Schmitt, P., Landais, B., and F. Yong Yang, "Control and User Plane Separation of EPC nodes (CUPS)", 3GPP The Mobile Broadband Standard, 3 July 2017, <http://www.3gpp.org/news-events/3gpp-news/1882-cups>.

[FOTIOU]   Fotiou, N. and G. Polyzos, "ICN privacy and name based
             security", ACM-ICN '14: Proceedings of the 1st ACM
             Conference on Information-Centric Networking ACM Digitial
             Library, pp. 5-6, September 2014, <https://dl.acm.org/
             doi/10.1145/2660129.2666711>.

[GALIS]   Galis, A., Makhijani, K., Yu, D., and B. Liu, "Autonomic
             Slice Networking", Work in Progress, Internet-Draft,
             draft-galis-anima-autonomic-slice-networking-05, 26
             September 2018, <http://www.ietf.org/internet-drafts/
             draft-galis-anima-autonomic-slice-networking-05.txt>.

[GRAYSON]   Grayson, M., Shatzkamer, M., and S. Wainner, "Cisco Press
             book "IP Design for Mobile Networks"", Cisco Press
             Networking Technology series, 15 June 2009, <http://
             www.ciscopress.com/store/ip-design-for-mobile-
             networks-9781587058264>.

[HICN]   Muscariello, L., Carofiglio, G., Auge, J., and M.
             Papalini, "Hybrid Information-Centric Networking", Work
             in Progress, Internet-Draft, draft-muscariello-intarea-
             hicn-04, 20 May 2020, <https://www.ietf.org/id/draft-
             muscariello-intarea-hicn-04.txt>.

[I-D.anilj-icnrg-dnc-qos-icn] Jangam, A., suthar, P., and M. Stolic,
             "QoS Treatments in ICN using Disaggregated Name
             Components", Work in Progress, Internet-Draft, draft-
             anilj-icnrg-dnc-qos-icn-02, 9 March 2020, <http://
             www.ietf.org/internet-drafts/draft-anilj-icnrg-dnc-qos-
             icn-02.txt>.

[ICN5G]   Ravindran, R., suthar, P., Trossen, D., and G. White,
             "Enabling ICN in 3GPP's 5G NextGen Core Architecture",
             Work in Progress, Internet-Draft, draft-ravi-icnrg-5gc-
             icn-04, 10 January 2021, <https://www.ietf.org/id/draft-
             irtf-icnrg-5gc-icn-04.txt>.

[ICNLOWPAN] Gundogan, C., Schmidt, T., Waehlisch, M., Scherb, C.,
             Marxer, C., and C. Tschudin, "ICN Adaptation to LowPAN
             Networks (ICN LoWPAN)", Work in Progress, Internet-Draft,
             draft-irtf-icnrg-icnlowpan-10, 10 February 2021,
             <https://www.ietf.org/id/draft-irtf-icnrg-
             icnlowpan-10.txt>.

[ICNQoS]   Al-Naday, M.F., Bontozoglou, A., Vassilakis, G., and M.
             J. Reed, "Quality of Service in an Information-Centric
             Network", 2014 IEEE Global Communications Conference IEEE
             Xplore DL, pp. 1861-1866, 8 December 2014, <https://
             ieeexplore.ieee.org/document/7037079>.

[IPoICN]   Trossen, D., Read, M J., Riihijarvi, J., Georgiades, M.,
             Fotiou, N., and G. Xylomenos, "IP over ICN - The better
             IP?", 2015 European Conference on Networks and
             Communications (EuCNC) IEEE Xplore DL, pp. 413-417, 29
             June 2015, <https://ieeexplore.ieee.org/document/
             7194109>.

[MBICN]   Carofiglio, G., Gallo, M., Muscariello, L., and D.
             Perino, "Scalable mobile backhauling via information-
             centric networking", The 21st IEEE International Workshop
             on Local and Metropolitan Area Networks, Beijing, pp.
             1-6, 22 April 2015, <https://ieeexplore.ieee.org/
             document/7114719>.

[MECSPEC]   "Mobile Edge Computing (MEC); Framework and Reference
             Architecture", ETSI European Telecommunication Standards
             Institute (ETSI) MEC specification, March 2016, <https://
             www.etsi.org/deliver/etsi_gs/MEC/001_099/003/01.01.01_60/
             gs_MEC003v010101p.pdf>.

[MPVCICN]   Jangam, A., Ravindran, R., Chakraborti, A., Wan, X., and
             G. Wang, "Realtime multi-party video conferencing service
             over information centric network", IEEE International
             Conference on Multimedia and Expo Workshops (ICMEW)
             Turin, Italy, pp. 1-6, 29 June 2015, <https://
             ieeexplore.ieee.org/document/7169810>.

[MUTHANA]   Muthana, A. and M. Saeed, "Analysis of User Identity
             Privacy in LTE and Proposed Solution", International
             Journal of Computer Network and Information
             Security(IJCNIS) MECS Press, pp. 54-63, January 2017,
             <http://www.mecs-press.org/ijcnis/ijcnis-v9-n1/
             v9n1-7.html>.

[NDNRTC]   Gusev, P., Wang, Z., Burke, J., Zhang, L., Yoneda, T.,
             Ohnishi, R., and E. Muramoto, "Real-time Streaming Data
             Delivery over Named Data Networking,", IEICE Transactions
             on Communications vol. E99.B, pp. 974-991, 1 May 2016,
             <https://doi.org/10.1587/transcom.2015AMI0002>.

[NGMN]   Robson, J., "Backhaul Provisioning for LTE-Advanced and
             Small Cells", Next Generation Mobile Networks, LTE-
             Advanced Transport Provisioning, V0.0.14, 20 October
             2015, <https://www.ngmn.org/wp-content/uploads/
             Publications/2015/150929_NGMN_P-

                        SmallCells_Backhaul_for_LTE-
                        Advanced_and_Small_Cells.pdf>.

   [NS3EPC]   Baldo, N., "The ns-3 EPC module", NS3 EPC Model,
               <https://www.nsnam.org/docs/models/html/lte-
               design.html#epc-model>.

   [NS3LTE]   Baldo, N., "The ns-3 LTE module", NS3 LTE Model,
               <https://www.nsnam.org/docs/models/html/lte-
               design.html#lte-model>.

   [OFFLOAD]   Rebecchi, F., Dias de Amorim, M., Conan, V., Passarella,
               A., Bruno, R., and M. Conti, "Data Offloading Techniques
               in Cellular Networks: A Survey", IEEE Communications
               Surveys and Tutorials, IEEE Xplore DL, vol:17, issue:2,
               pp.580-603, 11 November 2014, <https://
               ieeexplore.ieee.org/document/6953022>.

   [OLTEANU]   Olteanu, A. and P. Xiao, "Fragmentation and AES
               Encryption Overhead in Very High-speed Wireless LANs",
               Proceedings of the 2009 IEEE International Conference on
               Communications ICC'09, ACM DL, pp.575-579, 14 June 2009,
               <http://dl.acm.org/citation.cfm?id=1817271.1817379>.

   [Open5GCore] Open5GCore, M., "Open5GCore - Fundamental 4G Core
               Network Functionality", Open5GCore, <https://
               www.open5gcore.org>.

   [RFC4594]   Babiarz, J., Chan, K., and F. Baker, "Configuration
               Guidelines for DiffServ Service Classes", RFC 4594, DOI
               10.17487/RFC4594, August 2006, <https://www.rfc-
               editor.org/info/rfc4594>.

   [RFC6459]   Korhonen, J., Ed., Soininen, J., Patil, B., Savolainen,
               T., Bajko, G., and K. Iisakkila, "IPv6 in 3rd Generation
               Partnership Project (3GPP) Evolved Packet System (EPS)",
               RFC 6459, DOI 10.17487/RFC6459, January 2012, <https://
               www.rfc-editor.org/info/rfc6459>.

   [RFC7476]
               Pentikousis, K., Ed., Ohlman, B., Corujo, D., Boggia, G.,
               Tyson, G., Davies, E., Molinaro, A., and S. Eum,
               "Information-Centric Networking: Baseline Scenarios", RFC
               7476, DOI 10.17487/RFC7476, March 2015, <https://www.rfc-
               editor.org/info/rfc7476>.

   [RFC7927]
               Kutscher, D., Ed., Eum, S., Pentikousis, K., Psaras, I.,
               Corujo, D., Saucez, D., Schmidt, T., and M. Waehlisch,
               "Information-Centric Networking (ICN) Research

Challenges", RFC 7927, DOI 10.17487/RFC7927, July 2016,
<https://www.rfc-editor.org/info/rfc7927>.

[RFC7945] Pentikousis, K., Ed., Ohlman, B., Davies, E., Spirou, S.,
           and G. Boggia, "Information-Centric Networking:
           Evaluation and Security Considerations", RFC 7945, DOI
           10.17487/RFC7945, September 2016, <https://www.rfc-
           editor.org/info/rfc7945>.

[RFC8569] Mosko, M., Solis, I., and C. Wood, "Content-Centric
           Networking (CCNx) Semantics", RFC 8569, DOI 10.17487/
           RFC8569, July 2019, <https://www.rfc-editor.org/info/
           rfc8569>.

[RFC8609] Mosko, M., Solis, I., and C. Wood, "Content-Centric
           Networking (CCNx) Messages in TLV Format", RFC 8609, DOI
           10.17487/RFC8609, July 2019, <https://www.rfc-editor.org/
           info/rfc8609>.

[RFC9064] Oran, D., "Considerations in the Development of a QoS
           Architecture for CCNx-Like Information-Centric Networking
           Protocols", RFC 9064, DOI 10.17487/RFC9064, June 2021,
           <https://www.rfc-editor.org/info/rfc9064>.

[SDN5G]   Page, J. and J. Dricot, "Software-defined networking for
           low-latency 5G core network", 2016 International
           Conference on Military Communications and Information
           Systems (ICMCIS) IEEE Xplore DL, pp. 1-7, May 2016,
           <https://ieeexplore.ieee.org/document/7496561>.

[TLVCOMP] Mosko, M., "Header Compression for TLV-based Packets",
           ICNRG Buenos Aires IETF 95, 3 April 2016, <https://
           datatracker.ietf.org/meeting/interim-2016-icnrg-02/
           materials/slides-interim-2016-icnrg-2-7>.

[TOURANI] Tourani, R., Misra, S., Mick, T., and G. Panwar,
           "Security, Privacy, and Access Control in Information-
           Centric Networking: A Survey", IEEE Communications
           Surveys and Tutorials Volume 20, Issue 1, pp 566-600,
           September 2017, <https://ieeexplore.ieee.org/document/
           8027034>.

[TS23.203] 3GPP, "Policy and charging control architecture", 3GPP TS
           23.203 10.9.0, 12 September 2013, <http://www.3gpp.org/
           ftp/Specs/html-info/23203.htm>.

[TS23.401] 3GPP, "General Packet Radio Service (GPRS) enhancements
           for Evolved Universal Terrestrial Radio Access Network
           (E-UTRAN) access", 3GPP TS 23.401 10.10.0, 7 March 2013,
           <http://www.3gpp.org/ftp/Specs/html-info/23401.htm>.

[TS23.501]
3GPP, "System Architecture for the 5G System", 3GPP TS
23.501 15.2.0, 15 June 2018, <http://www.3gpp.org/ftp/
Specs/html-info/23501.htm>.

[TS23.714] 3GPP, "Technical Specification Group Services and System
Aspects: Study on control and user plane separation of
EPC nodes", 3GPP TS 23.714 0.2.2, 4 June 2016, <http://
www.3gpp.org/ftp/Specs/html-info/23714.htm>.

[TS29.060] 3GPP, "General Packet Radio Service (GPRS); GPRS
Tunneling Protocol (GTP) across the Gn and Gp interface",
3GPP TS 29.060 3.19.0, 24 March 2004, <http://www.
3gpp.org/ftp/Specs/html-info/29060.htm>.

[TS33.310] 3GPP, "Network Domain Security (NDS); Authentication
Framework (AF)", 3GPP TS 33.310 10.7.0, 21 December 2012,
<http://www.3gpp.org/ftp/Specs/html-info/33310.htm>.

[TS33.320] 3GPP, "Security of Home Node B (HNB) / Home evolved Node
B (HeNB)", 3GPP TS 33.320 10.5.0, 29 June 2012, <http://
www.3gpp.org/ftp/Specs/html-info/33320.htm>.

Authors' Addresses

Prakash Suthar
Google Inc.
Mountain View, California 94043
United States of America

Email: psuthar@google.com

Milan Stolic
Cisco Systems Inc.
Naperville, Illinois 60540
United States of America

Email: mistolic@cisco.com

Anil Jangam (editor)
Cisco Systems Inc.
San Jose, California 95134
United States of America

Email: anjangam@cisco.com

Dirk Trossen
Huawei Technologies
Riesstrasse 25
80992 Munich

Germany

Email: dirk.trossen@huawei.com

Ravi Ravindran
F5 Networks
3545 North First Street
San Jose, 95134
United States of America

Email: r.ravindran@f5.com