Deterministic Networking Use Cases
draft-ietf-detnet-use-cases-06

Abstract

   This draft documents requirements in several diverse industries to
   establish multi-hop paths for characterized flows with deterministic
   properties. In this context deterministic implies that streams can
   be established which provide guaranteed bandwidth and latency which
   can be established from either a Layer 2 or Layer 3 (IP) interface,
   and which can co-exist on an IP network with best-effort traffic.

   Additional requirements include optional redundant paths, very high
   reliability paths, time synchronization, and clock distribution.
   Industries considered include wireless for industrial applications,
   professional audio, electrical utilities, building automation
   systems, radio/mobile access networks, automotive, and gaming.

   For each case, this document will identify the application, identify
   representative solutions used today, and what new uses an IETF DetNet
   solution may enable.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

   This draft presents use cases from diverse industries which have in
   common a need for deterministic streams, but which also differ
   notably in their network topologies and specific desired behavior.
   Together, they provide broad industry context for DetNet and a
   yardstick against which proposed DetNet designs can be measured (to
   what extent does a proposed design satisfy these various use cases?)

   For DetNet, use cases explicitly do not define requirements; The
   DetNet WG will consider the use cases, decide which elements are in
   scope for DetNet, and the results will be incorporated into future
   drafts. Similarly, the DetNet use case draft explicitly does not
   suggest any specific design, architecture or protocols, which will be
   topics of future drafts.

   We present for each use case the answers to the following questions:

   o What is the use case?

   o How is it addressed today?

   o How would you like it to be addressed in the future?

   o What do you want the IETF to deliver?

   The level of detail in each use case should be sufficient to express
   the relevant elements of the use case, but not more.

   At the end we consider the use cases collectively, and examine the
   most significant goals they have in common.

2. Pro Audio Use Cases

2.1. Introduction

   The professional audio and video industry includes music and film
   content creation, broadcast, cinema, and live exposition as well as
   public address, media and emergency systems at large venues
   (airports, stadiums, churches, theme parks). These industries have
   already gone through the transition of audio and video signals from
   analog to digital, however the interconnect systems remain primarily

point-to-point with a single (or small number of) signals per link,
interconnected with purpose-built hardware.

These industries are now attempting to transition to packet based
infrastructure for distributing audio and video in order to reduce
cost, increase routing flexibility, and integrate with existing IT
infrastructure.

However, there are several requirements for making a network the
primary infrastructure for audio and video which are not met by
todays networks and these are our concern in this draft.

The principal requirement is that pro audio and video applications
become able to establish streams that provide guaranteed (bounded)
bandwidth and latency from the Layer 3 (IP) interface. Such streams
can be created today within standards-based layer 2 islands however
these are not sufficient to enable effective distribution over wider
areas (for example broadcast events that span wide geographical
areas).

Some proprietary systems have been created which enable deterministic
streams at layer 3 however they are engineered networks in that they
require careful configuration to operate, often require that the
system be over designed, and it is implied that all devices on the
network voluntarily play by the rules of that network. To enable
these industries to successfully transition to an interoperable
multi-vendor packet-based infrastructure requires effective open
standards, and we believe that establishing relevant IETF standards
is a crucial factor.

It would be highly desirable if such streams could be routed over the
open Internet, however even intermediate solutions with more limited
scope (such as enterprise networks) can provide a substantial
improvement over todays networks, and a solution that only provides
for the enterprise network scenario is an acceptable first step.

We also present more fine grained requirements of the audio and video
industries such as safety and security, redundant paths, devices with
limited computing resources on the network, and that reserved stream
bandwidth is available for use by other best-effort traffic when that
stream is not currently in use.

2.2. Fundamental Stream Requirements

The fundamental stream properties are guaranteed bandwidth and
deterministic latency as described in this section. Additional
stream requirements are described in a subsequent section.

2.2.1. Guaranteed Bandwidth

Transmitting audio and video streams is unlike common file transfer
activities because guaranteed delivery cannot be achieved by re-
trying the transmission; by the time the missing or corrupt packet
has been identified it is too late to execute a re-try operation and
stream playback is interrupted, which is unacceptable in for example
a live concert. In some contexts large amounts of buffering can be
used to provide enough delay to allow time for one or more retries,
however this is not an effective solution when live interaction is
involved, and is not considered an acceptable general solution for
pro audio and video. (Have you ever tried speaking into a microphone
through a sound system that has an echo coming back at you? It makes
it almost impossible to speak clearly).

Providing a way to reserve a specific amount of bandwidth for a given
stream is a key requirement.

2.2.2. Bounded and Consistent Latency

Latency in this context means the amount of time that passes between
when a signal is sent over a stream and when it is received, for
example the amount of time delay between when you speak into a
microphone and when your voice emerges from the speaker. Any delay
longer than about 10-15 milliseconds is noticeable by most live
performers, and greater latency makes the system unusable because it
prevents them from playing in time with the other players (see slide
6 of [SRP_LATENCY]).

The 15ms latency bound is made even more challenging because it is
often the case in network based music production with live electric
instruments that multiple stages of signal processing are used,
connected in series (i.e. from one to the other for example from
guitar through a series of digital effects processors) in which case
the latencies add, so the latencies of each individual stage must all
together remain less than 15ms.

In some situations it is acceptable at the local location for content
from the live remote site to be delayed to allow for a statistically
acceptable amount of latency in order to reduce jitter. However,
once the content begins playing in the local location any audio
artifacts caused by the local network are unacceptable, especially in
those situations where a live local performer is mixed into the feed
from the remote location.

In addition to being bounded to within some predictable and
acceptable amount of time (which may be 15 milliseconds or more or
less depending on the application) the latency also has to be

consistent. For example when playing a film consisting of a video
stream and audio stream over a network, those two streams must be
synchronized so that the voice and the picture match up. A common
tolerance for audio/video sync is one NTSC video frame (about 33ms)
and to maintain the audience perception of correct lip sync the
latency needs to be consistent within some reasonable tolerance, for
example 10%.

A common architecture for synchronizing multiple streams that have
different paths through the network (and thus potentially different
latencies) is to enable measurement of the latency of each path, and
have the data sinks (for example speakers) buffer (delay) all packets
on all but the slowest path. Each packet of each stream is assigned
a presentation time which is based on the longest required delay.
This implies that all sinks must maintain a common time reference of
sufficient accuracy, which can be achieved by any of various
techniques.

This type of architecture is commonly implemented using a central
controller that determines path delays and arbitrates buffering
delays.

2.2.2.1. Optimizations

The controller might also perform optimizations based on the
individual path delays, for example sinks that are closer to the
source can inform the controller that they can accept greater latency
since they will be buffering packets to match presentation times of
farther away sinks. The controller might then move a stream
reservation on a short path to a longer path in order to free up
bandwidth for other critical streams on that short path. See slides
3-5 of [SRP_LATENCY].

Additional optimization can be achieved in cases where sinks have
differing latency requirements, for example in a live outdoor concert
the speaker sinks have stricter latency requirements than the
recording hardware sinks. See slide 7 of [SRP_LATENCY].

Device cost can be reduced in a system with guaranteed reservations
with a small bounded latency due to the reduced requirements for
buffering (i.e. memory) on sink devices. For example, a theme park
might broadcast a live event across the globe via a layer 3 protocol;
in such cases the size of the buffers required is proportional to the
latency bounds and jitter caused by delivery, which depends on the
worst case segment of the end-to-end network path. For example on
todays open internet the latency is typically unacceptable for audio
and video streaming without many seconds of buffering. In such
scenarios a single gateway device at the local network that receives

the feed from the remote site would provide the expensive buffering
required to mask the latency and jitter issues associated with long
distance delivery. Sink devices in the local location would have no
additional buffering requirements, and thus no additional costs,
beyond those required for delivery of local content. The sink device
would be receiving the identical packets as those sent by the source
and would be unaware that there were any latency or jitter issues
along the path.

2.3. Additional Stream Requirements

The requirements in this section are more specific yet are common to
multiple audio and video industry applications.

2.3.1. Deterministic Time to Establish Streaming

Some audio systems installed in public environments (airports,
hospitals) have unique requirements with regards to health, safety
and fire concerns. One such requirement is a maximum of 3 seconds
for a system to respond to an emergency detection and begin sending
appropriate warning signals and alarms without human intervention.
For this requirement to be met, the system must support a bounded and
acceptable time from a notification signal to specific stream
establishment. For further details see [ISO7240-16].

Similar requirements apply when the system is restarted after a power
cycle, cable re-connection, or system reconfiguration.

In many cases such re-establishment of streaming state must be
achieved by the peer devices themselves, i.e. without a central
controller (since such a controller may only be present during
initial network configuration).

Video systems introduce related requirements, for example when
transitioning from one camera feed to another. Such systems
currently use purpose-built hardware to switch feeds smoothly,
however there is a current initiative in the broadcast industry to
switch to a packet-based infrastructure (see [STUDIO_IP] and the ESPN
DC2 use case described below).

2.3.2. Use of Unused Reservations by Best-Effort Traffic

In cases where stream bandwidth is reserved but not currently used
(or is under-utilized) that bandwidth must be available to best-
effort (i.e. non-time-sensitive) traffic. For example a single
stream may be nailed up (reserved) for specific media content that
needs to be presented at different times of the day, ensuring timely
delivery of that content, yet in between those times the full

bandwidth of the network can be utilized for best-effort tasks such as file transfers.

This also addresses a concern of IT network administrators that are considering adding reserved bandwidth traffic to their networks that users will just reserve a ton of bandwidth and then never un-reserve it even though they are not using it, and soon they will have no bandwidth left.

2.3.3. Layer 3 Interconnecting Layer 2 Islands

As an intermediate step (short of providing guaranteed bandwidth across the open internet) it would be valuable to provide a way to connect multiple Layer 2 networks. For example layer 2 techniques could be used to create a LAN for a single broadcast studio, and several such studios could be interconnected via layer 3 links.

2.3.4. Secure Transmission

Digital Rights Management (DRM) is very important to the audio and video industries. Any time protected content is introduced into a network there are DRM concerns that must be maintained (see [CONTENT_PROTECTION]). Many aspects of DRM are outside the scope of network technology, however there are cases when a secure link supporting authentication and encryption is required by content owners to carry their audio or video content when it is outside their own secure environment (for example see [DCI]).

As an example, two techniques are Digital Transmission Content Protection (DTCP) and High-Bandwidth Digital Content Protection (HDCP). HDCP content is not approved for retransmission within any other type of DRM, while DTCP may be retransmitted under HDCP. Therefore if the source of a stream is outside of the network and it uses HDCP protection it is only allowed to be placed on the network with that same HDCP protection.

2.3.5. Redundant Paths

On-air and other live media streams must be backed up with redundant links that seamlessly act to deliver the content when the primary link fails for any reason. In point-to-point systems this is provided by an additional point-to-point link; the analogous requirement in a packet-based system is to provide an alternate path through the network such that no individual link can bring down the system.

2.3.6. Link Aggregation

For transmitting streams that require more bandwidth than a single
link in the target network can support, link aggregation is a
technique for combining (aggregating) the bandwidth available on
multiple physical links to create a single logical link of the
required bandwidth. However, if aggregation is to be used, the
network controller (or equivalent) must be able to determine the
maximum latency of any path through the aggregate link (see Bounded
and Consistent Latency section above).

2.3.7. Traffic Segregation

Sink devices may be low cost devices with limited processing power.
In order to not overwhelm the CPUs in these devices it is important
to limit the amount of traffic that these devices must process.

As an example, consider the use of individual seat speakers in a
cinema. These speakers are typically required to be cost reduced
since the quantities in a single theater can reach hundreds of seats.
Discovery protocols alone in a one thousand seat theater can generate
enough broadcast traffic to overwhelm a low powered CPU. Thus an
installation like this will benefit greatly from some type of traffic
segregation that can define groups of seats to reduce traffic within
each group. All seats in the theater must still be able to
communicate with a central controller.

There are many techniques that can be used to support this
requirement including (but not limited to) the following examples.

2.3.7.1. Packet Forwarding Rules, VLANs and Subnets

Packet forwarding rules can be used to eliminate some extraneous
streaming traffic from reaching potentially low powered sink devices,
however there may be other types of broadcast traffic that should be
eliminated using other means for example VLANs or IP subnets.

2.3.7.2. Multicast Addressing (IPv4 and IPv6)

Multicast addressing is commonly used to keep bandwidth utilization
of shared links to a minimum.

Because of the MAC Address forwarding nature of Layer 2 bridges it is
important that a multicast MAC address is only associated with one
stream. This will prevent reservations from forwarding packets from
one stream down a path that has no interested sinks simply because
there is another stream on that same path that shares the same
multicast MAC address.

Since each multicast MAC Address can represent 32 different IPv4
multicast addresses there must be a process put in place to make sure
this does not occur. Requiring use of IPv6 address can achieve this,
however due to their continued prevalence, solutions that are
effective for IPv4 installations are also required.

2.4. Integration of Reserved Streams into IT Networks

A commonly cited goal of moving to a packet based media
infrastructure is that costs can be reduced by using off the shelf,
commodity network hardware. In addition, economy of scale can be
realized by combining media infrastructure with IT infrastructure.
In keeping with these goals, stream reservation technology should be
compatible with existing protocols, and not compromise use of the
network for best effort (non-time-sensitive) traffic.

2.5. Security Considerations

Many industries that are moving from the point-to-point world to the
digital network world have little understanding of the pitfalls that
they can create for themselves with improperly implemented network
infrastructure. DetNet should consider ways to provide security
against DoS attacks in solutions directed at these markets. Some
considerations are given here as examples of ways that we can help
new users avoid common pitfalls.

2.5.1. Denial of Service

One security pitfall that this author is aware of involves the use of
technology that allows a presenter to throw the content from their
tablet or smart phone onto the A/V system that is then viewed by all
those in attendance. The facility introducing this technology was
quite excited to allow such modern flexibility to those who came to
speak. One thing they hadn't realized was that since no security was
put in place around this technology it left a hole in the system that
allowed other attendees to "throw" their own content onto the A/V
system.

2.5.2. Control Protocols

Professional audio systems can include amplifiers that are capable of
generating hundreds or thousands of watts of audio power which if
used incorrectly can cause hearing damage to those in the vicinity.
Apart from the usual care required by the systems operators to
prevent such incidents, the network traffic that controls these
devices must be secured (as with any sensitive application traffic).
In addition, it would be desirable if the configuration protocols
that are used to create the network paths used by the professional

audio traffic could be designed to protect devices that are not meant
to receive high-amplitude content from having such potentially
damaging signals routed to them.

2.6. A State-of-the-Art Broadcast Installation Hits Technology Limits

ESPN recently constructed a state-of-the-art 194,000 sq ft, $125
million broadcast studio called DC2. The DC2 network is capable of
handling 46 Tbps of throughput with 60,000 simultaneous signals.
Inside the facility are 1,100 miles of fiber feeding four audio
control rooms. (See details at [ESPN_DC2]).

In designing DC2 they replaced as much point-to-point technology as
they possibly could with packet-based technology. They constructed
seven individual studios using layer 2 LANS (using IEEE 802.1 AVB)
that were entirely effective at routing audio within the LANs, and
they were very happy with the results, however to interconnect these
layer 2 LAN islands together they ended up using dedicated links
because there is no standards-based routing solution available.

This is the kind of motivation we have to develop these standards
because customers are ready and able to use them.

3. Electrical Utilities

3.1. Use Case Description

Many systems that an electrical utility deploys today rely on high
availability and deterministic behavior of the underlying networks.
Here we present use cases in Transmission, Generation and
Distribution, including key timing and reliability metrics. We also
discuss security issues and industry trends which affect the
architecture of next generation utility networks

3.1.1. Transmission Use Cases

3.1.1.1. Protection

Protection means not only the protection of human operators but also
the protection of the electrical equipment and the preservation of
the stability and frequency of the grid. If a fault occurs in the
transmission or distribution of electricity then severe damage can
occur to human operators, electrical equipment and the grid itself,
leading to blackouts.

Communication links in conjunction with protection relays are used to
selectively isolate faults on high voltage lines, transformers,
reactors and other important electrical equipment. The role of the

teleprotection system is to selectively disconnect a faulty part by
transferring command signals within the shortest possible time.

3.1.1.1.1. Key Criteria

The key criteria for measuring teleprotection performance are command
transmission time, dependability and security. These criteria are
defined by the IEC standard 60834 as follows:

o Transmission time (Speed): The time between the moment where state
   changes at the transmitter input and the moment of the
   corresponding change at the receiver output, including propagation
   delay. Overall operating time for a teleprotection system
   includes the time for initiating the command at the transmitting
   end, the propagation delay over the network (including equipments)
   and the selection and decision time at the receiving end,
   including any additional delay due to a noisy environment.

o Dependability: The ability to issue and receive valid commands in
   the presence of interference and/or noise, by minimizing the
   probability of missing command (PMC). Dependability targets are
   typically set for a specific bit error rate (BER) level.

o Security: The ability to prevent false tripping due to a noisy
   environment, by minimizing the probability of unwanted commands
   (PUC). Security targets are also set for a specific bit error
   rate (BER) level.

Additional elements of the the teleprotection system that impact its
performance include:

o Network bandwidth

o Failure recovery capacity (aka resiliency)

3.1.1.1.2. Fault Detection and Clearance Timing

Most power line equipment can tolerate short circuits or faults for
up to approximately five power cycles before sustaining irreversible
damage or affecting other segments in the network. This translates
to total fault clearance time of 100ms. As a safety precaution,
however, actual operation time of protection systems is limited to
70- 80 percent of this period, including fault recognition time,
command transmission time and line breaker switching time.

Some system components, such as large electromechanical switches,
require particularly long time to operate and take up the majority of
the total clearance time, leaving only a 10ms window for the

telecommunications part of the protection scheme, independent of the distance to travel. Given the sensitivity of the issue, new networks impose requirements that are even more stringent: IEC standard 61850 limits the transfer time for protection messages to 1/4 - 1/2 cycle or 4 - 8ms (for 60Hz lines) for the most critical messages.

3.1.1.1.3. Symmetric Channel Delay

Teleprotection channels which are differential must be synchronous, which means that any delays on the transmit and receive paths must match each other. Teleprotection systems ideally support zero asymmetric delay; typical legacy relays can tolerate delay discrepancies of up to 750us.

Some tools available for lowering delay variation below this threshold are:

o For legacy systems using Time Division Multiplexing (TDM), jitter buffers at the multiplexers on each end of the line can be used to offset delay variation by queuing sent and received packets. The length of the queues must balance the need to regulate the rate of transmission with the need to limit overall delay, as larger buffers result in increased latency.

o For jitter-prone IP packet networks, traffic management tools can ensure that the teleprotection signals receive the highest transmission priority to minimize jitter.

o Standard packet-based synchronization technologies, such as 1588-2008 Precision Time Protocol (PTP) and Synchronous Ethernet (Sync-E), can help keep networks stable by maintaining a highly accurate clock source on the various network devices.

3.1.1.1.4. Teleprotection Network Requirements (IEC 61850)

The following table captures the main network metrics as based on the IEC 61850 standard.

Teleprotection Requirement	Attribute
One way maximum delay	4-10 ms
Asymetric delay required	Yes
Maximum jitter	less than 250 us (750 us for legacy IED)
Topology	Point to point, point to Multi-point
Availability	99.9999
precise timing required	Yes
Recovery time on node failure	less than 50ms - hitless
performance management	Yes, Mandatory
Redundancy	Yes
Packet loss	0.1% to 1%

Table 1: Teleprotection network requirements

3.1.1.1.5. Inter-Trip Protection scheme

"Inter-tripping" is the signal-controlled tripping of a circuit
breaker to complete the isolation of a circuit or piece of apparatus
in concert with the tripping of other circuit breakers.

Inter-Trip protection Requirement	Attribute
One way maximum delay	5 ms
Asymetric delay required	No
Maximum jitter	Not critical
Topology	Point to point, point to Multi-point
Bandwidth	64 Kbps
Availability	99.9999
precise timing required	Yes
Recovery time on node failure	less than 50ms - hitless
performance management	Yes, Mandatory
Redundancy	Yes
Packet loss	0.1%

Table 2: Inter-Trip protection network requirements

3.1.1.1.6. **Current Differential Protection Scheme**

   Current differential protection is commonly used for line protection,
   and is typical for protecting parallel circuits. At both end of the
   lines the current is measured by the differential relays, and both
   relays will trip the circuit breaker if the current going into the
   line does not equal the current going out of the line. This type of
   protection scheme assumes some form of communications being present
   between the relays at both end of the line, to allow both relays to
   compare measured current values. Line differential protection
   schemes assume a very low telecommunications delay between both
   relays, often as low as 5ms. Moreover, as those systems are often
   not time-synchronized, they also assume symmetric telecommunications
   paths with constant delay, which allows comparing current measurement
   values taken at the exact same time.

   +--------------------------------+-------------------------------+
   | Current Differential protection | Attribute |
   | Requirement | |
   +--------------------------------+-------------------------------+
One way maximum delay	5 ms
Asymetric delay Required	Yes
Maximum jitter	less than 250 us (750us for
	legacy IED)
Topology	Point to point, point to
	Multi-point
Bandwidth	64 Kbps
Availability	99.9999
precise timing required	Yes
Recovery time on node failure	less than 50ms - hitless
performance management	Yes, Mandatory
Redundancy	Yes
Packet loss	0.1%
   +--------------------------------+-------------------------------+

                 Table 3: Current Differential Protection metrics

3.1.1.1.7. **Distance Protection Scheme**

   Distance (Impedance Relay) protection scheme is based on voltage and
   current measurements. The network metrics are similar (but not
   identical to) Current Differential protection.

Distance protection Requirement	Attribute
One way maximum delay	5 ms
Asymetric delay Required	No
Maximum jitter	Not critical
Topology	Point to point, point to Multi-point
Bandwidth	64 Kbps
Availability	99.9999
precise timing required	Yes
Recovery time on node failure	less than 50ms - hitless
performance management	Yes, Mandatory
Redundancy	Yes
Packet loss	0.1%

Table 4: Distance Protection requirements

3.1.1.1.8. Inter-Substation Protection Signaling

This use case describes the exchange of Sampled Value and/or GOOSE (Generic Object Oriented Substation Events) message between Intelligent Electronic Devices (IED) in two substations for protection and tripping coordination. The two IEDs are in a master-slave mode.

The Current Transformer or Voltage Transformer (CT/VT) in one substation sends the sampled analog voltage or current value to the Merging Unit (MU) over hard wire. The MU sends the time-synchronized 61850-9-2 sampled values to the slave IED. The slave IED forwards the information to the Master IED in the other substation. The master IED makes the determination (for example based on sampled value differentials) to send a trip command to the originating IED. Once the slave IED/Relay receives the GOOSE trip for breaker tripping, it opens the breaker. It then sends a confirmation message back to the master. All data exchanges between IEDs are either through Sampled Value and/or GOOSE messages.

```
+--------------------------------+-------------------------------+
|   Inter-Substation protection  |           Attribute           |
|          Requirement           |                               |
+--------------------------------+-------------------------------+
|      One way maximum delay     |             5 ms              |
|      Asymetric delay Required  |              No               |
|         Maximum jitter         |          Not critical         |
|            Topology            |    Point to point, point to   |
|                                |          Multi-point          |
|            Bandwidth           |            64 Kbps            |
|            Availability         |            99.9999           |
|      precise timing required   |              Yes              |
|   Recovery time on node failure |    less than 50ms - hitless   |
|      performance management    |         Yes, Mandatory        |
|            Redundancy          |              Yes              |
|            Packet loss         |              1%               |
+--------------------------------+-------------------------------+
```

Table 5: Inter-Substation Protection requirements

3.1.1.2. Intra-Substation Process Bus Communications

This use case describes the data flow from the CT/VT to the IEDs in
the substation via the MU. The CT/VT in the substation send the
sampled value (analog voltage or current) to the MU over hard wire.
The MU sends the time-synchronized 61850-9-2 sampled values to the
IEDs in the substation in GOOSE message format. The GPS Master Clock
can send 1PPS or IRIG-B format to the MU through a serial port or
IEEE 1588 protocol via a network. Process bus communication using
61850 simplifies connectivity within the substation and removes the
requirement for multiple serial connections and removes the slow
serial bus architectures that are typically used. This also ensures
increased flexibility and increased speed with the use of multicast
messaging between multiple devices.

+--------------------------------+-------------------------------+
| Intra-Substation protection | Attribute |
| Requirement | |
+--------------------------------+-------------------------------+
One way maximum delay	5 ms
Asymetric delay Required	No
Maximum jitter	Not critical
Topology	Point to point, point to
	Multi-point
Bandwidth	64 Kbps
Availability	99.9999
precise timing required	Yes
Recovery time on Node failure	less than 50ms - hitless
performance management	Yes, Mandatory
Redundancy	Yes - No
Packet loss	0.1%
+--------------------------------+-------------------------------+

              Table 6: Intra-Substation Protection requirements

3.1.1.3. Wide Area Monitoring and Control Systems

The application of synchrophasor measurement data from Phasor
Measurement Units (PMU) to Wide Area Monitoring and Control Systems
promises to provide important new capabilities for improving system
stability. Access to PMU data enables more timely situational
awareness over larger portions of the grid than what has been
possible historically with normal SCADA (Supervisory Control and Data
Acquisition) data. Handling the volume and real-time nature of
synchrophasor data presents unique challenges for existing
application architectures. Wide Area management System (WAMS) makes
it possible for the condition of the bulk power system to be observed
and understood in real-time so that protective, preventative, or
corrective action can be taken. Because of the very high sampling
rate of measurements and the strict requirement for time
synchronization of the samples, WAMS has stringent telecommunications
requirements in an IP network that are captured in the following
table:

WAMS Requirement	Attribute
One way maximum delay	50 ms
Asymetric delay Required	No
Maximum jitter	Not critical
Topology	Point to point, point to Multi-point, Multi-point to Multi-point
Bandwidth	100 Kbps
Availability	99.9999
precise timing required	Yes
Recovery time on Node failure	less than 50ms - hitless
performance management	Yes, Mandatory
Redundancy	Yes
Packet loss	1%

Table 7: WAMS Special Communication Requirements

3.1.1.4. IEC 61850 WAN engineering guidelines requirement classification

The IEC (International Electrotechnical Commission) has recently published a Technical Report which offers guidelines on how to define and deploy Wide Area Networks for the interconnections of electric substations, generation plants and SCADA operation centers. The IEC 61850-90-12 is providing a classification of WAN communication requirements into 4 classes. Table 8 summarizes these requirements:

WAN Requirement	Class WA	Class WB	Class WC	Class WD
Application field	EHV (Extra High Voltage)	HV (High Voltage)	MV (Medium Voltage)	General purpose
Latency	5 ms	10 ms	100 ms	> 100 ms
Jitter	10 us	100 us	1 ms	10 ms
Latency Asymetry	100 us	1 ms	10 ms	100 ms
Time Accuracy	1 us	10 us	100 us	10 to 100 ms
Bit Error rate	10-7 to 10-6	10-5 to 10-4	10-3	
Unavailability	10-7 to 10-6	10-5 to 10-4	10-3	
Recovery delay	Zero	50 ms	5 s	50 s
Cyber security	extremely high	High	Medium	Medium

Table 8: 61850-90-12 Communication Requirements; Courtesy of IEC

3.1.2. Generation Use Case

The electrical power generation frequency should be maintained within
a very narrow band. Deviations from the acceptable frequency range
are detected and the required signals are sent to the power plants
for frequency regulation.

Automatic generation control (AGC) is a system for adjusting the
power output of generators at different power plants, in response to
changes in the load.

FCAG (Frequency Control Automatic Generation) Requirement	Attribute
One way maximum delay	500 ms
Asymetric delay Required	No
Maximum jitter	Not critical
Topology	Point to point
Bandwidth	20 Kbps
Availability	99.999
precise timing required	Yes
Recovery time on Node failure	N/A
performance management	Yes, Mandatory
Redundancy	Yes
Packet loss	1%

Table 9: FCAG Communication Requirements

3.1.3. Distribution use case

3.1.3.1. Fault Location Isolation and Service Restoration (FLISR)

Fault Location, Isolation, and Service Restoration (FLISR) refers to
the ability to automatically locate the fault, isolate the fault, and
restore service in the distribution network. This will likely be the
first widespread application of distributed intelligence in the grid.

Static power switch status (open/closed) in the network dictates the
power flow to secondary substations. Reconfiguring the network in
the event of a fault is typically done manually on site to energize/
de-energize alternate paths. Automating the operation of substation
switchgear allows the flow of power to be altered automatically under
fault conditions.

FLISR can be managed centrally from a Distribution Management System
(DMS) or executed locally through distributed control via intelligent
switches and fault sensors.

FLISR Requirement	Attribute
One way maximum delay	80 ms
Asymetric delay Required	No
Maximum jitter	40 ms
Topology	Point to point, point to Multi-point, Multi-point to Multi-point
Bandwidth	64 Kbps
Availability	99.9999
precise timing required	Yes
Recovery time on Node failure	Depends on customer impact
performance management	Yes, Mandatory
Redundancy	Yes
Packet loss	0.1%

Table 10: FLISR Communication Requirements

3.2. Electrical Utilities Today

Many utilities still rely on complex environments formed of multiple
application-specific proprietary networks, including TDM networks.

In this kind of environment there is no mixing of OT and IT
applications on the same network, and information is siloed between
operational areas.

Specific calibration of the full chain is required, which is costly.

This kind of environment prevents utility operations from realizing
the operational efficiency benefits, visibility, and functional
integration of operational information across grid applications and
data networks.

In addition, there are many security-related issues as discussed in
the following section.

3.2.1. Security Current Practices and Limitations

Grid monitoring and control devices are already targets for cyber
attacks, and legacy telecommunications protocols have many intrinsic
network-related vulnerabilities. For example, DNP3, Modbus,

PROFIBUS/PROFINET, and other protocols are designed around a common paradigm of request and respond. Each protocol is designed for a master device such as an HMI (Human Machine Interface) system to send commands to subordinate slave devices to retrieve data (reading inputs) or control (writing to outputs). Because many of these protocols lack authentication, encryption, or other basic security measures, they are prone to network-based attacks, allowing a malicious actor or attacker to utilize the request-and-respond system as a mechanism for command-and-control like functionality. Specific security concerns common to most industrial control, including utility telecommunication protocols include the following:

o Network or transport errors (e.g. malformed packets or excessive latency) can cause protocol failure.

o Protocol commands may be available that are capable of forcing slave devices into inoperable states, including powering-off devices, forcing them into a listen-only state, disabling alarming.

o Protocol commands may be available that are capable of restarting communications and otherwise interrupting processes.

o Protocol commands may be available that are capable of clearing, erasing, or resetting diagnostic information such as counters and diagnostic registers.

o Protocol commands may be available that are capable of requesting sensitive information about the controllers, their configurations, or other need-to-know information.

o Most protocols are application layer protocols transported over TCP; therefore it is easy to transport commands over non-standard ports or inject commands into authorized traffic flows.

o Protocol commands may be available that are capable of broadcasting messages to many devices at once (i.e. a potential DoS).

o Protocol commands may be available to query the device network to obtain defined points and their values (i.e. a configuration scan).

o Protocol commands may be available that will list all available function codes (i.e. a function scan).

These inherent vulnerabilities, along with increasing connectivity between IT an OT networks, make network-based attacks very feasible.

Simple injection of malicious protocol commands provides control over
the target process. Altering legitimate protocol traffic can also
alter information about a process and disrupt the legitimate controls
that are in place over that process. A man-in-the-middle attack
could provide both control over a process and misrepresentation of
data back to operator consoles.

3.3. Electrical Utilities Future

The business and technology trends that are sweeping the utility
industry will drastically transform the utility business from the way
it has been for many decades. At the core of many of these changes
is a drive to modernize the electrical grid with an integrated
telecommunications infrastructure. However, interoperability
concerns, legacy networks, disparate tools, and stringent security
requirements all add complexity to the grid transformation. Given
the range and diversity of the requirements that should be addressed
by the next generation telecommunications infrastructure, utilities
need to adopt a holistic architectural approach to integrate the
electrical grid with digital telecommunications across the entire
power delivery chain.

The key to modernizing grid telecommunications is to provide a
common, adaptable, multi-service network infrastructure for the
entire utility organization. Such a network serves as the platform
for current capabilities while enabling future expansion of the
network to accommodate new applications and services.

To meet this diverse set of requirements, both today and in the
future, the next generation utility telecommunnications network will
be based on open-standards-based IP architecture. An end-to-end IP
architecture takes advantage of nearly three decades of IP technology
development, facilitating interoperability across disparate networks
and devices, as it has been already demonstrated in many mission-
critical and highly secure networks.

IPv6 is seen as a future telecommunications technology for the Smart
Grid; the IEC (International Electrotechnical Commission) and
different National Committees have mandated a specific adhoc group
(AHG8) to define the migration strategy to IPv6 for all the IEC TC57
power automation standards.

3.3.1. Migration to Packet-Switched Network

Throughout the world, utilities are increasingly planning for a
future based on smart grid applications requiring advanced
telecommunications systems. Many of these applications utilize
packet connectivity for communicating information and control signals

across the utility's Wide Area Network (WAN), made possible by
technologies such as multiprotocol label switching (MPLS). The data
that traverses the utility WAN includes:

o Grid monitoring, control, and protection data

o Non-control grid data (e.g. asset data for condition-based
   monitoring)

o Physical safety and security data (e.g. voice and video)

o Remote worker access to corporate applications (voice, maps,
   schematics, etc.)

o Field area network backhaul for smart metering, and distribution
   grid management

o Enterprise traffic (email, collaboration tools, business
   applications)

WANs support this wide variety of traffic to and from substations,
the transmission and distribution grid, generation sites, between
control centers, and between work locations and data centers. To
maintain this rapidly expanding set of applications, many utilities
are taking steps to evolve present time-division multiplexing (TDM)
based and frame relay infrastructures to packet systems. Packet-
based networks are designed to provide greater functionalities and
higher levels of service for applications, while continuing to
deliver reliability and deterministic (real-time) traffic support.

3.3.2. Telecommunications Trends

These general telecommunications topics are in addition to the use
cases that have been addressed so far. These include both current
and future telecommunications related topics that should be factored
into the network architecture and design.

3.3.2.1. General Telecommunications Requirements

o IP Connectivity everywhere

o Monitoring services everywhere and from different remote centers

o Move services to a virtual data center

o Unify access to applications / information from the corporate
   network

o Unify services

o Unified Communications Solutions

o Mix of fiber and microwave technologies - obsolescence of SONET/
   SDH or TDM

o Standardize grid telecommunications protocol to opened standard to
   ensure interoperability

o Reliable Telecommunications for Transmission and Distribution
   Substations

o IEEE 1588 time synchronization Client / Server Capabilities

o Integration of Multicast Design

o QoS Requirements Mapping

o Enable Future Network Expansion

o Substation Network Resilience

o Fast Convergence Design

o Scalable Headend Design

o Define Service Level Agreements (SLA) and Enable SLA Monitoring

o Integration of 3G/4G Technologies and future technologies

o Ethernet Connectivity for Station Bus Architecture

o Ethernet Connectivity for Process Bus Architecture

o Protection, teleprotection and PMU (Phaser Measurement Unit) on IP

3.3.2.2. Specific Network topologies of Smart Grid Applications

   Utilities often have very large private telecommunications networks.
   It covers an entire territory / country. The main purpose of the
   network, until now, has been to support transmission network
   monitoring, control, and automation, remote control of generation
   sites, and providing FCAPS (Fault, Configuration, Accounting,
   Performance, Security) services from centralized network operation
   centers.

Going forward, one network will support operation and maintenance of
electrical networks (generation, transmission, and distribution),
voice and data services for ten of thousands of employees and for
exchange with neighboring interconnections, and administrative
services. To meet those requirements, utility may deploy several
physical networks leveraging different technologies across the
country: an optical network and a microwave network for instance.
Each protection and automatism system between two points has two
telecommunications circuits, one on each network. Path diversity
between two substations is key. Regardless of the event type
(hurricane, ice storm, etc.), one path shall stay available so the
system can still operate.

In the optical network, signals are transmitted over more than tens
of thousands of circuits using fiber optic links, microwave and
telephone cables. This network is the nervous system of the
utility's power transmission operations. The optical network
represents ten of thousands of km of cable deployed along the power
lines, with individual runs as long as 280 km.

3.3.2.3. Precision Time Protocol

Some utilities do not use GPS clocks in generation substations. One
of the main reasons is that some of the generation plants are 30 to
50 meters deep under ground and the GPS signal can be weak and
unreliable. Instead, atomic clocks are used. Clocks are
synchronized amongst each other. Rubidium clocks provide clock and
1ms timestamps for IRIG-B.

Some companies plan to transition to the Precision Time Protocol
(PTP, [IEEE1588]), distributing the synchronization signal over the
IP/MPLS network. PTP provides a mechanism for synchronizing the
clocks of participating nodes to a high degree of accuracy and
precision.

PTP operates based on the following assumptions:

   It is assumed that the network eliminates cyclic forwarding of PTP
   messages within each communication path (e.g. by using a spanning
   tree protocol).

   PTP is tolerant of an occasional missed message, duplicated
   message, or message that arrived out of order. However, PTP
   assumes that such impairments are relatively rare.

   PTP was designed assuming a multicast communication model, however
   PTP also supports a unicast communication model as long as the
   behavior of the protocol is preserved.

Like all message-based time transfer protocols, PTP time accuracy is degraded by delay asymmetry in the paths taken by event messages. Asymmetry is not detectable by PTP, however, if such delays are known a priori, PTP can correct for asymmetry.

IEC 61850 will recommend the use of the IEEE PTP 1588 Utility Profile (as defined in [IEC62439-3:2012] Annex B) which offers the support of redundant attachment of clocks to Parallel Redundancy Protcol (PRP) and High-availability Seamless Redundancy (HSR) networks.

3.3.3. Security Trends in Utility Networks

Although advanced telecommunications networks can assist in transforming the energy industry by playing a critical role in maintaining high levels of reliability, performance, and manageability, they also introduce the need for an integrated security infrastructure. Many of the technologies being deployed to support smart grid projects such as smart meters and sensors can increase the vulnerability of the grid to attack. Top security concerns for utilities migrating to an intelligent smart grid telecommunications platform center on the following trends:

o Integration of distributed energy resources

o Proliferation of digital devices to enable management, automation, protection, and control

o Regulatory mandates to comply with standards for critical infrastructure protection

o Migration to new systems for outage management, distribution automation, condition-based maintenance, load forecasting, and smart metering

o Demand for new levels of customer service and energy management

This development of a diverse set of networks to support the integration of microgrids, open-access energy competition, and the use of network-controlled devices is driving the need for a converged security infrastructure for all participants in the smart grid, including utilities, energy service providers, large commercial and industrial, as well as residential customers. Securing the assets of electric power delivery systems (from the control center to the substation, to the feeders and down to customer meters) requires an end-to-end security infrastructure that protects the myriad of telecommunications assets used to operate, monitor, and control power flow and measurement.

"Cyber security" refers to all the security issues in automation and telecommunications that affect any functions related to the operation of the electric power systems. Specifically, it involves the concepts of:

o Integrity : data cannot be altered undetectably

o Authenticity : the telecommunications parties involved must be validated as genuine

o Authorization : only requests and commands from the authorized users can be accepted by the system

o Confidentiality : data must not be accessible to any unauthenticated users

When designing and deploying new smart grid devices and telecommunications systems, it is imperative to understand the various impacts of these new components under a variety of attack situations on the power grid. Consequences of a cyber attack on the grid telecommunications network can be catastrophic. This is why security for smart grid is not just an ad hoc feature or product, it's a complete framework integrating both physical and Cyber security requirements and covering the entire smart grid networks from generation to distribution. Security has therefore become one of the main foundations of the utility telecom network architecture and must be considered at every layer with a defense-in-depth approach. Migrating to IP based protocols is key to address these challenges for two reasons:

o IP enables a rich set of features and capabilities to enhance the security posture

o IP is based on open standards, which allows interoperability between different vendors and products, driving down the costs associated with implementing security solutions in OT networks.

Securing OT (Operation technology) telecommunications over packet-switched IP networks follow the same principles that are foundational for securing the IT infrastructure, i.e., consideration must be given to enforcing electronic access control for both person-to-machine and machine-to-machine communications, and providing the appropriate levels of data privacy, device and platform integrity, and threat detection and mitigation.

3.4. Electrical Utilities Asks

o Mixed L2 and L3 topologies

o Deterministic behavior

o Bounded latency and jitter

o High availability, low recovery time

o Redundancy, low packet loss

o Precise timing

o Centralized computing of deterministic paths

o Distributed configuration may also be useful

4. Building Automation Systems

4.1. Use Case Description

A Building Automation System (BAS) manages equipment and sensors in a
building for improving residents' comfort, reducing energy
consumption, and responding to failures and emergencies. For
example, the BAS measures the temperature of a room using sensors and
then controls the HVAC (heating, ventilating, and air conditioning)
to maintain a set temperature and minimize energy consumption.

A BAS primarily performs the following functions:

o Periodically measures states of devices, for example humidity and
   illuminance of rooms, open/close state of doors, FAN speed, etc.

o Stores the measured data.

o Provides the measured data to BAS systems and operators.

o Generates alarms for abnormal state of devices.

o Controls devices (e.g. turn off room lights at 10:00 PM).

4.2. Building Automation Systems Today

4.2.1. BAS Architecture

   A typical BAS architecture of today is shown in Figure 1.
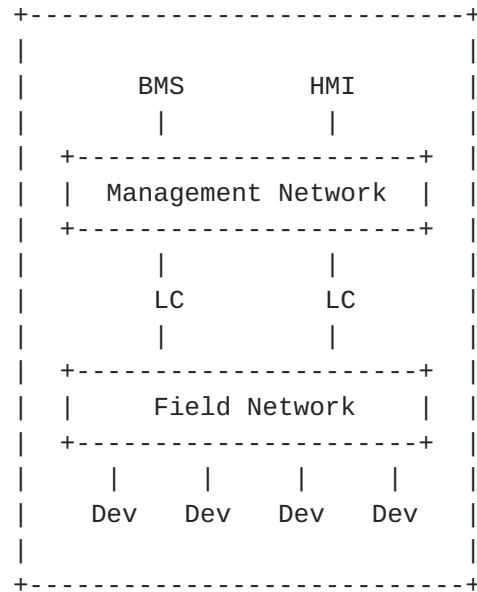
```
        +------------------------------+
        |                              |
        |       BMS         HMI        |
        |        |           |         |
        |   +----------------------+   |
        |   |  Management Network  |   |
        |   +----------------------+   |
        |        |           |         |
        |       LC          LC         |
        |        |           |         |
        |   +----------------------+   |
        |   |     Field Network    |   |
        |   +----------------------+   |
        |     |    |    |    |         |
        |    Dev  Dev  Dev  Dev        |
        |                              |
        +------------------------------+


            BMS := Building Management Server
            HMI := Human Machine Interface
            LC  := Local Controller
```

                     Figure 1: BAS architecture

   There are typically two layers of network in a BAS. The upper one is
   called the Management Network and the lower one is called the Field
   Network. In management networks an IP-based communication protocol
   is used, while in field networks non-IP based communication protocols
   ("field protocols") are mainly used. Field networks have specific
   timing requirements, whereas management networks can be best-effort.

   A Human Machine Interface (HMI) is typically a desktop PC used by
   operators to monitor and display device states, send device control
   commands to Local Controllers (LCs), and configure building schedules
   (for example "turn off all room lights in the building at 10:00 PM").

   A Building Management Server (BMS) performs the following operations.

   o Collect and store device states from LCs at regular intervals.

   o Send control values to LCs according to a building schedule.

   o Send an alarm signal to operators if it detects abnormal devices
      states.

The BMS and HMI communicate with LCs via IP-based "management
protocols" (see standards [bacnetip], [knx]).

A LC is typically a Programmable Logic Controller (PLC) which is
connected to several tens or hundreds of devices using "field
protocols". An LC performs the following kinds of operations:

o Measure device states and provide the information to BMS or HMI.

o Send control values to devices, unilaterally or as part of a
   feedback control loop.

There are many field protocols used today; some are standards-based
and others are proprietary (see standards [lontalk], [modbus],
[profibus] and [flnet]). The result is that BASs have multiple MAC/
PHY modules and interfaces. This makes BASs more expensive, slower
to develop, and can result in "vendor lock-in" with multiple types of
management applications.

4.2.2. BAS Deployment Model

An example BAS for medium or large buildings is shown in Figure 2.
The physical layout spans multiple floors, and there is a monitoring
room where the BAS management entities are located. Each floor will
have one or more LCs depending upon the number of devices connected
to the field network.

```
       +----------------------------------------------------+
       |                                          Floor 3   |
       |      +----LC~~~~+~~~~~+~~~~~+                       |
       |      |         |     |     |                       |
       |      |        Dev   Dev   Dev                      |
       |      |                                             |
       |---   |   -----------------------------------------|
       |      |                                   Floor 2   |
       |      +----LC~~~~+~~~~~+~~~~~+  Field Network        |
       |      |         |     |     |                       |
       |      |        Dev   Dev   Dev                      |
       |      |                                             |
       |---   |   -----------------------------------------|
       |      |                                   Floor 1   |
       |      +----LC~~~~+~~~~~+~~~~~+   +-----------------  |
       |      |         |     |     |   | Monitoring Room |  |
       |      |        Dev   Dev   Dev  |                 |  |
       |      |                         |     BMS    HMI  |  |
       |      |   Management Network     |     |      |    |  |
       |      +--------------------------------+-----+     |
       |                                 |                  |
       +----------------------------------------------------+
```
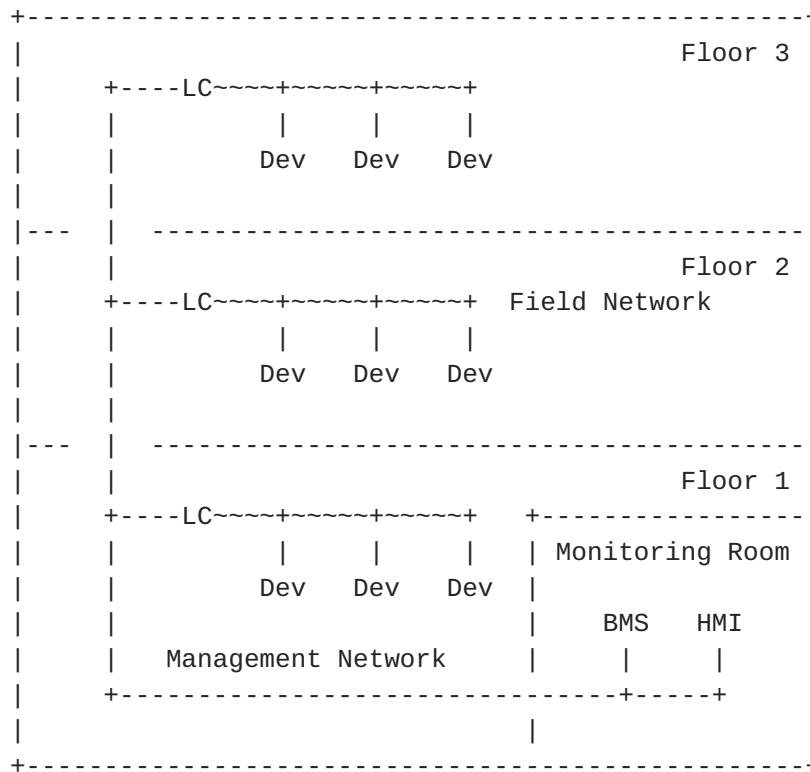
         Figure 2: BAS Deployment model for Medium/Large Buildings

   Each LC is connected to the monitoring room via the Management
   network, and the management functions are performed within the
   building. In most cases, fast Ethernet (e.g. 100BASE-T) is used for
   the management network. Since the management network is non-
   realtime, use of Ethernet without quality of service is sufficient
   for today's deployment.

   In the field network a variety of physical interfaces such as RS232C
   and RS485 are used, which have specific timing requirements. Thus if
   a field network is to be replaced with an Ethernet or wireless
   network, such networks must support time-critical deterministic
   flows.

   In Figure 3, another deployment model is presented in which the
   management system is hosted remotely. This is becoming popular for
   small office and residential buildings in which a standalone
   monitoring system is not cost-effective.

```
                                            +--------------+
                                            | Remote Center |
                                            |              |
                                            |  BMS    HMI  |
          +----------------------------------+  |  |     |   |
          |                       Floor 2 |  |   +---+---+   |
          |   +----LC~~~~+~~~~~+ Field Network|  |    |       |
          |   |         |     |            |  |  Router    |
          |   |        Dev   Dev           |  +-------|-------+
          |   |                            |          |
          |--- | ----------------------------|          |
          |   |                     Floor 1 |          |
          |   +----LC~~~~+~~~~~+            |          |
          |   |         |     |            |          |
          |   |        Dev   Dev           |          |
          |   |                            |          |
          |   |   Management Network       |    WAN   |
          |   +-----------------------Router-------------+
          |                            |
          +----------------------------------+
```
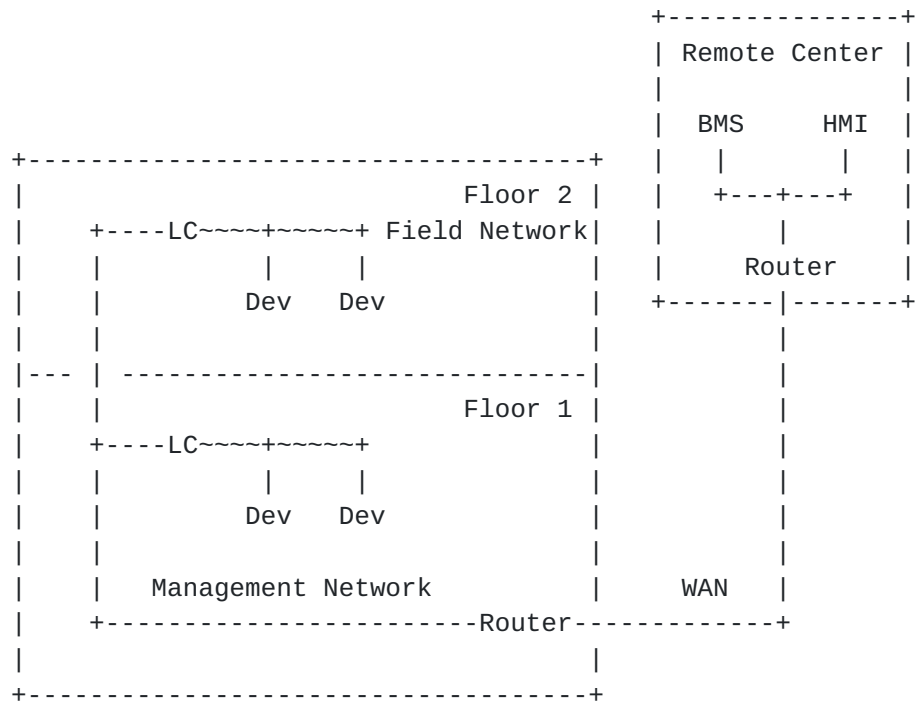
               Figure 3: Deployment model for Small Buildings

   Some interoperability is possible today in the Management Network,
   but not in today's field networks due to their non-IP-based design.

4.2.3. Use Cases for Field Networks

   Below are use cases for Environmental Monitoring, Fire Detection, and
   Feedback Control, and their implications for field network
   performance.

4.2.3.1. Environmental Monitoring

   The BMS polls each LC at a maximum measurement interval of 100ms (for
   example to draw a historical chart of 1 second granularity with a 10x
   sampling interval) and then performs the operations as specified by
   the operator. Each LC needs to measure each of its several hundred
   sensors once per measurement interval. Latency is not critical in
   this scenario as long as all sensor values are completed in the
   measurement interval. Availability is expected to be 99.999 %.

4.2.3.2. Fire Detection

   On detection of a fire, the BMS must stop the HVAC, close the fire
   shutters, turn on the fire sprinklers, send an alarm, etc. There are
   typically ~10s of sensors per LC that BMS needs to manage. In this

scenario the measurement interval is 10-50ms, the communication delay
is 10ms, and the availability must be 99.9999 %.

4.2.3.3. Feedback Control

BAS systems utilize feedback control in various ways; the most time-
critial is control of DC motors, which require a short feedback
interval (1-5ms) with low communication delay (10ms) and jitter
(1ms). The feedback interval depends on the characteristics of the
device and a target quality of control value. There are typically
~10s of such devices per LC.

Communication delay is expected to be less than 10 ms, jitter less
than 1 sec while the availability must be 99.9999% .

4.2.4. Security Considerations

When BAS field networks were developed it was assumed that the field
networks would always be physically isolated from external networks
and therefore security was not a concern. In today's world many BASs
are managed remotely and are thus connected to shared IP networks and
so security is definitely a concern, yet security features are not
available in the majority of BAS field network deployments .

The management network, being an IP-based network, has the protocols
available to enable network security, but in practice many BAS
systems do not implement even the available security features such as
device authentication or encryption for data in transit.

4.3. BAS Future

In the future we expect more fine-grained environmental monitoring
and lower energy consumption, which will require more sensors and
devices, thus requiring larger and more complex building networks.

We expect building networks to be connected to or converged with
other networks (Enterprise network, Home network, and Internet).

Therefore better facilities for network management, control,
reliability and security are critical in order to improve resident
and operator convenience and comfort. For example the ability to
monitor and control building devices via the internet would enable
(for example) control of room lights or HVAC from a resident's
desktop PC or phone application.

4.4. **BAS Asks**

   The community would like to see an interoperable protocol
   specification that can satisfy the timing, security, availability and
   QoS constraints described above, such that the resulting converged
   network can replace the disparate field networks. Ideally this
   connectivity could extend to the open Internet.

   This would imply an architecture that can guarantee

   o Low communication delays (from <10ms to 100ms in a network of
      several hundred devices)

   o Low jitter (< 1 ms)

   o Tight feedback intervals (1ms - 10ms)

   o High network availability (up to 99.9999%)

   o Availability of network data in disaster scenario

   o Authentication between management and field devices (both local
      and remote)

   o Integrity and data origin authentication of communication data
      between field and management devices

   o Confidentiality of data when communicated to a remote device

5. **Wireless for Industrial**

5.1. **Use Case Description**

   Wireless networks are useful for industrial applications, for example
   when portable, fast-moving or rotating objects are involved, and for
   the resource-constrained devices found in the Internet of Things
   (IoT).

   Such network-connected sensors, actuators, control loops (etc.)
   typically require that the underlying network support real-time
   quality of service (QoS), as well as specific classes of other
   network properties such as reliability, redundancy, and security.

   These networks may also contain very large numbers of devices, for
   example for factories, "big data" acquisition, and the IoT. Given
   the large numbers of devices installed, and the potential
   pervasiveness of the IoT, this is a huge and very cost-sensitive

market. For example, a 1% cost reduction in some areas could save
$100B

5.1.1. Network Convergence using 6TiSCH

Some wireless network technologies support real-time QoS, and are
thus useful for these kinds of networks, but others do not. For
example WiFi is pervasive but does not provide guaranteed timing or
delivery of packets, and thus is not useful in this context.

In this use case we focus on one specific wireless network technology
which does provide the required deterministic QoS, which is "IPv6
over the TSCH mode of IEEE 802.15.4e" (6TiSCH, where TSCH stands for
"Time-Slotted Channel Hopping", see [I-D.ietf-6tisch-architecture],
[IEEE802154], [IEEE802154e], and [RFC7554]).

There are other deterministic wireless busses and networks available
today, however they are imcompatible with each other, and
incompatible with IP traffic (for example [ISA100], [WirelessHART]).

Thus the primary goal of this use case is to apply 6TiSH as a
converged IP- and standards-based wireless network for industrial
applications, i.e. to replace multiple proprietary and/or
incompatible wireless networking and wireless network management
standards.

5.1.2. Common Protocol Development for 6TiSCH

Today there are a number of protocols required by 6TiSCH which are
still in development, and a second intent of this use case is to
highlight the ways in which these "missing" protocols share goals in
common with DetNet. Thus it is possible that some of the protocol
technology developed for DetNet will also be applicable to 6TiSCH.

These protocol goals are identified here, along with their
relationship to DetNet. It is likely that ultimately the resulting
protocols will not be identical, but will share design principles
which contribute to the eficiency of enabling both DetNet and 6TiSCH.

One such commonality is that although at a different time scale, in
both TSN [IEEE802.1TSNTG] and TSCH a packet crosses the network from
node to node follows a precise schedule, as a train that leaves
intermediate stations at precise times along its path. This kind of
operation reduces collisions, saves energy, and enables engineering
the network for deterministic properties.

Another commonality is remote monitoring and scheduling management of
a TSCH network by a Path Computation Element (PCE) and Network

Management Entity (NME). The PCE/NME manage timeslots and device
resources in a manner that minimizes the interaction with and the
load placed on resource-constrained devices. For example, a tiny IoT
device may have just enough buffers to store one or a few IPv6
packets, and will have limited bandwidth between peers such that it
can maintain only a small amount of peer information, and will not be
able to store many packets waiting to be forwarded. It is
advantageous then for it to only be required to carry out the
specific behavior assigned to it by the PCE/NME (as opposed to
maintaining its own IP stack, for example).

6TiSCH depends on [PCE] and [I-D.finn-detnet-architecture], and we
expect that DetNet will maintain consistency with [IEEE802.1TSNTG].

5.2. Wireless Industrial Today

Today industrial wireless is accomplished using multiple
deterministic wireless networks which are incompatible with each
other and with IP traffic.

6TiSCH is not yet fully specified, so it cannot be used in today's
applications.

5.3. Wireless Industrial Future

5.3.1. Unified Wireless Network and Management

We expect DetNet and 6TiSCH together to enable converged transport of
deterministic and best-effort traffic flows between real-time
industrial devices and wide area networks via IP routing. A high
level view of a basic such network is shown in Figure 4.
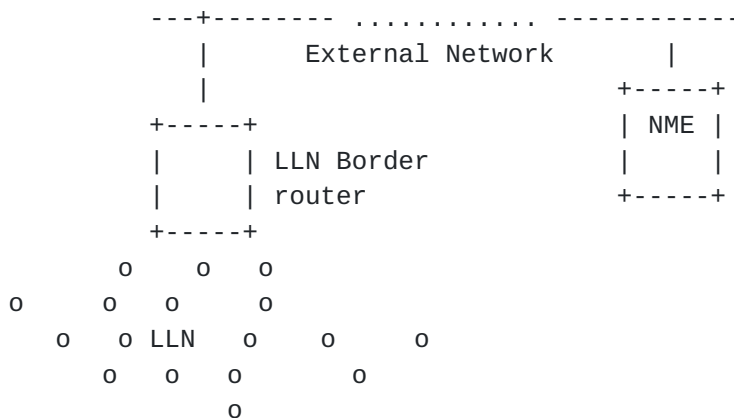
```
            ---+-------- ............ ------------
               |        External Network       |
               |                          +-----+
           +-----+                        | NME |
           |     | LLN Border             |     |
           |     | router                 +-----+
           +-----+
          o    o   o
     o     o   o     o
       o   o LLN   o    o      o
         o  o  o        o
               o


              Figure 4: Basic 6TiSCH Network
```

Figure 5 shows a backbone router federating multiple synchronized
6TiSCH subnets into a single subnet connected to the external
network.

```
                ---+-------- ............ ------------
                   |       External Network      |
                   |                       +-----+
                   |            +-----+     | NME |
              +-----+           |  +-----+  |     |
              |     | Router    |  | PCE |  +-----+
              |     |           +--|     |
              +-----+              +-----+
                  |                   |
                  | Subnet Backbone   |
              +--------------------+------------------+
              |                    |                  |
            +-----+             +-----+            +-----+
            |     | Backbone    |     | Backbone   |     | Backbone
        o   |     | router      |     | router     |     | router
            +-----+             +-----+            +-----+
          o                 o                  o              o   o
            o    o   o         o   o  o   o         o  o   o    o
        o              o           o  LLN     o        o        o   o
           o   o   o        o        o o     o  o   o   o   o      o
```
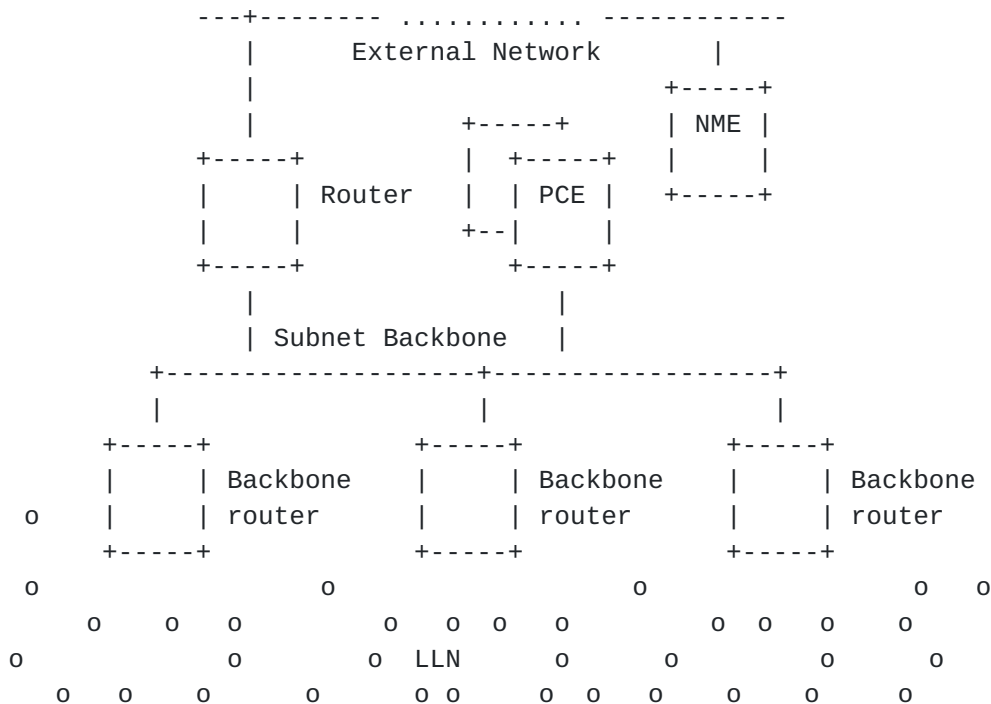
                    Figure 5: Extended 6TiSCH Network

The backbone router must ensure end-to-end deterministic behavior
between the LLN and the backbone. We would like to see this
accomplished in conformance with the work done in
[I-D.finn-detnet-architecture] with respect to Layer-3 aspects of
deterministic networks that span multiple Layer-2 domains.

The PCE must compute a deterministic path end-to-end across the TSCH
network and IEEE802.1 TSN Ethernet backbone, and DetNet protocols are
expected to enable end-to-end deterministic forwarding.

```
                      +-----+
                      | IoT |
                      | G/W |
                      +-----+
                        ^  <---- Elimination
                        | |
         Track branch   | |
                +-------+ +--------+ Subnet Backbone
                |                 |
           +--|--+           +--|--+
           |  |  | Backbone   |  |  | Backbone
      o    |  |  | router     |  |  | router
           +--/--+           +--|--+
       o    /    o      o---o----/       o
          o    o---o--/   o      o   o  o   o
      o     \  /    o               o   LLN    o
         o   v  <---- Replication
            o
```
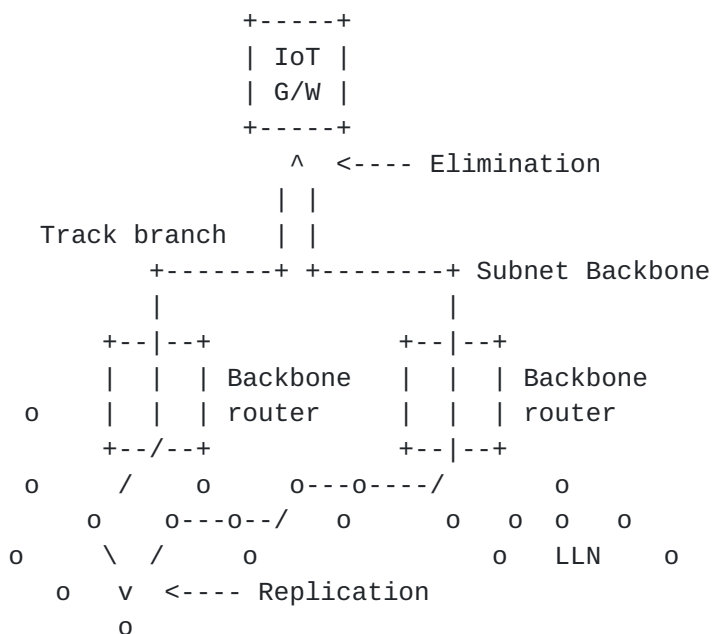
                     Figure 6: 6TiSCH Network with PRE

5.3.1.1. **PCE and 6TiSCH ARQ Retries**

   6TiSCH uses the IEEE802.15.4 Automatic Repeat-reQuest (ARQ) mechanism
   to provide higher reliability of packet delivery. ARQ is related to
   packet replication and elimination because there are two independent
   paths for packets to arrive at the destination, and if an expected
   packed does not arrive on one path then it checks for the packet on
   the second path.

   Although to date this mechanism is only used by wireless networks,
   this may be a technique that would be appropriate for DetNet and so
   aspects of the enabling protocol could be co-developed.

   For example, in Figure 6, a Track is laid out from a field device in
   a 6TiSCH network to an IoT gateway that is located on a IEEE802.1 TSN
   backbone.

   The Replication function in the field device sends a copy of each
   packet over two different branches, and the PCE schedules each hop of
   both branches so that the two copies arrive in due time at the
   gateway. In case of a loss on one branch, hopefully the other copy
   of the packet still arrives within the allocated time. If two copies
   make it to the IoT gateway, the Elimination function in the gateway
   ignores the extra packet and presents only one copy to upper layers.

At each 6TiSCH hop along the Track, the PCE may schedule more than
one timeSlot for a packet, so as to support Layer-2 retries (ARQ).

In current deployments, a TSCH Track does not necessarily support PRE
but is systematically multi-path. This means that a Track is
scheduled so as to ensure that each hop has at least two forwarding
solutions, and the forwarding decision is to try the preferred one
and use the other in case of Layer-2 transmission failure as detected
by ARQ.

5.3.2. Schedule Management by a PCE

A common feature of 6TiSCH and DetNet is the action of a PCE to
configure paths through the network. Specifically, what is needed is
a protocol and data model that the PCE will use to get/set the
relevant configuration from/to the devices, as well as perform
operations on the devices. We expect that this protocol will be
developed by DetNet with consideration for its reuse by 6TiSCH. The
remainder of this section provides a bit more context from the 6TiSCH
side.

5.3.2.1. PCE Commands and 6TiSCH CoAP Requests

The 6TiSCH device does not expect to place the request for bandwidth
between itself and another device in the network. Rather, an
operation control system invoked through a human interface specifies
the required traffic specification and the end nodes (in terms of
latency and reliability). Based on this information, the PCE must
compute a path between the end nodes and provision the network with
per-flow state that describes the per-hop operation for a given
packet, the corresponding timeslots, and the flow identification that
enables recognizing that a certain packet belongs to a certain path,
etc.

For a static configuration that serves a certain purpose for a long
period of time, it is expected that a node will be provisioned in one
shot with a full schedule, which incorporates the aggregation of its
behavior for multiple paths. 6TiSCH expects that the programing of
the schedule will be done over COAP as discussed in
[I-D.ietf-6tisch-coap].

6TiSCH expects that the PCE commands will be issued directly as CoAP
requests or be mapped back and forth into CoAP by a gateway function
at the edge of the 6TiSCH network. For instance, it is possible that
a mapping entity on the backbone transforms a non-CoAP protocol such
as PCEP into the RESTful interfaces that the 6TiSCH devices support.
This architecture will be refined to comply with DetNet
[I-D.finn-detnet-architecture] when the work is formalized. Related

information about 6TiSCH can be found at
[I-D.ietf-6tisch-6top-interface] and RPL [RFC6550].

If it appears that a path through the network does not perform as
expected, a protocol may be used to update the state in the devices,
but in 6TiSCH that flow was not designed and no protocol was selected
and it is expected that DetNet will determine the appropriate end-to-
end protocols to be used in that case.

A "slotFrame" is the base object that the PCE needs to manipulate to
program a schedule into an LLN node ([I-D.ietf-6tisch-architecture]).

The PCE should be able to read energy data from devices, and compute
paths that will implement policies on how energy in devices is
consumed, for instance to ensure that the spent energy does not
exceeded the available energy over a period of time.

6TiSCH devices can discover their neighbors over the radio using a
mechanism such as beacons, but even though the neighbor information
is available in the 6TiSCH interface data model, 6TiSCH does not
describe a protocol to proactively push the neighborhood information
to a PCE. DetNet should define this protocol, and it and should
operate over CoAP. The protocol should be able to carry multiple
metrics, in particular the same metrics as used for RPL operations
[RFC6551]

5.3.2.2. 6TiSCH IP Interface

"6top" ([I-D.wang-6tisch-6top-sublayer]) is a logical link control
sitting between the IP layer and the TSCH MAC layer which provides
the link abstraction that is required for IP operations. The 6top
data model and management interfaces are further discussed in
[I-D.ietf-6tisch-6top-interface] and [I-D.ietf-6tisch-coap].

An IP packet that is sent along a 6TiSCH path uses the Differentiated
Services Per-Hop-Behavior Group called Deterministic Forwarding, as
described in [I-D.svshah-tsvwg-deterministic-forwarding].

5.3.3. 6TiSCH Security Considerations

On top of the classical requirements for protection of control
signaling, it must be noted that 6TiSCH networks operate on limited
resources that can be depleted rapidly in a DoS attack on the system,
for instance by placing a rogue device in the network, or by
obtaining management control and setting up unexpected additional
paths.

5.4. Wireless Industrial Asks

   6TiSCH depends on DetNet to define:

   o Configuration (state) and operations for deterministic paths

   o End-to-end protocols for deterministic forwarding (tagging, IP)

   o Protocol for packet replication and elimination

   o Protocol for packet automatic retries (ARQ) (specific to wireless)

6. Cellular Radio Use Cases

6.1. Use Case Description

   This use case describes the application of deterministic networking
   in the context of cellular telecom transport networks. Important
   elements include time synchronization, clock distribution, and ways
   of establishing time-sensitive streams for both Layer-2 and Layer-3
   user plane traffic.

6.1.1. Network Architecture

   Figure 7 illustrates a typical 3GPP-defined cellular network
   architecture, which includes "Fronthaul" and "Midhaul" network
   segments. The "Fronthaul" is the network connecting base stations
   (baseband processing units) to the remote radio heads (antennas).
   The "Midhaul" is the network inter-connecting base stations (or small
   cell sites).

   In Figure 7 "eNB" ("E-UTRAN Node B") is the hardware that is
   connected to the mobile phone network which communicates directly
   with mobile handsets ([TS36300]).

```
            Y (remote radio heads (antennas))
             \
        Y__   \.--.                      .--.         +------+
           \_(      `.        +---+     _(Back`.      | 3GPP |
    Y------( Front  )----|eNB|----(  Haul  )----| core |
        ( ` .Haul )    +---+   ( `  .  )  )    | netw |
       /`--(___.-'       \        `--(___.-'    +------+
     Y_/      /            \.--.            \
         Y_/               _( Mid`.         \
                          (   Haul )        \
                          ( `  .  )  )        \
                           `--(___.-'\_____+---+    (small cell sites)
                              \           |SCe|__Y
                          +---+        +---+
                       Y__|eNB|__Y
                          +---+
                         Y_/   \_Y ("local" radios)
```
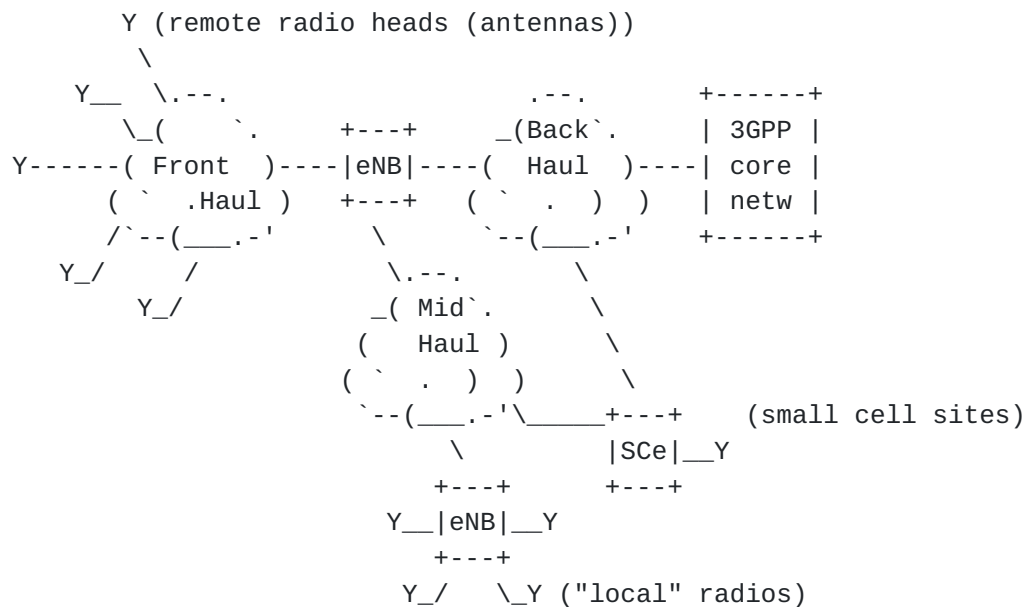
                Figure 7: Generic 3GPP-based Cellular Network Architecture

   The available processing time for Fronthaul networking overhead is
   limited to the available time after the baseband processing of the
   radio frame has completed. For example in Long Term Evolution (LTE)
   radio, processing of a radio frame is allocated 3ms, but typically
   the processing completes much earlier (<400us) allowing the remaining
   time to be used by the Fronthaul network. This ultimately determines
   the distance the remote radio heads can be located from the base
   stations (200us equals roughly 40 km of optical fiber-based
   transport, thus round trip time is 2*200us = 400us).

   The remainder of the "maximum delay budget" is consumed by all nodes
   and buffering between the remote radio head and the baseband
   processing, plus the distance-incurred delay.

   The baseband processing time and the available "delay budget" for the
   fronthaul is likely to change in the forthcoming "5G" due to reduced
   radio round trip times and other architectural and service
   requirements [NGMN].

6.1.2. Time Synchronization Requirements

   Fronthaul time synchronization requirements are given by [TS25104],
   [TS36104], [TS36211], and [TS36133]. These can be summarized for the
   current 3GPP LTE-based networks as:

   Delay Accuracy:
      +-8ns (i.e. +-1/32 Tc, where Tc is the UMTS Chip time of 1/3.84
      MHz) resulting in a round trip accuracy of +-16ns. The value is

this low to meet the 3GPP Timing Alignment Error (TAE) measurement
requirements.

Packet Delay Variation:
   Packet Delay Variation (PDV aka Jitter aka Timing Alignment Error)
   is problematic to Fronthaul networks and must be minimized. If
   the transport network cannot guarantee low enough PDV then
   additional buffering has to be introduced at the edges of the
   network to buffer out the jitter. Buffering is not desirable as
   it reduces the total available delay budget.

   * For multiple input multiple output (MIMO) or TX diversity
      transmissions, at each carrier frequency, TAE shall not exceed
      65 ns (i.e. 1/4 Tc).

   * For intra-band contiguous carrier aggregation, with or without
      MIMO or TX diversity, TAE shall not exceed 130 ns (i.e. 1/2
      Tc).

   * For intra-band non-contiguous carrier aggregation, with or
      without MIMO or TX diversity, TAE shall not exceed 260 ns (i.e.
      one Tc).

   * For inter-band carrier aggregation, with or without MIMO or TX
      diversity, TAE shall not exceed 260 ns.

Transport link contribution to radio frequency error:
   +-2 PPB. This value is considered to be "available" for the
   Fronthaul link out of the total 50 PPB budget reserved for the
   radio interface. Note: the reason that the transport link
   contributes to radio frequency error is as follows. The current
   way of doing Fronthaul is from the radio unit to remote radio head
   directly. The remote radio head is essentially a passive device
   (without buffering etc.) The transport drives the antenna
   directly by feeding it with samples and everything the transport
   adds will be introduced to radio as-is. So if the transport
   causes additional frequence error that shows immediately on the
   radio as well.

The above listed time synchronization requirements are difficult to
meet with point-to-point connected networks, and more difficult when
the network includes multiple hops. It is expected that networks
must include buffering at the ends of the connections as imposed by
the jitter requirements, since trying to meet the jitter requirements
in every intermediate node is likely to be too costly. However,

every measure to reduce jitter and delay on the path makes it easier
to meet the end-to-end requirements.

In order to meet the timing requirements both senders and receivers
must remain time synchronized, demanding very accurate clock
distribution, for example support for IEEE 1588 transparent clocks in
every intermediate node.

In cellular networks from the LTE radio era onward, phase
synchronization is needed in addition to frequency synchronization
([TS36300], [TS23401]).

6.1.3. Time-Sensitive Stream Requirements

In addition to the time synchronization requirements listed in
Section Section 6.1.2 the Fronthaul networks assume practically
error-free transport. The maximum bit error rate (BER) has been
defined to be 10^{-12}. When packetized that would imply a packet
error rate (PER) of $2.4*10^{-9}$ (assuming ~300 bytes packets).
Retransmitting lost packets and/or using forward error correction
(FEC) to circumvent bit errors is practically impossible due to the
additional delay incurred. Using redundant streams for better
guarantees for delivery is also practically impossible in many cases
due to high bandwidth requirements of Fronthaul networks. For
instance, current uncompressed CPRI bandwidth expansion ratio is
roughly 20:1 compared to the IP layer user payload it carries.
Protection switching is also a candidate but current technologies for
the path switch are too slow. We do not currently know of a better
solution for this issue.

Fronthaul links are assumed to be symmetric, and all Fronthaul
streams (i.e. those carrying radio data) have equal priority and
cannot delay or pre-empt each other. This implies that the network
must guarantee that each time-sensitive flow meets their schedule.

6.1.4. Security Considerations

Establishing time-sensitive streams in the network entails reserving
networking resources for long periods of time. It is important that
these reservation requests be authenticated to prevent malicious
reservation attempts from hostile nodes (or accidental
misconfiguration). This is particularly important in the case where
the reservation requests span administrative domains. Furthermore,
the reservation information itself should be digitally signed to
reduce the risk of a legitimate node pushing a stale or hostile
configuration into another networking node.

6.2. Cellular Radio Networks Today

Today's Fronthaul networks typically consist of:

o Dedicated point-to-point fiber connection is common

o Proprietary protocols and framings

o Custom equipment and no real networking

Today's Midhaul and Backhaul networks typically consist of:

o Mostly normal IP networks, MPLS-TP, etc.

o Clock distribution and sync using 1588 and SyncE

Telecommunication networks in the cellular domain are already heading
towards transport networks where precise time synchronization support
is one of the basic building blocks. While the transport networks
themselves have practically transitioned to all-IP packet based
networks to meet the bandwidth and cost requirements, highly accurate
clock distribution has become a challenge.

Transport networks in the cellular domain are typically based on Time
Division Multiplexing (TDM-based) and provide frequency
synchronization capabilities as a part of the transport media.
Alternatively other technologies such as Global Positioning System
(GPS) or Synchronous Ethernet (SyncE) are used [SyncE].

Both Ethernet and IP/MPLS [RFC3031] (and PseudoWires (PWE) [RFC3985]
for legacy transport support) have become popular tools to build and
manage new all-IP Radio Access Networks (RAN)
[I-D.kh-spring-ip-ran-use-case]. Although various timing and
synchronization optimizations have already been proposed and
implemented including 1588 PTP enhancements
[I-D.ietf-tictoc-1588overmpls][I-D.mirsky-mpls-residence-time], these
solution are not necessarily sufficient for the forthcoming RAN
architectures or guarantee the higher time-synchronization
requirements [CPRI]. There are also existing solutions for the TDM
over IP [RFC5087] [RFC4553] or Ethernet transports [RFC5086].

6.3. Cellular Radio Networks Future

We would like to see the following in future Cellular Radio networks:

o Unified standards-based transport protocols and standard
   networking equipment that can make use of underlying deterministic
   link-layer services

o Unified and standards-based network management systems and
   protocols in all parts of the network (including Fronthaul)

New radio access network deployment models and architectures may
require time sensitive networking services with strict requirements
on other parts of the network that previously were not considered to
be packetized at all. The time and synchronization support are
already topical for Backhaul and Midhaul packet networks [MEF], and
becoming a real issue for Fronthaul networks. Specifically in the
Fronthaul networks the timing and synchronization requirements can be
extreme for packet based technologies, for example, on the order of
sub +-20 ns packet delay variation (PDV) and frequency accuracy of
+0.002 PPM [Fronthaul].

The actual transport protocols and/or solutions to establish required
transport "circuits" (pinned-down paths) for Fronthaul traffic are
still undefined. Those are likely to include (but are not limited
to) solutions directly over Ethernet, over IP, and MPLS/PseudoWire
transport.

Even the current time-sensitive networking features may not be
sufficient for Fronthaul traffic. Therefore, having specific
profiles that take the requirements of Fronthaul into account is
desirable [IEEE8021CM].

The really interesting and important existing work for time sensitive
networking has been done for Ethernet [TSNTG], which specifies the
use of IEEE 1588 time precision protocol (PTP) [IEEE1588] in the
context of IEEE 802.1D and IEEE 802.1Q. While IEEE 802.1AS
[IEEE8021AS] specifies a Layer-2 time synchronizing service other
specification, such as IEEE 1722 [IEEE1722] specify Ethernet-based
Layer-2 transport for time-sensitive streams. New promising work
seeks to enable the transport of time-sensitive fronthaul streams in
Ethernet bridged networks [IEEE8021CM]. Similarly to IEEE 1722 there
is an ongoing standardization effort to define Layer-2 transport
encapsulation format for transporting radio over Ethernet (RoE) in
IEEE 1904.3 Task Force [IEEE19043].

All-IP RANs and various "haul" networks would benefit from time
synchronization and time-sensitive transport services. Although
Ethernet appears to be the unifying technology for the transport
there is still a disconnect providing Layer-3 services. The protocol
stack typically has a number of layers below the Ethernet Layer-2
that shows up to the Layer-3 IP transport. It is not uncommon that
on top of the lowest layer (optical) transport there is the first
layer of Ethernet followed one or more layers of MPLS, PseudoWires
and/or other tunneling protocols finally carrying the Ethernet layer
visible to the user plane IP traffic. While there are existing

technologies, especially in MPLS/PWE space, to establish circuits
through the routed and switched networks, there is a lack of
signaling the time synchronization and time-sensitive stream
requirements/reservations for Layer-3 flows in a way that the entire
transport stack is addressed and the Ethernet layers that needs to be
configured are addressed.

Furthermore, not all "user plane" traffic will be IP. Therefore, the
same solution also must address the use cases where the user plane
traffic is again another layer or Ethernet frames. There is existing
work describing the problem statement
[I-D.finn-detnet-problem-statement] and the architecture
[I-D.finn-detnet-architecture] for deterministic networking (DetNet)
that targets solutions for time-sensitive (IP/transport) streams with
deterministic properties over Ethernet-based switched networks.

6.4. Cellular Radio Networks Asks

A standard for data plane transport specification which is:

o Unified among all *hauls

o Deployed in a highly deterministic network environment

A standard for data flow information models that are:

o Aware of the time sensitivity and constraints of the target
   networking environment

o Aware of underlying deterministic networking services (e.g. on the
   Ethernet layer)

Mapping the Fronthaul requirements to IETF DetNet
[I-D.finn-detnet-architecture] Section 3 "Providing the DetNet
Quality of Service", the relevant features are:

o Zero congestion loss.

o Pinned-down paths.

7. Cellular Coordinated Multipoint Processing (CoMP)

7.1. Use Case Description

In cellular wireless communication systems, Inter-Site Coordinated
Multipoint Processing (CoMP, see [CoMP]) is a technique implemented
within a cell site which improves system efficiency and user quality
experience by significantly improving throughput in the cell-edge

region (i.e. at the edges of that cell site's radio coverage area).
CoMP techniques depend on deterministic high-reliability
communication between cell sites, however such connections today are
IP-based which in current mobile networks can not meet the QoS
requirements, so CoMP is an emerging technology which can benefit
from DetNet.

Here we consider the JT (Joint Transmit) application for CoMP, which
provides the highest performance gain (compared to other
applications).

7.1.1. CoMP Architecture

```
                    +---------------------------+
                    |           CoMP            |
                    +--+--------------------+--+
                       |                    |
                 +----------+         +------------+
                 |  Uplink  |         |  Downlink  |
                 +-----+----+         +--------+---+
                       |                       |
              -------------------      -----------------------
              |        |        |      |         |          |
         +---------+ +----+  +-----+   +------------+ +-----+  +-----+
         |  Joint  | | CS |  | DPS |   |   Joint    | | CS/ |  | DPS |
         |Reception| |    |  |     |   |Transmission| | CB  |  |     |
         +---------+ +----+  +-----+   +------------+ +-----+  +-----+
              |                             |
              |-----------                  |-------------
              |          |                  |             |
         +------------+  +---------+    +----------+   +------------+
         |   Joint    |  |  Soft   |    | Coherent |   |    Non-    |
         |Equalization|  |Combining|    |    JT    |   | Coherent JT|
         +------------+  +---------+    +----------+   +------------+
```
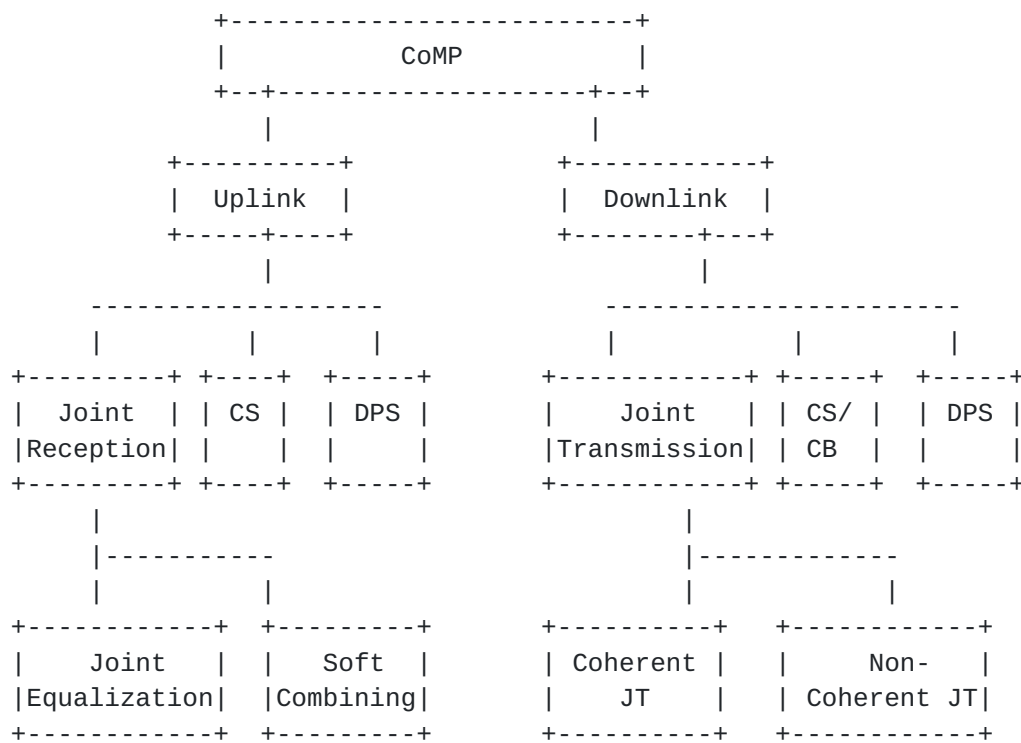
Figure 8: Framework of CoMP Technology

As shown in Figure 8, CoMP reception and transmission is a framework
in which multiple geographically distributed antenna nodes cooperate
to improve the performance of the users served in the common
cooperation area. The design principal of CoMP is to extend the
current single-cell to multi-UE (User Equipment) transmission to a
multi-cell- to-multi-UEs transmission by base station cooperation.

7.1.2. Delay Sensitivity in CoMP

   In contrast to the single-cell scenario, CoMP has delay-sensitive
   performance parameters, which are "backhaul latency" and "CSI
   (Channel State Information) reporting and accuracy". The essential
   feature of CoMP is signaling between eNBs, so the backhaul latency is
   the dominating limitation of the CoMP performance. Generally, JT can
   benefit from coordinated scheduling (either distributed or
   centralized) of different cells if the signaling delay between eNBs
   is within 4-10ms. This delay requirement is both rigid and absolute
   because any uncertainty in delay will degrade the performance
   significantly.

7.2. CoMP Today

   Due to the strict sensitivity to latency and synchronization, CoMP
   between eNB has not been deployed yet. This is because the current
   interface path between eNBs cannot meet the delay bound because it is
   usually IP-based and passing through multiple network hops (this
   interface is called "X2" or "eX2" for "enhanced X2"). Today lack of
   absolute delay guarantee on X2/eX2 traffic is the main obstacle to JT
   and multi-eNB coordination.

   There is still lack of Layer-3 (IP) transport protocol and signaling
   that is capable of low latency services; current techniques such as
   MPLS and PWE focus on establishing circuits using pre-routed paths
   but there is no such signaling for reservation of time-sensitive
   stream.

7.3. CoMP Future

7.3.1. Mobile Industry Overall Goals

   [METIS] documents the fundamental challenges as well as overall
   technical goals of the 5G mobile and wireless system as the starting
   point. These future systems should support (at similar cost and
   energy consumption levels as today's system):

   o 1000 times higher mobile data volume per area

   o 10 times to 100 times higher typical user data rate

   o 10 times to 100 times higher number of connected devices

   o 10 times longer battery life for low power devices

   o 5 times reduced End-to-End (E2E) latency

The current LTE networking system has E2E latency less than 20ms
[LTE-Latency] which leads to around 5ms E2E latency for 5G networks.
To fulfill these latency demands at similar cost will be challenging
because as the system also requires 100x bandwidth and 100x connected
devices, simply adding redundant bandwidth provisioning can no longer
be an efficient solution.

In addition to bandwidth provisioning, reserved critical flows should
not be affected by other flows no matter the pressure of the network.
Deterministic networking techniques in both layer-2 and layer-3 using
IETF protocol solutions can be promising to serve these scenarios.

7.3.2. CoMP Infrastructure Goals

Inter-site CoMP is one of the key requirements for 5G and is also a
near-term goal for the current 4.5G network architecture. Assuming
network architecture remains unchanged (i.e. no Fronthaul network and
data flow between eNB is via X2/eX2) we would like to see the
following in the near future:

o Unified protocols and delay-guaranteed forwarding network
   equipment that is capable of delivering deterministic latency
   services.

o Unified management and protocols which take delay and timing into
   account.

o Unified deterministic latency data model and signaling for
   resource reservation.

7.4. CoMP Asks

To fully utilize the power of CoMP, it requires:

o Very tight absolute delay bound (100-500us) within 7-10 hops.

o Standardized data plane with highly deterministic networking
   capability.

o Standardized control plane to unify backhaul network elements with
   time-sensitive stream reservation signaling.

In addition, a standardized deterministic latency data flow model
that includes:

o Network-aware constraints on the networking environment

o Time-aware description of flow characteristics and network
   resources, which may not need to be bandwidth based

o Application-aware description of deterministic latency services.

8. Industrial M2M

8.1. Use Case Description

Industrial Automation in general refers to automation of
manufacturing, quality control and material processing. In this
"machine to machine" (M2M) use case we consider machine units in a
plant floor which periodically exchange data with upstream or
downstream machine modules and/or a supervisory controller within a
local area network.

The actors of M2M communication are Programmable Logic Controllers
(PLCs). Communication between PLCs and between PLCs and the
supervisory PLC (S-PLC) is achieved via critical control/data streams
Figure 9.

```
         S (Sensor)
          \                                      +-----+
   PLC__   \.--.                        .--.   ---| MES |
       \_(     `.                     _(     `./    +-----+
   A------( Local  )-------------(   L2    )
         (     Net )             (     Net )   +-------+
        /`--(___.-'               `--(___.-' ----| S-PLC |
      S_/     /       PLC    .--. /          +-------+
        A_/            \_(     `.
     (Actuator)       (  Local )
                      (     Net )
                     /`--(___.-'\
                    /       \   A
                  S         A
```

            Figure 9: Current Generic Industrial M2M Network Architecture

This use case focuses on PLC-related communications; communication to
Manufacturing-Execution-Systems (MESs) are not addressed.

This use case covers only critical control/data streams; non-critical
traffic between industrial automation applications (such as
communication of state, configuration, set-up, and database
communication) are adequately served by currently available
prioritizing techniques. Such traffic can use up to 80% of the total

bandwidth required. There is also a subset of non-time-critical
traffic that must be reliable even though it is not time sensitive.

In this use case the primary need for deterministic networking is to
provide end-to-end delivery of M2M messages within specific timing
constraints, for example in closed loop automation control. Today
this level of determinism is provided by proprietary networking
technologies. In addition, standard networking technologies are used
to connect the local network to remote industrial automation sites,
e.g. over an enterprise or metro network which also carries other
types of traffic. Therefore, flows that should be forwarded with
deterministic guarantees need to be sustained regardless of the
amount of other flows in those networks.

8.2. Industrial M2M Communication Today

Today, proprietary networks fulfill the needed timing and
availability for M2M networks.

The network topologies used today by industrial automation are
similar to those used by telecom networks: Daisy Chain, Ring, Hub and
Spoke, and Comb (a subset of Daisy Chain).

PLC-related control/data streams are transmitted periodically and
carry either a pre-configured payload or a payload configured during
runtime.

Some industrial applications require time synchronization at the end
nodes. For such time-coordinated PLCs, accuracy of 1 microsecond is
required. Even in the case of "non-time-coordinated" PLCs time sync
may be needed e.g. for timestamping of sensor data.

Industrial network scenarios require advanced security solutions.
Many of the current industrial production networks are physically
separated. Preventing critical flows from be leaked outside a domain
is handled today by filtering policies that are typically enforced in
firewalls.

8.2.1. Transport Parameters

The Cycle Time defines the frequency of message(s) between industrial
actors. The Cycle Time is application dependent, in the range of 1ms
- 100ms for critical control/data streams.

Because industrial applications assume deterministic transport for
critical Control-Data-Stream parameters (instead of defining latency
and delay variation parameters) it is sufficient to fulfill the upper
bound of latency (maximum latency). The underlying networking

infrastructure must ensure a maximum end-to-end delivery time of
messages in the range of 100 microseconds to 50 milliseconds
depending on the control loop application.

The bandwidth requirements of control/data streams are usually
calculated directly from the bytes-per-cycle parameter of the control
loop. For PLC-to-PLC communication one can expect 2 - 32 streams
with packet size in the range of 100 - 700 bytes. For S-PLC to PLCs
the number of streams is higher - up to 256 streams. Usually no more
than 20% of available bandwidth is used for critical control/data
streams. In today's networks 1Gbps links are commonly used.

Most PLC control loops are rather tolerant of packet loss, however
critical control/data streams accept no more than 1 packet loss per
consecutive communication cycle (i.e. if a packet gets lost in cycle
"n", then the next cycle ("n+1") must be lossless). After two or
more consecutive packet losses the network may be considered to be
"down" by the Application.

As network downtime may impact the whole production system the
required network availability is rather high (99,999%).

Based on the above parameters we expect that some form of redundancy
will be required for M2M communications, however any individual
solution depends on several parameters including cycle time, delivery
time, etc.

8.2.2. Stream Creation and Destruction

In an industrial environment, critical control/data streams are
created rather infrequently, on the order of ~10 times per day / week
/ month. Most of these critical control/data streams get created at
machine startup, however flexibility is also needed during runtime,
for example when adding or removing a machine. Going forward as
production systems become more flexible, we expect a significant
increase in the rate at which streams are created, changed and
destroyed.

8.3. Industrial M2M Future

We would like to see a converged IP-standards-based network with
deterministic properties that can satisfy the timing, security and
reliability constraints described above. Today's proprietary
networks could then be interfaced to such a network via gateways or,
in the case of new installations, devices could be connected directly
to the converged network.

[8.4](). **Industrial M2M Asks**

o Converged IP-based network

o Deterministic behavior (bounded latency and jitter)

o High availability (presumably through redundancy) (99.999 %)

o Low message delivery time (100us - 50ms)

o Low packet loss (burstless, 0.1-1 %)

o Precise time synchronization accuracy (1us)

o Security (e.g. prevent critical flows from being leaked between
   physically separated networks)

[9](). **Internet-based Applications**

[9.1](). **Use Case Description**

There are many applications that communicate across the open Internet
that could benefit from guaranteed delivery and bounded latency. The
following are some representative examples.

[9.1.1](). **Media Content Delivery**

Media content delivery continues to be an important use of the
Internet, yet users often experience poor quality audio and video due
to the delay and jitter inherent in today's Internet.

[9.1.2](). **Online Gaming**

Online gaming is a significant part of the gaming market, however
latency can degrade the end user experience. For example "First
Person Shooter" (FPS) games are highly delay-sensitive.

[9.1.3](). **Virtual Reality**

Virtual reality (VR) has many commercial applications including real
estate presentations, remote medical procedures, and so on. Low
latency is critical to interacting with the virtual world because
perceptual delays can cause motion sickness.

9.2. Internet-Based Applications Today

Internet service today is by definition "best effort", with no guarantees on delivery or bandwidth.

9.3. Internet-Based Applications Future

We imagine an Internet from which we will be able to play a video without glitches and play games without lag.

For online gaming, the maximum round-trip delay can be 100ms and stricter for FPS gaming which can be 10-50ms. Transport delay is the dominate part with a 5-20ms budget.

For VR, 1-10ms maximum delay is needed and total network budget is 1-5ms if doing remote VR.

Flow identification can be used for gaming and VR, i.e. it can recognize a critical flow and provide appropriate latency bounds.

9.4. Internet-Based Applications Asks

o Unified control and management protocols to handle time-critical data flow

o Application-aware flow filtering mechanism to recognize the timing critical flow without doing 5-tuple matching

o Unified control plane to provide low latency service on Layer-3 without changing the data plane

o OAM system and protocols which can help to provide E2E-delay sensitive service provisioning

10. Use Case Common Elements

Looking at the use cases collectively, the following common desires for the DetNet-based networks of the future emerge:

o Open standards-based network (replace various proprietary networks, reduce cost, create multi-vendor market)

o Centrally administered (though such administration may be distributed for scale and resiliency)

o Integrates L2 (bridged) and L3 (routed) environments (independent of the Link layer, e.g. can be used with Ethernet, 6TiSCH, etc.)

o Carries both deterministic and best-effort traffic (guaranteed
   end-to-end delivery of deterministic flows, deterministic flows
   isolated from each other and from best-effort traffic congestion,
   unused deterministic BW available to best-effort traffic)

o Ability to add or remove systems from the network with minimal,
   bounded service interruption (applications include replacement of
   failed devices as well as plug and play)

o Uses standardized data flow information models capable of
   expressing deterministic properties (models express device
   capabilities, flow properties. Protocols for pushing models from
   controller to devices, devices to controller)

o Scalable size (long distances (many km) and short distances
   (within a single machine), many hops (radio repeaters, microwave
   links, fiber links...) and short hops (single machine))

o Scalable timing parameters and accuracy (bounded latency,
   guaranteed worst case maximum, minimum. Low latency, e.g. control
   loops may be less than 1ms, but larger for wide area networks)

o High availability (99.9999 percent up time requested, but may be
   up to twelve 9s)

o Reliability, redundancy (lives at stake)

o Security (from failures, attackers, misbehaving devices -
   sensitive to both packet content and arrival time)

11. Acknowledgments

11.1. Pro Audio

This section was derived from draft-gunther-detnet-proaudio-req-01.

The editors would like to acknowledge the help of the following
individuals and the companies they represent:

Jeff Koftinoff, Meyer Sound

Jouni Korhonen, Associate Technical Director, Broadcom

Pascal Thubert, CTAO, Cisco

Kieran Tyrrell, Sienda New Media Technologies GmbH

11.2. Utility Telecom

This section was derived from [draft-wetterwald-detnet-utilities-reqs-02](#).

Faramarz Maghsoodlou, Ph. D. IoT Connected Industries and Energy Practice Cisco

Pascal Thubert, CTAO Cisco

11.3. Building Automation Systems

This section was derived from [draft-bas-usecase-detnet-00](#).

11.4. Wireless for Industrial

This section was derived from [draft-thubert-6tisch-4detnet-01](#).

This specification derives from the 6TiSCH architecture, which is the result of multiple interactions, in particular during the 6TiSCH (bi)Weekly Interim call, relayed through the 6TiSCH mailing list at the IETF.

The authors wish to thank: Kris Pister, Thomas Watteyne, Xavier Vilajosana, Qin Wang, Tom Phinney, Robert Assimiti, Michael Richardson, Zhuo Chen, Malisa Vucinic, Alfredo Grieco, Martin Turon, Dominique Barthel, Elvis Vogli, Guillaume Gaillard, Herman Storey, Maria Rita Palattella, Nicola Accettura, Patrick Wetterwald, Pouria Zand, Raghuram Sudhaakar, and Shitanshu Shah for their participation and various contributions.

11.5. Cellular Radio

This section was derived from [draft-korhonen-detnet-telreq-00](#).

11.6. Industrial M2M

The authors would like to thank Feng Chen and Marcel Kiessling for their comments and suggestions.

11.7. Internet Applications and CoMP

This section was derived from [draft-zha-detnet-use-case-00](#).

This document has benefited from reviews, suggestions, comments and proposed text provided by the following members, listed in alphabetical order: Jing Huang, Junru Lin, Lehong Niu and Oilver Huang.

12. Informative References

   [ACE]   IETF, "Authentication and Authorization for Constrained
               Environments", <https://datatracker.ietf.org/doc/charter-
               ietf-ace/>.

   [bacnetip]
               ASHRAE, "Annex J to ANSI/ASHRAE 135-1995 - BACnet/IP",
               January 1999.

   [CCAMP]   IETF, "Common Control and Measurement Plane",
               <https://datatracker.ietf.org/doc/charter-ietf-ccamp/>.

   [CoMP]   NGMN Alliance, "RAN EVOLUTION PROJECT COMP EVALUATION AND
               ENHANCEMENT", NGMN Alliance NGMN_RANEV_D3_CoMP_Evaluation_
               and_Enhancement_v2.0, March 2015,
               <https://www.ngmn.org/uploads/media/
               NGMN_RANEV_D3_CoMP_Evaluation_and_Enhancement_v2.0.pdf>.

   [CONTENT_PROTECTION]
               Olsen, D., "1722a Content Protection", 2012,
               <http://grouper.ieee.org/groups/1722/contributions/2012/
               avtp_dolsen_1722a_content_protection.pdf>.

   [CPRI]   CPRI Cooperation, "Common Public Radio Interface (CPRI);
               Interface Specification", CPRI Specification V6.1, July
               2014, <http://www.cpri.info/downloads/
               CPRI_v_6_1_2014-07-01.pdf>.

   [DCI]   Digital Cinema Initiatives, LLC, "DCI Specification,
               Version 1.2", 2012, <http://www.dcimovies.com/>.

   [DICE]   IETF, "DTLS In Constrained Environments",
               <https://datatracker.ietf.org/doc/charter-ietf-dice/>.

   [EA12]   Evans, P. and M. Annunziata, "Industrial Internet: Pushing
               the Boundaries of Minds and Machines", November 2012.

   [ESPN_DC2]
               Daley, D., "ESPN's DC2 Scales AVB Large", 2014,
               <http://sportsvideo.org/main/blog/2014/06/
               espns-dc2-scales-avb-large>.

   [flnet]   Japan Electrical Manufacturers' Association, "JEMA 1479 -
               English Edition", September 2012.

   [Fronthaul]
              Chen, D. and T. Mustala, "Ethernet Fronthaul
              Considerations", IEEE 1904.3, February 2015,
              <http://www.ieee1904.org/3/meeting_archive/2015/02/
              tf3_1502_che n_1a.pdf>.

   [HART]   www.hartcomm.org, "Highway Addressable remote Transducer,
              a group of specifications for industrial process and
              control devices administered by the HART Foundation".

   [I-D.finn-detnet-architecture]
              Finn, N., Thubert, P., and M. Teener, "Deterministic
              Networking Architecture", draft-finn-detnet-
              architecture-03 (work in progress), March 2016.

   [I-D.finn-detnet-problem-statement]
              Finn, N. and P. Thubert, "Deterministic Networking Problem
              Statement", draft-finn-detnet-problem-statement-04 (work
              in progress), October 2015.

   [I-D.ietf-6tisch-6top-interface]
              Wang, Q. and X. Vilajosana, "6TiSCH Operation Sublayer
              (6top) Interface", draft-ietf-6tisch-6top-interface-04
              (work in progress), July 2015.

   [I-D.ietf-6tisch-architecture]
              Thubert, P., "An Architecture for IPv6 over the TSCH mode
              of IEEE 802.15.4", draft-ietf-6tisch-architecture-09 (work
              in progress), November 2015.

   [I-D.ietf-6tisch-coap]
              Sudhaakar, R. and P. Zand, "6TiSCH Resource Management and
              Interaction using CoAP", draft-ietf-6tisch-coap-03 (work
              in progress), March 2015.

   [I-D.ietf-6tisch-terminology]
              Palattella, M., Thubert, P., Watteyne, T., and Q. Wang,
              "Terminology in IPv6 over the TSCH mode of IEEE
              802.15.4e", draft-ietf-6tisch-terminology-06 (work in
              progress), November 2015.

   [I-D.ietf-ipv6-multilink-subnets]
              Thaler, D. and C. Huitema, "Multi-link Subnet Support in
              IPv6", draft-ietf-ipv6-multilink-subnets-00 (work in
              progress), July 2002.

   [I-D.ietf-roll-rpl-industrial-applicability]
              Phinney, T., Thubert, P., and R. Assimiti, "RPL
              applicability in industrial networks", draft-ietf-roll-
              rpl-industrial-applicability-02 (work in progress),
              October 2013.

   [I-D.ietf-tictoc-1588overmpls]
              Davari, S., Oren, A., Bhatia, M., Roberts, P., and L.
              Montini, "Transporting Timing messages over MPLS
              Networks", draft-ietf-tictoc-1588overmpls-07 (work in
              progress), October 2015.

   [I-D.kh-spring-ip-ran-use-case]
              Khasnabish, B., hu, f., and L. Contreras, "Segment Routing
              in IP RAN use case", draft-kh-spring-ip-ran-use-case-02
              (work in progress), November 2014.

   [I-D.mirsky-mpls-residence-time]
              Mirsky, G., Ruffini, S., Gray, E., Drake, J., Bryant, S.,
              and S. Vainshtein, "Residence Time Measurement in MPLS
              network", draft-mirsky-mpls-residence-time-07 (work in
              progress), July 2015.

   [I-D.svshah-tsvwg-deterministic-forwarding]
              Shah, S. and P. Thubert, "Deterministic Forwarding PHB",
              draft-svshah-tsvwg-deterministic-forwarding-04 (work in
              progress), August 2015.

   [I-D.thubert-6lowpan-backbone-router]
              Thubert, P., "6LoWPAN Backbone Router", draft-thubert-
              6lowpan-backbone-router-03 (work in progress), February
              2013.

   [I-D.wang-6tisch-6top-sublayer]
              Wang, Q. and X. Vilajosana, "6TiSCH Operation Sublayer
              (6top)", draft-wang-6tisch-6top-sublayer-04 (work in
              progress), November 2015.

   [IEC61850-90-12]
              TC57 WG10, IEC., "IEC 61850-90-12 TR: Communication
              networks and systems for power utility automation - Part
              90-12: Wide area network engineering guidelines", 2015.

   [IEC62439-3:2012]
              TC65, IEC., "IEC 62439-3: Industrial communication
              networks - High availability automation networks - Part 3:
              Parallel Redundancy Protocol (PRP) and High-availability
              Seamless Redundancy (HSR)", 2012.

   [IEEE1588]
              IEEE, "IEEE Standard for a Precision Clock Synchronization
              Protocol for Networked Measurement and Control Systems",
              IEEE Std 1588-2008, 2008,
              <http://standards.ieee.org/findstds/
              standard/1588-2008.html>.

   [IEEE1722]
              IEEE, "1722-2011 - IEEE Standard for Layer 2 Transport
              Protocol for Time Sensitive Applications in a Bridged
              Local Area Network", IEEE Std 1722-2011, 2011,
              <http://standards.ieee.org/findstds/
              standard/1722-2011.html>.

   [IEEE19043]
              IEEE Standards Association, "IEEE 1904.3 TF", IEEE 1904.3,
              2015, <http://www.ieee1904.org/3/tf3_home.shtml>.

   [IEEE802.1TSNTG]
              IEEE Standards Association, "IEEE 802.1 Time-Sensitive
              Networks Task Group", March 2013,
              <http://www.ieee802.org/1/pages/avbridges.html>.

   [IEEE802154]
              IEEE standard for Information Technology, "IEEE std.
              802.15.4, Part. 15.4: Wireless Medium Access Control (MAC)
              and Physical Layer (PHY) Specifications for Low-Rate
              Wireless Personal Area Networks".

   [IEEE802154e]
              IEEE standard for Information Technology, "IEEE standard
              for Information Technology, IEEE std. 802.15.4, Part.
              15.4: Wireless Medium Access Control (MAC) and Physical
              Layer (PHY) Specifications for Low-Rate Wireless Personal
              Area Networks, June 2011 as amended by IEEE std.
              802.15.4e, Part. 15.4: Low-Rate Wireless Personal Area
              Networks (LR-WPANs) Amendment 1: MAC sublayer", April
              2012.

   [IEEE8021AS]
              IEEE, "Timing and Synchronizations (IEEE 802.1AS-2011)",
              IEEE 802.1AS-2001, 2011,
              <http://standards.ieee.org/getIEEE802/
              download/802.1AS-2011.pdf>.

   [IEEE8021CM]
              Farkas, J., "Time-Sensitive Networking for Fronthaul",
              Unapproved PAR, PAR for a New IEEE Standard;
              IEEE P802.1CM, April 2015,
              <http://www.ieee802.org/1/files/public/docs2015/
              new-P802-1CM-dr aft-PAR-0515-v02.pdf>.

   [IEEE8021TSN]
              IEEE 802.1, "The charter of the TG is to provide the
              specifications that will allow time-synchronized low
              latency streaming services through 802 networks.", 2016,
              <http://www.ieee802.org/1/pages/tsn.html>.

   [IETFDetNet]
              IETF, "Charter for IETF DetNet Working Group", 2015,
              <https://datatracker.ietf.org/wg/detnet/charter/>.

   [ISA100]   ISA/ANSI, "ISA100, Wireless Systems for Automation",
              <https://www.isa.org/isa100/>.

   [ISA100.11a]
              ISA/ANSI, "Wireless Systems for Industrial Automation:
              Process Control and Related Applications - ISA100.11a-2011
              - IEC 62734", 2011, <http://www.isa.org/Community/
              SP100WirelessSystemsforAutomation>.

   [ISO7240-16]
              ISO, "ISO 7240-16:2007 Fire detection and alarm systems --
              Part 16: Sound system control and indicating equipment",
              2007, <http://www.iso.org/iso/
              catalogue_detail.htm?csnumber=42978>.

   [knx]   KNX Association, "ISO/IEC 14543-3 - KNX", November 2006.

   [lontalk] ECHELON, "LonTalk(R) Protocol Specification Version 3.0",
              1994.

   [LTE-Latency]
              Johnston, S., "LTE Latency: How does it compare to other
              technologies", March 2014,
              <http://opensignal.com/blog/2014/03/10/
              lte-latency-how-does-it-compare-to-other-technologies>.

   [MEF]   MEF, "Mobile Backhaul Phase 2 Amendment 1 -- Small Cells",
              MEF 22.1.1, July 2014,
              <http://www.mef.net/Assets/Technical_Specifications/PDF/
              MEF_22.1.1.pdf>.

   [METIS]   METIS, "Scenarios, requirements and KPIs for 5G mobile and
              wireless system", ICT-317669-METIS/D1.1 ICT-
              317669-METIS/D1.1, April 2013, <https://www.metis2020.com/
              wp-content/uploads/deliverables/METIS_D1.1_v1.pdf>.

   [modbus]   Modbus Organization, "MODBUS APPLICATION PROTOCOL
              SPECIFICATION V1.1b", December 2006.

   [net5G]   Ericsson, "5G Radio Access, Challenges for 2020 and
              Beyond", Ericsson white paper wp-5g, June 2013,
              <http://www.ericsson.com/res/docs/whitepapers/wp-5g.pdf>.

   [NGMN]   NGMN Alliance, "5G White Paper", NGMN 5G White Paper v1.0,
              February 2015, <https://www.ngmn.org/uploads/media/
              NGMN_5G_White_Paper_V1_0.pdf>.

   [PCE]   IETF, "Path Computation Element",
              <https://datatracker.ietf.org/doc/charter-ietf-pce/>.

   [profibus]
              IEC, "IEC 61158 Type 3 - Profibus DP", January 2001.

   [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate
              Requirement Levels", BCP 14, RFC 2119,
              DOI 10.17487/RFC2119, March 1997,
              <http://www.rfc-editor.org/info/rfc2119>.

   [RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6
              (IPv6) Specification", RFC 2460, DOI 10.17487/RFC2460,
              December 1998, <http://www.rfc-editor.org/info/rfc2460>.

   [RFC2474] Nichols, K., Blake, S., Baker, F., and D. Black,
              "Definition of the Differentiated Services Field (DS
              Field) in the IPv4 and IPv6 Headers", RFC 2474,
              DOI 10.17487/RFC2474, December 1998,
              <http://www.rfc-editor.org/info/rfc2474>.

   [RFC3031] Rosen, E., Viswanathan, A., and R. Callon, "Multiprotocol
              Label Switching Architecture", RFC 3031,
              DOI 10.17487/RFC3031, January 2001,
              <http://www.rfc-editor.org/info/rfc3031>.

   [RFC3209] Awduche, D., Berger, L., Gan, D., Li, T., Srinivasan, V.,
              and G. Swallow, "RSVP-TE: Extensions to RSVP for LSP
              Tunnels", RFC 3209, DOI 10.17487/RFC3209, December 2001,
              <http://www.rfc-editor.org/info/rfc3209>.

   [RFC3393] Demichelis, C. and P. Chimento, "IP Packet Delay Variation
              Metric for IP Performance Metrics (IPPM)", RFC 3393,
              DOI 10.17487/RFC3393, November 2002,
              <http://www.rfc-editor.org/info/rfc3393>.

   [RFC3444] Pras, A. and J. Schoenwaelder, "On the Difference between
              Information Models and Data Models", RFC 3444,
              DOI 10.17487/RFC3444, January 2003,
              <http://www.rfc-editor.org/info/rfc3444>.

   [RFC3972] Aura, T., "Cryptographically Generated Addresses (CGA)",
              RFC 3972, DOI 10.17487/RFC3972, March 2005,
              <http://www.rfc-editor.org/info/rfc3972>.

   [RFC3985] Bryant, S., Ed. and P. Pate, Ed., "Pseudo Wire Emulation
              Edge-to-Edge (PWE3) Architecture", RFC 3985,
              DOI 10.17487/RFC3985, March 2005,
              <http://www.rfc-editor.org/info/rfc3985>.

   [RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing
              Architecture", RFC 4291, DOI 10.17487/RFC4291, February
              2006, <http://www.rfc-editor.org/info/rfc4291>.

   [RFC4553] Vainshtein, A., Ed. and YJ. Stein, Ed., "Structure-
              Agnostic Time Division Multiplexing (TDM) over Packet
              (SAToP)", RFC 4553, DOI 10.17487/RFC4553, June 2006,
              <http://www.rfc-editor.org/info/rfc4553>.

   [RFC4903] Thaler, D., "Multi-Link Subnet Issues", RFC 4903,
              DOI 10.17487/RFC4903, June 2007,
              <http://www.rfc-editor.org/info/rfc4903>.

   [RFC4919] Kushalnagar, N., Montenegro, G., and C. Schumacher, "IPv6
              over Low-Power Wireless Personal Area Networks (6LoWPANs):
              Overview, Assumptions, Problem Statement, and Goals",
              RFC 4919, DOI 10.17487/RFC4919, August 2007,
              <http://www.rfc-editor.org/info/rfc4919>.

   [RFC5086] Vainshtein, A., Ed., Sasson, I., Metz, E., Frost, T., and
              P. Pate, "Structure-Aware Time Division Multiplexed (TDM)
              Circuit Emulation Service over Packet Switched Network
              (CESoPSN)", RFC 5086, DOI 10.17487/RFC5086, December 2007,
              <http://www.rfc-editor.org/info/rfc5086>.

   [RFC5087] Stein, Y(J)., Shashoua, R., Insler, R., and M. Anavi,
              "Time Division Multiplexing over IP (TDMoIP)", RFC 5087,
              DOI 10.17487/RFC5087, December 2007,
              <http://www.rfc-editor.org/info/rfc5087>.

   [RFC6282] Hui, J., Ed. and P. Thubert, "Compression Format for IPv6
              Datagrams over IEEE 802.15.4-Based Networks", RFC 6282,
              DOI 10.17487/RFC6282, September 2011,
              <http://www.rfc-editor.org/info/rfc6282>.

   [RFC6550] Winter, T., Ed., Thubert, P., Ed., Brandt, A., Hui, J.,
              Kelsey, R., Levis, P., Pister, K., Struik, R., Vasseur,
              JP., and R. Alexander, "RPL: IPv6 Routing Protocol for
              Low-Power and Lossy Networks", RFC 6550,
              DOI 10.17487/RFC6550, March 2012,
              <http://www.rfc-editor.org/info/rfc6550>.

   [RFC6551] Vasseur, JP., Ed., Kim, M., Ed., Pister, K., Dejean, N.,
              and D. Barthel, "Routing Metrics Used for Path Calculation
              in Low-Power and Lossy Networks", RFC 6551,
              DOI 10.17487/RFC6551, March 2012,
              <http://www.rfc-editor.org/info/rfc6551>.

   [RFC6775] Shelby, Z., Ed., Chakrabarti, S., Nordmark, E., and C.
              Bormann, "Neighbor Discovery Optimization for IPv6 over
              Low-Power Wireless Personal Area Networks (6LoWPANs)",
              RFC 6775, DOI 10.17487/RFC6775, November 2012,
              <http://www.rfc-editor.org/info/rfc6775>.

   [RFC7554] Watteyne, T., Ed., Palattella, M., and L. Grieco, "Using
              IEEE 802.15.4e Time-Slotted Channel Hopping (TSCH) in the
              Internet of Things (IoT): Problem Statement", RFC 7554,
              DOI 10.17487/RFC7554, May 2015,
              <http://www.rfc-editor.org/info/rfc7554>.

   [SRP_LATENCY]
              Gunther, C., "Specifying SRP Latency", 2014,
              <http://www.ieee802.org/1/files/public/docs2014/
              cc-cgunther-acceptable-latency-0314-v01.pdf>.

   [STUDIO_IP]
              Mace, G., "IP Networked Studio Infrastructure for
              Synchronized & Real-Time Multimedia Transmissions", 2007,
              <http://www.ieee802.org/1/files/public/docs2047/
              avb-mace-ip-networked-studio-infrastructure-0107.pdf>.

   [SyncE]   ITU-T, "G.8261 : Timing and synchronization aspects in
              packet networks", Recommendation G.8261, August 2013,
              <http://www.itu.int/rec/T-REC-G.8261>.

   [TEAS]   IETF, "Traffic Engineering Architecture and Signaling",
              <https://datatracker.ietf.org/doc/charter-ietf-teas/>.

   [TS23401] 3GPP, "General Packet Radio Service (GPRS) enhancements
              for Evolved Universal Terrestrial Radio Access Network
              (E-UTRAN) access", 3GPP TS 23.401 10.10.0, March 2013.

   [TS25104] 3GPP, "Base Station (BS) radio transmission and reception
              (FDD)", 3GPP TS 25.104 3.14.0, March 2007.

   [TS36104] 3GPP, "Evolved Universal Terrestrial Radio Access
              (E-UTRA); Base Station (BS) radio transmission and
              reception", 3GPP TS 36.104 10.11.0, July 2013.

   [TS36133] 3GPP, "Evolved Universal Terrestrial Radio Access
              (E-UTRA); Requirements for support of radio resource
              management", 3GPP TS 36.133 12.7.0, April 2015.

   [TS36211] 3GPP, "Evolved Universal Terrestrial Radio Access
              (E-UTRA); Physical channels and modulation", 3GPP
              TS 36.211 10.7.0, March 2013.

   [TS36300] 3GPP, "Evolved Universal Terrestrial Radio Access (E-UTRA)
              and Evolved Universal Terrestrial Radio Access Network
              (E-UTRAN); Overall description; Stage 2", 3GPP TS 36.300
              10.11.0, September 2013.

   [TSNTG]   IEEE Standards Association, "IEEE 802.1 Time-Sensitive
              Networks Task Group", 2013,
              <http://www.IEEE802.org/1/pages/avbridges.html>.

   [UHD-video]
              Holub, P., "Ultra-High Definition Videos and Their
              Applications over the Network", The 7th International
              Symposium on VICTORIES Project PetrHolub_presentation,
              October 2014, <http://www.aist-
              victories.org/jp/7th_sympo_ws/PetrHolub_presentation.pdf>.

   [WirelessHART]
              www.hartcomm.org, "Industrial Communication Networks -
              Wireless Communication Network and Communication Profiles
              - WirelessHART - IEC 62591", 2010.

Authors' Addresses

Ethan Grossman (editor)
Dolby Laboratories, Inc.
1275 Market Street
San Francisco, CA 94103
USA

Phone: +1 415 645 4726
Email: ethan.grossman@dolby.com
URI: http://www.dolby.com

Craig Gunther
Harman International
10653 South River Front Parkway
South Jordan, UT 84095
USA

Phone: +1 801 568-7675
Email: craig.gunther@harman.com
URI: http://www.harman.com

Pascal Thubert
Cisco Systems, Inc
Building D
45 Allee des Ormes - BP1200
MOUGINS - Sophia Antipolis 06254
FRANCE

Phone: +33 497 23 26 34
Email: pthubert@cisco.com

Patrick Wetterwald
Cisco Systems
45 Allees des Ormes
Mougins 06250
FRANCE

Phone: +33 4 97 23 26 36
Email: pwetterw@cisco.com

Jean Raymond
Hydro-Quebec
1500 University
Montreal H3A3S7
Canada

Phone: +1 514 840 3000
Email: raymond.jean@hydro.qc.ca

Jouni Korhonen
Broadcom Corporation
3151 Zanker Road
San Jose, CA 95134
USA

Email: jouni.nospam@gmail.com

Yu Kaneko
Toshiba
1 Komukai-Toshiba-cho, Saiwai-ku, Kasasaki-shi
Kanagawa, Japan

Email: yu1.kaneko@toshiba.co.jp

Subir Das
Applied Communication Sciences
150 Mount Airy Road, Basking Ridge
New Jersey, 07920, USA

Email: sdas@appcomsci.com

Yiyong Zha
Huawei Technologies

Email: zhayiyong@huawei.com

Balazs Varga
Ericsson
Konyves Kalman krt. 11/B
Budapest 1097
Hungary

Email: balazs.a.varga@ericsson.com

Janos Farkas
Ericsson
Konyves Kalman krt. 11/B
Budapest 1097
Hungary

Email: janos.farkas@ericsson.com

Franz-Josef Goetz
Siemens
Gleiwitzerstr. 555
Nurnberg 90475
Germany

Email: franz-josef.goetz@siemens.com

Juergen Schmitt
Siemens
Gleiwitzerstr. 555
Nurnberg 90475
Germany

Email: juergen.jues.schmitt@siemens.com