IETF92 - Dallas

Chairs:
Pascal Thubert
Thomas Watteyne
Mailing list:
6tisch@ietf.org
Jabber:
6tisch@jabber.ietf.org
Etherpad for minutes:
http://etherpad.tools.ietf.org:9000/p/notes-ietf-92-6tisch

IPv6 over the TSCH mode of IEEE 802.15.4e

Note Well

Any submission to the IETF intended by the Contributor for publication as all or part of an IETF Internet-Draft or RFC and any statement made within the context of an IETF activity is considered an "IETF Contribution". Such statements include oral statements in IETF sessions, as well as written and electronic communications made at any time or place, which are addressed to:

- The IETF plenary session
- The IESG, or any member thereof on behalf of the IESG
- Any IETF mailing list, including the IETF list itself, any working group or design team list, or any other list functioning under IETF auspices
- Any IETF working group or portion thereof
- Any Birds of a Feather (BOF) session
- The IAB or any member thereof on behalf of the IAB
- The RFC Editor or the Internet-Drafts function

All IETF Contributions are subject to the rules of RFC 5378 and RFC 3979 (updated by RFC 4879).

Statements made outside of an IETF session, mailing list or other function, that are clearly not intended to be input to an IETF activity, group or function, are not IETF Contributions in the context of this notice. Please consult RFC 5378 and RFC 3979 for details.

A participant in any IETF activity is deemed to accept all IETF rules of process, as documented in Best Current Practices RFCs and IESG Statements.

A participant in any IETF activity acknowledges that written, audio and video records of meetings may be made and may be available to the public.

Reminder:

Minutes are taken *

This meeting is recorded **

Presence is logged ***

* Scribe: please contribute online to the minutes at http://etherpad.tools.ietf.org:9000/p/notes-ietf-91-6tisch

** Recordings and Minutes are public and may be subject to discovery in the event of litigation.

*** Please make sure you sign the blue sheets

Administrivia

- Blue Sheets
- Scribes
- Jabber

Objectives

- Monday (1520-1650 CDT, Continental)
  - DetNet
  - Security
- Thursday (0900-1130 CDT, Continental)
  - WG drafts, including in last call
  - Plugtest
  - Distributed scheduling
  - Rechartering discussion

Agenda

```
Intro and Status                                  [2min]  (Chairs)

   Note-Well, Blue Sheets, Scribes, Agenda Bashing

DetNet

   * <draft-finn-detnet-architecture-00>          [20min]  (Norm Finn)
   * <draft-gunther-detnet-proaudio-req-00>       [10min]  (Jouni Korhonen)
   * <draft-wetterwald-detnet-utilities-reqs-01> [10min]  (Patrick Wetterwald)
   * <draft-wang-6tisch-track-use-cases-00>       [10min]  (Chonggang Wang)

Security                                          [30min]
   * DT status and design goals                            (Michael Richardson)
   * <draft-struik-6tisch-security-considerations-01>     (Rene Struik)

Wrap up for rechartering                           [8min]  (Chairs)
```

draft-finn-detnet-architecture

Draft Full Name

Norman Finn

Pascal Thubert

Michael Johas Teener

Status

- Status:
  - Adopted at IETFXX (only for WG docs)
  - Latest version -**01** published on **09.03.15**
    available at: https://datatracker.ietf.org/doc/draft-finn-detnet-architecture

- Changes since IETF91 (only if existed)
  - **New**

Field Bus → IP and Ethernet

- The world of **real-time apps**, including
  - Automotive (and other vehicle) control
  - Industrial control
  - Audio/video program creation

  has gone **digital** over the last 30 years.
- But, for the most part, they have gone with "field busses" == **not** Ethernet, **not** Internet Protocols, and the ones that are Ethernet are seldom from RAND SDOs.

What the applications require

- Time synchronization to < 1µs accuracy.
  - Not a direct concern of DetNet in IETF.
- Fixed-bandwidth critical streams.
  - No throttling.
- Packet loss ratio 10^{-10} to 10^{-12} or better.
- Guaranteed worst-case latency.
- Coexistence with “normal” traffic on same physical network, with no interference.

How to get low loss ratio

Throttling and gross overprovisioning are not useful options. What we do, instead, is:

1. Eliminate **congestion loss** (and guarantee **latency**) by **allocating resources** (bandwidth and buffers) along the path(s) before data flow starts, and use **shaping and/or scheduling** at every hop. (Not necessarily IntServ!)
   - State at every hop == “circuit”.
2. (Nearly) eliminate **equipment failure** losses via **seamless redundancy**: Sequence number near source, replicate data over multiple paths, eliminate duplicates at or near destination.

This has been done for L2

- IEEE 802.1 Time-Sensitive Networking (TSN) Task Group and its predecessor Audio Video Bridging (AVB) Task Group have standards for resource reservation, shaping, and scheduling by brides for L2.
- This technology is being deployed, now, in theaters, studios, theme parks, and automobiles.

This has been done for L2

- But, that's not enough for many applications. We need:
  - L3 and mixed L2/L3 solutions.
  - More options for resource reservation.
  - More options for centralized control.
  - Solutions that, insofar as possible, given the requirement for pre-allocated resources, have no impact on (are orthogonal to) existing networking paradigms.
- We do **not** need:
  - A top-to-bottom tweaking of all layers for a particular application space. (We have too many of those, already!)

Queuing, shaping, scheduling

IEEE 802.1 and 802.3 have completed and nearly-completed standards for:

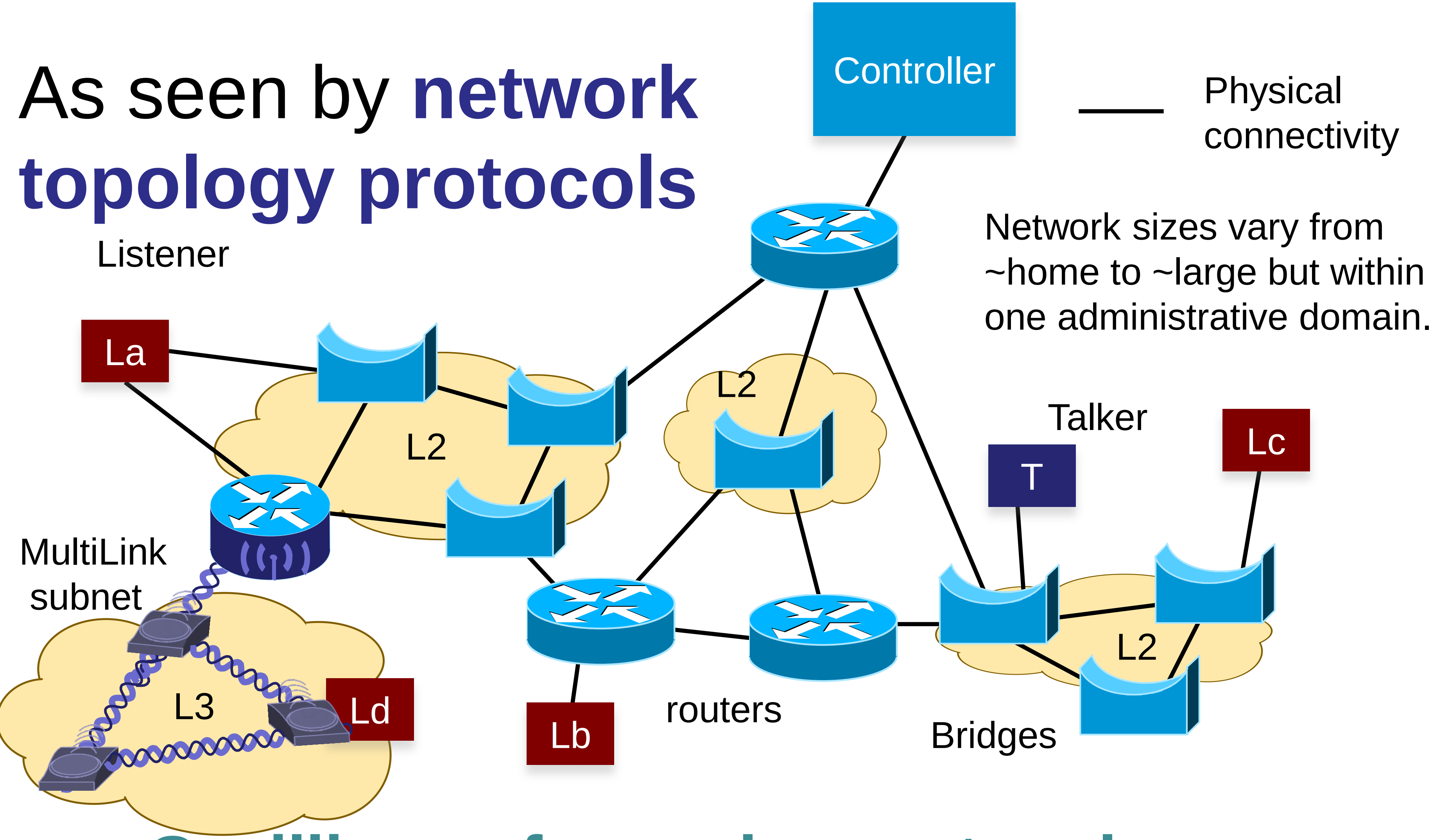
1. Output shapers that, when configured properly, guarantee zero congestion loss.
2. Output gates on a synchronized, rotating schedule that give essentially zero jitter.
3. ISIS features to build disjoint paths.
4. Resource reservation without regard to what topology control protocol, IEEE 802.1 or other, is being used.

Why do we care about IEEE queuing models?

- The various IEEE 802.1 queuing features work together in a predictable manner.
- Tight standards are required in this space – any uncertainty in one node’s behavior adds buffers and latency to the next.
- **Once packets are queued on an output port awaiting selection, it doesn’t matter whether or not the addresses are IPv6 or Ethernet, or whether a TTL was decremented.**

Reference network

As seen by **network topology protocols**

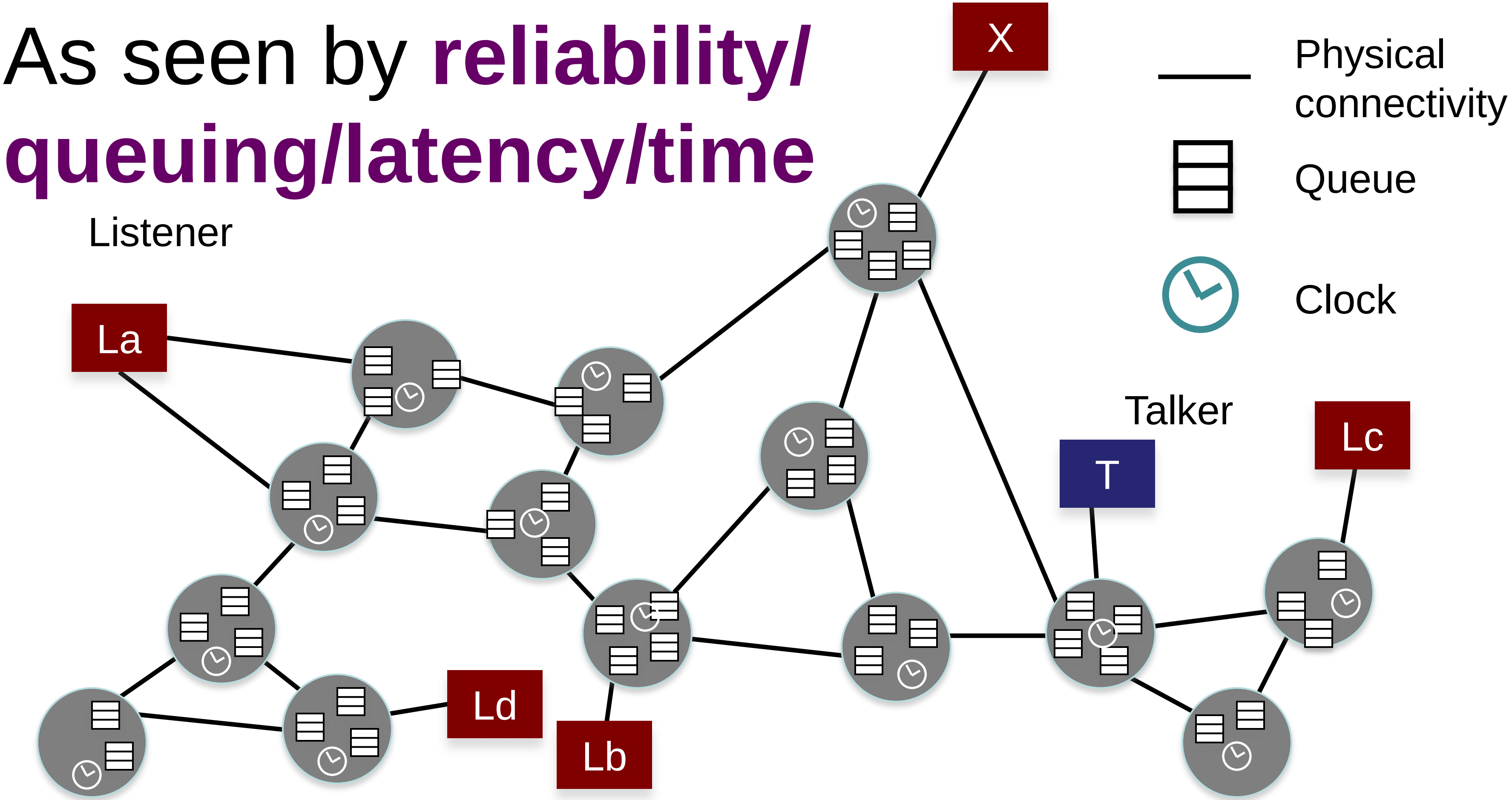


Network sizes vary from ~home to ~large but within one administrative domain.

- **Gazillions of complex protocols**

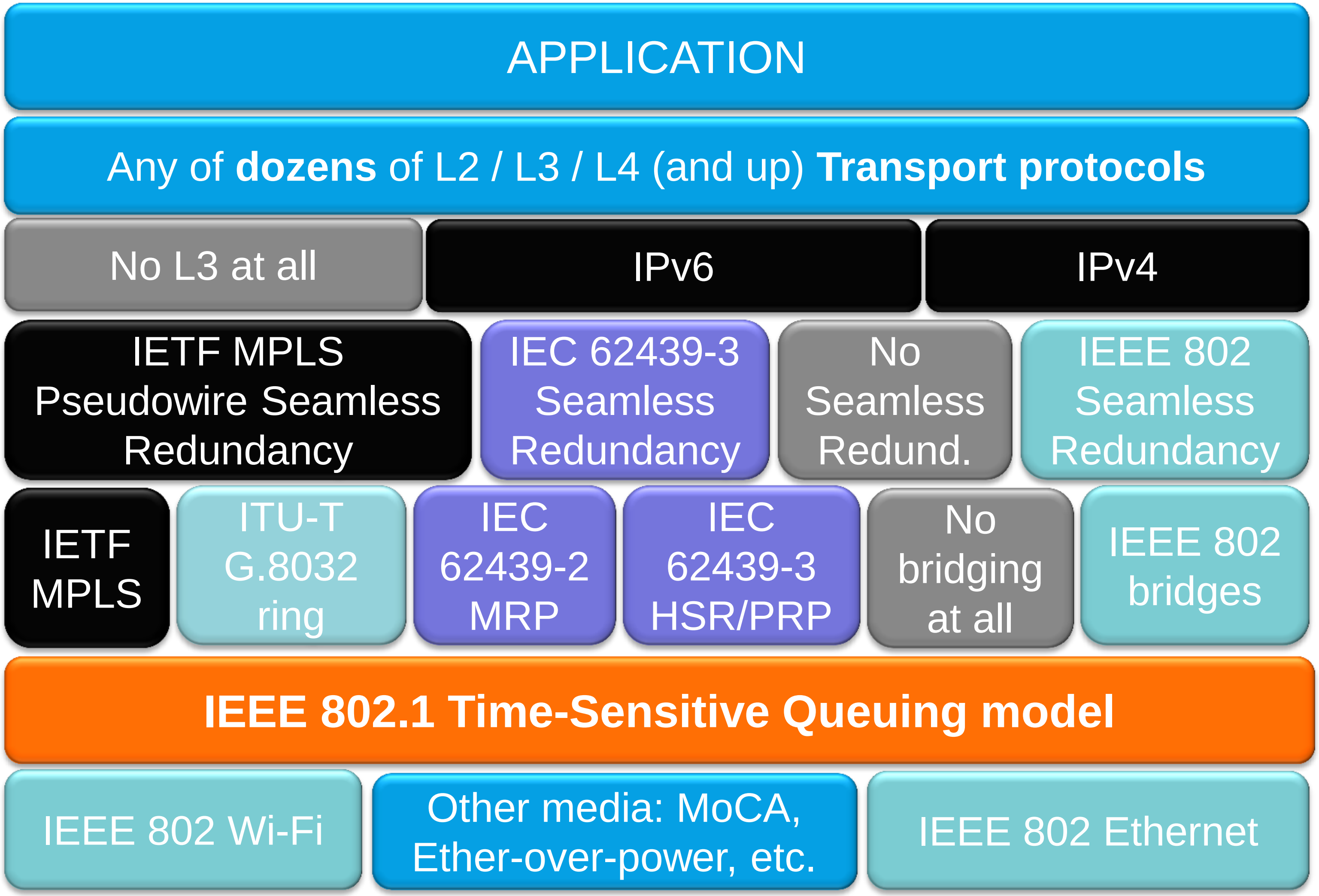
Reference network

As seen by **reliability/ queuing/latency/time**



- **Just nodes, queues, clocks, and wires!!**

DetNet data plane menu??



APPLICATION

Any of **dozens** of L2 / L3 / L4 (and up) **Transport protocols**

No L3 at all

IPv6

IPv4

IETF MPLS Pseudowire Seamless Redundancy

IEC 62439-3 Seamless Redundancy

No Seamless Redund.

IEEE 802 Seamless Redundancy

IETF MPLS

ITU-T G.8032 ring

IEC 62439-2 MRP

IEC 62439-3 HSR/PRP

No bridging at all

IEEE 802 bridges

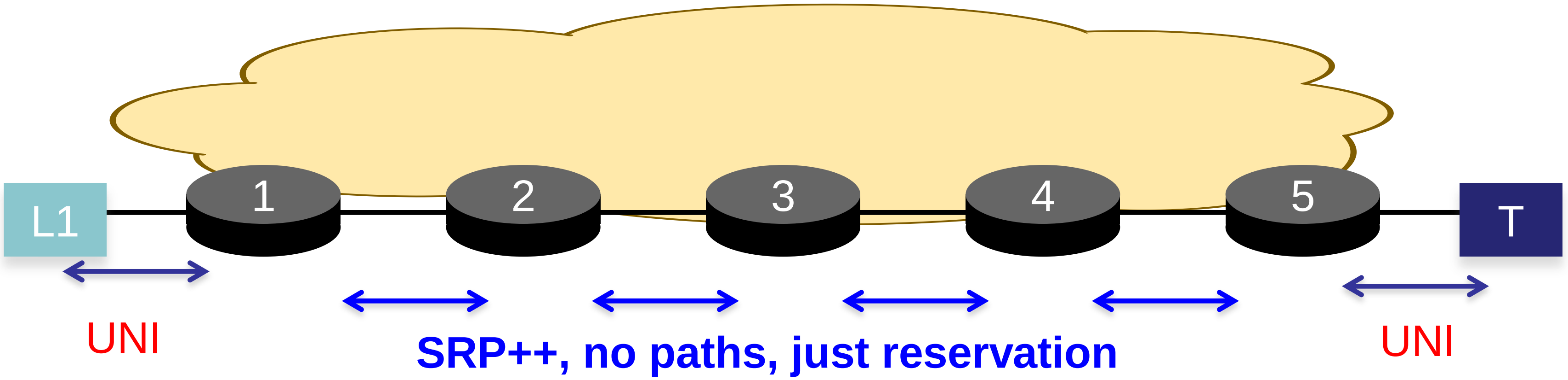
IEEE 802.1 Time-Sensitive Queuing model

IEEE 802 Wi-Fi

Other media: MoCA, Ether-over-power, etc.

IEEE 802 Ethernet

Control plane: peer-to-peer



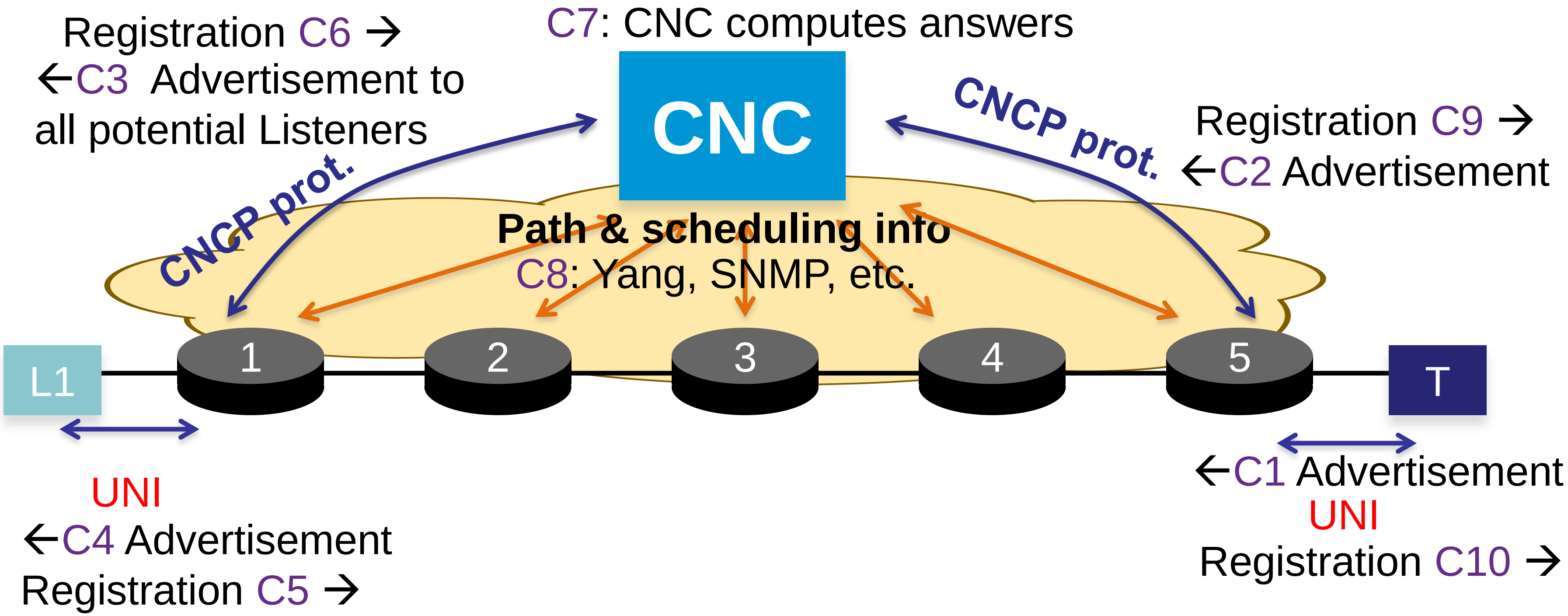
← P3 Advertisement
Registration P4→

← P2 Advertisement (hop by hop)
Registration P5 → (hop by hop)

←P1 Advertisement
P6 Registration →

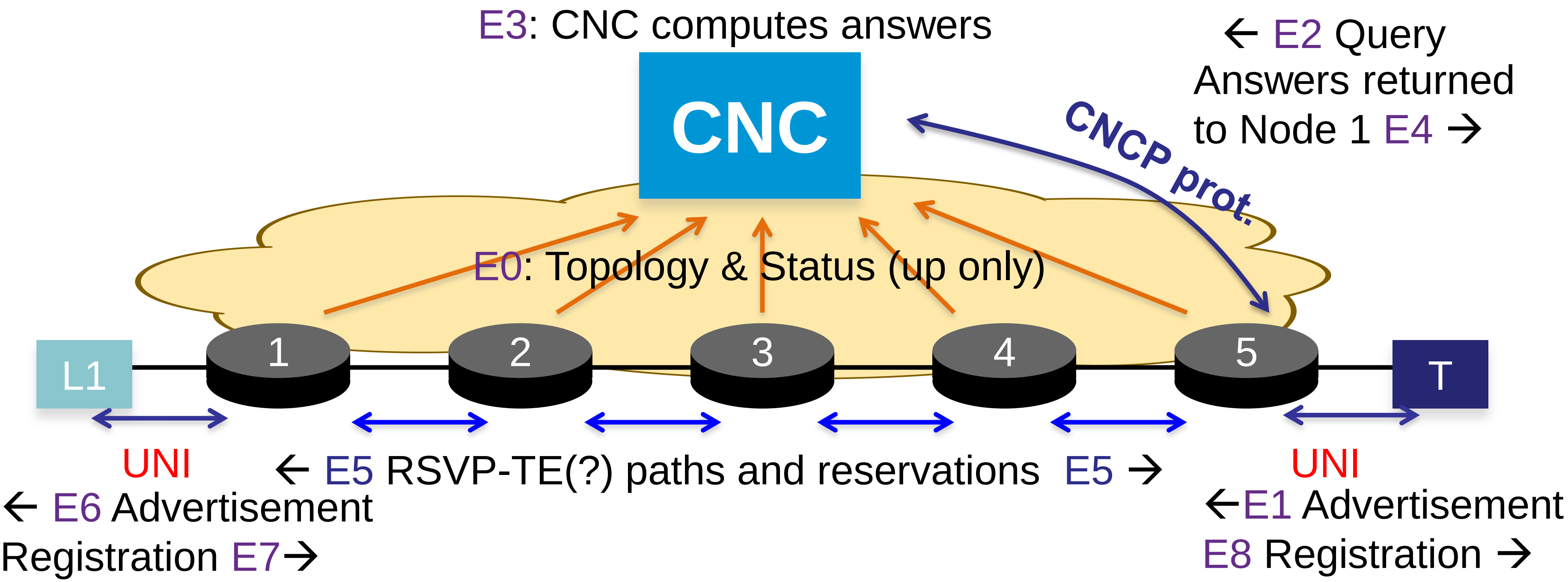
- A peer-to-peer control paradigm is used by IEEE SRP (and RSVP).
- This paradigm is adequate for some data plane queuing methods, but not for all. (Some require a central brain.)

Control plane: hub and spoke



- A central server communicating radially with network nodes can support all schedulers/shapers with the minimum amount of standards writing, and maximum velocity of features.
- Several existing IETF solutions available as the basis for “CNCP” and transferring “Path & scheduling info”.

Control plane: hybrid



E3: CNC computes answers

← E2 Query

Answers returned to Node 1 E4 →

E0: Topology & Status (up only)

← E5 RSVP-TE(?) paths and reservations E5 →

← E6 Advertisement

Registration E7→

←E1 Advertisement

E8 Registration →

- Edge node turns user request into query/response with central server, then propagates the answer peer-to-peer through the network. Hybrid model supports mixed central/peer networks.
- This is the current IETF PCE model, with the addition of hosts and UNI.

draft-gunther-detnet-proaudio-req-00

Craig Gunther (Ed.)
Jouni Korhonen (presenter)

Goals

- What is Pro-A and what are they looking for
- Introduce Pro-A needs and concerns
- Highlight requirements unique to Pro-A
- Stimulate ideas from other Pro-A participants

Overview

- What is Pro-Audio?
  - Theme parks, churches
  - PA systems in airports, train stations, sports stadiums
  - Cinema, theater, garage bands
  - Recording studios, production facilities
- Unique (?) Pro-Audio requirements
  - Health & Safety certification requirements (ISO7240, EN54, etc)
  - Super Streams and latency requirements
  - Unused reservation bandwidth available for Best Effort traffic
  - Using Link Aggregation
  - IPv4 multicasting

Overview (continued)

- Use Cases
  - Existing layer 2 networks that need layer 3 interconnect
  - Streaming from remote sites
- Security concerns
  - Hearing damage from multi-thousand watt speaker systems
  - Malicious attacks on PA systems infrastructure preventing health/safety/fire announcements

Next Steps

- Encourage review and comments
- Feedback please
  - What pieces of draft are relevant?
  - What pieces are not?
- Any other unique Pro-A requirements?
- Other health/safety equipment requirements (e.g. EN54)?
- Other use cases?
- Add in Pro-Video requirements and use cases?

draft-wetterwald-detnet-utilities-reqs

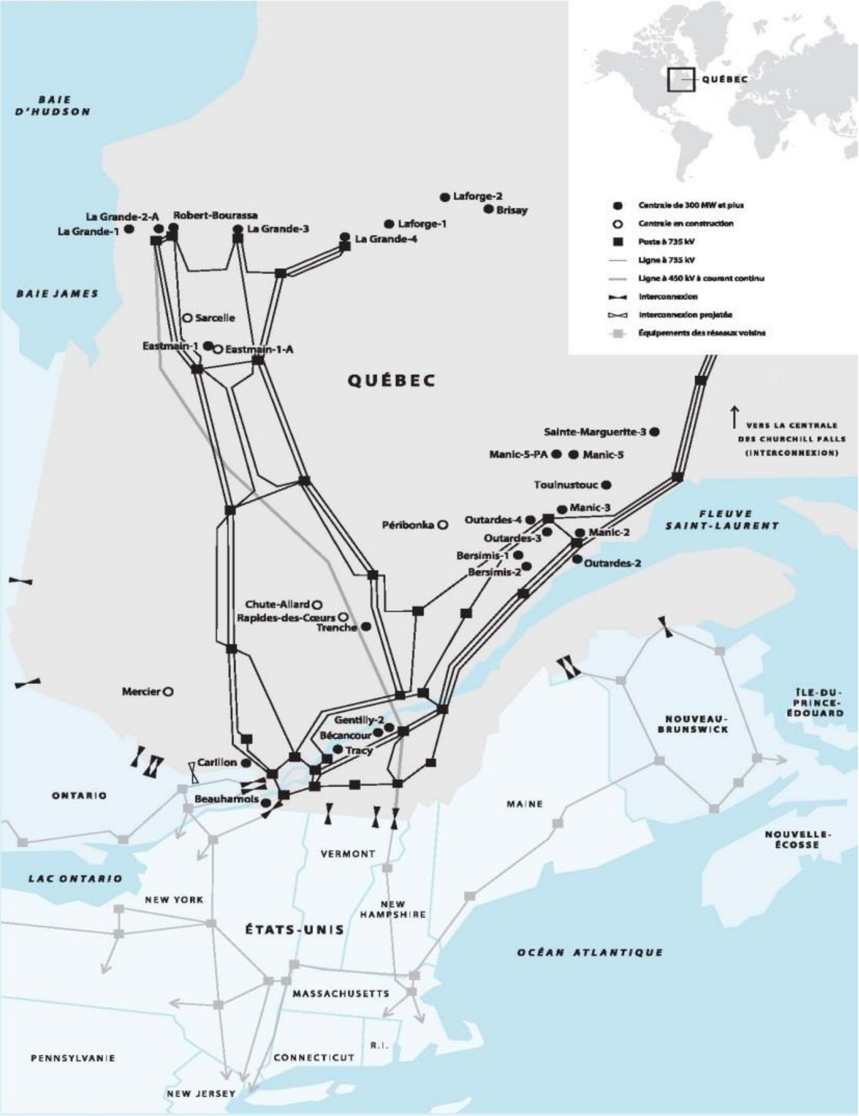
Deterministic Networking
Utilities requirements

Patrick Wetterwald, Jean Raymond

pwetterw@cisco.com
Raymond.Jean@hydro.qc.ca

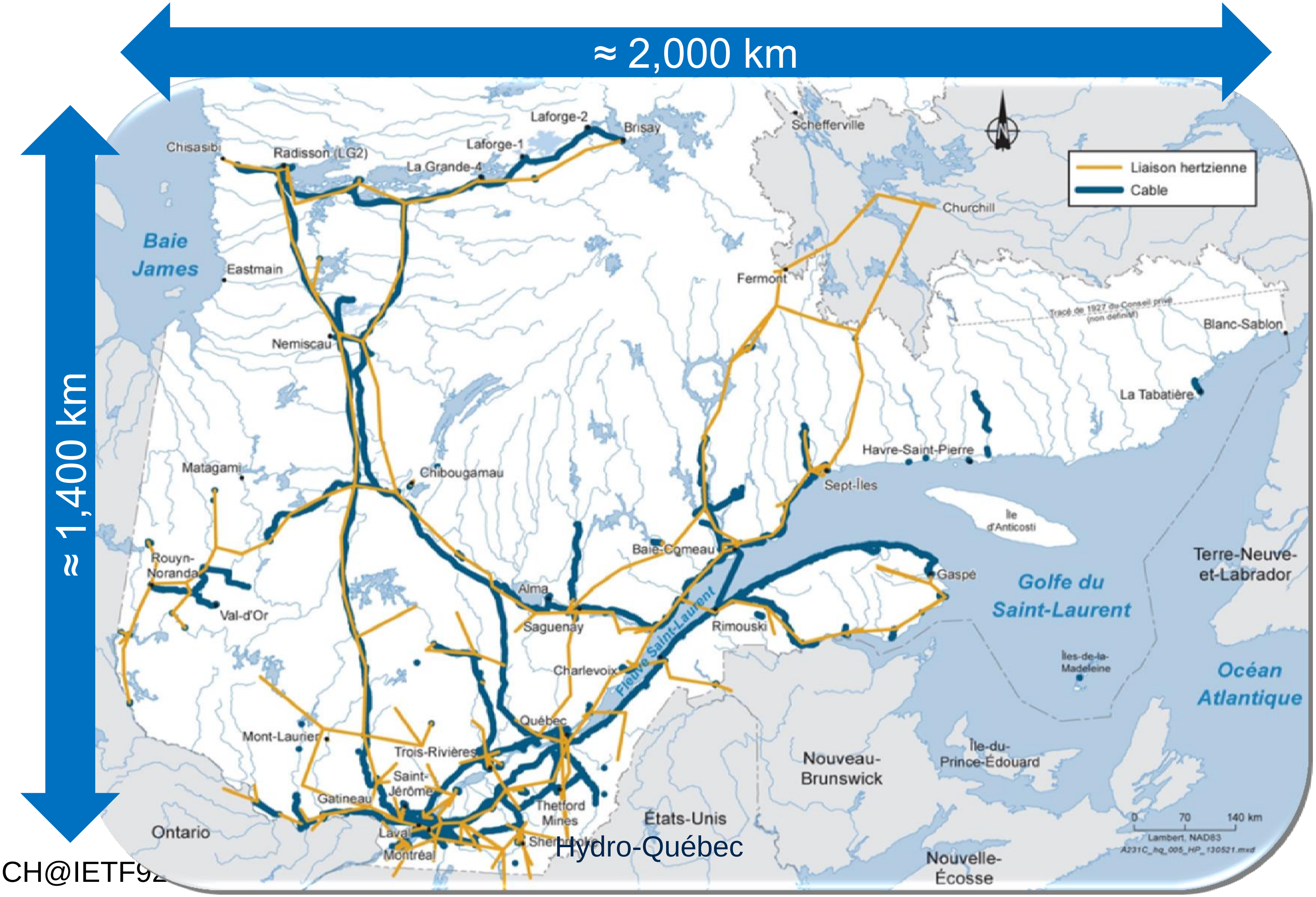
Electrical Transmission Network Characteristics

- Designed to transport over long distances
- Specificity and complexity of the separation between generation and load (~ 1200 km)
- Distance between substations (max 280 km)
- Interconnected with:
  - Ontario
  - New York
  - Nouvelle-Angleterre
  - Nouveau-Brunswick



Hydro-(

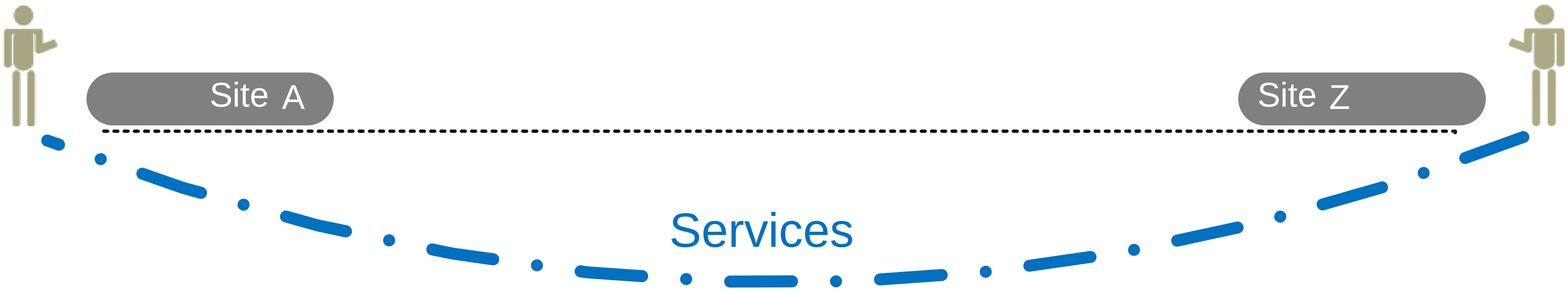
Extensive Network



Hydro-Québec

Infrastructure Footprint

514 substations
60 generating stations
143 administrative buildings
10,500 km of optical fibre
315 microwave links covering 10,000 km
205 mobile radio repeater sites



835 telecom sites across Québec

Hydro-Québec

Utility needs

- Increase Grid Reliability / Optimization ➔ Migration to new standards / equipment :
  - IEC 61850 implies new communication requirements.
- Optimization of Telecommunication network ➔ Multi-Services network (Mission critical to work force management):
  - Transition from TDM to packet switching

Deterministic requirements

- All requirements are based on use cases, 2 main areas where deterministic communications are needed (mainly communication between Intelligent Electronic Devices “IEDs”):
  - Intra Substation Communications
  - Inter Substation Communications
- Information carried are instantaneous electrical information and real time commands:
  - Currents, Voltages, Phases, Active and Reactive power…
  - Trip, open/close relay…
- Need to re-act in a fraction of a cycle (50 – 60 Hz).
- Latency, Asymetric delay, Jitter, Availability, Recovery time, Redundancy, Packet loss and precise timing being most important parameters.

- We are playing with lines moving electrical power with voltage level from 110 volts to 735 Kvolts. Power has to be transported by electrical lines not consumed.

Substation Automation

Applications	Transfer time (ms) (top of the stack to top of the stack)
Trips, Blockings	3
Releases, status changes	10
Fast automatic interactions	20
Slow automatic interactions	100
Operator commands	500
Events, Alarms	1000
Files, Events, log contents	> 1000

Time Synchronization: High synchronized sampling requires **1us** time synchroniza accuracy

Based on IEC 61850 requirements

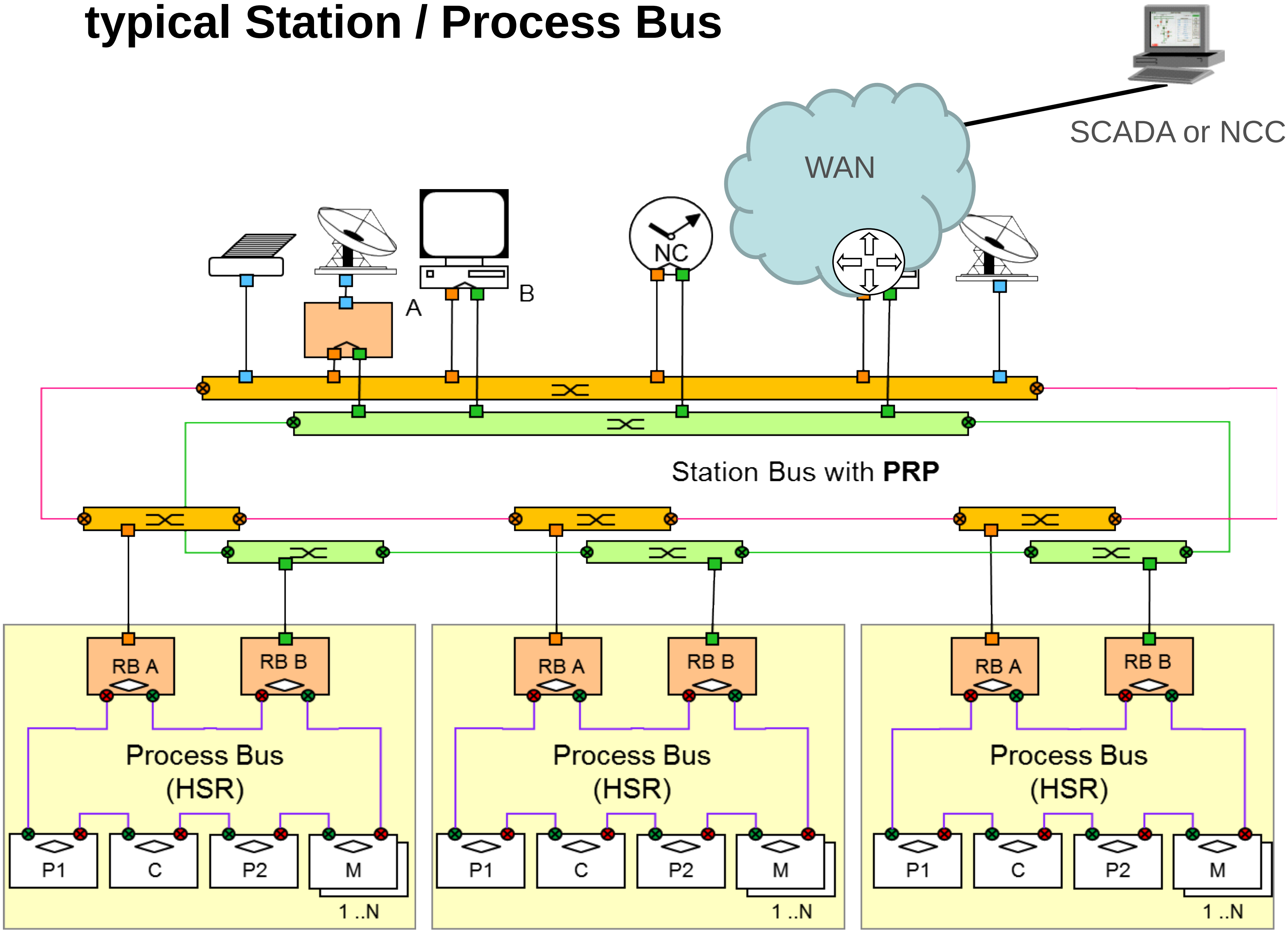
Substation Automation

Communicating partners	Application recovery delay (in ms)	Communication recovery delay (in ms)
SCADA to IED	800	400
IED to IED	12	4
Protecting Trip	8	4
Bus bar protection	< 1	Hitless
Sampled values	Less than few consecutive samples	Hitless

Use of redundant schemes mandatory for some use cases.

GOOSE and SV (Sample values) traffic in large substation could reach 900 Mb/s

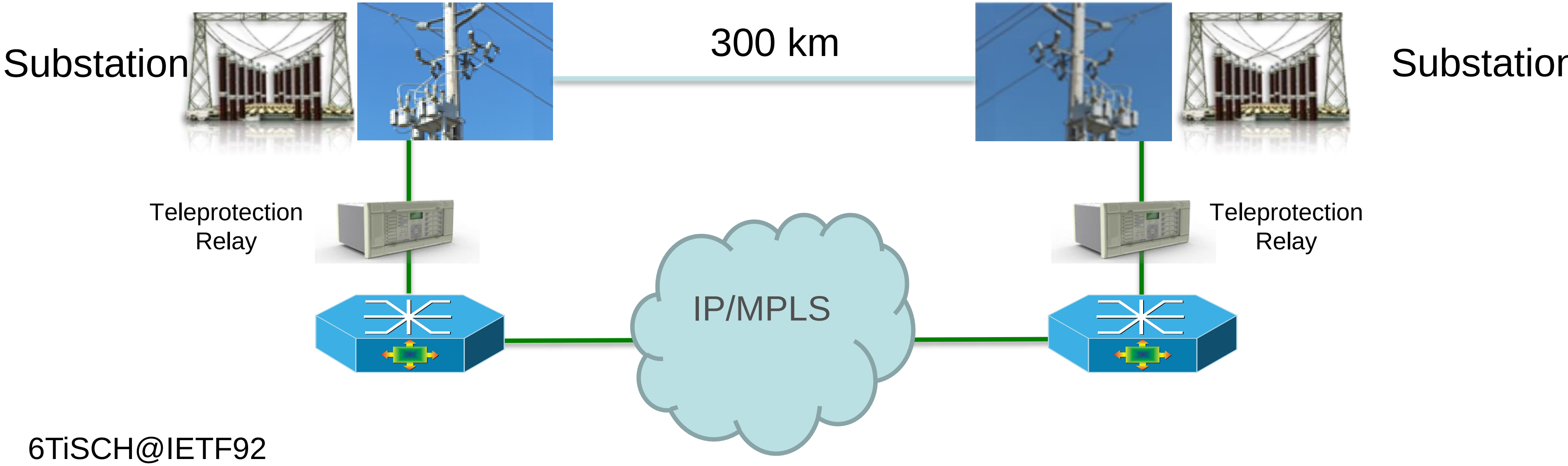
typical Station / Process Bus



WAN requirements

- **draft-wetterwald-detnet-utilities-reqs-**01 is currently focusing on WAN most stringent requirements for communications.

- Current differential protection scheme (transmission):



Teleprotection use cases

Teleprotection requirement	Attribute
One way maximum delay	4-10 ms
Asymetric delay required	Yes
Maximum jitter	250 us
Topology	Point to point, point to multi-points
Availability	99.9999 %
Precise timing required	Yes
Recovery time on node failure	Hitless – less than 50ms
Redundancy	Yes
Packet loss	0.1 %

WAN Engineering Guidelines (IEC 61850-90-12) will address more detailed requirer when available

Use Cases and Requirements for Using Track in 6TiSCH Networks

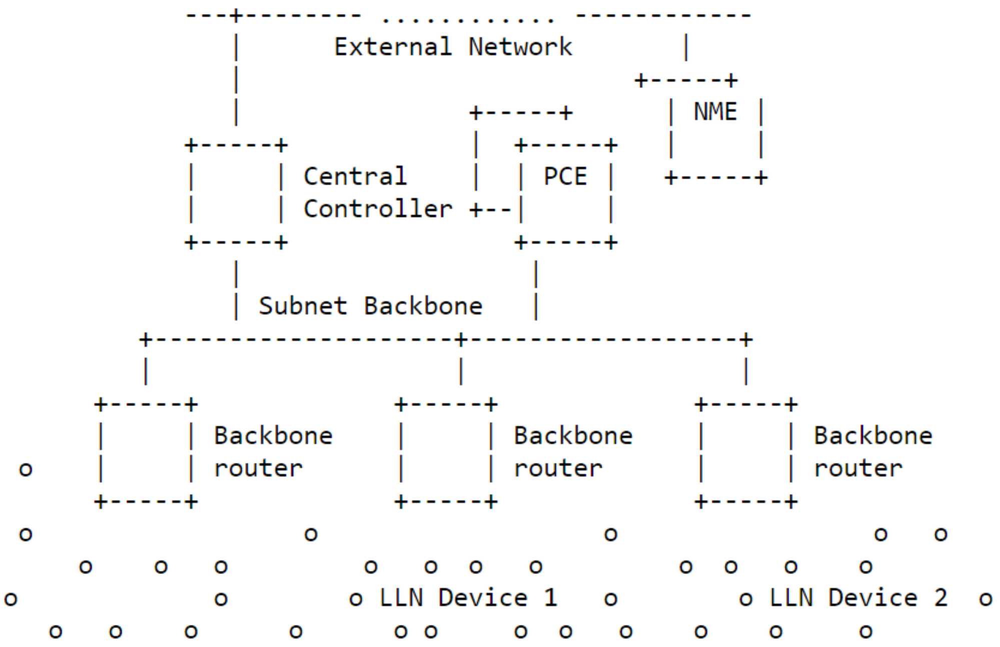
Zhuo Chen, Chonggang Wang

Status

- Status:
  - Latest version -00 published on 03.06.15
    available at: http://tools.ietf.org/html/draft-wang-6tisch-track-use-cases-00

Use Case – Industrial Networks

- Industry Process Control and Automation Applications
- Industrial Monitoring Applications



```
            ---+-------- ............ ------------
               |      External Network       |
               |                          +-----+
               |               +-----+      | NME |
            +-----+            |  +-----+   |     |
            |     | Central    |  | PCE |   +-----+
            |     | Controller +--|     |
            +-----+               +-----+
               |                   |
               | 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 Device 1   o        o LLN Device 2  o
   o   o    o      o      o o     o  o   o    o    o     o
```

Figure 1: Use Case of an Industry Network

Handling Tracks in 6TiSCH Networks

- Benefits for Using Track
  - Less process delay and overhead than layer-3 forwarding
  - Guaranteed delay, jitter, and throughput
  - Enable sleeping node and save energy
  - Better reliability
- Track Reservation
  - Remote track reservation
  - Hop-by-hop track reservation

Requirements for Track Reservation

- Centralized Track Reservation
  - Need a protocol for LLN devices to report their topology and TSCH schedule information to the central controller.
  - Need a lightweight protocol for the central controller to configure hard cells of LLN Devices.
- Distributed Track Reservation
  - Need a fast reaction protocol to reserve a Track.
  - Need a protocol which can quickly detect a Track reservation failure.
  - Need an efficient negotiation protocol between LLN Devices multi-hop away from each other.

Next Step

- TBD

Security DT status

6TiSCH Security Considerations

(draft-struik-6tisch-security-architectural-considerations-01)

Subir Das

Yoshihiro Ohba

René Struik

Status

- Status:
  - Latest version -01 published January 9, 2015

    available at https://datatracker.ietf.org/doc/draft-struik-6tisch-security-considerations/
- Intent:
  - Work-in-progress document capturing security architectural design considerations, including the join process; fit with 802.15.4e/TSCH specification; gap analysis; identification of outstanding issues that need to be addressed; contributions towards addressing these.
  - Current version: frame work, no full specifications (yet)
- Changes since IETF-91:
  - Extensive detail on MAC operations, join protocol flows, and rationale (compared to draft-struik-6tisch-security-architecture-elements-01)

Note: Security not yet part of current 6TiSCH charter

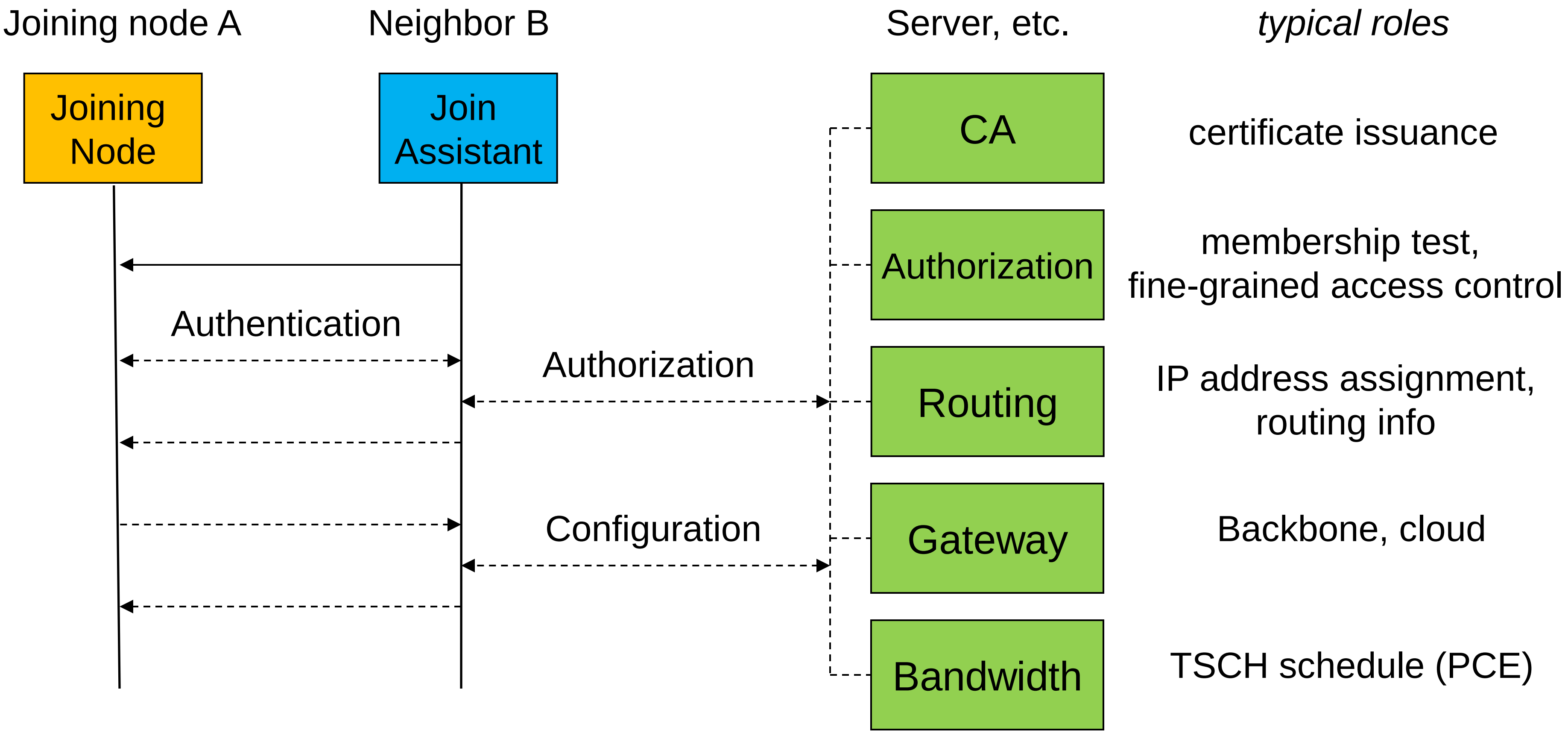
Device Enrolment Steps

Device authentication. Joining Node A and Join Assistant B authenticate each other and establish a shared key (so as to ensure on-going authenticated communications). *This may involve server KDC as third party.*

Authorization. Join Assistant B decides on whether/how to authorize device A (if denied, this may result in loss of bandwidth). *Authorization decision may be delegated to server KDC or other 3rd-party device.*

Configuration/Parameterization. Router B distributes configuration information to Node A, such as ♦ IP address assignment info; ♦ Bandwidth/usage constraints; ♦ Scheduling info (including on re-authentication policy details). *This may originate from other network devices, for which it acts as proxy.*

Networking Joining (1)



NOTE: in some existing applications, Router B acts as relay only and third-party provides both authentication and authorization.

Desired Properties

Security:

- Authenticated key agreement (incl. PFS)
- Mitigation DoS attacks (both re computation, communication)
- End-to-end security (joining node vs. server (PCE, JCE, etc.))

Privacy:

- Hiding of device identity joining node (against passive observers)

Communication:

- Minimization of non-local flows*

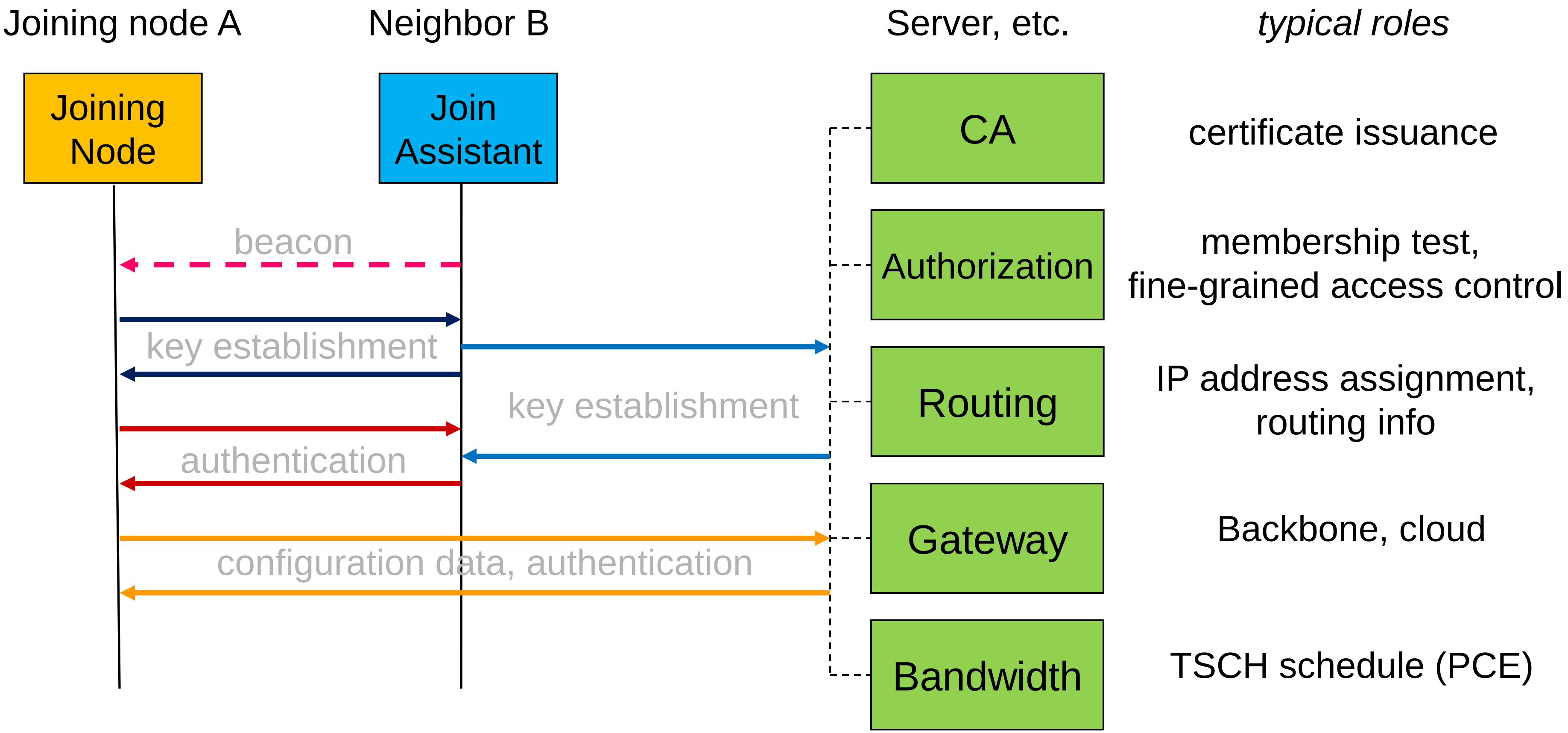
Computation:

- Shift from constrained node to less constrained node

General:

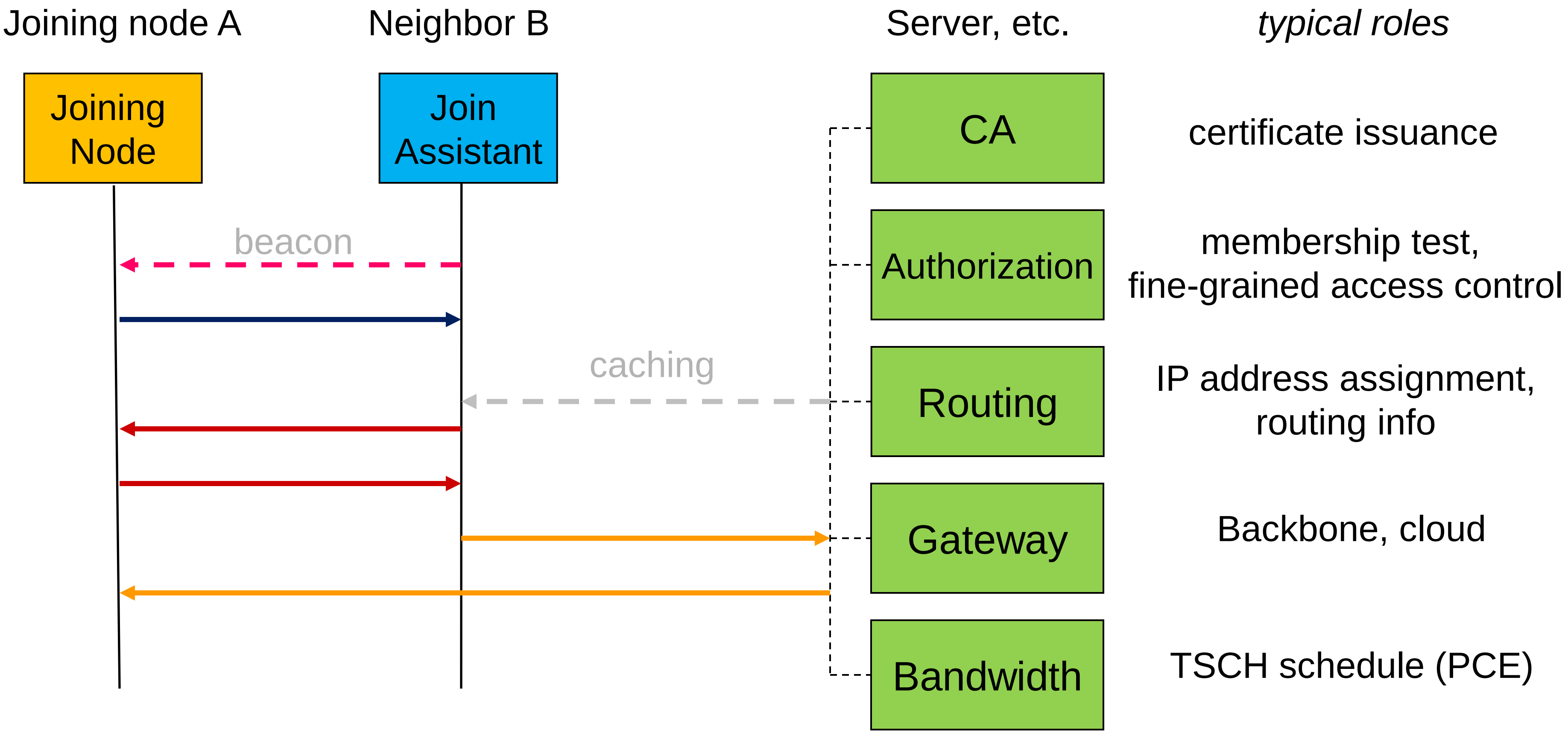
- "Separation of concerns"
- Minimization of dependencies
- Flexibility re deployment models

Network Joining (2)



NOTE: Router B may transfer configuration data to Node A as part of its authentication to Node A.

Network Joining (3)



NOTE: Optimized flows, based on caching of server-side information on Router B (this would benefit from secure multicast…)

Realized Properties w/ Current Draft

Security:

- Authenticated key agreement (incl. PFS)
- Mitigation DoS attacks (both re computation, communication)
- End-to-end security (joining node vs. server (PCE, JCE, etc.))

Privacy:

- Hiding of device identity joining node

Communication:

- Minimization of non-local flows*

Computation:

- Shift from constrained node to less constrained node

General:

- "Separation of concerns"
- Minimization of dependencies

Security and 802.15.4e aspects:

- No need to trust ASN in beacon for security

Security vs. status information:

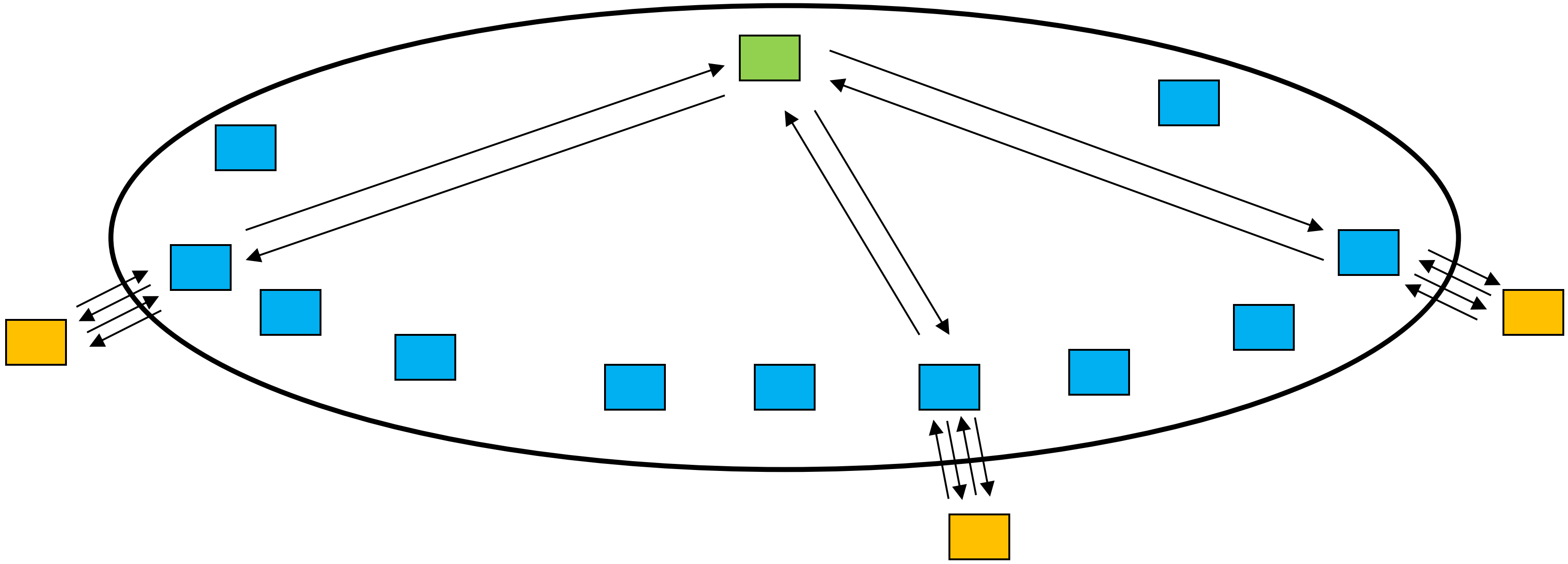
- Prioritization of DoS attack prevention

Separation of concerns:

- 802.15.4e: no need for other beacon
- Routing: no need for "tweaks" (e.g., joining node can use link local address)
- Extensibility: fits with semi-automatic network management concepts and provisioning/configuration concepts

Protocol easy to analyze by security and crypto community (no "short cuts")

Network Joining (4)



The “big picture”...

🟨 Joining node

🟦 Neighbor node

🟩 Server, etc.

Current Draft …

- Current draft includes
  - Extensive detail on behavior MAC (802.15.4e/TSCH)
  - Extensive detail on join protocol
    - Protocol flows
    - Design considerations
- Security assumptions and threat model:
  - Security-first approach, tailored towards 6TiSCH-typical constraints (e.g., minimization protocol flows)
  - Initial set-up *description*, assuming public-key -based crypto

    NOTE: Model also fits PSK-approach
- Routing model:
  - Communication path between Join Assistant and "server"

    No need to be secured (simply "should be there")

… and Next Draft

- Next draft:
  - Include description when current initial set-up requirements not met
    - This includes out-of-sync behavior (no cert, etc.)
    - This includes non-public-key based approach (“PSK”)
- Join Protocol:
  - Add details (formats, byte count, etc.)
- Security assumptions and threat model:
  - TO-DO: Study impact “relaxing” security conditions
  - TO-DO: Include description of non-public-key based approach
  - TO-DO: Add more details on initial keying and (deployment lifecycle)
  - TO-DO: Add text on privacy considerations
  - TO-DO: Add material on impact key compromise, etc.
- Routing model:
  - TO-DO: Add IPv6-addressing-related detail
  - TO-DO: Add more details on network discovery, etc.

Final Note

Plethora of drafts circulating in various IETF groups can be unified, as extension of current join protocol model:

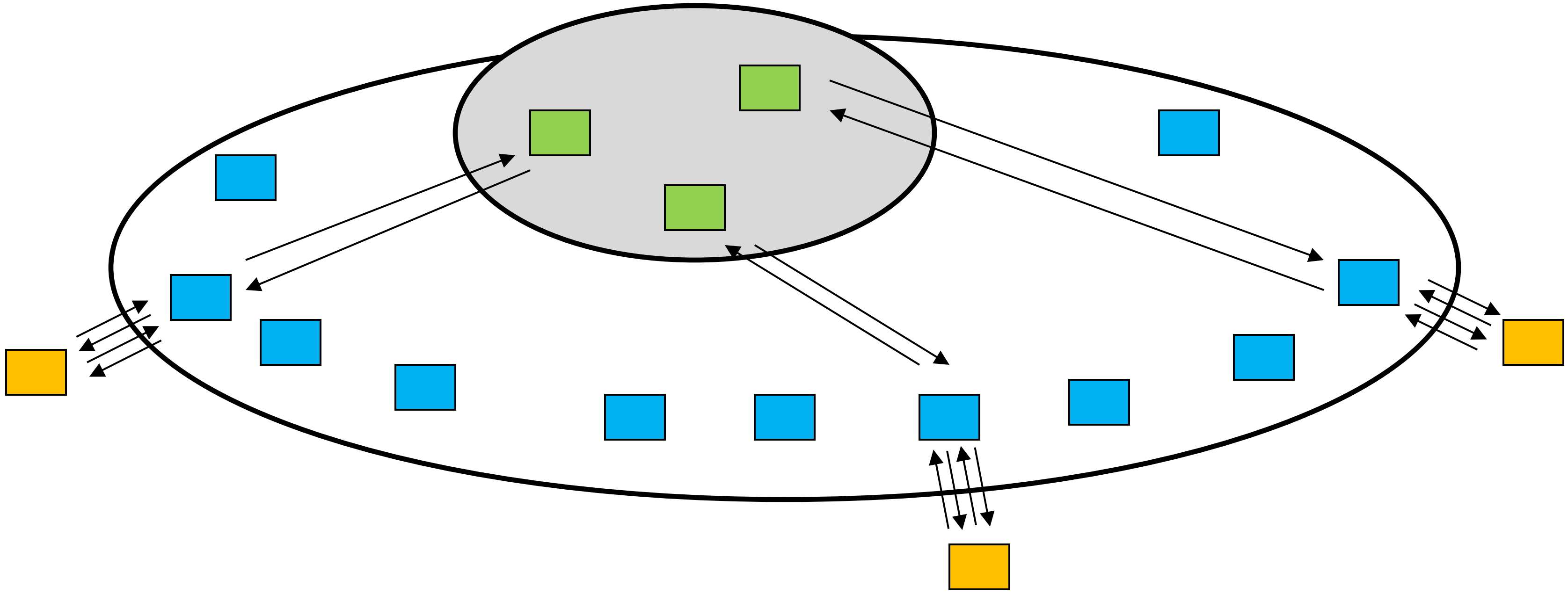
- 6TiSCH, 6lo, Anima, etc.

Flexible use cases can be supported, including:

- Random provisioning order
- Sequential provisioning order

Most differences can be captured with security policy “profile”

Network Joining (4a)



The “big picture”... But now with multiple servers

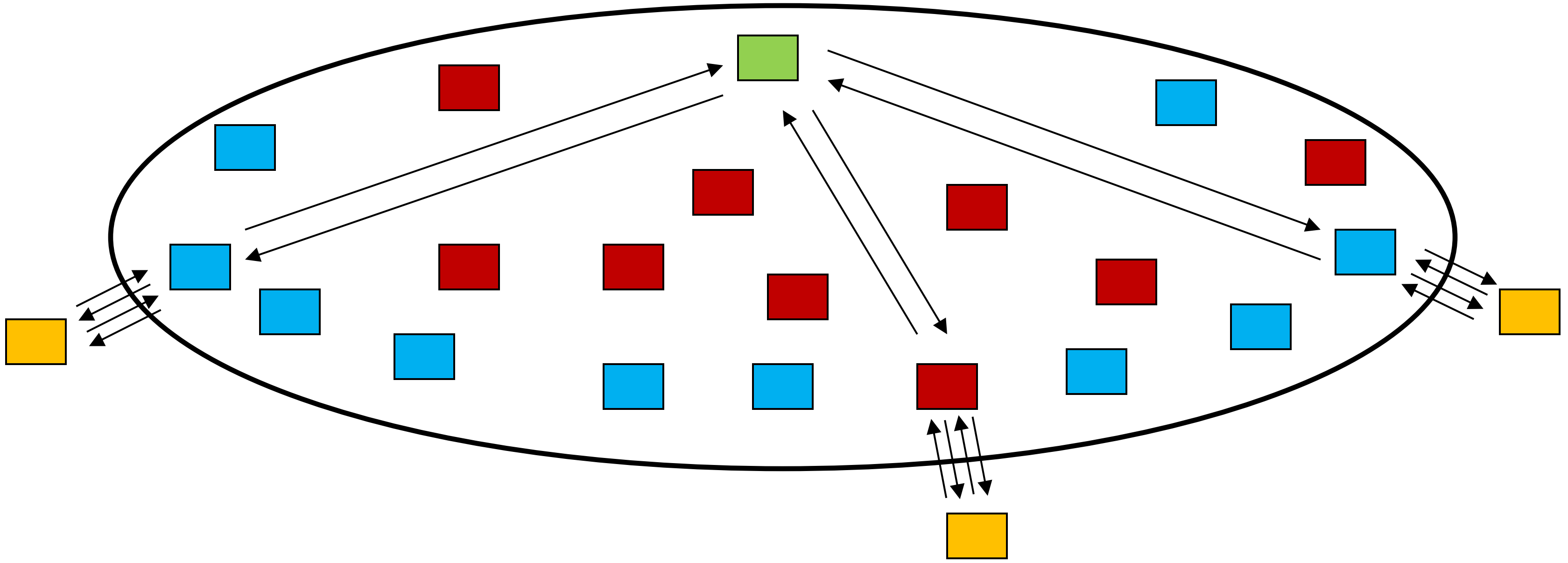
🟨 Joining node

🟦 Neighbor node

🟩 Server, etc.

This facilitates distributed/decentralized schemes

Network Joining (4b)



The “big picture”... But now with sprinkled-in initial provisioning nodes (aka “throw-away nodes)

This facilitates “random” provisioning order use cases

🟨 Joining node

🟦 Neighbor node

🟩 Server, etc.

🟥 Sprinkled-in Router

Wrap Up session 1

Wrap-up for Rechartering

- DetNet
  - – Mature requirements
  - – Elaborate architecture
  - – Continue incubation or spinoff?
- Security
  - – Mature join model – Charter the work?
  - – Should we document PSK? In what form?
  - – Relation with other IoT security work

Any Other Business?

Thank you!