BNG - Control & User Plane Separation Protocol Requirements

draft-wadhwa-rtgwg-bng-cups-protocol-requirements-00

Sanjay Wadhwa - Nokia

Killian De Smedt - Nokia

Rajesh Shinde – Reliance Jio

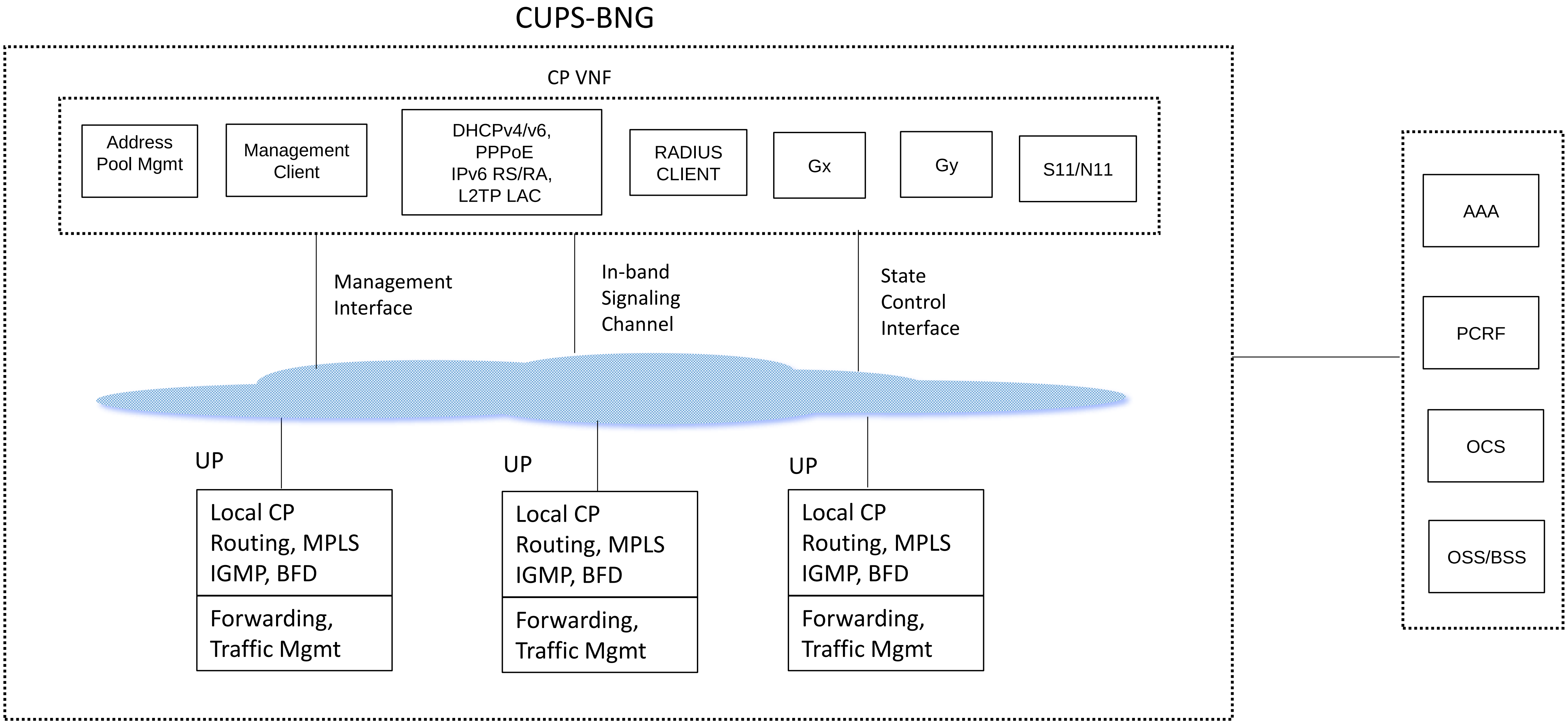
Jonathan Newton - Vodafone

Ryan Hoffman - TELUS

Subrat Pani – Juniper Networks

Praveen Muley - Nokia

CUPS – Functional Decomposition



“CUPS protocol” Requirements

1. Baseline “state control interface”
2. Extensibility
3. In-band control channel
4. Scalability & Performance
5. Transport Protocol
6. Resiliency
7. Security

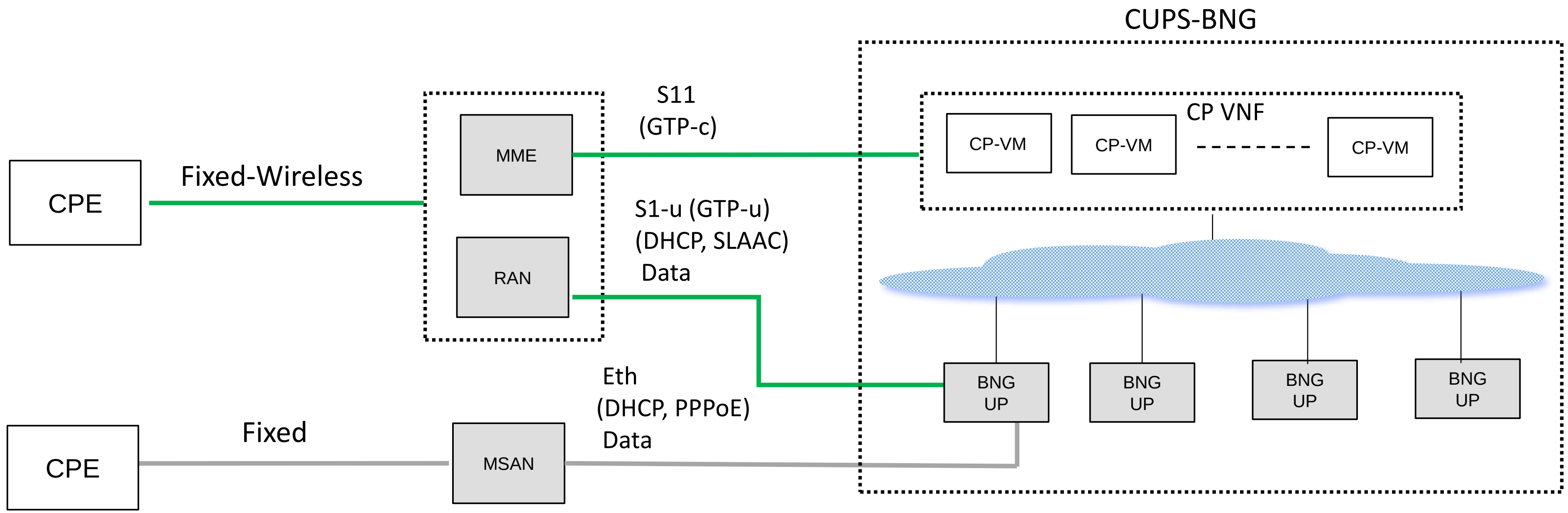
State Control Interface – "CUPS protocol" Requirements

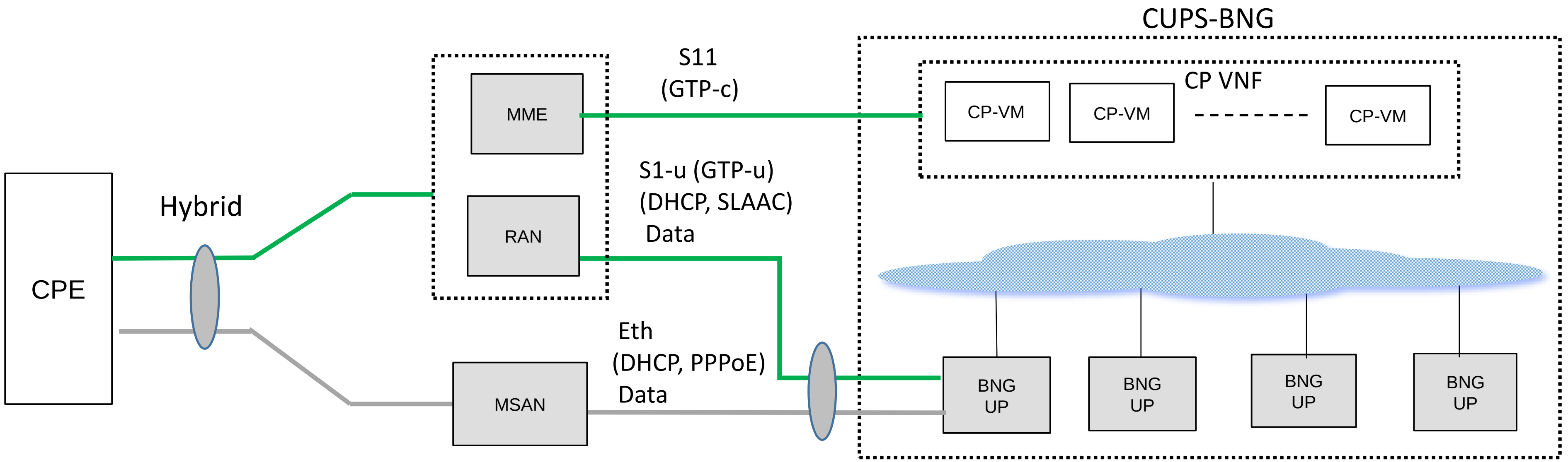
- "CUPS protocol" MUST support downloading forwarding, traffic management and SLA management related state from CP to UP for subscriber sessions.
- MUST support fixed, fixed-wireless and hybrid access.
- MUST support IPoE (IPv4 and IPV6) and PPPoE subscriber sessions. For PPPoE sessions, both PPP termination and tunneling (L2TP) MUST be supported.
- MUST work for subscriber sessions transported to the BNG over L2 connection or L3 tunnels. Common access encapsulations that MUST be supported for fixed-access include Ethernet (.1q or q-in-q), MPLS PW, L2oGRE, L2TPv3 and VxLAN. For Fixed-wireless sessions over GTP-u tunnels MUST be supported.
- MUST allow CP to specify forwarding and traffic management state for subscriber sessions as flexible packet matching rules and actions rather than fixed format lookup tables tied to UP implementation.
- MUST allow CP to specify subscriber routing and IP interface related information.
- MUST provide support for CP to specify QoS parameters (e.g. rates, queues, markings) and the QoS hierarchy to which the CPE belongs, to the UP.

State Control Interface – “CUPS protocol” Requirements

- MUST support a liveness detection between CP and UP based on periodic heartbeat exchange mechanism.
- MUST support asynchronous session level event notifications from UP to CP. Examples (periodic usage-reporting, threshold based usage reporting, subscriber un-reachability detection, inactivity timeout etc).
- MUST support asynchronous node level event notifications from UP to CP.

CUPS BNG – Deployment Scenarios (Fixed/Fixed-Wireless/Hybrid Access)





Protocol Extensibility

- “CUPS protocol” MUST encode information elements (IE) in messages as TLVs.
- MUST allow addition of new IEs in existing messages.
- MUST allow adding new information to existing IEs while maintaining backwards compatibility.
- MUST support vendor specific IEs by partitioning TLV type space for vendor specific extensions.
- MUST support graceful handling of unknown TLVs. Allows CP to send new non-mandatory TLVs to UPs.

In-Band Signaling Channel - Requirements

- “CUPS protocol” MUST support dynamically setting up the control channel between UP and CP to transport in-band control protocol messages (e.g. DHCPv4, DHCPv6, PPPoE) between UP and CP.
- UP MUST pass signaling messages received from CPE unmodified to CP over control channel.
- UP MUST pass unmodified the signaling (response) messages from CP over control channel to CPE.
- UP MUST signal “access circuit ID” as meta-data with messages passed to CP.
- UP MUST pass received Ethernet frame to CP. UP MUST pass local MAC@ to CP. CP MUST encapsulate response messages and pass the Ethernet frame to UP.
- The in-band signaling channel MUST support converged access.
    - It MUST therefore support transporting both Ethernet and IP payloads.
- CP MUST be able to indicate to UP specific message types that MUST be sent to CP over signaling channel.
- CP MUST be able to dynamically instruct UP to block certain messages over a signaling channel.
- CP MUST be able to control the UP to limit the rate of control messages (on a per message-type basis) sent to the CP.
- CP MUST be able to control the relative priority with which the UP sends certain control messages (e.g. prioritize DHCP Renews over Discovers, or PPP Keepalives over PADI).

Scalability & Performance

- "CUPS protocol" MUST minimize latency to bring subscribers online even during events triggering a high rate of subscriber creation and teardown.
- SHOULD limit "chattiness" by minimizing message exchange (request/response round-trips) between CP and UP to create subscriber sessions.
- MUST support graceful handling on UP under overload. SHOULD support signaling of overload state and optionally overload mitigation parameters from UP to CP).
- MUST allow dynamic scale-out of CP VNF with the growth in subscriber scale of the CUPS system.
- MUST allow mechanism for balancing of processing load amongst compute resources of control-plane VNF that supports dynamic scale-out.
- SHOULD optimize amount of information passed where possible (e.g. if forwarding actions or QOS enforcement is shared for multiple sessions, then this should be passed by reference after initial creation).

Transport Protocol

- Transport protocol used by “CUPS protocol” MUST NOT suffer from HOL blocking.
- SHOULD preserve message boundary with datagram semantics.
- SHOULD be available or easily implementable in simple forwarding devices.
- “CUPS protocol” over this transport MUST support reliability of message exchange via request/response transactions and retransmissions.

Resiliency

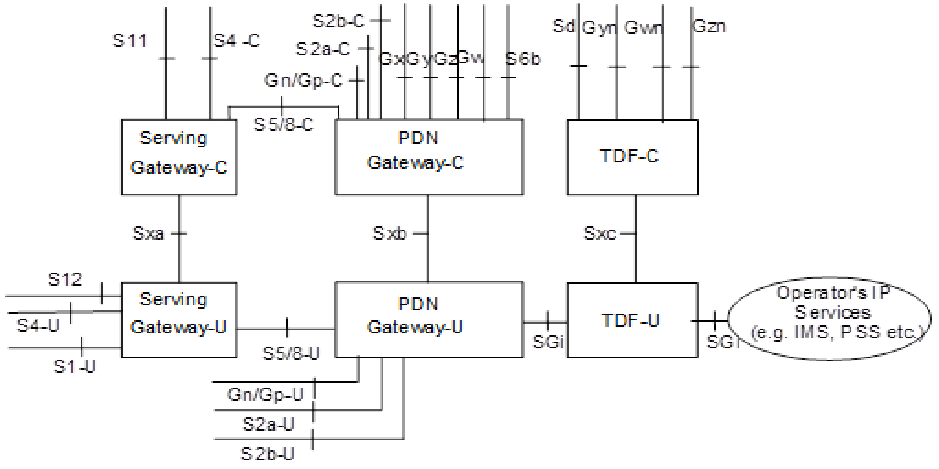
- “CUPS protocol” MUST allow support for 1:1 (hot-standby) and SHOULD allow support for N:M (warm-standby) UP node level redundancy.
- "CUPS protocol" MUST provide support for CP to specify the redundancy domain" that a subscriber session is associated with during session level state creation on the UP.
- The "CUPS protocol" MUST provide support for UP to notify the CP about switchover event. This notification must be on the granularity of "redundancy domain" on a UP.
- For warm standby redundancy, "CUPS protocol" MUST provide support for CP to create session level state on the backup UP
- “CUPS protocol” MUST support CP level redundancy without impact on subscriber sessions in case of failure of CP-VNF resources (e.g. failure of VM that provides control plane processing as part of CP-VNF).

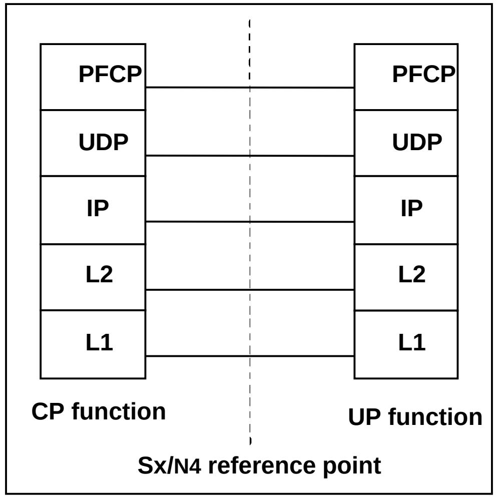
Security

- “CUPS protocol” MUST be compatible with proven security mechanisms such as (D)TLS or IPSEC to provide:
    - Data-integrity and confidentiality for information exchanged via "CUPS protocol“
    - Protection against man-in-the-middle attacks.
    - Anti-replay protection MUST be provided.

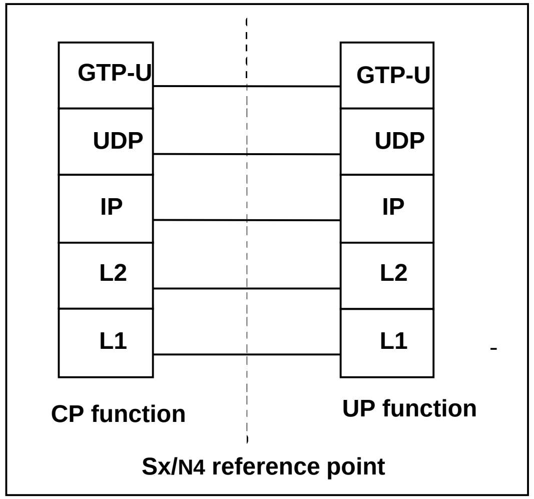
Protocol Selection Input

- 3GPP has already defined a protocol for CUPS between gateways – PFCP (Packet Forwarding Control Protocol) in [TS 29.244].
- The protocol machinery is purpose built for large scale state management between CP and UP.
- The containers used to convey forwarding state, QOS enforcement, usage-reporting are defined generically and can be applied to state relevant to BNG.
- Requires extensions in the form of new IEs or extending a small subset of existing IEs for BNG, mainly for :
  - L2 access that is typical for BNG, and IP/Routing interactions on UP specific to BNG (e.g. prefix aggregation, Gateway IP for CPEs).
- PFCP IEs are extendable and defined as TLVs.
- The 32 bit number space for TLV types is already partitioned into "3GPP specified" and "vendor specified". BNG specific TLVs can be defined by IETF or IANA.
- Extend PFCP for BNG CUPS:
  - Allows convergence
    - Multiple access types (Fixed, FWA, Hybrid) on BNG upfront.
    - In future will allow fixed broadband integration with 5GC (as defined in BBF SD-407).
    - Provides the possibility of "unified" CP to control different UPs (e.g. BNG on PNF, EPC or 5GC elements on VNF).
  - Provides a scalable and hardened/deployed baseline. No need to reinvent the wheel
- Consider undertaking protocol extensions to PFCP for CUPS BNG in IETF RTGWG





PFCP Protocol Stack



PFCP User-Plane for In-Band Control Protocol Messages

Future Work

- Add more details on requirement for management interface between CP and UP for configuration and state.
- Define protocol extensions (e.g. IE extensions , new IEs) required to realize BNG CUPS.

Thank you