BNG - Control & User Plane Separation Architecture, Requirements & Interfaces

draft-wadhwa-rtgwg-bng-cups-01.txt

Authors: Sanjay Wadhwa (sanjay.wadhwa@nokia.com)
          Killian De Smedt (Killian.de_smedt@nokia.com)
          Rajesh Shinde (Rajesh.A.Shinde@ril.com)
          Jonathan Newton (jonathon.newton@vodafone.com)
Why CUPS on BNG?

- Allows control and data plane to scale independently.
- **Flexible placement of control plane and data plane elements**
  - Data plane for BNG can be distributed e.g. if CDN caches are distributed.
  - Control plane can be centralized.
  - Control plane as VNF. Data plane can be PNF or VNF.
- **Operational Simplicity**
  - Single point for management and control for cluster of BNGs.
  - Single interface towards external systems (AAA servers, PCRF, OCS, OSS/BSS).
- **Convergence of BNG control plane with session management (control plane) functions in 4G/5G packet core**
  - BNG terminating fixed, fixed-wireless and hybrid access.
  - BBF and 3GPP defining converged architecture for 5G (fixed access integrated or interworked with 5G core).
  - CUPS is de facto in EPC and 5GC.
CUPS BNG – Deployment Scenarios (Fixed/Fixed-Wireless/Hybrid Access)

Fixed-Wireless

CPE

Fixed

CPE

Hybrid

CPE

MME

S11 (GTP-c)

S1-u (GTP-u) (DHCP, SLAAC) Data

Eth (DHCP, PPPoE) Data

CP-VM

CP VNF

CP-VM

BNG UP

BNG UP

BNG UP

BNG UP

CP-VM

BNG UP

BNG UP

BNG UP

CP-VM

BNG UP

BNG UP

BNG UP

MME

RAN

MSAN

S1-u (GTP-u) (DHCP, SLAAC) Data

Eth (DHCP, PPPoE) Data

CPE

S1-u (GTP-u) (DHCP, SLAAC) Data

Eth (DHCP, PPPoE) Data

CPE

CPE

CPE

CPE

CPE

CPE

CPE

CPE
CUPS – Functional Decomposition

CUPS-BNG

CP VNF

Address Pool Mgmt
Management Client
DHCPv4/v6, PPPoE IPv6 RS/RA, L2TP LAC
RADIUS CLIENT
Gx
Gy
S11/N11

Management Interface
In-band Signaling Channel
State Control Interface

Local CP Routing, MPLS IGMP, BFD
Forwarding, Traffic Mgmt

Local CP Routing, MPLS IGMP, BFD
Forwarding, Traffic Mgmt

Local CP Routing, MPLS IGMP, BFD
Forwarding, Traffic Mgmt

AAA
PCRF
OCS
OSS/BSS
State Control Interface – Session-Level State Management

- CPE
- UP
- CP
- AAA

Flow Diagram:
- DHCP Discover → DHCP Offer → DHCP Request → DHCP ACK
- In-Band Signaling Channel
- Access Request → Access Response
- Session Creation Request → Session Creation Response
- Upstream/Downstream Forwarding State Installed
State Control Interface - Session Level State Management

Session Modification - Triggers
- RAIDUS COA
- Gx RAR
- Administrative action
- Credit Control

Session Deletion - Triggers
- CPE Initiated (DHCP Release, PPPoE PADT)
- Timeouts (DHCP lease, PPP KA)
- Inactivity Detected
- Subscriber Unreachability Detected
- RAIDUS initiated disconnect
- Administrative action
- End of Credit Action
State Control Interface - Session Level Event Notification

Examples of Session Level Notifications
- Periodic Usage Reporting
- Threshold Based Usage Reporting
- Inactivity Timeout
- Subscriber Unreachability Detected

Examples of Node Level Management
- Association Establishment (capabilities, s/w release, load/overload information, resource info etc)
- Periodic Heartbeats (for liveness detection)
- Asynchronous notifications (e.g. to report switchover)
State Control Interface – Session Level State Management

Packet Detection Rule (Upstream: Access->Network)
Match Rule
- Port/VLAN-Tag(s)
- MAC@
- [Session-ID]
- [IPv4@ / IPv6@ / IPv6 Prefix]
Action: Remove L2 Encaps, IP FIB Lookup, Fwd to network

Packet Detection Rule (Downstream: Network -> Access)
Match Rule
- IPv4 @ / IPv6 @ /IPv4 prefix / IPv6 prefix
Action: Add Encaps { Port/VLAN-Tag(s), Subscriber MAC, [Session ID] }, Fwd to Access

Routing Info
- IPv4/v6 Address, Prefix Length
- Gateway IP Address
- Aggregation Prefix

QoS Info
- Local QoS Profile
- MBR/CBR
- Markings...

Usage Reporting Info
- Reporting Triggers
- Time thresholds, quotas.
- Volume thresholds, quotas
State Control Interface – Protocol Requirements

• MUST allow fixed, fixed-wireless (4G/5G) and hybrid access on BNG.
• MUST support tunneled/non-tunneled, L2/L3 access.
• Underlying transport SHOULD not have HOL Blocking.
• MUST support application level reliability (request/response mechanism).
• MUST be extensible (messages MUST support carrying Information Elements as TLVs).
• MUST allow vendor specific extensions.
• SHOULD minimize “chatiness” (e.g. minimize message round-trips to create session state on UP)
• MUST support setting of in-band signaling channel between CP and UP.
• MUST support state management for forwarding state, QOS enforcement, and usage-tracking (both periodic and threshold based).
• MUST support asynchronous notifications from UP to CP.
• MUST support graceful handling under overload (e.g. via temporary message throttling from CP to UP under overload).
• MUST support liveness detection between CP and UP.
• MUST support mechanisms for CP and UP redundancy.
• 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).
In-Band Signaling Channel - Requirements

- UP MUST pass signaling messages received from CPE unmodified to CP.
- UP MUST pass unmodified the signaling (response) messages from CP 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.
- In-Band Signaling Channel MUST be dynamically setup between CP and UP via signaling.
- 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).
- The in-band signaling channel MUST support converged access.
  - It MUST therefore support transporting both Ethernet and IP payloads.
**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.
Thank you