Application-aware Networking (APN)

Shuping Peng, Zhenbin Li
Huawei Technologies
Application is the program installed in user terminals or hosts, such as WhatsApp and Youtube, etc.

App-Info is application characteristic information, including application identifier, SLA requirements, etc.

App-Info can be encapsulated directly by the applications, or derived at network edge devices, or via QinQ, etc.
APN Key Elements

Open App-Info
(carried based on Agreements)
- App-aware ID
  - SLA
  - APP ID
  - User ID
  - Flow ID
  - ...
- Service-para
  - Bandwidth
  - Delay
  - Jitter
  - Packet Loss
  - ...

Rich Network Services
(enhanced with app awareness)
- SLA Guarantee
- Network Slicing
- Deterministic Networking
- SFC

Accurate Network Measurement
- Fine granularity matching and optimization
- Comprehensive measurements
Work Items in APN

- New Services:
  - App-aware Network Slicing
  - App-aware Detnet
  - App-aware SFC
  - App-aware Network Measurement
  - Fine-granularity SLA Guarantee

- Architecture:
  - Application-aware Networking Framework
  - Functional Components
  - Security
  - Privacy

- Automation / Control Plane (Provisioning & Management):
  - Routing Plane (IGP/BGP)
  - PCEP
  - BGP-LS
  - YANG
  - ...

- Data Plane:
  - Encapsulation
    - IPv6
    - SRv6
    - MPLS
    - VxLAN
    - ...

- Application-aware ID

- Key:
  - New Work
  - Work Possibly Needing Extensions

- Annotations:
  - Work Items in APN
  - Privacy
  - Possibly Needing Extensions
  - Key
  - Fine-granularity SLA Guarantee
  - QoS
App-Info is injected into the network to describe the service and behavior needed by the application.
APN Scope - APN vs. PANRG

AAI (Application-aware Internet)

The scope of APN

APN
Application-aware Network

APP
Edge Device

Network

APP Info

APP
Edge Device

APP

PANRG
Path-aware Networking

APP

Network

Network Info

APP

APP
APN6 Hackathon @IETF108

- **Champion(s)**
  - Weihong Wu <lara@...>
  - Jiang Liu <liujiang@...>
- **Project(s)**
  - The implementation of a demo of APN6. The implementation is based on P4 and BMv2
  - The encapsulation of 2 types of Application-aware ID Options and 4 types of Service-Para Sub-TLVs
  - The SRv6-based traffic control according to IPv6 DA, Application-aware ID Options, and Service-Para Sub-TLVs
- **Specifications:**
APN Side Meeting @IETF108

Chairs: Zhenbin Li, Daniel King

Date: 12:30-14:00 UTC, Thursday, 2020-07-30

Webex: https://github.com/APN-Community/IETF108-Side-Meeting-APN

Tentative Agenda

- Introduction & Agenda Bashing (5 mins)
- Attempts in IETF History (15 mins)
  - What attempts (SPUD and PLUS BoFs)? What lessons learned?
- Requirements on Application-awareness in Networks (20 mins, 5 mins each)
  - Operators present their use cases to make clear that they have the Requirements on Application-awareness in their Networks
  - Bell Canada – Service/Application aware
  - Telefonica – CDN
  - China Mobile – MEC
  - China Unicom – Game Acceleration
- APN Framework (5 mins)
  - Introduce APN Framework and the available Demo, Hackathon, INFOCOM, etc.
- Acquisition, Encapsulation and Conveying of Application-related Information (30 mins)
  - Network Tokens
  - FAST
  - APN6
- Discussions & Clarifications – Collecting views from the IETF community (10 mins)
  - Whether it will bring privacy issue? If yes, how to overcome?
  - Whether it will bring security issue? If yes, how to overcome?
- Conclusion – the way forward (5 mins)
Privacy Issues

1. **No privacy issue**: Operators run their own applications – e.g. CMCC MIGU Music
2. **No privacy issue**: App providers build and run their own networks – e.g. Google B4
3. **No privacy issue**: APN works only within an operator’s controlled limited domain no matter where the App-info is added and encapsulated.
4. **No privacy issue**: If added at the edge device (i.e. an network operator-controlled device), e.g. Enterprise CPE or Home broadband RG or BNG or WiFi AP or 5GC UPF.
5. **No privacy issue**: If added at the APP, the App-info is encrypted.
6. **May have privacy issue**: If added at the APP, the explicit App-info is not encrypted.
Security Issues

- No Security Issue: Inter-DC scenario
- No Security Issue: Enterprise scenario, access through a controlled BNG interface
- APN only imposes security issues when users access from an untrusted domain, but
  - **Home broadband scenario** can be validated via BNG
  - **Mobile broadband scenario** can be validated via 5GC
- APN potentially imposes four types of security issues
  1. Within one terminal – can be tackled via OS; blocked via BNG or 5GC
     a) An application in one terminal (UE) adds arbitrary App-Info (incl. Request)
     b) An application in one terminal adds the App-Info of the other App in the same terminal
  2. Once sent out it will be validated via Network-side security solutions
     a) An application in one terminal forges the App-Info of the same App in another terminal
     b) App-Info is tampered along the way between the App-Info creator and the Network Boundary
APN Related Information

• Problem statement & Use cases:
  • https://tools.ietf.org/html/draft-liu-apn-edge-usecase-00
  • https://tools.ietf.org/html/draft-zhang-apn-acceleration-usecase-00

• Framework

• Requirements on Application-awareness in Networks

• APN Community including Information about APN6 Side meetings
  • https://github.com/APN-Community
  • https://github.com/APN-Community/IETF105-Side-Meeting-APN6
  • https://github.com/APN-Community/IETF108-Side-Meeting-APN
Thank you for your attention!