

Network Working Group
Internet-Draft
Intended status: Informational
Expires: December 19, 2021

S. Peng
Z. Li
Huawei Technologies
D. Voyer
Bell Canada
C. Li
China Telecom
P. Liu
China Mobile
C. Cao
China Unicom
June 17, 2021

APN Security and Privacy Considerations
draft-peng-apn-security-privacy-consideration-02

Abstract

Application-aware Networking (APN) aims to convey Application-aware Information (APN attribute) including APN ID and APN parameters indicating application group-level and user group-level requirements along with the data packets into the network and enable the network to provide corresponding fine-granular network services.

There have been challenges of the privacy and security issues that could potentially be introduced by conveying the APN attribute into the network. This document describes the security and privacy considerations of APN in various possible scenarios wherein APN will be deployed.

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <https://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on December 19, 2021.

Copyright Notice

Copyright (c) 2021 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

| | |
|--------------------------------------|---|
| 1. Introduction | 2 |
| 2. Terminologies | 3 |
| 3. APN Framework | 3 |
| 4. Privacy Considerations | 4 |
| 5. Security Considerations | 4 |
| 6. IANA Considerations | 6 |
| 7. Contributors | 6 |
| 8. Normative References | 7 |
| Authors' Addresses | 7 |

1. Introduction

Application-aware Networking (APN) is introduced in [I-D.li-apn-framework] and [I-D.li-apn-problem-statement-usecases]. APN conveys Application-aware Information (APN attribute) along with data packets into network and make the network aware of applications' requirements in order to provide corresponding network services. The ever-emerging network services such as network slicing and iOAM can be further enhanced with the application awareness in the network enabled by APN.

Since APN conveys an APN attribute along with the data packets into network, APN has been challenged that it may potentially impose privacy and security issues.

This document describes the privacy and security considerations of APN.

2. Terminologies

AI: Artificial Intelligence

APN: Application-aware Networking

BNG: Broadband Network Gateway

CPE: Customer Premise Equipment

DPI: Deep Packet Inspection

OS: Operating System

RG: Residential Gateway

UPF: User Plane Function

5GC: 5G Core

3. APN Framework

The APN framework is introduced in [I-D.li-apn-framework], as shown in the Figure 1.

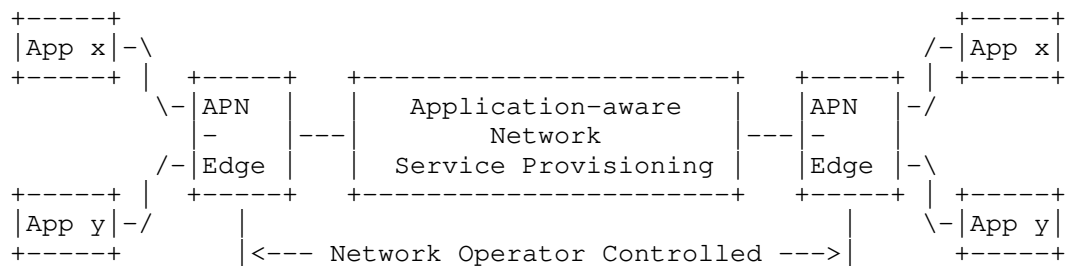


Figure 1. APN6 Framework

With APN, the APN attribute is acquired based on the existing information in the packet header such as 5-tuple and/or QinQ (S-VLAN and C-VLAN) at the edge devices of the APN domain (i.e. APN-Edge in the Figure 1), added to the data packets in the tunnel encapsulation, and delivered to the network, wherein, according to the carried APN attribute, the fine-granular network services are provisioned.

The APN attribute is added by the edge device of an APN domain according to the local policy at the network edge device (i.e. APN-Edge), which is under the control of the network operator.

4. Privacy Considerations

The APN attribute is only used within the network operator's controlled limited domain. A limited domain is intended as a portion of the operator infrastructure where APN is deployed. When a packet reaches the boundary of the limited domain, an APN attribute is added to the packet, used in order to steer the packet within the limited domain and then removed when the packet leaves the limited domain.

Within the APN network domain, the APN attribute is added at the ingress node and removed from the egress node. In the APN network domain, the APN attribute only serves for the fine-granular network service provisioning, and there is no harm for the outside of the APN network domain.

5. Security Considerations

There are two typical scenarios besides the SD-WAN scenario described in the draft [I-D.yang-apn-sd-wan-usecase]: the home broadband scenario and the mobile broadband scenario.

In the home broadband scenario, generally a home broadband user is authorized by the BNG. If the validation is passed and the access control is released, so the user group can start enjoying the value-added service. With APN, when the traffic traverses the metro network, the traffic flow can be indicated by the APN attribute that is added/removed at the edge devices of the Metro Network (APN domain) based on the mapping from the existing information (e.g. the QinQ which is composed of C-VLAN and S-VLAN) in the packet header and then carried in the tunnel encapsulation header. The APN attribute will facilitate the fine-granular service in the APN domain. Once the packets leave the APN domain, the APN attribute will be removed together with the tunnel encapsulation header.

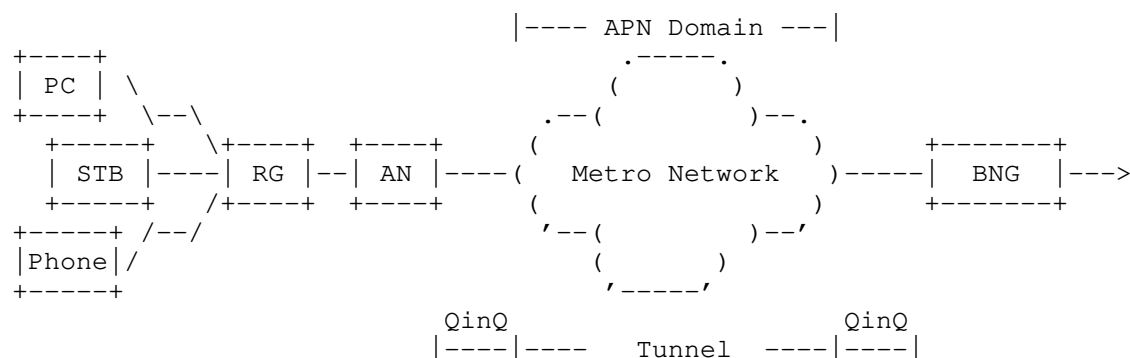


Figure 2. Home Broadband Scenario

In the mobile broadband scenario, a UE is authorized by the 5GC function, and the traffic steering and QoS policy are enforced by the UPF (User Plane Function) node. If the validation is passed and the access control is released, so the user can start enjoying the value-added service. With APN, when the traffic traverses the mobile transport network, the traffic flow can be indicated by the APN attribute that is added at the edge devices of the mobile transport network (APN domain) based on mapping from the existing information (e.g. GTP-u tunnel encapsulation information) in the packet header and then carried in the tunnel encapsulation header. The APN attribute will facilitate the fine-granular service in the APN domain. Once the packets leave the APN domain, the APN attribute will be removed together with the tunnel encapsulation header. In fact, the APN attribute can also be acquired at the gNB based on the mapping of the existing information of the packet header (e.g. 5-tuple information) and carried along with the GTP-u tunnel encapsulation. The mobile transport network can provide the corresponding service according to the APN attribute. When the packet leaves the UPF, the APN attribute can be removed together with the GTP-u tunnel encapsulation.

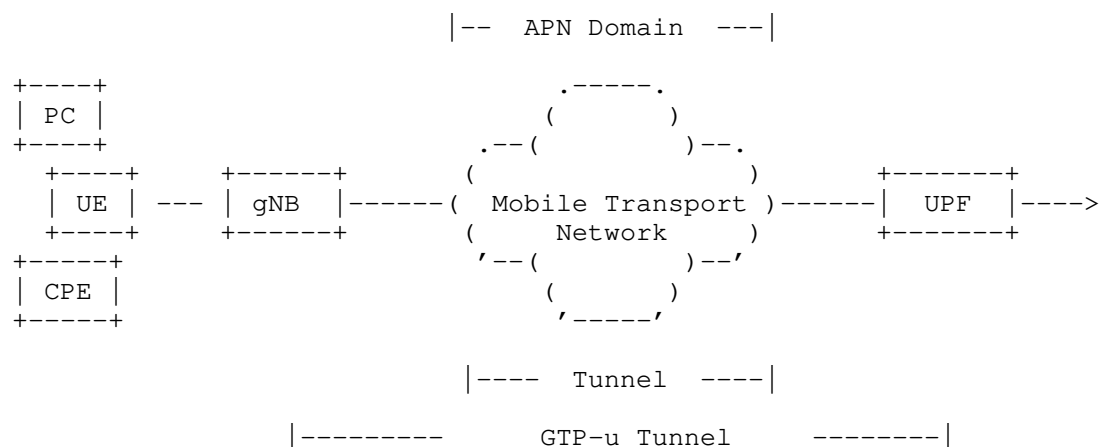


Figure 3. Mobile Broadband Scenario

In the typical APN scenarios like the home broadband scenario and the mobile broadband scenario, before the traffic is delivered to the network domain, the end user must be authenticated and authorized firstly to guarantee the security of the network domain. When the traffic traverses the APN domain, the APN attribute is added and removed at the edge of the APN domain along with the tunnel encapsulation. That is, the APN attribute is only used locally in the APN domain and will not introduce the extra security issues.

6. IANA Considerations

There are no IANA considerations in this document.

7. Contributors

Chongfeng Xie
China Telecom
China

Email: xiechf@chinatelecom.cn

Liang Geng
China Mobile
China

Email: gengliang@chinamobile.com

Shuai Zhang
China Unicom
China

Email: zhangs366@chinaunicom.cn

8. Normative References

[I-D.li-6man-app-aware-ipv6-network]

Li, Z., Peng, S., Li, C., Xie, C., Voyer, D., Li, X., Liu, P., Cao, C., and K. Ebisawa, "Application-aware IPv6 Networking (APN6) Encapsulation", draft-li-6man-app-aware-ipv6-network-03 (work in progress), February 2021.

[I-D.li-apn-framework]

Li, Z., Peng, S., Voyer, D., Li, C., Liu, P., Cao, C., Ebisawa, K., Previdi, S., and J. N. Guichard, "Application-aware Networking (APN) Framework", draft-li-apn-framework-02 (work in progress), February 2021.

[I-D.li-apn-problem-statement-usecases]

Li, Z., Peng, S., Voyer, D., Xie, C., Liu, P., Qin, Z., Ebisawa, K., Previdi, S., and J. N. Guichard, "Problem Statement and Use Cases of Application-aware Networking (APN)", draft-li-apn-problem-statement-usecases-01 (work in progress), September 2020.

[I-D.yang-apn-sd-wan-usecase]

Yang, F., Cheng, W., Peng, S., and Z. Li, "Usage scenarios of Application-aware Networking (APN) for SD-WAN", draft-yang-apn-sd-wan-usecase-01 (work in progress), February 2021.

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

Authors' Addresses

Shuping Peng
Huawei Technologies
Beijing
China

Email: pengshuping@huawei.com

Zhenbin Li
Huawei Technologies
Beijing
China

Email: lizhenbin@huawei.com

Daniel Voyer
Bell Canada
Canada

Email: daniel.voyer@bell.ca

Cong Li
China Telecom
China

Email: licong@chinatelecom.cn

Peng Liu
China Mobile
China

Email: liupengyjy@chinamobile.com

Chang Cao
China Unicom
China

Email: caoc15@chinaunicom.cn