RTGWG
Internet-Draft
Intended status: Standards Track
Expires: 29 June 2026

F. Yang
China Mobile
C. Lin
New H3C Technologies

26 December 2025

Application-Responsive Network Framework
draft-yang-rtgwg-arn-framework-05

Abstract

With the deployment of increasingly advanced technologies on a large scale, such as SRv6 and network slicing, there is a growing need to expose these new capabilities to applications. The current practice involves using ACLs to classify packets and then map the traffic onto appropriate network resources. This approach results in the application being passively perceived by the network, rather than the application actively interfacing with the network. Furthermore, changes in application characteristics necessitate triggering network configuration adjustments, making it challenging to deploy at scale.

The document proposes a new framework called Application Responsive Network (ARN), by encapsulating more network functions into ARN ID, thus it opens up interfaces to applications. The vision is to enable applications to access network resources like they access an operating system.

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 29 June 2026.

Table of Contents

1. Introduction

With the widespread application of new technologies such as 5G, cloud computing, big data, and AI, network traffic patterns are becoming increasingly complex and diversified. Various emerging services have higher requirements for QoS parameters such as network latency, bandwidth, jitter, and packet loss.

Networks typically need to prioritize critical services. For example, in office networks, video conferencing requires network priority to ensure that video and voice services do not experience buffering and excessive delays. However, the applications used for video and voice services may vary in different industries and office network scenarios, so it is necessary to identify these applications to further ensure the quality of service.

Some specific services have explicit SLA (Service Level Agreement) requirements. In business scenarios such as autonomous driving, industrial control, and remote control, there are clear SLA requirements for the network, such as latency not exceeding 50ms and jitter not exceeding 1ms.

In traditional IP networks, ACLs are typically used on critical network devices to implement application identification and policy configuration. Based on packet characteristics such as the five-tuple, network can provide guaranteed service for specific users or applications. Different network services have their own ACL matching entries and policies, which need to be continuously adjusted as services evolve. Over time, configurations become invalid due to not being revoked or modified in a timely manner. This is not sufficient for general solution.

This article proposes a new framework called Application Responsive Network (ARN), which abstracts and represents personalized network services based on user demand awareness, provided through ARN Service identifiers (ARN IDs). Network services can be encapsulated by ARN IDs, thus it can be called by user. The vision is to enable applications to access network resources like they access an operating system.

The application here can be network service implemented on a gateway or software that can program the ARN ID.

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

1.2. Terminology

ARN: Application-Responsive Networking

ACL: Access Control List

Subscriber: the user who subscribed a network service, which can be represented by an ARN ID

2. Gaps

There are still the following key gaps in current network technology:

Application-aware features. It is necessary to provide differentiated services based on the different services of the same user. For example, video conferencing needs to avoid stuttering or screen tearing due to congestion and packet loss to ensure a customer experience, while general web browsing services can strive for the best.

Data plane programming capabilities. Identify and classify user application data, and transfer it to the appropriate service-level tunnel based on the results.

Ability to perceive the user experience. Through real-time detection and perception of user-level service experience, it works with intelligent routing to ensure service assurance for high-priority services. Currently, there is a lack of traffic identification for rapid classification and statistical analysis of the user experience of this type of traffic.

Ability to prevent leakage of network services. The security of the access network is relatively poor, and there is a risk of leakage of information related to user applications.

3. Design Goal

As shown in Figure 1, an ARN intermediate layer is added between the application and the network, mapping is accomplished using ARN IDs. The ARN ID is a simple number that encapsulates network capabilities internally and hides network information externally, thus avoiding the exposure of application privacy and facilitating user application invocation.

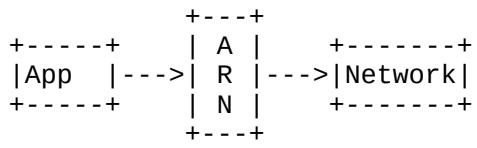


Figure 1: ARN Intermediate Layer Diagram

ARN Network Design Goals:

* Opening network services.

One of the design principles of ARN is to open and program network capabilities based on the data plane. By opening programming interfaces on the data plane in a software-based manner, applications can call network resources like calling an operating system. In today's digital world, user demands for the network far exceed simple connectivity functions. Users expect the network to provide stable, high-speed connections to meet diverse application requirements. Even for the same type of application, usage requirements may vary across different industries and scenarios. Allowing applications to call on network capabilities through data plane programming provides corresponding guarantees for different types of packets.

* Decoupling of addresses and services.

Another design principle of ARN is to decouple addresses and services. Traditional network design is based on addresses, managing and routing based on destination addresses to determine the forwarding services provided by the network. However, with the increasing variety of user applications, relying on addresses to carry service levels has made network management increasingly complex. Therefore, it is necessary to manage and optimize the network based on the characteristics and requirements of user applications, separating addresses from services to provide multidimensional forwarding services.

* Decoupling of network and applications.

The third design principle of ARN is to decouple the network and applications. By adding an ARN layer between the network and applications, the network does not need to directly perceive the applications, thus shielding the diversity of applications and preventing direct access to network capabilities. Through ARN, the network and applications can be encapsulated separately, achieving application privacy and the concealment of internal network information. At the same time, based on this encapsulation, access control can be implemented during the application's network calls, realizing an authorization token-based calling mechanism similar to software programming.

* Unified abstraction of network resources.

The fourth design principle of ARN is the unified abstraction of multiple network resources. With the development of personalized and diversified network services, the network resources used in forwarding user packets are becoming increasingly rich, such as computing power, network slicing, service chaining, and more. During the use of these network resources, additional identifiers are often carried in the packets to determine the mapping relationship between users or applications and network resources, or ACLs are used to parse and match the feature information in the packet to determine the associated network resources. In the ARN network, multiple network resources can be uniformly represented by ARN IDs, reducing the complexity of data plane identifiers and simplifying operational deployments.

4. ARN Framework and Components

ARN Framework, as illustrated in Figure 2, consists of key components including user edge devices, network edge devices, and network controllers at different levels.

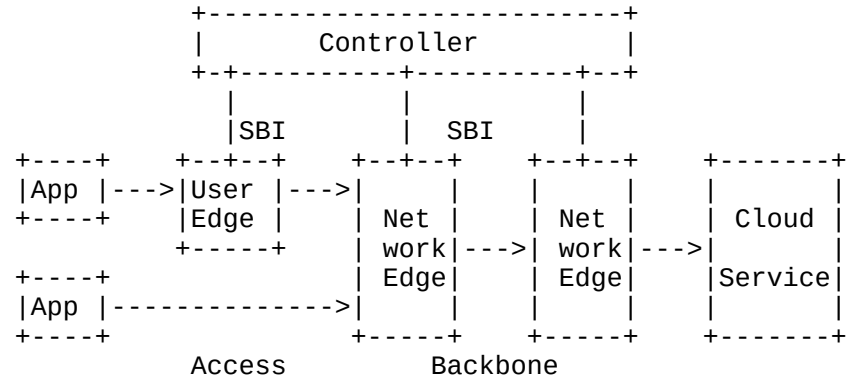


Figure 2: Framework and Key Components

4.1. ARN ID

The ARN ID can be generated by the controller based on the user service subscription information and network service information, and the generated ARN ID will be configured to both user edge devices and network edge devices. User service subscription information may include user information, e.g. PPPoE, and application information, e.g. 5 tuple. The network service information can be pre-planed network pathes, e.g. SR policies.

The ARN ID represents the application’s invocation of network capabilities and/or the network’s ability to be open to the application.

The ARN ID also represents a contractual relationship, and therefore requires lifecycle management of ARN ID, e.g., revocation, loss reporting, replacing, aging, and deferring operations.

A method of allocating ARN ID by PPPoE mechanism is as follows: Firstly, the user edge device such as BRAS sends the configuration request used to query ARN ID which characterizes a service subscribed by a user. The request includes at least one or more of protocol typr, protocol length, and service id based on the pre-set protocol. The network device connected to the user device receives the request according to the pre-set protocol(e.g. NCP) and allocates the configuration with ARN ID to the user device based on the request. According to pre-set service information including service type and identification information of user device, network device determines the service type of user device. Furthermore, it determines ARN ID of the user device based on the said service type information. Secondly, the user device sends the configuration request with ARN ID to confirm that the ARN ID is correct. The network device receives the message and sends the confirmation message to the user device based on the confirmation request, which is used to characterize whether ARN ID is correct. When the ARN ID in the configuration request sended from the user device is matching the ARN ID in the congfiguration information sended from the network device, the network device sends the confirmation message characterizing tha accuracy of ARN ID which is allocated to the user device.

4.2. Application

User applications require networks to provide differentiated services, especially those based on SR technology. There are two scenarios.

The first scenario is that the user’s application supports ARN. By delivering ARN ID to user, user can encapsulate ARN ID for certain application to achieve differentiated services. In this case, the application needs to insert the ARN ID into the extension header of the IPv6 packet.

The second scenario is that the user’s application does not support ARN. In this case, network service provider needs to deliver ARN ID to user edge device and map application traffic to the ARN ID to achieve differentiated services.

4.3. User Edge Device

The user edge devices are responsible for accessing the user applications and are the boundary of the access network. The access network will not be a part of SRv6 or MPLS domains.

The ARN IDs are configured between the user edge device and the network edge device, and the controller only needs to ensure that the ARN ID generated based on different user subscription information and network service information is unique within this range.

4.3.1. ARN ID Marking

The user edge device will identify the relevant IP traffic and mark the packet based on the received ARN ID, and then transmits it to network edge device.The ARN ID may be encapsulated into the extension header of the IPv6 packet, which will be explained in detail in Section 5. In this case, an extra IPv6 header is needed.

4.4. Network Edge Device

The network edge devices aggregate the traffic from access network, which is the edge of the backbone network. The backbone network runs SRv6 and MPLS.

The network edge device is the boundary of the backbone network, which is the starting point of network service, e.g. tunnels such as SR Policies with various characteristics. Of course, SR Policies are pre-planned by the network operator. The network edge devices will receive both ARN IDs and the mapping of ARN IDs to those pre-planed tunnels from the network controller.

If network edge device is PE, it is desired that VPN services are carried by multiple SRv6 Policies with different color. In this case, the ARN ID in the packet from user can be used to select the appropriate SRv6 Policy.

4.4.1. Ingress Processing

The processing of ARN occurs on the edge devices at the boundary of the ARN domain. When external packets with ARN ID enter the ARN domain, they will be mapped to SRv6 Policy or slice through the ARN Ingress mapping table. At this point, the ARN ID can be considered as the Color of the data plane, corresponding to the Color of the SRv6 Policy.

4.4.2. Egress Processing

When packets leave the ARN domain, the SRv6 Policy can also be mapped to the ARN ID of the next domain. Like ingress processing, there will be an egress mapping table. The mapping operation is quite similar to VLAN translation.

4.4.3. Access Control

Before trusting the incoming ARN ID of the packet outside limited domain, verification is necessary.

The user facing interface should support configuration option to enable or disable the ARN function. When a network edge device receives a packet carrying an ARN ID, if the ARN function on the interface is enabled, it should perform ARN related access control and forwarding processing on the packet. If the ARN function on the interface is disabled, the ARN ID in the packet should be ignored, that is, the processing associated with ARN should be skipped.

The received packet contains source information of the packet, such as source address, PPPoE, tunnel, and other information, which is used to identify subscribers. When the ARN function is enabled on the interface, access control verification can be performed based on the sender’s information and the ARN ID in the packet; after successful verification, forwarding is carried out based on the ARN ID.

If the verification is failed, the ARN ID in the packet should be ignored, that is, the processing associated with ARN should be skipped.

Access control requires a pre-configured ARN ID verification table to verify the source information and ARN ID in the packet. The ARN ID verification table is pre-populated with the following information:

* The source information of the packet, which represents the subscriber.

* The subscribed ARN ID.

* The mapping relationship between the ARN ID and network services (such as SR Policy/Flex Algo).

This table is used to verify the source information and ARN ID in the packet. If ARN ID is valid, the network edge device will perform path mapping function and rate limiting, then do packet forwarding. Otherwise, the ARN ID is cleared or the packet is discarded.

4.4.4. Cross-domain Aggregation and Mapping

The network edge device in current domain(domain A) receives the message with the A ARN ID which is sent by another network edge device, and queries the B ARN ID of A ARN ID mapped in the target domain from a predetermined cross-domain mapping relationship. Then it replaces A ARN ID with B ARN ID to obtain the new message and sends it to the device in target domain(domain B). After the controller of current domain receives the request of allocating ARN ID in the target domain, it will establish cross-domain mapping relationship to achieve the mapping of ARN ID between in the current domain and target domain for the same application-required netwoik path and send it to the netwoik edge devices. The ARN ID configured in flow label, Destination Option Header （DOH）, or Hop-by-Hop Option Header(HBH) is changed to the new ARN ID, then the modified message is obtained and sended the target domain.

4.4.5. Service Funtion Chain Based on ARN

In the SRv6 SFC scenario, the traditional solution of SRv6 SFC requires allocating SIDs for each service (including each SF or each user) and advertising relevant routes, leading to high complexity in the number of SIDs and routes, which makes it impossible to truly implement. The ARN-based approach can greatly simplify this SID and route allocation mechanism. It only uses ARN IDs to integrate network and service capabilities, while SIDs are only used as network path identifiers, reducing the coupling with services.

The gateway device of SFC received and parsed the SID in the service flow. According to the instruction information of the SID function, the IPv6 packet in the service flow and the corresponding extension header are parsed to obtain the application and network capability identifier(that is ARN ID), which is used to indicate the service function SF. Furthermore, the outgoing interface or IP address to the next-hop node corresponding to the SF indicated by the ARN ID is obtained. According to the association table sent by the controller device (or statically configured), the outgoing interface or IP address to the next-hop node corresponding to the SF indicated by ARN ID is searched, including the association between SF and destination IP address or between SF and virtual interface.

4.4.6. Rate Limiting

Imposes traffic limits on specific ARN IDs, typically deployed at the network edge device.

4.5. Controller

The controller generates ARN IDs in the way mentioned in Section 4.1. The controller also configures user edge devices and network edge devices, and manages the lifecycle of ARN IDs.

The controller will send the ARN ID and the application characteristics corresponding to the ARN ID to the user edge device.

The controller will send user information and ARN ID preset correspondence information to network edge device, which is used for access control. At the same time, the controller will send the path information and the preset correspondence of the ARN ID to the network edge device, and the path information can be SR Policy.

A single controller can be centrally used, or multiple controllers can be utilized to collectively fulfill the functions across various stages of the network.

4.6. The Southbound Interface (SBI) of the Controller

The ARN ID and ARN service policies are transmitted from the controller to the relevant network devices for execution through this interface. Candidate protocols for this interface include PCEP, BGP, and YANG-based protocols (NETCONF/RESTCONF).

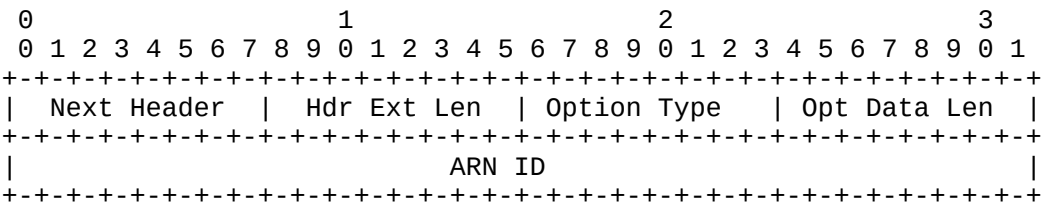
5. ARN Encapsulation

5.1. Locations for IPv6 ARN

ARN carries ARN ID option including ARN ID through the extension of the IPv6 data plane. The location for carrying this information is within the IPv6 Destination Options Header (DOH) or IPv6 Hop-by-Hop Options Header (HBH).

The ARN ID option can be carried in the IPv6 Destination Options Header. By using the DOH Options Header, the information carried can be read by the destination node but would not normally be seen by other nodes along the path.

The ARN ID option can be carried in the IPv6 Hop-by-Hop Options Header. By using the HBH Options Header, the information carried can be read by every node along the path.



Option Type: 8 Bits, ARN option, value to be allocated
ARN ID: 32 Bits

Figure 3: ARN ID Option

5.2. Locations for IPv4 ARN

TBD.

6. Use Cases

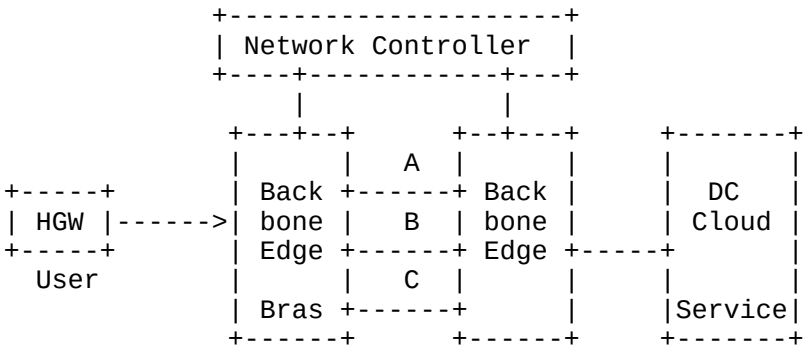


Figure 4: Use case of ARN

This is a typical network where users access the network through a Bras server, then via the backbone network, and finally access the data center cloud services. Functions implemented by each device:

Home Gate Way(HGW): Acts as the user edge device, ARN ID can be directly marked by it based on the services user has purchased and flow characteristics of the application.

Bras: Provides functions such as access control based on Service-ID, path mapping, service aggregation, and rate limiting. If the incoming datagram carries an ARN ID, and the receiving interface has turned on ARN. The legitimacy of the ARN ID can be verified. If the ARN ID does not belong to the user, the verification will fail, and the ARN ID will be cleared or the entire datagram will be discarded. Otherwise, it will perform Path Mapping based on incoming ARN ID.

Network Controller: Configure user information and ARN ID mappings for HGW. Configure access control, path mapping, and rate limiting based on ARN ID for Bras.

Cloud Services: Provides specific application services.

Based on the different types of ARN services purchased by users, when mapping paths in the domain for forwarding user traffic, three network paths can be chosen according to the rules deployed by the controller to meet the users' network requirements. As different applications may have varying network demands, the five-tuple of the datagrams is mapped to corresponding ARN IDs for different network services. This enables the network's entry router to select different network paths based on the different ARN IDs:

* Network Path A: Network path characterized by high bandwidth

* Network Path B: Network path characterized by low latency

* Network Path C: Network path characterized by low packet loss

If a user's different applications have varying network requirements, the user can directly include the corresponding network service's ARN ID in the transmitted datagrams. This allows the network's entry router to select different network paths based on the different ARN IDs.

7. IANA Considerations

Option type number in the header should be allocated.

8. Security Considerations

This document will not affect the security of the Internet.

9. Normative References

[RFC8200] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", STD 86, RFC 8200, DOI 10.17487/RFC8200, July 2017, <https://www.rfc-editor.org/rfc/rfc8200>.

[RFC8402] Filsfils, C., Ed., Previdi, S., Ed., Ginsberg, L., Decraene, B., Litkowski, S., and R. Shakir, "Segment Routing Architecture", RFC 8402, DOI 10.17487/RFC8402, July 2018, <https://www.rfc-editor.org/rfc/rfc8402>.

[RFC8754] Filsfils, C., Ed., Dukes, D., Ed., Previdi, S., Leddy, J., Matsushima, S., and D. Voyer, "IPv6 Segment Routing Header (SRH)", RFC 8754, DOI 10.17487/RFC8754, March 2020, <https://www.rfc-editor.org/rfc/rfc8754>.

[RFC8986] Filsfils, C., Ed., Camarillo, P., Ed., Leddy, J., Voyer, D., Matsushima, S., and Z. Li, "Segment Routing over IPv6 (SRv6) Network Programming", RFC 8986, DOI 10.17487/RFC8986, February 2021, <https://www.rfc-editor.org/rfc/rfc8986>.

[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/rfc/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

Contributors

Joel Halpern
Email: jmh@joelhalpern.com

Many thanks to Joel Halpern for reviewing the ARN ID mapping mechanism.

Authors' Addresses

Feng Yang
China Mobile
China
Email: yangfeng@chinamobile.com

Changwang Lin
New H3C Technologies
China
Email: linchangwang.04414@h3c.com