Signaling and Control Requirements of Network Attachment Control Function for NGN

Jin Seek Choi[1], Member, IEEE
Dept. of Computer Science Education, Hanyang University, (133-070) Seoul, Korea
E-mail: jinseek@hanyang.ac.kr

***Abstract*—The paper shows an overview of the network attachment control function (NACF) in next generation network environments. In particular, we derive the requirements of the signaling and control protocol of network attachment control function (NACF) related to other transport functional entities. For example, ?? provide to the functionalities of detecting the identity of its currently attached link and location, connection establishment and release, bearer resources configuration (including Quality of Service control), and other applications to interact with existing services and legacy networks.**

***Index Terms*—NGN, NACF, signaling protocol, control protocol.**

I. Introduction

Next Generation Network (NGN) defines an architecture for which users enable to access all networks and use seamless services from anywhere and anytime [1-3]. It is a common occurrence for a host to change its point-of attachment to any network. This can happen due to mobile usage (e.g., a mobile phone moving among base stations) or nomadic usage (e.g., road-warrior case) to support seamless services.

When a host changes its point-of attachment to the network, it may end up changing its subnet and require re-configuration of a connection, such as network address, default gateway information, and network layer identification. It is also needed that a host collects the appropriate information and detects the identity of its currently attached link to ascertain the validity of configuration of its currently attached point.

The network attachment control function (NACF) specified in the output document of Draft Y.NGN-FRA v.1.0 has the role of the registration at the access level and initialization of end-user functions for accessing NGN services [5]. These functions contain discovery for network attachment, network-level identification/authentication, manage the IP address space of the access network, and authenticate access sessions. They also announce the contact point of NGN Service/Application support functions to the end user.

To sum up, the NACF provide the following functionalities:

- By endorsement of user, auto-discovery of user equipment capabilities and other parameters.
- Authentication of end user and network at the IP layer (and possibly other layers). Authorization of network access, based on user profiles.
- Dynamic provisioning of IP addresses and other user equipment configuration parameters.
- Access network configuration, based on user profiles.
- Location management at the IP layer.

In order to perform these functions, NACF defines four functional entities (FEs), Transport Location Management Functional Entity (TLM-FE), Transport User Profile Functional Entity (TUP-FE), Transport Authentication and Authorization Functional Entity (TAA-FE), and Network Access Control Functional Entity (NAC-FE). In NACF architecture, each FE is characterized by specific technology-oriented contexts identified as sufficiently unique with respect to other FEs. These FEs allow a uniform control paradigm to span various access technologies and create a single converged control capability that facilitate network performance optimization and lower operational expenses.

This paper describes the requirements of the signaling and control protocol on the basis of a specific instantiation of the functional entity at a given reference point in network attachment control function. These requirements contain how the NACF-FE processes the user profiles provided by Customer Premises Equipment (CPE), the binding information of the logical/physical port address to an assigned IP address related location information, network-level identification/authentication, and the CPE configuration information that ascertains of the common physical layer configuration problems, such as the transport network topology, the maximum bandwidth per subscriber, port mismatches or duplex problems.

II. NACF Functional Architecture

A. Functional Entities

Fig. 1 provides the NGN architecture overview based on the NGN architecture overview provided in Section 6 [5]. The NGN architecture provides capabilities and resources to third party applications for value added services. To provide these services, the network attachment control functional entities (FEs) related to transport control are needed in the transport

[1] This work was partially supported by the OIRC funded by KOSEF.

89-955301-4-6 98560 ©2006 OSIA

Authorized licensed use limited to: KTH THE ROYAL INSTITUTE OF TECHNOLOGY. Downloaded on March 6, 2009 at 05:04 from IEEE Xplore. Restrictions apply.

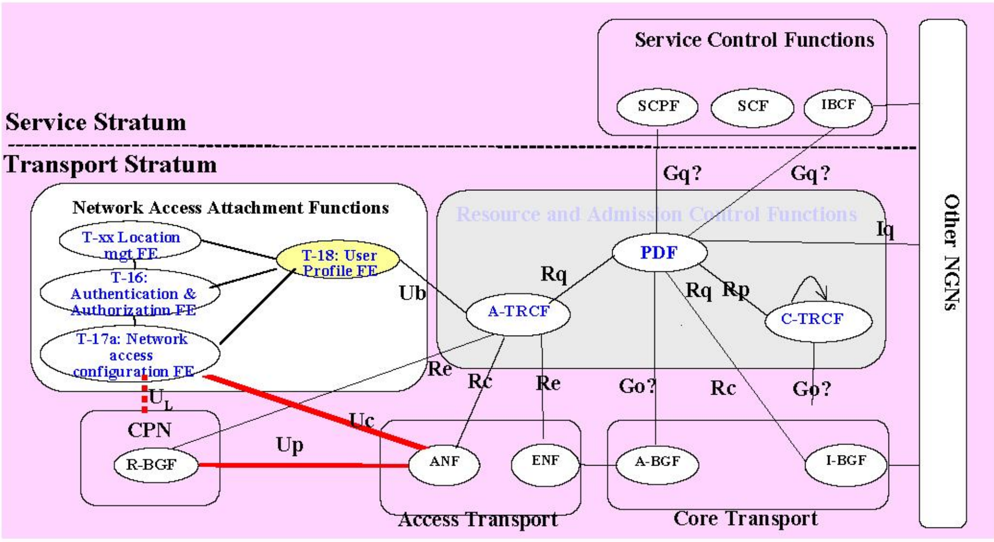

Fig. 1 The NACF functional entities related to transport functions

stratum. The FEs in the transport stratum cover transport functions and associated control functions up to the IP layer. On the other hand, the FEs in the service stratum handle the layers above the IP layer. The control links between the FEs represent high-level logical interactions.

As shown in Fig.1, NACF includes functional entities related to transport control, such as network access control FE (NAC-FE), transport authentication and authorization FE (TAA-FE), transport user profile FE (TUP-FE) and transport location management FE (TLM-FE). The network access control functional entity (NAC-FE) is responsible for IP address allocation and configuration to terminals. It may also distribute other network configuration parameters, such as the addresses of DNS servers and signaling proxies (e.g., the address of the P-CSC-FE in order to have access to service stratum functions). The TAA-FE provides authentication and authorization functions in the transport stratum cooperated with commonly used authentication, authorization, and accounting (AAA) and security schemes. The TUP-FE is responsible for storing user profiles, subscriber-related location data, and presence status data at the transport stratum. The TLM-FE processes current attached location information and register the association between the IP address allocated to a terminal and related network location information, i.e., a line identifier (Line ID). It also traces moving terminals and manages their location in order to minimize the time required and to provide precise information for supporting handover.

B. *NACF Reference points*

To control interface is of crucial importance in NGN since it conveys control and signaling messages. As shown in Fig.1, NACF interacts with RACF to deliver the transport user profile as well as configuration information via U_b interface. NACF interacts with access network function (ANF) via the U_c interface, which makes requests for the binding of the logical/physical port address to an assigned IP address. NACF also interacts with customer premises equipment (CPE) to exchange the appropriate the subscription profile for signaling initiation via U_L.

C. *Requirements on Network Attachment control function*

In NGN environment, CPE frequently changes its point-of attachment to the network. When CPE changes its point-of-attachment, it may end up changing its point of attachment and require re-configuration of a connection automatically, such as physical/logical port address, location information, user profiles including network address, default gateway information, authentication server information and network layer identification.

Conventionally, network operators manually set and configure the network parameters and user profiles. Recently, the NACF protocols are considered in management plane in many standards organizations. For example, there are IETF DHCP, OIF UNI, IEEE LLDP for auto-configuration [4].

Comparing to the existing static configuration protocols, the NACF protocol in NGN should be a dynamic control protocol within the scope of real time environment. This is because NGN has an important objective of the network convergence, the development of the PSTN/ISDN and Packet-based public networks, including services and control plane protocol. Many services can be interoperable and harmonized over various access technologies for a seamless service. For those services across multiple providers or operators, the functions may interact with the corresponding functions in other packet networks. It complements the “access independence” requirements as a real-time automatic configuration. The need for the “access independence” requirements on the signaling and control plane is critical. Here, the signaling and control plane should be understood as the set of functionalities required to control network attachment procedures including parameter discovery, automatic network configuration, mobility management and authentication.

Authorized licensed use limited to: KTH THE ROYAL INSTITUTE OF TECHNOLOGY. Downloaded on March 6, 2009 at 05:04 from IEEE Xplore. Restrictions apply.

The following requirements can be defined for the NACF.

- The network attachment detection for automatic configuration: The NACF is responsible for the automatic discovery of network topology to support auto configuration when detecting network attachment. The discovery function is also responsible for a transport control function to detect the identity of its currently attached network, collect the appropriate network configuration parameters, and ascertain the validity of configuration of its currently attached network based on user profiles.

- An access network identifier to a terminal: This information uniquely identifies the access network to which the terminal is attached. The NACF detects the identity of its currently attached link and location as a function of terminal mobility.

- Bearer connection establishment and release: The NACF control protocol must have the capability to automatically establish, release, and maintain connection segment between CPE and NACF. These operations relieves NACF from unnecessary and time consuming manual operations such as connection establishment and release, bearer resources configuration (including Quality of Service control), and other applications to interact with existing services and legacy networks.

- Network level configuration: The NACF also exchanges the network configuration parameter in NGN environment to support user mobility. These requirements are neither specific to a particular type of access network nor limited to a particular category of service, but do provide sufficient details on the unrestricted seamless service in a multi-protocol, multi-service, multi-vendor environment.

- Location management: The NACF should be able to support location information functions and register the association between the IP address allocated to a terminal and related network location information, i.e., a line identifier (Line ID), and so forth.

- An authentication and authorization: The NACF shall specify how users or terminals are identified in networks. The identification function is the first step and is used for authentication, authorization, and accounting (AAA) of users/terminals. Support for commonly used AAA and security schemes is provided. The NACF is thus required to cooperate with commonly used AAA and security schemes to support authentication, authorization, accounting, and security for services.

- User profile management: The NACF is responsible for storing user profiles, subscriber-related location data, and presence status data at transport stratum (e.g., the current network access point and network location). The user profile may be stored in one database or separated into several databases. The NACF is responsible for responses to queries for user profiles through the basic data management and maintenance functions. Other network functions require some user data in order to be appropriately customized. This function provides filtered access to the user data, which may be restricted to certain interrogating entities (i.e., restricted rights to access user data), in order to guarantee user data privacy.

III. NACF Control Procedure.

A. Network Attachment Control Procedure

The network attachment control procedure can be summarized into the following five steps.

1) Initial Terminal Provisioning (link initialization, and exchange commonly used link-independent profile such as Device name, time, MAC address, and device capability)
2) Dynamic Link provisioning: Collect commonly used link-independent parameters that will be used for resource control and configuration., based on these information, build network topology
3) Transport user configuration: CPE subscribes resource status (BW, connection type, QOS SLA, assign a signaling port to execute authorization)
4) Authorization of the terminal via NA signaling port
5) Network access configuration: stateless auto-configuration (IP, address prefix, DHCP) & Establish session signaling channel through signaling port

Fig.2 shows the network attachment control procedure. As shown in this figure, CPE turns on the power and initializes the provisioning link. It exchanges link parameters such as device name, MAC address, resource capability with access node functional entity, through discovery procedure over U_p. Next, NACF should detect a new point of attachment and collects the link parameters such as an identity, location and resource availability of its currently attached interface via U_c. After then, NACF builds physical network topology based on the discovery information.

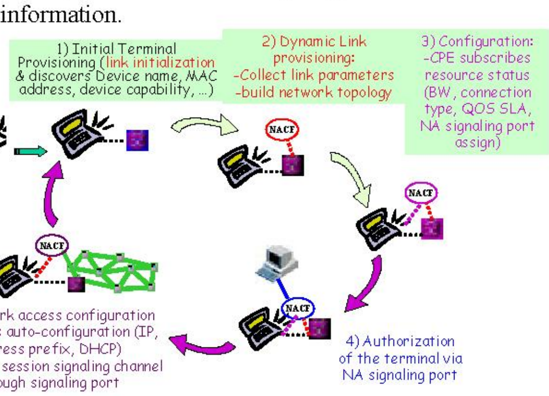

Fig. 2 The network attachment procedure.

Next, NACF exchanges the appropriate configuration information (such as bandwidth, connection type, signaling port, and so on) to ascertain the validity of configuration of its currently attached point through U_L. The address for

Authorized licensed use limited to: KTH THE ROYAL INSTITUTE OF TECHNOLOGY. Downloaded on March 6, 2009 at 05:04 from IEEE Xplore. Restrictions apply.

authentication and configuration will be configured by the end user using mechanisms such as static provisioning, NACF, or other access-specific techniques. NACF also announces the contact point of NGN Service/Application support functions to the end user. Next, NACF exchanges the functional entities such as network-level identification/authentication and authenticates access sessions. Finally, NACF manages the IP address space of the access network, and network access configuration that provide user access network management and configuration based on user profiles.

B. The Control Signal Exchange

Fig.3 illustrates example of control signal exchanging process to configure a network connection on network attachment. At initial terminal provisioning step, ANF detects the terminal attachment by using impedance matching or other mechanisms. Then, CPE and ANF exchange link initialization frames for synchronization. During the dynamic provisioning step, the transport information such as device name, timer values, MAC address, and device capability will be exchanged between CPE and ANF in order to find the control and signaling channel establishment. At the transport user configuration step, CPE subscribes resource status and assign a signaling port to execute authorization. At authorization step, NACF initiates authentication procedure. Finally, network access configuration step, NACF configures the transport information and establishes session signaling channel between CPE and authentication server (or IP multimedia subsystem (IMS)).

Such signaling interfaces must be defined within the scope of the NACF. These interfaces may be either in-band or out-of-band signaling. In-band signaling is useful to support users to signal to the network via a direct communication channel. Out-of-band signaling is attractive where large numbers of channels are managed and the control information associated with different connections can be aggregated. The signaling and control plane also requires resource management and traffic engineering algorithms to efficiently utilize network resources. However, in this paper, we focus on the control and signaling protocol for auto configuration. So, we do not discuss these factors.

IV. CONCLUSION

NGN has an important objective of the network convergence, the development of the PSTN/ISDN and Packet-based public networks, including services and control plane protocol. Therefore, the NACF should be described within the scope of signaling and control protocol. In this paper, we reviewed various requirements to develop the signaling and control protocol on the NACF. We also studied the control procedure and exchange mechanisms. However, it will still require control protocols to specific descriptions of functional entities.

REFERENCES

[1] C.-S. Lee, and D. Knight, "Realization of the Next-generation network," *IEEE Commun. Mag.*, vol. 10, pp. 34–41, Oct. 2005.

[2] K. Knightson, N. Morita, and T. Towle, "NGN Architecture: Generic principles, functional architecture, and implementation," *IEEE Commun. Mag.*, vol. 10, pp. 49–56, Oct. 2005.

[3] M. Carugi, B. Hirschman, and A. Narita, "Introduction to the ITU-T NGN Focus Group Release 1: Target Environment, Services, and Capabilities," *IEEE Commun. Mag.*, vol. 10, pp. 42–48, Oct. 2005

[4] J. S. Choi and T. Kim, ." Proposal to specify adjacency discovery protocol in NACF for supporting parameter configuration," T05-SG13-060116-D-0501 in SG13, Geneva, 16 - 27 Jan. 2006

[5] ITU-T draft document, **Y.NGN-FRA v.1.0,** in SG13, Geneva, 16 - 27 Jan. 2006

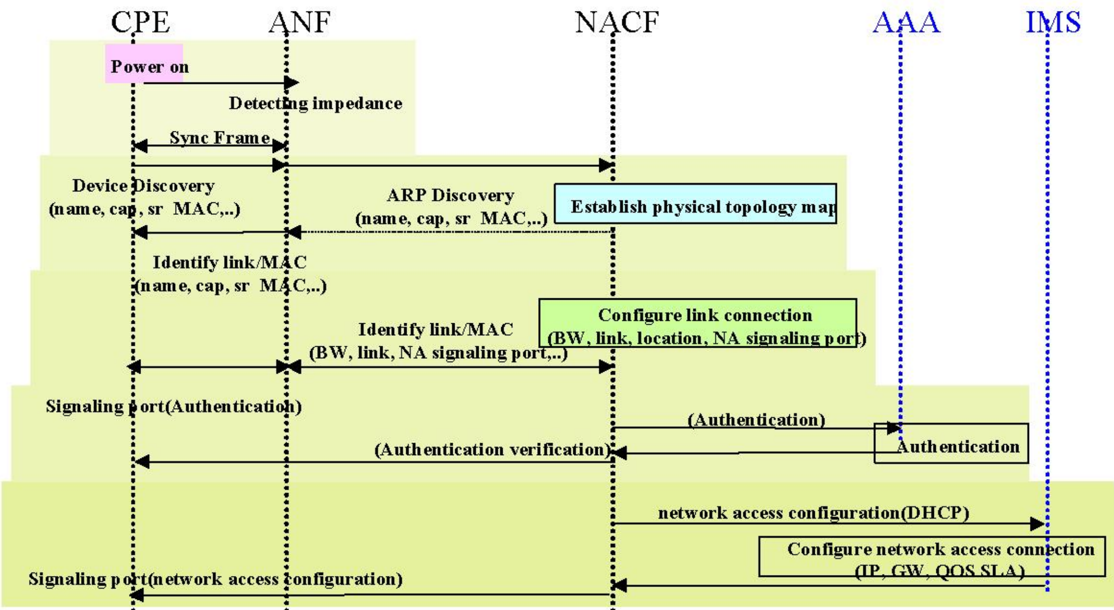

Fig. 3 The control signal exchanges for network attachment procedure

Authorized licensed use limited to: KTH THE ROYAL INSTITUTE OF TECHNOLOGY. Downloaded on March 6, 2009 at 05:04 from IEEE Xplore. Restrictions apply.