A uniform AAA handling scheme for heterogeneous networking environments

Daniel Granlund, Karl Andersson, Muslim Elkotob, Christer Åhlund
Luleå University of Technology
SE-971 87 Luleå, Sweden
{daniel.granlund,karl.andersson,muslim.elkotob,christer.ahlund}@ltu.se

Abstract—Starting with an efficient mobility management scheme for heterogeneous wireless networks, this paper proposes a solution for AAA handling using a common database for storing user information. Regardless of the access technology selected, user@realm identities are used for authentication, authorization, and accounting. In particular, a new function is introduced in which port-based network access control is used in combination with dynamic host configuration protocol mechanisms for IP address allocation. This way, PPP-based and Ethernet-based access technologies are handled uniformly.

Advantages with the proposed solution include: using only standardized mechanisms in the mobile node, as well as in the access networks. Only an additional plug-in in the AAA server (located in the access networks) needs to be deployed.

The proposed AAA architecture has been implemented and evaluated in a live experimental environment. Results show authentication and authorization to perform efficiently and seamlessly.

Keywords—Authentication; authorization; accounting; mobility management; heterogeneous networking environments

I. INTRODUCTION

Today's handsets are typically equipped with more than one radio access card and users want to benefit from connecting to the Internet seamlessly through the best access technology being available at any place any time. Also, network operators want to leverage existing investments and to introduce new access technologies gradually.

Gustafsson et al. [1] presented their Always Best Connected vision and typically a connection should be moved to another radio access technology (RAT) whenever a weighted average of some user-defined parameters exceeds some predefined levels. Mobility detection, access network selection, and mobility management are crucial functions in such an environment. Ideally, uniform schemes for handling quality of service (QoS) and authentication, authorization, and accounting (AAA) are also needed to deliver a full featured networking architecture.

Over the past years, a great number of mobility management schemes have been proposed to provide seamless mobility between access networks. Typically mobility management solutions provide high efficiency when it comes

to networking specifics. However, AAA related problems are often mentioned as future work.

In heterogeneous networking environments, security and other AAA handling are often key issues when it comes to practical implementations. User access control, data security, data integrity and configuration management are important security concerns that have to be addressed in an efficient way, regardless of access technology.

This paper describes a solution where the IEEE 802.1x protocol is combined with the DHCP protocol to provide IP address allocation for Ethernet based connections. A number of access technologies are used in a realistic scenario and a user is able to connect to any network using the same credentials and obtain an IP configuration controlled by the home network. The rest of the paper is organized as follows. Section II describes the proposed AAA management scheme while Section III contains implementation details. Section IV outlines the evaluation setup while Section V indicated the results. Finally, Section VI discusses the results and presents related and future work.

II. PROPOSED AAA MANAGEMENT SCHEME FOR MOBILITY MANAGEMENT SCENARIOS

Network layer based mobility management solutions such as Mobile IP [2] typically associates a fixed IP address for a mobile user belonging to the user's home network, namely the Home Address or HoA. The HoA is often statically configured in the mobile client and no verification is required in order to use it. This type of configuration results in a per-client rather than a per-user mobility management. Ideally the user should, regardless of access network provider and device, only need to authenticate using a common username/password login to achieve their associated configuration.

Using layer 2 tunneling techniques such as L2TP [3], CDMA/UMTS service providers have the ability to provide a service to subscribers that supports user-based IP mobility to the customer network. This mechanism is triggered by a user authenticating with a user@realm + password set. The realm is then used to determine to which network the user belongs, e.g. using the DNS service to locate the Home AAA server. The access service provider AAA server, often called Local AAA or AAA-L will then proxy the AAA request to the AAA server where the user is registered. This server is typically called

Home AAA or AAA-H and is located in the user's home network.

When authentication is complete, the realm information is used to determine the tunnel destination point. The service provider AAA server holds a map of bindings between users and home network L2TP Network Servers, LNS. A tunnel is created between the service provider L2TP Access Concentrator and the home network LNS and the user is thereby allowed IP access into the home network. This technique however relies on the fact that the connection uses the Point-to-Point Protocol (PPP) [4]. Since the PPP protocol supports IP address assignment, the user can be assigned an IP address from the AAA-H server.

It would be very beneficial for the mobile user if the same behavior could be replicated for any access technology and preferably using the same user profile in the AAA-H. Depending on the access technology used, a widely different set of methods is used for AAA handling. In the case of a PPP connection such as UMTS or CDMA2000, the user is typically identified with a username and a password. The user profile is stored in the service provider's own AAA server. During the Link Control Protocol (LCP) phase of the PPP connection establishment, the user is authenticated and allowed access to the network. Later during the Network Configuration Protocol (NCP) phase, the client is provided with a valid configuration and a connection is fully established.

In the case of an Ethernet based technology such as IEEE 802.11, the IEEE 802.1x [5] and Extensible Authentication Protocol, EAP [6] is typically used. The IEEE 802.1x protocol is used for network access control and operates by allowing a supplicant access to only a Port Access Entity, PAE. The PAE handles forwards the supplicant AAA request to an AAA server and upon a successful reply it will open a path and allow access to the network. The IEEE 802.1x mechanism is depicted in figure 1. EAP is a protocol framework for providing user authentication and exists in a variety of versions. The version that is most widely supported in different operating systems like Apple OS and Microsoft Windows is PEAPv0/EAP-MSCHAPv2 [7]. This version incorporates Protected EAP by tunneling the EAP packets over Transport Layer Security, TLS [8].

Figure 1. IEEE 802.1x mechanism

PEAP falls within the WPA and WPA2 Enterprise certification program created by the Wi-Fi Alliance. The PEAP authentication takes place in two distinct phases. Phase 1 secures the communications channel by setting up a secure TLS session and then negotiates for a security parameter that will be used to secure the authentication procedure. Phase 2

involves authenticating the user which is done with EAP messages inside the TLS tunnel. The Microsoft Challenge Handshake Authentication Protocol version 2, MSCHAPv2 [9] is used for username/password authentication. User authentication is typically done to an AAA server using the RADIUS [10] or Diameter [11] protocols. When the user is successfully authenticated the AP will provide access to the network using IEEE 802.1x mechanisms. A key generated in the EAP process is then used to protect the radio communication.

Even though PEAPv0/EAP-MSCHAPv2 and IEEE 802.1x provide a secure and reliable way to authenticate and authorize the user's access they have a lack in support for configuration management such as providing the user with an IP address. In a typical WPA Enterprise implementation this is handled separately by the Dynamic Host Configuration Protocol which will provide a configuration to the host once the host is allowed access to the network. This configuration however is typically network specific and often allocated from a common pool which leaves no insurance that the same client will retrieve the same configuration every time it gains access to the network.

Using the RADIUS protocol the same user profile can successfully be used to access both an 802.1x/PEAP based access network as well as a PPP based. In fact, the user@realm identifier can be used in the same way by an AAA-L in an 802.1x/PEAP as in a PPP based access network to proxy the request depending on the entered realm. Even though the 802.1x/PEAP network has no use of the user IP address since it does not support address assignment, this information is provided along with the rest of the user profile in the RADIUS request reply.

The proposed solution is to have the AAA-L, when proxying a successful RADIUS request, record the Framed-IP-Address and Calling-Station-ID which are the configured user IP address and the client MAC address. This information is then used to update the local DHCP server database with a temporary static entry mapping the client MAC address to the user IP address. This way the client will, upon successful authentication immediately receive the correct IP address that is associated with the authenticated user.

Besides IEEE 802.11 authentication, the same mechanism with IEEE 802.1x + RADIUS authentication is also used for other Ethernet based technologies such as IEEE 802.3 and IEEE 802.16 or WiMAX. The proposed solution should therefore be applicable in these cases as well. The use of DHCP client configuration in the access network is not mandatory since this solution could be used only to distribute addresses to mobile users.

III. IMPLEMENTATION

The software prototype implementation has been done on an AAA server based on the open source FreeRadius [12] software package. The host system for both the AAA-L and AAA-H servers are Intel Pentium 4, 2.8 GHz systems running Fedora Core 10 operating system with kernel version 2.6.x.x. The FreeRadius software package consists of a high performance RADIUS server core provided with a number of interchangeable plug-in modules for additional functionality.

Figure 2. Evaluation setup

Modules are written in ANSI C code, compiled and inserted into the FreeRadius server. Module functions are registered and invoked in one or more steps of the AAA process. The purpose of this implementation is to provide a module that is called during the post-proxy step in the AAA-L server.

The post-proxy step will occur immediately after a message has been proxied by the FreeRadius core. The module function extracts the Calling-Station ID and the Framed-IP-address from the RADIUS message and then creates and writes an entry in the DHCP server configuration file ensuring that the client when querying will receive the correct IP address. The AAA and DHCP servers are in this case co-located on the same system to improve performance. The DHCP server used is the DHCP daemon shipped with Fedora Core namely DHCPD v. 4.0.0 [13].

in the chain of called modules to ensure that it will have sufficient time to update the DHCP configuration.

IV. EVALUATION AND RESULTS

In order to evaluate the proposed architecture a testbed was built up including two access networks and one home network. The mobile node (MN) was equipped with two radio access interfaces, namely CDMA2000 and IEEE WLAN 802.11g. Figure 2 depicts the evaluation testbed setup. This setup was also used in [14] where a mobility management scheme was proposed.

The parameter evaluated is the total delay experienced from authentication, authorization, and configuration when connecting to a new access network that typically was never visited before.

Both WLAN and CDMA2000 [15] accesses were evaluated. Authentication to a WLAN access network includes EAP, TLS, RADIUS, and DHCP transactions. The results are shown in figure 4 below.

Figure 3. FreeRadius modules

Figure 3 shows the module design and application. The implemented module, here called DOT1X-DHCP is placed first

Figure 4. Results from accessing WLAN network

The above graph shows EAP negotiation steps taking place up until approx. 0.42 s. The EAP phase is then immediately followed by the DHCP configuration request, fully completed at 0.47 s. The steps up until 0.2 s is TLS tunnel establishment and the messages sent between 0.24 – 0.42 s are inner tunnel messages.

Authentication to CDMA2000 access network includes PPP LCP/NCP and RADIUS transactions. The results are shown in figure 5 below.

Figure 5. Results from accessing CDMA2000 network

In this case, the total time for PPP link establishment including IP address assignment was 0.89 s.

V. CONCLUSIONS

From the above obtained results we conclude that a uniform AAA scheme using the proposed extension to IEEE 802.1x is feasible with quite good performance in the range of 0.5 seconds for the total link establishment phase. Other solutions using DHCP experience at least a one second or more delay when assigning IP addresses from a dynamic pool. Since we don't have control over the CDMA network used in this evaluation we are not able to dissect and explain delays experienced during PPP link establishment.

For seamless mobility such values in heterogeneous networking environments link establishment has to be efficient and fast. Only then seamless mobility is enabled for real-time sensitive applications such as VoIP, IPTV, video streaming, etc.

VI. RELATED AND FUTURE WORK

We are combining mobility management and AAA solutions for heterogeneous networking environments. A similar solution can be found in [16] where inter technology handoff between CDMA2000 and WLAN is supported by introducing a gateway entity for handling AAA and network layer mobility tasks. However, we argue that since an AAA server is typically already present in many access networks no additional hardware is required for implementation of our proposed scheme.

An architecture for Ubiquitous Mobile Communication, AMC, is described in [17] where a Mobile IP-based mobility management scheme is proposed that supports AAA and QoS handling. It also supports inter operator billing by adding a third-party entity that is trusted by all operators. The AMC architecture however requires a somewhat substantial modification of the networking environment.

When it comes to optimizing the delay of the actual authentication steps a method referred to as context transfer is often used to eliminate steps that are considered unnecessary [18]. Context transfer involves moving the user security context, typically including AAA states and other security parameters such as encryption keys and shared passwords to the target network gateway and/or access point. Context transfer can be carried out reactively or proactively, i.e. during roaming or before roaming. Proactive context transfer however relies on fast and reliable prediction of target network selection. Although the context transfer mechanism speeds up the process of authentication it will introduce some level of security impairment since some crucial steps and procedures are overseen. The Context Transfer Protocol (CXTP) is described in [19].

Context transfer-based solutions and applications are further described in [20] where an overview of different methods for fast authentication during handoff is presented. The authors also discuss problems around inter domain mobility and the need for trust relationships between service providers.

A method for smart proactive context transfer based on neighbor graphs predicting user movement is presented in [21]. Low handover latencies were achieved when roaming among IEEE 802.11 access points using the proactive algorithm.

Next step in our research will be on extending the AAA solution with a SIM card based authentication. Also, we intend to implement this solution in a live WLAN/CDMA2000 heterogeneous network operated by multiple operators also considering a context transfer-based solution in order to achieve even better handover performance.

ACKNOWLEDGMENT

The work presented in this article is based on results from the BasicNet [22] project supported by VINNOVA.

REFERENCES

- [1] E. Gustafsson and A. Jonsson, Always best connected, In IEEE Wireless Communications, Vol. 10, Issue 1, pp. 49-55, February 2003
- [2] C. Perkins (ed.), IP Mobility Support for IPv4, IETF, RFC 3344, August 2002
- [3] W. Townsley (ed.), Layer Two Tunneling Protocol "L2TP", IETF, RFC 2661, August 1999
- [4] W. Simpson (ed.), The Point-to-Point Protocol (PPP), IETF, RFC 1661, July 1994
- [5] P. Congdon (ed.), IEEE 802.1X Remote Authentication Dial In User Service, IETF, RFC 3580, September 2003
- [6] B. Aboba (ed.), Extensible Authentication Protocol (EAP), IETF, RFC 3748, June 2004

- [7] V. Kamath and M. Wodrich, Microsoft's PEAP version 0 (Implementation in Windows XP SP1), Internet Draft, draft-kamath-pppext-peapv0-00.txt, October 2002
- [8] T. Dierks, The TLS protocol, IETF, RFC 2246, January 1999
- [9] G. Zorn, Microsoft PPP CHAP Extensions, Version 2, IETF, RFC 2759 January 2000
- [10] C. Rigney (ed.), Remote Authentication Dial In User Service (RADIUS), IETF, RFC 2865, June 2000
- [11] P. Calhoun (ed.), Diameter Base Protocol, IETF, RFC 3588, September 2003
- [12] FreeRadius, www.freeradius.org
- [13] DHCPD, www.isc.org/software/dhcp
- [14] K. Andersson, D. Granlund, M. Elkotob, and C. Åhlund, Bandwidth efficient mobility management for heterogeneous wireless networks, Submitted for review
- [15] ice.net
- [16] M. Buddhikot, G. Chandranmenon, S. Han, Y-W Lee, S. Miller, and L. Salgarelli, Design and Implementation of a WLAN/CDMA2000 Interworking Architecture, In IEEE Communications Magazine, Vol. 41, Issue 11, pp. 90-100, November 2003
- [17] I. Akyildiz, S. Mohanty, and J. Xie, A Ubiquitous Mobile Communication Architecture for Next-Generation Heterogeneous Wireless Systems, In IEEE Communications Magazine, Vol. 43, Issue 6, pp. S29-S36, June 2005
- [18] M. Shin, J. Ma, A. Mishra, and W. Arbaugh, Wireless Network Security and Interworking, In Proceedings of the IEEE, Vol. 94, No. 2, pp. 455-466, February 2006
- [19] J. Loughney, M. Nakhjiri, C. Perkins, and R. Koodli, Context Transfer Protocol (CXTP), IETF, RFC 4067, July 2005
- [20] M. S. Bargh, R. J. Hulsebosch, E. H. Eertink, A. Prasad, H. Wang, and P. Schoo, Fast authentication methods for handovers between IEEE 802.11 wireless LANs, In Proceedings of the 2nd ACM Int. Workshop on Wireless Mobile Applications and Services on WLAN Hotspots (WMASH'04), pp. 51-60, Philadelphia, Pennsylvania, USA, October 2004
- [21] A. Mishra, M. Shin, and W. A. Arbaugh, Context caching using neighbor graphs for fast handoffs in a wireless network, In Proceedings of the 23rd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2004), pp. 351-361, Hong Kong, China, March 2004
- [22] BasicNet, www.cdt.ltu.se/~basicnet