INTERLINK
NETWORKS

Introduction to Diameter

February 19, 2002

Interlink Networks, Inc.

775 Technology Drive, Suite 200
Ann Arbor, MI 48108 USA
Phone: 734-821-1200
Sales: 734-821-1228
Fax: 734-821-1235
info@interlinknetworks.com
sales@interlinknetworks.com
www.interlinknetworks.com

Table of Contents

Introduction to the Diameter Protocol

INTRODUCTION

The RADIUS protocol (Remote Access Dial In User Services) has been widely and successfully deployed to provide authentication, authorization, and accounting (AAA) services for dial-up PPP/IP and Mobile IP access. However, inherent shortcomings of the RADIUS protocol have limited its ability to adapt to the ever-increasing capabilities of routers and network access servers, and the ever-expanding set of desired AAA services.

A number of working groups have specified their requirements for AAA protocols, and these requirements drove the design of the Diameter protocol.

- The Roaming Operations (ROAMOPS) Working Group of the IETF published a set of requirements for roaming networks.
- The NAS Requirements (NASREQ) Working Group of the IETF documented the next generation NAS AAA requirements.
- The Mobile IP Working Group of the IETF documented AAA requirements that would help Mobile IP scale for Inter-Domain mobility.
- The Telecommunication Industry Association (TIA) TR-45.6 Adjunct Wireless Packet Data Technology working group documented the CDMA2000 Wireless Data Requirements for AAA. Based on the work of TR-45.6, 3GPP2 has specified a two-phased architecture for supporting Wireless IP networking based on IETF protocols; the second phase requiring AAA functionality not supportable in RADIUS.

Diameter was specifically designed to meet the requirements indicated by these various groups.

Diameter is currently focused on, and limited to, supporting access to IP networks. The Diameter protocol was designed as an improved version of the RADIUS protocol. A goal was to maximize compatibility and ease migration from RADIUS to Diameter. For example, a Diameter message, like a RADIUS message, conveys a collection of attribute value pairs.

Diameter is defined in terms of a base protocol and a set of applications. This design allows the protocol to be extended to new access technologies. The base protocol provides basic mechanisms for reliable transport, message delivery, and error handling.

The base protocol must be used in conjunction with a Diameter application. Each application relies on the services of the base protocol to support a specific type of network access. The two major applications are Mobile IPv4 and NASREQ (Network Access Server REQuirements). The NASREQ application supports dial-in PPP/IP and is the intended replacement for RADIUS.

THE CASE FOR DIAMETER

There are several general shortcomings of the RADIUS protocol that were addressed in the design of the Diameter base protocol. These are described in this section.

In addition to the protocol shortcomings, there are further application-specific RADIUS deficiencies that limit its capability to support AAA services in specific areas (e.g. Mobile IP).

Limited size of attribute data

A RADIUS attribute is carried in a RADIUS message as a variable-length {Attribute Type, Attribute Length, Attribute Value} 3-tuple. The Attribute Length field is one octet, hence its maximum value of 255 puts a ceiling on the number of octets of a given attribute's data.

A Diameter attribute is carried in a Diameter message as a variable-length {Attribute Type, Flags, Attribute Length, Vendor-ID, Attribute Value} 5-tuple. The Attribute Length field is three octets, hence its maximum value allows for over 16,000,000 octets of data for a given attribute.

Limited number of concurrent pending messages

An *Identifier* field in the header of the RADIUS packet is used to recognize retransmissions. The identifier field is one octet, imposing a maximum of 255 outstanding messages between a RADIUS client and a RADIUS server.

An *End-to-End Identifier* field in the header of a Diameter message is used to recognize retransmissions. This field is four octets, allowing over 4 billion outstanding messages from a Diameter client.

Inability to control flow to servers

RADIUS operates over UDP (User Datagram Protocol), a simple connectionless datagram-delivery transport protocol that lacks any mechanism for the receiving node to regulate the data flow from the sending node.

Diameter operates over TCP (Transmission Control Protocol) or SCTP (Stream Control Transmission Protocol). TCP and SCTP are connection-oriented transport protocols with flow control and congestion avoidance mechanisms.

Limited server failure detection

There are many reasons why a NAS fails to receive a timely response to a given RADIUS request. These include network congestion, a temporary network failure in the path from the NAS to the home server, failure of the next-hop proxy server, failure of the home server, etc. With RADIUS/UDP, the NAS cannot distinguish the cause of the failure, assumes failure of the next-hop server and retransmits to an alternate next-hop server. This may be an inappropriate failover.

With a connection-oriented transport layer and Diameter keepalive messages, a Diameter node can detect the local failure of a peer.

Silent discarding of packets

The RADIUS protocol specifies that messages are silently discarded for a variety of error conditions. In such cases, the NAS will assume the home server did not receive the message, and will engage in futile retransmissions before finally abandoning the request.

The Diameter protocol returns a response for all but a few error conditions.

Inefficient Server Fail-Over

Most NAS implementations configure multiple RADIUS servers, a primary server and a set of alternate servers. When failing over to an alternate, the NAS doesn't know if the alternate server is even reachable. This can result in a lengthy delay of service to users until a suitable alternate is found.

With a connection-oriented transport layer and Diameter keepalive messages, a Diameter node can effectively failover. It can also fail back to the primary server when it becomes available without having to time out real requests.

Inefficient use of RADIUS servers in proxy environments

Under RADIUS, all retransmissions are done by the NAS. Proxy servers do not retransmit RADIUS requests. The NAS, not knowing whether the failure is local or remote, may inappropriately retransmit to an alternate next-hop peer.

Under the Diameter protocol, each Diameter node that a message traverses on the path from the origin node to the home server will detect a failure of his next-hop peer and do failover and retransmission. Thus, failovers are locally performed at the place where the failures occur.

No unsolicited server messages

The RADIUS protocol does not allow a server to send unsolicited messages to the NAS. Where server initiated actions are needed, vendors are forced into solutions outside of the RADIUS protocol (e.g. SNMP) or solutions involving proprietary extensions to the RADIUS protocol in ways that often compromise interoperability.

Diameter, a peer-to-peer rather than a client/server protocol, allows server-initiated messages. The base protocol defines two server-initiated messages, one requesting that the Diameter client terminate a specific user session, another requesting that the Diameter client re-authenticate and/or reauthorize a specific user.

Replay Attacks

The RADIUS protocol does not offer replay attack prevention. An old packet can be replayed without detection by a malicious NAS impersonator. This can result in denial of service if the server limits concurrent sessions for a user. Duplicate accounting messages can also create havoc.

Only Hop-by-Hop security; no End-to-End security

The RADIUS protocol offers only hop-by-hop security and has no facility for securing AVPs between the NAS and the home server. This offers proxy servers the opportunity to collect confidential information or modify messages (e.g. accounting information) without detection by the endpoints.

The Diameter protocol offers end-to-end security in addition to hop-by-hop security. Digital signatures can ensure the integrity of selected AVPs, and the confidentiality of selected AVPs can be ensured by encryption.

No support for vendor-specific commands

The RADIUS protocol supports vendor-specific attributes but not vendor-specific commands. This has enticed vendors to create private command codes with resulting interoperability problems.

The Diameter protocol supports both vendor-specific attributes and vendor-specific commands.

No alignment requirements

The RADIUS protocol imposes no alignment requirements, which can add an unnecessary burden on many processors. All fields within the header and attributes must be treated as byte aligned characters.

The Diameter protocol requires all attributes to align on 32-bit boundaries. Individual 32-bit fields in the Diameter message header and AVP header also align on 32-bit boundaries.

Mandatory Shared Secret

The RADIUS protocol requires that a shared secret exist between two peers, even if IP Security is employed over a local communication.

The Diameter protocol can secure communications between peers with either IP Security or Transport Layer Security (TLS).

SUMMARY OF DIAMETER ADVANTAGES OVER RADIUS

Better Transport

- Diameter runs over a reliable transport, TCP or SCTP.
- Lost packets are retransmitted at each hop.
- A persistent connection with an application-level heartbeat message (called a Watchdog message) supports timely failover.
- TCP and SCTP adapt to network congestion.

Better Proxying

- Hop-by-hop transport failure detection allows failover to occur at the appropriate place — proxies can locally failover to an alternate next-hop peer.
- The proxy automatically does retransmission of pending request messages following a failover.
- An AVP that identifies the ultimate destination allows multiple transactions for a given session to be routed to the same home server.

Better Session Control

- Session management is independent of accounting. Accounting information can be routed to a different server than authentication/authorization messages. Session termination is conveyed by a specific *Session-Termination* message rather than an Accounting Stop message.
- The server may initiate a message to request session termination.
- The server may initiate a message to request re-authentication and/or reauthorization of a user.

Better Security

- Hop-by-hop security is provided using IPsec or TLS.
- End-to-end security protects the integrity and/or confidentiality of sensitive AVPs through intermediate proxies.

OVERVIEW OF DIAMETER

The Diameter model is a base protocol and a set of applications. The base protocol provides common functionality to the supported applications. The following figure depicts the Diameter architecture.

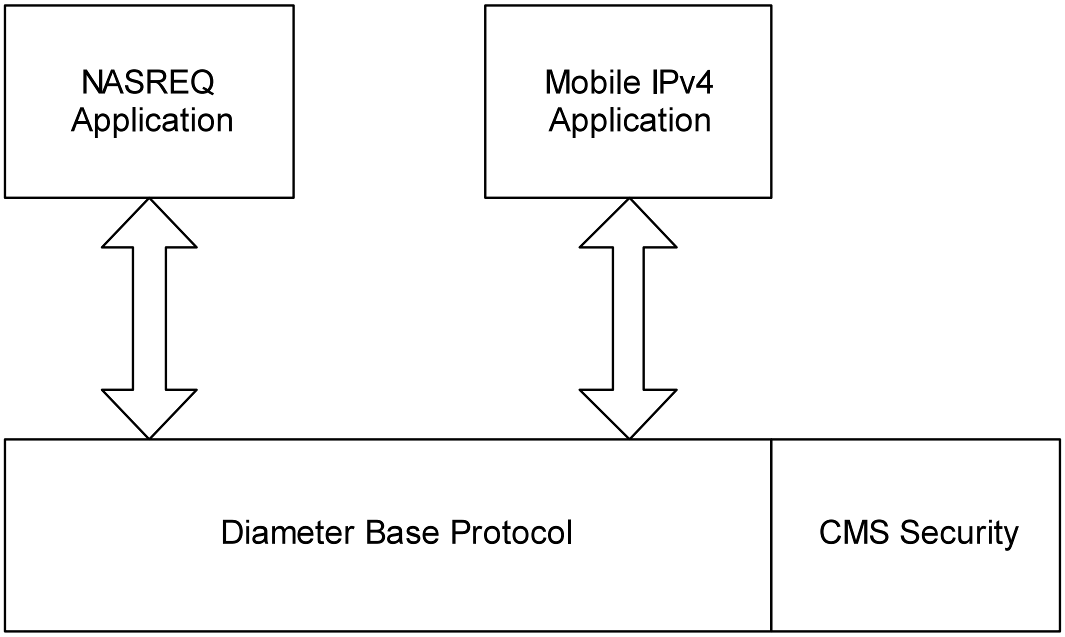

Figure 1: Diameter Protocol Architecture

The base protocol defines the basic Diameter message format. Data is carried within a Diameter message as a collection of Attribute Value Pairs (AVPs). An AVP is like a RADIUS attribute. An AVP consists of multiple fields: an AVP *Code*, a *Length*, some *Flags*, and *Data*. Some AVPs are used by the Diameter base protocol; other AVPs are intended for the Diameter application (e.g. NASREQ); while yet others may be used by the higher-level end-system application that employs Diameter.

A BRIEF OVERVIEW OF SCTP

Diameter, unlike RADIUS, operates over a reliable transport layer (either TCP or SCTP) that provides flow control, transport-level acknowledgements, and retransmissions. While TCP is well known, Stream Control Transmission Protocol (SCTP) is a fairly new IP transport protocol, existing at the level of UDP and TCP. In 2000, SCTP became a Proposed Standard and is specified in RFC 2960.

SCTP is similar to TCP in that:

- SCTP provides a connection-oriented transport service between two endpoints.
- SCTP provides reliable transmission, ensuring that data is delivered in order, without loss or duplication.
- SCTP is full duplex.
- SCTP employs a windowing mechanism to provide flow control.

SCTP, however, provides some capabilities not provided by TCP:

- SCTP provides multiple data streams between the two endpoints. Within each data stream, messages are delivered in order without loss or duplication. Independent data exchanges may be delivered over different streams; message loss in any one stream does not affect data delivery within other streams. TCP provides a single stream of data, where a message loss delays delivery of all subsequent messages. This is sometimes referred to as the *head-of-line blocking* problem. Minimizing the head-of-line blocking problem is the SCTP feature of greatest benefit to Diameter.
- SCTP is message oriented; that is, SCTP maintains message boundaries and delivers complete messages (PDUs), which SCTP calls *chunks*, between the upper layer protocols employing SCTP. TCP is byte oriented; that is, TCP does not preserve data units within a transmitted byte stream, requiring the upper layer protocol to count and accumulate the bytes of each message.
- SCTP understands, and makes use of, the notion of multi-homed hosts. A *multi-homed* host is one with more than one IP interface. At initialization time, SCTP peers exchange lists of their IP interface addresses. An SCTP message requiring retransmission can be sent to an alternate IP address, which increases the survivability of an SCTP session in the event of network failures. SCTP uses multi-homing for redundancy, not for load-sharing. In contrast, a TCP session involves a single IP address at each endpoint, resulting in session failure should that single IP interface become unreachable.

TYPES OF DIAMETER NODES

In addition to clients and servers, the Diameter protocol defines relay, proxy, redirect, and translation agents.

Client

A Diameter Client is a device at the edge of the network that performs access control. Examples of Diameter clients are Network Access Servers (NAS) and mobility agents (Foreign Agent).

Server

A Diameter Server is one that handles authentication, authorization, and accounting requests for a particular realm.

Relay Agent

A Relay Agent routes Diameter messages based on information found in the messages. This routing decision is performed using a list of supported realms and known peers.

Relay agents are largely transparent. A Relay Agent may modify Diameter messages only by inserting and/or removing routing information but may not modify any other portion of a message.

Proxy Agent

A Proxy agent also routes Diameter messages. However, a proxy agent may modify messages to implement policy decisions, such as controlling resource usage, providing admission control, and provisioning.

Redirect Agent

A redirect agent also provides a routing function, generally acting as a centralized source of Realm→Server address mappings for members of a roaming consortium.

Unlike the other agents that relay requests, a redirect agent returns a special type of answer message to the peer that sent the request. This answer message contains routing information that allows the peer to resend the request directly to the correct destination server. The redirect agent is then out of the routing path; a redirect agent does not relay requests.

Translation Agent

A Translation Agent translates between two protocols, such as RADIUS and Diameter. In this case, the translation agent supports a RADIUS to Diameter migration, allowing server conversions to Diameter, for example, while permitting the NASes to be converted at a slower pace.

DIAMETER MESSAGES

Diameter Message Format

A Diameter message consists of a fixed-length 20-octet header followed by a variable number of AVPs. The format of a Diameter message is:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Version    |                                               |
|0 0 0 0 0 0 0 1|                Message Length                 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Flags     |                                               |
|R P E x x x x x|                 Command-Code                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           Vendor-ID                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                      Hop-by-Hop Identifier                    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                      End-to-End Identifier                    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  AVPs ...
+-+-+-+-+-+-+-+-+-+-+-+-+-
```

The Diameter message header contains two 32-bit message identifiers, a Hop-by-Hop Identifier and an End-to-End Identifier.

The *Hop-by-Hop Identifier* aids in matching requests and replies. In requests, the Hop-by-Hop Identifier is replaced at each hop as the Diameter message is relayed to its final destination. The sender of an Answer message returns the same value that was found in the corresponding request

The *End-to-End Identifier*, in conjunction with the origin host's identity, is used to detect duplicate request messages. The End-to-End Identifier is unmodified as a request is forwarded to its final destination. The originator of an Answer message returns the same value that was found in the corresponding request.

Diameter AVP Format

The format of a Diameter AVP is:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           AVP Code                            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Flags       |                                               |
|V M P x x x x x|                  AVP Length                   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                  Vendor-ID (if vendor-specific AVP)           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   AVP Data ... (variable length)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

The *AVP Code* plus the *Vendor-Id* field uniquely identify the attribute. The first 256 AVP numbers, with the Vendor-Id set to zero, are reserved for backward compatibility with RADIUS.

The *AVP Data* field is zero or more octets and contains information specific to the Attribute. The AVP Code and AVP Length fields determine the format and length of the Data field. Diameter defines data types of *Integer32, Unsigned32, Integer64, Unsigned64, Float32, Float64, Float128, OctetString*, and *Grouped.*

A Grouped AVP is an AVP whose data is a sequence of AVPs. The other types are self-explanatory. Derived data formats are also defined, including *enumerated* (derived from integer32), *DiameterIdentity* (derived from octetstring), and *time* (derived from unsigned32), and *UTF8String* (derived from octetstring), *IPFilterRule* (derived from octetstring), and *QosFilterRule* (derived from octetstring).

The Diameter Identity

Each Diameter process running on a host generates, or is configured with, a Diameter Identity. The *DiameterIdentity* is a URI-syntax string with substrings representing the host's fully qualified domain name (FQDN), one of the ports used to listen for incoming connections, the transport used to listen for incoming connections (i.e. TCP or SCTP), the AAA protocol (i.e. Diameter), and the transport security (i.e. none or TLS).

The following is an example of a valid Diameter host identity:

```
aaa://host.abc.com:1812;transport=tcp;protocol=diameter
```

Since the identity carries the host's FQDN, and since multiple Diameter processes on a single host cannot listen for incoming connections on the same port on a given protocol, the DiameterIdentity of any process is guaranteed to be unique.

Diameter Message Content and Routing

A Diameter message consists of a fixed-length header followed by a variable number of AVPs.

There are two types of messages, Requests and Answers. There are few circumstances where a request is silently discarded, so in general the originator of a request will receive an answer. Every answer message carries a *Result-Code* AVP. The data value of the *Result-Code* AVP is an integer code indicating whether a particular request was completed successfully or whether an error occurred.

Every Diameter message carries the Diameter Identity of the originating Diameter process in the *Origin-Host* AVP.

Every Diameter message carries the realm of the originating Diameter process in the *Origin-Realm* AVP.

Request messages may be *proxiable* or *non-proxiable*, indicated by a flag in the message header. Non-proxiable requests are intended strictly for the next-hop peer, and are never forwarded. Proxiable requests are routable and are routed by realm. Every proxiable request carries the target realm in the *Destination-Realm* AVP.

A Diameter message pertaining to a specific user session includes a *Session-Id* AVP, the value of which is constant throughout the life of a session. The value of the *Session-Id* AVP is a globally and eternally unique text string, intended to uniquely identify a user session without reference to any other information. The Diameter client initiating the session creates the Session-Id. The Session-Id begins with the originator's Diameter Identity string and is followed by any sequence guaranteeing both topological and temporal uniqueness.

DIAMETER PEERS

Diameter peers — the set of Diameter nodes with which a given Diameter node will directly communicate — may be statically configured or may be dynamically discovered using SLPv2 or DNS SRV RRs.

Capabilities Exchange

The first Diameter messages exchanged between two Diameter peers, after establishing the transport connection, are *Capabilities Exchange* messages. A *Capabilities Exchange* message carries a peer's identity and its capabilities (protocol version number, supported Diameter applications, etc.). A Diameter node only transmits commands to peers that have advertised support for the Diameter application associated with the given command.

Transport Failure Detection

Application-level heartbeat messages, called the *Device-Watchdog-Request* and *Device-Watchdog-Answer* messages, are used to proactively detect transport failures. These messages are sent periodically when a peer connection is idle and when a timely response has not been received for an outstanding request.

Failover/Failback Procedures

In the event that a transport failure is detected with a peer, a Diameter node attempts to *failover* to an alternate peer, which means that all pending request messages sent to the failed peer will be forwarded to the alternate peer.

A Diameter node periodically attempts to re-establish the transport connection with a failed peer. Should connection be re-established, a node can *failback* to this peer, i.e. messages can once again be forwarded to this peer.

A failover to an alternate proxy agent may result in the reception of duplicate request messages by the home server.

ACCOUNTING

Accounting support and accounting messages are defined as part of the base protocol.

The accounting protocol is based on a *server directed* model that supports real-time delivery of accounting information. The server directed model means that the Diameter client generating the accounting data receives direction from the (authorization or accounting) server regarding accounting record timeliness requirements.

Batch accounting is not a requirement and is currently not supported by Diameter.

CMS security may be applied to Diameter accounting messages, providing strong authentication and integrity protection for accounting data.

The base protocol defines some AVPs that must be present in accounting request messages, such as the *Session-Id* AVP and the *User-Name* AVP. Each Diameter application (e.g. NASREQ, Mobile IPv4), additionally defines application-specific AVPs required in the Accounting-Request.

The *Session-Id* AVP can be used to correlate multiple accounting messages for a user session. Additionally, for applications that require multiple accounting sub-sessions, an *Accounting-Sub-Session-Id* AVP has been defined. Furthermore, for applications where a user receives service from different access devices (each with distinct Session-Ids), such as Mobile IPv4, the *Accounting-Multi-Session-Id* AVP, carried over from RADIUS, can be used for correlation.

THE NASREQ APPLICATION

The Diameter NASREQ application provides AAA services for dial-in PPP users and is the next generation replacement for the RADIUS protocol.

The Diameter NASREQ application, as often as possible, uses existing RADIUS attributes to carry the data objects. This, by design, eases migration of existing

RADIUS servers to Diameter. This also reduces the protocol conversion work required for a server that acts as a RADIUS/Diameter gateway.

RFC 3169, *Criteria for Evaluating Network Access Server Protocols*, defines a number of requirements for AAA protocols used by Network Access Servers (NASes), addressing transport requirements, scalability, server failover, AVP requirements, security, authentication, authorization, policy, resource management, accounting, and more. RFC 2477, *Criteria for Evaluating Roaming Protocols*, similarly addresses the needs of AAA protocols supporting a roaming environment. The Diameter NASREQ application (combined with the base protocol) satisfies the requirements of both specifications.

The NASREQ application, with native Extensible Authentication Protocol (EAP), offers secure authentication. The NASREQ application defines the *Diameter-EAP-Request* and *Diameter-EAP-Answer* messages, which allow the EAP payload to be encapsulated within the Diameter protocol.

The NASREQ application's *AA-Request* message corresponds to the RADIUS Access-Request. The *AA-Answer* message corresponds to the RADIUS Access-Accept and Access-Reject messages.

The NASREQ application also suggests some basic guidelines to be used by a server that acts as a RADIUS–Diameter protocol gateway, i.e. a server that receives a RADIUS message that is to be translated and transmitted as a Diameter message, and vice versa.

THE MOBILE IPV4 APPLICATION

The Diameter Mobile IPv4 application allows a Diameter server to provide AAA support for Mobile IPv4 services rendered to a mobile node. The Diameter Mobile IPv4 application cannot be used with the Mobile IPv6 protocol.

The Diameter Mobile IPv4 application meets the requirements specified in CDMA2000 Wireless Data Requirements for AAA (RFC 3141), and Mobile IP Authentication, Authorization, and Accounting Requirements (RFC 2977).

The Diameter Mobile IPv4 application, in conjunction with extensions to the Mobile IP protocol, supports some of the recent work in the Mobile IP Working Group involving:

- Better scaling of security associations.
- Mobility across administrative domain boundaries.
- Dynamic home agent assignment, in either the home or visited network.

The Mobile IPv4 application defines Diameter functions that allow the AAA server to act as a Key Distribution Center (KDC), whereby dynamic session keys (or key material) are created and distributed to the mobility entities for the purposes of securing a particular session's Mobile IP Registration messages. The mobile node and its home AAA server share a security association (a secret), which the AAA server uses to manufacture these derivative security associations (keys).

THE CMS SECURITY APPLICATION

The Diameter protocol may employ either IPsec or TLS for hop-by-hop integrity and confidentiality between two Diameter peers. However, Diameter endpoints might communicate through relay and proxy agents, and in such environments, security may be compromised.

The Diameter CMS (Cryptographic Message Syntax) application provides end-to-end authentication, integrity, confidentiality and non-repudiation at the AVP level. Individual AVPs may be digitally signed and/or encrypted. Diameter proxies can add, delete or modify unsecured AVPs in a message.

The Diameter CMS security application makes use of two main techniques. Digital signatures, along with digital certificates, provide authentication, integrity and non-repudiation. Encryption provides confidentiality. The techniques can be used simultaneously to provide the required security.

The Diameter CMS security application defines the Diameter messages and AVPs that are used to establish a security association between two Diameter nodes, and the AVPs used to subsequently carry secured data within Diameter messages.

ABOUT INTERLINK NETWORKS

Interlink Networks is a worldwide leader in securing access to public and private networks. The company's products manage user access to dial-in, broadband, mobile, and wireless LAN networks. Interlink Networks' RADIUS-based access control software provides the authentication, authorization, and accounting infrastructure that enables secure and reliable network access for thousands of enterprise and service provider networks worldwide.

In 1992, Merit Networks Inc. developed and deployed the first RADIUS AAA server in a service provider network. In 2000, Merit spun out its AAA technology and engineers to form Interlink Networks, Inc. Interlink Networks offers the strong heritage that was Merit Network with a commitment to continuing to advance AAA solutions with new protocols such as Diameter and 802.1x.

Interlink Networks has launched a Diameter Mobile-IP Authentication Acceleration Program. This program is designed for next generation mobile operators and OEMs interested in integrating AAA technology based on the Diameter protocol into their Mobile IP products and services. [For more information on Mobil IP see the Interlink Networks white paper *Introduction to the Mobile IP Protocol*.] Interlink Networks is currently the only company offering a Diameter implementation to interested companies.

OEMs and service providers looking to deploy Mobile IP networks based upon the Diameter protocol in the next 12-18 months can greatly decrease their cost of development and testing and reduce time to market by participating in the Interlink Networks Diameter Acceleration Program. The program includes roundtable discussions, access to subject matter experts, and compiled and source Diameter server code.

For more information on Interlink Networks and our products and services, please visit http://www.interlinknetworks.com, email info@interlinknetworks.com or call (734) 821-1228.

REFERENCES

Diameter Protocol Drafts.

Diameter Base Protocol, Internet draft-ietf-aaa-diameter-08.txt, P. Calhoun, H. Akhtar, J. Arkko, E. Guttman, A. Rubens, IETF work in progress, November 2001.

Diameter Mobile IPv4 Application, Internet draft-ietf-aaa-diameter-mobileip-08.txt, P. Calhoun, C. Perkins, IETF work in progress, November 2001.

Diameter CMS Security Application, Internet draft-ietf-aaa-diameter-cms-sec-03.txt, P. Calhoun, W. Bulley, S. Farrell, IETF work in progress, November 2001.

Diameter NASREQ Application, Internet draft-ietf-aaa-diameter-nasreq-08.txt, P. Calhoun, W. Bulley, A. Rubens, J. Haag, IETF work in progress, November 2001.

Requirements Documents.

Criteria for Evaluating AAA Protocols for Network Access, http://www.ietf.org/rfc/rfc2989.txt, B. Aboba et al, RFC 2989, November 2000.

CDMA2000 Wireless Data Requirements for AAA, http://www.ietf.org/rfc/rfc3141.txt, T. Hiller et al, RFC 3141, June 2001.

Mobile IP Authentication, Authorization, and Accounting Requirements, http://www.ietf.org/rfc/rfc2977.txt, S. Glass, S. Jacobs, C. Perkins, RFC 2977. October 2000.

Criteria for Evaluating Roaming Protocols, http://www.ietf.org/rfc/rfc2477.txt, Aboba, Zorn, RFC 2477, January 1999.

Criteria for Evaluating Network Access Server Protocols, http://www.ietf.org/rfc/rfc3169.txt, M. Beadles, D. Mitton, RFC 3169, September 2001.

Other References.

Wireless IP Architecture Based on IETF Protocols, 3GPP2 P.R0001, Version 1.0.0, July 14, 2000. http://www.3gpp2.org/Public_html/specs/P.R0001-0_v1.0.pdf .

Wireless IP Network Standard, 3GPP2 P.S0001-A, Version 3.0.0, July 16, 2001. http://www.3gpp2.org/Public_html/specs/P.S0001-A_v3.0.pdf .

Stream Control Transmission Protocol, http://www.ietf.org/rfc/rfc2960.txt, Stewart, Xie, et al, RFC 2960, October 2000.

Authentication, Authorization and Accounting (AAA) Transport Profile, Internet draft-ietf-aaa-transport-05.txt, B. Aboba, J. Wood, IETF Work in Progress, June 2001.

Service Location Protocol, Version 2, http://www.ietf.org/rfc/rfc2165.txt, E. Guttman, C. Perkins, J. Veizades, M. Day. RFC 2165, June 1999.

A DNS RR for specifying the location of services (DNS SRV), http: //www.ietf.org/rfc/rfc2782.txt, A. Gulbrandsen, P. Vixie, L. Esibov, RFC 2782, February 2000.