INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.2902

Amendment 2
(06/2008)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

Next Generation Networks – Available

Carrier grade open environment components

Amendment 2: Annex B, The Diameter server CGOE component

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure e.g. interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU [had/had not] received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

ITU-T Recommendation Y.2902, Carrier grade open environment components - Amendment 2:

Annex B, The Diameter server CGOE component

(This annex forms an integral part of this Recommendation)

Summary

This Annex specifies the Diameter server CGOE component.

B.1 Scope

This Annex specifies the Diameter server CGOE component.

The Diameter base protocol can be used to provide an authentication, authorization and accounting (AAA) framework for applications. A Diameter server CGOE component operating in conjunction with a Diameter Client CGOE component can be used to provide an AAA facility.

B.2 References

The following ITU-T Recommendations and other references contain provisions, which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published.

The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[RFC 3588] IETF RFC 3588 (Diameter) (2003), *Diameter Base Protocol*

[RFC 4301] IETF RFC 4301 (2005), *Security Architecture for the Internet Protocol*

[RFC 4346] IETF RFC 4346 (2006), *The Transport Layer Security (TLS) Protocol Version 1.1*

[RFC 4960] IETF RFC 4960 (2007), *Stream Control Transmission Protocol*

B.3 Definitions

B.3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

B.3.1.1 agent [Q.1290]: An entity acting on behalf of another.
Note: In client server systems an agent is the part of the system that performs information preparation and exchange on behalf of a client or server application

B.3.1.2 application [Y.2901]**:** An application is a piece of software answering a set of user's requirements using telecommunication network services via an IT system.

B.3.1.3 carrier grade [Y.2901]**:** Colloquially, a "carrier grade" implementation of a solution, building block, or a COTS component exhibits particular qualities beyond regular information technology (IT) reliability, availability, serviceability, and manageability (RASM) features enabling its mission-critical use in a service provider's offering.

B.3.1.4 CGOE component [Y.2901]**:** A CGOE component is an abstract description of technical tasks, interfaces and properties.

B.3.1.4 Diameter [Y.2901]**:** An IETF protocol that may be used to provide an authentication, authorization and accounting (AAA) framework for applications.

B.3.1.5 functional requirements [Y.2901]**:** The set of interfaces, capabilities, and features, developed with respect to a service architecture associated with a building block.

B.3.1.6 middleware [Y.2901]**:** The mediating entity between two information elements. Such an element can be, for example, an application, infrastructure component, or another mediating entity.

B.3.1.7 non-functional requirements [Y.2901]**:** A list of features that a building block must provide in order to ensure certain behaviour within the service architecture.

B.3.2 Terms defined in this Recommendation

B.3.2.1 Diameter agent: A Diameter agent is a Diameter component that provides either relay, proxy, redirect or translation services.

B.3.2.2 Diameter client: A Diameter client is a device at the edge of the network that performs access control.

B.3.2.3 Diameter peer: A Diameter peer is a Diameter component to which a given Diameter component has a direct transport connection.

B.3.2.4 Diameter server: A Diameter server handles authentication, authorization and accounting requests.

NOTE ─ A diameter server shall support diameter applications in addition to the base protocol.

B.3.2.5 proxy: A system authorized to work on behalf of another system including responding to protocol requests.

B.3.2.6 proxy agent: An agent that acts as a proxy.

NOTE: In addition to forwarding requests and responses, proxy agents may make policy decisions relating to resource usage and provisioning. This would typically be accomplished by tracking the state of network access server devices. While proxies typically do not respond to client requests prior to receiving a response from the server, they may originate reject messages in cases where policies are violated. As a result, proxies need to understand the semantics of the messages passing through them, and may not support all Diameter applications.

B.3.2.7 relay agent: An agent that performs a relay function.

NOTE: Relay agents forward requests and responses based on routing-related attribute value pairs (AVPs) and realm routing table entries. Relays do not make policy decisions and thus, they do not examine or alter non-routing AVPs. Consequently, relay agents never originate messages, do not need to understand the semantics of messages or non-routing AVPs, and are expected to be capable of handling all Diameter application or message types. As relays make decisions based on information solely in routing AVPs and realm forwarding tables they do not keep state on network access server resource usage or sessions in progress.

B.3.2.8 redirect agent: An agent that performs a redirect function.

NOTE: Rather than forwarding requests and responses between clients and servers, redirect agents refer clients to servers and allow them to communicate directly. Since redirect agents do not sit in the forwarding path after a redirect function has been invoked, they can not alter any AVPs transiting between clients and servers. Redirect agents do not originate messages and are capable of handling any message type, although they may be configured only to redirect messages of certain typesRedirect agents do not keep state with respect to sessions or network access server resources.

B.3.2.9 translation agent: A translation agent is a stateful Diameter component that performs protocol translation between Diameter and another AAA protocol, such as RADIUS.

B.4 Abbreviations and acronyms

AAA	Authentication, Authorization and Accounting
AVP	Attribute Value Pair
CGOE	Carrier Grade Open Environment
IANA	Internet Assigned Numbers Authority
IPSec	IP Security
OAM&P	Operation, Administration, Maintenance, and Provisioning
RADIUS	Remote Authentication Dial In User Service
SCTP	Stream Control Transmission Protocol
TACACS	Terminal Access Controller Access Control System
TLS	Transport Layer Security

B.5 Conventions

This Recommendation uses the CGOE component diagram conventions detailed in clause 5 of the main body of this Recommendation.

In this Recommendation:

- End-to-end security refers to the security between two Diameter nodes, possibly communicating through Diameter agents.
- Transport connection is used to refer to a TCP or SCTP connection existing directly between two Diameter peers.

B.6 The Diameter server CGOE component

B.6.1 General

A technology independent description of the Diameter server CGOE component is in Figure B.1.

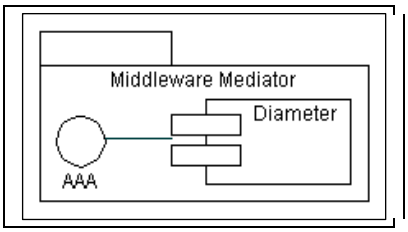

Figure B.1 Implementation independent view

The primary purpose of Diameter is to offer the capability for authentication, authorization, and accounting. .

Diameter has client-server architecture. A principle description is in Figure B-2.

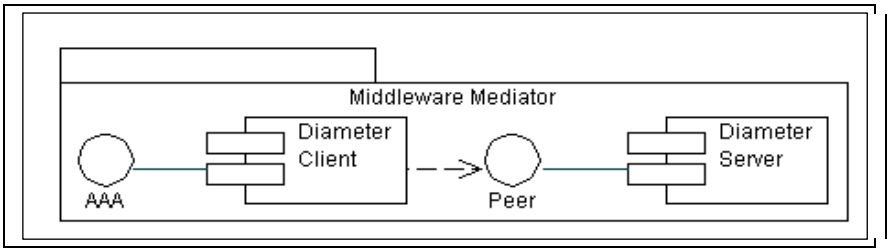

Figure B.2 Diameter client-server-architecture

This Annex focuses on the server component of Diameter. However, while most of the description holds also for the client CGOE component of Diameter, it is outside the scope of this Annex and is the subject of Annex A to Y.2902.

B.6.2 Relationship with other CGOE components

A CGOE compliant Diameter server component may make use of other interfaces as shown in Figure B.3. These are secondary interfaces which are described in the CGOE documentation for each component. Each of these secondary interfaces will have one or more technology-specific instances.

The CGOE component Diameter server is used by the CGOE component OAM&P middleware. Diameter is an optional interface which may be present or not to the OAM&P middleware.

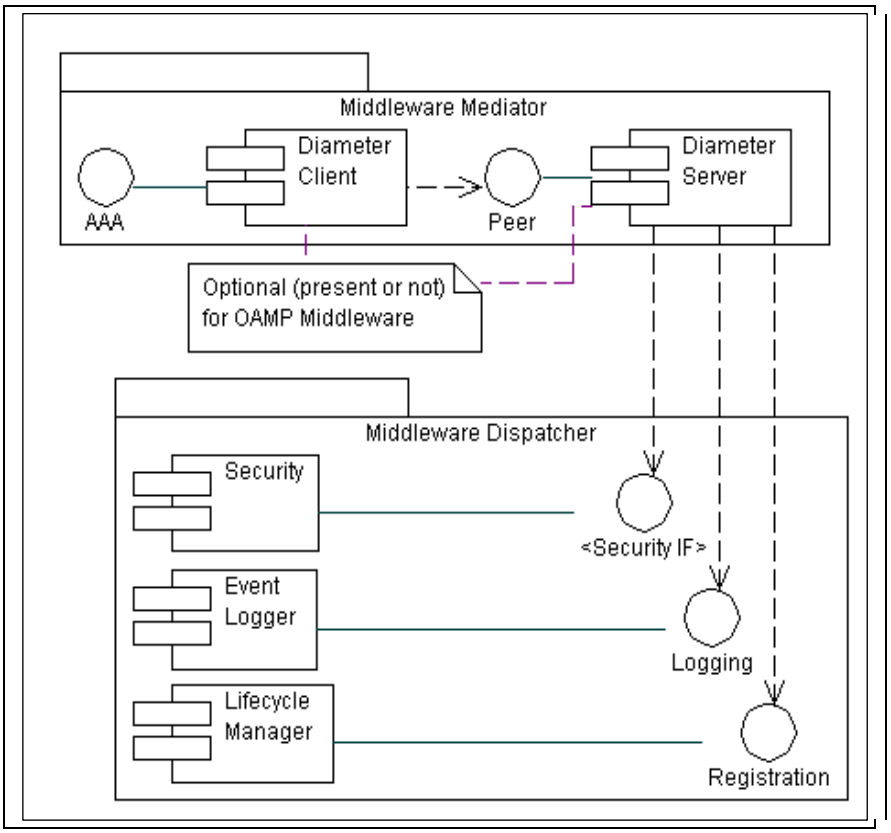

Figure B.3 Diameter client-server architecture with secondary interfaces of the server side

B.6.3 Internal functional properties

B.6.3.1 Diameter relay function

The CGOE Diameter server component shall be capable of performing the Diameter relay function. A Diameter relay agent that performs the relay function shall be protocol transparent and thus shall transparently support the Diameter base protocol, which includes accounting and all Diameter applications.

Standards:

- [RFC 3588]

B.6.3.2 Diameter redirect agent function

The CGOE Diameter server component shall be capable of performing the diameter redirect agent function. A Diameter redirect agent that performs the redirect function shall be protocol transparent and thus shall transparently support the Diameter base protocol, which includes accounting and all Diameter applications.

Standards:

[RFC 3588]

B.6.3.3 Proxy capability of the Diameter server

Diameter proxies must support the Diameter base protocol, which includes accounting. Additionally, they must fully support each Diameter application that is needed to implement proxied services.

Standards

- IETF [RFC 3588]

B.6.3.4 Translation agent

A translation agent is a stateful Diameter node that performs protocol translation between Diameter and another AAA protocol. The CGOE Diameter client component may be capable of performing the translation agent function between:

- Diameter and RADIUS
  Standards:
  - [RFC 3588]
  - [b-RFC 2865]
  - [b-RFC 2868]
  - [b-RFC 3575]
- Diameter and TACACS
  Standards:
  - [RFC 3588]
  - [b-RFC 1492]

B.6.4 Non-functional properties

B.6.4.1 Transport failure detection

- This property measures the occurrence of Diameter messages failures during transport. Detection of such failures will minimize the occurrence of messages sent to unavailable agents, resulting in unnecessary delays, and will provide for better failover performance.
- Unit of measure: not applicable

B.6.4.2 Recovery

- This property measures the behaviour of the components after an outage condition has been restored.
- Unit of measure: yes / partly / no

B.6.5 Interfaces

B.6.5.1 Diameter Server-IF-01 <Applications>

The AAA application interface is the primary interface of a Diameter server CGOE component and it supports the interface to authentication, authorization and accounting applications. When the base Diameter protocol is in use for authentication and authorization, it is always extended for a particular application. For example two Diameter applications are defined: NASREQ and Mobile IPv4. These applications are not part of the Diameter server CGOE component.

Standard:

- [RFC 3588]

B.6.5.2 Diameter Server-IF-02 <Peer>

The peer interface is the basic connection interface offered by the Diameter server CGOE component. For connection to a peer CGOE Diameter component when the communications channel is not contained within a trusted environment this interface shall connect to an IPSec or TLS CGOE component. At a minimum, a Diameter node SHOULD have an established connection with two peers per realm, known as the primary and secondary peers.

- Diameter Server-IF-02 <IPSec peer>
    - Standard
        - [RFC 2401]
        - [RFC 3588]
- Diameter Server-IF-02 <TLS peer>
    - Standard
        - [RFC 2246]
        - [RFC 3588]

B.6.5.3 Diameter Server-IF-03<Logging>

The logging interface is a secondary interface of the Diameter server CGOE component and provides the capability to log any transaction in relation to the Diameter server CGOE component.

Standard:

- GAP (Possible solution the logging component of the specific middleware can be used)

B.6.5.4 Diameter Server-IF-04<Registration>

The registration interface is a secondary interface of the diameter server CGOE component and is the interface used to connect to the CGOE component lifecycle manager.

Standard:

- GAP

B.6.5.4 Diameter Server-IF-05 <Security: End– to-End >

The security IF is a secondary interface of the Diameter server CGOE component. End-to-end security refers to security between two Diameter nodes, possibly communicating through Diameter Agents. It should be noted that TLS and IPsec provide hop-by-hop security or security across only a transport connection. Thus when Diameter relays or proxies are involved hop-by-hop security does not fully protect the Diameter session. This security interface protects the Diameter communications path from the originating Diameter component to the terminating diameter component.

Standard:

- [RFC 3588]
- GAP – Possible solution, IETF work in progress on End-to-End security

B.6.5.6 Diameter Server-IF-06 <Stream Control Transmission Protocol>

The diameter server CGOE component provides a number of interfaces. For those instances where the interface requires a transport capability, the interface may use TCP over IP or SCTP over IP. This interface provides mechanisms to transfer Diameter messages over the Internet Protocol using the stream control transmission protocol.

Standards:

- [RFC 3588]
- [RFC 4960]

B.6.5.7 Diameter Server-IF-07 <Transmission Control Protocol>

The diameter server CGOE component provides a number of interfaces. For those instances where the interface requires a transport capability, the interface may use TCP over IP or SCTP over IP. This interface provides mechanisms to transfer diameter messages over the Internet protocol using the transmission control protocol.

Standards:

- [RFC 3588]
- [RFC 4960]

B.6.5.8 Relationship with Internet Assigned Numbers Authority

Each Diameter application must have an Internet Assigned Numbers Authority (IANA) assigned application identifier. Implementations must only use Diameter applications for which an IANA assigned application identifier has been obtained.

Standards:

- [b-RFC 3692]

B.7 Security

The Diameter server CGOE component will communicate with other CGOE components through its primary and secondary interfaces. In some cases these inter CGOE component links will occur in fully trusted environments while in other cases this will not be true. As a result, the Diameter server CGOE component shall be able to make use of standard transmission links and transmission links that are protected through the use of TLS or IPSec.

The Diameter protocol shall not pass through an untrusted environment without the benefit of a security mechanism, viz. TLS or IPsec.

Bibliography

ETSI TS 129.228 *Digital cellular telecommunications system (Phase 2+);Universal Mobile Telecommunications System (UMTS);IP Multimedia (IM) Subsystem Cx and Dx Interfaces;Signalling flows and message contents*

ETSI TS 129.229 *Digital cellular telecommunications system (Phase 2+);Universal Mobile Telecommunications System (UMTS);Cx and Dx interfaces based on the Diameter protocol;Protocol details*

ETSI TS1 29.329 *Digital cellular telecommunications system (Phase 2+);Universal Mobile Telecommunications System (UMTS);Sh interface based on the Diameter protocol;Protocol detail*

[b-RFC 1492] IETF RFC 1492 *(TACACS) An Access Control Protocol, Sometimes Called TACACS*

[b-RFC 2865] IETF RFC 2865 (2000), *Remote Authentication Dial In User Service (RADIUS)*

[b-RFC 2868] IETF RFC 2868 (2000), *RADIUS Attributes for Tunnel Protocol Support*

[b-RFC 3575] IETF RFC 3575 (2003), *IANA Considerations for RADIUS*

[b-RFC 5080] IETF RFC 5080 (2007) *Common Remote Authentication Dial In User Service (RADIUS) Implementation Issues and Suggested Fixes*