Internet Draft
Expiration: December 2000
File: draft-durham-aaa-cops-reqments-00.txt

Hormuzd Khosravi
David Durham
Jesse Walker
Intel

Comparison of COPS Against AAA Network Access Requirements

Last Updated: May 31, 2000

Status of this Memo

Abstract

The AAA Working Group has completed a document that itemizes their requirements for Network Access Applications (NASREQ, Mobile IP, and ROAMOPS). This specification compares the COPS protocol against the requirements, and is provided to the AAA Working Group as an official submission for an AAA protocol.

1.0 Introduction

The AAA Working Group has completed a document that itemizes their

requirements for Network Access Applications (NASREQ, Mobile IP, and ROAMOPS). This specification compares the COPS protocol against the requirements, and is provided to the AAA Working Group as an official submission for an AAA protocol.

1.1 Requirements language

In this document, the key words "MAY", "MUST, "MUST NOT", "optional", "recommended", "SHOULD", and "SHOULD NOT", are to be interpreted as described in [1].

Please note that the requirements specified in this document are to be used in evaluating AAA protocol submissions. As such, the requirements language refers to capabilities of these protocols; the protocol documents will specify whether these features are required, recommended, or optional. For example, requiring that a protocol support confidentiality is NOT the same thing as requiring that all protocol traffic be encrypted.

A protocol submission is not compliant if it fails to satisfy one or more of the MUST or MUST NOT requirements for the capabilities that it implements. A protocol submission that satisfies all the MUST, MUST NOT, SHOULD and SHOULD NOT requirements for its capabilities is said to be "unconditionally compliant"; one that satisfies all the MUST and MUST NOT requirements but not all the SHOULD or SHOULD NOT requirements for its protocols is said to be "conditionally compliant."

2.0 Requirements Summary

This section contains the same four sections as found in the AAA Network Access requirements. Each section contains a new column, named COPS. For each requirement, it is noted whether the COPS protocol meets (T), Partially meets (P), or does not meet (F) the stated requirement. Furthermore, each requirement has a footnote, which contains additional justification.

2.1 General requirements

These requirements apply to all aspects of AAA and thus are

considered general requirements.

General Reqts.	NASREQ	ROAMOPS	MOBILE IP	COPS
Scalability	M	M	M	Ta
Failover	M		M	Tb
Mutual auth AAA client/server	M		M	Tc
Transmission level security		M	S	Td
Data object Confidentiality	M	M	S	Te
Data object Integrity	M	M	M	Tf
Certificate transport	M		S	Tg

Reliable AAA transport mechanism	M		M	T h
Run Over IPv4	M	M	M	T i
Run Over IPv6	M		S	T j
Support Proxy and Routing Brokers	M		M	T k
Auditability	S			T l

Shared secret not required	S	O	O/M	T m
Ability to carry service-specific attr.	M		S	T n

Key
M = MUST
S = SHOULD
O = MAY
N = MUST NOT
B = SHOULD NOT

T = Meets Requirement
P = Partly Meets Requirement
F = Does Not Meet Requirement

Clarifications

[a] The COPS protocol provides the following features that help scaling:

[1] supports very large number of pending requests since the request handle is unbounded

[2] support for message forwarding and redirect servers

[3] can create COPS server hierarchies that will help increase scalability

[b] The COPS Protocol [3] defines the failover and synchronization mechanisms that can be used in event of failure of the primary COPS server to switch to the secondary or backup server.

[c] The COP Protocol [3] defines three different authentication mechanisms:

[1] None - When the local policy demands that no security is needed or when an underlying security service is used.

[2] Hop-by-Hop - The COPS Protocol [3] provides a security mechanism using the Integrity Object to provide authentication, replay protection, and message integrity.

[3] End-to-End - COPS object-level integrity using CMS.

[d] The COPS Protocol [3] provides message authentication, integrity and confidentiality using the security mechanism defined in the protocol or uses other underlying mechanisms such as IPSec and TLS.

[e] COPS uses CMS [5] to provide object level confidentiality. See COPS Usage for AAA [6] for details and See RFC 2797.

[f] COPS uses CMS[5] to provide object level integrity. COPS uses RFC 1510 Certificate Management Messages over CMS to provide object level integrity. See COPS Usage for AAA [6] for details.

[g] This MUST be part of the Information Model that is carried with the COPS messages.

[h] The COPS Protocol [3] runs over TCP which provides reliable transport and addresses the AAA requirements.

[i] The COPS Protocol [3] has no reliance on the underlying IP version, and is capable of running over IPv4.

[j] The COPS Protocol [3] has no reliance on the underlying IP version, and is capable of running over IPv6.

[k] The COPS Protocol supports proxies and brokers in both transparent forwarding, as well as in the redirect mode. See COPS Usage for AAA [6] for details.

[l] The Information Model such as a History PIB MUST be used to carry information about how the COPS messages are audited by proxies/brokers as they travel from the home server to the network device.

[m] All COPS security mechanisms are based on local policies and only used as required.

[n] The COPS Protocol [3] is highly extensible in two ways, it supports new Client Types which can define Client Specific Info. objects and COPS-PR [4] separates the Information Model from the protocol allowing third parties to define service-specific Data (a.k.a. PIBs), that are carried over the protocol.

2.2 Authentication Requirements

Authentication Reqts.	NASREQ	ROAMOPS	MOBILE IP	COPS

NAI Support	M	M	S	T a
CHAP Support	M	M	O	T b
EAP Support	M	S	O	T c
PAP/Clear-Text Support	M	B	O	T d
Re-authentication on demand	M		S	T e
Authorization Only without Authentication	M		O	T f

Key
M = MUST
S = SHOULD
O = MAY
N = MUST NOT
B = SHOULD NOT

T = Meets Requirement
P = Partly Meets Requirement

F = Does Not Meet Requirement

Clarifications

[a] The Information Model MUST define NAI attributes which are then carried in the COPS messages. Note that when using certificate

based authentication, the naming scheme MUST conform to RFC 2459 naming conventions for subjectAltName and/or Subject name. This is more restrictive than NAI.

[b] The Information Model MUST define CHAP attributes which are then carried in the COPS messages.

[c] The Information Model MUST define EAP attributes which are then carried in the COPS messages.

[d] The Information Model MUST define PAP which are then carried in the COPS messages.

[e] The COPS Protocol being Stateful supports unsolicited Decision and Request messages that can be used to trigger re-authentication. The Authentication time limit MUST be specified in the Information Model.

[f] The COPS protocol allows the authentication and authorization information to be carried in separate Request messages. Therefore, it is possible to send a request for authorization only. Please note: with existing algorithms, any authorization scheme not based on a prior authentication is meaningless.

2.2 Authorization Requirements

Authorization Reqts.	NASREQ	ROAMOPS	MOBILE IP	COPS
Static and Dynamic IPv4/6 Address Assign.	M	M	M	Ta
RADIUS gateway capability	M	M	O	Tb

Reject capability	M	M	M	T c
Precludes layer 2 tunneling	N	N		T d
Re-Authorization on	M		S	T

demand				e
Support for Access Rules, Restrictions, Filters	M		O	T f
State Reconciliation	M			T g
Unsolicited Disconnect	M			T h

Key
M = MUST
S = SHOULD
O = MAY
N = MUST NOT
B = SHOULD NOT

T = Meets Requirement

P = Partly Meets Requirement
F = Does Not Meet Requirement

Clarifications

[a] The Information Model MUST define the static & dynamic addresses which can be carried in the COPS messages during the authorization phase.

[b] The Information Model can define RADIUS attributes which can be carried in the COPS messages and used for protocol compatibility. Additionally, COPS can carry RADIUS AVPs directly without modification using its Client Specific Information object.

[c] A forwarding agent, be it a Proxy or Broker, MAY reject a COPS Request by sending a Decision message with the appropriate Error Object.

[d] The COPS information model MUST define support for L2TP configuration.

[e] The COPS Protocol being Stateful supports unsolicited Decision and Request messages that can be used to trigger re-authoriza-

tion. The Authorization time limit MUST be specified in the Authorization Information Model.

[f] The Data/Information Model like the PIB MUST define the Access Rules and Filters that are carried in the COPS messages.

[g] The AAA network access requirements describe State Reconciliation as requiring:

[1] Re-authorization capabilities - This is described in 2.2[e].

[2] Session disconnect message - The COPS Client Handle is used to maintain the session state. The Client can remove the session state by sending COPS Delete Request with the same Client Handle. This message thus acts as a session disconnect message. The COPS connection can also be closed.

[3] Transport and application-layer reliability - COPS uses TCP which satisfies this requirement as well as its own session

Keep-Alive mechanism.

[4] An interim message - The COPS protocol supports unsolicited Report messages that can be used for this purpose. The Accounting Timer is used to set the interval for the accounting Reports or interim messages.

[5] A mechanism for the AAA server to retrieve state information from the NAS. This mechanism will provide timely information though a complete state dump may not be immediately available. - The COPS failover and synchronization mechanism can be used for this purpose.

[6] A NAS reboot message - This MUST be part of the Information Model.

[7] Accounting On/Off messages - This MUST be part of the Information Model. (The COPS Accounting Timer can also be used for this purpose.)

[h] The COPS Base Protocol defines the Client Close message that can be used by either the COPS client or server to terminate the session. If the state is a subset of the TCP connection, then this could also be part of the Client-Handle signaling (Decision message and Delete Handle message).

2.3 Accounting Requirements

Accounting Reqts.	NASREQ	ROAMOPS	MOBILE IP	COPS
Real-time accounting	M	M	M	Ta
Mandatory Compact Encoding		M	M	Tb

Accounting Record Extensibility	M	M	M	T c
Batch Accounting	S			T d
Guaranteed Delivery	M		M	T e
Accounting Time Stamps	M		S	T f
Dynamic Accounting	M		S	T g

Key
M = MUST
S = SHOULD
O = MAY
N = MUST NOT
B = SHOULD NOT

T = Meets Requirement
P = Partly Meets Requirement
F = Does Not Meet Requirement

Clarifications

[a] The COPS Protocol has provisions for sending unsolicited Report messages that can be used to send real-time accounting data.

[b] The COPS-PR ClientSI objects can be used to carry ADIF records directly. The AAA Accounting Record and Attributes specification states "[ROAM-ADIF] proposes a standard accounting record format, the Accounting Data Interchange Format (ADIF), which is designed to compactly represent accounting data in a protocol-independent manner." Likewise, this format can also be stored within a PIB structure.

[c] The ADIF Accounting Data Format MAY be extended by assigning new keywords for new accounting data objects by IANA. Likewise, new PIBs (which are fully described data structures) can be easily developed to represent future accounting records.

[d] In COPS, the Report messages are used to carry Accounting data. The Accounting Timer object can be used to set the interval at which periodic accounting updates are sent to the COPS server.

[e] COPS runs over TCP that provides guaranteed delivery at the application layer. The application layer can acknowledge Reports using a COPS Decision message if needed (all acknowledged accounting records on the client can be marked as acknowledged by the server).

[f] This MUST be defined as an attribute in the Accounting Data Model (a.k.a. PIB) that will be carried in the COPS Report messages.

[g] The COPS-PR uses PIBs which use the PRID to identify separate instances of the same data structure for a single session.

2.4 Unique Mobile IP requirements

In addition Mobile IP also has the following requirements:

Unique Mobile IP requirements	NASREQ	ROAMOPS	MOBILE IP	COPS
Encoding of Mobile IP registration messages			M	Ta
Firewall friendly			M	T

					b

Allocation of local Home agent				S/M	T c

Key
M = MUST
S = SHOULD
O = MAY
N = MUST NOT
B = SHOULD NOT

T = Meets Requirement
P = Partly Meets Requirement
F = Does Not Meet Requirement

Clarifications

[a] The Information/Data Model or PIB like structure MUST be defined for Mobile IP Registration messages, which can be used to carry the Registration messages over COPS.

[b] The COPS Protocol [3] runs over TCP and uses a fixed port number defined by IANA, which is why it is considered firewall friendly. Additionally, COPS proxy servers can easily be supported.

[c] This MUST be part of the Information Model which can be extended to support a Mobile IP Home Agent on any platform.

3.0 Conclusion

The COPS Protocol [3], when used with the appropriate Information Model, is unconditionally compliant with the AAA Network Access requirements [2].

4.0 References

[1] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[2] Aboba et al, "Network Access AAA Evaluation Criteria", IETF workin progress, draft-ietf-aaa-na-reqts-02.txt, March 2000.

[3] Boyle, J., Cohen, R., Durham, D., Herzog, S., Rajan, R., Sastry, A., "The COPS (Common Open Policy Service) Protocol", RFC 2748, August 1999.

[4] Reichmeyer, F., Herzog, S., Chan, K.H., Seligson, J., Durham, D., Yavatkar, R., Gai, S., McCloghrie, K., Smith, A., "COPS Usage for Policy Provisioning", IETF , March 2000.

[5] R. Housley, "Cryptographic Message Syntax", RFC 2630, June 1999.

[6] D. Durham, H. Khosravi, W. Weiss, A. Doria, "COPS Usage for AAA", IETF, June 2000.

5.0 Security Considerations

This document, being a protocol evaluation document, does not have any security concerns. The security requirements on protocols to be evaluated using this document are described in the referenced documents.

6.0 IANA Considerations

This draft does not create any new number spaces for IANA administration.

7.0 Acknowledgements

Special thanks to the authors and contributors to the various COPS documents. Thanks also to the authors of the AAA Network Access Evaluation Criteria document from which this document was formed.

8.0 Authors Addresses

David Durham
Intel
2111 N.E. 25th Avenue JF3-206
Hillsboro OR 97124-5961
1 503 264 6232
david.durham@intel.com

Hormuzd M Khosravi
Intel
2111 N.E. 25th Avenue JF3-206
Hillsboro OR 97124-5961
1 503 264 0334
hormuzd.m.khosravi@intel.com

Jesse R. Walker
Intel Corporation
2111 N.E. 25th Avenue
Hillsboro, OR 97214
USA

jesse.walker@intel.com

9.0 Full Copyright Statement