Network Working Group
Request for Comments: 3169
Category: Informational

M. Beadles
SmartPipes, Inc.
D. Mitton
Nortel Networks

September 2001

Criteria for Evaluating Network Access Server Protocols

Status of this Memo

Copyright Notice

Abstract

This document defines requirements for protocols used by Network Access Servers (NAS).

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 [KEYWORDS].

2. Introduction

This document defines requirements for protocols used by Network Access Servers (NAS). Protocols used by NAS's may be divided into four spaces: Access protocols, Network protocols, AAA protocols, and Device Management protocols. The primary focus of this document is on AAA protocols.

The reference model of a NAS used by this document, and the analysis of the functions of a NAS which led to the development of these requirements, may be found in [NAS-MODEL].

3. Access Protocol Requirements

There are three basic types of access protocols used by NAS's. First are the traditional telephony-based access protocols, which interface to the NAS via a modem or terminal adapter or similar device. These protocols typically support asynchronous or synchronous PPP [PPP]

carried over a telephony protocol. Second are broadband pseudo-telephony access protocols, which are carried over xDSL or cable modems, for example. These protocols typically support an encapsulation method such as PPP over Ethernet [PPPOE]. Finally are the virtual access protocols used by NAS's that terminate tunnels. One example of this type of protocol is L2TP [L2TP].

It is a central assumption of the NAS model used here that a NAS accepts multiple point-to-point links via one of the above access protocols. Therefore, at a minimum, any NAS access protocol MUST be able to carry PPP. The exception to this requirement is for NAS's that support legacy text login methods such as telnet [TELNET], rlogin, or LAT. Only these access protocols are exempt from the requirement to support PPP.

4. Network Protocol Requirements

The network protocols supported by a NAS depend entirely on the kind of network to which a NAS is providing access. This document does not impose any additional requirements on network protocols beyond the protocol specifications themselves. For example, if a NAS that serves a routed network includes internet routing functionality, then that NAS must adhere to [ROUTING-REQUIREMENTS], but there are no additional protocol requirements imposed by virtue of the device being a NAS.

5. AAA Protocol Requirements

5.1. General protocol characteristics

There are certain general characteristics that any AAA protocol used by NAS's must meet. Note that the transport requirements for authentication/authorization are not necessarily the same as those for accounting/auditing. An AAA protocol suite MAY use the same transport and protocol for both functions, but this is not strictly required.

5.1.1. Transport requirements

5.1.1.1. Transport independence

The design of the AAA protocol MUST be transport independent. Existing infrastructures use UDP-based protocols [RADIUS], gateways to new protocols must be practical to encourage migration. The design MUST comply with congestion control recommendations in RFC 2914 [CONGEST].

5.1.1.2. Scalability

Very large scale NAS's that serve up to thousands of simultaneous sessions are now being deployed. And a single server system may service a large number of ports. This means that, in the extreme, there may be an almost constant exchange of many small packets between the NASes and the AAA server. An AAA protocol transport SHOULD support being optimized for a long-term exchange of small packets in a stream between a pair of hosts.

The protocol MUST be designed to support a large number of ports, clients, and concurrent sessions. Examples of poor design would include message identifiers which values are so small that queues and reception windows wrap under load, unique session identifier ranges that are so small that they wrap within the lifetime of potential long sessions, counter values that cannot accommodate reasonable current and future bandwidth usage, and computational processes with high overhead that must be performed frequently.

5.1.1.3. Support for Multiple AAA Servers and Failure Recovery

In order to operationally support large loads, load balancing and fail-over to multiple AAA servers will be required. The AAA protocol MUST provide for NAS's to balance individual AAA requests between two or more AAA servers. The load balancing mechanism SHOULD be built in to the AAA protocol itself.

The AAA protocol MUST be able to detect a failure of the transport protocol to deliver a message or messages within a known and controllable time period, so it can engage retransmission or server fail-over processes. The reliability and robustness of authentication requests MUST be predictable and configurable.

The AAA protocol design MUST NOT introduce a single point of failure during the AAA process. The AAA protocol MUST allow any sessions between a NAS and a given AAA server to fail-over to a secondary server without loss of state information. This fail-over mechanism SHOULD be built in to the AAA protocol itself.

5.1.1.4. Support for Multiple Administrative Domains

NAS's operated by one authority provide network access services for clients operated by another authority, to network destinations operated by yet another authority. This type of arrangement is of growing importance; for example, dial roaming is now a nearly ubiquitous service. Therefore, the AAA protocol MUST support AAA

services that travel between multiple domains of authority. The AAA protocol MUST NOT use a model that assumes a single domain of authority.

The AAA protocol MUST NOT dictate particular business models for the relationship between the administrative domains. The AAA protocol MUST support proxy, and in addition SHOULD support other multi-domain relationships such as brokering and referral.

The AAA protocol MUST also meet the protocol requirements specified in [ROAMING-REQUIREMENTS].

5.1.2. Attribute-Value Protocol Model

Years of operational experience with AAA protocols and NAS's has proven that the Attribute-Value protocol model is an optimal representation of AAA data. The protocol SHOULD use an Attribute-Value representation for AAA data. This document will assume such a model. Even if the AAA protocol does not use this as an on-the-wire data representation, Attribute-Value can serve as abstraction for discussing AAA information.

Experience has also shown that attribute space tends to run out quickly. In order to provide room for expansion in the attribute space, the AAA protocol MUST support a minimum of 64K Attributes (16 bits), each with a minimum length of 64K (16 bits).

5.1.2.1. Attribute Data Types

The AAA protocol MUST support simple attribute data types, including integer, enumeration, text string, IP address, and date/time. The AAA protocol MUST also provide some support for complex structured data types. Wherever IP addresses are carried within the AAA protocol, the protocol MUST support both IPv4 and IPv6 [IPV6] addresses. Wherever text information is carried within the AAA protocol, the protocol MUST comply with the IETF Policy on Character Sets and Languages [RFC 2277].

5.1.2.2. Minimum Set of Attributes

At a minimum, the AAA protocol MUST support, or be easily extended to support, the set of attributes supported by RADIUS [RADIUS] and RADIUS Accounting [RADIUS-ACCOUNTING]. If the base AAA protocol does not support this complete set of attributes, then an extension to that protocol MUST be defined which supports this set.

5.1.2.3. Attribute Extensibility

NAS and AAA development is always progressing. In order to prevent the AAA protocol from being a limiting factor in NAS and AAA Server development, the AAA protocol MUST provide a built-in extensibility mechanism, which MUST include a means for adding new standard attribute extensions. This MUST include a method for registering or requesting extensions through IANA, so that long-term working group involvement is not required to create new attribute types. Ideally, the AAA protocol SHOULD separate specification of the transport from specification of the attributes.

The AAA protocol MUST include a means for individual vendors to add value through vendor-specific attributes and SHOULD include support for vendor-specific data types.

5.1.3. Security Requirements

5.1.3.1. Mutual Authentication

It is poor security practice for a NAS to communicate with an AAA server that is not trusted, and vice versa. The AAA protocol MUST provide mutual authentication between AAA server and NAS.

5.1.3.2. Shared Secrets

At a minimum, the AAA protocol SHOULD support use of a secret shared pairwise between each NAS and AAA server to mutually verify identity. This is intended for small-scale deployments. The protocol MAY provide stronger mutual security techniques.

5.1.3.3. Public Key Security

AAA server/NAS identity verification based solely on shared secrets can be difficult to deploy properly at large scale, and it can be tempting for NAS operators to use a single shared secret (that rarely changes) across all NAS's. This can lead to an easy compromise of the secret. Therefore, the AAA protocol MUST also support mutual verification of identity using a public-key infrastructure that supports expiration and revocation of keys.

5.1.3.4. Encryption of Attributes

Some attributes are more operationally sensitive than others. Also, in a multi-domain scenario, attributes may be inserted by servers from different administrative domains. Therefore, the AAA protocol

MUST support selective encryption of attributes on an attribute-by-attribute basis, even within the same message. This requirement applies equally to Authentication, Authorization, and Accounting data.

5.2. Authentication and User Security Requirements

5.2.1. Authentication protocol requirements

End users who are requesting network access through a NAS will present various types of credentials. It is the purpose of the AAA protocol to transport these credentials between the NAS and the AAA server.

5.2.1.1. Bi-directional Authentication

The AAA protocol MUST support transport of credentials from the AAA server to the NAS, between the User and the NAS, and between the NAS and the AAA server.

5.2.1.2. Periodic Re-Authentication

The AAA protocol MUST support re-authentication at any time during the course of a session, initiated from either the NAS or the AAA server. This is a requirement of CHAP [CHAP].

5.2.1.3. Multi-phase Authentication

The AAA protocol MUST be able to support multi-phase authentication methods, including but not limited to support for:

- Text prompting from the NAS to the user
- A series of binary challenges and responses of arbitrary length
- An authentication failure reason to be transmitted from the NAS to the user
- Callback to a pre-determined phone number

5.2.1.4. Extensible Authentication Types

Security protocol development is going on constantly as new threats are identified and better cracking methods are developed. Today's secure authentication methods may be proven insecure tomorrow. The AAA protocol MUST provide some support for addition of new authentication credential types.

5.2.2. Authentication Attribute Requirements

In addition to the minimum attribute set, the AAA protocol must support and define attributes that provide the following functions:

5.2.2.1. PPP Authentication protocols

Many authentication protocols are defined within the framework of PPP. The AAA protocol MUST be able to act as an intermediary protocol between the authenticate and the authenticator for the following authentication protocols:

- PPP Password Authentication Protocol [PPP]
- PPP Challenge Handshake Authentication Protocol [CHAP]
- PPP Extensible Authentication Protocol [EAP]

5.2.2.2. User Identification

The following are common types of credentials used for user identification. The AAA protocol MUST be able to carry the following types of identity credentials:

- A user name in the form of a Network Access Identifier [NAI].
- An Extensible Authentication Protocol [EAP] Identity Request Type packet.
- Telephony dialing information such as Dialed Number Identification Service (DNIS) and Caller ID.

If a particular type of authentication credential is not needed for a particular user session, the AAA protocol MUST NOT require that dummy credentials be filled in. That is, the AAA protocol MUST support authorization by identification or assertion only.

5.2.2.3. Authentication Credentials

The following are common types of credentials used for authentication. The AAA protocol MUST be able to carry the following types of authenticating credentials at a minimum:

- A secret or password.
- A response to a challenge presented by the NAS to the user
- A one-time password

- An X.509 digital certificate [X.509]

- A Kerberos v5 ticket [KERBEROS]

5.2.3. Authentication Protocol Security Requirements

5.2.3.1. End-to-End Hiding of Credentials

Where passwords are used as authentication credentials, the AAA protocol MUST provide a secure means of hiding the password from intermediates in the AAA conversation. Where challenge/response mechanisms are used, the AAA protocol MUST also prevent against replay attacks.

5.3. Authorization, Policy, and Resource management

5.3.1. Authorization Protocol Requirements

In all cases, the protocol MUST specify that authorization data sent from the NAS to the AAA server is to be regarded as information or "hints", and not directives. The AAA protocol MUST be designed so that the AAA server makes all final authorization decisions and does not depend on a certain state being expected by the NAS.

5.3.1.1. Dynamic Authorization

The AAA protocol MUST support dynamic re-authorization at any time during a user session. This re-authorization may be initiated in either direction. This dynamic re-authorization capability MUST include the capability to request a NAS to disconnect a user on demand.

5.3.1.2. Resource Management

Resource Management MUST be supported on demand by the NAS or AAA Server at any time during the course of a user session. This would be the ability for the NAS to allocate and deallocate shared resources from a AAA server servicing multiple NASes. These resources may include, but are not limited to; IP addresses, concurrent usage limits, port usage limits, and tunnel limits. This capability should have error detection and synchronization features that will recover state after network and system failures. This may be accomplished by session information timeouts and explicit interim status and disconnect messages. There should not be any dependencies on the Accounting message stream, as per current practices.

This feature is primarily intended for NAS-local network resources. In a proxy or multi-domain environment, resource information should only be retained by the server doing the allocation, and perhaps it's backups. Authorization resources in remote domains should use the dynamic authorization features to change and revoke authorization status.

5.3.2. Authorization Attribute Requirements

5.3.2.1. Authorization Attribute Requirements - Access Restrictions

The AAA protocol serves as a primary means of gathering data used for making Policy decisions for network access. Therefore, the AAA protocol MUST allow network operators to make policy decisions based on the following parameters:

- Time/day restrictions. The AAA protocol MUST be able to provide an unambiguous time stamp, NAS time zone indication, and date indication to the AAA server in the Authorization information.

- Location restrictions: The AAA protocol MUST be able to provide an unambiguous location code that reflects the geographic location of the NAS. Note that this is not the same type of thing as either the dialing or dialed station.

- Dialing restrictions: The AAA protocol MUST be able to provide accurate dialed and dialing station indications.

- Concurrent login limitations: The AAA protocol MUST allow an AAA Server to limit concurrent logins by a particular user or group of users. This mechanism does not need to be explicitly built into the AAA protocol, but the AAA protocol must provide sufficient authorization information for an AAA server to make that determination through an out-of-band mechanism.

5.3.2.2. Authorization Attribute Requirements - Authorization Profiles

The AAA protocol is used to enforce policy at the NAS. Essentially, on granting of access, a particular access profile is applied to the user's session. The AAA protocol MUST at a minimum provide a means of applying profiles containing the following types of information:

- IP Address assignment: The AAA protocol MUST provide a means of assigning an IPv4 or IPv6 address to an incoming user.

- Protocol Filter application: The AAA protocol MUST provide a means of applying IP protocol filters to user sessions. Two different methods MUST be supported.

  First, the AAA protocol MUST provide a means of selecting a protocol filter by reference to an identifier, with the details of the filter action being specified out of band. The AAA protocol SHOULD define this out-of-band reference mechanism.

  Second, the AAA protocol MUST provide a means of passing a protocol filter by value. This means explicit passing of pass/block information by address range, TCP/UDP port number, and IP protocol number at a minimum.

- Compulsory Tunneling: The AAA protocol MUST provide a means of directing a NAS to build a tunnel or tunnels to a specified end- point. It MUST support creation of multiple simultaneous tunnels in a specified order. The protocol MUST allow, at a minimum, specification of the tunnel endpoints, tunneling protocol type, underlying tunnel media type, and tunnel authentication credentials (if required by the tunnel type). The AAA protocol MUST support at least the creation of tunnels using the L2TP [L2TP], ESP [ESP], and AH [AH] protocols. The protocol MUST provide means of adding new tunnel types as they are standardized.

- Routing: The AAA protocol MUST provide a means of assigning a particular static route to an incoming user session.

- Expirations/timeouts: The AAA protocol MUST provide a means of communication session expiration information to a NAS. Types of expirations that MUST be supported are: total session time, idle time, total bytes transmitted, and total bytes received.

- Quality of Service: The AAA protocol MUST provide a means for supplying Quality of Service parameters to the NAS for individual user sessions.

5.3.2.3. Resource Management Requirements

The AAA protocol is a means for network operators to perform management of network resources. The AAA protocol MUST provide a means of collecting resource state information, and controlling resource allocation for the following types of network resources.

- Network bandwidth usage per session, including multilink sessions.

- Access port usage, including concurrent usage and usage pools.
- Connect time.
- IP Addresses and pools.
- Compulsory tunnel limits.

5.3.3. Authorization Protocol Security Requirements

5.3.3.1. Security of Compulsory Tunnel Credentials

When an AAA protocol passes credentials that will be used to authenticate compulsory tunnels, the AAA protocol MUST provide a means of securing the credentials from end-to-end of the AAA conversation. The AAA protocol MUST also provide protection against replay attacks in this situation.

5.4. Accounting and Auditing Requirements

5.4.1. Accounting Protocol Requirements

5.4.1.1. Guaranteed Delivery

The accounting and auditing functions of the AAA protocol are used for network planning, resource management, policy decisions, and other functions that require accurate knowledge of the state of the NAS. NAS operators need to be able to engineer their network usage measurement systems to a predictable level of accuracy. Therefore, an AAA protocol MUST provide a means of guaranteed delivery of accounting information between the NAS and the AAA Server(s).

5.4.1.2. Real Time Accounting

NAS operators often require a real time view onto the status of sessions served by a NAS. Therefore, the AAA protocol MUST support real-time delivery of accounting and auditing information. In this context, real time is defined as accounting information delivery beginning within one second of the triggering event.

5.4.1.3. Batch Accounting

The AAA protocol SHOULD also support delivery of stored accounting and auditing information in batches (non-real time).

5.4.1.4. Accounting Time Stamps

There may be delays associated with the delivery of accounting information. The NAS operator will desire to know the time an event actually occurred, rather than simply the time when notification of the event was received. Therefore, the AAA protocol MUST carry an unambiguous time stamp associated with each accounting event. This time stamp MUST be unambiguous with regard to time zone. Note that this assumes that the NAS has access to a reliable time source.

5.4.1.5. Accounting Events

At a minimum, the AAA protocol MUST support delivery of accounting information triggered by the following events:

- Start of a user session
- End of a user session
- Expiration of a predetermined repeating time interval during a user session. The AAA protocol MUST provide a means for the AAA server to request that a NAS use a certain interval accounting time.
- Dynamic re-authorization during a user session (e.g., new resources being delivered to the user)
- Dynamic re-authentication during a user session

5.4.1.6. On-Demand Accounting

NAS operators need to maintain an accurate view onto the status of sessions served by a NAS, even through failure of an AAA server. Therefore, the AAA protocol MUST support a means of requesting current session state and accounting from the NAS on demand.

5.4.2. Accounting Attribute Requirements

At a minimum, the AAA protocol MUST support delivery of the following types of accounting/auditing data:

- All parameters used to authenticate a session.
- Details of the authorization profile that was applied to the session.
- The duration of the session.

- The cumulative number of bytes sent by the user during the session.

- The cumulative number of bytes received by the user during the session.

- The cumulative number of packets sent by the user during the session.

- The cumulative number of packets received by the user during the session.

- Details of the access protocol used during the session (port type, connect speeds, etc.)

5.4.3. Accounting Protocol Security Requirements

5.4.3.1. Integrity and Confidentiality

Note that accounting and auditing data are operationally sensitive information. The AAA protocol MUST provide a means to assure end-to-end integrity of this data. The AAA protocol SHOULD provide a means of assuring the end-to-end confidentiality of this data.

5.4.3.2. Auditibility

Network operators use accounting data for network planning, resource management, and other business-critical functions that require confidence in the correctness of this data. The AAA protocol SHOULD provide a mechanism to ensure that the source of accounting data cannot easily repudiate this data after transmission.

6. Device Management Protocols

This document does not specify any requirements for device management protocols.

7. Acknowledgments

Many of the requirements in this document first took form in Glen Zorn's, "Yet Another Authentication Protocol (YAAP)" document, for which grateful acknowledgment is made.

8. Security Considerations

See above for security requirements for the NAS AAA protocol.

Where an AAA architecture spans multiple domains of authority, AAA information may need to cross trust boundaries. In this situation, a NAS might operate as a shared device that services multiple administrative domains. Network operators are advised take this into consideration when deploying NAS's and AAA Servers.

9. IANA Considerations

This document does not directly specify any IANA considerations. However, the following recommendations are made:

Future development and extension of an AAA protocol will be made much easier if new attributes and values can be requested or registered directly through IANA, rather than through an IETF Standardization process.

The AAA protocol might use enumerated values for some attributes, which enumerate already-defined IANA types (such as protocol number). In these cases, the AAA protocol SHOULD use the IANA assigned numbers as the enumerated values.

10. References

[AH] Kent, S. and R. Atkinson, "IP Authentication Header (AH)", RFC 2402, November 1998.

[CHAP] Simpson, J., "PPP Challenge Handshake Authentication Protocol (CHAP)", RFC 1994, August 1996.

[CONGEST] Floyd, S., "Congestion Control Principles", RFC 2914, Sept. 2000.

[EAP] Blunk, L. and J. Vollbrecht, "PPP Extensible Authentication Protocol (EAP)", RFC 2284, March 1998.

[ESP] Kent, S. and R. Atkinson, "IP Encapsulating Security Payload (ESP)", RFC 2406, November 1998.

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

[KERBEROS] Kohl, J. and C. Neuman, "The Kerberos Network Authentication Service (V5)", RFC 1510, September 1993.

[IPV6] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.

[L2TP] Townsley, W., Valencia, A., Rubens, A., Pall, G., Zorn, G. and B. Plater, "Layer Two Tunneling Protocol (L2TP)", RFC 2661, August 1999.

[NAI] Aboba, B. and M. Beadles, "The Network Access Identifier", RFC 2486, January 1999.

[NAS-MODEL] Mitton, D. and M. Beadles, "Network Access Server Requirements Next Generation (NASREQNG) NAS Model", RFC 2881, July 2000.

[NAS-EXT] Mitton, D., "Network Access Servers Requirements: Extended RADIUS Practices", RFC 2882, July 2000.

[PPP] Simpson, W., "The Point-to-Point Protocol (PPP)", STD 51, RFC 1661, July 1994.

[PPPOE] Mamakos, L., Lidl, K., Evarts, J., Carrel, D., Simone, D. and R. Wheeler, "A Method for Transmitting PPP Over Ethernet (PPPoE)", RFC 2516, February 1999.

[ROUTING-REQUIREMENTS] Baker, F., "Requirements for IP Version 4 Routers", RFC 1812, June 1995.

[TELNET] Postel, J. and J. Reynolds, "Telnet Protocol Specification", STD 8, RFC 854, May 1983.

[RFC 2277] Alvestrand, H., "IETF Policy on Character Sets and Languages", BCP 18, RFC 2277, January 1998.

[X.509] ITU-T Recommendation X.509 (1997 E): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, June 1997.

[RADIUS] Rigney, C., Rubens. A., Simpson, W. and S. Willens, "Remote Authentication Dial In User Service (RADIUS)", RFC 2138, April 1997.

[RADIUS-ACCOUNTING] Rigney, C., "RADIUS Accounting", RFC 2139, April 1997.

[ROAMING-REQUIREMENTS] Aboba, B. and G. Zorn, "Criteria for Evaluating Roaming Protocols", RFC 2477, January 1999.

11. Authors' Addresses

Mark Anthony Beadles
SmartPipes, Inc.
565 Metro Place South Suite 300
Dublin, OH 43017

Phone: 614-923-6200

David Mitton
Nortel Networks
880 Technology Park Drive
Billerica, MA 01821

Phone: 978-288-4570
EMail: dmitton@nortelnetworks.com

12. Full Copyright Statement

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.