AAA PROTOCOLS: Authentication, Authorization, and Accounting for the Internet

Christopher Metz • *Cisco Systems* • *chmetz@cisco.com*

Internet service providers (ISPs) offering dial-up access and purveyors of enterprise networks supporting telecommuters face some difficult challenges. Ever-increasing residential dial-up subscribers demand available modem (or ISDN) ports, or threaten to take their business elsewhere. To meet this demand, ISPs (dial providers) are deploying a large number of complex, port-dense network access servers (NAS) to handle thousands of individual dial-up connections.

At the same time, the miniaturization of stationary office essentials, such as the laptop computer and cellular telephone, has coupled with the need for maximum customer face time to create a workforce in perpetual motion. These "road warriors" require secure and reliable access to e-mail and Web resources from hotels, airports, and virtual offices around the world.

But dial providers must do more than simply offer an available modem port at the other end of a telephone call. They must protect against theft-of-service attacks by unscrupulous individuals with excess free time; they must verify subscribers' levels of access authorization; and for cost recovery, billing, and resource planning purposes, they may need to meter the connection time to the network. Furthermore, to provide maximum coverage to a growing roaming and mobile subscriber base, they may choose to pool their NAS resources while retaining control over their subscribers' access, usage, and billing information. All these services require coordination between the various administrative systems supported by the dial providers in partnership with each other.

AAA Framework

Meeting these challenges in a simplified and scalable manner lies at the heart of Authentication, Authorization, and Accounting. AAA essentially defines a framework for coordinating these individual disciplines across multiple network technologies and platforms. In practice, an AAA server with a database of user profiles and configuration data communicates with AAA clients residing on network components, such as NAS and routers, to provide distributed AAA services.

A closer look at the individual pieces is the best way to understand the services provided within the AAA framework. *Authentication* involves validating the end users' identity prior to permitting them network access. This process keys on the notion that the end-user possesses a unique piece of information—a username/password combination, a secret key, or perhaps biometric data (fingerprints, for example)—that serves as unambiguous identification credentials. The AAA server compares the user-supplied authentication data with the user-associated data stored in its database, and if the credentials match, the user is granted network access. A nonmatch results in an authentication failure and a denial of network access.

Authorization defines what rights and services the end user is allowed once network access is granted. This might include providing an IP address, invoking a filter to determine which applications or protocols are supported, and so on. Authentication and authorization are usually performed together in an AAA-managed environment.

Accounting, the third "A," provides the methodology for collecting information about the end user's resource consumption, which can then be processed for billing, auditing, and capacity-planning purposes.

Figure 1 illustrates the components of an AAA solution. The AAA server—multiple servers can be used for resiliency—is attached to the network and serves as a central repository for storing and distributing AAA information. The device acting as the point of entry into the network is typically a NAS (although it could also be a router, a terminal server, or perhaps another host) that contains an AAA client function. AAA processing can be summarized in the following steps:

- End user connects to the point-of-entry device and requests access to the network.

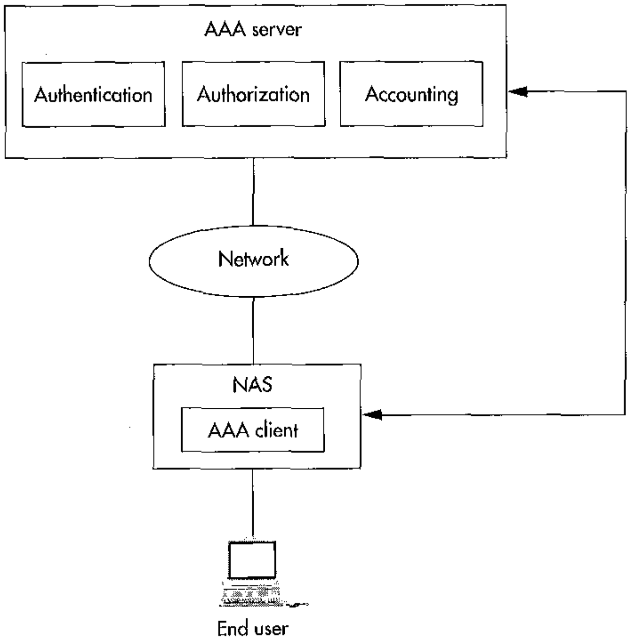

Figure 1. AAA architecture. The AAA client at the network point of entry (NAS) communicates with the AAA server to provide AAA services.

- NAS AAA client function collects and forwards the end user's credentials to the AAA server.
- AAA server processes the data and returns an accept or reject response and other relevant data to the AAA client.
- AAA client on the NAS notifies the end user that access is granted or denied for the specified resources.

The NAS may also send an accounting message to the AAA server during connection setup and termination for record collection and storage.

AAA Computing Needs

One of this architecture's benefits is that the AAA server can be housed on a general-purpose computing system, which can typically be found at a good price-to-performance ratio, offering high-volume disk storage and optimized database administration. This gives dial providers the horsepower needed to process bursts of AAA requests from the many port-dense NAS devices as well as the storage capacity needed to record accounting information on each of the many end-user connections.

A single AAA server can act as a centralized administrative control point for multiple AAA clients contained within different vendor-sourced NAS and network components. Thus, AAA functions can be added to the server, and incrementally to the client, without disrupting existing network functions. There is no need to incur the operational burden of placing AAA information on the NAS itself. The AAA Working Group within the IETF is also currently developing a set of requirements to support AAA across dial, roaming, and mobile IP environments.[1]

RADIUS

The best-known and most widely deployed AAA protocol is RADIUS—a clever acronym for the rather ordinary-sounding Remote Access Dial-In User Service. It was developed in the mid-1990s by Livingston Enterprises (since acquired by Lucent) to provide authentication and accounting services to their NAS devices. The IETF formalized that effort in 1996 with the RADIUS Working Group,[2] and the protocol's basic functions and message formats are documented in RFC 2138.[3] Its functional attributes consist of

- *Client-server-based operations.* A RADIUS client resides on the NAS and communicates over the network with a RADIUS server running on a host computer. Additionally, a RADIUS server may serve as a proxy client for another RADIUS or authentication server.
- *Network security.* All communications between a RADIUS client and server are authenticated by virtue of a shared secret key that is never sent over the network. In addition, user passwords contained in RADIUS messages are encrypted to prevent hackers from reading them by snooping the network.
- *Flexible authentication.* RADIUS can support multiple authentication mechanisms, including PAP and CHAP.
- *Attribute/value pairs.* RADIUS messages carry AAA information encoded in type-length-value fields, called attributes (or attribute/value pairs). Common examples of attributes include User-Name, User-Password, Framed-Protocol (such as PPP), Framed-IP-Address (IP address for end user), and so on. RFC 2138 and vendor-specific documentation contain more complete lists of RADIUS attributes supported by servers and clients.

Figure 2 illustrates a typical configuration employing RADIUS authentication. An end-user dials into a NAS that supports a RADIUS client. Using a prompt, or perhaps PPP frames, the NAS collects the username and password from the end user. It then uses UDP/IP to forward an encrypted Access-Request message over the network to the RADIUS server. The message may also contain attributes such as the NAS port ID and IP address.

The RADIUS server then checks the User-Name attribute for a matching entry stored in its database. If there is no match, then the server returns an Access-Reject message to the NAS along with an optional text message indicating the reason for the failure. The NAS, in turn, notifies the end user of the authentication failure. If a match is found and the password is correct, then the RADIUS server returns an Access-Accept message to the NAS along with any additional configuration information required to complete the connection, such as an IP address for the end user or a filter that limits them to a specific protocol type, like Telnet or HTTP.

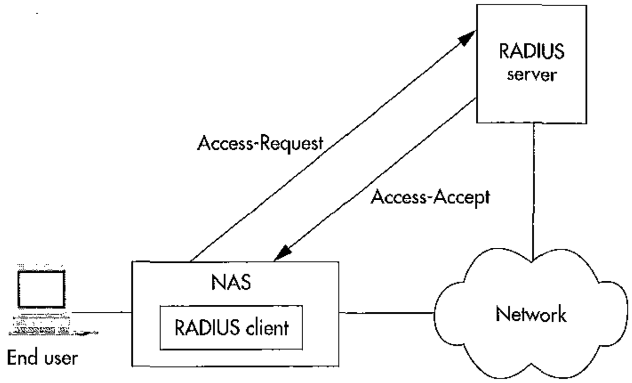

Figure 2. The RADIUS client on the NAS forwards the end user's credentials in an Access-Request message to the RADIUS server. After validating the end user's credentials, the RADIUS server returns an Access-Accept message to the client.

RADIUS Tunnels. RADIUS is also important for provisioning compulsory tunnels in a dial-up virtual private network (dial VPN) environment.4 A compulsory tunnel between the NAS and the corporate network gateway extends the dial end-user's PPP connection all the way to the corporate network so that it appears to be directly attached. Tunneling protocols, like the Layer 2 Tunneling Protocol (L2TP), are used to create the IP tunnels that carry PPP connections through IP networks.[5] The tunnel is compulsory (mandatory) because the end user has no choice in the matter: Any packets destined for the corporate network will flow through the tunnel between the NAS and corporate network gateway.

Figure 3 illustrates how RADIUS supports dial VPN compulsory tunneling. The end user dials into a NAS, and is authenticated by a RADIUS proxy server (the master RADIUS server is maintained inside the corporate network). RADIUS provides authentication services at both ends and assists in provisioning the tunnel by supplying configuration parameters to the NAS in the form of RADIUS attributes. The Access-Accept message from the proxy server to the NAS may also contain tunnel attributes such as the tunnel-type (L2TP, for instance) and tunnel endpoint IP addresses. The NAS then establishes an L2TP tunnel to the corporate network (home) gateway, and the end user is reauthenticated by the same master RADIUS server that was used by the NAS (via proxy) during the initial authentication.

Using RADIUS to authenticate and provision dial VPN compulsory tunnels enhances network security by offering dual authentication from the same corporate-maintained RADIUS server. Further, this approach enables corporate networks to outsource their dial VPN services to other ISPs while retaining strict control over the AAA process. The only requirements are for the ISP to maintain a RADIUS proxy server that contains information on the corporate dial end-user community and for the master to be able to reach it.

RADIUS Accounting. In addition to authentication and authorization, RADIUS was extended to provide a technique for collecting accounting information specific to the end user's communication session and storing it on an accounting server. If the NAS is configured for RADIUS accounting, it forwards an Accounting-Start message to the accounting server as soon as the connection is established and then collects information about the session, including input and output

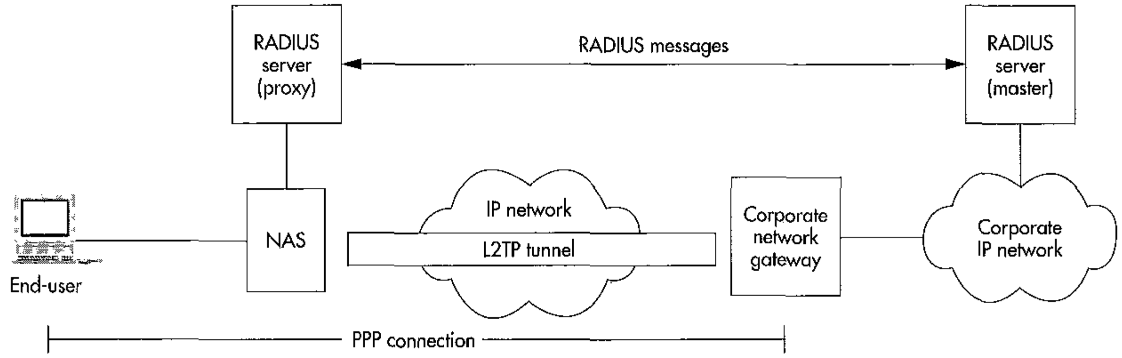

Figure 3. L2TP tunnel establishment using RADIUS. A proxy RADIUS server and master RADIUS server provide AAA services for end-users "tunneling" through an IP network and facilitate L2TP tunnel establishment.

octets, input and output packets, session duration, and termination cause (such as user request or idle timeout). When the session is terminated, the NAS sends an Accounting-Stop message to the server indicating that the session is over. RADIUS accounting is described in RFC 2139.[6]

TACACS+

Another protocol that provides AAA services is the Terminal Access Controller Access Control Systems protocol. Originally described in RFC 1492,[7] it has been reengineered over the years by Cisco and is supported on many terminal servers, routers, and NAS devices found in enterprise networks today. The current version is called TACACS+, which reflects the many enhancements made to the original TACACS protocol.

TACACS+ is a client-server AAA protocol and offers many of the same AAA services as RADIUS. The primary differences are in

- *Transport*. TACACS+ uses TCP as a transport whereas RADIUS uses UDP.
- *Packet encryption*. TACACS+ will encrypt the entire packet payload whereas RADIUS encrypts only the user password.
- *Authentication and authorization*. TACACS+ permits separate authentication and authorization solutions whereas RADIUS combines the two.

Roaming

The significant role performed by AAA protocols in enabling global Internet connectivity cannot be overstated. For example, they will be used to facilitate connectivity for the service known as roaming. Roaming is a generalization of the dial VPN concept in which remote end-users connect to, and are authenticated by, a local (visited) ISP that is different from their home ISP. Roaming service will offer traveling end users fast, convenient, and inexpensive local access to the Internet from anywhere in the world.

Visited ISP RADIUS proxy servers support AAA services in a distributed fashion, and the home ISP maintains a master RADIUS server for its subscriber base to support access control and billing. A third-party server or "broker" could also be used to scale this approach and reduce configuration requirements on the visited proxy servers. In that scenario, AAA data exchanges between the visited and home RADIUS servers would be funneled through the broker.

In addition to the dial VPN for corporate networks, other candidates for roaming service include regional or national ISPs looking to form consortiums to provide broader coverage to a constituency in different geographic areas. One such group is the Global Reach Internet Consortium (GRIC), which offers roaming Internet connectivity and services to its collective subscribers. I-Pass is another that offers its ISP members a roaming authentication and clearinghouse service.

In both cases, a distributed AAA approach enables the home ISP to maintain access control while providing enhanced connectivity services. Roaming customers can access the network through visited ISPs. The IETF has also formed the ROAMOPS Working Group to further study the requirements and solutions for roaming Internet operations.[8]

Diameter Protocol

RADIUS and TACACS+ continue to enjoy widespread support among ISP and enterprise network managers. Both protocols, however, were originally engineered for small network devices supporting just a few end-users requiring simple server-based authentication. Dial providers must now provide AAA services for hundreds and thousands of concurrent end users accessing network services over a variety of technologies. They must also support AAA services across ISP boundaries in a secure and scalable manner. This is beginning to place a burden on the functional capabilities of the existing AAA protocols. Therefore, the IETF has undertaken an effort to develop a next-generation AAA protocol.[9]

AAA Protocol Activity

on the Web

IETF Mobile IP Working Group •
http://www.ietf.org/html.charters/mobileip-charter.html

IETF Network Access Server Requirements Working Group •
http://www.ietf.org/html.charters/nasreq-charter.html

Lucent Technologies' RADIUS Server •
http://www.livingston.com:80/marketing/products/radius.html

Nortel RADIUS Server •
http://www.nortelnetworks.com/products/01/presidepolicy/index.html

TACACS Authentication Protocols •
http://www.cisco.com/warp/public/480/4.html#tacacs+

Global Reach Internet Consortium (GRIC) •
http://www.gric.net/

I-Pass •
http://www.ipass.com/

Merit Network RADIUS-based AAA server •
http://www.merit.edu/aaa/

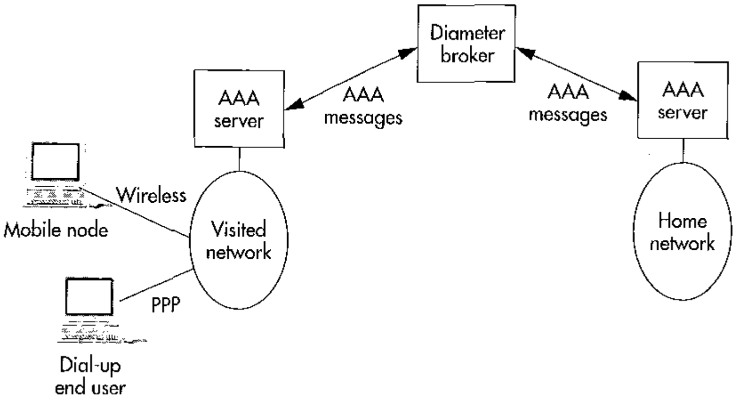

Figure 4. Roaming/mobile IP AAA with Diameter. Diameter brokers AAA information between AAA servers on the visited and home networks.

A New Foundation. Diameter is a lightweight, peer-based AAA protocol designed to offer a scalable foundation for introducing new policy and AAA services over existing (PPP) and emerging (roaming, mobile IP) network technologies.[10] It employs many of the same mechanisms as RADIUS, including UDP transport, encoded attribute/value pairs, and proxy server support.[11]

Diameter also attempts to correct limitations inherent in the RADIUS protocol. For example, a RADIUS attribute value cannot exceed 255 bytes, which may be too small in some cases, and a RADIUS component can only have 255 messages outstanding before an acknowledgment is necessary. For a server or NAS dealing with thousands of individual connections requiring AAA services, these are severe limitations.

Diameter supports a much larger attribute-value length and incorporates a reliable, window-based transport that permits a sender (Diameter server) to transmit as many messages as the receiver (NAS) can handle. Furthermore, while a RADIUS server cannot send unsolicited commands to a client, Diameter permits such interaction, which may be useful if the server needs to instruct the NAS to perform a specific accounting function or terminate a connection.

Diameter also employs an improved retransmission and fail-over scheme that provides improved network resilience over the relatively primitive and slow technique used by RADIUS. And finally, recognizing that AAA cannot afford to be compromised in any way, Diameter provides an end-to-end security mechanism that is not found in RADIUS.

Made to Move. Diameter was designed from the beginning to support roaming and mobile IP networks. Figure 4 illustrates how a Diameter "broker" facilitates AAA service delivery to roaming and mobile IP end users attached to a visited (foreign) network and accessing resources on the home network. In each case, the Diameter server in the visited ISP communicates as a peer with the broker to execute AAA functions.

Any communication between the Diameter servers and the broker is performed over a secure connection because the broker can act as a certificate authority (CA). Distributing certificates to the servers is a much more scalable and effective technique than having all servers share a secret key.

AAA protocols will continue to play a vital role in operating and administering network policies and security. While RADIUS is suitable for now, its inherent scaling limitations will force it to give way to a new solution supporting secure and efficient inter-provider AAA services. In all likelihood, this means introducing Diameter to perform a broker service for ISP-operated RADIUS servers. In addition, some components will employ the directory services provided by the Lightweight Directory Access Protocol (LDAP) to access AAA information from a centralized directory. ■

REFERENCES

1. Internet Engineering Task Force (IETF) Authentication, Authorization, and Accounting (AAA) Working Group Charter; available at http://www.ietf.org/html.charters/aaa-charter.html.
2. IETF Remote Authentication Dial-In User Service (RADIUS) Working Group Charter; available at http://www.ietf.org/html.charters/radius-charter.html.
3. C. Rigney et al., "Remote Authentication Dial In User Service (RADIUS)," IETF RFC 2138, Apr. 1997; available at ftp://ftp.isi.edu/in-notes/rfc2138.txt.
4. D. Kosiur, *Building and Managing Virtual Private Networks*, Wiley Computer Publishing, 1998.
5. W. Townsley et al., "Layer Two Tunneling Protocol," IETF RFC 2661, Aug. 1999; available at ftp://ftp.isi.edu/in-notes/rfc2661.txt.
6. C. Rigney, "RADIUS Accounting," IETF RFC 2139, Apr. 1997; available at ftp://ftp.isi.edu/in-notes/rfc2139.txt.
7. C. Finseth, "An Access Control Protocol, Sometimes Called TACACS," IETF RFC 1492, July 1993; available at ftp://ftp.isi.edu/in-notes/rfc1492.txt.
8. IETF Roaming Operations (ROAMOPS) Working Group Charter; available at http://www.ietf.org/html.charters/roamops-charter.html.
9. P.R. Calhoun, A.C. Rubens, and H. Akhtar, "Diameter Base Protocol," IETF AAA Working Group, Internet draft, Oct. 1999, work in progress.
10. P.R. Calhoun et al., "Diameter Framework Document," IETF AAA Working Group, Oct. 1999, work in progress.
11. R. Ekstein, Y. T'Joens, and B. Sales, "AAA Protocols: Comparison between RADIUS, Diameter, and COPS," IETF NASREQ Working Group, Internet draft, Oct. 1999, work in progress.

Chris Metz is a consulting systems engineer for Cisco Systems. He is the author of *IP Switching: Protocols and Architectures* (McGraw-Hill, 1999).