;login:

THE MAGAZINE OF USENIX & SAGE

April 2001 • volume 26 • number 2

inside:

SYSADMIN

ISPadmin

USENIX & SAGE

The Advanced Computing Systems Association &
The System Administrators Guild

ISPadmin

by Robert Haskins

Robert Haskins is currently employed by WorldNET, an ISP based in Norwood, MA. After many years of saying he wouldn't work for a telephone company, he is now affiliated with one.

<rhaskins@usenix.org>

Remote Authentication Dial-In User Services

Introduction

In this installment of ISPadmin, I examine the lifeblood of any service provider's remote access system: Remote Authentication Dial-In User Services, or RADIUS. RADIUS provides the following functions to service providers in support of their dial-up subscribers:

- Authentication (who can and cannot have access to their network)
- Authorization (specify what services any given user can access)
- Accounting (track usage of services on their network)

In a nutshell, RADIUS is what makes an ISP's dial-up networks function sanely. There are alternatives to RADIUS (such as Cisco's TACACS), but they are not appropriate for anything but the smallest dial-up networks (10 modems or less), as they do not provide nearly enough functionality for service providers.

Exactly What Is RADIUS?

RADIUS is a UDP-based protocol developed by Livingston (now Lucent) expressly for their Portmaster Network Access Server (NAS) hardware in the early 1990s. The protocol is specified by a set of request for comments (RFCs), most currently RFC 2865 for Authentication and Authorization (commonly referred to as AA) and RFC 2866 for Accounting. Together the three functions of Authentication, Authorization, and Accounting are referred to as AAA.

The RADIUS protocol has seen many extensions over the years; a list of RADIUS-related RFCs in the references section. A number of draft Internet Engineering Task Force (IETF) standards relate to RADIUS, most prominently the replacement to the RADIUS protocol (aptly named DIAMETER). The references section also contains a link to the IETF RFC Web site as well as the draft IETF standards Web site.

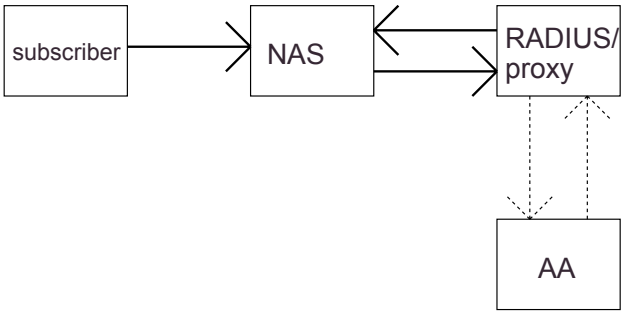

Figure 1

Figure 1 depicts RADIUS functions in the most generic way. A subscriber initiates a connection by dialing into a port on the NAS. After protocol negotiation with the subscriber's machine, the NAS sends a RADIUS "access request" to the RADIUS server to see if that subscriber is allowed onto the network. This request contains, among other things, the subscriber's username and password encrypted with an MD5 hash. (The RADIUS protocol also specifies optional proxy functionality, indicated by the dashed arrows to the box marked "AA" in the diagram.) The RADIUS server returns either a negative response ("access reject") in the case the user is not allowed or a positive response ("access accept") with the access rights for that particular session.

If the server allows access and if RADIUS accounting is configured on the NAS (which it should be for any commercial entity or organization interested in tracking subscriber usage), then the NAS will send an "accounting-start" record to the RADIUS server. Once the session is terminated, the NAS will send an "accounting-stop" record to the RADIUS server to account for the subscriber's usage for that particular session. Some NAS equipment will send what is known as "interim accounting" records

so that the RADIUS accounting server can track sessions in progress. Without such interim records, information about these sessions would be sent too late for use by certain types of applications which require it.

Small Provider Setup

A small provider's goals for AAA services are:

- Low cost, for both initial acquisition and ongoing maintenance
- Simple implementation

A small ISP's primary concern is cost, not features. As a result, a small ISP will probably use a free RADIUS server such as Livingston or Cistron. Also, they are not going to utilize RADIUS proxy functionality but, rather, have one or two RADIUS servers directly answering AA requests and logging accounting records. They will not likely be using the lightweight directory access protocol (LDAP) for end-user authentication or multiple servers to scale the load, as a small provider will not have the traffic to justify it.

Figure 2 outlines how a small ISP might set up their RADIUS infrastructure. Most NAS equipment is configured to be able to send RADIUS requests to (up to) two separate RADIUS servers, for ser-vicing both AA and accounting requests. This means that each NAS can specify up to four different IP addresses for RADIUS servers: a primary and secondary for AA, and a primary and secondary for accounting. (Figure 2 identifies the RADIUS servers by the labels "RAD1" and "RAD2".) Even the smallest ISP will likely utilize two RADIUS servers for redundancy purposes, preferably on separate subnets fed by separate switches/hubs and routers, if possible. This setup does require some additional work on the provisioning system to allow the account and password information to be sent to two RADIUS servers rather than simply one machine.

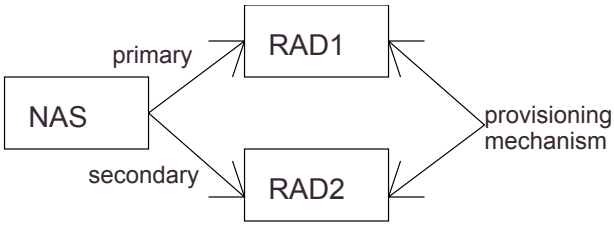

Figure 2

The RADIUS servers are usually set up to accept both AA and accounting requests. Although separate servers can be dedicated to AA and accounting, engineering each RADIUS server to accept all types of requests is a more flexible setup. It does, however, cause some additional work to reconstruct sessions on the back end, as the accounting-start record may go to one server and the accounting-stop record may go to another.

Several free or low-cost RADIUS servers are available to the small-scale operation, including the original Livingston server and its derivatives, such as Cistron and Freeradius.org servers. Also, Microsoft ships a RADIUS server with Microsoft Windows NT 4.0 Option Pack. The RADIUS software module itself is called "Internet Authentication Service," or IAS. These servers are covered in more detail in the "RADIUS Server Software" section below.

Medium/Large Provider Setup

The goals of a medium to large provider differ from those of a small ISP in the areas of functionality, extensibility, performance, and scalability.

A larger service provider will typically utilize a commercial RADIUS server such as Cisco's Access Registrar or create their own modified RADIUS server from one that has available source, such as the Livingston or Merit RADIUS servers. This modification is due to the fact that the original RADIUS servers with available source (Livingston and Merit) typically do not have the functionality and performance required for a 10,000 port or larger network. (According to the Merit Web site, the Merit RADIUS server was

licensed to Interlink Networks in June 2000; it is unclear if source is still available for the Merit RADIUS servers outside of Merit Network affiliates.)

A large provider is concerned about the performance and fault tolerance of the RADIUS server. They do not want a large customer's RADIUS server outage to affect the rest of their customers' ability to utilize their network. If not properly designed, one customer's outage can bring down even a 7,500-port network running Livingston or Merit. Also, wholesale customers usually have a number of authentication servers and would like more than one method of access to them: typically these modes include "round robin" and "fail over." In addition, the ability to set such parameters as server timeouts and number of retries is very desirable.

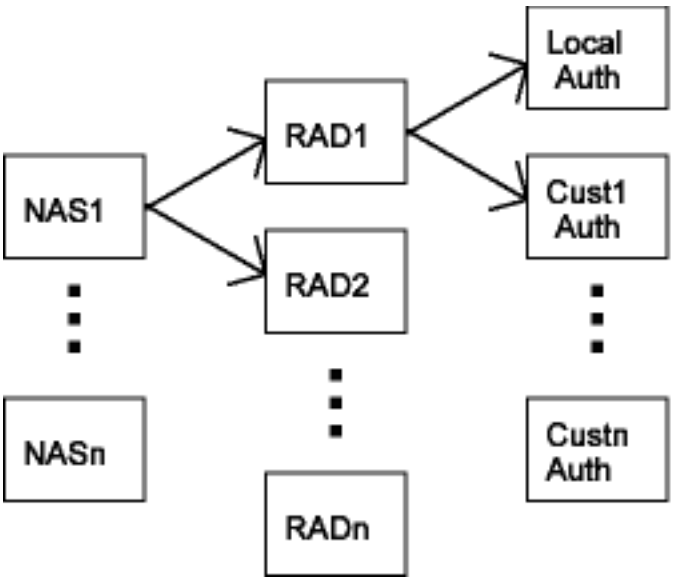

Figure 3

Figure 3 outlines a RADIUS implementation for a medium to large service provider. (Arrows are shown as one-way in the diagram for clarity.) The boxes marked RAD indicate RADIUS servers. These usually act as proxy RADIUS servers (as opposed to end authentication servers) in order to scale operations efficiently. Unlike a small ISP, a larger ISP will often wholesale their service to others, thereby utilizing the RADIUS proxy functionality. The diagram shows this by listing wholesale customer RADIUS servers below the "Local Auth" RADIUS server. "Local Auth" indicates a server that performs local authentication for the larger ISP. This would include retail accounts or virtual ISP services for customers who don't want to house their own servers in order to offer ISP type services (for example retailers, manufacturers, or affinity groups).

Authenticating End Subscribers

There are a number of methods to authenticate end subscribers. Most RADIUS servers support the following techniques:

- UNIX "passwd" file (or the NT equivalent in the case of MS IAS)
- RADIUS "users" text file (based on the original Livingston format)
- RADIUS "users" dbm file (hashed version of the plain text users file)
- SQL database
- LDAP

Only the smallest operations can utilize a UNIX "passwd" file. Most ISPs utilize one of the native RADIUS "users" file formats, usually growing from the plain text format to the hashed format as their business grows. A large service provider will utilize an SQL database or LDAP directory for authentication due to the scalability of these methods.

RADIUS and the Provisioning Process

When talking about RADIUS, one must always discuss provisioning. In a smaller ISP, provisioning is usually achieved by sending account information via a password file (or in the case of authentication via native Livingston RADIUS, a plain text users file or hashed users file) to the various servers that require it. Once the number of users gets too high (approximately 10,000), an alternative method must be used, as the performance of most commercial and open source RADIUS servers begins to suffer. After this threshold is reached, LDAP (or other directory service) or SQL is typically utilized.

LDAP is easily scalable, which is why it is recommended for large service providers. Once the maximum performance is reached on an LDAP server, another one is added

and linked into the LDAP tree. Another benefit to LDAP is the fact that the pluggable authentication module (PAM) directly supports LDAP, which makes integration into other applications (like email) seamless. SQL does not have the wide application support that LDAP has through the integration with PAM, which is why it is not utilized as often as LDAP.

LDAP Integration with RADIUS

Cistron and Livingston RADIUS include support of LDAP through PAM. However, this support is not nearly as thorough as a commercial product like Access Registrar. The Freeradius.org RADIUS server claims to have some built-in support for LDAP, but this author has no experience with it.

Cisco's Access Registrar 1.3 has a number of parameters which can be set when binding with an LDAP server (parameter on the left, example value on the right of the equal sign):

Name = ldap:cust.isp.net
Description = Cust
Protocol = ldap
IPAddress = 1.2.3.4
Port = 389
ReactivateTimerInterval = 300000
Timeout = 15
HostName = ldap.isp.net
BindName = uid=radius,ou=readers,o=isp.net,c=us
BindPassword = password
UseSSL = FALSE
SearchPath = ou=customers,ou=cust,ou=resellers,o=isp.net,c=us
Filter = (uid=%s)
UserPasswordAttribute = userpassword
LimitOutstandingRequests = FALSE
MaxOutstandingRequests = 0
MaxReferrals = 0
ReferralAttribute = <no value>
ReferralFilter = <no value>
PasswordEncryptionStyle = None
LDAPToRadiusMappings/
LDAPToEnvironmentMappings/

RADIUS Server Software

As with most software, RADIUS servers appear in two categories: open source and closed source (commercial). The first RADIUS server was Livingston's 1.x/2.x series of servers, which is the basis for the commonly used Cistron RADIUS server and others. The most recent version of the Livingston server is 2.1, which is available for free (without support) from the Lucent Web site.

The Cistron server is widely used. (It has several variants, including a MySQL back end; see the Cistron page for a complete list.) The Freeradius.org server is a follow-on to the Cistron server. The Freeradius.org server is currently in early alpha stage and not ready for production at this point. Development for these servers should merge at some future point. The current version of the Cistron RADIUS server is 1.6.4.

REFERENCES

Cisco TACACS+ starting point: <http://www.cisco.com/pcgi?bin/Support/PSP/psp_view.pl?p=Internetworking:Tacacs_plus>

Lucent INS (formerly Livingston Enterprises): <http://www.lucent.com/ins/>

RFC Web site: <http://www.ietf.org/rfc.html>

Draft IETF Web site: <http://search.ietf.org/search/brokers/internet-drafts/query.html>

RADIUS-specific draft IETF documents: <ftp://ftp.livingston.com/pub/archive/ietf-radius>

Livingston RADIUS servers (1.x and 2.1): <ftp://ftp.livingston.com/pub/le/radius>

Cistron RADIUS: <http://www.miquels.cistron.nl/radius/>

Freeradius.org: <http://www.freeradius.org>

Microsoft IAS: <http://www.microsoft.com/NTServer/commserv/deployment/moreinfo/ICS_FAQ.asp#4>

White paper on setting IAS: <http://zipdial.ziplink.net/docs/radius-nt.shtml>

Merit Networks: <http://www.merit.edu>

Interlink Networks (formerly Merit RADIUS): <http://www.interlinknetworks.com>

Cisco Access Registrar: <http://www.cisco.com/warp/public/779/servpro/operate/csm/nemnsw/car/prodlit/index.shtml>

LDAP man (articles on configuring LDAP): <http://www.ldapman.org>

Linux-PAM: <http://www.lyre-mit-edu.lkams.kernel.org/pub/linux/libs/pam/>

WideSpan from Bridgewater Systems: <http://www.bridgewatersystems.com/products/widespan/index.html>

RFCs related to the RADIUS protocol:

RFC 1227 SNMP MUX Protocol and MIB

RFC 2107 Ascend Tunnel Management Protocol – ATMP

RFC 2548 Microsoft Vendor-specific RADIUS Attributes

RFC 2607 Proxy Chaining and Policy Implementation in Roaming

RFC 2618 RADIUS Authentication Client MIB

RFC 2619 RADIUS Authentication Server MIB

[continued]

RFC 2620 RADIUS Accounting Client MIB

RFC 2621 RADIUS Accounting Server MIB

RFC 2809 Implementation of L2TP Compulsory Tunneling via RADIUS

RFC 2865 Remote Authentication Dial-In User Service (RADIUS)

RFC 2866 RADIUS Accounting

RFC 2867 RADIUS Accounting Modifications for Tunnel Protocol Support

RFC 2868 RADIUS Attributes for Tunnel Protocol Support

RFC 2869 RADIUS Extensions

RFC 2881 Network Access Server Requirements Next Generation (NASREQNG) NAS Model

RFC 2882 Network Access Servers Requirements: Extended RADIUS Practices

Another server which has been around for some time is the Merit AAA server (now licensed to Interlink Networks). Originally, the Merit server was distributed in two versions: AA and AAA. The AA version was free and the AAA was licensed for a fee. The future of the Merit AA server (the free version) for non-Merit-affiliated organizations is unclear. The AAA version will be maintained by the Interlink Networks organization. BSDi shipped a version of the Merit AA server as part of the distribution of BSD/OS.

Microsoft ships IAS (as part of the NT 4.0 Option Pack), which is a RADIUS server. It is an acceptable RADIUS server for smaller NT-only shops and the UNIX averse. The references contains a pointer to an excellent white paper covering the setup of a Microsoft IAS server.

A number of commercial RADIUS servers are available on the market. Two common stand-alone servers are Cisco's Access Registrar and Funk's Steel-Belted RADIUS. Many RADIUS servers are part of other larger software applications (e.g., ISP billing systems, provisioning systems, and policy management systems). However, stand-alone RADIUS servers are moving toward integrating policy management into them. WideSpan from Bridgewater Systems is an example of such a system.

Both the Access Registrar and Steel-Belted RADIUS/SPE (the Service Provider Edition) are designed expressly for the service provider market. Funk also has versions for the non-service provider market, as well as NT. Access Registrar was designed expressly for the telephone company market. Incidentally, Ziplink was the first ISP to deploy Access Registrar in a traditional ISP setting in October 1998.

Conclusion

RADIUS has three functions: authentication, authorization, and accounting. It is defined by a number of RFCs and is implemented by NAS equipment and software running on dedicated servers. Small ISPs design their infrastructure for low cost, while larger ISPs are more concerned about functionality, scalability, extensibility, and performance. Small ISPs tend to utilize open source RADIUS servers like Livingston 2.1 or Cistron. Larger providers tend to utilize commercial RADIUS servers like Access Registrar or Steel-Belted RADIUS/SPE and an LDAP back end.

Next time, I'll take a look at the topic of ISP billing systems and provisioning systems. In the meantime, please send your comments on UNIX, systems administration, the ISP industry, or related areas to me. I'd love to hear from you!