Patton Tech Notes
About RADIUS

Synopsis

This Tech Note covers the basics of the RADIUS protocol. It defines key terms and provides an overview of RADIUS services and procedures. It gives a concise history of the relevant standards, cites those which Patton supports, and lists selected sources for RADIUS software -- both free and for purchase. Finally, online resources for more information are provided. To learn how to configure a Patton RAS for RADIUS, please read the Patton Tech Note *Configuring RADIUS for Patton RAS Products* at http://www.patton.com/technotes/ras_configuring_radius.pdf

What Is RADIUS?

Remote Authentication Dial-In User Service (RADIUS) is a data-communications protocol designed to provide security management and statistics collection in remote computing environments, especially for distributed networks with dial-in users. A central database, the RADIUS Server, maintains network security data (such as user profiles) and statistics (such as bytes transmitted and received). Centrally stored security data is more secure, easier to manage, and scales more smoothly than data scattered throughout the network on multiple devices.

RADIUS Client/Server Architecture

RADIUS operates on the client/server model. A *RADIUS Authentication Server* provides security services and stores security data. A *RADIUS Accounting Server* collects and stores statistical data. Most often a single machine provides both functions, however the two RADIUS servers may reside on separate machines. Network managers may configure a RADIUS Client to use RADIUS security services, RADIUS accounting services, or both.

A RADIUS *client* consists of a *Network Access Server (NAS)* -- such as your Patton RAS – which provides one or more remote users with access to network resources. A single RADIUS Server can serve hundreds of RADIUS clients and up to tens of thousand of end users. Fault tolerance and redundancy concerns can be addressed by configuring a RADIUS client to use one or more alternate RADIUS servers. A NAS (your Patton RAS) can access a local RADIUS Server on the connected LAN, or a remote RADIUS Server via WAN connections.

PATTON Electronics Co.
7622 Rickenbacker Drive, Gaithersburg, MD USA 20879
Phone 1.301.975.1000 Fax 1.301.869.9293
http://www.patton.com

RADIUS Services

AAA. RADIUS provides three network services, known as authentication, authorization, and accounting, or AAA. These services give network managers an easy way to:

- *Identify* remote users, and *Control* which users can access the network (*authentication*)
- *Define* what each user can do by controlling access to network resources (*authorization*)
- *Track* what resources each user consumes in order to bill them for services (*accounting*).

RADIUS login procedures combine authentication and authorization services to provide security functions.

Authentication is essentially a login procedure involving a username and password: the process by which the network validates a dial-in user's identity – distinguishing a legitimate user from a malicious or mischievous hacker. RADIUS supports multiple authentication protocols including Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP) (RFC 1994), as well as Unix login. PAP and CHAP are specified within the Point-to-Point Protocol (PPP) authentication procedures (RFC 1661). To prevent interception by snoopers on the network, RADIUS encrypts user passwords for transmission between client and server.

A RADIUS Authentication Server will respond to requests from known clients and discard requests from unknown clients. Before authenticating any users, the NAS (your Patton RAS) must validate it's own identity by authenticating with the RADIUS server using a common *shared secret.*

The shared secret is a text string configured on both the RADIUS client and server, and is never sent across the network in its pure original form. During authentication, the RADIUS server sends a random number to the NAS, which is combined with the shared secret using a hash-code algorithm (RSA Message Digest Algorithm MD5), and then sent back to the RADIUS server. The RADIUS server will decode the received message for validation against its own copy of the shared secret. The RAS will disconnect users that fail to authenticate with the RADIUS server.

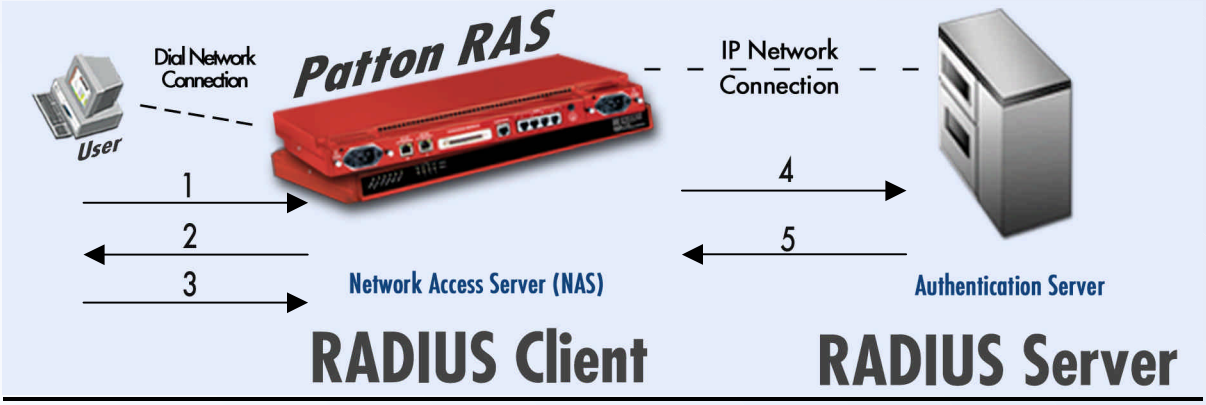
Authorization is the process of restricting and enabling what each user can do. RADIUS servers are responsible for knowing which services and privileges a given user may legitimately access (for example, PPP, SLIP, Telnet, rlogin), and returning that information to the communications server when the user successfully authenticates.

Accounting is the process of collecting and reporting statistics. The RADIUS Accounting server collects and stores the statistics sent by RADIUS clients and responds to client queries for statistics. These data include user login times and durations, packets sent/received, bytes sent/received, and so on, and may be used for billing, traffic and performance analysis, and troubleshooting.

PATTON Electronics Co.
7622 Rickenbacker Drive, Gaithersburg, MD USA 20879
Phone 1.301.975.1000 Fax 1.301.869.9293
http://www.patton.com

RADIUS Authentication Procedure

The procedure for RADIUS authentication and authorization is outlined below:



1. User dials into the RAS and establishes a connection.
2. The RAS prompts for user ID and password (PAP) or challenge (CHAP).
3. User responds with user ID and password (PAP) or challenge response (CHAP).
4. RAS forwards an Authentication Request Packet to the RADIUS Server, containing user identification, encrypted password, and RAS identification.
5. RADIUS Server validates the user and sends the RAS an Authentication Acknowledgement packet containing user configuration and either
   a) Specifying what network services and privileges the RAS should provide to the user *(Access-accept)*, or
   b) Denying the Authentication Request *(Access-reject)*.

RADIUS Standards

RADIUS was initially developed in January 1977 by Lucent Technologies on recommendation from the Internet Engineering Task Force (IETF). The second generation IETF Standards for RADIUS (RFC 2138) and RADIUS Accounting (RFC 2139) were published in April 1977. The second set of RFCs changed the assigned UDP port number for RADIUS from 1645 (conflicting with "`datametrics`" service) to 1812, and changed the assigned UDP port number for RADIUS Accounting from 1646 (conflicting with "`sa-msg-port`" service) to 1813. The April 1977 standards have been widely implemented and remain extensively deployed in public and private networks.

PATTON Electronics Co.
7622 Rickenbacker Drive, Gaithersburg, MD USA 20879
Phone 1.301.975.1000 Fax 1.301.869.9293
http://www.patton.com

RADIUS Resources

Patton Tech Notes:

Configuring RADIUS for Patton RAS Products
http://www.patton.com/technotes/ras_configuring_radius.pdf

RADIUS Standards Specifications

http://www.ietf.org/rfc/rfc2138.txt	(Authentication, April 1977)
http://www.ietf.org/rfc/rfc2139.txt	(Accounting, April 1977)
http://www.ietf.org/rfc/rfc2865.txt	(Authentication, June 2000)
http://www.ietf.org/rfc/rfc2866.txt	(Accounting, June 2000)

PPP Standard Specification
http://www.faqs.org/rfcs/rfc1331.html

Lucent White Paper
http://portmasters.com/marketing/whitepapers/radius_paper.html

Cisco: How Does RADIUS WORK?
http://www.cisco.com/warp/public/707/32.html

Microsoft: RADIUS Security and Best Practices:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/itsolutions/network/maintain/security/radiusec.asp

Intel: RADIUS Overview
http://support.intel.com/support/si/library/bi0407.htm

PATTON Electronics Co.
7622 Rickenbacker Drive, Gaithersburg, MD USA 20879
Phone 1.301.975.1000 Fax 1.301.869.9293
http://www.patton.com