Remote Authentication Dial In User Service (RADIUS)

Status of this Memo

   This document specifies an Internet standards track protocol for the
   Internet community, and requests discussion and suggestions for
   improvements. Please refer to the current edition of the "Internet
   Official Protocol Standards" (STD 1) for the standardization state
   and status of this protocol. Distribution of this memo is unlimited.

Abstract

   This document describes a protocol for carrying authentication,
   authorization, and configuration information between a Network Access
   Server which desires to authenticate its links and a shared
   Authentication Server.

Implementation Note

   This memo documents the RADIUS protocol. There has been some
   confusion in the assignment of port numbers for this protocol. The
   early deployment of RADIUS was done using the erroneously chosen port
   number 1645, which conflicts with the "datametrics" service. The
   officially assigned port number for RADIUS is 1812.

Table of Contents

1. Introduction

   Managing dispersed serial line and modem pools for large numbers of
   users can create the need for significant administrative support.
   Since modem pools are by definition a link to the outside world, they
   require careful attention to security, authorization and accounting.
   This can be best achieved by managing a single "database" of users,
   which allows for authentication (verifying user name and password) as
   well as configuration information detailing the type of service to
   deliver to the user (for example, SLIP, PPP, telnet, rlogin).

   Key features of RADIUS are:

   Client/Server Model

      A Network Access Server (NAS) operates as a client of RADIUS. The
      client is responsible for passing user information to designated
      RADIUS servers, and then acting on the response which is returned.

      RADIUS servers are responsible for receiving user connection
      requests, authenticating the user, and then returning all
      configuration information necessary for the client to deliver
      service to the user.

      A RADIUS server can act as a proxy client to other RADIUS servers
      or other kinds of authentication servers.

   Network Security

      Transactions between the client and RADIUS server are
      authenticated through the use of a shared secret, which is never
      sent over the network. In addition, any user passwords are sent
      encrypted between the client and RADIUS server, to eliminate the
      possibility that someone snooping on an unsecure network could
      determine a user's password.

Flexible Authentication Mechanisms

   The RADIUS server can support a variety of methods to authenticate
   a user. When it is provided with the user name and original
   password given by the user, it can support PPP PAP or CHAP, UNIX
   login, and other authentication mechanisms.

Extensible Protocol

   All transactions are comprised of variable length Attribute-
   Length-Value 3-tuples. New attribute values can be added without
   disturbing existing implementations of the protocol.

1.1. Specification of Requirements

   In this document, several words are used to signify the requirements
   of the specification. These words are often capitalized.

   MUST   This word, or the adjective "required", means that the
              definition is an absolute requirement of the specification.

   MUST NOT   This phrase means that the definition is an absolute
              prohibition of the specification.

   SHOULD   This word, or the adjective "recommended", means that there
              may exist valid reasons in particular circumstances to
              ignore this item, but the full implications must be
              understood and carefully weighed before choosing a
              different course.

   MAY   This word, or the adjective "optional", means that this
              item is one of an allowed set of alternatives. An
              implementation which does not include this option MUST be
              prepared to interoperate with another implementation which
              does include the option.

1.2. Terminology

   This document frequently uses the following terms:

   service   The NAS provides a service to the dial-in user, such as PPP
             or Telnet.

   session   Each service provided by the NAS to a dial-in user
             constitutes a session, with the beginning of the session
             defined as the point where service is first provided and
             the end of the session defined as the point where service
             is ended. A user may have multiple sessions in parallel or
             series if the NAS supports that.

   silently discard
             This means the implementation discards the packet without
             further processing. The implementation SHOULD provide the
             capability of logging the error, including the contents of
             the silently discarded packet, and SHOULD record the event
             in a statistics counter.

2. Operation

   When a client is configured to use RADIUS, any user of the client
   presents authentication information to the client. This might be
   with a customizable login prompt, where the user is expected to enter
   their username and password. Alternatively, the user might use a
   link framing protocol such as the Point-to-Point Protocol (PPP),
   which has authentication packets which carry this information.

   Once the client has obtained such information, it may choose to
   authenticate using RADIUS. To do so, the client creates an "Access-
   Request" containing such Attributes as the user's name, the user's
   password, the ID of the client and the Port ID which the user is
   accessing. When a password is present, it is hidden using a method
   based on the RSA Message Digest Algorithm MD5 [1].

   The Access-Request is submitted to the RADIUS server via the network.
   If no response is returned within a length of time, the request is
   re-sent a number of times. The client can also forward requests to
   an alternate server or servers in the event that the primary server
   is down or unreachable. An alternate server can be used either after
   a number of tries to the primary server fail, or in a round-robin
   fashion. Retry and fallback algorithms are the topic of current
   research and are not specified in detail in this document.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.