RADIUS Security For Legacy Applications

Overview

Changes in the network are inevitable. New technologies are continually being developed to make networking faster. For example, new protocols such as PPP and IP swept into the network arena, providing access to millions of Internet sites and seemingly obsoleting serial data transmission methods using dial-in modems. As new modems are added to a computer or communications server on a corporate network, that network becomes more vulnerable to security breaches. Network managers are left with serious security problems, and state-of-the-art security systems generally require special hardware or are only compatible with a small number of products.

To answer many of the Internet's security needs, a new standard of authentication was required. Remote Authentication Dial In User Service (RADIUS) brought a client-server architecture to ISPs, enabling efficient, secure authentication of dial-in users. RADIUS manages a database of users, provides authentication so that the dial-in user is allowed access, and delivers configuration information detailing the type of service to deliver to the user — such as SLIP, PPP, telnet, etc.

As networks grow increasingly complex — both in size and technology — network managers are also faced with the challenge of minimizing downtime. With literally hundreds of locations to keep up and running, network managers seek solutions that enable them to remotely manage all of the devices in the network.

Many have turned to the Internet as the solution. Inband management via the Internet offers many benefits, chief among them security. However, Internet-based solutions have one major flaw: reliance on the very network the solutions are intended to manage. If part of the network goes down, remote management disappears with it.

In addition, much of the legacy equipment simply does not have the appropriate networking ports to allow Internet-based management. These older devices, such as PBXs, X.25 pads, and Front End Processors (FEPs), are only manageable through their serial port. To further complicate matters, each of these devices has their own — often proprietary — management method.

Ironically, some legacy security measures create problems for LAN or Internet based solutions. Many UNIX servers do not allow reconfiguration via network connections. Early network designers did not want remote users to be able to significantly reconfigure the devices — possibly rendering them useless.

Clearly, network managers need a standards-based solution that enables remote management via a serial port, while protecting the network from unauthorized users and destructive hackers.

The Solution

Just as RADIUS answered the needs of ISPs for security, network managers can use dial-in serial connections for remote management, providing contact with every device in the network. This provides the perfect way to authenticate users of legacy equipment and applications.

General DataComm

General DataComm

Key features of RADIUS include:

- Client/Server Model

  A Network Access Server (NAS) — operating as a client of RADIUS — passes user information to designated RADIUS servers and acts upon the response. RADIUS servers receive connection requests, authenticate the users and return the appropriate configuration information.
- Network Security

  Authentication occurs through a "secret" that the RADIUS client and server share, but never sent over the network. User passwords are encrypted, eliminating the possibility that hackers can determine any passwords.
- Flexible Authentication Mechanisms for Legacy Applications

  GDC's RADIUS for legacy applications supports ASCII Async formats used by Terminal Emulation Programs.
- RADIUS Servers are Industry Standard

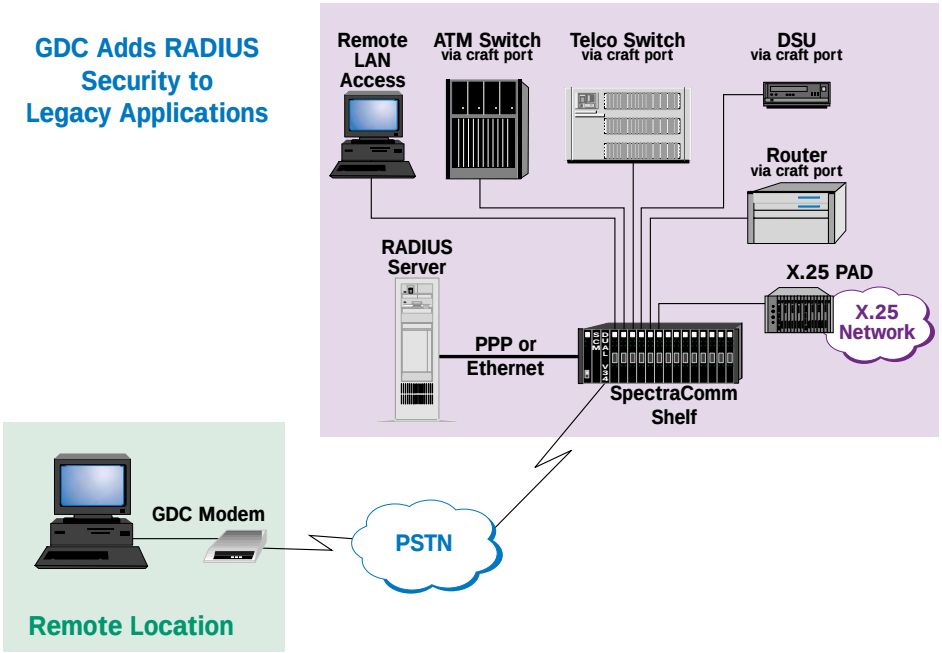
  Easy to maintain and manage database of passwords stored in the RADIUS Server.

GDC's Implementation of RADIUS

GDC's SpectraComm Manager (SCM), Dual V.34 and single SpectraComm V.34 modems' management support RADIUS Security. The V.34 modems prompt the user for name and password and forward this information to the RADIUS server. The RADIUS server authenticates the user and returns a message to the modem to grant or deny access. Optionally, the RADIUS server may challenge the remote user and request additional information before granting access.

GDC's modems offer additional protection from "hackers" via GDC's patented SteadFast Security®. This exclusive system delivers multiple levels of security, providing additional or fail-safe protection if the RADIUS server is out of service.

GDC Adds RADIUS Security to Legacy Applications



The only analog V.34 NEBS-compliant modems with RADIUS Authentication for Secure Dial-In Access. Enables the addition of RADIUS security to legacy applications such as PBXs, X.25 PADs, craft ports, and FEPs for ASCII Asynchronous standards-based remote management.

Note: Some products and features may still be in development

World Headquarters
Middlebury, Connecticut USA 06762-1299 • Tel: 1-203-574-1118 • Fax: 1-203-758-9468 • 1-203-758-9518 (GDC International) • www.gdc.com

Printed in U.S.A XXXXXXAB-1100YA