Ascend

Technical Overview

RADIUS

Remote Authentication Dial-in User Service

May 14, 1996

ASCEND

TABLE OF CONTENTS

Page

1.0 Introduction 2

2.0 RADIUS Protocol Overview 4

3.0 Benefits of Ascend Radius 5

4.0 RADIUS Platforms 5

5.0 RADIUS Applications 6

5.1 Simple RADIUS Authentication and Accounting 6

5.2 RADIUS Authentication and Accounting with Backup Servers 7

5.3 RADIUS with Security Dynamics SecureID 7

5.4 RADIUS with Enigma Logic’s SafeWord 9

5.5 RADIUS with External Database 11

5.6 RADIUS to sign-up new customers 12

6.0 How to obtain Ascend RADIUS 13

1.0 INTRODUCTION

RADIUS (Remote Authentication Dial-In User Service) is an emerging security administration standard that provides management services to authentication servers on a distributed network. It was developed for service providers and corporations that need a flexible, non-proprietary protocol for centralized user authentication, password encryption, service selection, filtering and call accounting. As of May 1996, RADIUS is currently in the process of being approved by the Internet Engineering Task Force (IETF) as an industry-wide standard.

RADIUS functions as an information clearinghouse that stores authentication information about all of a network's users as well as complete user profiles consisting of access restrictions, destination-specific routing, packet filtering and billing information. Used in conjunction with PAP/CHAP or other third-party authentication servers, a single RADIUS database server can administer multiple security systems across complex networks and maintain security profiles for thousands of users.

The main features of RADIUS are :

- User Identification
- User Authentication
- User Authorization and User Profile Information
- Call Accounting

The term “RADIUS” refers to the software program that runs on a server, as well as the protocol that allows Network Access Server (e.g. the MAX) to interoperate with a RADIUS server.

Ascend RADIUS

RADIUS has gained widespread popularity since it was introduced three years ago. It is now used by a majority of service providers and corporations with large-scale security requirements. The Ascend implementations of RADIUS supports standard RADIUS attributes/features as well as an extensive set of Ascend-specific attributes/features that allow network managers to more effectively manage their network resources. In fact, Ascend has taken the lead in expanding the popularity of RADIUS by defining these Ascend-specific attributes.

How RADIUS Works

When remote users with modems, ISDN terminal adapters or bridge/routers request access to a RADIUS-managed network, a network access server, such as the MAX, answers the call. The MAX obtains the user name and password and attempts to authenticate the user locally (i.e. at the network access server). If the information is not available locally, then it forwards that information to the RADIUS server for authentication. Once the user is authenticated, the RADIUS server passes the authentication information back to the MAX or other network access server, along with the user profile information contained in the RADIUS database. The user is then granted access to the network according to the settings contained in the RADIUS profile.

***Figure*-1.1**

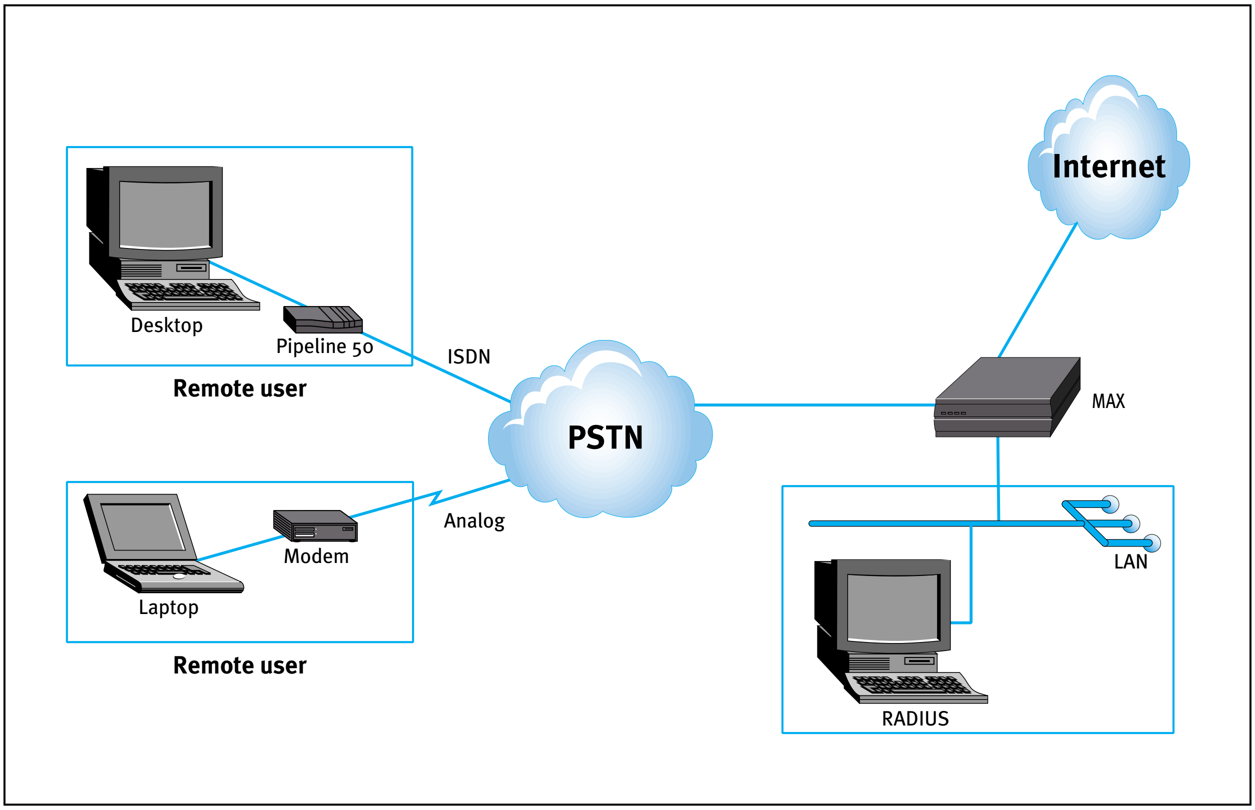


***Figure*-1.1.** In the above example, a laptop user with an analog modem or a desktop user with a Pipeline 50 router dials into a MAX. The MAX obtains the user's name and password using either PAP or CHAP. If user authentication information is not available in the MAX database, it then forwards the authentication request to the RADIUS server. If the RADIUS server authenticates the user, it sends the user profile information to the MAX and the MAX then completes the connection according to the parameters in the RADIUS profile. If the RADIUS server denies the request, the MAX terminates the call.

Once the remote user has been authenticated and a network connection established, the MAX notifies the RADIUS server that the session has begun. The MAX notifies the RADIUS server again when the session ends. In this way, accounting records kept by RADIUS can be used by service providers for billing purposes or by MIS managers to charge back departments within a corporation.

2.0 RADIUS OVERVIEW

A RADIUS server consists of two parts:

- Authentication
- Accounting

For a RADIUS server to distinguish between authentication information and accounting information, the two different types of information must use different User Datagram Protocol (UDP) ports. Authentication information is communicated via UDP port 1645; accounting information is communicated via UDP port 1646. Authentication information and accounting information can operate on different ports of the same RADIUS server or on different RADIUS servers on different systems.

To provide another level of security, RADIUS servers authenticate not only the end user that dials into the network, but also the network access server or MAX that the user dials into. In other words, a RADIUS server only accepts authentication requests from network access servers it has been able to authenticate for itself.

To provide separate authentication for end-users and for network access servers, RADIUS maintains two separate files called "Clients" and "Users."

The "Users" file consists of:

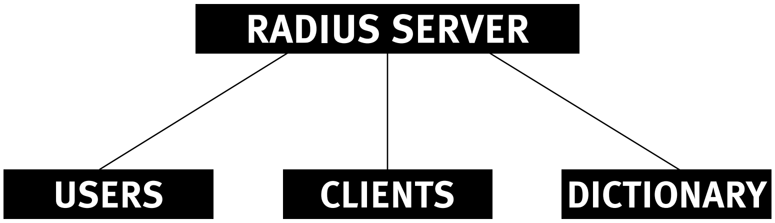
- Username
- Password
- Other parameters or attributes such as IP address, subnet mask, framed protocol, etc.

The "Clients" file consists of:

- Client name
- Client password

The client is the Network Access Server such as MAX.

A third file called the "Dictionary" file, which is not generally configured by a service provider or corporation, but included as part of the RADIUS server, determines the types of attributes that may be used in the "Users" file. It consists of all the attributes that may be supported by RADIUS.



** For more information about the “Users”, “Clients” and “Dictionary” files, refer to the Security and RADIUS Supplements of the MAX documentation set.*

3.0 BENEFITS OF ASCEND RADIUS

RADIUS server with the Ascend dictionary, provides users with numerous benefits:

Widely Used:
Ascend RADIUS with Ascend extensions is one of the most widely used authentication servers on the market today.

Increased Attributes:
Ascend has added over 70 specific attribute extensions to its version of RADIUS in addition to the standard attributes defined in the RADIUS specification. These extensions are extremely useful for telephone companies, Internet Service Providers and corporate customers for efficiently managing the network resources.

Flexibility:
The Ascend version of RADIUS does not limit the UDP ports that RADIUS can use to ports 1645 and 1646. Because of its flexibility in handling UDP ports, Ascend RADIUS is an ideal solution in cases where users have defined or allocated these ports for other purposes.

Wider Authentication Support:
Ascend's version of RADIUS supports a wide range of authentication devices and mechanisms including:

- Local passwords on RADIUS
- UNIX passwords
- Enigma Logic's SafeWord Dynamic Password library
- Token caching
- Security Dynamics' ACE/server
- RADIUS/LOGOUT for remote validation of incoming calls
- Password expiration

Filtering:
Ascend RADIUS supports call, data and generic filtering, a feature which manages and controls the type of applications and resources an end user can access, such as Telnet, WWW and FTP. For increased network security, the filtering can be configured based on source/destination IP addresses, protocols and port numbers.

Generic filtering provides similar filtering capability for other protocols such as IPX and NetBIOS.

4.0 RADIUS PLATFORMS

The Ascend RADIUS server runs on the following platforms:

- IBM AIX
- HP-UX
- SCO UNIX
- SunOS
- Solaris with GCC
- Solaris with CC
- Unixware
- BSDI
- Linux
- SGI IRIX

5.0 APPLICATIONS

5.1 Simple RADIUS Authentication and Accounting

Figure-5.1

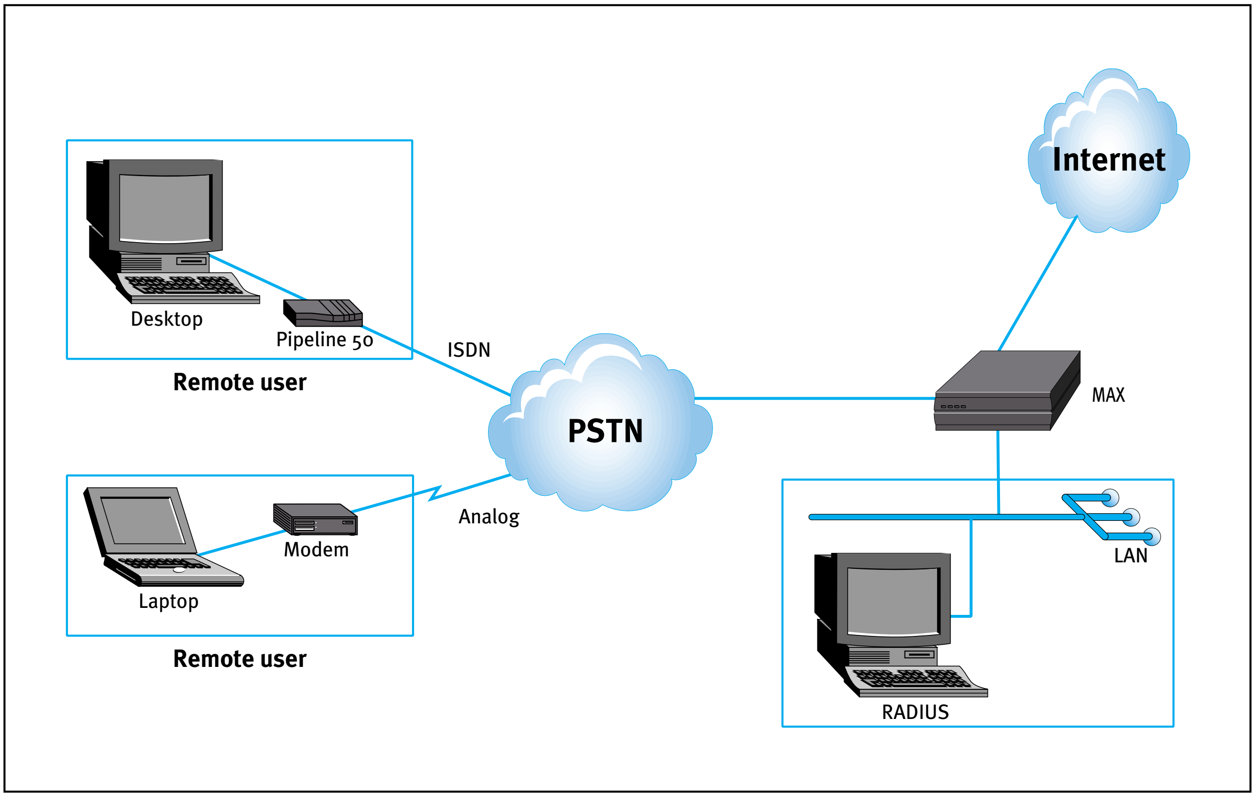


Figure 5.1 This simple network configuration is ideal for cost-conscious service providers and corporations that do not want to invest in different machines for security and backup. Here, the RADIUS server resides on a LAN where it performs the authentication. The same RADIUS server is also acting as an accounting server and collects accounting information.

5.2 RADIUS Authentication and Accounting With Backup Servers

Figure-5.2

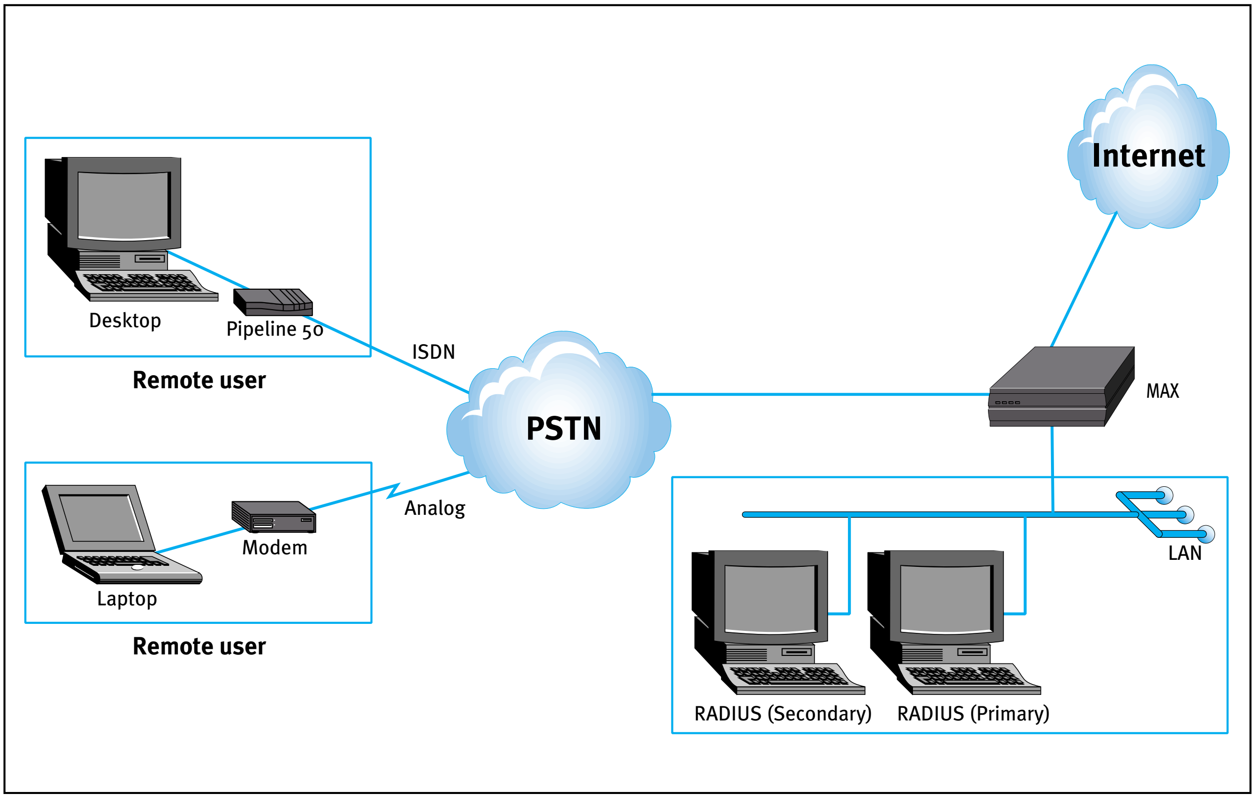


Figure 5.2 In this example, a service provider or corporate client has a second RADIUS server performing as a backup. If the primary RADIUS server fails, the MAX automatically contacts the secondary RADIUS server to authenticate a user. If the secondary server fails, a third RADIUS server can be used for authentication. Customers also can use one RADIUS server for authentication information and the other for accounting information.

5.3 RADIUS with Security Dynamics' ACE/Server System

For more secure networks, service providers and corporate customers can use RADIUS as a front end to a Security Dynamics' ACE/Server system.

Security Dynamics' ACE/Server is a dynamic password authentication system that provides a greater level of authentication than traditional name/password logins offered by terminal servers and host computers. Security Dynamics' solution is commonly used by Fortune 1000 companies, government agencies and customers in the banking, financial services and pharmaceutical industries.

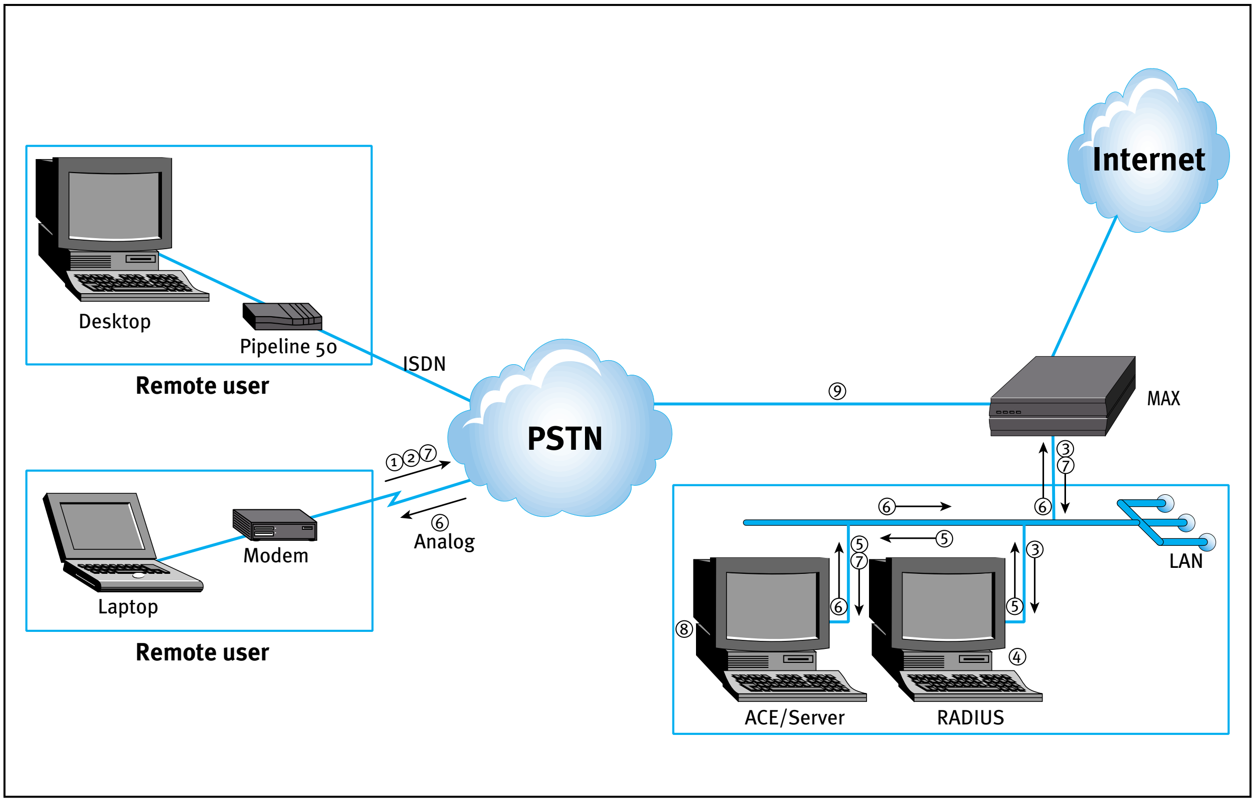
Security Dynamics' solution consists of two parts:

- SecureID token cards carried by each end user
- ACE/Server software that runs on a central site server that actually authenticates the user

SecureID, a hand-held token the size of a credit card, displays a randomly generated access code that automatically changes every 60 seconds. Each token is time-synchronized with the ACE/Server.

ACE/Server runs on SunOS/Solaris, IBM AIX, HP-UX, Microsoft NT/RAS, Digital UNIX, Digital Ultrix, SGI IRIX, SCO UNIX, Novell Netware and other platforms.

Figure - 5.3



How does the ACE/Server solution work?

1. Remote user initiates the call to the MAX
2. Remote user sends username to MAX
3. MAX after attempting to authenticate locally, forwards the information to RADIUS
4. Radius forwards the information to ACE client residing on the same system as the RADIUS
5. ACE client forwards the information to ACE/server
6. ACE/server sends the challenge back to the user through ACE client, RADIUS and MAX
7. User answers the challenge with the one-time only password within 60 seconds
8. ACE/server authenticates the user
9. MAX establishes the connection with the user if authentication succeeds; if authentication fails, it terminates the call.

The user may either be in the terminal server mode or use the Ascend Password Protocol (APP) utility during the authentication phase. Once the authentication is complete then the user may switch to PPP mode.

5.4 RADIUS with Enigma Logic's SafeWord

For more secure networks, service providers and corporate customers can use RADIUS as a front end to the Enigma Logic's SafeWord Server.

SafeWord is a dynamic password authentication system that provides a greater level of authentication than traditional name/password logins offered by terminal servers and host computers.

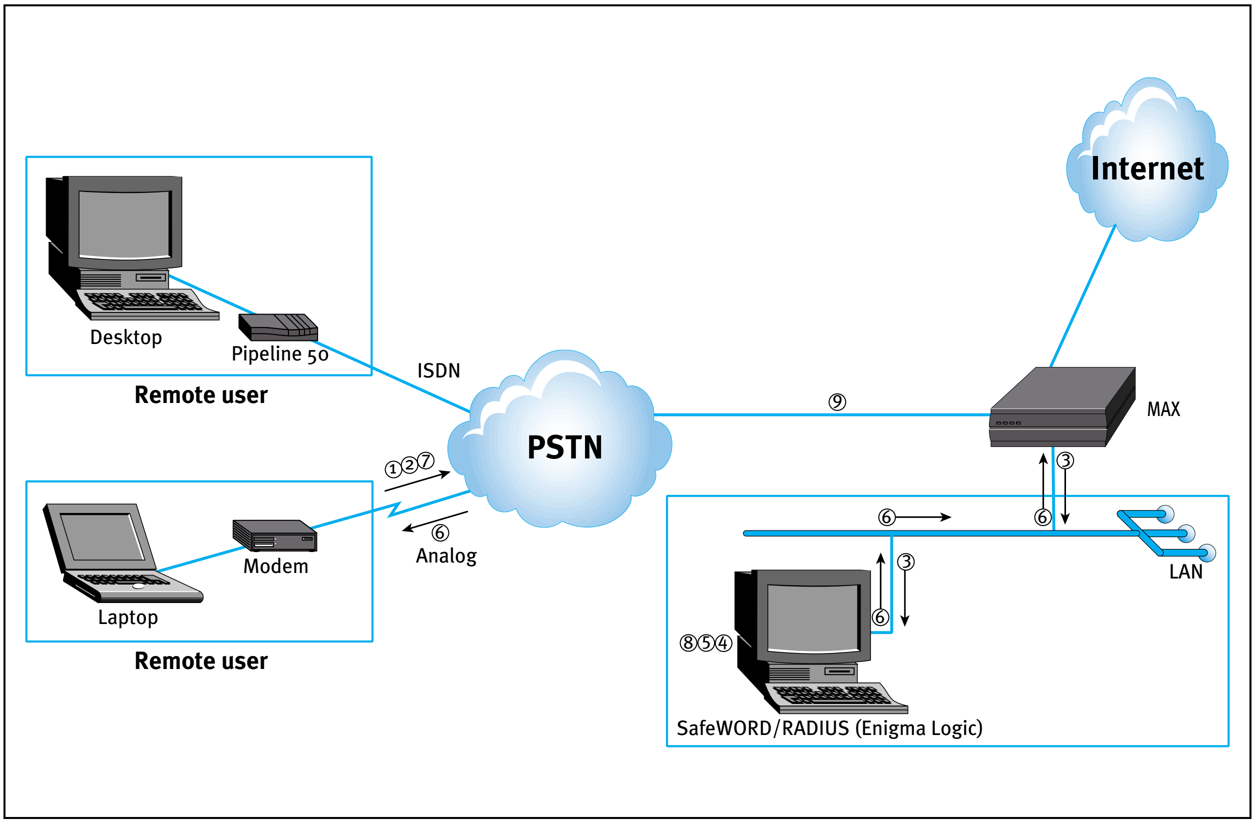
SafeWord consists of:

- Hand-held token cards carried by the end user
- SafeWord Server, software running on a server at the central site that actually performs the authentication for the user

The SafeWord server runs on SunOS/Solaris, IBM AIX, HP-UX, SCO UNIX, Novell Netware, Linux, Ultrix and other platforms.

SafeWord supports the following token cards: ActivCard, CryptoCard (CryptoCard), DES Gold (Enigma Logic), DES Silver (Enigma Logic), SafeWord SofToken (Enigma Logic), SafeWord MultiSync (Enigma Logic), DigiPass (Digiline), SecureNet Key (Digital Pathways) and WatchWord (Racal).

Figure-5.4



How does SafeWord function?

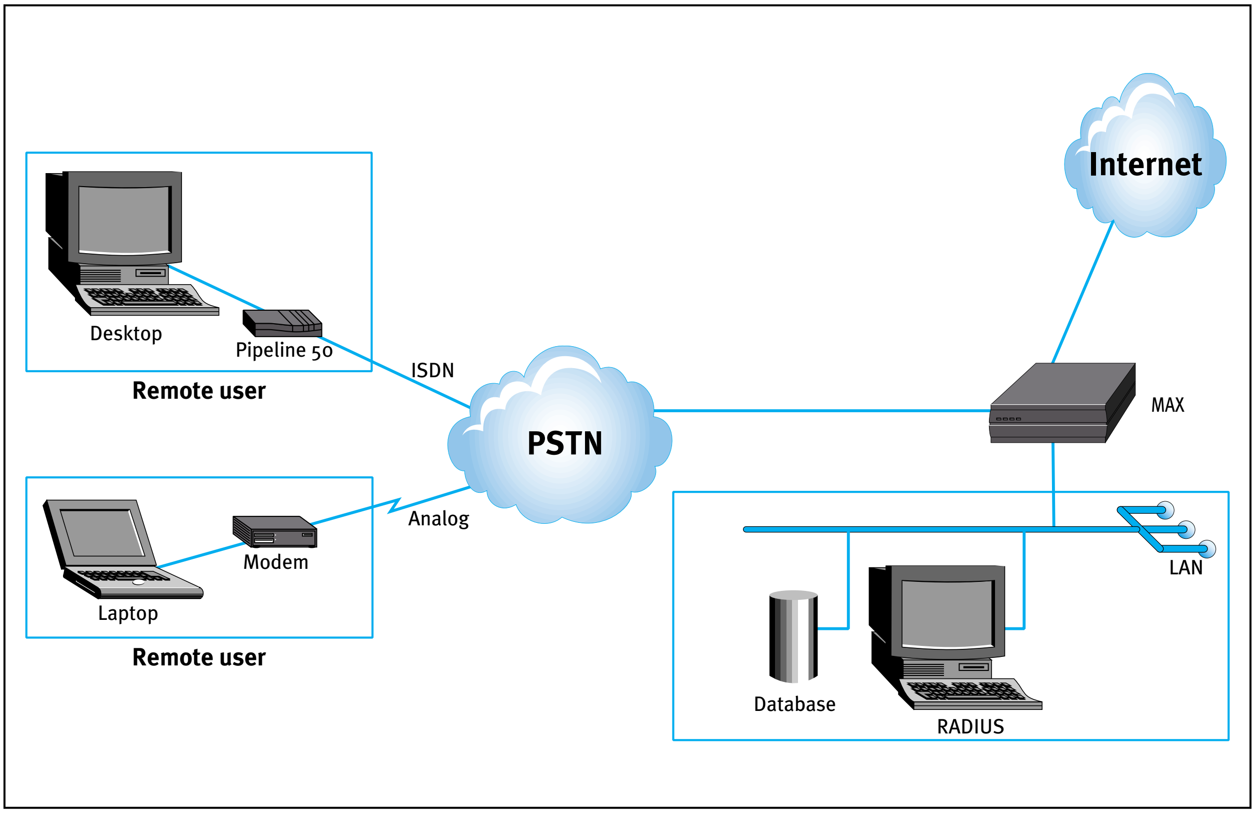
1. Remote user initiates the call to the MAX
2. Remote user sends username to MAX
3. MAX after attempting to authenticate locally forwards the information to RADIUS
4. RADIUS forwards the information to SafeWord client residing on the same system as the RADIUS
5. SafeWord client forwards the information to SafeWord server
6. SafeWord server sends challenge back to the user through SafeWord client, RADIUS and MAX
7. User enters the challenge into the token security card and obtains the one-time only password from the hand-held card; the user then enters the password to be forwarded to the SafeWord server
8. SafeWord server authenticates the user
9. MAX establishes the connection with the user if authentication succeeds; if authentication fails it terminates the call

The user may either be in the terminal server mode or use the Ascend Password Protocol (APP) utility during the authentication phase. Once the authentication is complete then the user may switch to PPP mode.

5.5 RADIUS with External DataBases

Some corporations and service providers that support a large number of remote callers use a central database server to maintain their user/client names. For security reasons, these customers typically will modify RADIUS themselves and convert RADIUS to act as the front end to their user/client databases.

Figure-5.5



How does it work ?

When a user with a PPP client dials into the MAX, the MAX obtains the UserID and password using PAP/CHAP. After attempting to authenticate the user locally, the MAX forwards the information to the RADIUS server. The RADIUS server interacts with the external database and then performs the authentication. The MAX either completes the call or terminates it.

5.6 Using RADIUS to Sign-Up New Customers

Figure-5.6

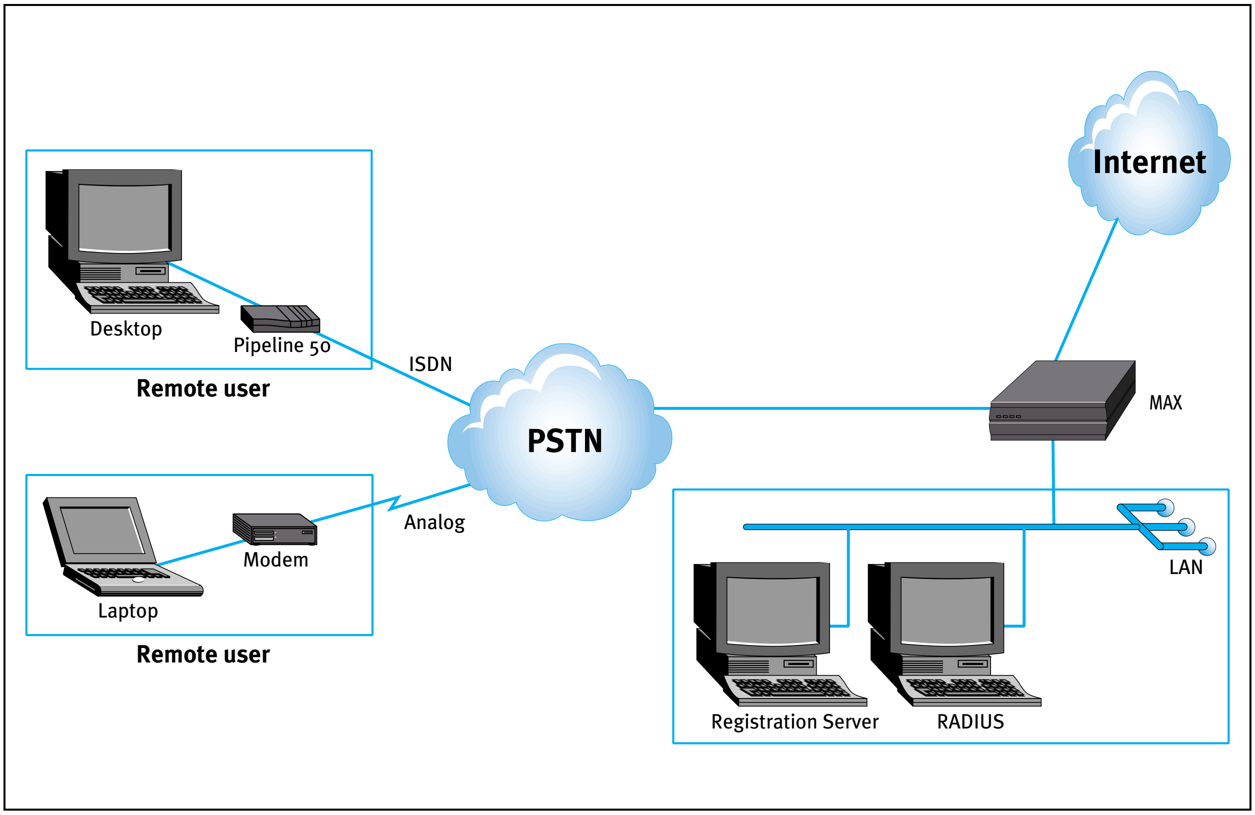


Figure 5.6 The Ascend RADIUS data-filter or immediate telnet features may be used effectively by service providers to sign up new customers. In this example, the service provider has a RADIUS server and a separate registration server. When new customers connect to the network using a specific name and password contained in the company's advertising, their request is passed to the registration server and they are prompted to enter sign-up information such as name, address and credit card number.

Users cannot access any other resource on the system until they have provided all the registration details and signed up for the service. After a new user has completed the signup procedure, the registration server issues them a permanent UserID and Password.

6.0 HOW TO OBTAIN ASCEND RADIUS

Ascend RADIUS may be downloaded from Ascend's FTP server:

FTP site	:	ftp.ascend.com
Username	:	anonymous
Password	:	guest
directory	:	/pub/Software-Releases/Radius/

ASCEND

05-6

Ascend Communications, Inc.
1275 Harbor Bay Parkway
Alameda, CA 94502, USA
TEL: 510.769.6001
FAX: 510.814.2300

E-mail: info@ascend.com
Toll Free: 800.621.9578
FAX Server: 415.688.4343
Internet Home Page:
http://www.ascend.com