Ascend

Ascend Access Control

PRODUCT UPDATE

Ascend Access Control is a comprehensive authentication and accounting server that was developed for carriers, service providers and corporations. It is a flexible, non-proprietary protocol for centralized authentication, password encryption, service selection, filtering and call accounting. It also is fully compliant with the RADIUS protocol and supports the RADIUS attributes along with the Ascend Dictionary.

Ascend Access Control provides identification, authentication, authorization and accounting. It overcomes the limitations of other authentication servers; that is, it handles authentication of both analog and digital users.

Identification features comprising of Calling Line ID (CLID) and Callback ensure that calls originate from a pre-approved location and deliver the first tier of authentication. Calls that originate from an intruder or hacker site can be terminated without prompting the intruder for a username and password, thus eliminating the opportunity for a hacker to guess a password or launch a "denial of service" attack on your network access server.

Authentication function of the Access Control can be your first tier or second tier of verifying the dial-up user. This involves obtaining the user's ID and a password. It verifies against a wide range of authentication databases such as UNIX password file, flat file, Kerberos, ODBC-compliant database or a token card security server. The ODBC interface lets network administrations manage hundreds and thousands of users from a central or distributed database such as Sybase, Oracle, Informix or any ODBC-compliant database.

Authorization within the Access Control offers a flexible mechanism to tighten your remote networking security. The authorization feature permits you to set up access control on a per-user basis, which is enforced when the user dials into your network and remains active until the session is terminated.

You may utilize the data filters within the Access Control server to authorize individual users' access to specific hosts, specific subnetworks or specific networks based on source and destination IP addresses. Moreover, authorization may be controlled based on the type of protocols such as UDP, TCP, ICMP and type of applications such as FTP, TFTP, PING and WWW using source/destination ports.

The call filters enhance the authorization by allowing you to define what types of traffic are accounted as legitimate data when maintaining a connection to your network. In other words, users may be permitted to send and receive ICMP data. Yet, they also can be limited in how long a connection is maintained when they keep ports open with applications such as Ping, thereby increasing network availability for other legitimate callers.

For protocols other than IP such as IPX and NetBios, Access Control offers generic filters to perform similar types of authorization and manages users' access to your network resources.

ASCEND

Accounting details generated by the Access Control include but are not limited to user name, connection date/time, duration of the call, analog or digital, what IP address was assigned, number of input/output packets and data rate.

The accounting information may be stored as a simple ASCII text file or automatically formatted and sent to an ODBC-compliant database, which can be used for billing and report generation.

Proxy-RADIUS and Ascend Intranet Authentication features, in conjunction with tunneling protocols such as Point to Point Tunneling Protocol (PPTP) and Ascend Tunnel Management Protocol (ATMP), deliver unparalleled Intranet and Virtual Private Network capabilities for corporations and service providers.

PROXY-RADIUS

ISP/carriers may have a primary Access Control that acts as a proxy to other authentication servers such as RADIUS, Kerberos, TACACS+, and TACACS servers residing at the corporate/small ISP customer site. The primary Access Control at the ISP/Carrier will process the authentication request from end users. Then, looking at the domain name within the username entry (i.e. john@ascend.com), it may forward the user information to the respective server for authentication. This involves maintaining and managing RADIUS or other authentication servers at customer sites.

ASCEND INTRANET AUTHENTICATION

The Ascend Intranet Authentication within Access Control eliminates the need to maintain and manage different authentication servers at the corporate/ISP site when offering VPN service.

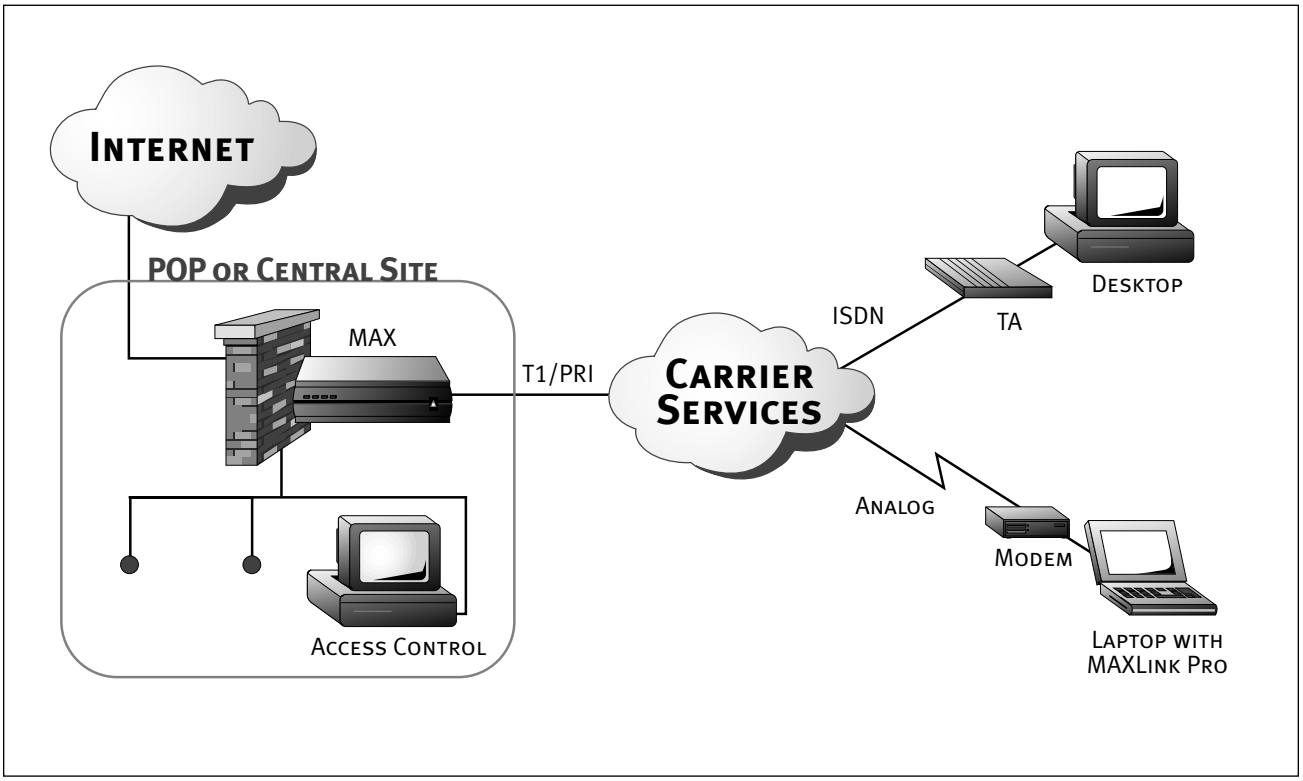
A single Access Control can reside at the ISP/Carrier site, communicating to an ODBC-compliant database server. Within the database server, the ISP may create several database tables, one for each one of the corporate or small ISP customers for using a VPN service. The network administrator from these corporations or small ISPs may be given access rights only to their respective database tables. The corporate/ISP customers can then manage their own clients' user name list and other information within the database table.

When end users dial into the ISP/Carrier's network with the domain name as part of the user name (e.g. john@ascend.com), Access Control interacts with the respective database table using the domain name and performs authentication and other tasks. This functionality may be used in conjunction with Proxy-RADIUS to meet a wide range of VPN requirements.

Access Control Manager, a Java-based application with a point-and-click interface, simplifies the configuration and management of Access Control. It eliminates the complex setup procedures normally required to install an authentication server. It also allows creation of templates for common user profiles, which are easily duplicated to create new user profiles. All attributes/features are listed so network administrators can simply scroll through the list and select the ones they want to add to user profiles.

Applications

- Analog and digital subscriber authentication
- Intranet and Virtual Private Network
- Back-up authentication servers
- Centralized user database management
- Token card security
- Secured Dynamic Bandwidth Allocation
- New user registration
- Dynamic IP address assignment
- Out-dial calls
- Accounting



Ascend Access Control Features

- Network Access Server authentication
- Analog and digital user authentication
  - SLIP, PPP, Multilink PPP, MP+, Login User, PAP, CHAP
- User Identification
  - Calling Line ID (CLID), Callback Security
- User authentication
  - User name, password, UNIX password, Kerberos, token card security (e.g. Security Dynamics, AssureNet Pathways, Enigma Logic, Bellcore S/Key, Cryptocard)
- Per-user authorization
  - Data filters, call filters, generic filters, immediate Telnet
- Outdial calls
- Resource management
  - Dynamic IP address assignment, static route, banner messages, assignment of Frame Relay DLCI, routing or bridging, extensive switched data services, password expiry, idle timeout
- Intranet/Virtual Private Network (VPN)
  - Proxy RADIUS, Ascend Intranet Authentication
- Secured dynamic bandwidth allocation
  - Authentication of multiple B-channels, static/token-card/cached password
- Backup servers
- Extensive accounting information
- ODBC-compliant database support
  - Sybase, Oracle, Informix, etc.
  - User authentication and user profile
  - Accounting

Platforms

SunOS 4.1.4	(Sparc)
Solaris 2.5.1	(Intel/Sparc)
HP-UX 10.0	(PA RISC)
IBM AIX	(RS 6000)

Positioning

Ascend Access Control is:

- a standards-based comprehensive and scalable, network-wide security management and authentication solution
- a multitiered authentication system for increased security of remote networking
- part of a comprehensive Ascend network security architecture

Product Information

New Feature Requests : prod-mgmt@ascend.com
Collateral & product Information : info@ascend.com

Ordering Guidelines

Model#	Description	US List Price
AAC-CD	Ascend Access Control in CD-ROM	$ 3,000

Scheduled Availability

United States	October 31, 1996
International	October 31, 1996

ASCEND
Remote Networking
Solutions That Work.™

Ascend Communications, Inc.
One Ascend Plaza
1701 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