White Paper

RADIUS Security
Technology

ISPs Simplify Remote Access For Enterprises.

Bay Networks

Executive Summary

Companies want to simplify the implementation and support of remote access capabilities over the Internet. Many of these companies are transferring the creation, administration and maintenance of their remote access infrastructure to Internet Service Providers (ISPs) willing to assume this important responsibility.

The RADIUS remote access standard allows both parties to benefit from this outsourcing trend. RADIUS provides an industry-standard, client/server-based solution which lets authorized remote users access Enterprise data. User authentication, authorization, and accounting are all accomplished via the RADIUS standard to ensure network integrity and security.

The RADIUS security protocol is a key component of Virtual Private Networks (VPNs). A VPN is a connectivity service that appears to users as a direct connection to a private network, yet actually uses a public infrastructure such as the Internet to provide the connection. VPNs offer the Enterprise and the ISP a sophisticated remote access alternative by establishing secure, logical connections to various endpoints throughout a WAN without requiring major investments in new hardware and software. Furthermore, the combination of VPNs and RADIUS reduce administrative burdens for the Enterprise and benefit ISPs through higher equipment utilization rates and a resulting return increase on investment.

Introduction

Enterprise sites are focusing on outsourcing, another area of their Information Technology operations to reduce operational complexity and expense. Enterprise sites are looking for suppliers who will create and manage remote access services for their off-site workers.

Remote access outsourcing is a richly rewarding new business opportunity for ISPs. ISPs can relieve Enterprises of tedious telco line requirements and day-to-day management of modems, remote access servers and other hardware required to operate secure, virtual private networks.

The benefits to both parties are obvious and growing. For Enterprises, communications professionals simplify their operations by using a service that can be purchased like any value-added service from a telephone company. For ISPs, management of remote access operations on behalf of their Enterprise clients can increase equipment utilization and yield a better return on investment.

One of the technologies making both of these benefits possible is the network technology known as RADIUS, an industry-standard client/server security protocol for remote access. RADIUS (Remote Access Dial-In User Service), evolved from the remote access community's need to serve the security interests of those requiring virtual private networking.

RADIUS satisfies those requirements by concentrating on three, key security functions:

- *Authentication* users' ability to identify themselves through a log-in name and password match
- *Authorization* assignment of data access parameters based on pre-defined user profiles and security clearances.
- *Accounting* creation of a continuous audit trail, tracking every RADIUS-based transaction for accurate billing by the ISP.

To successfully create a VPN, the RADIUS standard provides initial user Authentication/Authorization/Accounting (AAA) at the ISP on what is called the Proxy RADIUS Server. The access request is then redirected to a RADIUS server at the Enterprise destination for a tighter level of AAA security processing.

Using this network access topology, ISPs serve as a front-end screening mechanism for Enterprise access. At the same time, the Enterprise retains their own sensitive user security profiles and uses them to authorize user access to valuable corporate network resources. The VPN is secured for AAA transactions because the ISP and Enterprise deploy complementary RADIUS servers.

Access Control Using RADIUS

ISPs implementing a turnkey RADIUS remote access solution for their Enterprise subscribers must provide a suite of easy-to-use and reliable features to create a cost-effective service. Criteria ISPs and their Enterprise subscribers should consider in a well-architected RADIUS server solution include:

- Versatile platform support to adapt to existing and changing subscriber environments such as NT, NetWare, and UNIX
- Access to network operating system (NOS) security information normally unavailable via remote access: Windows NT Domain and Workgroups, NetWare Bindery and Directory Services (NDS), or UNIX Network Information Services (NIS)
- Embedded database engine for flexible user AAA profile management
- Interoperability through support of vendor-specific attributes from a wide range of remote access equipment vendors
- Extensive, well-presented, real-time user statistics
- Centralized administration of user information for remote access servers, Proxy RADIUS servers, VPN tunneling, and Internet firewalls
- GUI interfaces for user convenience
- 3rd party security integration including token card security systems
- Global, 7x24 technical service and support

Ideally, a complete implementation of the RADIUS standard should run as a native application in Microsoft NT, Novell NetWare, and UNIX environments. On a Microsoft Windows NT server, it should run as a set of NT services; on a Novell NetWare server, it should run as a set of NetWare Loadable Modules (NLMs); and on UNIX, it should run as a set of UNIX services.

When a RADIUS implementation is tightly integrated with Windows NT, Novell NetWare, or UNIX, Enterprise network administrators can use the passwords and groupings already created in the Windows NT Domain/Windows NT workgroups, the NetWare Bindery/NetWare Directory Services (NDS), or UNIX Network Information Services as the basis for authenticating remote users dialing into any Remote Access Server. This tight integration with NT, NetWare, and UNIX user directories allows the network manager to simplify administration, save time, and ensure that security profiles are completely current.

ISP Remote Access with RADIUS

The ISP remote access environment using RADIUS has four main components: Remote Users, Remote Access Servers (RAS), Proxy RADIUS Servers, and the Enterprise RADIUS server. Each user is a client of a RAS; each RAS is both server to the user and client of the RADIUS server. Each of the four components of the ISP remote access environment participates in the AAA transaction process.

Remote Users

The remote user (Figure 1) is the person trying to gain access to the Enterprise network from home or a remote location.

Typically, the remote user has a Serial Line Internet Protocol (SLIP) or Point-to Point Protocol (PPP) dialer such as the MS Windows 95 dial-up networking client that allows the user to dial over the Internet Protocol (IP) into a Remote Access Server (RAS) at the ISP. The user can obtain access to the Enterprise network either through a virtual private network connection or directly to the Enterprise network without going through an ISP.

Internet Service Provider

The Remote Access Server (Figure 1) resides at the ISP and supports SLIP or PPP dial-in calls, authenticates each user via the RADIUS (or Proxy RADIUS) Server, and then routes that user onto the Enterprise network.

Most RAS devices can handle multiple dial-in users at once, and the corporate network might include a single RAS or multiple remote access servers working in tandem.

The "Proxy RADIUS" server resides at the ISP, and forwards requests from the RAS located at the ISP to a RADIUS server located at the Enterprise. This is like call-forwarding, where an ISP can direct all authentication and accounting transactions to an Enterprise LAN's RADIUS server. The user name is parsed, usually by domain such as jdoe@company.com, to obtain the organization name. The organization's name determines the IP address of the target RADIUS server.

Enterprise (ISP Subscriber)

The Enterprise RADIUS Server (Figure 1) accepts authentication requests from the ISP's Proxy RADIUS server, performs the authentication, and responds with the result—either an accept or a reject.

In a typical Enterprise installation, a single RADIUS server handles all remote access. Companies with Remote Access Servers at multiple sites could elect to have a separate RADIUS Server at each site. However, if the various sites were linked over a WAN of reasonable speed or over the Internet, a single RADIUS server could handle multiple Remote Access Servers at multiple sites.

Figure 1 **RADIUS Security for Virtual Private Networks**

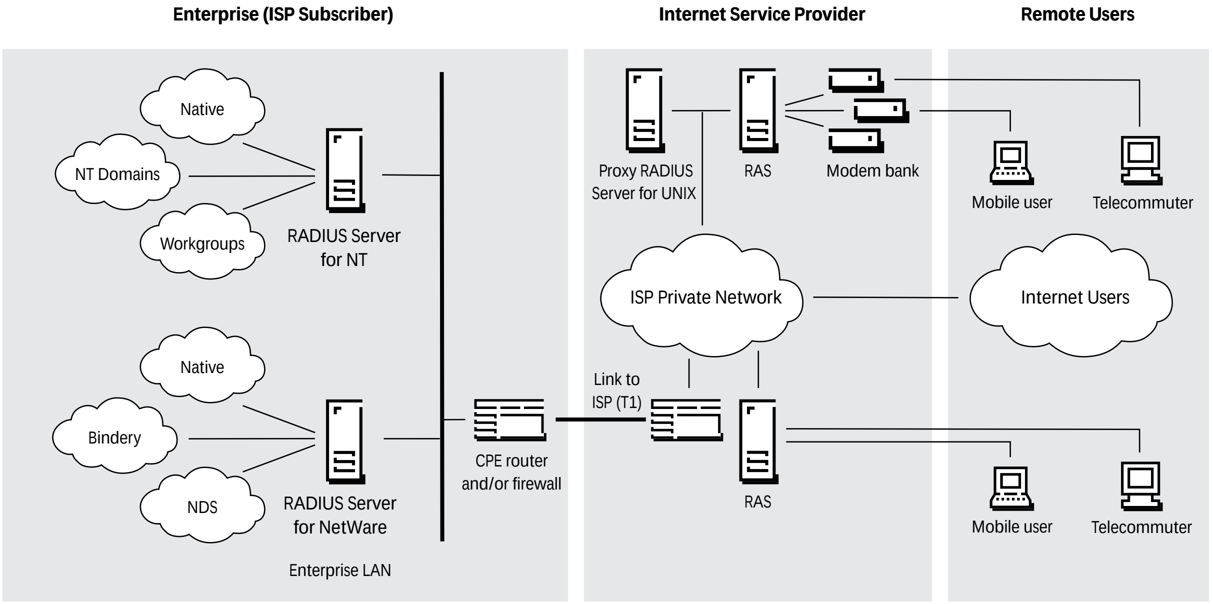


Figure 1: RADIUS provides a gateway between users, ISP "Proxy RADIUS" access, and Enterprise LAN authentication.

RADIUS Authentication

The primary function of the RADIUS server is authentication, the first "A", of the AAA transaction process. This section covers basics of authentication:

- What happens during the authentication process
- Types of authentication available
- RADIUS attribute exchange
- RADIUS dictionaries

User authentication at the ISP is a multi-step process. Process steps occur both at the ISP and at the subscriber site (Refer to Figure 1):

1. A user dials in to one of several remote access servers at the ISP and PPP negotiation begins.
2. The RAS passes authentication information—username and password—obtained during PPP negotiations to the ISP's local Proxy RADIUS server.
3. The Proxy RADIUS server parses the user name e.g., username@companyname. The RADIUS server performs a translation in its database to determine the IP address of the "username's" Enterprise RADIUS server for "companyname". After establishing the proper remote link to the username's Enterprise network, the username and password are forwarded to the Enterprise's RADIUS server for further authentication.
4. If the username's Enterprise RADIUS server is able to authenticate the user, it issues an accept response to the ISP's Proxy RADIUS server. The Proxy RADIUS server, in turn, issues an accept response to the ISP's RAS, along with the user profile information obtained from the subscriber's Enterprise RADIUS server. The RAS requires the profile to set up the connection.
   If the subscriber's Enterprise RADIUS server is unable to authenticate the user, it issues a reject response to the ISP's RAS, along with a text string indicating the reason.
5. Using this information, the RAS completes PPP negotiation with the user: If the ISP's RAS received an "accept" response, it allows access to the username's Enterprise network. If the ISP's RAS received a "reject" response, it terminates the user's connection. It may pass on the reason for termination so that it can be displayed at the user's terminal.

Authentication Types

During an authentication transaction, password information is transmitted between the User, RAS and RADIUS server. The password information is always encrypted between the RAS and the RADIUS server using a secret key entered both at the RAS and at the RADIUS server.

The password information originally comes from the user, usually as part of PPP negotiations. The RAS is really just an intermediary. The authentication transaction occurs between the user and the RADIUS server.

Authentication Between the User and RAS

RADIUS supports two types of authentication transactions between a remote access user and a RAS: Password Authentication Protocol (PAP) and Challenge Handshake Administration Protocol (CHAP). PAP and CHAP are authentication methods used in Point to Point Protocol (PPP).

- PAP is very simple. The user sends his or her password to the RADIUS server, and the RADIUS server validates it either against its own database or against the Microsoft NT Domain or Workgroup, NetWare Bindery or NDS, or the UNIX NIS. Of the two legs of the journey the password takes between user and RADIUS server, the first leg, from the user to the RAS, is usually unencrypted, and the RAS gets the password from the user in clear text. In the second leg, from the RAS to the RADIUS server, the RAS encrypts the password and the RADIUS server decrypts it using a shared secret key. Ultimately, the RADIUS server has the password in clear text form and is able to use it directly for authentication.
- CHAP avoids sending passwords in clear text over any communication link. Using CHAP, the RAS generates a random number, the challenge, and sends it to the user. The user's PPP client creates a "digest"—a one-way encryption—of the password concatenated with the challenge, and sends this digest to the RAS. Because the digest is a one-way encryption, the RADIUS server cannot recover the password from the digest. Instead, it performs the identical digest operation using its own copy of the user's password stored in clear text in the RADIUS server's database along with the same challenge. If the two digests match, the user is authenticated.

The Option of NOS Authentication

There are a number of options for performing NOS authentication. All of the methods that rely on Windows NT, NetWare, or UNIX NOS security for authentication require that authentication be done with PAP, as NT, NetWare, and UNIX already store encrypted passwords. Only Native authentication, i.e., using the user records from the RADIUS servers' embedded database, permits use of either PAP or CHAP as passwords can be stored unencrypted.

One or more of the following NOS authentication methods can be chosen:

- Windows NT-based authentication as a:
    - Domain User within a Windows NT Domain
    - Domain Group within a Windows NT Domain
    - Workgroup User on a specific workgroup machine
- NetWare-based authentication as a:
    - Bindery User on a NetWare file server
    - Bindery Group on a NetWare file server
    - NDS User as a distinguished name in the NDS tree
    - NDS Group as a distinguished name of a group in the NDS tree; or
    - NDS Context as a distinguished name of a container object in the NDS tree
- UNIX-based authentication as a:
    - NIS User
    - NIS Group

Figure 2 **Simple Administration Using Existing NOS User Database**

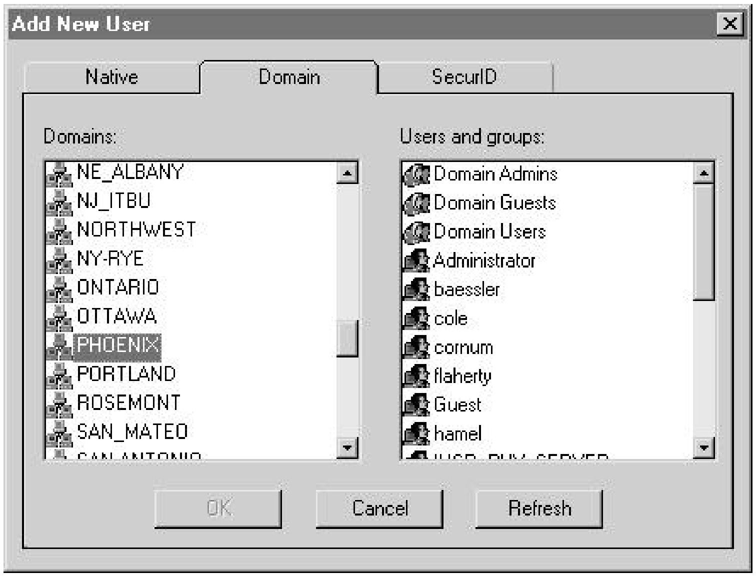


Figure 2: RADIUS technology allows authentication based on an NT Domain User, Domain Group, or as a Workgroup User.

RADIUS technology on NetWare and UNIX also includes a GUI for configuring Bindery, NDS, or NIS Users and Groups.

RADIUS Authorization

Table 1 **Vendors Supporting RADIUS**

Vendors Supporting RADIUS
3Com
ACC
ADC Kentrox
Ascend
Bay Networks
Check Point
Cisco
Compatible Systems
Digi International
DEC
Gandalf
IBM
Lantronix
LeeMah
Livingston
Motorola
Kasten Chase
Penril
Perle
Raptor Systems
Secure Computing
Shiva
US Robotics
Xyplex

Table 1: RADIUS provides full support to remote access equipment from vendors which conform to the RADIUS standard.

Following authentication in the AAA transaction is authorization. Along with the authentication information that the user includes as part of a RADIUS request, the RAS also passes information about the type of connection the user is trying to establish. The RADIUS server uses this information either to further authorize the user and issue an accept, or to deny access based upon disallowed conditions and issue a reject.

Authorization is controlled by the user's profile residing in the RADIUS server's database. Each profile lists two types of RADIUS-standard attributes: check-list attributes and return-list attributes. Vendor-Specific Attributes are commonly used variants of RADIUS-standard check-list and return-list attributes and represent proprietary vendor extensions to the RADIUS protocol.

Check-list Attributes

Check-list attributes define a set of requirements for the connection. During the authentication transaction, the RAS must send attributes to the RADIUS server that match the check-list; if they don't match, the RADIUS server will issue a reject even if the user can be authenticated. By including appropriate attributes in the check-list, a variety of rules could be enforced. For example, only certain users might be permitted to either use ISDN connections, or to dial in to a particular RAS. Or, Caller ID could be used to validate a user against a list of legal, originating phone numbers.

Return-list Attributes

Return-list attributes are attributes that the RADIUS server sends back to the RAS once authentication is successful. The return-list defines additional parameters that the RAS should assign to the connection, typically as part of PPP negotiations. For example, specific users could be assigned either a particular IP addresses, an IP address from a dynamically allocated pool of IP addresses, or IPX network numbers. Other attributes could include IP header compression enabling/disabling, or a time limit could be assigned to the connection.

Vendor-Specific Attributes

A RADIUS server may use Dictionary files to establish vendor-specific check-list and return list attribute values in environments where the remote access equipment is from a variety of vendors. The Dictionary file contains vendor-specific, proprietary items which may be set for a particular vendor's RAS equipment. The RADIUS server differentiates between various vendors' RAS equipment. Its Dictionary files provide communications between various makes of remote access servers. This provides an open and adaptive solution, embracing whatever RAS products the subscriber has implemented, while allowing the subscriber to fulfill application needs where the RADIUS standard does not yet provide coverage.

RADIUS Accounting

RADIUS Accounting tracks the Authentication and Authorization transactions from beginning to end. RADIUS Accounting captures statistics about each session. For instance, the accounting process allows a RADIUS server to track when users start and stop their dial-in connections.

Using RADIUS Accounting, the RADIUS server can maintain:

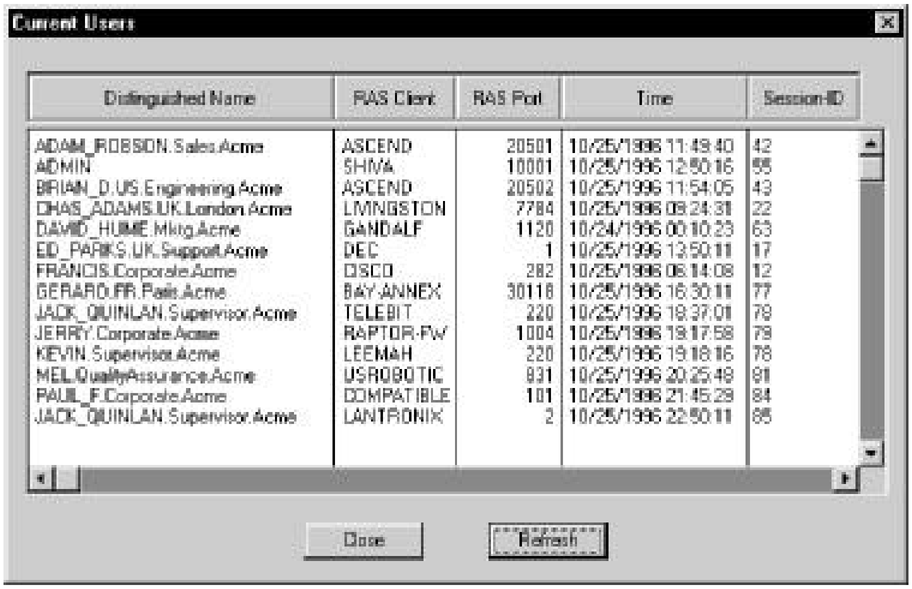
- A history of all user dial-in sessions, indicating start time, stop time, and various statistics for the session
- A current User list indicating which users are currently connected to which Remote Access Servers

All Accounting transactions are logged to a comma-delimited file that can be imported into standard word processors, spreadsheets, and database programs and can be used to generate reports, and for billing.

One of the most useful outputs provided by RADIUS server software is a real-time list of active RADIUS users. The snapshot of user activity in Figure 3 displays the following fields:

- Distinguished Name shows the full user name which was used for the authentication. If the user name is part of NT Domain directory services or NetWare Directory Services (NDS), or part of UNIX Network Information Services (NIS), the distinguished name is the NT/NDS/NIS common name or container object name prepended with the user name.
- The RADIUS server displays RADIUS clients, either the RAS's name or IP address.
- RAS Port shows the Remote Access Server port number, which represents a unique port number on the RAS.
- Time contains the date and time at which the connection was started, according to the accounting transactions.
- Session ID contains the unique session key generated by the RADIUS server.

Figure 3 **Snapshot of Current User Connections**



Distinguished Name	RAS Client	RAS Port	Time	Session-ID
ADAM_ROBSON.Sales.Acme	ASCEND	20501	10/25/1996 11:49:40	42
ADMIN	SHIVA	10001	10/25/1996 12:50:16	55
BRIAN_D.US.Engineering.Acme	ASCEND	20502	10/25/1996 11:54:05	43
CHAS_ADAMS.UK.London.Acme	LIVINGSTON	7784	10/25/1996 09:24:31	22
DAVID_HUME.Mktg.Acme	GANDALF	1120	10/24/1996 00:10:23	63
ED_PARKS.UK.Support.Acme	DEC	1	10/25/1996 13:50:11	17
FRANCIS.Corporate.Acme	CISCO	282	10/25/1996 06:14:08	12
GERARD.FR.Paris.Acme	BAY-ANNEX	30118	10/25/1996 16:30:11	77
JACK_QUINLAN.Supervisor.Acme	TELEBIT	220	10/25/1996 18:37:01	78
JERRY.Corporate.Acme	RAPTOR-FW	1004	10/25/1996 19:17:58	79
KEVIN.Supervisor.Acme	LEEMAH	220	10/25/1996 19:18:16	78
MEL.QualityAssurance.Acme	USROBOTIC	831	10/25/1996 20:25:48	81
PAUL_F.Corporate.Acme	COMPATIBLE	101	10/25/1996 21:45:29	84
JACK_QUINLAN.Supervisor.Acme	LANTRONIX	2	10/25/1996 22:50:11	85

Figure 3: RADIUS technology provides a snapshot showing each current connection made through all RAS devices.

Conclusion

ISPs are busy providing new remote access technologies, including higher-speed DSP modems and ISDN capabilities, to their Enterprise subscribers. To leverage this investment, ISPs can offer VPN dial-in services to their Enterprise subscribers without the tremendous overhead entailed in managing user-level authentication and authorization issues, or in supporting "freeware" RADIUS servers at subscriber sites.

Most Enterprise subscriber environments today are already using Microsoft Windows NT, Novell NetWare, or UNIX authentication to manage access. It makes sense for subscribers to use their existing infrastructure to manage all types of remote access for authentication, authorization, and accounting. This practice also increases control, since all access is managed locally and can be audited with full assurance that all entries into the LAN are accounted for. The major remote access and firewall vendors support the RADIUS standard, so that subscribers' investment in Windows NT, NetWare, or UNIX is protected.

RADIUS provides a complete solution, centralizing authentication, authorization, and accounting for all remote access. Because it integrates Proxy RADIUS authentication with the existing Windows NT, NetWare, or UNIX user directory databases, it simplifies administration. And because it runs as either a Windows NT service, a NetWare Loadable Module (NLM), or a UNIX service on a network file server or host, it does not require additional expensive and difficult-to-manage hardware devices.

Bay Networks Value-Added RADIUS Solution

Bay Networks provides one of the most sophisticated, comprehensive RADIUS solutions available. Bay Networks has championed the RADIUS standard by participating and driving the RADIUS definition in both the IETF and in the Merit industry consortium, thus ensuring full compliance to the RADIUS IETF RFCs 2138 and 2139. Bay Networks RADIUS strategy incorporates industry compliance and a comprehensive, turn-key RADIUS solution. Bay Networks includes RADIUS client support in its remote access router product lines (See Table 2).

Table 2 **Bay Networks Products Supporting RADIUS**

Remote Access Servers
Remote Annex 2000, 4000
8000 Remote Access Concentrator (RAC)
5390 Access Server Module
5399 RAC Module for the 5000 MSX
Routers
Access Stack Node (ASN)
Backbone Link Node (BLN)
Backbone Concentrator Node (BCN)
Nautica Marlin

These clients are complemented by the BaySecure Access Control RADIUS server technology, licensed from Funk Software, which won the LAN Times Best Product Of The Year award in February, 1997, and Network Computing's Best Connected award for authentication services in May of 1997. BaySecure Access Control™ fulfills RADIUS server requirements for both the ISP and Enterprise sites. For further information on BaySecure Access Control, consult your sales rep or visit the Bay Networks web site (www.baynetworks.com).

Bay Networks

For more sales and product information, please call **1-800-8-BAYNET**.

United States

Bay Networks, Inc.
4401 Great America Parkway
Santa Clara, CA 95054
1-800-8-BAYNET

Bay Networks, Inc.
8 Federal Street
Billerica, MA 01821-5501
1-800-8-BAYNET

Europe, Middle East, and Africa

Bay Networks EMEA, S.A.
Les Cyclades – Immeuble Naxos
25 Allée Pierre Ziller
06560 Valbonne, France
+33-4-92-96-69-96 Fax
+33-4-92-96-69-66 Phone

Pacific Rim, Canada, and Latin America

Australia +61-2-9927-8888
Brazil +55-11-5182-1244
Canada 416-733-8348
China +8610-6238-5177
Hong Kong +852-2-539-1388

India +91-11-613-7401
Japan +81-3-5402-7001
Mexico +52-5-480-1241
Singapore +65-323-3522

World Wide Web: **http://www.baynetworks.com**

10/97 WP522-2841EC-A

Printed on recycled paper.