Lucent Technologies
Bell Labs Innovations

Lucent NavisRadius™ 4.0

Commercial RADIUS-compliant AAA Server

1. What is Lucent NavisRadius 4.0?

NavisRadius 4.0 is an implementation of the RFC standard RADIUS protocol that provides Authentication, Authorization and Accounting (AAA) services. NavisRadius 4.0 provides an integrated network-wide remote access security solution for service providers and carriers. NavisRadius 4.0 supports the RADIUS standard as defined by the IETF RADIUS RFC 2865 (RADIUS Authentication) and 2866 (RADIUS accounting) and is used to provision a wide range of network services. NavisRadius 4.0 includes capabilities and features required to meet the needs of ISPs and carriers in provisioning AAA services for dial port wholesaling. It also includes additional useful features such as support for third-party security methods, an embedded runtime SQL DBMS database (BP versions only), support for IP tunneling and resource management capabilities.

2. How can one server meet all needs?

In order to provide the best and most-cost effective AAA solution to our customers, Lucent delivers NavisRadius 4.0 in two versions: NavisRadius (Base Platform 4.0) and NavisRadius-SP (Service Provider edition). The BP version is designed for enterprise networks and is available for under $1,000 street price in the special BP/SE version. The SP version is designed for large-scale service providers and major private networks. Both products are identical in terms of features and functionality. The difference is in the licensing terms. The "BP" version is licensed “per-server” and provides support for up to 15 RADIUS clients — typically NASs. The "SP" version allows deployment of an unlimited number of servers and is licensed based on the number of ports or users on the network.

3. What key features are available in NavisRadius 4.0?

NavisRadius 4.0 has the following major features:

- The PolicyFlow AAA programming language
- LDAP interface
- SQL (JDBC) Interface
- Text file support for existing RADIUS implementations as well as standard delimited files.
- Syslog logging
- Graphical user interfaces (GUIs) for server administration and user records
- New test client with a graphical interface.
- Graphical RADIUS "perfmeter" to monitor system loading, rejects, etc.
- DHCP address pool assignment
- Expanded Universal State Server (USS) with unlimited session counters
- Allow Lists, Stop Lists and Access Control Lists (ACL) based on any RADIUS attribute
- The most flexible accounting in the business. Session records can be saved to: Flat files with fixed or variable record length and custom formats – one file for all, one file per realm, etc.; Databases, remote servers (proxy)

4. Can something this powerful also be easy to use?

Yes. The new NavisRadius PolicyAssistant makes installation and setup a snap. For the most common requirements you need only fill-in a few simple forms and you are up and running. Support is provided for

LDAP, SQL Proxy and Text files. Session limits can be applied to individual user sessions, Realms and DNIS. The PolicyAssistant logic can even be altered to meet your custom requirements.

5. What OS platforms are supported by NavisRadius?

NavisRadius-SP 4.0 is available for

- Sun Solaris SPARC 2.5.1, 2.6, 2.7 & 2.8
- Sun Solaris x86; 2.6, 2.7 & 2.8
- HP-UX
- Compaq/DEC TRU-64 UNIX
- RedHat Linux 7.1
- Windows NT 4.0 & Windows 2000

The Server Management Tool (GUI) can also be run on Windows 95/98/ME and MacOS X

Java version 1.2.2 or 1.3 required on all platforms.

NavisRadius is available for download with a 30-day evaluation license from http://www.lucentradius.com/.

6. Can NavisRadius 4.0 run on any other platforms?

Because NavisRadius 4.0 is written in Java, it can run on most UNIX systems, including other Linux versions and FreeBSD, as long as Java v1.2.2 or 1.3 is available. Note that on unsupported platforms some minor installation tasks may need to be performed manually and some features may not be available.

7. How is NavisRadius delivered?

NavisRadius is provided over the web from http://www.lucentradius.com/. Hardcopy documentation and a CD-ROM are available on request at the time of product registration. A fully functional 30-day evaluation copy is available from the web site.

8. Why should I pay for NavisRadius 4.0 when RADIUS 2.1 is free for anyone and source is available?

NavisRadius 4.0 is an advanced architecture written entirely in Java. As a fully supported product, it is designed to meet the needs of the professional service provider. NavisRadius 4.0 permits extremely flexible policymaking with a low total cost of ownership. The flexible PolicyFlow plug-in architecture can solve virtually any problem that would otherwise require custom programming. Extensions are provided for executing any executable program or script as well as compiled libraries.

9. What remote access devices are supported by NavisRadius?

NavisRadius 4.0 supports any access server, or other device or application, which implements a standards-compliant RADIUS client. This support includes the full line of Lucent NAS devices: the MAX™ family, MAX TNT™ and APX, PortMaster® products and SpringTide equipment. NavisRadius 4.0 also provides full support for Lucent (and Ascend) specific extensions (such as the Lucent Dictionary) to deliver enhanced capabilities. Support is also included for major third-party remote access products: RedBack, Cisco, Nortel and 3-COM as well as any RADIUS compliant client.

10. Is source for NavisRadius 4.0 available?

No. However, unlike other commercial RADIUS servers NavisRadius 4.0 is fully programmable and extensible. With the PolicyFlow AAA programming language virtually any AAA requirement can be easily met.

©2001 Lucent Technologies, Inc.

11. What kind of performance can I expect from NavisRadius 4.0?

NavisRadius 4.0 features an internal architecture optimized to reduce the possibility of lost data. A special process thread is dedicated to receiving packets from the network interface and queuing them for processing. This allows NavisRadius to receive packets at the full line rate and buffer them during periods of very high traffic volume. In a UDP based protocol like RADIUS, this extra buffering can often make the difference between lost packets, especially accounting packets, and a continuous data flow.

NavisRadius 4.0 also helps increase packet throughput by automatically detecting and discarding duplicate and stale requests. When NASs are set to short time-out periods they, may at peak busy times, send a second request while NavisRadius is still processing the first request. Detecting and discarding the duplicate requests allows NavisRadius to reduce unnecessary processing and better channel its efforts to essential tasks.

RADIUS server performance is usually measured in AAAs (one Authentication request and two Accountings packets¾ Start and Stop). On a typical dual-processor SPARC server NavisRadius 4.0 will perform over 450 authentications per second and over 250 AAAs per second. Faster machines will provide faster performance. The final answer, of course, depends on your operating system and hardware and the complexity of your PolicyFlow.

12. Is a database included with NavisRadius 4.0?

Yes. The "BP" versions of NavisRadius 4.0 includes a runtime version of the Sybase Adaptive Server Anywhere 6.0.2 SQL database. This DBMS is perfect for those customers who need a database solution to store user profiles and accounting data for relatively small user populations. Tables for creating user profiles for authentication and logging accounting records in a dedicated format are defined in the database. Necessary scripts used to create the database tables are included and documented. A full GUI is provided for maintaining and managing both user and accounting records. SP customers requiring a database must provide their own software.

13. What are the authentication methods supported by NavisRadius?

NavisRadius 4.0 supports authentication methods such as UNIX-PW, text user files, RADIUS proxy, external token card security (RSA SecurID, Axent Defender DSS, and SafeWord), LDAP directories, bundled Sybase DBMS (BP only), NT SAM, Windows Active Directory and generic SQL/JDBC DBMS.

14. Can I use server-based IP pools with NavisRadius 4.0 and implement dynamic IP address allocation?

NavisRadius 4.0 includes support for DHCP-based IP address pools that can be shared across multiple NAS. This feature allows an administrator to centrally manage all the IP addresses across multiple network access servers. Support is also provided for Dynamic DNS (DDNS) allowing NavisRadius to set a session domain name.

15. Will NavisRadius 4.0 help in creating time-restricted user accounts?

NavisRadius 4.0 supports time-of-day restrictions in user profiles. This feature enables setting access restrictions based on times of the day and days of the week as well as activation and expiration dates.

16. What are the accounting options supported by NavisRadius 4.0?

Accounting information may be stored in a simple native flat file (ASCII text file) in “standard” or custom formats. Custom formats support both fixed and variable length records. Accounting records can also be saved to SQL databases, or sent in real-time to the Kenan Arbor billing system. Finally, full support is provided for accounting proxy. Multiple accounting methods can also be combined.

©2001 Lucent Technologies, Inc.

17. What are the features provided by NavisRadius 4.0 to deliver AAA services in a dial port wholesaling environment?

NavisRadius 4.0 includes a sophisticated proxy RADIUS environment to enable wholesalers to forward authentication requests to the downstream service providers' user database, based on the user realm, the dialed number (DNIS), or the calling number (ANI). For example, the port wholesaler could assign each ISP a hunt group number on the MAX TNT, which is the client to the proxy NavisRadius 4.0 server. The proxy server forwards the MAX TNT's authentication requests to the ISP authentication servers, based on the hunt group telephone number dialed by the users.

NavisRadius 4.0 supports the "Pre-Auth" capability on the MAX, MAX TNT, and PortMaster NAS to verify call limits prior to answering the incoming phone call. Limits can be based on the dialed number, the POP or NAS, or even the calling number.

NavisRadius supports DHCP-managed IP pools that can be shared by multiple NAS. Dynamic IP address allocation and release is included in the management of these pools. With this capability, each downstream ISP or enterprise corporation can provide or specify a unique block of addresses to be allocated to its users when they dial into the port wholesaler's network.

NavisRadius also supports the implementation of individual and group user session limits, and can limit users to a single simultaneous session over an entire network, or limit a downstream provider to a total number of simultaneous sessions across the network

Using these features, wholesalers can create outsourcing groups and assign to each of the groups a specific number of ports available for connection. You can therefore use this group session limit feature to control the number of users by means other than traditional hunt group and physical port limits.

18. Is fault-tolerance available for NavisRadius 4.0 servers?

Lucent NAS products allow the definition of up to three accounting servers and three authentication servers, other vendors' NAS may differ slightly. If the primary server fails, the NAS device communicates with the secondary server for authentication. If the secondary server fails, the NAS device communicates with the tertiary server. This approach holds true for accounting servers as well.

19. Can I use NavisRadius 4.0 to configure outbound calls (dial-out)?

Users on the LAN side of the Lucent NAS device can send data to several remote locations. The NAS fetches the necessary information from the NavisRadius 4.0 server to securely call the correct remote location and then forward the data.

20. What authorization rules are available on a per-user basis in NavisRadius?

NavisRadius 4.0 provides a comprehensive yet adaptable authorization mechanism on a per-user basis. You may utilize the data filters within NavisRadius 4.0 to give individual users access only to specific hosts, specific subnets, or specific networks, based on source and destination IP addresses. Additionally, authorization may be controlled based on the type of protocol such as UDP, TCP and ICMP. Authorization can also be based on the type of application such as ftp, tftp, ping, or www using source/destination ports. Call filters can be used to define what types of data traffic are considered legitimate. For example, even though a user may be permitted to send and receive ICMP data, the user may not be permitted to maintain the connection with a simple continuous ping to an interface for more than a pre-configured duration. Hence, you can open ports for other legitimate users dialing into your network. For protocols other than IP, such as IPX, NavisRadius 4.0 can describe generic filters to perform similar types of authorization and manage the user's access to network resources.

©2001 Lucent Technologies, Inc.