Policy Management in GSM Data Networks

GPRS, EDGE, UMTS

December 2005

A Juniper Networks company

Funk Software, Inc.
222 Third Street
Cambridge, MA 02142
(617) 497-6339
http://www.funk.com

Executive Summary

GSM wireless operators benefit from improved customer satisfaction and significant return on their investment in packet data networking capabilities as they roll out 3G networks. 3G wireless services provide carriers with a diverse revenue stream and the opportunity to become the primary voice and data service provider to residential and business users. To implement next-generation wireless data access, wireless service providers have invested heavily in licensing and infrastructure in order to tap into the large installed base of users, and to be the first to offer a range of mobile services and applications — premium, applications such as m-commerce, pushed personalized content, streaming media, push-to-connect, text and photo messaging and many more that are helping wireless operators to maximize their average revenue per user and lower the cost of customer servicing and retention.

A comprehensive policy management solution provides those wireless service provider with a suite of tools to recognize the user, offer and enforce service delivery and track usage and network resources; all integrated seamlessly with the OSS and billing systems.

Current wireless infrastructure requires an advanced authentication, authorization, and accounting platform providing high availability AAA services in 2G, 2.5G and 3G networks in both the existing RADIUS and next generation DIAMETER protocols.

To monetize high-value applications, wireless service providers are demanding an especially robust AAA solution that:

- Enhances the value of Business Systems and the investment in the wireless network through management of subscriber policies.
- Provides dynamic IP address management and user-managed services across both legacy circuit switched and newer packet network technologies
- Enables authentication of both pre-paid and post-paid mobile users based upon any number of wireless operator-defined attributes such as Mobile Station Identifier and Network Access Identifier and redirects unauthorized or malicious users to management portals.
- Quickly and easily bundles, packages and delivers differentiated services to individual subscribers.
- Provides comprehensive session-based logging and accounting to capture usage-based revenue and deliver on Service Level Agreements and develop trust and customer loyalty.
- Pushes state information to devices such as WAP and SMS gateways, cache servers, and filter servers and proxies.
- Integrates with existing business systems such as provisioning, rating, and billing systems and rapidly updates dictionaries for new and modified network elements.
- Scales to process thousands of transactions per second (TPS) and manages unexpected rapid growth as the infrastructure evolves to incorporate new services. The introduction of new services has been shown to add significant

growth in TPS over an extremely short period, often by 100% over a period of days.

- Delivers maximum strategic value (ROI) by accommodating operator-class transaction levels, leveraging a operator's existing infrastructure and management resources, and scaling to support exponential traffic growth over the short term.

This paper will discuss in greater detail the role of policy management in wireless networks. It will present Funk Software's Carrier Grade Steel-Belted Radius, the most widely deployed policy management solution in both wired and wireless infrastructures facilitating customer-managed services-on-demand and capitalizing on the growth in wireless data services.

The Business Drivers of Mobile Data Services

The GSM industry's success can be attributed to cooperation and support across the entire vendor and service provider community that have resulted in a true end-to-end infrastructure-to-terminal environment and seamless global roaming for users of mobile voice and data services. More than 70% of global mobile use is on the GSM networks, covering 80% of the world's population. GSM Subscriber growth in 2004 exceeded 280 million new users to more than one and quarter billion users. GSM use is projected at more than two and a half billion users by the end of this decade. Regardless of the wireless infrastructure being implemented – 2G, GPRS, 2.5G, EDGE, and more recently 3G / WCDMA, UMTS, WiFi and CDMA2000 there is a significant untapped opportunity in offering wireless data services due to large numbers of existing mobile phone users, low cost handsets and high-value mobile applications that are being developed and introduced constantly. In 2004, data revenue represented less than 10% of the industry's total revenue yet was the fastest growing segment.

The recent introduction of advanced data bearer technologies and the packet switched nature of GPRS networks present a rich opportunity for efficient, attractive applications. Subscribers are using their mobile terminals for much more than basic text content such as news, information and messaging. New network features, policy management tools and exciting handsets offer enhanced applications to customize use and drive revenue including:

- **Wireless Internet access**. Faster transfer rates allow faster delivery of richer applications and content to wireless devices. UMTS networks are deployed in more than 30 countries and global subscriber growth in 2004 was 2 million new users every month.
- **Wireless Virtual Private Networks**. Operators recognize the potential of offering companies dedicated wireless VPN access to their corporate Intranets via the wide area and wireless local area WiFi networks, enabling employees to easily and securely retrieve up-to-date company information from anywhere.
- **IP- based Services**. Wireless operators offer a rich set of mobile, IP-based telephony, messaging, conferencing and contact center applications that integrate the office with the mobile environment.

- **Pushing content**. Wireless operators continue to build an attractive service offering including real-time delivery of personalized content and virtual user groups with push-to-connect features.
- **Profile-and location-based services**. Wireless operators offer advertisers the opportunities to push content based on a caller's stated preferences, click path, or recent m-commerce purchases.
- **Entertainment**, including downloaded content, streaming audio and video, and wireless gaming with effective digital rights management.

An Introduction to AAA

Mobile data service offerings require the integration of the new data infrastructure elements with the legacy voice network to provide packet-based functionality. Many wireless operators are replacing their earlier use of enterprise grade AAA systems with Funk's **Steel Belted Radius Carrier Grade Servers** that are centrally managed and configured and readily scale and integrate with newer service delivery platforms

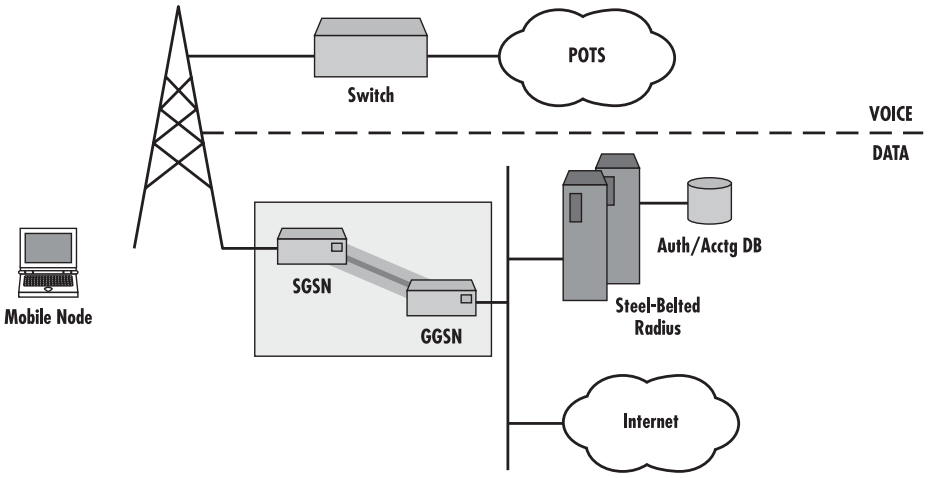


Figure 1. The migration from a voice-only network to an infrastructure supporting voice and data.

The AAA (authentication, authorization, and accounting) server provides the following functions in a wireless environment:

- **Authentication**. Authentication is the process of identifying a user or device attempting access to a network though a network access server; typically this attempt is based on a number of attributes or user's established credentials, which may include Network Access Identifier, MSISDN number, username and password or a SIM card authentication. To authenticate a wireless user, a AAA server matches the user's credentials with credentials stored in a central database or directory residing on the home wireless network.

  Naturally, the radio infrastructure also authenticates users whenever they request access, however the GGSN uses the AAA server to perform additional authorization:

- To differentiate users, individually, within a tribe or across service providers to deliver the appropriate level of profile-determined services and redirect to portals if necessary.
- In a wholesaling, roaming or MVNO environments, to route or proxy the authentication request based on user credentials.
- To converge services in order to provide subscribers with a consistent experience across all services and access networks.

- **Accounting**. The AAA server records all access activity in a format recognized by the wireless operator's billing, provisioning, and customer care systems. In a mobile data deployment, the AAA server, in addition, provides accounting capabilities beyond those required for traditional voice services:
  - Provides differentiation between traditional voice traffic and various data services, which may include IP voice, a key requirement for tracking and billing data services separately from traditional voice calls and indicates a subscribers presence on the network such as in an IM or a hosted dispatch service.
  - Enables usage-based billing for services such as tiering, time on the network (e.g., your first 30 minutes of Internet access are free) peak time premiums, QoS parameters, or total bytes transferred to the network.
  - Provides seamless integration with the operational systems with detailed traffic and network usage information that is used to model and plan network upgrades.
  - Provides integration with Prepaid Services to meter and manage sessions against a subscriber profile or quota.
  - Provides tools to model user profiles, generate alarms and detect and terminate fraudulent, unauthorized, concurrent (shared account) use and malicious network access.
- **IP address assignment and mobility management**. Once the wireless user is authenticated, the AAA server may assign that user or device an IP address, which functions as the user's identity on the Internet. The AAA server may also retain the same IP address for the entire duration of the subscriber's connection across multiple access networks and must contain a sufficiently large dictionary of various vendors' network access devices
- **Service delivery and state management**. The AAA server must also determine, deliver, and enforce the level of service granted to the wireless user. It does this by authorizing the user to access certain resources on the network and set restrictions such as time-of-day, maximum bandwidth, timeout lengths; and pushing connection information to other devices on the network such as WAP and SMS gateways, cache servers, and filter servers, to:
  - Deliver personalized content and set up specialized connections to the subscriber
  - Manage access based upon specific geographical areas or roaming agreements
  - Manage service level agreements that guarantee certain premium customers preferential access and specific number of concurrent sessions or users from

one enterprise account or restrict the number of visiting concurrent sessions from a specific roaming partner.

The logical components of Funk's Steel Belted Radius Server are shown in Figure 2

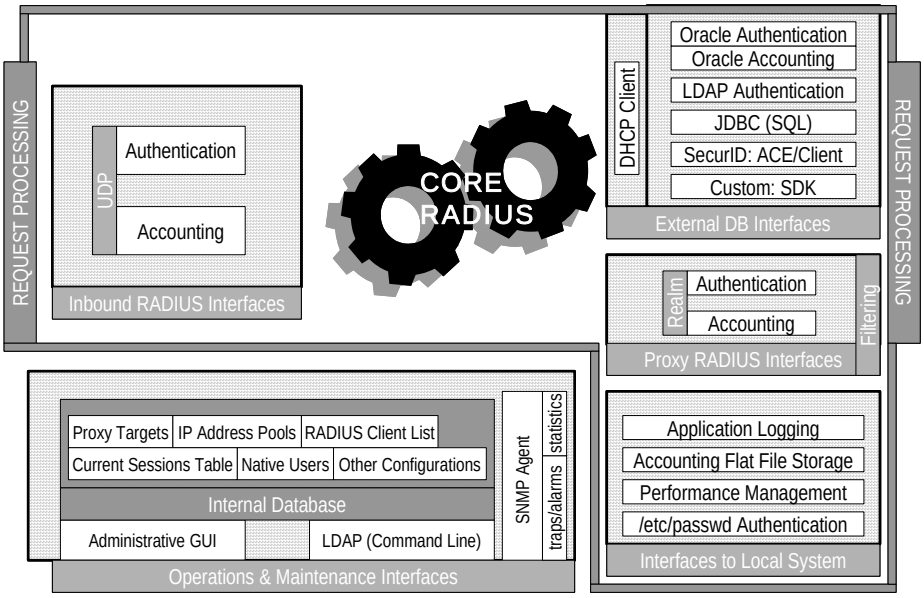


Figure 2 The logical components of Funk Software's Steel-Belted Radius AAA server

AAA and IP Address Management

A major feature of a wireless service is the ability to provide a single IP address to the user's mobile terminal for the entire session; in some cases, the IP address must persist, even as point-to-point radio connections are made and broken as the user moves from cell to cell in the wireless operator's network or from one wireless technology to another such as when the GPRS network receives or makes a handoff to an 802.11 WiFi or private network.

IP for GSM provides a limited degree of IP address mobility. IP for GSM is handled at network layer 2, and can guarantee IP address mobility if a user moves to a cell handled by a different SGSN, provided the mobile node continues to be serviced by the same GGSN.

Before describing IP for GSM, we'll define some terms and acronyms that are used in the discussion of this service architecture.

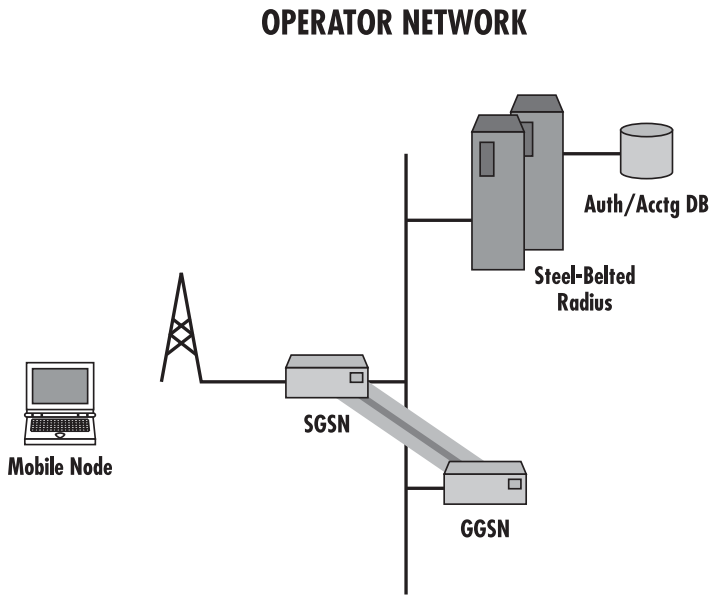
Wireless Term	**Definition**
Subscriber	A wireless user, someone who is paying a subscription for wireless service.
Mobile node	A multi mode wireless IP device (phone, PDA, Laptop etc.)
Provider Network	A network owned by the subscriber's wireless provider.
Partner network	A network owned by another provider with which the subscriber's provider has a roaming agreement
SGSN (Serving GPRS Support Node)	A network access server through which the mobile node connects to the wireless network.

GGSN (Gateway GPRS Support Node)	Access point for GSM data activity onto the network.
APN Access Point Name	The APN defines the network connection and QoS parameters

A typical GSM data network encompassing GPRS, EDGE or UMTS maintains multiple GGSNs but a particular user's traffic is usually serviced by the same GGSN for any given session. The user's mobile node connects to the network via an arbitrary SGSN. The SGSN contacts the appropriate GGSN on behalf of the user, based on the APN value stored in the SGSN or provided during the connection to the SGSN. A tunnel is established between the SGSN and the GGSN to carry the user's traffic. The user's mobile node is assigned an IP address that is maintained by the GGSN. As the mobile node connects with each new SGSN, a new tunnel is established from the new SGSN to the original GGSN. The GGSN is able to keep the user's IP address constant, and simply route the mobile node's traffic to the current SGSN via the tunnel. Figure 3 illustrates IP for GSM.

The AAA server performs several key roles on GSM data networks. The GGSN performs an authentication request via a RADIUS protocol Access Request message to the AAA server prior to admitting the user to the network. The AAA server checks with the subscriber database and responds with user- and session- specific authorization information which configures the GGSN with the user's IP address and permissions on the network. The RADIUS accounting packets generated by the GGSN are logged by the AAA server, providing a complete record of user network access.

Figure 3. IP for GSM



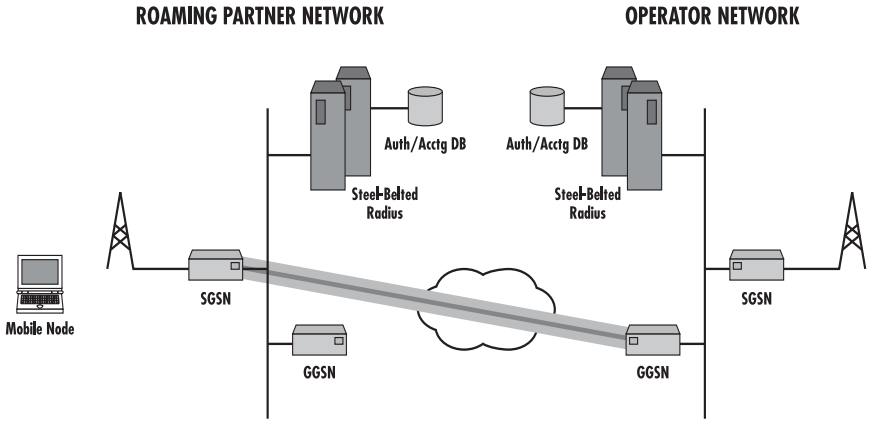
IP Address Mobility And Roaming

A mobile node may request mobile data access while roaming on a visiting network. The visiting network SGSN is provided the address of the GGSN on the user's home network that is to be his access point onto the network.The SGSN contacts the home GGSN to establish a connection. The GGSN attempts to authenticate the user by sending an "access request" message to the AAA server. The AAA server verifies the user's credentials, sends an "accept" message along with information about how to

configure the connection, including IP address and connection filters, permitting the GGSN to route the user onto the network.

Figure 4 illustrates a GPRS roaming scenario. In this scenario, the SGSN forwards the access request to the appropriate GGSN server at the user's home operator network. If the address of the home GGSN is not known, the request is forwarded to a GRX (Global Roaming Exchange Carrier) who resolves the APN address and forwards the request to the appropriate GGSN. The GPRS session is set up in the same way as in the non-roaming case, except that the tunnel is between the SGSN on the partner network and the GGSN on the operator network.

Figure 4. Roaming

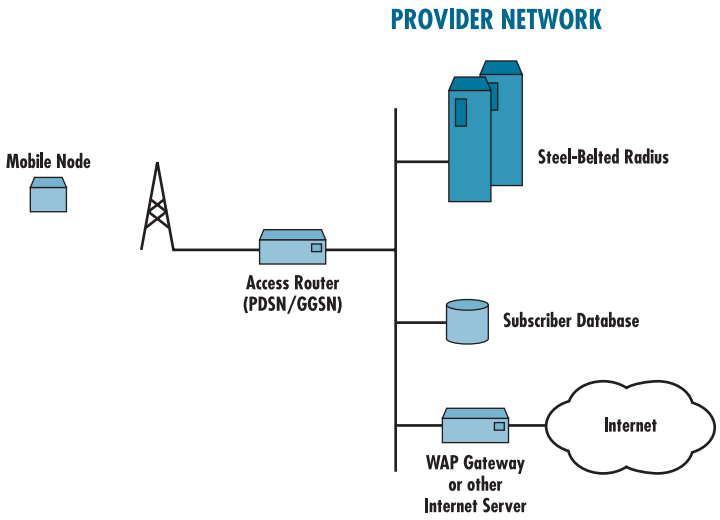


State Management for WAP Gateways

Devices such as WAP gateways, cache servers, and filter servers allow wireless operators to offer such premium services as pushing personalized content and delivering profile- or location-based services to subscribers. A challenge is the delivery of the appropriate content or service, when the subscriber wants it. Since these devices are not designed to manage subscriber mobility, they need to be kept apprised by a separate device of each subscriber's "state" or connection status.

The AAA server provides the WAP gateway and other devices with real time subscriber connection details, including the user's credentials (typically the MSISDN number, handset serial number or user name) and the currently assigned IP address for that user. In addition, the AAA server may append other information retrieved from the subscriber database that the WAP gateway requires.With this information, the Internet Server is able to deliver the appropriate level of service to each subscriber.

Figure 5. An AAA server can write state information to a subscriber database for use by an Internet Server, or push the information directly to any server that supports RADIUS accounting.



Wholesale Access Services

An operator, offering wholesale access services is able to generate revenue by providing capacity to other operators and service providers. An MVNO service provider, sourcing capacity from these operators provides access and other services to their customers without having to build and manage the radio infrastructure. While the role of an AAA server in this environment is much the same as already described (i.e., it authenticates users, authorizes connections, and accounts for their presence), the MVNO environment presents additional requirements.

In this type of environment, the AAA server must perform the additional function of proxying access and accounting requests to the service provider or customer site, which has the database necessary to perform AAA. By proxying requests, an operator can distribute AAA functions to different sites, which is advantageous in many situations. The operator may also elect to host the entire infrastructure and share the AAA platform across multiple MVNO's via a Directed Realm configuration.

Distributing AAA functions

In a wholesale environment, the responsibility for authentication, accounting, and the management and upkeep of user authentication credentials may be distributed from the AAA server at the operator site (wholesaler) receiving the access and accounting requests to a AAA server at another site (MVNO).

- As an operator providing capacity, a distributed architecture greatly simplifies the customer facing administrative burden. Rather than having the responsibility for maintaining all of your customers' authentication data, you can simply proxy AAA requests to the appropriate customer network for authentication or host the authentication in a directed realm AAA configuration. Accounting records are distributed as appropriate to the various MVNO partners.
- As a MNVO service provider sourcing capacity, a distributed architecture lets you maintain complete control of your own customer authentication data, including your subscriber credentials database and which services each customer is entitled to. The wholesale purchase of capacity provides the MVNO with leverage at the network service wholesalers to provide the MVNO with

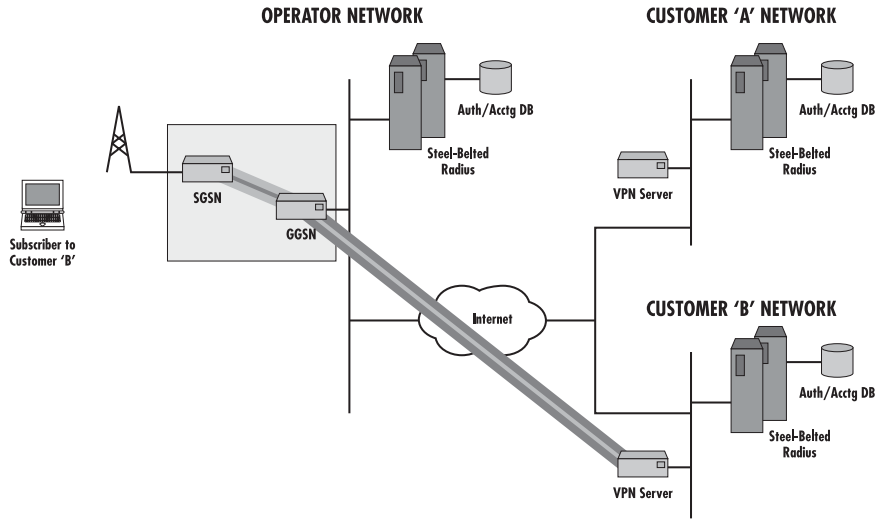
aggressive rates. Ownership of the AAA platform provides greater security, provides the tools to bundle and offer differentiated services and allows the MVNO to update customer information as necessary, without having to rely on the operator.

Managed VPN Services

VPN services can be layered onto the wireless radio infrastructure, creating significant new revenue opportunities beyond phone subscriptions for operators and providers. For example, many operators have recognized the potential of offering companies dedicated wireless VPN access to their corporate Intranets, enabling employees to easily and securely retrieve up-to-date company information from anywhere.

In a managed VPN scenario, the AAA server performs the tasks already discussed in the previous sections. In addition, it provides the key additional function of configuring the tunnel – including providing such information as encryption protocol, tunnel endpoint, and tunnel password to the GGSN or VPN server.

Figure 6. Managed VPN architecture using a distributed AAA platform.



The AAA server on the operator network can store user information, tunnel configuration information, or both. The information it doesn't store, it gets via proxy from the AAA server at the customer site. The more security-conscious a customer is, the more likely it is to want to maintain complete control over all user and tunnel configuration information.

When a VPN user requests access, the GGSN sends an access request to the AAA server at the operator site. The AAA server recognizes that it's a tunnel request, and either provides the configuration information to the GGSN, or proxies the request to the AAA server at the customer site to provide the appropriate configuration information. Once the GGSN correctly configures the tunnel to the VPN server at the customer site, the VPN server sends a user authentication request to the AAA server at the customer site. If the authentication is successful, the user's tunnel is established.

Meeting Business Requirements

Beyond providing the technical features and attributes described above; to support a wireless infrastructure, a AAA policy management system should enable a wireless operator to deliver the fast, high-quality wireless data services that subscribers will demand, as cost-effectively as possible. To do this, the AAA server must:

- **Handle a transaction volume that is significantly larger than that of a "wired" Internet subscriber base**. During a single wireless Internet session, the AAA server must process authentication, authorization, and accounting transactions not only when the subscriber first connects to the Internet, but also every time the subscriber moves between coverage zones. These wireless connection models, coupled with the huge existing and projected wireless subscriber volumes, require AAA policy management servers that can support transaction rates in the thousands-per-second range.
- **Integrate seamlessly with the operator's existing or planned/future network infrastructure, customer care data, and management tools**. To minimize the operator's administrative overhead and leverage existing investments, a AAA server must support network access servers and services from the widest possible range of vendors and integrate with existing provisioning and billing systems.
- **Deliver the reliability and scalability projected wireless growth will require**. An AAA server should enable redundant access to authentication, authorization, and accounting systems, and should easily scale vertically and horizontally without sacrificing performance.
- **Support advanced proxy capabilities** to support roaming and wholesaling agreements, and wireless VPN services.
- **Include comprehensive attribute support**, for compatibility on any network providing any type of service.

Funk Software's Steel-Belted Radius exceeds these requirements.

Funk Software Steel-Belted Radius

Several years ago, corporations, ISPs, and others providing "wired" remote intranet and Internet access faced authentication, service delivery, and billing issues similar to those facing wireless operators today. Over time they turned to solutions based on *RADIUS* (Remote Authentication Dial-In User Service), a specification developed and maintained by a working group within the Internet Engineering Task Force (IETF) that describes how a network access device communicates with a server for AAA purposes.

In 1996, Funk Software introduced Steel-Belted Radius, a full-fledged implementation of the RADIUS specification designed to leverage existing authentication data, maximize infrastructure choices, and operate reliably. Owing to its support for virtually every leading remote access vendor *and* every leading network directory format, Steel-Belted Radius quickly became the leading RADIUS solution in the market.

In 1999 Funk Software introduced Steel-Belted Radius/Service Provider Edition, a carrier-grade version of Steel-Belted Radius designed to exceed the reliability, service delivery, and performance requirements of the global service providers. In 2000,

Funk Software introduced Steel-Belted Radius/Advanced Wireless Edition, the first deployed RADIUS/AAA server to meet the IP address management requirements of 3G wireless networks. Funk Software has developed a suite of policy management servers including session control, port allocation and concurrency servers, all designed to drive revenue for the wireless operators. The family of Funk Software Steel-Belted Radius products are deployed by most of the worlds largest ISPs and wireless operators.

Specifically, Steel-Belted Radius provides:

- **Performance equal to the unique and heavy call frequencies of wireless Internet access**. Based on the top-performing AAA engine in the industry, *Steel-Belted Radius handles thousands of AAA transactions per second on suitable hardware* —to accommodate the demands of a carrier-class wireless network.
- **RADIUS accounting that supports consumptive billing.** Steel-Belted Radius's accounting capabilities track and document all remote access to the network. All information — remote username, duration of connection, device to which the user connected, and amount of data transmitted — is captured to a log file or written directly to a SQL-based system, enabling wireless operators to charge customers on virtually any basis.
- **Capability and features to deliver the full range of wireless services**. Steel-Belted Radius manages the delivery of any wireless service offering, from low-cost on-demand Internet access to premium wireless applications. It enables operators to grant access based on time of day, connect time limits, or any other criteria. It fully supports the mobility management requirements imposed by GSM architectures. In addition, it easily scales to meet the 3G/CDMA2000 IP address and mobility requirements of tomorrow's wireless infrastructures.
- **Seamless, customizable integration with SQL or LDAP customer data**. Steel-Belted Radius integrates well with existing credentials and network configuration data that an operator has already deployed — in any SQL database or LDAP directory. It can be configured to work with any SQL table structure and LDAP schema.
- **Carrier-grade proxy options for flexible roaming configurations**. Steel-Belted Radius's *proxy* capabilities enable passing of authentication requests to another AAA server that contains the necessary information to perform the authentication. These authentication options enable authentication of mobile users dialing into a roaming partner's network, or connecting to one of your corporate clients' wireless networks that you may be hosting.

  Steel-Belted Radius can also proxy accounting data to any back-end system or to a content management infrastructure such as a WAP gateway, communicating the connection status of a subscriber, and enabling the delivery of personalized content.
- **WAP gateway integration**. Steel-Belted Radius is fully customizable to deliver subscriber connection details to a WAP gateway or other Internet Server in whatever manner is appropriate for your requirements.
- **SS7 network integration** Steel Belted Radius supports the entire set of EAP methods including EAP SIM authentication and one time password via SMS messaging to extend services into unlicensed radio environements.

- **SNMP support**. Steel-Belted Radius can report to any SNMP network management application, and includes full support for statistics, traps, and alarms.
- **IP address allocation management in all wireless scenarios**. Steel-Belted Radius supports assignment of static IP addresses, or address pooling either set up within Steel-Belted Radius or based on your own DHCP address pools.
- **Comprehensive VPN capabilities,** including full support for L2TP and IPSec.
- **The widest vendor and platform support in the industry**. Steel-Belted Radius is fully compliant with the IETF RFCs for RADIUS protocols, and supports wireless equipment from Juniper, UT Starcom, 3Com, Cisco, Ericsson, Lucent, Motorola, Nokia, Nortel, and others.
- **Infrastructure neutrality**. Steel-Belted Radius works with any radio infrastructure, from today's GSM/GPRS and CDMA2000 networks to tomorrow's IMS and 3G/Mobile IP-based infrastructures.
- **Carrier-grade reliability**. Based on a server already used to manage AAA on some of the world's largest Internet and wireless operator networks, Steel-Belted Radius provides carrier-grade reliability and capacity so operators can meet their stringent uptime requirements.

Conclusion

To fully realize the opportunity presented by next-generation all IP networks, wireless service operators rely on a AAA solution that combines the necessary authentication, IP Address management, service delivery and accounting technology with the raw performance, ease of integration, manageability, and scalability that ensures the fastest and highest return on their infrastructure investment. Based on a AAA server that's already proven itself in carrier-class environments, Funk Software's Steel-Belted Radius is the one AAA solution that can integrate directly into a operator's existing infrastructure today, and completely support that infrastructure's transition from GPRS to 3G.

To learn more about Steel-Belted Radius, contact Funk Software at (617) 497-6339, or visit the Funk Software web site at www.funk.com.

A Juniper Networks company

Funk Software, Inc.
222 Third Street
Cambridge, MA 02142
(617) 497-6339
http://www.funk.com