



iPhonica AAA & RADIUS

iPhonica's AAA RADIUS Server provides fully customizable standards-based authentication schemes and security for a variety of telecom access networks. Our RADIUS server enables Carriers & Service Providers to centrally manage access to their network. iPhonica's RADIUS server delivers unique extensibility, advanced policy, and customizability making it ideal for Carriers, ISPs, System Integrators and network equipment OEMs.

It comes with an extremely flexible dictionary that can be made to support any type of non-standard vendor-specific attributes, including multiple attributes inside the same VSA, non-standard attribute IDs or length fields, subfields, and much much more.

Authentication and Accounting Methods

iRADIUS integrates security issues and supports authentication and accounting from Livingston formatted text files and databases. Supported database connections are ODBC, Oracle and MySQL. It incorporates increased security into the database by using encrypted passwords in users' text profiles. Supported encryptions are MD3, MD5, and TEXT (no encryption) and password authentication from local system shadow file is also supported. You can use Password-Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP) for user-password authentication type and at the same time, time-based authentication and authorization of users is also supported. Furthermore, iRADIUS is fully configurable for use with your own choice check-reply attributes for authentication, authorization and custom-attribute selection for accounting.

Flexible session handling

You can also configure iRADIUS to store online users' sessions or active sessions. An active session record may be kept in a database or in iRADIUS's internal structure. iRADIUS uses these active sessions to track online users' status and to control simultaneous multi-sessions. Session records are stored temporarily by default, i.e. a session record of a user is deleted when the user disconnects or stops using the service. iRADIUS can also be configured to store these records in a permanent storage (database / accounting log file).

Realm based authentication and accounting

Another far reaching benefit of iRADIUS is that it supports realm based authentication and accounting which it performs by selecting a realm from user-name@realm-name. This 'realm-name' is used to handle an authentication and accounting request from the 'user-name' if the realm is defined in RADIUS configurations, otherwise a default authentication/accounting handler will be used to process the request.

Best multi-vendor and multiple-RADIUS-client support

iRADIUS can also be deployed in a large scale network using multiple-vendors' equipment that in turn work as RADIUS-clients. You can handle authentication, authorization and accounting (AAA) differently for each of your NAS equipments simultaneously with same server configurations. Such a distributed handling of NAS equipments (RADIUS clients) with a centralized server provides a great deal of localized management and stability.

Configurable multi-session currency control

iRADIUS enables you to allow/restrict multiple logins with same user information. iRADIUS can be configured to specify a default maximum multi-session and/or user-specific multi-session attribute. By default, a user's login name is the only attribute identifying multiple sessions of the same user and a set of attributes have to be configured in order to create a unique user-login.

CLI and MAC address based authentication support

IRADIUS can also be configured to authenticate users by using their calling numbers or by using the MAC address of the user's equipment. This technique is usually used for wireless authentication.

ANI, PIN and account based authentication support

VoIP gateways from different vendors have different authentication schemes. For example, Cisco AS5300 has two authentication policies for VoIP, which are PIN system and PIN-less system. Similarly Quintum gateways support ANI authentication, PIN based authentication, account based authentication and mix of PIN and account based authentication. IRADIUS can be configured with any authentication scheme including the ones mentioned above for users' authentication. See your gateways documentation for more information about related policies.

Redundant/Backup CDR recording support

IRS can be configured to record Call Details Records (CDRs) / Accounting information in multiple databases/text-files in a redundant or backup fashion. In case of redundancy, IRS writes records in all the configured accounting handlers. In case of backup, it writes CDR information in the first accounting handler only, but if it fails (due to database crashing, input/Output errors or lost connection to database error) then the subsequent accounting handler records the CDR.

Highly configurable to be integrated with different billing software

Different billing software's have different methods of storing user information in their databases. Some billing software use a single record per table to store user information for authentication by RADIUS, while others use multiple records in a table in attribute-value pair format. iRADIUS can be easily configured with such types of billing software.

Simultaneous Multi-Vendor gateway Support

iRADIUS can be readily deployed in a network environment where VoIP gateways or access servers from different vendors are working on centralized authentication using the RADIUS protocol. It can be easily configured to fully serve all multi-vendor gateways with Vendor Specific Attribute (VSA) support.

Configurable Logging

iRADIUS also supports multi-level logging for RADIUS server packet tracing. Low-level logging is very helpful in identifying configuration errors, when the RADIUS server is not handling requests properly.

Following are the log levels in descending order:

OFF - No Debugging

SEVERE - Only errors

WARNING - Errors + warnings

INFO - Debugging of RADIUS processing. Good for tracing errors

ALL - intensive debugging
Log output can be generated on a console or a text file. A low log level has a considerable impact on performance, so it should only be used for testing purposes.

RADIUS Proxy & Roaming

Proxy and roaming service is also provided by IRADIUS Server. You can use iRADIUS as a forwarding proxy server to one or more RADIUS servers for load balancing and roaming support. This feature makes iRADIUS a beneficial choice for large distributed networks.

Supported Authentication Protocols

Radius Server supports following authentication methods to be used between RADIUS-client and RADIUS server. Different authentication protocols may be configured at the same time to be used for different RADIUS-clients.

- Password Authentication Protocol (PAP)
- Challenge Handshake Authentication Protocol (CHAP)
- EAP-MD5
- Digest Authentication

Supported Databases

Though RADIUS server supports all types of database-servers that provide JDBC or ODBC interface, however following are tested Database servers and are in production at numerous customer locations.

- ODBC
- Oracle
- MySQL

Cluster Setup

iRADIUS can also be setup in a clustered environment where more than two servers are deployed. These servers run side by side in a parallel load balanced environment that ensures high availability. Setup details for a clustered setup are dynamic and are based on customer specific requirements. Its complete specification is customer specific and out of scope of this document.

Failover Setup

For high availability iRADIUS can be configured in a primary/secondary mechanism as well as in a fully redundant clustered environment. The failover setup is provided at multiple levels to ensure high availability of the solution.

