Transform your AAA Infrastructure using Alepo AAA, which is a performance driven AAA with in-built Policy Framework

A cornerstone of DSL and other wireline IP data networks, AAA infrastructure serves as an important service and policy control framework, enabling internet service providers to control how their subscribers access and consume IP data services. In this capacity, AAA touches a number of areas within the core network and back office, from security to provisioning to billing and beyond.

While the core functions of AAA have remained, for the most part, unchanged since its inception in dialup and, later in DSL internet networks over a decade ago, today’s rapid growth in subscriber numbers and overall data usage has placed new demands on the AAA infrastructure, not only in terms of network capacity and performance, but also in the creation and delivery of innovative, differentiated services that heighten the customer experience. Throughout the years, service providers have commonly introduced workarounds or stopgap solutions in an effort to extend the capabilities of the legacy AAA infrastructure to meet these new demands. Over time, this can create a complex and operationally inefficient AAA environment, one that inevitably limits scalability and hinders performance.

To emerge successful and profitable, service providers must employ an advanced AAA and policy framework, and do so efficiently without impacting existing services or the customer experience.

AAA TRANSFORMATION

AAA Transformation is about more than replacing a “box” in your network; it is a holistic approach to evolving the AAA and policy framework in a legacy core network to one that is modern, scalable, and highly extensible, in order to realize sophisticated end-to-end business processes and to achieve greater network optimization. The following sections detail Alepo’s AAA solution, including architecture and key features of Alepo’s high-performance AAA and Policy Framework for wireline internet service providers.
FEATURES & HIGHLIGHTS

Robust and Carrier-grade AAA

Alepo AAA performs Standard Authentication, Authorization and Accounting functions along with the in-built PCRF-Lite function to support Policy Management requirements. Provides SNMP Support; also features AAA EMS Web-Service which supports SOAP based Web Services to provision AAA users. Alepo AAA also provides support for multiple databases like Oracle and MySQL for subscriber and CDR storage, supports LDAP as user authentication database.

Vendor Neutrality and Standards Compliancy

Alepo’s dual stack (RADIUS/DIAMETER) AAA Server is vendor neutral because it comes from a pure B/OSS player instead of a hardware vendor. A vendor neutral and standards-compliant AAA solution allows providers to choose mix-brand, best-of-breed networks at inception and as the network grows, saving money at network launch and beyond.

Scalability and Failover Support with High Performance

Alepo’s AAA Server is extremely high-performing. A high performing solution decreases churn by creating a highly responsive system that maximizes efficiency of network elements. The product has the capability scale horizontally or vertically and is reliable to support scalable business model with 99.999% availability.

Multi-Service Support

Designed to support multiple services, Alepo’s AAA Server is able to provide a centralized session and identity management system for a variety of services ranging from data, voice, video, and content in fixed line (xDSL/DOCSIS) and wireless (CDMA/EVDO, EDGE/UMTS/HSPA, LTE, Wimax & Wi-Fi)

Centralized Identity Management

Alepo’s AAA Server provides a centralized location for subscriber data, including logon and session management parameters. This provides a secure, centralized location for subscriber information, streamlining networks and assuring security of login details by utilization of cryptographic algorithms while being FIPS 140-2 certified.

Session Management

Supporting both prepaid and postpaid, Alepo’s AAA Server offers leakage-free session management. Alepo’s AAA Server tracks usage in real-time to enforce session disconnect policies, and even offers quota-based policy management to ensure zero leakage, even in the event of multiple simultaneous sessions on a single prepaid account.
**IP Address Management**

The Alepo AAA server provides IP allocation using AAA (DHCP not mandated). It supports dynamic and fixed IP addresses, with correlation between IP Pools and policy profiles. Additionally, the 16e AAA Server supports different IP pools for multiple hosts and different services (data, voice, management) and ensures efficient management of IPs even in the event of network failure.

**Session Caching**

Comprehensive, real-time information on any given subscriber’s session is available to network elements that require it.

**Advance Handling of Forwarding**

Enables RADIUS Accounting messages forwarding. Support for SNMP MIBs enables interface with NMS to raise performance alarms.

**Scripting Engine**

Includes a high-performing scripting engine which enables you to write and implement custom authentication/authorization rules in-house and run them without having to recompile or “dirty up” the source code. The scripts are written in human-readable language to facilitate faster implementation, hence reducing the risk of errors.

**Support for Emergency Mode**

Supports to avoid a single point of failure when database is on separate subnet from AAA application servers. Database connectivity loss with Alepo AAA due to any simple routing, firewall or network change can cause serious outages and revenue loss. Alepo AAA Emergency Mode ensures seamless availability from such outages due to database connectivity issues:

- All customers will get authenticated in the case of database connectivity loss.
- Revenue loss will be minimized during such a scenario

**Noise Reduction**

Alepo’s AAA intelligently handles and reduces signaling “noise” on a network that is created by endless loops of authentication requests by CPEs and Modems. This is achieved by setting network counters, policy rules and by using Alepo’s Notification Center to redirect disturbing users, instructing them to make corrective actions.

**Security**

SSL encryption, customer password protection and lockout configuration can be set above a certain minimal strength. Identifiers, such as phone numbers, or device MAC addresses can be blacklisted.
Usage Monitoring and Notification

Supports enforcement of FUP policies on reaching maximum usage cap accumulated over a specific period. The usage cap can be defined either in time units or in volume units. Also supports notification based on usage levels.

Technical Specifications

Alepo’s AAA software supports the following RFCs and EAP methods. It can also be designed to meet extended requirements at the request of the Service Provider.
**RFCs & Standards Compliance**

- RFC2865 -- Remote Authentication Dial-In User Service (obsoletes RFC 2138; updated by RFC 2868)
- RFC2866 -- RADIUS Accounting (obsoletes RFC 2139; updated by RFC 2867)
- RFC2869 -- RADIUS Extensions
- RFC2882 -- NAS Requirements: Extended RADIUS Practices
- RFC4282 -- The Network Access Identifier
- RFC5080 -- Common Remote Authentication Dial In User Service (RADIUS) Implementation Issues and Suggested Fixes
- RFC2548 -- Microsoft Vendor-Specific RADIUS Attributes
- RFC2759 -- Microsoft PPP CHAP Extensions, Version 2
- RFC 2284 -- PPP Extensible Authentication Protocol (EAP)
- RFC3748 -- Extensible Authentication Protocol (EAP)
- RFC4017 -- Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs
- RFC5176 -- Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)
- RFC3574 -- IANA Considerations for RADIUS (Remote Authentication Dial In User Service)
- RFC4186 -- Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP - SIM)
- RFC 2809 -- Implementation of L2TP Compulsory Tunneling via RADIUS
- RFC2251 -- Lightweight Directory Access Protocol (v3)
- RFC2716 -- EAP-TLS, B. Aboba and D. Simon, PPP EAP TLS Authentication Protocol (EAP-TLS)
- RFC5216 -- The EAP-TLS Authentication Protocol
- RFC5218 -- Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0)
- RFC2716 -- EAP-TLS, B. Aboba and D. Simon, PPP EAP TLS Authentication Protocol (EAP-TLS)
- RFC5216 -- The EAP-TLS Authentication Protocol
- RFC3162 -- RADIUS and IPv6
- RFC3539 -- Authentication, Authorization and Accounting (AAA) Transport Profile

Copyright © Alepo 2015.
Specifications subject to change without notice.
**3GPP Standards**

3GPP Gy interface Rel9,10 (TS 32.240 and TS 32.299)
3GPP SWx interface Rel10 (TS 23.402)

**3GPP2 Standards**

3GPP2 X.S0011-002-C - Simple IP and Mobile IP Access Services
3GPP2 X.S0011-005-E - Accounting Services and 3GPP2 Radius VSAs
3GPP2 X.S0011-006-C - Prepaid Packet Data Service

**WiMAX Support**

WiMAX 16e NWG Release 1 v1.5

**LDAP Support**

RFC 2251 – Lightweight Directory Access Protocol (v3)

**SNMP Support**

RFC4668 - RADIUS Authentication Client MIB for IPv6
RFC4669 - RADIUS Authentication Server MIB for IPv6
RFC4670 - RADIUS Accounting Client MIB for IPv6
RFC4671 - RADIUS Accounting Server MIB for IPv6
RFC4672 - RADIUS Dynamic Authorization Client MIB
RFC4673 - RADIUS Dynamic Authorization Server MIB

**Supported EAP-Authentication mechanisms**

EAP-TLS, EAP-TTLS-MSCHAPv2, EAP-TTLS-CHAP, EAP-TTLS-PAP, EAP-AKA, EAP-AKA', EAP-SIM, EAP-FAST, EAP-IKEv2, EAP-PEAP/MSCHAPv2, EAP-PEAP/TLS, EAP-PEAP/GTC, EAP State Machine according to RFC 4137

**EAP methods cryptography is FIPS 140-2 certified**