Aptilo Access Controller

Data sheet

At a Glance

The Aptilo Access Controller™ (AC) gateway is purpose-built for access control, usage monitoring and policy enforcement in Wi-Fi networks. It runs on standard hardware and features true client plug-and-play functionality. The AC dynamically handles user sessions, QoS and routing from the local network to the Internet.

Depending on the business model and integration level, the Access Controller can either be locally, regionally or centrally placed in the network, catering to several separate sites.

The AC software can assume 3 different roles; Load Balancer (front-end), Traffic node (back-end) and Backup node.

The Aptilo Access Controller™ (AC) forms part of a state-of-the-art platform from Aptilo Networks that facilitates the creation of wireless broadband access services. The Aptilo AC, together with the Aptilo Service Management Platform™ (SMP) and Service Portal™ (SPA), forms a comprehensive, seamless solution that creates unique capabilities for administration and control of services in Wi-Fi networks. The solution enables Wi-Fi services in large public service provider networks and semi-public places such as airports, hotels, shopping malls, conference centers and networks in metropolitan areas as well as guest Internet access on enterprise campuses.

Access Control and Policy enforcement

The Aptilo Access Controller is purpose-built for access control, usage monitoring and policy enforcement in Wi-Fi networks. It can lookup policies from AAA and PCRF via RADIUS pull.

Aptilo AC runs on standard hardware and features true client plug-and-play functionality. It dynamically handles user sessions, QoS and routing from the local network to the Internet.

Together with the *Service Profiles* defined in the Aptilo Service Management Platform (SMP) the AC constitutes a powerful tool for handling differentiated service bundles with prioritization of traffic on the user level.

Service Profile "Premium"

QoS:

Main Service: 8 Mbit/s, prio2
Service 1: Web, no cap, prio2
Service 2: FTP, 500 kbit/s, prio 6
Default: All other, 1 Mbit/s, prio 3

Additional Service:
VoIP, 128 kbit/s, prio1

Firewall: Blacklist "subscriber"

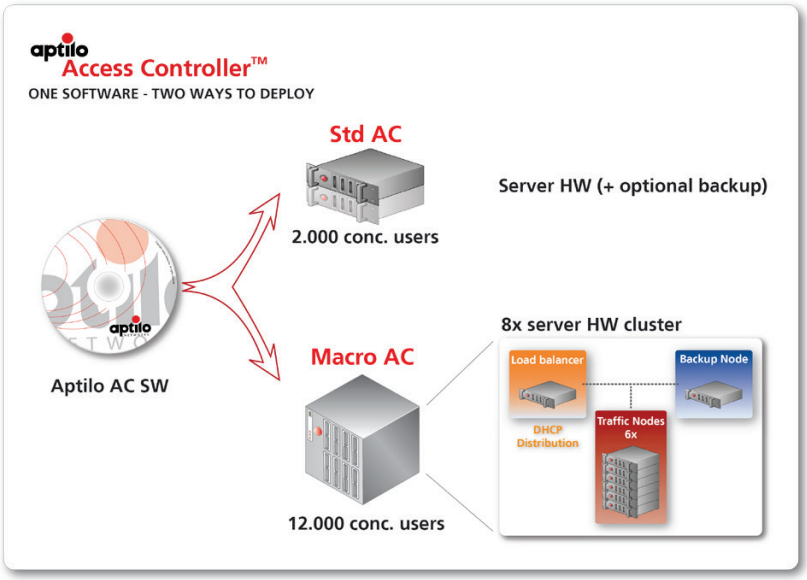
Route: Route through VLAN 60

In the sample *Service Profile* "Premium" to the right, the *main service* is capped to 8 Mbit/s of total bandwidth allowance for the "premium" user. Listed below the *main service* are services that can be capped or defined as unlimited, these are prioritized within the *main service*. Optionally an *additional service* can be defined outside the *main service* and prioritized on the same level. This ensures that there is additional capacity left for e.g. real-time critical applications even if the bandwidth of the *main service* is consumed. Specific *firewall* and *route* policies can be set for each *Service Profile*. The automatic bandwidth balancer feature of the Aptilo AC distributes available bandwidth between all active sessions according to the priorities set in the service profiles. A service can be automatically throttled down to a certain capacity if the pre-paid quota has been depleted to a specified level.

Scalability & Redundancy - an AC for every need

The Aptilo Access Controller software runs on standard hardware scaling from 2000 to 12.000 concurrent users. Depending on the business model and integration level, the Access Controller can either be locally, regionally or centrally placed in the network, catering to several separate sites.

In a cluster configuration the AC software can assume three different roles: *Load Balancer, Traffic node* and *Backup node.*



The Aptilo AC can be deployed behind third-party Wi-Fi access gateways and Wi-Fi access point controllers to enable functionality that cannot otherwise be achieved, in these cases the Aptilo AC becomes a critical service enabler.

Authentication & User Session

Session Management
- Session kill
- Service Profile change: Different QoS, Routing, Firewall etc
- Auto re-authentication
- Quota support

User interaction
- "Plug & Play", zero config.
- Built-in Captive portal
- Walled garden, free sites
- Captive portal based on subnet

User authentication RADIUS
- Device/MAC (Automatic login)
- Intelligent 802.1x proxy
- HTTPS
- Smart-client support
- WEB-server for WISPr login
- Custom RADIUS attributes

Plug-and-Play
- Static IP Support
- Proxy auto detection
- NX domain handling
- Proxy http handling

Service Profiles (Aptilo SMP)
- Hierarchical service definitions, main service with underlying sub-services
- QoS cap, priority, guarantee
- QoS tagging DSCP (DiffServ)
- Firewall rules e.g. white lists
- Routing e.g. different VLAN

Automatic login
- Support for SIM Authentication
- HTTP request based on MAC
- HTTP request based on cookie
- Client discovery based on MAC
- Client discovery based on DHCP option 82

Network Capabilities

IP-address Management
- DHCP Server
- DNS Server
- Custom DNS (operator defined)
- Multi subnet option
- Multi NIC support

Routing
- Policy based routing
- Source based routing
- Dynamic and Static NAT
- Static route support
- OSPF routing protocol

IP-address Assignment
- Static
- DHCP client and server
- Proxy ARP

Mobile IP FA Support
- Mobile node pass-through
- Authorized Networks
- Security Associations

Network Structure
- LAN VLAN (802.1q) handling
- WAN - VLAN (802.1q) handling
- Support for external http proxy
- Multi NIC support
- Local subnets
- Routed remote subnets

Location Mapping
- Mapping of subnet to location
- Mapping of APs to location
- RADIUS Option 82 for location identification

Policy Enforcement

Per session QoS
- Enforcement of the QoS Policies set in the service profiles
- Automatic Bandwidth Balancer
- Dynamic Bandwidth Throttling
- DiffServe
- DSCP

Per access controller QoS
- Bandwidth limit in / out (bps)
- TCP Connection limit per user
- Radius Bandwidth Override

Policy Lookup
- RADIUS policy lookup (Pull) from AAA / PCRF
- Policy lookup triggered by Session Duration , Data Volume and Change of Authorization (CoA)

Time of Day Service Control
- Allow / disallow users at a certain time of day based on the service profile
- Differentiated policy and rating based on time-of-day and day of week.

Monitoring & Management

Handling Local Nodes
- Monitoring of access points, xDSL routers etc through icmp ping or SNMP
- Management of nodes in the private address space through Aptilo SMP

SNMP
- SNMP v1, v2, v2c and v3
- Allow SNMP requests Yes/No
- Allow traps / trap hosts
- Multiple trap destinations

Management
- Management interfaces: SSH, HTTPS, RS-232
- Management via Aptilo SMP through VPN
- Remote software upgrade
- Multi-Config. from Aptilo SMP

Reporting
- Mail
- Multiple trap hosts
- Aptilo SMP escalation
- Support for external syslog server

Redundancy & Scalability

AC in traffic node role
- Back-end Access Controller(s) taking the traffic load
- Scaling up by adding more traffic nodes

AC in load balancer role
- Front-end DHCP Server
- Distributes clients over the different traffic nodes
- Round Robin DHCP

AC in backup role
- One-to-many redundancy for traffic and load balancer nodes
- Number of backup nodes is dependent on the required level of high-availability

High availability functions
- Internal monitoring with auto-recovery
- Hot standby
- Synchronization of settings to backup ACs

Security

VPN
- Tunnel carries authentication information to the Aptilo SMP
- Tunnel allows placement behind firewall and NAT

Network Security
- Built in Firewall
- Dos and DDos protection
- IP Address Spoofing protection
- Black- and white-lists
- Green lists, allow incoming traffic from certain addresses
- VPN pass-through for IPSec, PPTP and L2TP VPNs
- PCI compliant (Payment Card Industry)

Legal Intercept
- Collection of tracking table for TCP and UDP session data: Source IP/Port, Destination IP/Port, NAT IP/Port, Timestamp
- Routing to wiretapping server

Platform

Integration and API's
- Hotel Property Management System (PMS) via serial cable

Server AC hardware requirements
- 2.000 concurrent users per server
- Certified HW: Standard Servers (single server or blade server) with at least two physical network interfaces.
- At least 2 GB RAM, 4 GB if > 1000 sessions

SMP = Aptilo Service Management Platform™

About Aptilo Networks

Aptilo Networks is a leading provider of systems to manage mobile data services for Wi-Fi, WiMAX and 3G/LTE networks, including mobile data offloading. Aptilo's carrier-class solutions boast pre-integrated authentication, policy control and charging functions to maximize the capabilities of the wireless network and fast-track deployments while minimizing impact on existing systems. They feature a multitude of interfaces and APIs for seamless integration to external systems of choice. Aptilo's solutions are delivered as software licenses, or as a hosted, cloud-based service using the Aptilo Managed Service™ from one of our many regional data centers located worldwide, or handled remotely by Aptilo's experts from servers at the customer premises. With proven interoperability with all leading vendors in the wireless ecosystem, Aptilo's solutions are currently in operation in more than 60 countries.

AMERICAS
+1-866 861 3900

APAC
+60 3 2780 6900

EMEA
+46-8 5089 8900

aptilo NETWORKS

www.aptilo.com
info@aptilo.com