

# Aphelion

A fully managed private and public WiFi solution offering quality of service and security



## Total control of your WiFi network

Providing Wi-Fi both for business and public access needs careful consideration – open up public access and you could find that not only are you compromising your security, but that all the bandwidth you require for essential business services such as card payments or VoIP is used up.

**Aphelion** gives you the control to prioritise bandwidth, so that if you make a public hotspot available, you can control how different users can have separate levels of access to different services – securely and without risk to escalating bandwidth usage costs and user congestion.

The latest beam forming technology of our Access Points provides ubiquitous coverage for your users, and content filtering ensures that non business essential or inappropriate content is not available unless authorised.

Organisations that are able to install secure Wi-Fi will not only have a more flexible communications infrastructure that reduces traditional cabling costs throughout their buildings, but they will provide an enhanced user experience for their employees and customers.

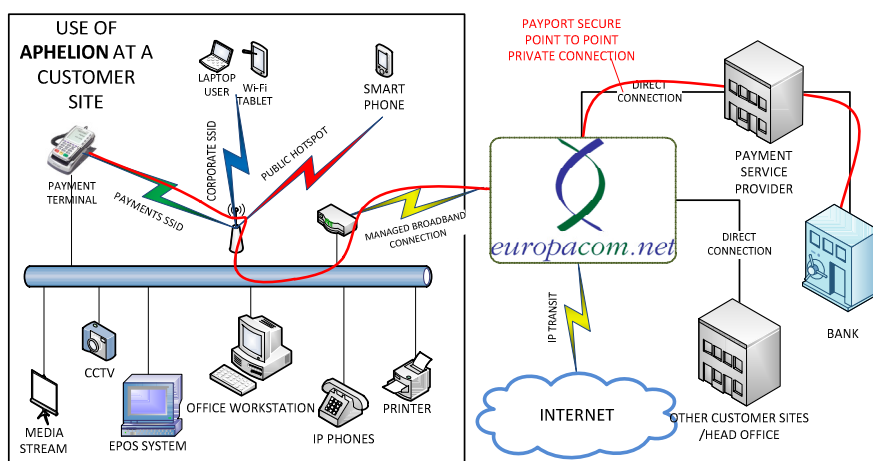
## Hosted central control and remote monitoring

The significant defining features of Aphelion are the quality of the wireless coverage and its remote management. Aphelion Access Points (AAP) are backhauled into hosted intelligent Wi-Fi controller (so need for expensive dedicated equipment for each customer) that centrally manage all administrative, management and maintenance tasks, providing monitoring right the way down to each individual wireless access point. A distributed standard template can be applied for the deployment configuration of SSID, Security and connectivity options that can be remotely changed on a site or estate basis.

Active Monitoring can identify unconnected inventory by geographical site showing when it was last in service, connected WiFi clients connected at any particular time and the traffic protocols being used or downloaded. Protocol characteristics can then be priority controlled or even barred if appropriate (e.g. a hotspot could bar Peer2Peer traffic that might be consuming considerable bandwidth). Remote access to this level of detail and upon demand, allows for very comprehensive diagnostic analysis to be undertaken, assisting in resolving potential service calls.

Wi-Fi can variably be connected to the local LAN, Head Office, directly to the internet, via a Hotspot with user recording or by subscription with AV, spam and URL filtering also available.

## A typical deployment



## KEY FEATURES:

- Guaranteed full coverage in a designated area
- Public or private Wi-Fi service
- Fast, reliable and secure wireless broadband service providing access to Voice, Internet and Data systems
- Control and priority of service to ensure that bandwidth is ring fenced for essential business services
- Carrier class equipment and service including remote management and monitoring
- PCI DSS compliant service

## Hotspot management and reporting

The status of each individual AAP can be monitored remotely, including not only measuring the performance output but identifying the number of users on the AAP at any given time.

Hotspot management allows you to control how much free or chargeable access time you might want to give a public user to your hotspot, and what you allow them to access or otherwise.

Furthermore, valuable insights can be contained from the reporting suite that is available with Aphelion Hotspot management.

Standard available reports include:

- **Subscriber:** full details of all those who have logged into your public hotspot, including emails, that with necessary permissions, can be sued for future marketing campaigns
- **Accounting:** Measure time on line and usage by each user
- **Access log:** Identify successful and failure logs in helping you to identify any potential user problems
- **Online users:** see who is accessing the service at any given site at each access point and site

Aphelion Diagnostic

Name	Serial	IP Address	State	Uptime	CR	MSC
CRGateshead-AP1of2	k095-02438	10.8.91.24	Connected	163.05:04:43	0	TRA1
CRGateshead-AP2of2	k095-02162	10.8.91.22	Connected	163.05:10:39	2	TRA1

MAC Address	IP Address	Radio	SNR	Signal	Noise	SSID
DB:1:5D:E1	10.8.91.43	1	48	-53	-101	tpt
DB:1:5F:1D	10.8.91.41	1	44	-57	-101	tpt

Subscribers Accounting

Username	Session Stop Time	Bytes Uploaded	Bytes Downloaded	Client IP Address	Customer	Location	Time Online	Termination Cause
francois@com	14-02-2011 11:29:20	140283	83099	10.18.53.00000	Qualife-Network	Qualife-Headsh	00:01:09	Lost-Service

Access Log

Username	Date & Time	Result	Reason
dan@ec.com	26-01-2011 15:01:33	Success	Good Password
dan@ec.com	26-01-2011 15:53:54	Success	Good Password
dan@ec.com	26-01-2011 15:56:19	Failure	Bad Password
dan@ec.com	26-01-2011 15:56:40	Success	Good Password
dan@ec.com	27-01-2011 11:44:51	Failure	No such user
dan@ec.com	27-01-2011 11:45:03	Failure	No such user

Online users

Username	Session Start Time	Client IP Address	NAS IP Address	Time Online	Acct Session ID	Customer	Location
ps@ps@ps.com	10-05-2011 14:48:17	10.19.24.12	127.0.0.1	00:18:39	130503211117697	Qualife-Network	Qualife-Headsh
ps@ps@ps.com	10-05-2011 14:48:17	10.19.24.12	127.0.0.1	00:18:39	130503211117697	Qualife-Network	Qualife-Headsh
ps@ps@ps.com	10-05-2011 14:48:20	10.19.24.12	127.0.0.1	00:18:31	130503211117697	Qualife-Network	Qualife-Headsh
ps@ps@ps.com	10-05-2011 14:48:20	10.19.24.12	127.0.0.1	00:18:31	130503211117697	Qualife-Network	Qualife-Headsh
ps@ps@ps.com	10-05-2011 14:48:20	10.19.24.12	127.0.0.1	00:18:27	130503211117697	Qualife-Network	Qualife-Headsh

## Managed connectivity with real time active monitoring

Europacom utilises CWMP (CPE Wide Area Network Management Protocol) which allows for the remote management of end-user devices. This allows equipment to be deployed in a raw state and then to collect its configuration settlements from Europacom's Auto Configuration Server automatically as it logs into the network, enabling fast, efficient and dynamic deployment within large estates of users.

Additionally, support of end user equipment is easy with real time active monitoring, and a self healing "phone-home" process which restores the original configuration if the hardware is tampered with. This ensures that the integrity of sites and company security policies are not compromised and provides the ability to actively monitor CPE "heart beat" in real time to identify any possible problems at the earliest opportunity.

