v1.14_SoftWLC

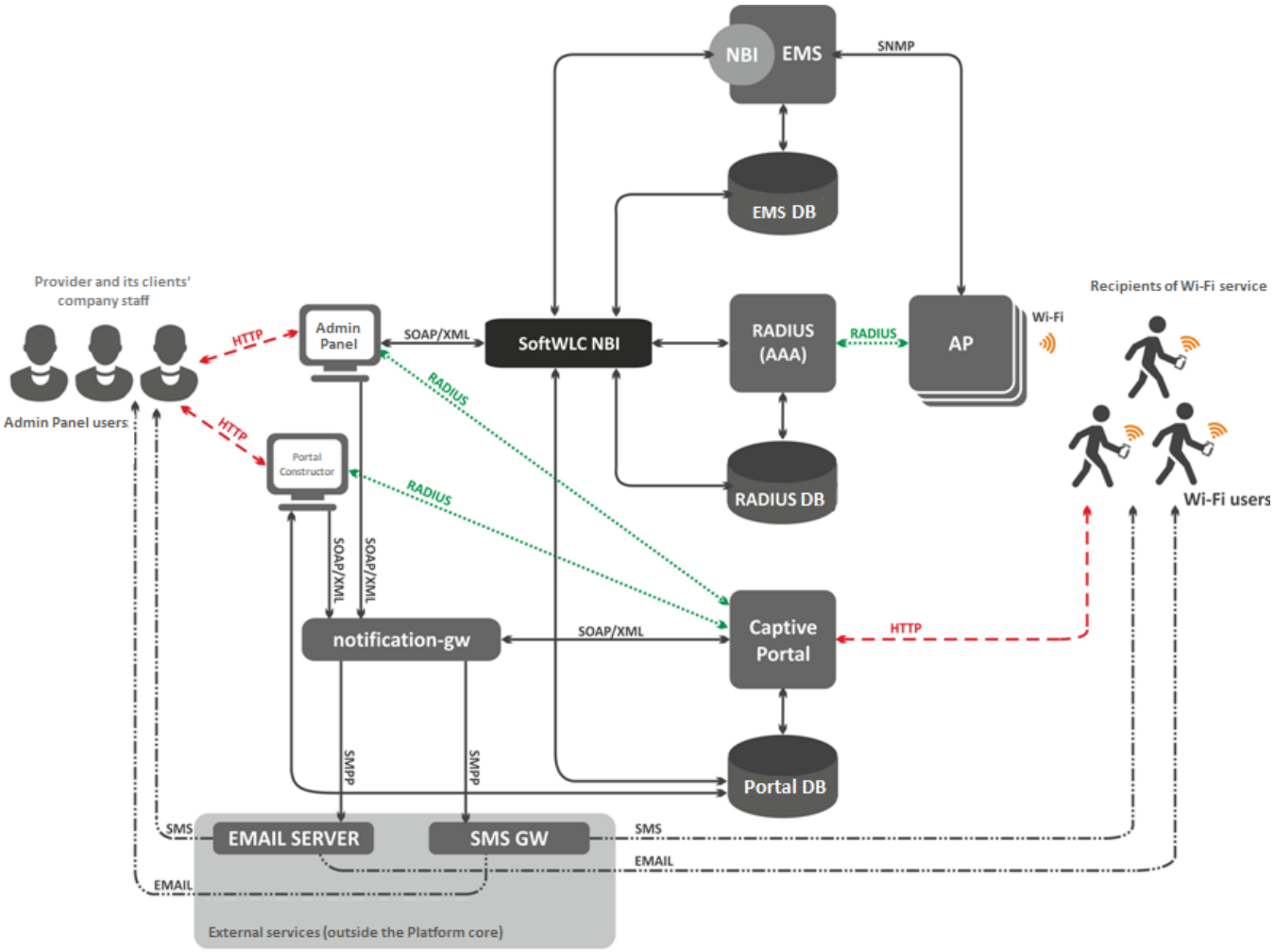
General features

SoftWLC **is a software Wi-Fi controller** that consists of several modules performing various operations in order to provide complex solution for organization of centralized Wi-Fi networks with Portal and Enterprise authorization. According to project requirements, certain modules can be included into the system or excluded from it.

Key features of SoftWLC:

- Control and monitoring of Eltex equipment that forms the basis of Wi-Fi solutions.
- Flexible administrative access policies distribution for various objects and features to be provisioned to SoftWLC users within a carrier's distributed hierarchy
- Hotspot service implementation with portal authorization that allows:
    - Integration of advertising providers' resources into a portal
    - Integration with payment systems
    - Portal design branding according to a client's requirements
- Enterprise authorization
- Possibility of integration with the external Active Directory
- Providing end users with a WEB tool for service management, portal branding and user account creation.
- SSID sheduling

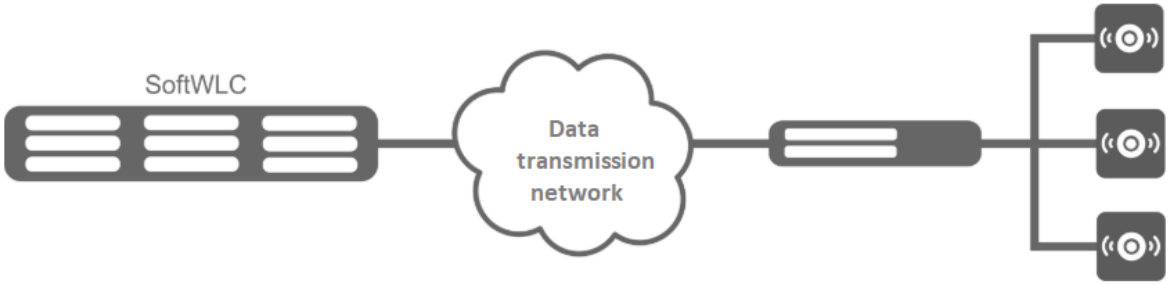
SoftWLC main modules



- **EMS-server** is a SoftWLC central component that provides management and monitoring of other modules of the system, GUI for an operator to work with SoftWLC and NBI interface for integration to a carrier's OSS.
- **WEB portal** is a module based on tomcat6 WEB server and providing a set of WEB portals for user authorization in Hotspot networks and Portal Constructor for their customization. The list of the WEB portal's features includes integration with SMS gateways and auto generation of Wi-Fi user accounts in a database.
- **B2B Admin Panel** is a WEB resource that provides a user with convenient interface for new Wi-Fi users' accounts creation and basic service management operations like SSID name change.
- **Database** – SoftWLC single database built on Mysql. Contains all the information about the system: from equipment configuration to user activity statistics.
- **RADIUS server** based on freeRADIUS is a module responsible for AAA operations (Authentication, Authorization, Accounting).
- **DHCP server** is a module that issues addresses for access points and Wi-Fi users. The server is based on isc-dhcp server. An operator can optionally use custom DHCP servers.
- **APB service** is a service intended for centralized synchronization of users' status information between access points. It provides seamless roaming between Hotspot access points.
- **Auth Service** is a common module for user authentication and authorization. Based on the RADIUS server. The service is used for authentication and authorization in the systems: B2B Admin Panel and WEB portal.
- **Notification Gateway** provides centralized communication between platform components and external systems that allow sending SMS and Email. The module interacts with B2B Admin Panel and WEB portal.
- **PCRF** is used for SoftWLC and ESR-1000 interaction in BRAS mode, when ESR-1000 implements Internet access policies for Wi-Fi subscribers and redirects users to an authorization portal.

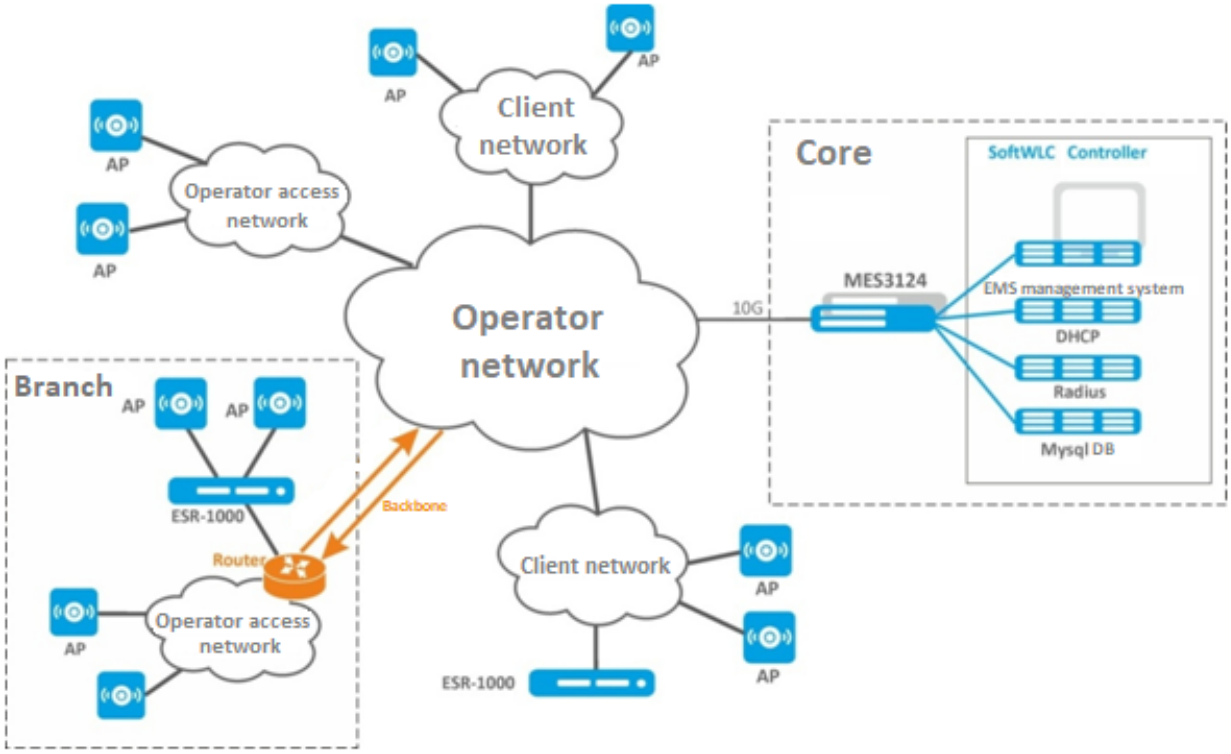
Typical applications

Minimal scheme



Minimal solution requires two servers: each server includes all the modules with Active-Active redundancy. SoftWLC servers are integrated to an operator's network. L3 connectivity is provided between the servers and access points. That is enough to use the product. Management interfaces are configured on each access point to provide interaction with SoftWLC within a special control VLAN. Client data goes from access points in clients' VLANs (one VLAN for each SSID) to carrier network and then to the Internet.

Global distributed scheme for large carriers



This scheme is a case for large distributed networks deployed between several cities or regions. The number of servers required for SoftWLC operation depends on the planned traffic load. 10 servers are needed for the maximum solution: the first pair of servers is reserved for EMS, WEB portal and APB, the second pair – for Database, the third pair – for RADIUS, the fourth pair – for DHCP. It is recommended to install Customer Cabinet to a separate redundant front-end server with maximum security. All the servers are connected to a pair of stacked switches that are connected to a redundant pair of routers in a carrier network. If a client decides to terminate subscriber sessions on his own territory, it is possible to move one or more ESR-1000 routers to a client's network. If a carrier network has global distributed backbone structure, it is possible to move ESR-1000 routers to subsidiaries.

Scheme using ESR-1000 service routers

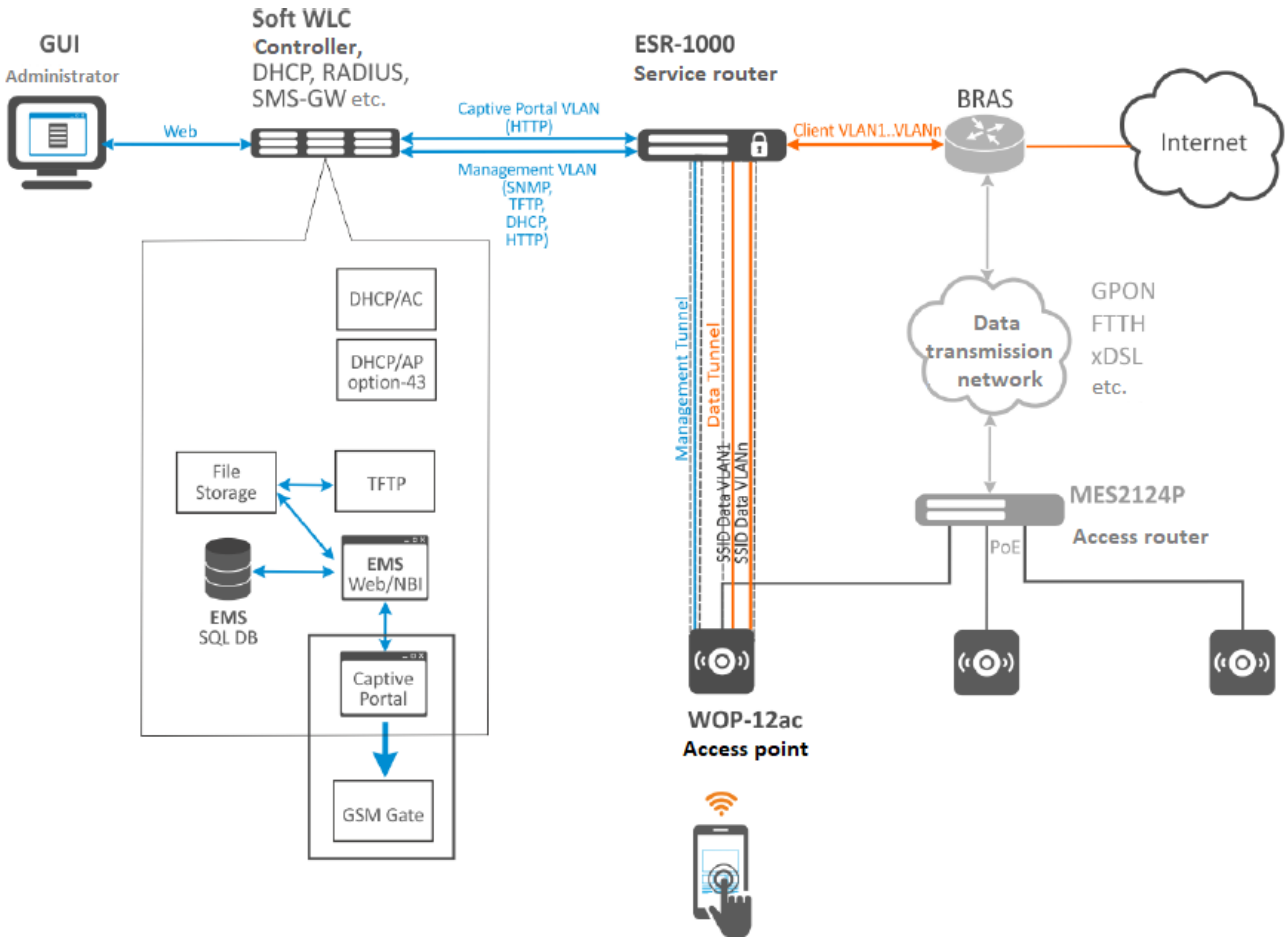
ESR-1000 service routers are used to solve the next tasks:

- relieving carrier network from subscriber session termination load;
- organization of automatic tunnel creation (L2 over GRE) between ESR-1000 and access points. The need for tunnel creation is to isolate subscriber traffic from management one. Due to the use of tunnels, an access point can be connected both to a client's or to a third-party access network and to interfaces that operate in "access" mode when processing L2 headers;
- network security organization by configuring a firewall integrated in ESR-1000;
- NAT (optionally);
- VRF implementation.

Access points can be connected both to a carrier's access network and to a client's one. When enabled, access points create Soft-GRE tunnels to ESR-1000 service routers over a carrier network. Then data is routed to SoftWLC or to the Internet.

SoftGRE tunnels between ESR-1000 and access points are created over a carrier L3 structure. Each access point has two tunnels: The *Management tunnel* for management traffic and the *Data tunnel* for subscriber traffic transmission.

The *Management tunnel* is used to transfer management traffic from/to an access point located in a separate management network. This subnet is invisible for a carrier's L3 segment due to *GRE tunnel* headers. Subscriber traffic is transffered within the *Data tunnel*. The traffic is terminated to ESR-1000 and then routed to a carrier network (to its NAT).



System requirements for the SoftWLC server

SoftWLC software controller should be installed on a server with **Ubuntu Server 14.04 LTS** operating system

Technical support is carried out only with **Ubuntu Server 14.04 LTS** operating system

When choosing a server, the following system requirements should be taken into account:

The number of devices	HP Proliant	CPU core, Xeon	RAM, Gb	HDD
up to 50 AP*	DL20	4, E3-1240v5, 8M Cache, 3.50 GHz	8	2x500G
from 50 to 200 AP	DL60	6, E5-2603v3, 15M Cache, 1.60 GHz	16	2x500G
from 200 to 500 AP	DL160	8, E5-2630v3, 20M Cache, 2.40 GHz	32	2x1T
from 500 to 1 thousand AP	DL160	8, E5-2630v3, 20M Cache, 2.40 GHz	64	2x1T