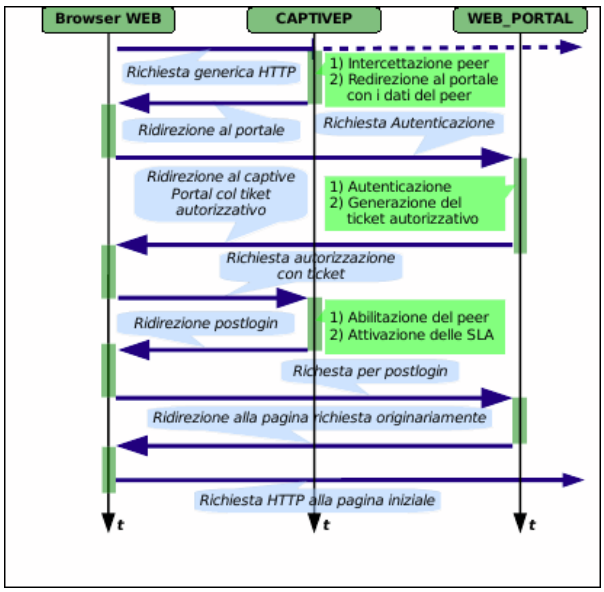
Documentazione/Documentatione v0.1

< Documentazione

Contents

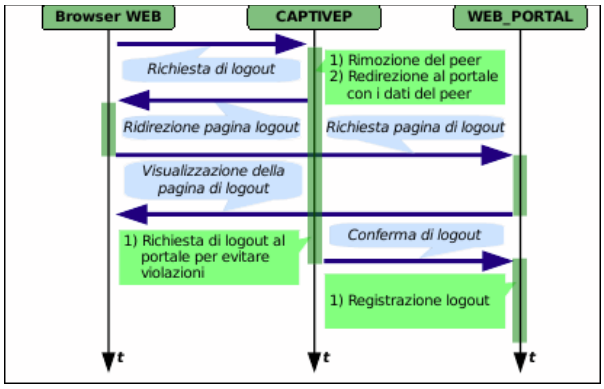
I processi

Login



/Esempio di sessione di login

Logout



/Esempio di sessione di logout

Portale autorizzativo

Il portale autorizzativo riceve richieste dal browser utente e dal captive portal point attraverso le seguenti interfacce http(s):

Pagina di accoglienza

- *URL*:

```
http(s)://<ip-address-portale>/
```

- *Metodo*: GET
- *Funzionalita'*: presentazione della pagina di accoglienza del servizio come effetto della redirect fatta dal captive portal al portale autorizzativo.
- *Parametri*:
  - *mac*: mac address della scheda di rete del pc

- *ip*: indirizzo ip assegnato dal dhcp server
- *redirect*: redirect al sito richiesto dall'utente (attualmente viene "forzata" una redirect a un sito impostato in configurazione (http://www.google.it/)
- *gateway*: indirizzo ip del gateway (captive portal) che ha fatto la redirect al portale autorizzativo (es: 10.30.1.113:5280)
- *timeout*:
  - valorizzato a 0: indica che captive portal lavora in modalita' *slave* (subordinato al portale autorizzativo). Questa e' l'impostazione attuale del sistema.
  - diverso da 0: indica che il captive portal lavora in modalita' non "slave". Questo significa che il captive portal e' abilitato a chiudere autonomamente il firewall per l'utente che ha consumato le risorse assegnate dal portale autorizzativo in fase di autorizzazione.
- *token*: <ip-address-pc-user>&<expire-date>&<message-authentication-code>, dove:
  - <*ip-address-pc-user*>: ip address assegnato al pc dell'utente
  - <*expire-date*>: data di scadenza del token. Impostato a 30 minuti. Definisce l'intervallo di tempo entro il quale deve essere completata la procedura di autenticazione sul portale.
  - <*message-authentication-code*>: generato come hash della stringa "<ip-address-pc-user>&<expire-date>" e firmata con chiave random generata dal server (HMAC)
    - esempio: 192.168.210.215&1256576515&7fb697caacaad8f30f9abff6b36b93ff
- *ap*: nome dell'acces point

NB: il sistema HMAC garantisce l'integrita e l'autenticita del token (http://en.wikipedia.org/wiki/HMAC).

- *Esempio*: http://10.30.1.102/?mac=00%3A14%3Aa5%3A6e%3A9c%3Acb&ip=192.168.210.215&redirect=http%3A//www.google.it/&gateway=10.30.1.113%3A5280&timeout=0&token=192.168.210.215%261256576285%26293b943f1fac04a8c58e1d9e3ceeaa82&ap=ap1.rspro

Autorizzazione/Login

- *URL*:

```
http(s)://<ip-address-portale>/login_request
```

- *Metodo*: POST
- *Funzionalita'*: consente di autorizzarzi al portale e invia la richiesta di apertura del firewall al captive portal di pertinenza per l'utente autorizzato
- *Parametri*:
  - *realm*: selettore che indirizza il database da utilizzare per l'autorizzazione
  - *uid*: il login dell'utente (numero di cellulare)
  - *pass*: la password dell'utente

Logout utente

- *URL:*

```
http(s)://<ip-address-portale>/logout
```

- *Metodo*: GET
- *Funzionalita'*: logout dello user. A fronte di questa richiesta il portale autorizzativo chiede al captive portal, tramite richiesta http e con un ticket firmato, di chiudere il firewall per l'utente (vedi: Richiesta di logout del portale autorizzativo per un utente connesso). Il captive portal, a sua volta, notifica al portale autorizzativo l'avvenuta chiusura del firewall (vedi: Comunicazione della chiusura del firewall da parte del captive portal)
- *Parametri*:

- *nessuno*

Comunicazione informazioni di stato dello user da parte del captive portal

- *URL*:

```
http(s)://<ip-address-portale>/logout
```

- *Metodo*: GET
- *Funzionalita*: acquisizione delle informazioni su traffico e tempo consumati e stato della connessione dell'utente. La richiesta viene inviata dal captive portal a fronte di una richiesta di *check* inviata dal portale autorizzativo (vedi: Informazioni sugli utenti serviti da un captive portal)
- *Parametri*:
  - *mac*: mac address del computer dell'utente
  - *ip*: indirizzo ip assegnato al computer dell'utente
  - *gateway*: indirizzo ip del gateway (captive portal)
  - *ap*: nome dell'access point
  - *user*: uid dell'utente (numero del cellulare)
  - *logout*:
    - valorizzato a 0: passaggio delle informazioni di stato dello user
    - valorizzato a -1: il captive portal ha rilevato che non c'e' piu' attivita' dell'utente (via system arp). In questo caso il portale autorizzativo assegna all'utente un bonus di 5 minuti. Viene registrato sul file di log l'operazione **"EXIT"** dell'utente. Esempio:
      - 2009/12/18 16:40:02 op: EXIT, uid: 3289784466, ap: semaforo-guidoni, ip: 172.19.118.101, mac: 00:13:e8:89:a1:37, timeout: 2807, traffic: 311228799
    - valorizzato a valore > 0: corrisponde alla notifica da parte del captive portal della chiusura del firewall per l'utente. Viene registrato sul file di log l'operazione **"LOGOUT"** dell'utente. Esempio:
      - 2009/12/18 12:16:01 op: LOGOUT, uid: 055340773, ap: ap0.rs, ip: 192.168.208.215, mac: 00:14:a5:6e:9c:cb, timeout: 3283, traffic: 312727474
  - *connected*: tempo consumato
  - *traffic*: traffico consumato
- *Esempio*: https://10.30.1.111/logout?Mac=70%3A1a%3A04%3A02%3Ab8%3A60&ip=192.168.208.139&gateway=10.30.1.112%3A5280&ap=ap0.rs&User=055340773&logout=0&connected=98&traffic=1310604

Notifica operativita' del captive portal

- *URL:*

```
http(s)://<ip-address-portale>/start_ap
```

- *Metodo*: GET
- *Funzionalita'*: notifica al portale autorizzativo dello stato di operativita' del captive portal. La richiesta viene fatta al portale autorizzativo dal captive portal contestualmente al raggiungimento dello suo stato operativo, ovvero la disponibilita' a ricevere e soddisfare richieste. Il portale autorizzativo provvede a mettere nello stato di logout gli eventuali utenti che risultano essere ancora loggati sul quell'access point. Viene registrato sul file di log l'operazione **"QUIT"** dell'utente. Esempio:
  - 2009/12/17 05:01:16 op: QUIT, uid: 055340773, ap: ap0.rs, ip: 192.168.208.215, mac: 00:14:a5:6e:9c:cb, timeout: 3368, traffic: 312737089
- *Parametri*:
  - *ap*: nome dell'access point su cui gira l'istanza del captive portal

Stato di un utente

- *URL*:

```
http(s)://<ip-address-portale>/stato_utente
```

- *Metodo*: GET
- *Funzionalita'*: l'utente connesso puo' ottenere informazioni sui propri consumi. Vengono visualizzate, relativamente a l'utente:
  - Il nome e il cognome
  - UID: il numero del cellulare
  - indirizzo IP (IP address)
  - Connection time
  - Il tempo trascorso dall'inizio della connessione (Elapsed connection time)
  - Il tempo rimasto a disposizione (Left connection time)
  - Il traffico consumato dall'inizio della connessione (Consumed traffic)
  - Il traffico consumato (Left traffic)
  - Mac address
  - Status: PERMIT, firewall aperto per l'utente
- *Parametri*:
  - *nessuno*

Captive portal

Il portale autorizzativo comunica con il captive portal attraverso le seguenti interfacce http(s):

Stato

- *URL:*

```
http://<ip-address-ap>:5280/status
```

- *Metodo*: GET
- *Visibilita'*: protetta, puo' essere chiamata solo dal portale
- *Funzionalita'*: fornisce una pagina html che riporta le informazioni sulla configurazione di rete dell'access point e la lista degli utenti serviti. Per la descrizione delle informazioni riportate relativamente a un utente, vedi la descrizione successiva *Stato di uno user*:
- *Parametri*:
  - Nessuno
- *Esempio*:
  - Pagina html di risposta: **/status**

Stato di uno user

- *URL:*

```
http://<ip-address-ap>:5280/status?ip=<ip-address-pc-user>
```

- *Metodo*: GET
- *Visibilita'*: protetta, puo' essere chiamata solo dal portale
- *Funzionalita'*: fornisce lo stato di uno user servito da quel captive portal

- UID: valori possibili
  - il numero del cellulare, nei casi in cui lo status dell'utente e' DENY o PERMIT
  - anonymous, nei casi in cui l'utente non si sia mai loggato su quel captive portal (N.B.: a ogni boot dell'access point queste info vengono rimosse)
- indirizzo IP (IP address)
- Connection time
- Il tempo trascorso dall'inizio della connessione (Elapsed connection time)
- Il tempo rimasto a disposizione dell'utente (Left connection time)
- Il traffico consumato dall'inizio della connessione (Consumed traffic)
- Il traffico consumato (Left traffic)
- Mac address
- Status: valori possibili
  - DENY, firewall chiuso per l'utente
  - PERMIT, firewall aperto per l'utente

- *Parametri*:
  - *ip address*: indirizzo ip del pc dello user

Informazioni sugli utenti serviti da un captive portal

- *URL:*

```
http://<ip-address-ap>:5280/check
```

- *Metodo*: GET
- *Visibilita'*: protetta, puo' essere chiamata solo dal portale
- *Funzionalita'*: fornisce al portale autorizzativo le informazioni tempo e traffico consumati, nonché sullo stato della connessione relativamente agli utenti serviti da quel captive portal. Il captive portal che riceve la richiesta comunica le informazioni al portale autorizzativo attraverso http redirect (vedi: Comunicazione informazioni di stato dello user da parte del captive portal). Questa richiesta e' inviata in automatico a ogni captive portal e con frequenza stabilita da configurazione (cron).
- *Parametri*:
  - *nessuno*

Richiesta di logout del portale autorizzativo per un utente connesso

- *URL:*

```
http://<ip-address-ap>:5280/logout
```

- *Metodo*: GET
- *Visibilita'*: protetta, puo' essere chiamata solo dal portale
- *Funzionalita'*: notifica il logout di un utente al captive portal che procede alla chiusura del firewall per quell'utente
- *Parametri*:
  - richiesta firmata*: la richiesta firmata (gpg) contentente i seguenti dati:*

```
ip=<ip-address-pc-user>&mac=<mac-address-pc-user>
```

- *Esempio*: `http://10.30.1.112:5280/logout?owEBHgHh%2FpANAwACAcI....owNDowMjpiODo2MAqI3AQAAQIABgUCSyD`

Server

High Availability

Software: heartbeat 2.99.3-14.3 (http://www.linux-ha.org/)

Descrizione

Il sistema e' configurato affinche' al boot entrambe le macchine avviino il portale autorizzativo (server http) e l'ldap autorizzativo.

L'HA, solo sulla prima macchina, attiva la sincronizzazione (stato del portale) della seconda macchina, il servizio voip e infine configura l'indirizzo virtuale del servizio. I vari captive portal (uno per ogni access point) referenziano il portale attraverso l'indirizzo virtuale del servizio. Di fatto la prima macchina eroga il servizio mentre la seconda rimane in standby.

Gli ldap sulle 2 macchine si mantengono allineati utilizzando il meccanismo MirrorMode.

A fronte di un down della prima macchina, la seconda macchina attiva il servizio voip e configura l'indirizzo virtuale del servizio. La sincronizzazione viene attivata ma di fatto non produrra' effetti fino a che la prima macchina non ritornera' disponibile.

Non e' attivato l'automatismo che consenta alla prima macchina, una volta che torna disponibile di riprendersi in carico il servizio. L'amministratore del servizio puo' indurre lo switch del servizio sulla prima macchina abbassando hearbeat sulla seconda

```
/etc/init.d/hearbeat stop
```

Una volta che la prima macchina ha ripreso in carico il servizio, puo' essere fatto ripartire l'hearbeat sulla seconda

```
/etc/init.d/hearbeat start
```

E' possibile configurare il sistema affinche' avvisi con un messaggio di posta elettronica alla partenza (e qundi al passaggio del servizio da una macchina all'altra) e al fermo del servizio.

E' possibile interrogare lo stato del sistema HA, con il seguente comando:

```
/sbin/cls
```

Configurazione

- /etc/ha.d/ha.cf: contiene la configurazione generale dei nodi
- /etc/ha.d/haresources: contiene la configurazione dei servizi da attivare
- /etc/ha.d/authkeys: contiene le key per la comunicazione tra i nodi

Mirror disco di sistema

Il disco di sistema e' mirrorato con una scheda hardware dedicata LSI SAS3442E-R (http://www.lsi.com/storage_home/products_home/host_bus_adapters/sas_hbas/lsisas3442er/index.html).

Il sistema e' configurabile affinche' mandi un avviso via posta elettronica a fronte di variazioni del suo stato.

Lo stato del mirror e' interrogabile con il seguente comando:

```
/usr/bin/mpt-status -ni 1
```

Access point

Backup

- Per effettuare il backup eseguire la seguente procedura:

```
echo -n 'ip address ? ' ; read ip

ssh root@$ip tar -C / -czf - /jffs | dd of=$ip.`date +%y%m%d%H%M%S`.jffs.tgz
```

Si otterrá un tar file che contiene tutto quello che serve per poter eseguire un restore.

Restore

Le board router station pro, usate per gli access point, hanno preinstallato openwrt e sono raggiungibili via ssh all'indirizzo 192.168.20.1 (passwd: ubnt)

- Per effettuare il restore, partire da un file tar di backup, eseguire la seguente procedura:

```
echo -n 'backup file ? ' ; read jffs
echo -n 'ip address ? ' ; read ip

dd if=$jffs | ssh root@$ip 'rm -rf /jffs/* ; tar -C / -xvzf -'
```

- Qualora si rendessero necessarie modifiche alla configurazione, modificare i seguenti file di configurazione:
  - /jffs/etc/config/system ### hostname ...
  - /jffs/etc/config/network ### ipaddr ...
  - /jffs/etc/nodog.conf ### mod_nocat ...