università di ferrara

L’accesso alla rete wireless di UniFe e la sua integrazione con la federazione IDEM

Relatore: Michele Lugli

Introduzione

- Wi-Fe è il servizio di connettività wireless dell'Università di Ferrara

- Il sistema è attivo da febbraio 2004
- Offre la copertura di tutte le aree didattiche e parte dei dipartimenti: sono installati oltre 250 access point

Obiettivi

- Offrire il servizio alla federazione IDEM
- Integrare l’infrastruttura esistente con l’architettura Shibboleth
- Rispettare le normative in tema di sicurezza informatica (logging degli accessi e del traffico)

Architettura di Wi-Fe

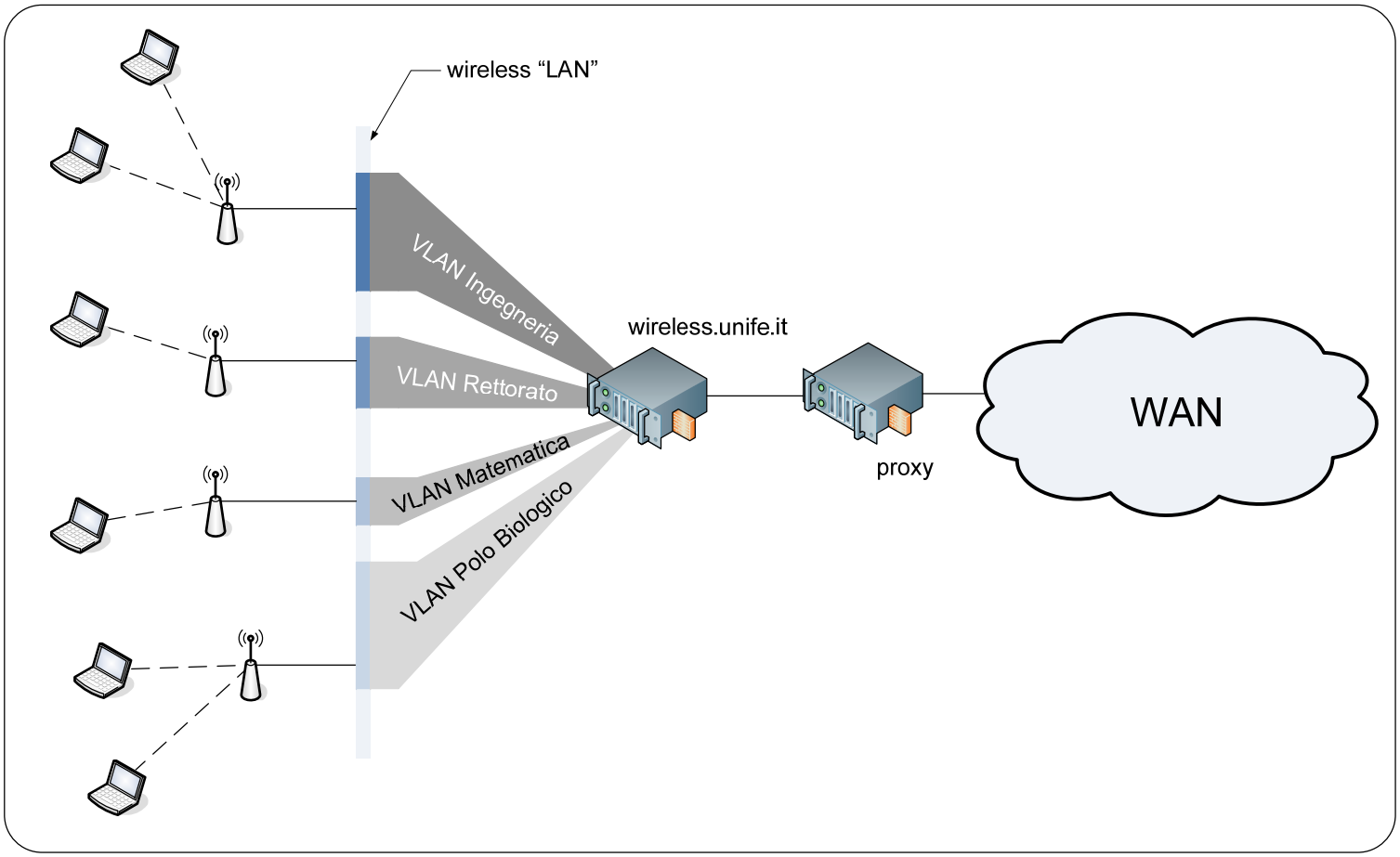
Architettura di Wi-Fe: infrastruttura

- Non vengono utilizzati sistemi di tipo proprietario (no WLAN controller e lightweight access point)
- Il sistema è centralizzato. L'infrastruttura di rete è realizzata in modo tale che tutto il traffico wireless sia convogliato verso un server Linux con funzioni di:
  - Bridge
  - Firewall
  - DHCP server
  - Captive Portal
  - RADIUS server
- E' stato scelto di non utilizzare chiavi WEP/WPA per aumentare al massimo la fruibilità del sistema da parte degli utenti.

Architettura di Wi-Fe: autenticazione e logging

- Il servizio è autenticato tramite un sistema di tipo “captive portal”. Esso effettua il logging di tutti gli accessi.
- Il traffico WEB viene monitorato attraverso un transparent proxy.
- Il traffico non WEB viene monitorato attraverso l’uso di iptables.

Architettura di Wi-Fe: schema



Scelta del captive portal

Scelta del captive portal: panoramica

- Il numero di utenti in costante aumento rende critica la scelta del captive portal

- Esistono molteplici soluzioni:
  - Opensource vs commercial
  - Windows based vs Unix based
  - Embedded vs server

Scelta del captive portal: panoramica

Nel corso degli anni sono stati valutati differenti sistemi di captive portal per piattaforma Linux:

- **NoCat** (software sviluppato in Perl, progetto interrotto)
- **WifiDog** (software sviluppato in C e PHP)
- **Zeroshell** (distribuzione Linux)
- **Chillispot** (sviluppato in C, utilizzato dall'organizzazione FON, progetto interrotto)

http://en.wikipedia.org/wiki/Captive_portal

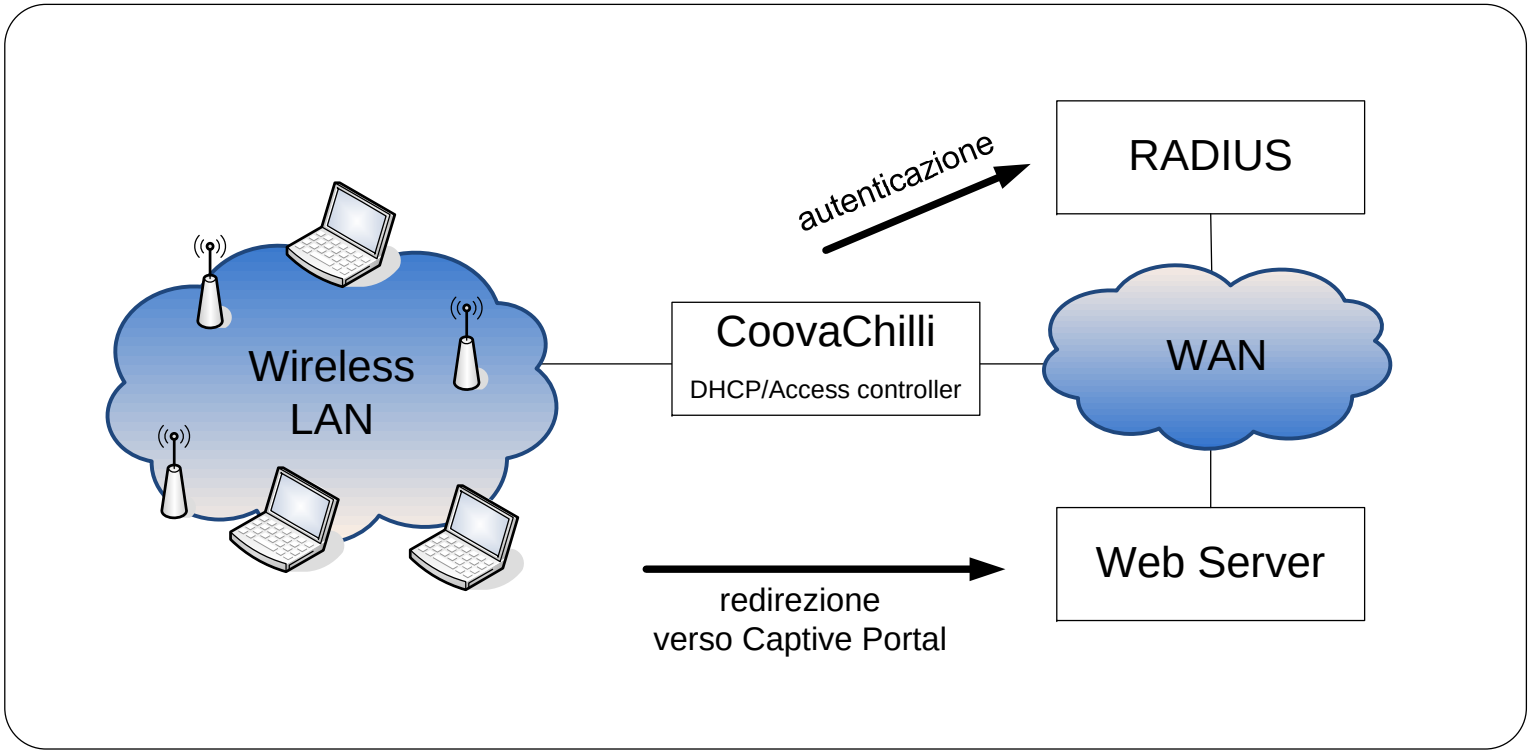
Scelta del captive portal: CoovaChilli

- Progetto basato su Chillispot, con continuo sviluppo
- Disponibile anche per sistemi embedded (CoovaAP)
- Utilizza RADIUS per l'autenticazione
- Non fa uso di iptables per la redirezione e il controllo del traffico
- Utilizza un device virtuale TUN/TAP
- Implementa al suo interno un DHCP server, utilizzato come keepalive di sessione

http://www.coova.org/

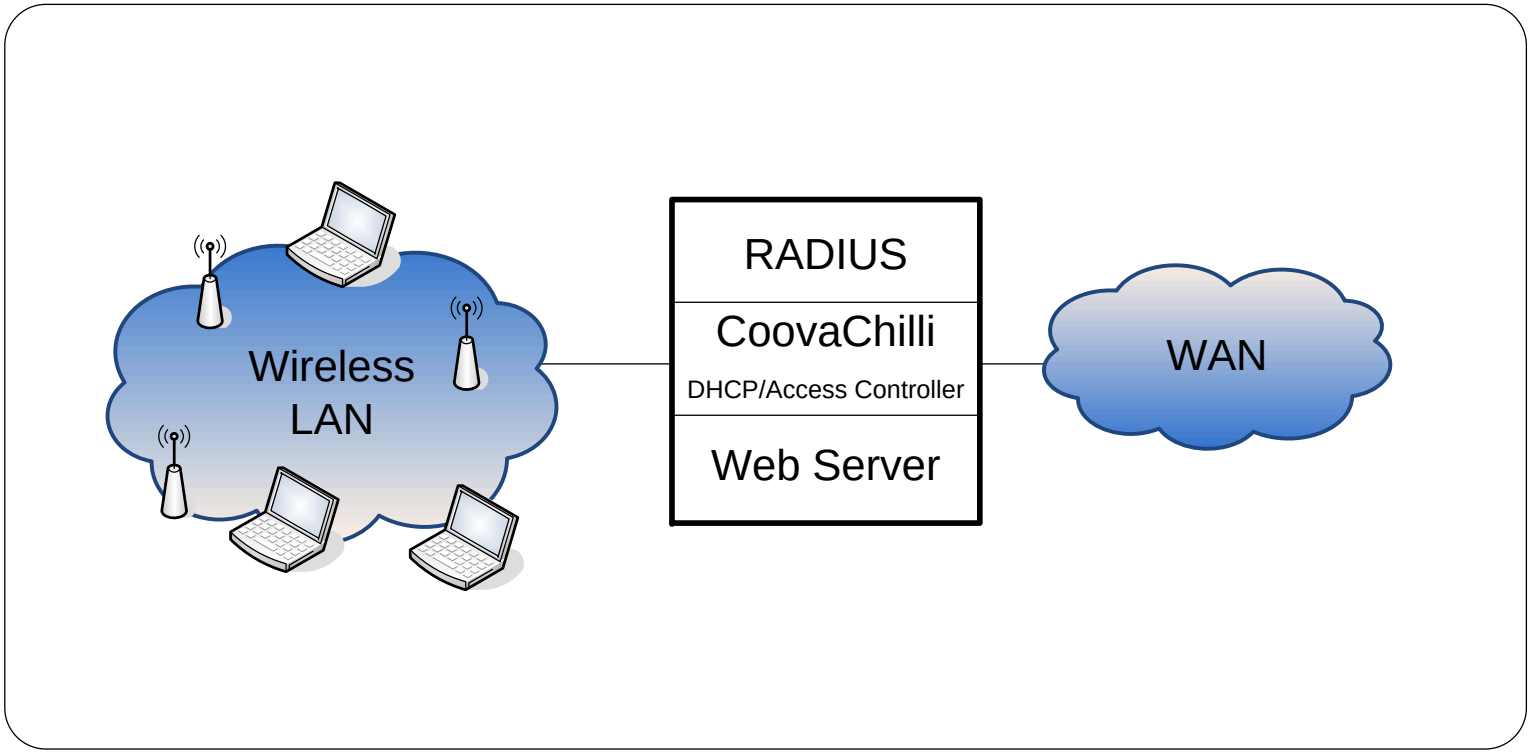
CoovaChilli

Schema di funzionamento:

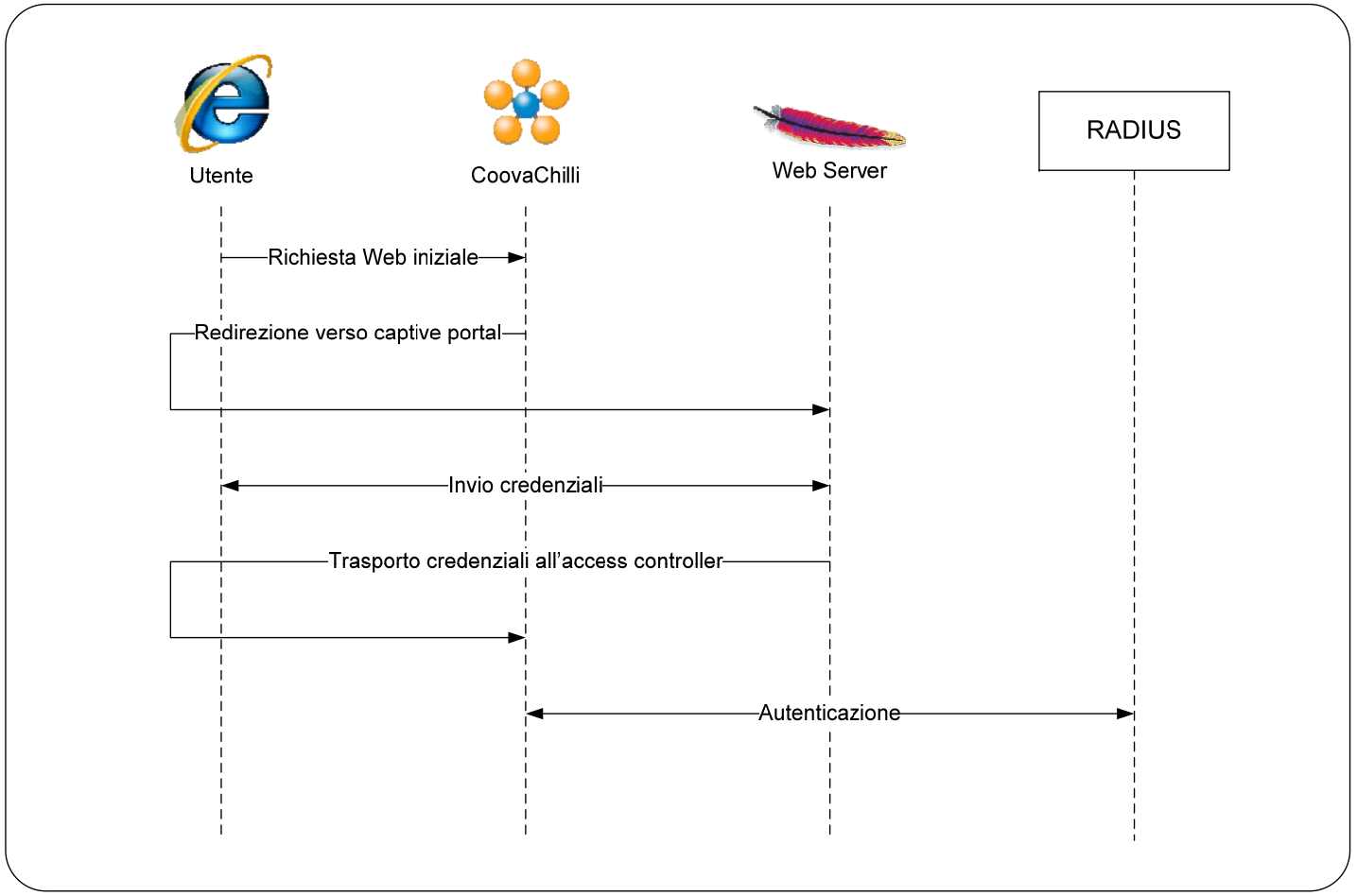


CoovaChilli

Schema di funzionamento in UNIFE:



CoovaChilli: autenticazione



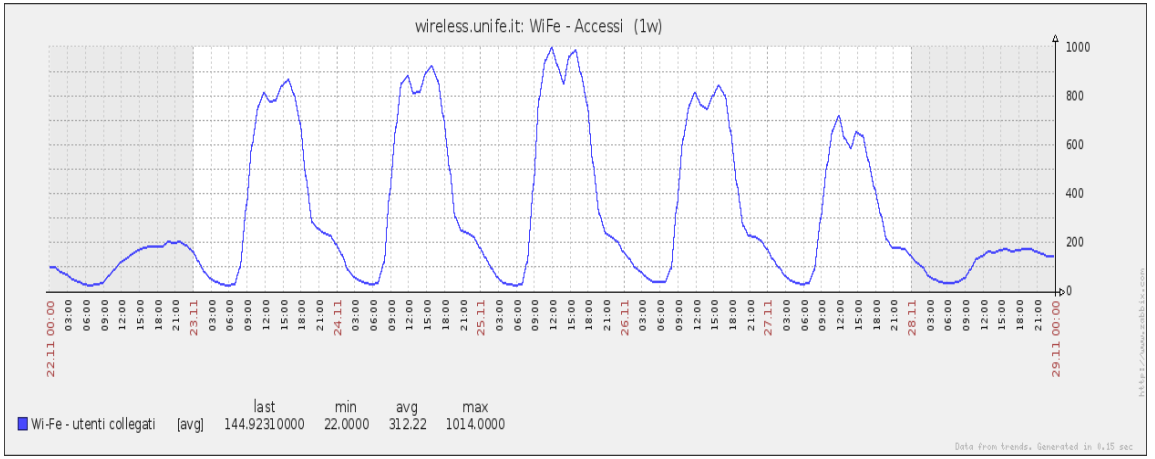
Prestazioni

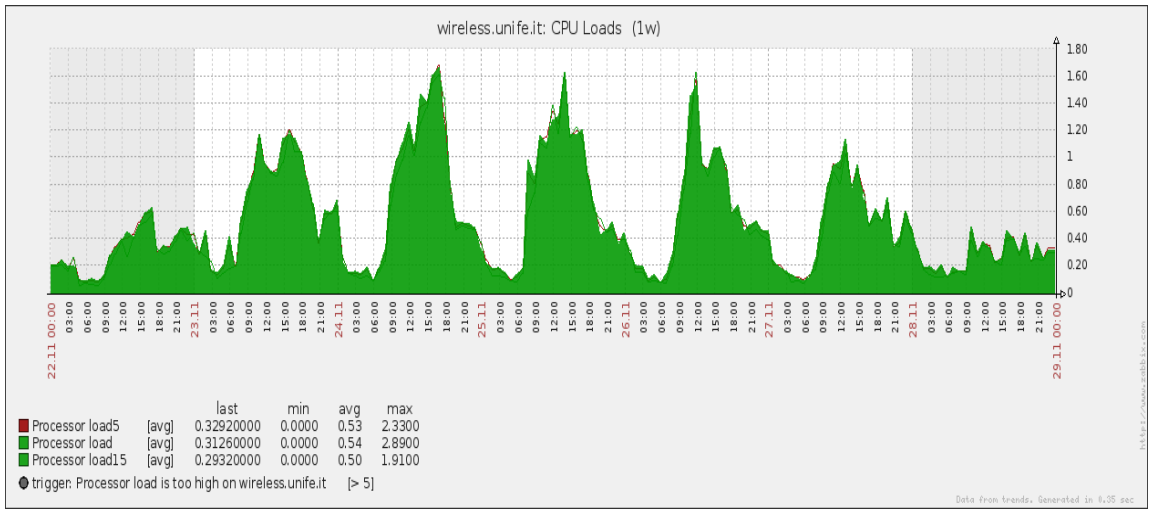
Hardware:

CPU Xeon 3.4 Ghz 2 core

RAM 2Gb

- Oltre 1000 accessi contemporanei nelle ore di picco
- Load average 0,5
- Load max < 2





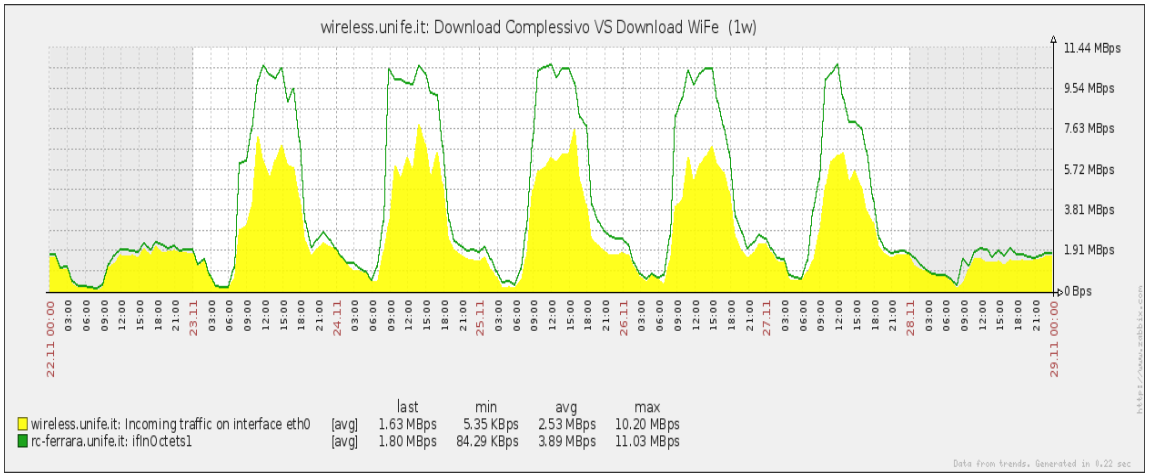
Prestazioni

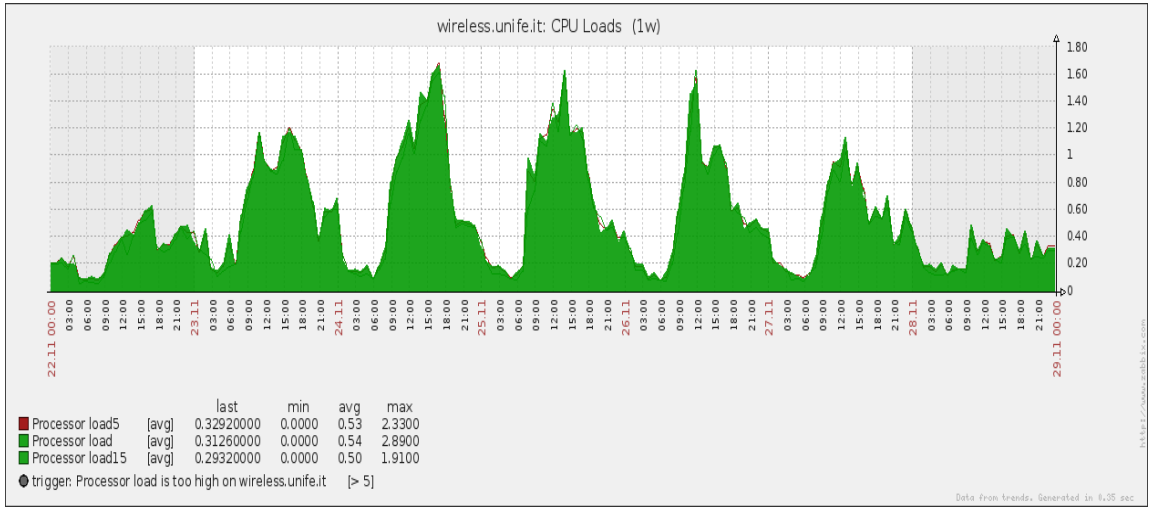
Hardware:

CPU Xeon 3.4 Ghz 2 core

RAM 2Gb

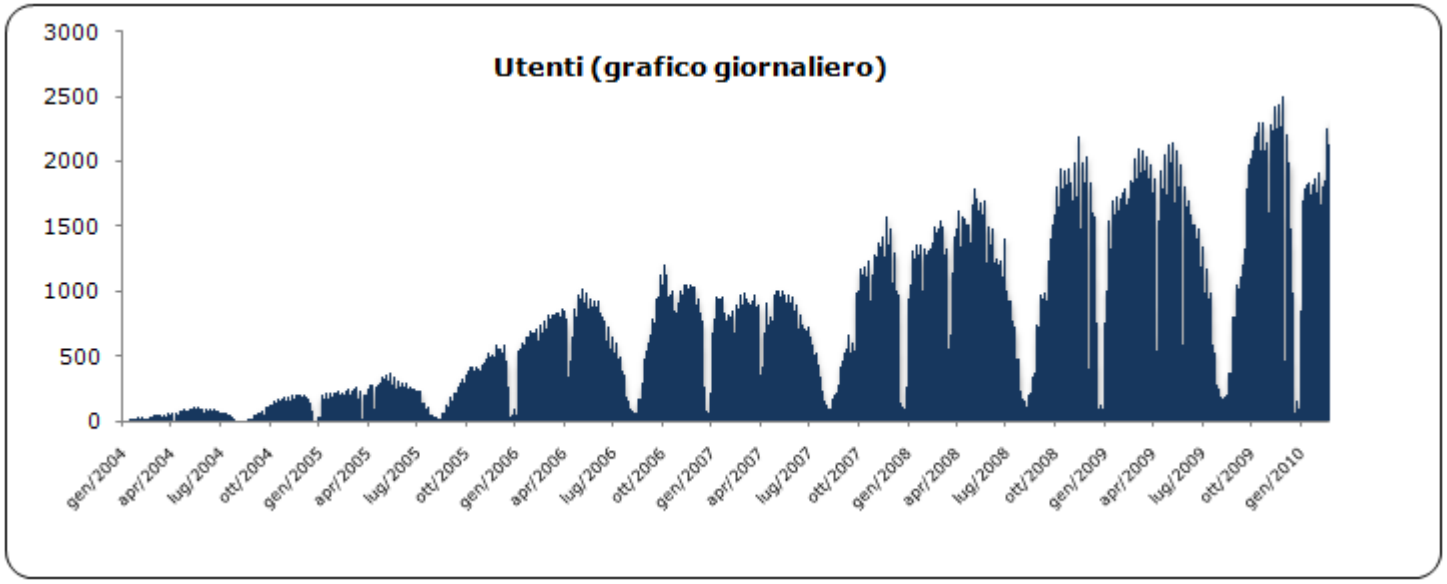
- Picchi di 60Mbps (8MByte/s)
- Il traffico di Wi-Fe rappresenta circa il 70% del traffico complessivo di Ateneo





Prestazioni

- Oltre 2500 differenti utenti utilizzano quotidianamente il sistema



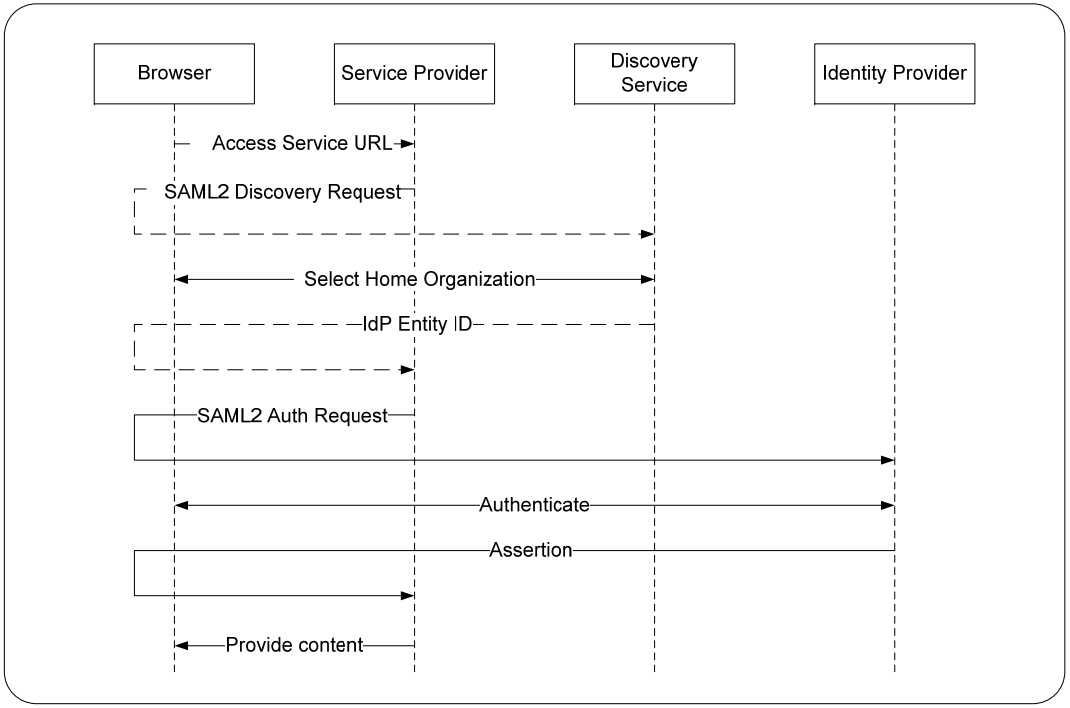
Integrazione di Wi-Fe con IDEM

Integrazione di Wi-Fe con IDEM

- Si vuole mantenere il sistema di Captive Portal in uso, per motivi di affidabilità e costi.

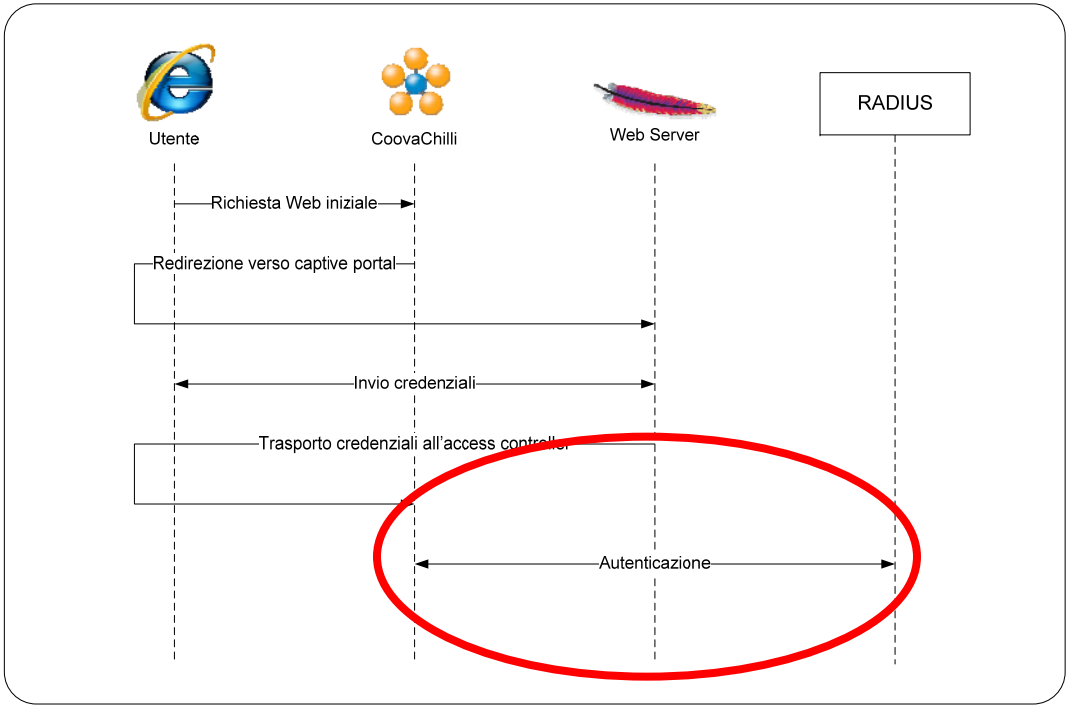
- Il sistema fa uso del protollo RADIUS e l’architettura non è compatibile con Shibboleth

Integrazione di Wi-Fe con IDEM



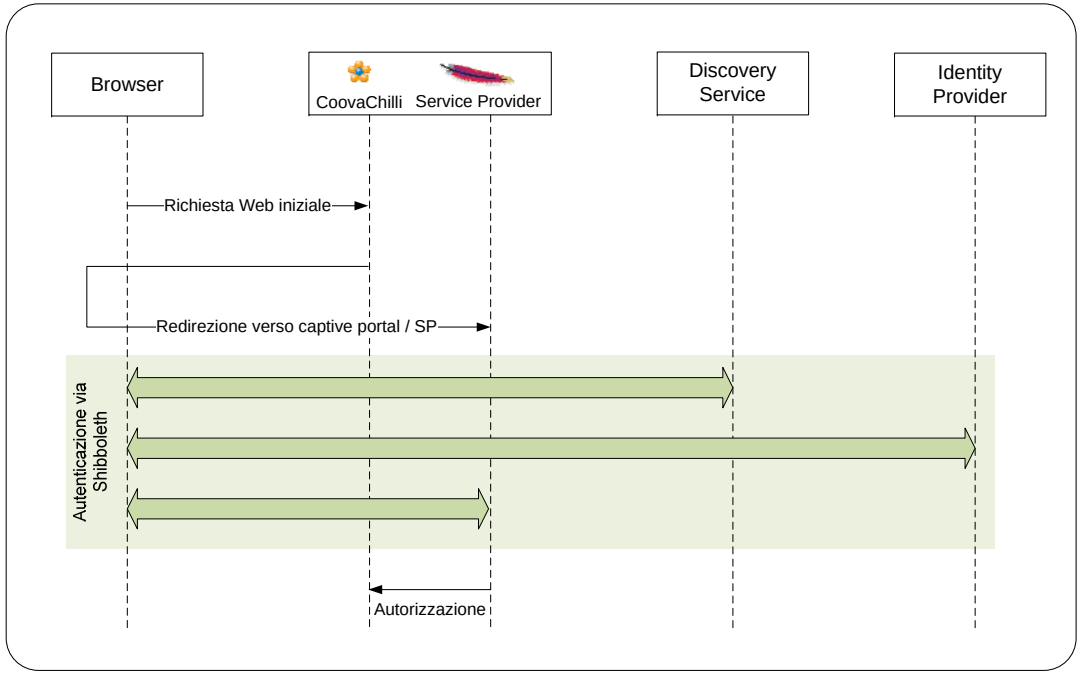
- Nell'architettura Shibboleth è l'IdP responsabile dell'autenticazione
- L'IdP comunica l'esito dell'autenticazione tramite una assertion.

Integrazione di Wi-Fe con IDEM



- Nelle applicazioni di accesso alle reti, l'autenticazione è effettuata direttamente dall'access controller (servizio)
- Manca la fase di authentication assertion

Integrazione di Wi-Fe con IDEM



- Soluzione di tipo “sistemistico”
- L’accesso alla risorsa web protetta invoca una richiesta di autorizzazione all’access controller
- E’ indispensabile che Service Provider e access controller risiedano sullo stesso server

Walled garden

- E’ necessario poter contattare gli Identity Provider senza autenticazione

- Uno script aggiorna periodicamente il walled garden di coovachilli sulla base delle informazioni nei metadati

```
1  uamallowed idp.idem.garr.it
2  uamallowed idp2.fi.infn.it
3  uamallowed sp-test.garr.it
4  uamallowed dev.garr.it
5  uamallowed idp.unica.it
6  uamallowed idp.infn.it
7  uamallowed idp.istat.it
8  uamallowed identity.unife.it
9  uamallowed idp.unimib.it
10 uamallowed idp.unitn.it
11 uamallowed idp.unipv.it
```

Autorizzazione e logging

- Accedendo alla risorsa web protetta, si autorizza l'accesso alla rete e si effettua il logging

```php
<?php
        # parametri
        $ip   = $_SERVER['REMOTE_ADDR'];
        $user = $_SERVER['eduPersonPrincipalName']

        # autorizzazione su chilli
        $homepage=shell_exec("sudo /usr/sbin/chilli_query authorize ip $ip username $user");

        # scrivo nel file di log di coovachilli
        openlog("Shibboleth-SP", LOG_CONS | LOG_NDELAY, LOG_LOCAL6);
        syslog(LOG_NOTICE, "login from username=".$user." IP=".$ip);
        closelog();
?>
<html>
        <head>
                <title>Shibboleth Service Provider, Universit&agrave; degli Studi di Ferrara - Login</title>
        </head>
              <body style="margin:0;">
               <div style="width:100%;background-color:#011845;">
                    <img src="<?php print_r('https://'.$_SERVER['HTTP_HOST']); ?>/idem/logounife.jpg" />

    ..................
```

Autorizzazione e logging

- Occorre fornire i diritti al comando che autorizza l'accesso (sudo)

```
# /etc/sudoers
#
# This file MUST be edited with the 'visudo' command as root.
#
# See the man page for details on how to write a sudoers file.
#

Defaults        env_reset

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL) ALL

# Uncomment to allow members of group sudo to not need a password
# (Note that later entries override this, so you might need to move
# it further down)
# %sudo ALL=NOPASSWD: ALL

# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL

www-data  wireless.unife.it = NOPASSWD: /usr/sbin/chilli_query list,\
                                        /usr/sbin/chilli_query authorize
```

Autorizzazione e logging

```
Mar  2 09:18:54 wireless coova-chilli[3807]: chilli.c: 2661: Client MAC=00-1C-BF-0F-09-58 assigned IP 10.14.216.158
Mar  2 09:18:55 wireless coova-chilli[3807]: chilli.c: 3050: Successful UAM login from username=[redacted] IP=10.14.214.185
[...]

Mar  2 09:47:40 wireless coova-chilli[3807]: chilli.c: 3050: Successful UAM login from username=[redacted] IP=10.14.211.139
Mar  2 09:47:41 wireless Shibboleth-SP: login from username=michele@unife.it IP=10.14.216.158
Mar  2 09:47:44 wireless coova-chilli[3807]: chilli.c: 3050: Successful UAM login from username=[redacted] IP=10.14.217.133
Mar  2 09:47:49 wireless coova-chilli[3807]: chilli.c: 3050: Successful UAM login from username=[redacted] IP=10.14.211.207
Mar  2 09:47:58 wireless coova-chilli[3807]: chilli.c: 3050: Successful UAM login from username=[redacted] IP=10.14.221.250
Mar  2 09:48:01 wireless coova-chilli[3807]: chilli.c: 2694: New DHCP request from MAC=00-1F-F3-BF-25-F6
Mar  2 09:48:01 wireless coova-chilli[3807]: chilli.c: 2661: Client MAC=00-1F-F3-BF-25-F6 assigned IP 10.14.219.106
[...]

Mar  2 09:59:31 wireless coova-chilli[3807]: chilli.c: 2661: Client MAC=00-21-FE-D1-4A-49 assigned IP 10.14.218.65
Mar  2 09:59:32 wireless Shibboleth-SP: login from username=test1@example.org IP=10.14.216.158
Mar  2 09:59:35 wireless coova-chilli[3807]: chilli.c: 3050: Successful UAM login from username=[redacted] IP=10.14.214.207
Mar  2 09:59:42 wireless coova-chilli[3807]: chilli.c: 2694: New DHCP request from MAC=34-7E-39-D6-51-97
Mar  2 09:59:42 wireless coova-chilli[3807]: chilli.c: 2661: Client MAC=34-7E-39-D6-51-97 assigned IP 10.14.223.249
Mar  2 09:59:44 wireless coova-chilli[3807]: chilli.c: 3050: Successful UAM login from username=[redacted] IP=10.14.219.200
Mar  2 09:59:48 wireless coova-chilli[3807]: chilli.c: 2694: New DHCP request from MAC=00-00-E2-68-B4-F4
```

Considerazioni finali

Considerazioni finali

- Logout?
- Collaborazione con Lepida SpA al sistema “FedERa”
- Sviluppo di CoovaChilli