Adozione open source per i servizi e la filiera applicativa LABS

Luca Ferroni <luca.ferroni@labs.it>, Luca Benassi <luca.benassi@labs.it>

Laboratori Guglielmo Marconi S.p.A.

http://www.labs.it

Agenda

- Messaggio
- Scenario
- Obiettivi
- I servizi
- La filiera applicativa
- Conclusioni

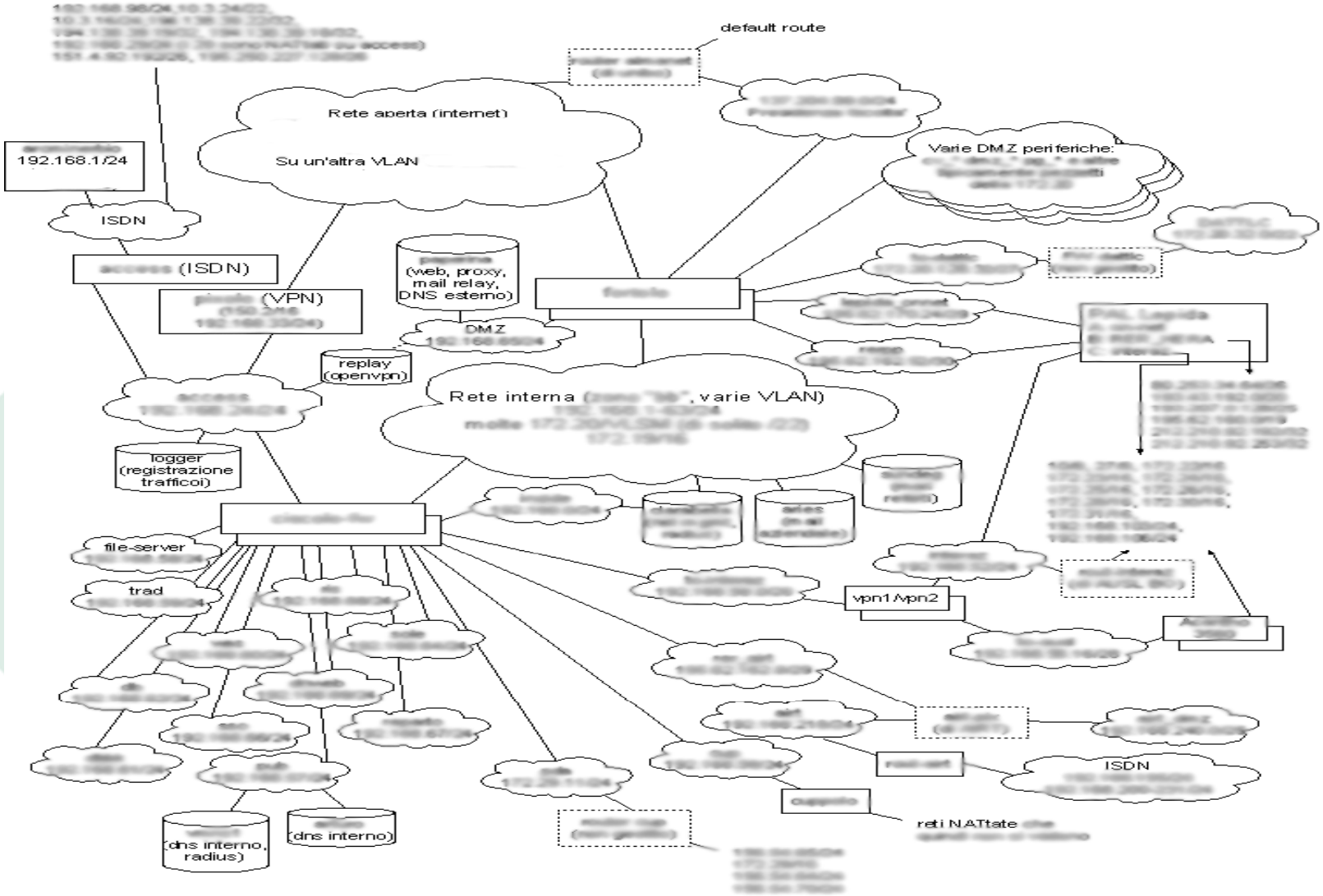
LABORATORI GUGLIELMO MARCONI

Il messaggio

Perché, quando possibile, preferiamo e consigliamo open source ai nostri clienti

LABORATORI GUGLIELMO MARCONI

Ma quale rete ?



LABORATORI GUGLIELMO MARCONI

Conoscenza

Fatti non foste a viver come bruti,
ma per seguir virtute e canoscenza

Dante Alighieri

LABORATORI GUGLIELMO MARCONI

Conoscenza (da Wikipedia)

- Consapevolezza e comprensione di
  - Fatti
  - Verità
  - Informazioni
- e loro interazioni...

LABORATORI GUGLIELMO MARCONI

Dalla conoscenza all'implementazione (1/3)



LABORATORI GUGLIELMO MARCONI

Dalla conoscenza all'implementazione (2/3)



LABORATORI
GUGLIELMO
MARCONI

E qui accade l'imprevisto: arriva un messaggio ICMP da qualcuno in transito. Osserviamo bene come e' fatto, e come puo' il kernel associarlo ad una precisa connessione TCP.

```
Frame 8 (590 bytes on wire, 590 bytes captured)
    Arrival Time: Oct  3, 2008 15:37:39.748070000
    Time delta from previous packet: 0.001211000 seconds
    Time since reference or first frame: 6.360461000 seconds
    Frame Number: 8
    Packet Length: 590 bytes
    Capture Length: 590 bytes
Ethernet II, Src: 00:50:fc:54:64:92, Dst: 00:04:76:f8:2a:21
    Destination: 00:04:76:f8:2a:21 (3Com_f8:2a:21)
    Source: 00:50:fc:54:64:92 (EdimaxTe_54:64:92)
    Type: IP (0x0800)
Internet Protocol, Src Addr:  (  ), Dst Addr:  (  )
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0xc0 (DSCP 0x30: Class Selector 6; ECN: 0
        1100 00.. = Differentiated Services Codepoint: Class Selector 6 (0x3
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 576
    Identification: 0x66cc (26316)
    Flags: 0x00
        0... = Reserved bit: Not set
        .0.. = Don't fragment: Not set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: ICMP (0x01)
    Header checksum: 0x0f27 (correct)
```




Dalla conoscenza all'implementazione (3/3)

```
#! /bin/sh /usr/share/dpatch/dpatch-run
## 40_fix_max_datasize.dpatch by Luca Ferroni <luca.ferroni@labs.it>
##
## All lines beginning with `## DP:' are a description of the patch.
## DP: Max databytes in a packet expanded to 9000 (Jumbo frame)

@DPATCH@

--- lib/Net/Ping.pm.orig    2009-04-15 02:23:48.000000000 +0000
+++ lib/Net/Ping.pm 2009-04-15 02:24:05.000000000 +0000
@@ -26,7 +26,7 @@
 $def_timeout = 5;           # Default timeout to wait for a reply
 $def_proto = "tcp";         # Default protocol to use for pinging
 $def_factor = 1.2;          # Default exponential backoff rate.
-$max_datasize = 1024;       # Maximum data bytes in a packet
+$max_datasize = 9000;       # Maximum data bytes in a packet (Jumbo frame)
 # The data we exchange with the server for the stream protocol
 $pingstring = "pingschwingping!\n";
 $source_verify = 1;         # Default is to verify source endpoint
```


LABORATORI GUGLIELMO MARCONI

Dalla conoscenza all'implementazione (schema)



LABORATORI GUGLIELMO MARCONI

E qui accade l'imprevisto: arriva un messaggio ICMP da qualcuno in transito. Osserviamo bene come e' fatto, e come puo' il kernel associarlo ad una precisa connessione TCP.

```
Frame 8 (590 bytes on wire, 590 bytes captured)
    Arrival Time: Oct  3, 2008 15:37:39.748070000
    Time delta from previous packet: 0.001211000 seconds
    Time since reference or first frame: 6.360461000 seconds
    Frame Number: 8
    Packet Length: 590 bytes
    Capture Length: 590 bytes
Ethernet II, Src: [illegible], Dst: [illegible]
    Destination: [illegible]
    Source: [illegible]
    Type: IP (0x0800)
Internet Protocol, Src Addr: [illegible], Dst Addr: [illegible]
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0xc0 (DSCP 0x30: Class Selector 6; ECN: 0
        1100 00.. = Differentiated Services Codepoint: Class Selector 6 (0x3
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 576
    Identification: 0x66cc (26316)
    Flags: 0x00
        0... = Reserved bit: Not set
        .0.. = Don't fragment: Not set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: ICMP (0x01)
    Header checksum: 0x0f27 (correct)
```

Perché non riesco ad inviare pacchetti IP che riempiono la MTU del mezzo fisico ?

```
#! /bin/sh /usr/share/dpatch/dpatch-run
## 40_fix_max_datasize.dpatch by Luca Ferroni <luca.ferroni@labs.it>
##
## All lines beginning with `## DP:' are a description of the patch.
## DP: Max databytes in a packet expanded to 9000 (Jumbo frame)

@DPATCH@

--- lib/Net/Ping.pm.orig    2009-04-15 02:23:48.000000000 +0000
+++ lib/Net/Ping.pm 2009-04-15 02:24:05.000000000 +0000
@@ -26,7 +26,7 @@
 $def_timeout = 5;           # Default timeout to wait for a reply
 $def_proto = "tcp";         # Default protocol to use for pinging
 $def_factor = 1.2;          # Default exponential backoff rate.
-$max_datasize = 1024;       # Maximum data bytes in a packet
+$max_datasize = 9000;       # Maximum data bytes in a packet (Jumbo frame)
 # The data we exchange with the server for the stream protocol
 $pingstring = "pingschwingping!\n";
 $source_verify = 1;         # Default is to verify source endpoint
```


LABORATORI GUGLIELMO MARCONI

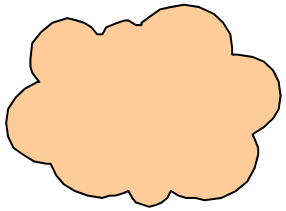
Implementazione

Il cliente sta alla società di consulenza

come

la società di consulenza sta al proprio fornitore

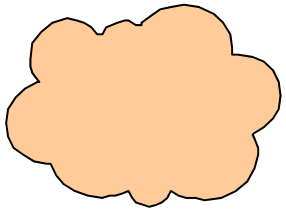
LABORATORI GUGLIELMO MARCONI



Panoramica dei servizi (1 di 2)

- Gestione indirizzi IP (dhcpd, bind9)
- Routing (quagga)
- Firewall (iptables, ebtables)
- Web (apache, squid)
- Mail (qmail, postfix, horde, spamassassin, clamav, amavis)
- VPN (openvpn, strongswan)

LABORATORI GUGLIELMO MARCONI



Panoramica dei servizi (2 di 2)

- Monitoraggio (SANET)
- Auditing and security (tcpdump, wireshark, tethereal, iperf, kismet, snort, ntop, nmap)
- Captive portal (chillispot)
- Storicizzazione configurazioni (rancid)

LABORATORI GUGLIELMO MARCONI

Gestione indirizzi IP

- DHCP con dhcpd
  - Relay
  - Configurazione Ip statici
- DNS con bind9
  - Domain maintainer: DNS autoritativo

LABORATORI GUGLIELMO MARCONI

Firewall con iptables

- Esigenze
  - 3 linee Internet (di cui una di backup)
  - Instradare il traffico interno sulle linee a seconda di una politica definita
  - Gestione linea di backup
- Soluzione
  - Applicare il policy routing al traffico entrante
  - Instradare i pacchetti marcati
  - Scripting per la linea di backup

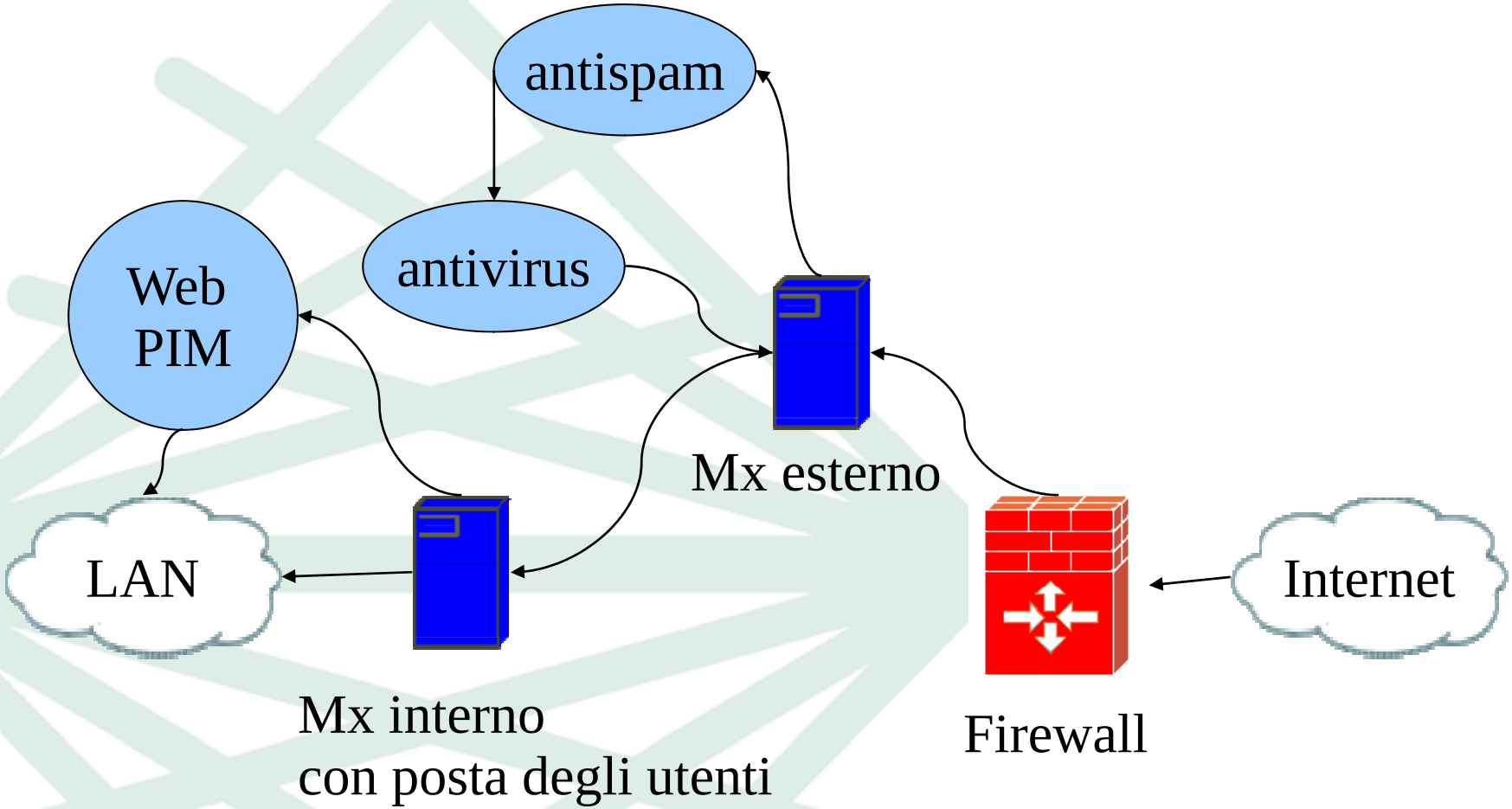
LABORATORI GUGLIELMO MARCONI

Proxy con Squid

- Esigenze
  - Gestire l'accesso web per migliaia di client
  - Autenticazione NTLM su Active Directory
  - Politiche specifiche per
    - Indirizzo sorgente / destinazione
    - Url di destinazione
- Soluzione
  - Proxy con squid
  - Script per la configurazione automatica
  - Patch per cache indirizzo IP su autenticazione NTLM
  - squidGuard

LABORATORI GUGLIELMO MARCONI

Servizio mail



LABORATORI GUGLIELMO MARCONI

Quando lo strumento non centra l'obiettivo...

Entra in gioco NAD

Networking Application Division

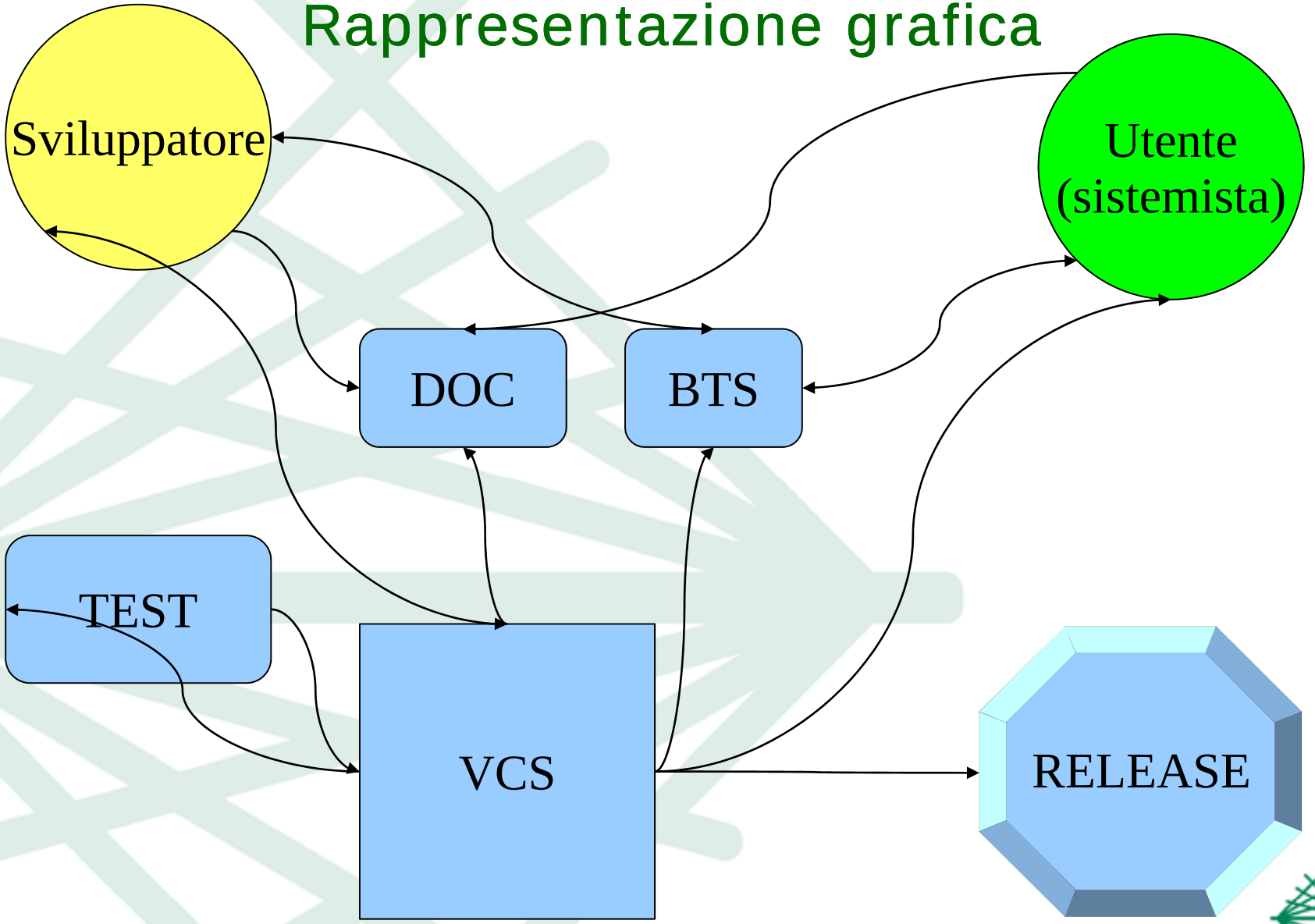
LABORATORI GUGLIELMO MARCONI

La filiera applicativa LABS

- Realizzata con strumenti Open Source
  - Sistema di versionamento (VCS)
  - Sistema di tracciamento bug (BTS)
  - Literate programming (DOC)
  - Test continui (TEST)
  - Distribuzione del software (RELEASE)
  - Pianificazione funzionalità e rilasci (PLAN)
  - Collante collaborativo (GLUE)

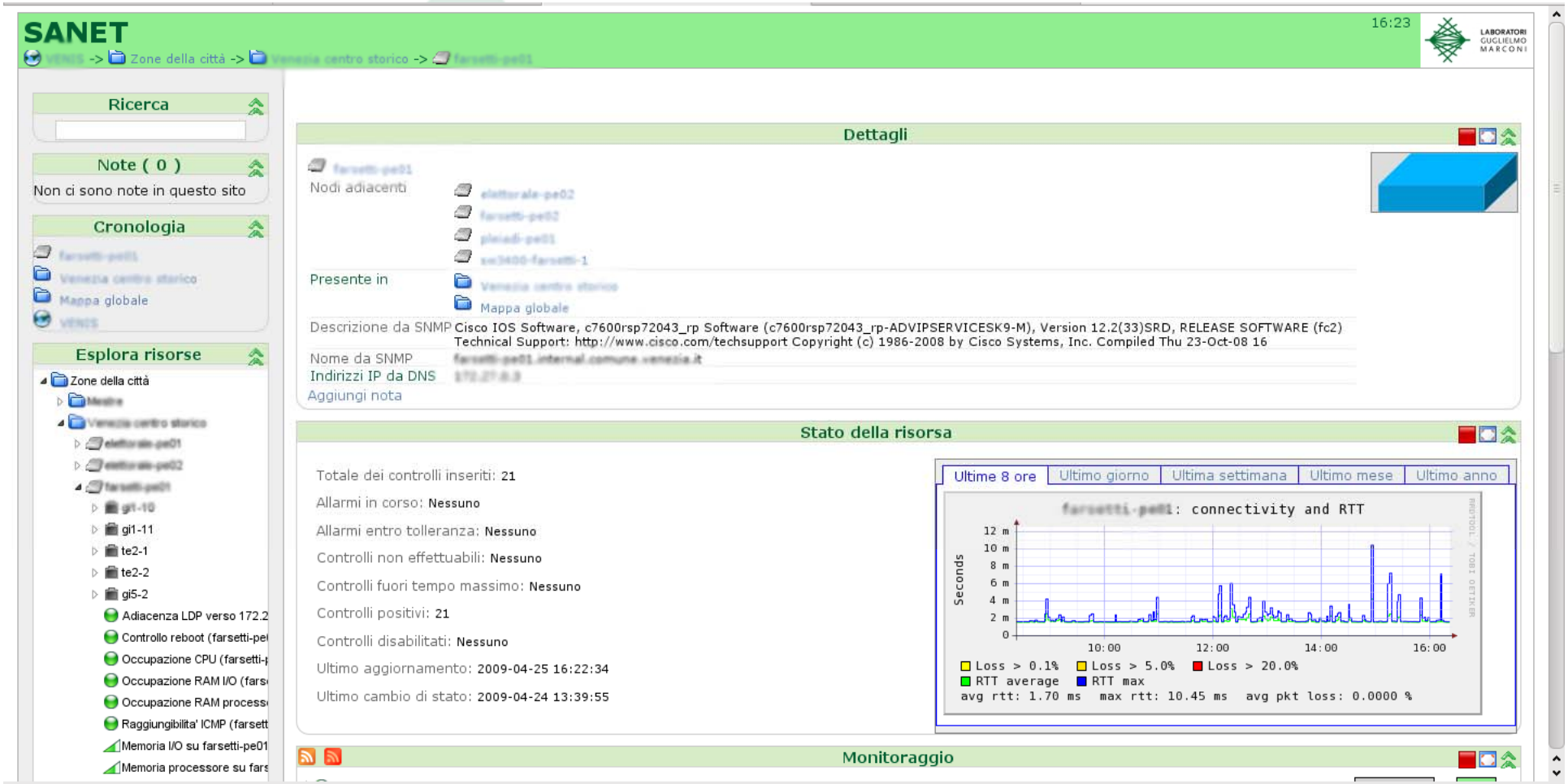
LABORATORI GUGLIELMO MARCONI

Rappresentazione grafica

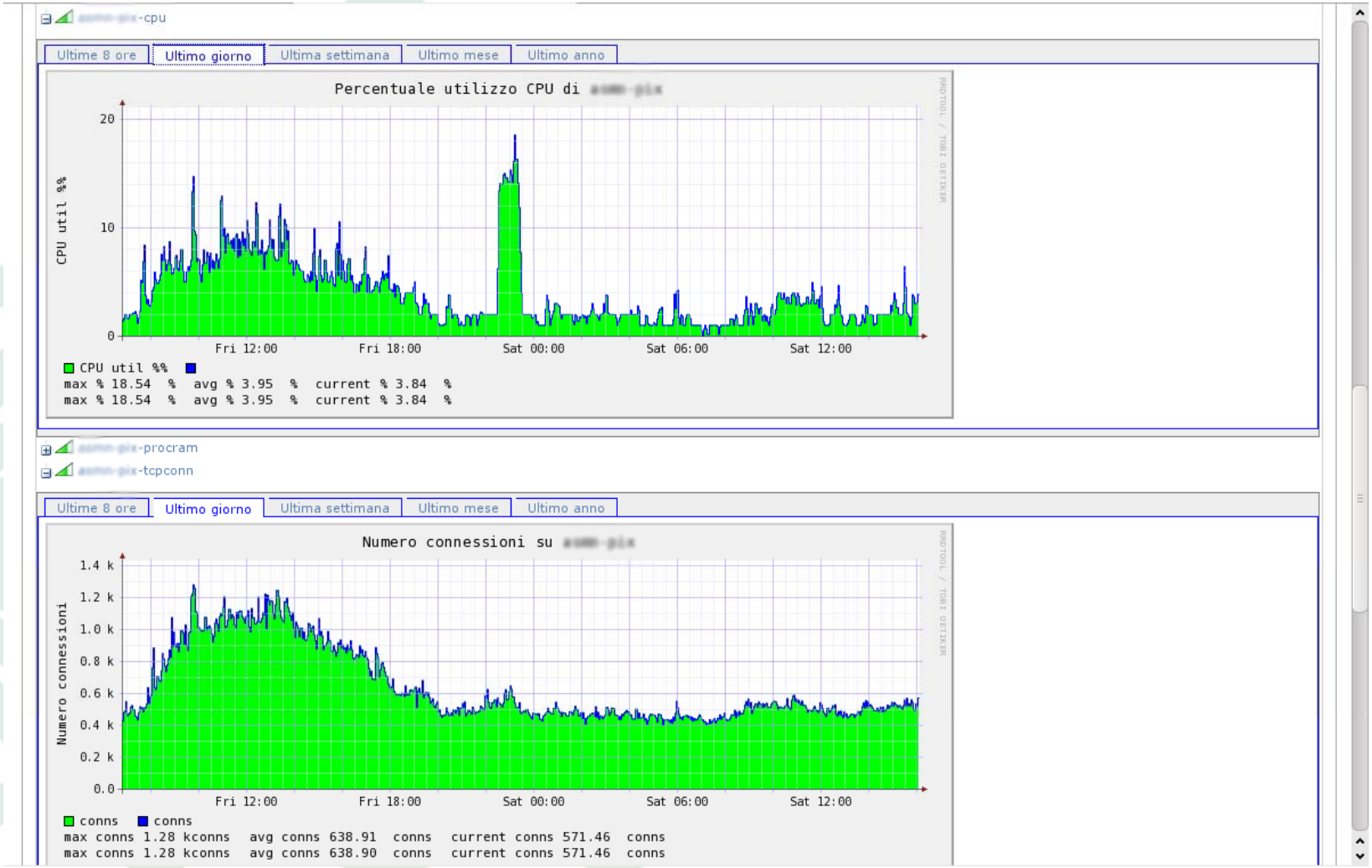


LABORATORI GUGLIELMO MARCONI

SANET (1/3)

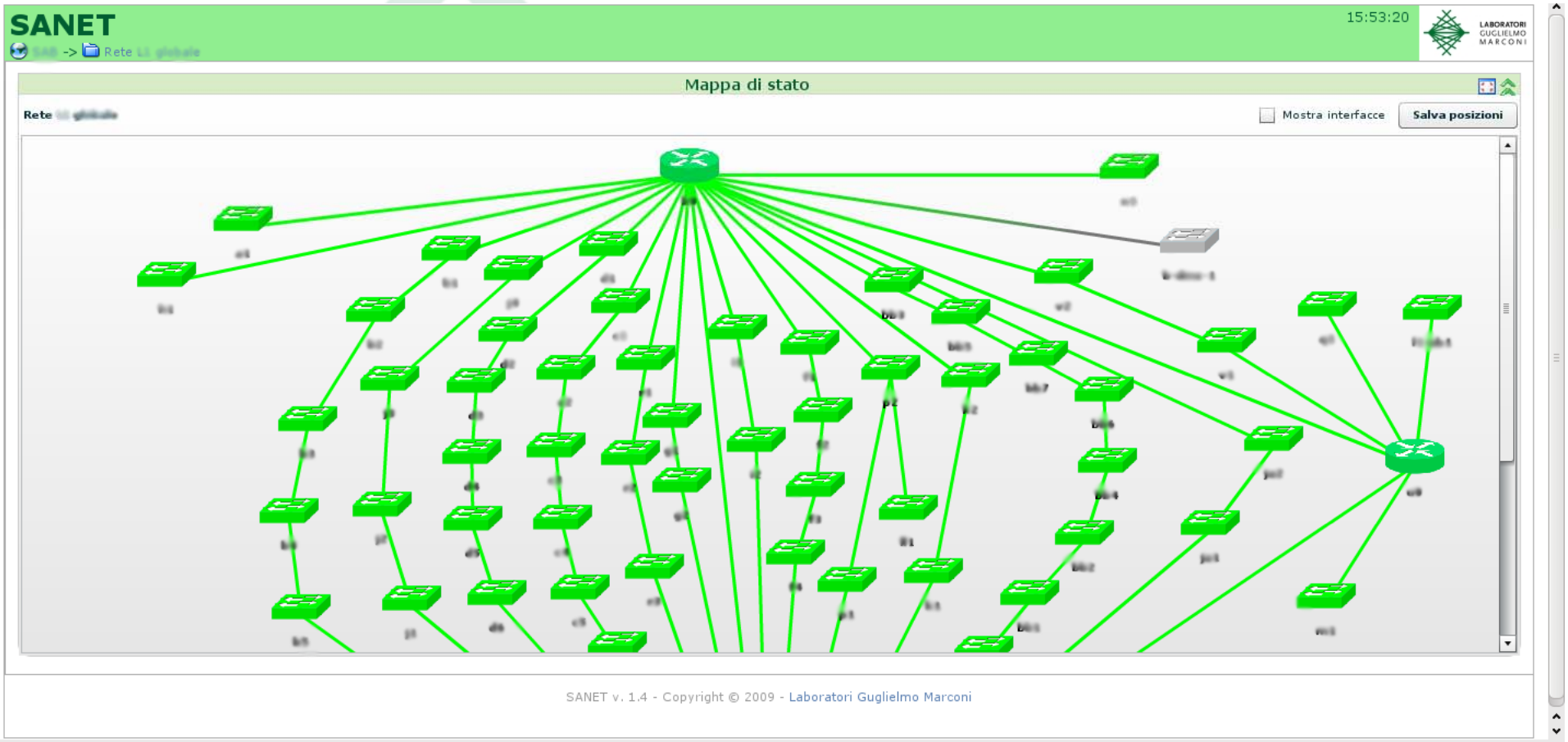

SANET
16:23
Zone della città
Ricerca
Note (0)
Non ci sono note in questo sito
Cronologia
Mappa globale
Esplora risorse
Zone della città
Dettagli
Nodi adiacenti
Presente in
Mappa globale
Descrizione da SNMP
Cisco IOS Software, c7600rsp72043_rp Software (c7600rsp72043_rp-ADVIPSERVICESK9-M), Version 12.2(33)SRD, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2008 by Cisco Systems, Inc. Compiled Thu 23-Oct-08 16
Nome da SNMP
Indirizzi IP da DNS
Aggiungi nota
Stato della risorsa
Totale dei controlli inseriti: 21
Allarmi in corso: Nessuno
Allarmi entro tolleranza: Nessuno
Controlli non effettuabili: Nessuno
Controlli fuori tempo massimo: Nessuno
Controlli positivi: 21
Controlli disabilitati: Nessuno
Ultimo aggiornamento: 2009-04-25 16:22:34
Ultimo cambio di stato: 2009-04-24 13:39:55
Ultime 8 ore
Ultimo giorno
Ultima settimana
Ultimo mese
Ultimo anno
: connectivity and RTT
Seconds
12 m
10 m
8 m
6 m
4 m
2 m
0
10:00
12:00
14:00
16:00
Loss > 0.1%
Loss > 5.0%
Loss > 20.0%
RTT average
RTT max
avg rtt: 1.70 ms
max rtt: 10.45 ms
avg pkt loss: 0.0000 %
Monitoraggio
Completato

SANET (2/3)

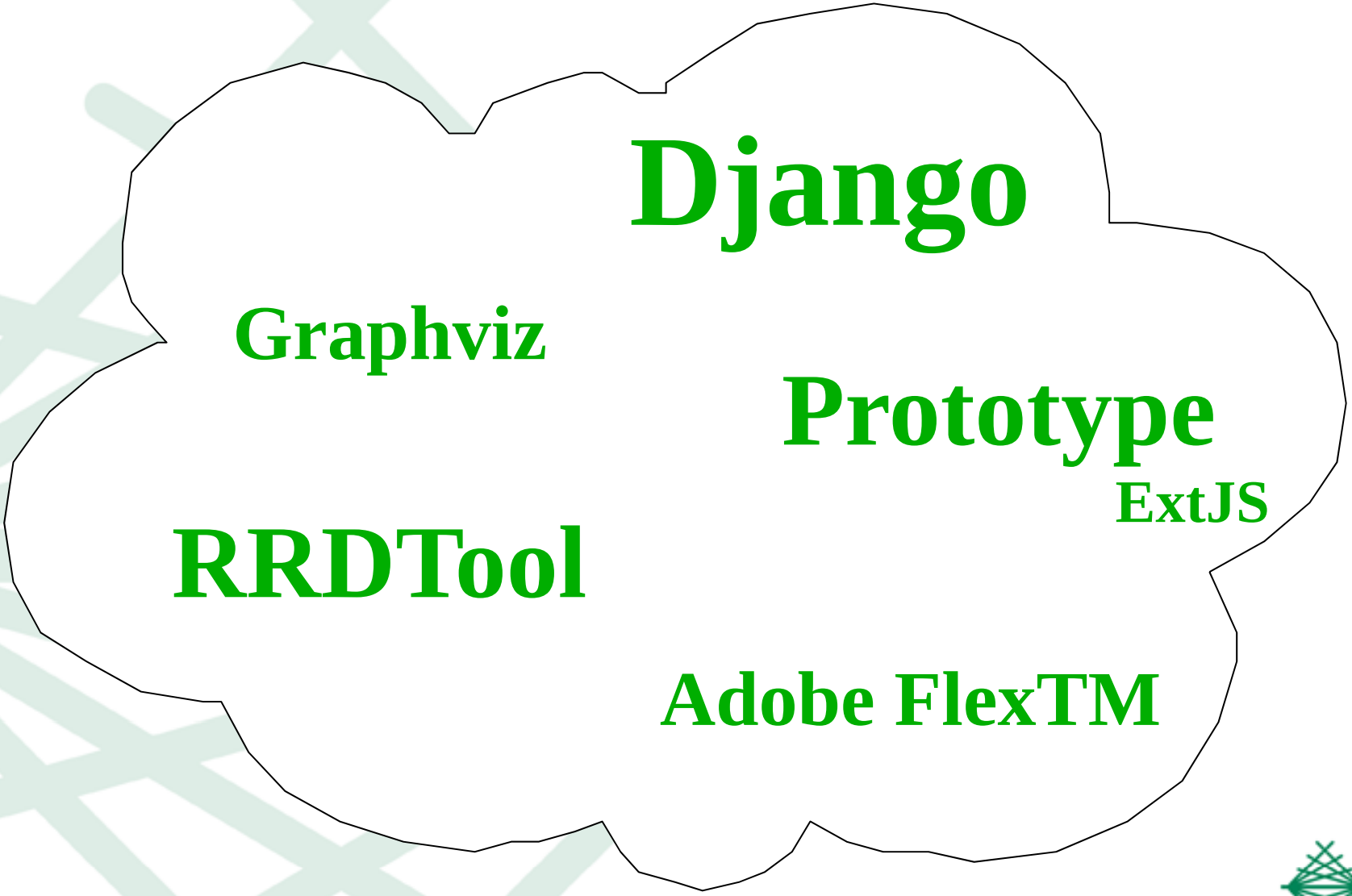


LABORATORI GUGLIELMO MARCONI

SANET (3/3)


SANET
15:53:20
Mappa di stato
Mostra interfacce
Salva posizioni
SANET v. 1.4 - Copyright © 2009 - Laboratori Guglielmo Marconi
Completato

SANET è



LABORATORI GUGLIELMO MARCONI

Giusto per chiarire...

LABS offre servizi di consulenza, assistenza e reperibilità per le reti

SANET è uno strumento ad uso interno, rilasciato con licenza Open Source AGPL v3 affinché la comunità benefici dei risultati ottenuti

disponibile online
http://sanet.sourceforge.net

LABORATORI GUGLIELMO MARCONI

Concludendo

- Preferenza open source per
  - Completa comprensione e formazione
  - Personalizzazione peculiare
  - Interfaccia diretta con il problema
  - Riduzione tempi di attesa
- Vale a dire per
  - Conoscere
  - Implementare
  - Monitorare
  - Reagire

LABORATORI GUGLIELMO MARCONI

Un compito importante

Garantire la soddisfazione del cliente

LABORATORI GUGLIELMO MARCONI