smau 2009

Implementazione della Sicurezza Perimetrale e del Networking Geografico Attraverso Soluzioni Open Source

Un Caso di Successo

Fondazione CNR / Regione Toscana Gabriele Monasterio

Giuseppe Augiero – Alessandro Mazzarisi

aipsi

Agenda

Questa presentazione offrirà una visione sinottica dell'attività del gruppo reti e ICT della nostra azienda che ci ha visto impegnati **nell'analisi**, la **progettazione** e il **deploy** del nuovo layout della rete clinica aziendale, **guidato** da un approccio di business in un contesto di evoluzione da uno scenario accademico ad uno scenario tipico della sanità e della P.A. in genere.

I due approcci di Business e Tecnologico vi verranno presentati in due sessioni separate .

- Approccio Business
- Approccio Tecnologico

APPROCCIO DI BUSINESS

Fondazione Toscana Gabriele Monasterio

Le nostre cinque W inglesi

- **Chi siamo**
  - CNR-IFC
  - Regione Toscana
  - Università Pi-Si-Fi
- **Cosa facciamo**
  - Sviluppo Assistenza Sanitaria Specialistica
  - Incubatore Tecnologico ICT per la Sanità
  - Ricerca di base in collaborazione con IFC-CNR

Adult & elderly cardiology & cardiac surgery

Pediatric & GUCH cardiologist & cardiac surgery

Adult & pediatric interventional cardiology

Imaging (CT, PET, NM. EM, Echo...)

Prenatal & cardiovascular neonatology

Fondazione Toscana Gabriele Monasterio

Le nostre cinque W inglesi

- **Quando nasce la FTGM**
  - Novembre 2007
    - Parte a carattere Privatistico
    - Ora Costola della Sanità Pubblica della Reg. Toscana
- **Dove opera**
  - Area della Ricerca del CNR di Pisa e presso l'Ospedale Pasquinucci di Massa

Eredita obblighi e doveri, strutture e requisiti richiesti alla Pubblica Amministrazione

Dal contesto accademico ad un contesto di bussines - (il Servizio Sanitario Nazionale e la P.A.)

Perché oggi siamo qui

Parti attive di uno switch di contesto da un ambito accademico ad un contesto di business, interessante anche per molti altri soggetti che come noi hanno competenze nel campo delle tecnologie ICT e nell'area OPEN.

Come affrontare lo switch tecnologico

•Metodi e strumenti appropriati per passare da un contesto accademico ad un contesto di business

Coinvolgimento del management aziendale

valutazione di temi propri della P.A. quali:

- Uso di tecnologie Open Source
- Riuso del software
- Necessità di competenze di alto profilo
- Costi di investimento infrastrutturale e tecnologico
- Risorse umane

Obiettivi Aziendali che hanno guidato il passaggio da ente accademico a P.A.

- Mantenere nel tempo la conformità dell'azienda a leggi e regolamenti
- Raggiungere un rapido ritorno degli investimenti tecnologici e infrastrutturali
- Partecipare con i risultati ottenuti al supporto all'innovazione

Soddisfare le esigenze di business, ha perciò richiesto di andare a gestire il rischio legato al cambiamento in maniera efficace andando a preservare e aumentare il valore dell'Azienda.

L'ipotesi Open Source per la FTGM

L'ipotesi sostenuta dal management

"la trasformazione delle infrastrutture ICT da ente accademico a ente sanitario inserito in un organizzazione complessa, già in corsa da anni, doveva essere fatta per passi, con strumenti flessibili"

Obiettivo finale

"il consolidamento della struttura ICT basata sulle regole dalla nuova organizzazione di appartenenza"

Consolidamento dell'infrastruttura ICT

L'ipotesi Open Source per la FTGM

Progettazione, scelte iniziali e proposta di soluzioni O.S.

Per arrivare all'implementazione della sicurezza perimetrale e del networking geografico attraverso soluzioni Open Source è stato necessario un approccio strategico connesso al contesto di business nel quale opera la FTGM e che riguarda sia la sicurezza logica che la sicurezza fisica per tutti gli aspetti **tipici** e **non** delle aziende sanitarie

Contesto di business

- L'erogazione di servizi sanitari
- La ricerca
- L'innovazione Tecnologica
- Il pareggio del Bilancio
- L'attrazione di finanziamenti
- La gestione delle Risorse Umane

L'ipotesi Open Source per la FTGM

Gestione del rischio

Nella ristrutturazione dell'infrastruttura ICT è stato necessario andare ad adottare soluzioni per evitare che si interrompessero i servizi di business arrecando danni materiali, economici e di reputazione dell'azienda.

Aree a rischio per il contesto della Sanità Pubblica

Aree a rischio

- Accettazione e sistemi di prenotazione
- Attività degli sportelli al pubblico
- Erogazione di cure appropriate al paziente (cartelle cliniche, registri, protocolli…)
- Connettività in tra ed inter-aziendale
- Connettività verso sistemi di governo centrale
- Connettività verso i fornitori di servizi
- Servizi per l'informazione al pubblico
- Servizi per la formazione del personale

Open Source precursore per le infrastrutture HW e SW commerciali

Perché scegliere di promuovere internamente con proprie risorse l'approccio O.S.

Analisi, progettazione, testing, deploy di sistemi complessi in alta affidabilità con personale interno

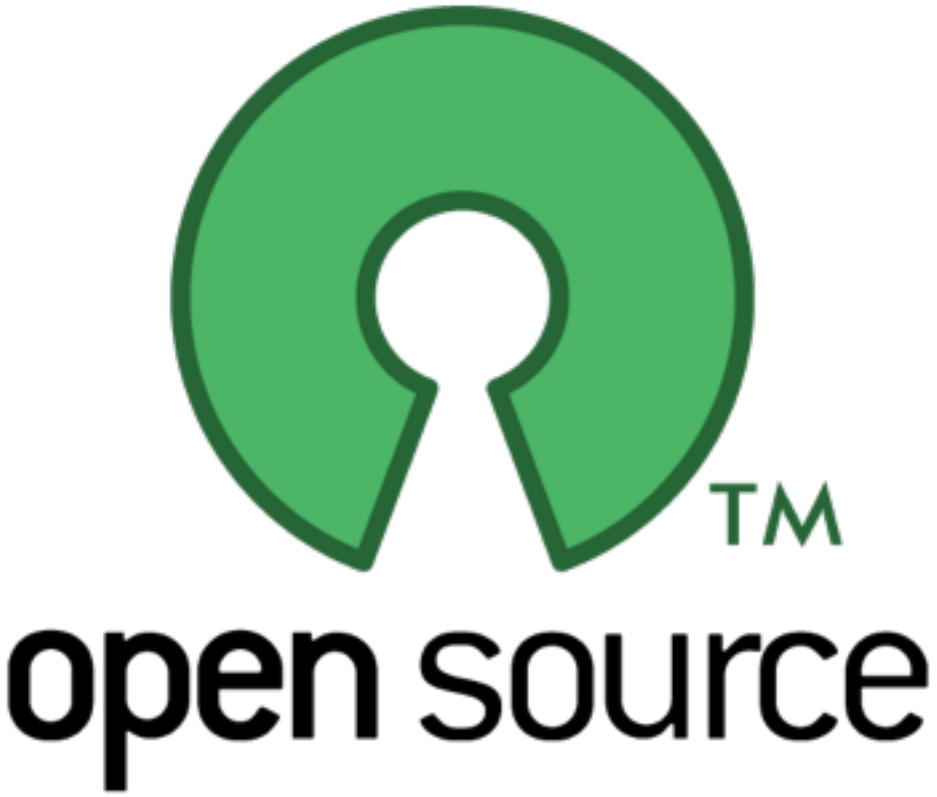
Il raggiungimento dell'obiettivo di un approccio integrato alla sicurezza, passa attraverso la conoscenza di dettaglio delle specificità che l'area ICT ha sviluppato negli anni.

Approccio Open con Risorse interne, un'esigenza facilmente riscontrabile in realtà istituzionali che hanno la necessità di cambiare

Open Source precursore per le infrastrutture HW e SW commerciali

La scelta iniziale

L'approccio concordato si è basato sulla scelta iniziale di utilizzare un design dell'infrastruttura di rete canonica, sia a livello geografico sul territorio che di singolo presidio, tecnologie Open Source applicate ad Hardware di alto livello e strumenti di analisi e gestione dell'l'infrastruttura ICT, conformi ai protocolli e gli standard industriali correntemente in uso.



Open Source precursore per le infrastrutture HW e SW commerciali

Pro

- ***Investimento iniziale economicamente vantaggioso***

Contro

- ***Costi di gestione da valutare con un approccio di business***

Dopo la fase di consolidamento, questo modello organizzativo permetterà di andare a valutare le tecnologie adottate in relazione ai prodotti commerciali, qualora si intendano effettuare economie di scala, gestibili con tradizionali contratti di manutenzione, in regime di libera concorrenza.

Open Source precursore per le infrastrutture HW e SW commerciali

La logica di questa tecnologia e filosofia di approccio ai problemi **è** che le competenze richieste per andare a gestire progetti di una certa consistenza, sono ormai facilmente reperibili in rete, scegliendo i prodotti in base al rischio di impresa che si intende accettare.

Prodotti e risorse Open Source

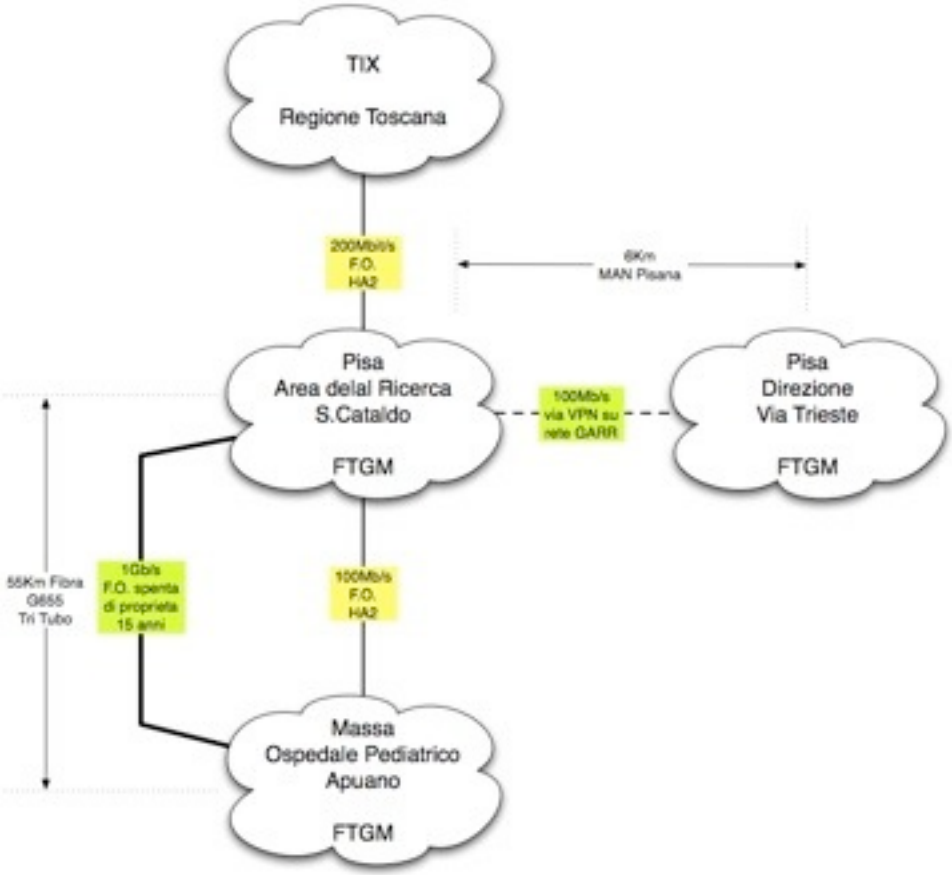
- parti e progetti stabili e consolidati
- progetti con una vasta comunità alle spalle
- progetti innovativi in base a livello di skill dello staff tecnico reperibile all'interno dell'organizzazione

Persone con competenze specifiche nel campo dell'Open Source, largamente presenti ad esempio nella P.A., sono un esempio di risorse che è possibile aggregare a livello di "consorzi aziendali" .

Obiettivi di business: risultati dell'analisi

Ottimizzazione del traffico di rete in relazione alla tipologia del servizio richiesto: clinico e da e verso internet (Traffic Engineering), andando ad utilizzare contemporaneamente le due connessioni a 100MBit/sec e 200MBit/sec offerte da RTRT per collegare Massa a Pisa e il link ad 1GB/sec in funzione della tipologia del traffico da veicolare:

- Diagnostica per immagini PACS
- Servizi Multimediali
- Sperimentazioni ICT e ricerca di base



Obiettivi di business: risultati dell'analisi

Riconfigurazione automatica dei percorsi di instradamento delle comunicazioni digitali tra i tre presidi, indipendentemente dallo stato delle linee offerte dagli operatori pubblici senza perdita di connessione da parte degli applicativi e senza interruzione delle attività di servizio (completa trasparenza all'utente finale).

Situazioni da evitare

Interruzione dei servizi di business

- danni materiali,
- danni economici
- danni di reputazione

Obiettivi di business: risultati

Architettura del sistema di instradamento scalabile a piacere per esigenze future, realizzato con tecnologie Open Source, riutilizzabile in ambito pubblico e di ricerca con costi iniziali estremamente contenuti.

Realizzazione di un sistema in grado di offrire un servizio continuo ad alta affidabilità che garantisse in automatico senza interruzioni di servizio, il corretto funzionamento di ciascun punto di fallimento dell'architettura.

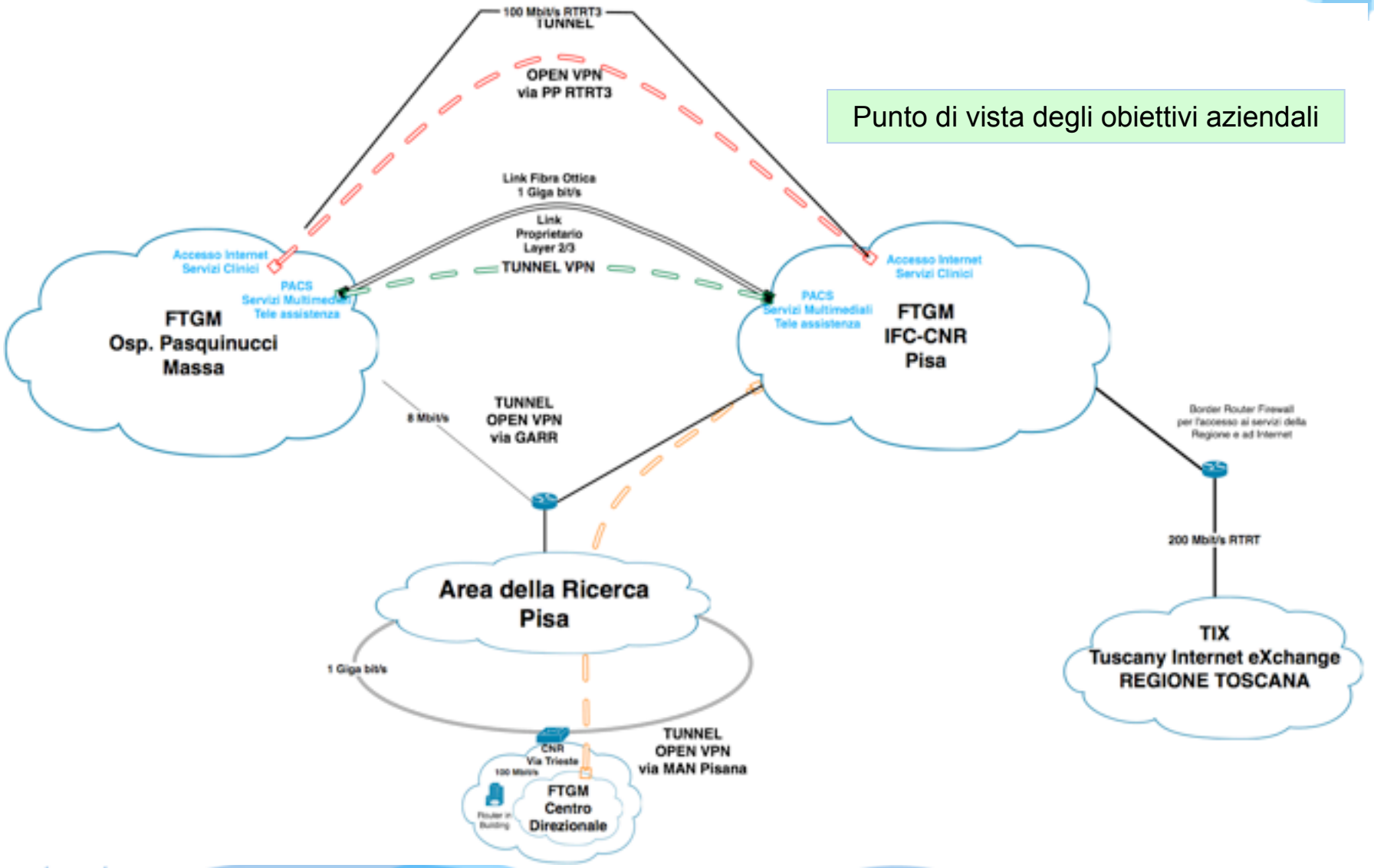
Obiettivi di business: risultati

Realizzazione di una infrastruttura di trasporto su rete geografica pubblica, adeguata per il transito di informazioni cliniche e dati sensibili, mediante Reti Virtuali Private

Realizzazione di una rete integrata tra le aree di ricerca (IFC-CNR) e di servizio (FTGM-RTRT) comunicante in modo trasparente all'interno dei singoli presidi, rispettando le peculiarità reciproche delle due organizzazioni rispettando i vincoli di sicurezza imposti dal sistema pubblico di connettività

CNIPA
Centro Nazionale per l'Informatica nella Pubblica Amministrazione

Schema di partenza dell'infrastruttura di rete



Punto di vista degli obiettivi aziendali

APPROCCIO TECNOLOGICO

Internet Open Environment

Le tecnologie legate ad Internet sono state sviluppate in maniera aperta.

Tutti protocolli e le architetture di questo mondo sono pubblicamente descritti e accessibili a tutti.

Chiunque può facilmente sviluppare una soluzione (hw o sw) da utilizzare in rete o adatta a sviluppare la rete.

E' possibile creare un "open router".

Think Different

In un ambiente sperimentale e sempre in fase di crescita come Internet è possibile individuare contesti eterogenei che hanno trovato soluzioni diverse per le proprie necessità.

La comunità scientifica ha spesso, a causa della sua continua ricerca e sperimentazione, necessità di utilizzare modelli e approcci diversi che sono offerti spesso dal mondo dell'Open Source.

Anche il mondo business, in alcuni casi, si sta adeguando a soluzioni suggerite dalla filosofia O.S.

Scelte implementative

Abbiamo deciso di utilizzare per creare i Router-Ip dei nostri tre stabilimenti e per il border router d'area, hardware general purpose e Software Open Source (Gnu/Linux).

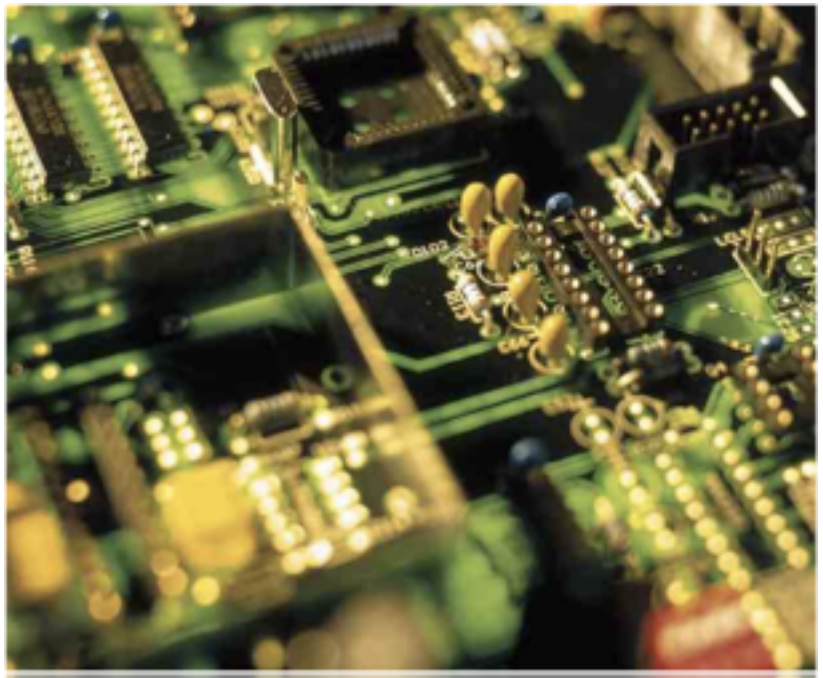
Il motivo principale di questa scelta va cercato nella duttilità delle soluzioni offerte dal mondo dell'O.S. e dalle competenze presenti all'interno della Fondazione.

Architettura Hardware

L'architettura di un pc general purpose normalmente non è particolarmente ottimizzata per le operazioni di rete.

A prima vista non potrebbe raggiungere le stesse prestazioni di una soluzione di apparati di rete che contengono hw ad hoc soprattutto dal punto di vista del data plane.

La potenza di computazione di un normale pc e' nettamente superiore rispetto a quella di un prodotto di rete.

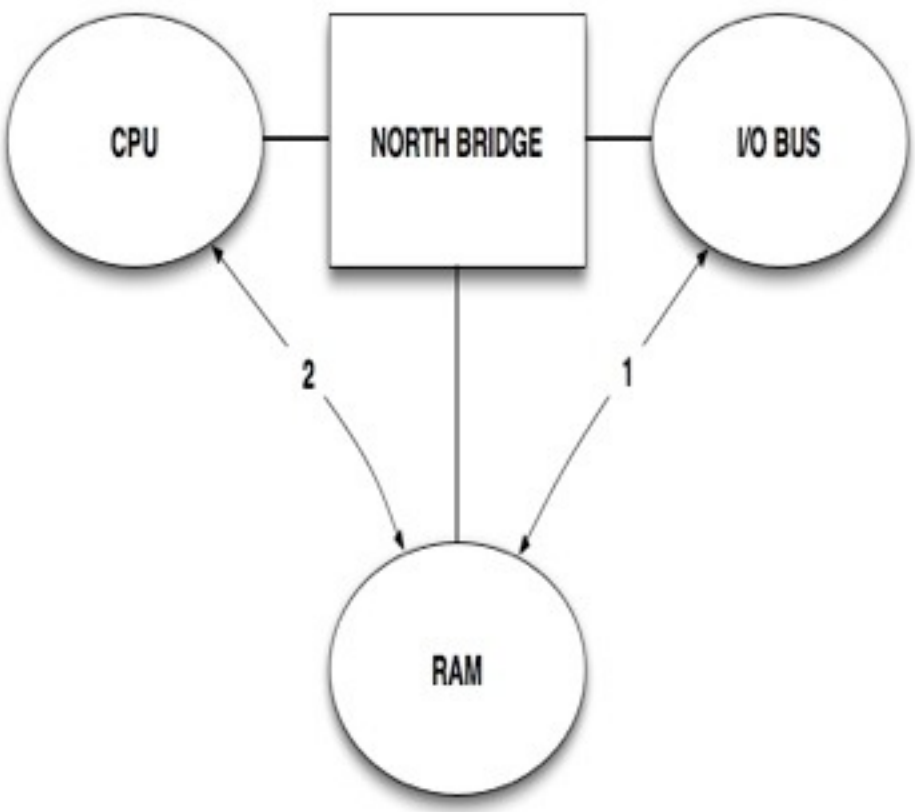


Il Viaggio dei pacchetti di rete

Durante le operazioni di rete, il percorso interno dei dati utilizza massicciamente la struttura I/O del PC.

La struttura e' composta da:

- il bus I / O.
- Il canale di memoria.
- Il processore
- Il North Bridge



Questioni di larghezza

E' evidente che la larghezza di banda del bus e la capacità computazionale del Pc rappresentano i due elementi hardware più critici coinvolti nella determinazione delle massime prestazioni.

Questi due elementi influenzano il valore di picco della larghezza di banda e il massimo numero di pacchetti trasmessi al secondo.

Abbiamo quindi scelto di utilzzare un bus molto veloce e due processori con ram ad alte prestazioni.

Le interfacce di rete

Altro elemento cruciale sono le schede di rete in quanto possono condizionare le performance del sistema.

Sul mercato esistono diverse nic con diversi gradi di prestazioni e configurabilità.

La bontà in termini di velocità tra una scheda e l'altra si nota quando il collegamento di rete utilizzato cresce sino ad arrivare a velocità pari a 1 Gigabit o 10 Gigabit.

Hardware adottato

Per i nostri "Open Router" abbiamo utilizzato 8 Server rack mount con le seguenti caratteristiche:

-Dual processor Amd 3 Ghz (dual core)

- 4 gb di memoria Ram

- 2 dischi sata da 150 gb

- Controller Raid (in config. Mirror)

- 8 interfacce di rete Gigabit con bus Pci-X (10/100/1000)

-Doppio alimentatore

Architettura Software (I)

L'architettura software deve provvedere a gestire le due attività principali:

- Il processo di inoltro dei pacchetti (data plane)
- la gestione delle comunicazioni per la parte di control plane.

Linux integra tutte le funzioni di forwarding direttamente nel kernel.

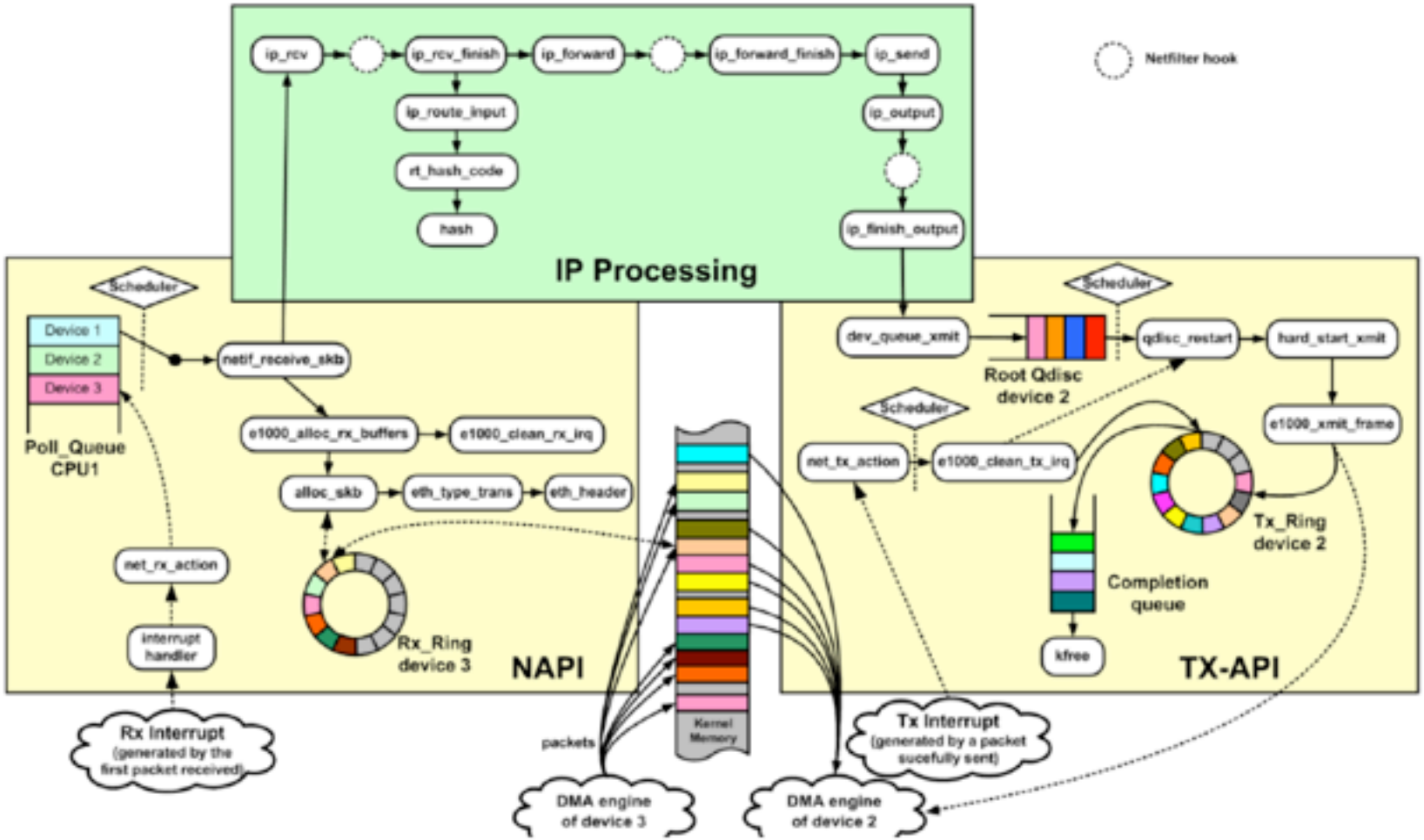
Le funzioni di control plane sono gestite da demoni che girano in user space.

Architettura Software (II)

I processi di data e control plane, a differenza dei prodotti commerciali, condividono la Cpu del sistema.

Il kernel 2.6 di Linux implementa tecniche per migliorare al massimo la gestione e l'inoltro dei pacchetti (Napi architecture, zero-copy statement, preemptyness kernel ecc..).

In caso di supporto SMP, la gestione di ogni interfaccia di rete e' assegnata ad una singola CPU (rx e tx).



Kernel Linux 2.6

Sistema Operativo adottato

Sistema Operativo: Gnu/Linux.

Debian versione 5.0

Distribuzione testing (Squeeze).

Installati solo i pacchetti strettamente necessari.

Nessuna interfaccia grafica o applicazioni non necessarie per il nostro scopo.

Best practice

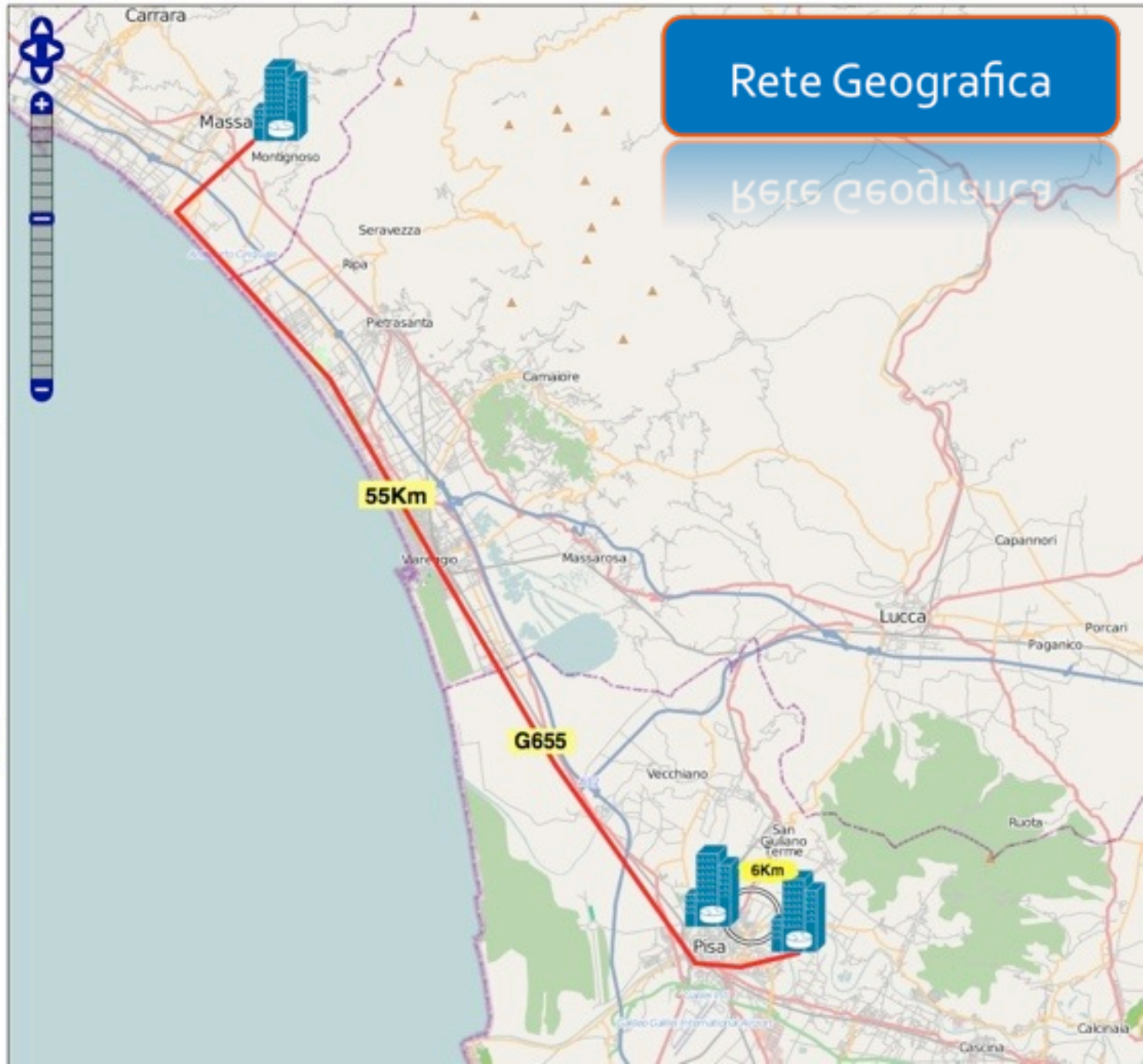
Hardware:

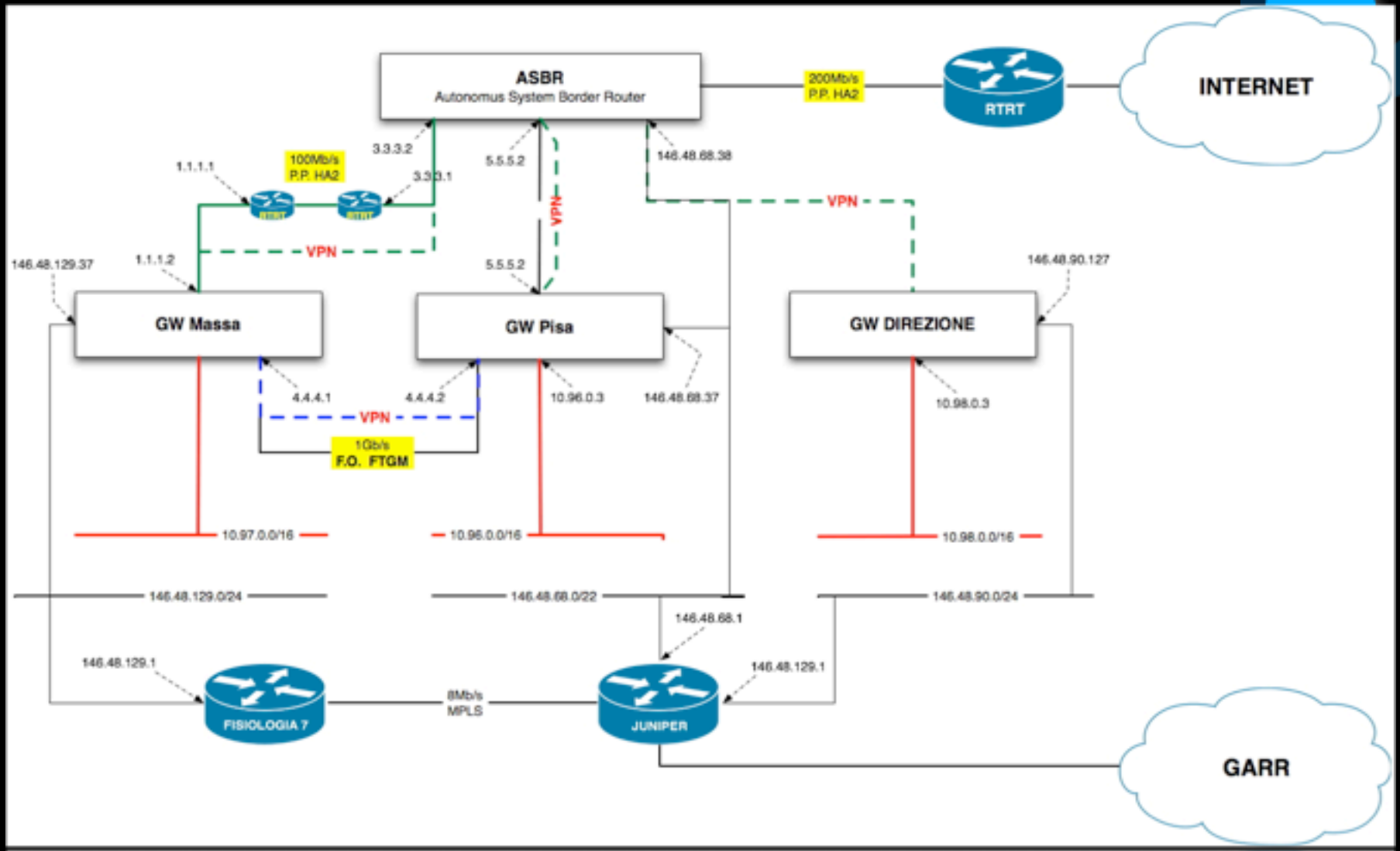
- Bus I/O estremamente veloce.
- Tenere il numero di richieste di interrupts a una soglia bassa.
- Memoria Ram ad alte prestazioni.

Software:

- Evitare la frammentazione.
- Prendere in considerazione di ricompilare il kernel.
- Evitare attività di firewall.

Rete Geografica





Rete Geografica

Firewall (I)

Per implementare le politiche di sicurezza abbiamo utilizzato Netfilter.

Netfilter è un componente del kernel di Linux che permette l'intercettazione e la manipolazione dei pacchetti di rete.

Il firewall di Linux offre funzionalità di filtraggio statefull dei pacchetti e di gestione del Nat.

Per configurare le policy di netfilter e' possibile usare iptables.

Firewall (II)

Pro:

- Identificazione dei pacchetti che fanno parte di una singola connessione
- Facilmente estendibile attraverso moduli aggiuntivi.
- Possibilità di gestire configurazioni complesse di Nat

Contro:

- Manca una vera interfaccia grafica di gestione (FwBuilder)

Intrusion Detection System (I)

Snort e' risultato la scelta vincente per identificare traffico anomalo e accessi non autorizzati verso computer della nostra rete.

Numero basso di falsi positivi.

Non e' possibile analizzare traffico crittografato.

Attualmente usiamo Snort solo in modalità "Alert" (ids passivo).

Intrusion Detection System (II)

Pro:

- Possibilità di utilizzo di più preprocessori (es. clamav).
- Set di ruleset disponibili su Internet.
- Interfaccia web di gestione.

Contro:

- Esoso di risorse.
- Non è sempre possibile riconoscere traffico p2p.

Vpn (I)

Per creare tunnel crittografati per la comunicazione dei vari router abbiamo utilizzato Openvpn.

Il traffico e' trasportato attraverso il protocollo udp.

Il tunnel cifrato viene creato utilizzando le librerie openssl e del protocollo TLS.

Esistono diversi modi di autenticazione.

Vpn (II)

Pro:

- Multipiattaforma.
- Supporto per interfacce L2/L3.
- Utilizza una sola porta per veicolare il traffico.

Contro:

- Non esistono apparati di rete con supporto Openvpn.

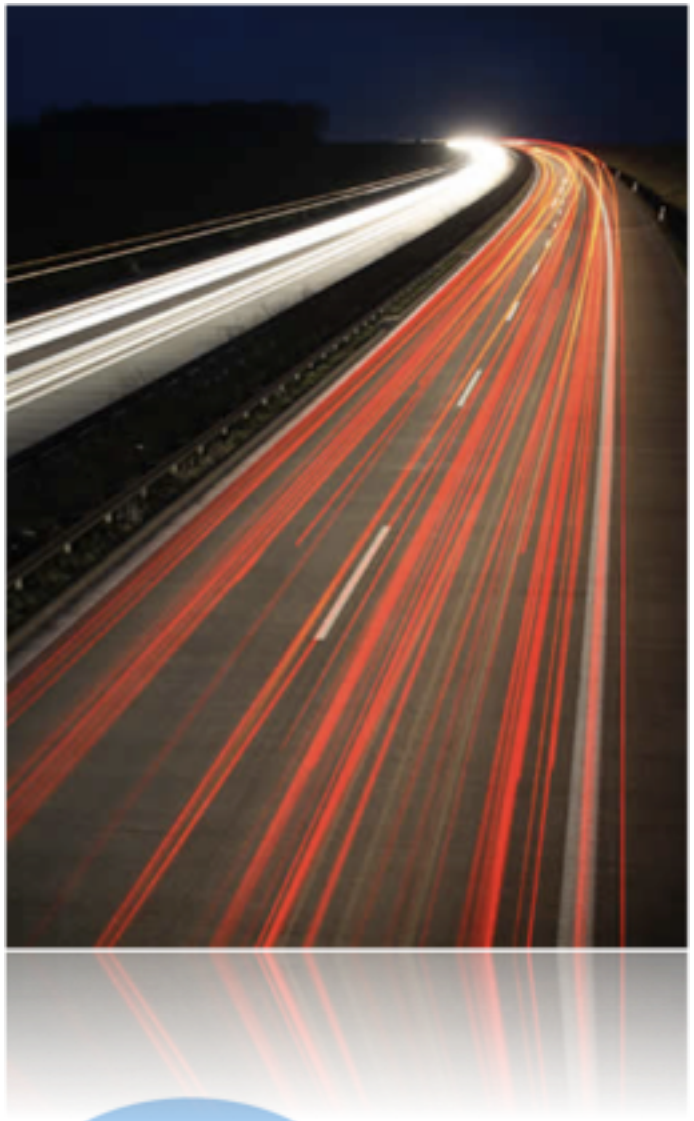
Routing (I)

Il protocollo di routing utilizzato è Ospf.

Il demone utilizzato per gestire il routing dinamico è Quagga.

Quagga è composto da tanti demoni quanti sono i protocolli di routing gestiti più un demone "manager" per gestire la tabella di routing del kernel.

L'architettura multi-daemon permette modularità, scalabilità e facile manutenzione del sistema.



Routing (II)

Pro:

- Command line interface Cisco like.
- Supporta vari protocolli di routing.
- Supporta Ipv6.

Contro:

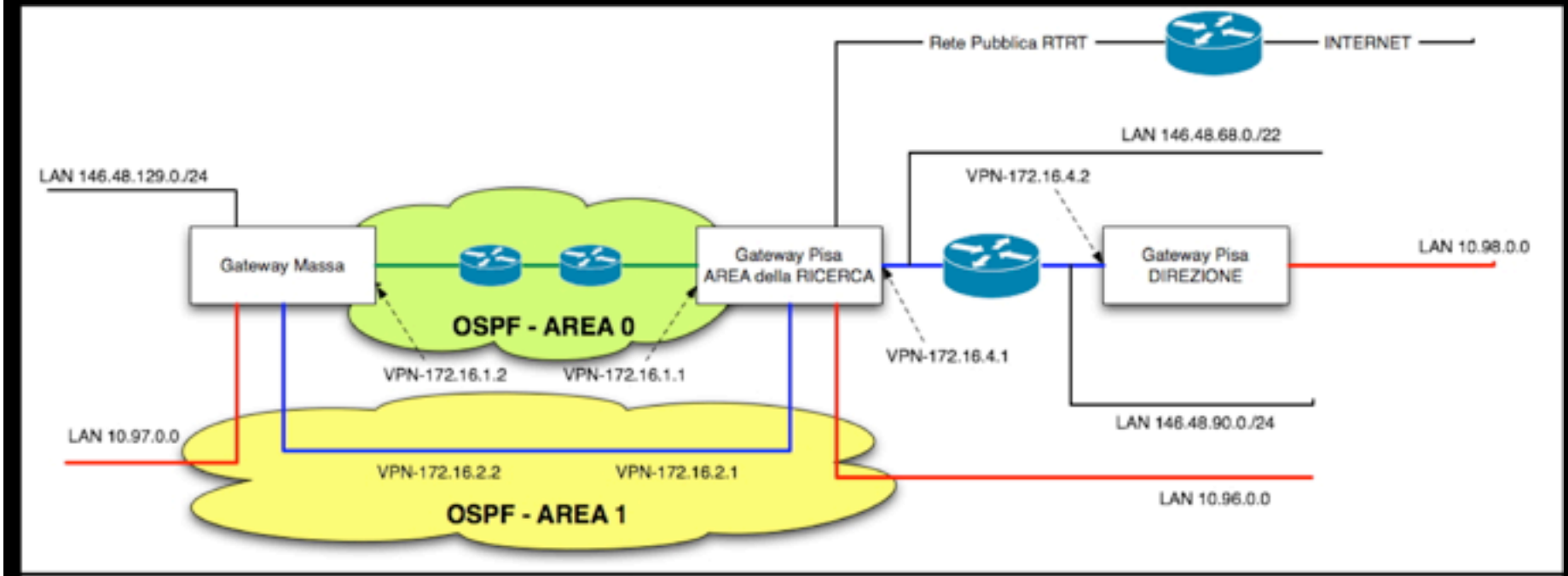
- Set di funzionalità limitate.
- Molti file di configurazione da gestire.

Traffic Engineering

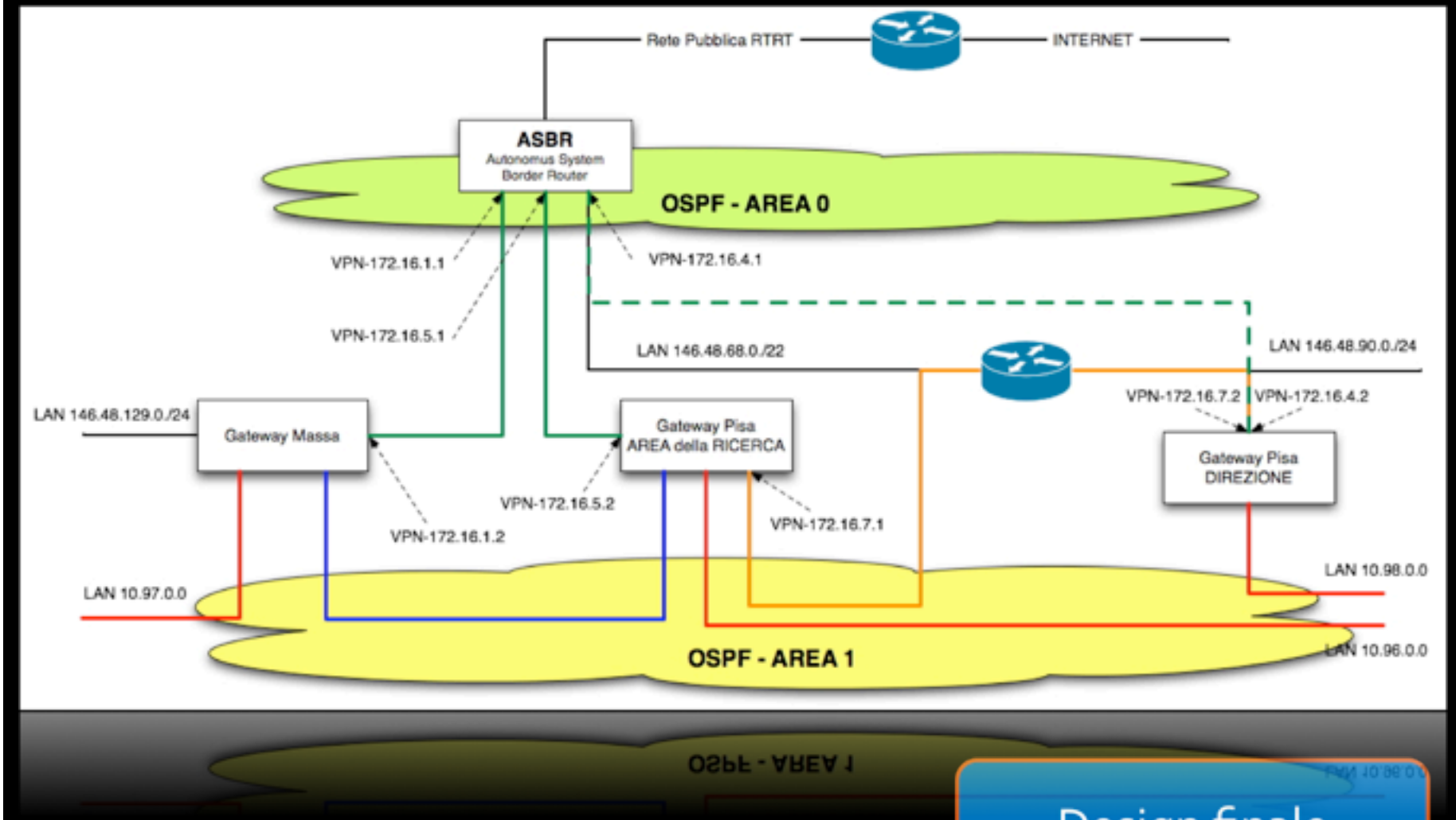
Le tecniche di traffic engineering hanno lo scopo di ottimizzare le prestazioni della rete.

Il nostro obiettivo prestazionale è utilizzare tutte le risorse di rete (collegamenti) tra le sedi di Pisa e Massa, trasportare il traffico di rete sul link appropriato a seconda della sua tipologia.

Inoltre vogliamo garantirci di minimizzare la perdita di pacchetti, il ritardo e la congestione, massimizzare il throughput.



Design (1°ipotesi)



Design finale

Qos

Il trasporto del traffico clinico deve avere precedenza rispetto al trasporto di altre tipologie di traffico.

Abbiamo la necessità di caratterizzare la qualità del servizio offerto dalla nostra rete in modo da dare priorità al traffico clinico.

Per implementare la qualità del servizio sulla nostra rete abbiamo adottato le politiche di shaping offerte da Traffic Control (TC).

Alta Affidabilità

I servizi di rete devono rimanere sempre attivi e disponibili.

I nostri router non possono rappresentare un punto di fallimento.

La disponibilità del servizio viene garantita attraverso vari metodi:

- Duplicazione dei sistemi
- Doppia Alimentazione
- Doppi link di rete
- Adozione di sistemi Raid

Alta Affidabilità – Keep Alive

Per gestire l'alta affidabilità dei sistemi utilizziamo il protocollo VRRP e il demone KeepAlive.

Ogni router e' composto da due server (master/slave).

Il master eroga il servizio mentre lo slave e' in "attesa calda" pronto ad entrare in funzione in caso di necessità.

I due server sono connessi attraverso un collegamento di rete dedicato (punto punto) che permette lo scambio di messaggi di stato.

Monitoring

I nostri sistemi hanno bisogno di un monitoraggio continuo e puntuale.

Il monitoring ci permette di conoscere sia le prestazioni dei sistemi di rete (Cacti) e sia di essere informati in tempo reale su eventuali malfunzionamenti degli apparati.

Per effettuare il controllo utilizziamo Nagios con l'aggiunta di plug-in di terze parti o direttamente scritti da noi.

Il malfunzionamento ci viene segnalato via Email, Sms e Dashboard.

Prestazioni ?!?

Quali sono le reali prestazioni del sistema?

E' possibile prevedere un degrado di performance al superare di una determinata soglia?

Come e' possibile paragonare diverse soluzioni implementate con prodotti Open Source?

CONCLUSIONI

Andiamo in produzione con l'Open Source!

Tecnologia Open Source per costruire valide soluzioni di rete anche in contesti di business.

Consapevolezza di non essere soli ad affrontare vecchie e nuove soluzioni O.S.

Il nostro lavoro non e' un punto di arrivo ma semplicemente una pietra miliare che apre nuovi orizzonti.

Lavoriamo per rinforzare i consorzi di conoscenza.

DOMANDE?
RISPOSTE!

Giuseppe Augiero – giuseppe@ftgm.it - g.augiero@ifc.cnr.it
Alessandro Mazzarisi – mazzaris@ifc.cnr.it

Giuseppe Augiero – giuseppe@ftgm.it - g.augiero@ifc.cnr.it
Alessandro Mazzarisi – mazzaris@ifc.cnr.it