



REGIONE TOSCANA  
Giunta Regionale

# Summary

## *Tuscany Internet eXchange*

Un contributo: per migliorare il livello delle infrastrutture di rete in Toscana, per lo sviluppo di internet in Italia, per i servizi ai Cittadini e alle Imprese.

Firenze Luglio 2002.

## *INDICE*

<b>INTRODUZIONE</b>	<b>3</b>
<b>1 PROGETTO DELLA SOLUZIONE NAP DEL TIX</b>	<b>7</b>
<b>2 SERVIZI DELLA RTRT</b>	<b>8</b>

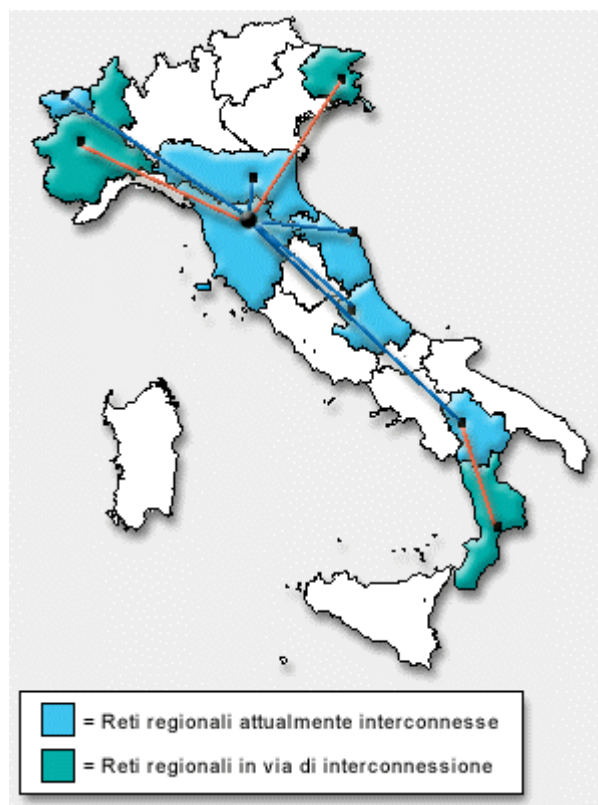
## Introduzione

Il presente documento descrive sinteticamente la “Realizzazione e gestione di un Punto Neutrale di Interconnessione (NAP) fra la Rete Telematica Regione Toscana e le reti di accesso sul territorio toscano degli operatori privati (ISP) denominato : Tuscany Internet eXchange – (T.I.X.)”, per approfondimenti si rimanda al documento di progetto.

L'intervento in oggetto si colloca nell'ambito del piano regionale di e-government denominato e.Toscana con particolare riferimento al settore delle azioni infrastrutturali e realizza uno dei nodi di interconnessione della **Community Network delle Regioni**, che a sua volta contribuisce alla realizzazione della **Rete Nazionale della pubblica amministrazione**.

Le principali linee di sviluppo perseguite nella progettazione e realizzazione del T.I.X. sono relative ai seguenti obiettivi:

1. poter disporre sul territorio di una infrastruttura di trasporto a banda larga;
2. poter garantire molteplici modalità di collegamento a tale infrastruttura, per garantire e diffondere il più possibile l'accesso ai servizi su di essa distribuiti, anche attraverso dispositivi mobili (cellulari, palmari, ecc.);
3. poter disporre di modalità di accesso sicure (VPN)
4. costituire un Centro Servizi per la Rete Telematica Regionale Toscana;
5. garantire l'estensione della connettività ed interoperabilità all'intero tessuto socio-economico della Toscana;
6. fornire un sostanziale contributo alla realizzazione della rete nazionale della pubblica amministrazione così come delineato nelle linee guida approvate dalla Conferenza Unificata Stato Regioni del Febbraio 2001.



Il progetto tende quindi a sommare i benefici derivanti dal disporre di una rete della pubblica amministrazione fortemente interconnessa, a quelli di una copertura territoriale totale di servizi

di qualità garantita e controllata per tutta la popolazione servita da ISP accreditati, pur nel rispetto dei diversi obiettivi di finalità pubblica o di mercato.

Il progetto si propone inoltre di ottenere la copertura territoriale tramite la realizzazione di un sistema **Neutral Access Point** (NAP) Toscano denominato Tuscany Internet eXchange (**TIX**), cioè un punto d'interconnessione comune tra tre o più Internet Service Provider per lo scambio paritetico, cioè neutrale e senza privilegi, dei loro flussi IP attraverso lo stabilimento di canali diretti (peer) tra i domini di rete di ciascun ISP/peerer partecipante al NAP.

La partecipazione degli ISP al TIX avverrà tramite la costituzione di un elenco di ISP accreditati, in grado di fornire servizi Internet alle pubbliche amministrazioni che desiderino aderire alla RTRT e che per motivi organizzativi e/o di costi non possano essere direttamente connessi all'infrastruttura fisica di RTRT.

Il TIX, oltre alla funzione di NAP, svolgerà il ruolo di Centro Servizi per la Rete Telematica Regionale Toscana presso un fornitore terzo che garantisca locali e servizi accessori (alimentazione con continuità, protezioni antincendio ecc.) secondo standard predefiniti e ad un livello di servizio adeguato e controllabile. In particolare il Centro Servizi del TIX consentirà il decentramento (Housing) di server e apparati di rete attualmente situati presso il CED della Regione Toscana, nonché la fornitura ai soggetti di RTRT di servizi in modalità Hosting.

Tra gli scopi fondamentali del Centro Servizi assume notevole rilievo la realizzazione di un servizio per il **mantenimento di adeguati livelli di qualità dei servizi** (SLA) attraverso il **monitoraggio** della parte NAP, dell'infrastruttura di trasporto di RTRT, nonché dei servizi tramite essa erogati. Verrà inoltre implementato un **servizio di Help Desk** per supporto di primo e secondo livello, che risponda a problematiche sui servizi erogati dal TIX, su eventuali malfunzionamenti presso il TIX e su RTRT e sulle modalità di accreditamento degli ISP.

Intervento complementare alla realizzazione del T.I.X. è il potenziamento della dorsale di RTRT in termini di banda ed affidabilità sarà realizzato tramite:

- potenziamento degli accessi ATM utilizzati per la raccolta delle sedi collegate da 34 Mbps a 155 Mbps ed incremento del numero delle sedi collegate;
- aggiunta di un router presso il nodo di Firenze con equipaggiamento per la raccolta di linee ISDN di backup al fine di incrementare l'affidabilità della dorsale;
- realizzazione di un nuovo collegamento ATM, con banda minima garantita 10 Mbps, fra i nodi di Pisa e Siena al fine di garantire un rafforzamento della dorsale di RTRT e la continuità del servizio;
- passaggio da 6 Mbps a 15 Mbps di banda minima garantita sui collegamenti ATM Firenze-Pisa e Firenze-Siena

- il potenziamento ed estensione delle tipologie di accesso( xDSL, Lan Metropolitane, satellite, wireless, Gprs, UMTS, ecc.)

L'estensione della RTRT attraverso ISP privati garantirà una migliore e capillarmente diffusa connettività fra i soggetti della Pubblica Amministrazione Toscana, con l'obiettivo di mantenere un appropriato livello di prestazioni e sicurezza ottenuto attraverso un albo di ISP accreditati su specifici prerequisiti.

I benefici non saranno limitati alla PA Toscana: infatti un NAP commuta i traffici IP degli ISP ad esso connessi, tramite opportune politiche di routing. con lo scopo di migliorare l'interconnessione tra gli ISP medesimi. La partecipazione ad un NAP offre generalmente notevoli vantaggi operativi e commerciali a ciascun ISP, in quanto ne consente la redistribuzione del traffico di rete, con la conseguente liberalizzazione delle connessioni internazionali e nazionali dal traffico locale diretto agli altri peerers partecipanti al NAP.

La realizzazione della "RTRT estesa" tramite TIX e ISP accreditati, oltre ad aprire nuove possibilità al mercato per gli ISP, permette un risparmio economico alla P.A.L. Toscana in quanto vengono sfruttate infrastrutture già esistenti, senza ulteriori pesanti investimenti per distribuire ancora più capillarmente l'accesso ai servizi forniti su RTRT.

In sostanza, la possibilità per tutti i soggetti della P.A.L. Toscana di poter disporre di una infrastruttura di trasporto potente, flessibile, fortemente integrata al resto dell'Internet-paese senza affrontare singolarmente i pesanti investimenti altrimenti necessari, permetterà innanzi tutto economie di scala, inoltre, ogni altro progetto e-government, e non solo, istanziato in Toscana, potrà assumere l'infrastruttura di trasporto di RTRT e di servizi centralizzati presso il TIX come una risorsa comune immediatamente fruibile, senza doversi quindi occupare di disperdere energie e risorse nello sviluppo di un proprio livello infrastrutturale.

Nei successivi capitoli verranno descritte sinteticamente le diverse componenti architetture ed organizzative del TIX, oltre ai servizi offerti.

Sono partner tecnico scientifici della Regione Toscana per la iniziativa del TIX:

**Università di Firenze - Centro di Eccellenza per la  
Comunicazione e l'Integrazione dei media** diretto  
dal Prof. Vito Cappellini

**Consiglio Nazionale delle Ricerche - Istituto per  
l'Informatica e la Telematica** diretto dal Prof.  
Franco Denoth.

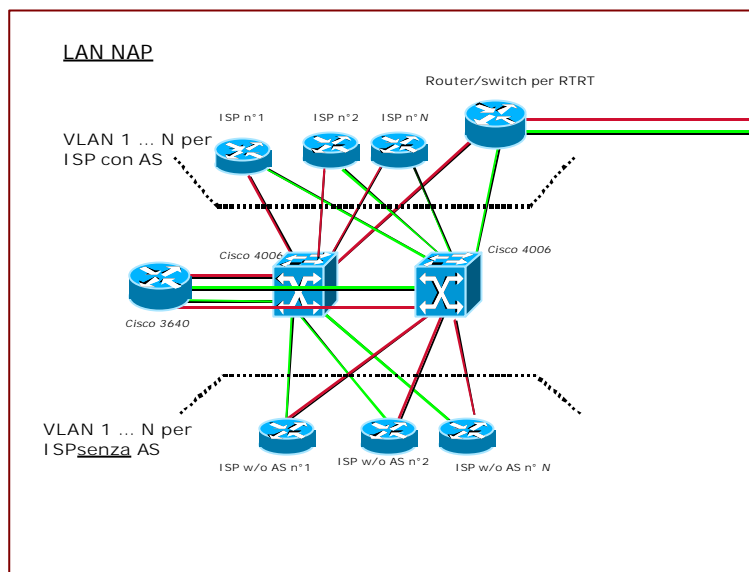
La realizzazione del progetto del TIX e la relativa conduzione è stata affidata, tramite bando di gara, a:

**Telecom Italia S.p.A., Getronics Solutions S.p.A.,  
Brain Technology S.p.A.**

## 1 Progetto della soluzione NAP del TIX

Come si evince dallo schema la LAN NAP è divisa in due o più VLAN da dimensionare correttamente in fase di installazione. La prima VLAN è dedicata a funzioni di monitoraggio e controllo delle politiche implementate dagli ISP che accedono al NAP per le proprie politiche di peering verso RTRT o verso

gli altri ISP. Ogni ISP collegato al NAP attraverso una VLAN dovrà presentarsi con un router in grado di annunciare le proprie reti e il proprio AS (pubblico per gli ISP che ne sono dotati, privato per chi ancora non ne sia fornito) attraverso l'uso del protocollo di routing BGP (Border Gateway Protocol). Il compito



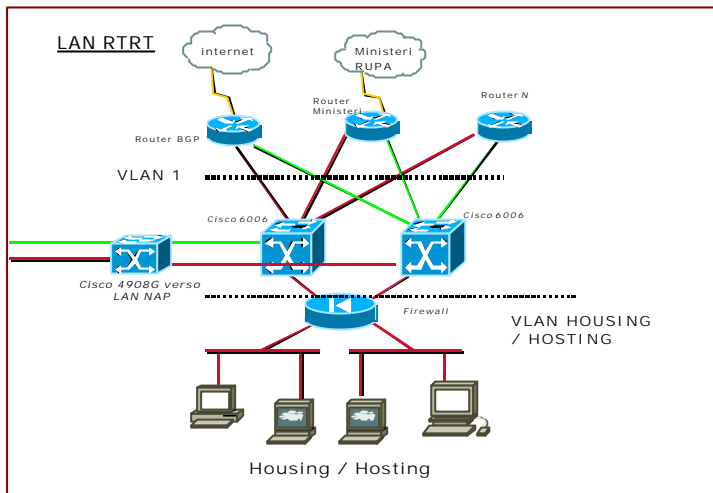
dei due switch è relativo alla continuità e alle performance del solo livello 2 della rete.

Sono inoltre attivati servizi di supporto per:

- a) **Sistema di monitoraggio e reportistica** con l'obiettivo di controllare il sistema realizzato presso il TIX con particolare attenzione all'analisi dei livelli di traffico per la verifica del rispetto delle politiche di peering/routing adottate e degli SLA contrattualizzati tra "RTRT estesa" e ISP accreditati;
- b) **servizio di help desk di primo e secondo livello per gli ISP accreditati** per fornire consulenza e supporto su tutte le problematiche relative al servizio NAP offerto, incluso un servizio informativo agli ISP circa le modalità di accreditamento.

## 2 Servizi della RTRT

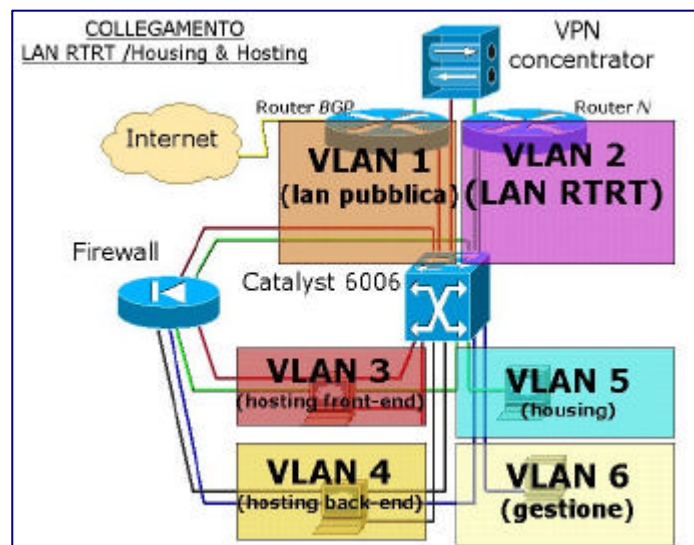
Similmente a quanto proposto per LAN NAP, anche in questo caso vengono create delle VLAN così suddivise :



- La VLAN 1, definibile “pubblica”, atta ad alloggiare la parte dei collegamenti di RTRT verso il mondo esterno;
- La VLAN 2, la vera e propria LAN RTRT, è dedicata ai collegamenti verso i Ministeri ed altri Enti Pubblici, nonché verso il resto di RTRT;
- La VLAN 3, contenente la parte

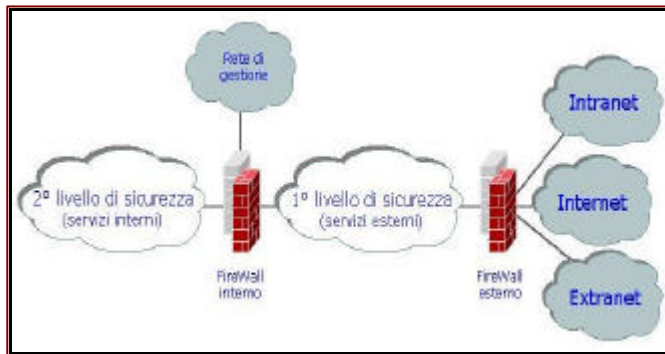
front-end di hosting, tipicamente servizi visibili dall'esterno (web sever, mail server, ecc.);

- La VLAN 4, contenente la parte back-end di hosting, servizi non necessariamente visibili dall'esterno (database, server LDAP, ecc.);
- La VLAN 5, destinata ad apparati in housing;
- La VLAN 6, destinata all'accoglienza dei sistemi di gestione.



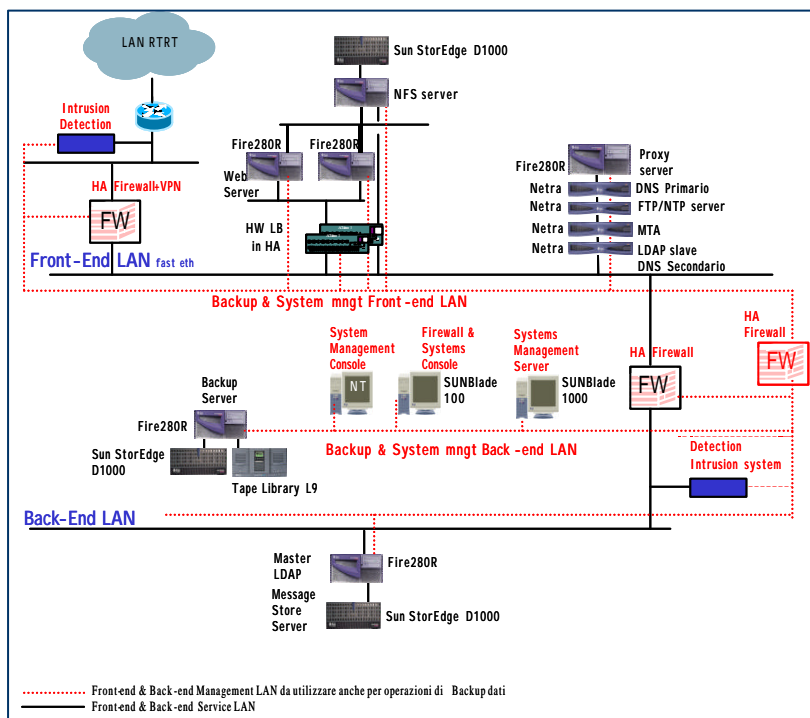
La connessione fra i due ambienti NAP e RTRT è un punto nevralgico del TIX in cui è necessario far fronte a due esigenze primarie: la prima riguarda la potenza, la stabilità e la futura scalabilità del throughput; la seconda esigenza nasce dal fatto che in questo punto RTRT diventa “visibile” agli altri ISP aderenti al NAP, con la conseguente necessità di implementare politiche di routing abbastanza raffinate, pertanto l'apparato utilizzato per la connessione dei due ambienti è uno switch a livello 3.

La realizzazione di servizi applicativi in hosting si basa su una soluzione infrastrutturale altamente integrata che copre tutti gli aspetti di fornitura e gestione ed amministrazione dei servizi e della piattaforma hardware e software. Tutte le componenti sono viste come moduli assolutamente indipendenti, interpretando in chiave architeturale il concetto di plug-in. La decomposizione funzionale dei



singoli servizi in moduli permette, come conseguenza, eventuali riconfigurazioni all'interno di ciascun blocco con minimo impatto sulla continuità di esercizio del Data Center.

L'architettura del Data Center proposto è basata sul modello di rete a doppio livello di sicurezza (sicurezza perimetrale) che consiste sia nella separazione logica e fisica dei due diversi gruppi di



reti (Front-end e Back-end) con sensibilità differenti, rispettivamente media (front-end) e alta (back-end), sia nella creazione di due punti di controllo delle policy di sicurezza aziendali, con conseguente miglioramento delle funzionalità di controllo accessi ai dati/servizi.

L'architettura di sicurezza per le funzionalità di controllo accessi e difesa

perimetrale è basata principalmente su sistemi di Firewall e di Intrusion Detection, rispettivamente in grado di separare logicamente le LAN del Centro Servizi e di rilevare eventuali tentativi d'attacco.

L'infrastruttura di rete prevede due sottoreti di servizio, una di Front End e una di Back End, all'interno delle quali si attestano i server che implementano la logica applicativa del servizio e i sistemi specializzati preposti alla gestione dei dati (DBMS).

Sono inoltre presenti i seguenti servizi di supporto:

- a) **Servizio di help desk di primo e secondo livello per i soggetti RTRT**, rivolto esclusivamente a tutti i soggetti aderenti alla RTRT, fornisce supporto su tutte le problematiche di prima attivazione o utilizzo, malfunzionamenti, servizi disponibili e modalità di fruizione, servizio informativo e consulenza tecnica generica, instradamento verso centri di responsabilità specifici o Help Desk di secondo livello;
- b) **Verifica delle misure di sicurezza adottate dai soggetti RTRT**, con successiva proposizione di azioni da intraprendere al fine dell'innalzamento del livello di sicurezza complessivo dei soggetti e della rete.

Ai fini della sicurezza, inoltre, i soggetti direttamente collegati a RTRT usufruiscono di servizi riservati (Infocamere, Banche dati de sole24ore, SIATEK Edicola Telematica Integrazione anagrafi, ...) securizzati a livello applicativo tramite l'utilizzazione di certificati digitali o a livello IP tramite l'appartenenza alla classe B assegnata ad RTRT (159.213.0.0/16). Per permettere l'accesso alla RTRT da parte degli utenti provenienti da altro ISP con lo stesso livello di sicurezza attualmente esistente per i soggetti direttamente collegati ad RTRT, sarà messo a disposizione un sistema di concentrazione delle VPN al fine di garantire:

- l'individuazione dell'origine;
- la riservatezza dell'informazione.

Il VPN Concentrator realizza quindi, una rete privata virtuale creando una connessione sicura sulla rete TCP/IP e gli utenti vedono tale connessione come una vera e propria connessione privata.