PREMESSA

Il presente documento rendiconta le attività di sviluppo e ricerca effettuate per l'esecuzione ed attivazione del sistema descritto dal Progetto dell'Infrastruttura Tecnologica ed Informativa di cui la Fondazione IME si è dotato.
Verranno pertanto ripercorse le linee guida del progetto, riportandone di volta in volta i dettagli tecnici e le scelte compiute.
Si evidenzia che la presente rendicontazione riporta le attività svolte e lo stato di avanzamento dei singoli elementi al novembre 2004.

ELEMENTI ESSENZIALI DELL'INFRASTRUTTURA

L'infrastruttura tecnologica rappresenta un elemento strategico per la rete sanitaria nazionale ed internazionale che sta alla base del mandato della Fondazione IME e del Progetto Internazionale.

La rete sanitaria si concretizza infatti sulla possibilità di attivare funzioni di integrazione informativa tra i vari nodi, sulla condivisione di database clinico-scientifici, sulla disponibilità di servizi avanzati di *e-medicine* e di *second opinion*.

I nodi sanitari della rete devono assicurare infatti omogeneità nell'applicazione dei protocolli di cura e nel management clinico delle tecniche di trapianto, secondo standard definiti dalla Direzione Scientifica di IME e controllati attraverso la costante integrazione informativa sulla gestione e sull'outcome dei percorsi sanitari.

In particolare, la rappresentazione iconografica del paziente attraverso il supporto dell'immagine digitale (radiologica, ecografia, endoscopica, istologica, *live*, etc..) costituisce l'elemento portante del percorso di cura, condiviso ed accessibile da parte di tutti gli operatori sanitari della rete.

Le applicazioni informatiche-informative sono quindi pensate per essere integrate con applicazioni di tipo PACS (Picture Archive & Communication Services) e distribuite su rete in modalità Fast-Internet con caratteristiche adeguate di accessibilità e di larghezza di banda.

La progettazione di un sistema complesso di rete ha comportato la necessaria individuazione di un metodo, ovvero di un percorso progettuale, che ha guidato la scansione delle realizzazioni, mantenendo la coerenza tecnologica ed informatica generale.

Detto percorso è stato accompagnato da una serie di scelte sugli standard tecnologici (protocolli, sistemi operativi, database, formati dati e immagini, etc.), da mantenere uniformi per tutte le realizzazioni della rete.

La ideazione di "layers" di Progetto sovrapposti, individua la sequenza di implementazione dei supporti tecnologici, dei database informativi condivisi, dei servizi comuni e distribuiti ed infine delle specifiche applicazioni.
Ciascun "layer" riceve da quello precedente supporti informativi e servizi, garantendo la completa integrazione dei flussi, delle basi dati e delle applicazioni.

Con riferimento alle strutture informatiche già esistenti presso i centri che entrano a far parte della rete IME, la scelta di Progetto è riferita ad una integrazione "parallela" dei flussi informativi esistenti, a partire dal primo livello dei "Database condivisi".

L'integrazione proposta da IME sulla propria rete è una integrazione "bottom-up" a partire dai flussi informativi condivisi (anagrafiche, info cliniche di base, progetti comuni di ricerca, etc.), da sviluppare progressivamente in modalità Internet e datawarehouse e da estendere via via al crescere quali-quantitativo delle attività in rete.

Linee guida del sistema informativo

La natura dell'istituto e la collocazione del networking organizzativo tecnologico in posizione di staff al Commissario della Fondazione, impongono una caratterizzazione forte della funzione, verso la progettazione e la governance del sistema.

In tal senso, le attività di progettazione, scelta dei fornitori e dei prodotti, gestione dei fornitori, dei contratti, dei prodotti, la gestione delle policy (profilazione utenti), l'analisi ed elaborazione dati sono realizzate mediante risorse stabili e continuative, all'interno dello staff.

Le analisi e lo sviluppo di soluzioni *ad hoc* sono realizzate con il supporto di fornitori esterni, su stretto indirizzo degli specialisti IME; la gestione server farm e il monitoraggio delle reti, la manutenzione hardware centrale e decentrata e la funzione di help desk utente saranno progressivamente consolidate verso soluzioni in outsourcing, servizi in ASP, e/o in hosting.

Il sistema informativo IME si realizza nel rispetto dei seguenti principi fondanti:

1. il supporto di rete tra le sedi è garantito (laddove possibile) in banda larga;
2. il sistema risponde a una architettura prevalentemente web based;
3. i sistemi software sono sistemi aperti e garantiscono l'interoperabilità mediante gli standard XML/HL7/IHE;
4. le basi dati e le applicazioni rispondono o possono rispondere a un modello Application Server Provider;
5. il sistema garantisce l'accesso in single sign on, per ogni utente e per ogni applicazione
6. la profilazione utenti è governata da IME;
7. il livello gestionale alimenta le basi dati decisionali in maniera surrettizia.

Il sistema informativo IME è progettato per garantire le aree di risultato definite e le funzioni di supporto gestionale operativo:

- regolamentazione: gestione documentale e atti amministrativi;
- cura e assistenza: gestione clinica, secondo logiche di workflow;
- ricerca: basi dati analitiche, repository e strumenti data mining, data drill;
- formazione e aggiornamento: strumenti di e-learning;
- supporto clinico-scientifico e di progettazione organizzativa, all'attività di altri organismi sanitari nazionali ed esteri: strumenti di project management;
- supporto finanziario nello sviluppo di iniziative di ricerca sanitaria: strumenti di contabilità.

Pertanto è possibile definire le seguenti aree:

In ambito amministrativo

- Gestione contabilità generale;
- Gestione contabilità analitica;
- Gestione ciclo passivo ordini a fornitori;
- Inventario beni;
- Gestione documentale, atti amministrativi e protocollo.

In ambito sanitario

- Gestione accettazione amministrativa;
- Gestione processo clinico "Patient Work Flow";
- Archiviazione informatizzata della documentazione clinica;
- Gestione richieste verso fornitori convenzionati.

La topologia di distribuzione delle funzione è tale per cui, per ciascuna sede, si possa accedere alle funzioni necessarie, ovvero ai subset funzionali per i quali i soggetti gestori siano abilitati, secondo uno schema di massima rappresentato nella figura a seguire.

Le soluzioni tecnologiche prevedono, nell'ambito amministrativo, l'individuazione di prodotti standard ottimali, ricercati nel mercato dei prodotti in uso dalla Sanità, possibilmente verso soluzioni di tipo ERP.

Le soluzione tecnologiche prevedono, nell'ambito sanitario, l'individuazione di prodotti di software orientati al supporto del processo clinico, in ottica di Patient Workflow, e all'archiviazione informatizzata dei dati clinici del paziente in repository storici.

L'infrastruttura informatica di sistema garantisce inoltre le funzionalità standard di automazione di ufficio, comprensive dei servizi di posta certificata e accesso Internet controllato.

Ogni applicazione gestionale è e dovrà comunque essere conforme a quanto previsto dalla normativa vigente; fra l'altro tutto il sistema informativo dell'Ente è e sarà progettato e realizzato in coerenza con quanto previsto dal D.L. 30.06.2003 n. 196 – Codice in materia di protezione dei dati personali.

Modalità di realizzazione del Sistema informativo di IME

La creazione di una infrastruttura tecnologica ed informatica rappresenta un elemento strategico per la realizzazione della rete sanitaria nazionale ed internazionale che sta alla base del mandato della Fondazione IME (art. 2 dello Statuto).

La rete si concretizza infatti sulla possibilità di attivare:

- funzioni gestionali proprie della Fondazione e dei suoi centri di attività, sia in ambito amministrativo che sanitario;
- la integrazione informativa tra i vari nodi;
- la condivisione dei database relativi all'attività di ricerca e dei database clinico-scientifici;
- la disponibilità di servizi avanzati di *e-medicine* e di *second opinion*.

I nodi sanitari della rete devono assicurare infatti omogeneità nel pianificazione, programmazione e gestione delle attività organizzative proprie, dei progetti di ricerca, nonché nell'applicazione dei protocolli di cura e nel management clinico delle tecniche di trapianto.

Detta integrazione informativa è realizzata secondo standard definiti dalla Alta Direzione e dalla Direzione Scientifica di IME e controllata attraverso la costante integrazione informativa sulla gestione e sull'outcome dei progetti di ricerca e dei percorsi sanitari.

La realizzazione del sistema informatico informativo IME procede quindi, nel rispetto degli indirizzi sopradescritti, secondo metodo di approssimazioni successive, al fine di sperimentare direttamente le soluzioni architetturali, funzionali e tecnologiche, prima di procedere alla delega verso soggetti terzi partner gestionali di IME, contestualmente da individuare.

E' del tutto evidente infatti che nella realizzazione di soluzioni, amministrative e sanitarie, a servizio di una rete di centri distribuiti in Italia ed all'estero, ci troviamo di fronte a soluzioni oggetto di vera e propria ricerca e sviluppo di applicazioni prototipali.

Il metodo di progettazione/realizzazione utilizzato finora segue un percorso legato:

- alla scelta di piattaforme tecnologiche di riferimento che realizzino lo *standard* da applicare a tutte le soluzioni in rete;
- all'individuazione di partner tecnologici di dimensioni nazionali/internazionali che abbiano capacità adeguate e co-interesse ad investire sullo sviluppo di soluzioni assolutamente innovative e replicabili;
- allo sviluppo congiunto e progressivo di applicazioni in rete, parallelamente allo sviluppo organizzativo della rete IME in Italia e all'estero;
- alla acquisizione di una infrastruttura fisica di collegamento tra i centri della rete IME che fornisca tutti i necessari supporti/servizi in termini di connettività a larga banda.

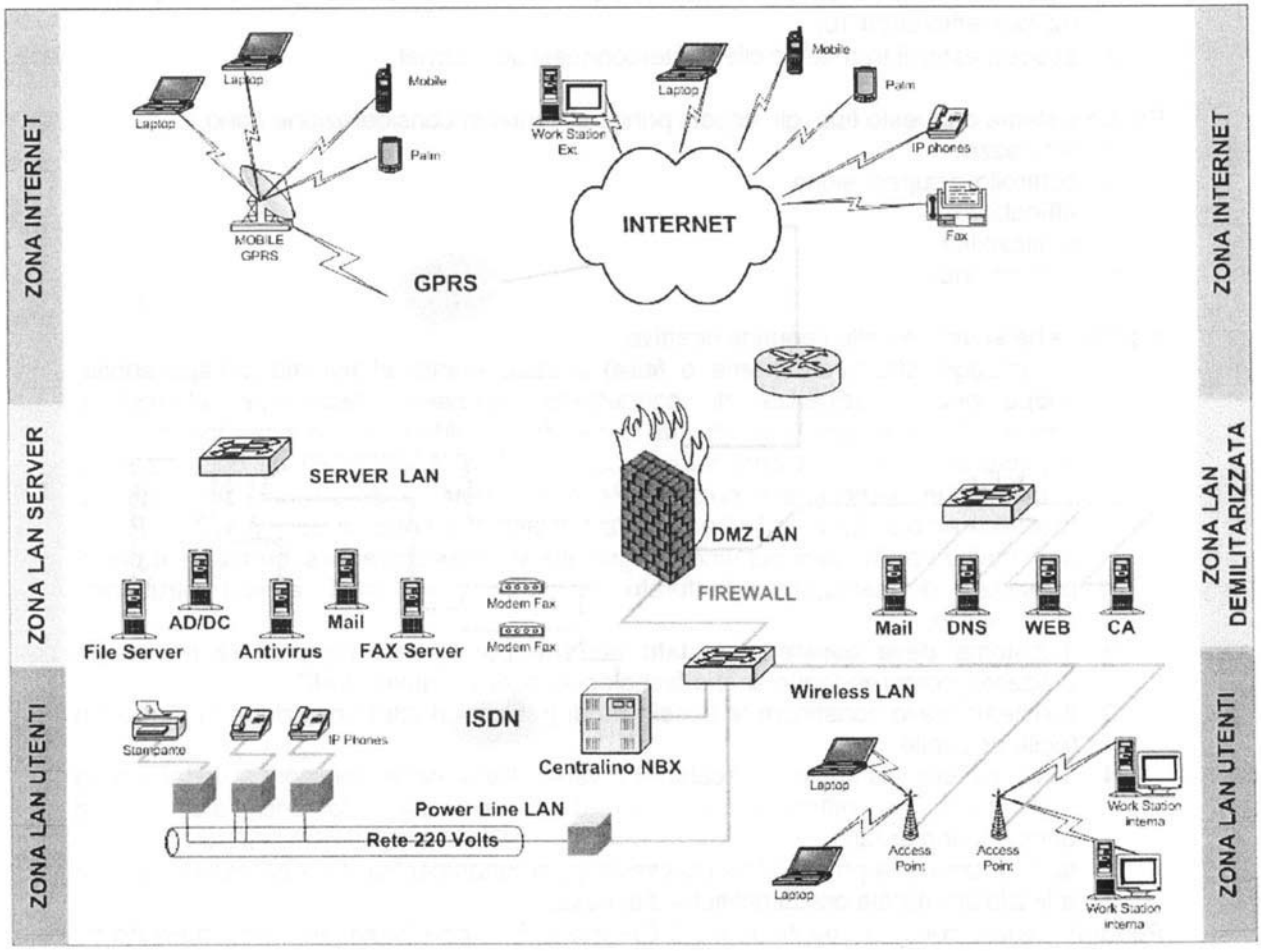
L'entità degli investimenti utilizzati finora e pianificati per il futuro è frutto di una pre-analisi condotta sugli elementi macro del sistema, dove le voci più rilevanti sono rappresentate da:

- acquisizione e sviluppo della infrastruttura di interconnessione a larga banda;
- acquisizione e sviluppo di soluzioni informatiche da elaborare in *partneship* con fornitori di rilevanza nazionale/internazionale;
- forniture di hardware di sistema e per la dotazione degli utilizzatori;
- progettazione, realizzazione e testing delle soluzioni;
- *outsourcing* a regime delle soluzioni stabilizzate in una logica *web based.*

PROGETTO INFRASTRUTTURA REALIZZATO

Schema generale realizzato

Di seguito si riporta lo schema relativo al nodo prototipale realizzato nelle varie parti nella sede di Pesaro.
Per quanto riguarda le altre sedi le parti costituenti sono un sottogruppo di quanto sotto riportato.



Dettaglio di sistema

Topologia funzionale del nodo tipico

Premessa

Tutto il sistema informatico è stato progettato con l'obiettivo di utilizzare quanto di meglio la tecnologia attuale può offrire per un utilizzo in una realtà di tipo enterprise costituita da:

- n nodi (sedi) periferici, a loro volta popolati da un numero variabile di pc client (variabile da 10 a 100),
- n pc client di tipo roaming facenti capo ad utenti mobili su tutto il territorio mondiale (al momento circa 10)
- accessi esterni tramite pc client interconnessi ad internet

Per un sistema di questo tipo, gli aspetti principali tenuti in considerazione sono:

1. sicurezza
2. controllo e supervisione
3. affidabilità
4. replicabilità
5. performance

Il sistema ha sottostato alle seguenti direttive:

1. il cablaggio strutturato (rame o fibra) è stato ridotto al minimo indispensabile, sopperendo all'esigenza di connettività attraverso tecnologie alternative, compatibilmente con le necessità di banda e affidabilità richiesta dai servizi e applicazioni che dovrà sostenere e compatibilmente con i vincoli della struttura ospitante; in particolare il nodo di Pesaro è, date le dimensioni, stato attivato facendo ampio uso dell'infrastruttura wireless, mentre i due nodi di Roma Marchiafava e Forlanini per vincoli legati alla struttura portante schermante e per la presenza di cablaggio strutturato esistente sono stati attivati sfruttando quest'ultimo;
2. il sistema deve essere allo stato dell'arte per quanto riguarda le tecnologie utilizzate, comprendendo anche tecnologie ancora in stato "draft";
3. il sistema deve consentire la possibilità di trasloco in altra ubicazione in modo più facile possibile;
4. deve essere garantita la scalabilità verso l'alto delle soluzioni adottate e la replicabilità su siti differenti, avendone incamerato il know-how specifico dall'utilizzo anche sperimentale;
5. la sicurezza e la privacy devono essere parti fondamentali della progettazione, sia a livello strutturale che di politiche d'accesso.

Pertanto, tenuto conto di quanto sopra, il Gruppo di Sviluppo Informatico ha progettato ed attivato una infrastruttura come da schema sopra riportato che di seguito viene descritto nelle varie parti costituenti. In particolare viene descritto il nodo tipico di rete che, da un punto di vista del network, vede al centro un sistema firewall in grado di isolare una serie di zone le une dalle altre e di consentire l'interscambio dei pacchetti soltanto in base a precise regole definite. Rispetto ad una tradizionale suddivisione in rete locale, dmz, internet, il modello prevede ulteriori suddivisioni dei gruppi di apparati ed in particolare viene differenziata la zona cui appartengono i client locali dalla zona cui appartengono i server dalla zona cui appartengono i client remoti. Detta soluzione consente l'isolamento (in termini di sicurezza) dei server aziendali ed il controllo del traffico ad essi destinato,

tuttavia richiede l'utilizzo di firewall di recente concezione con elevate performance di processamento dei pacchetti.
Detto nodo è stato sviluppato completamente nella sede di Pesaro, mentre per le altre sedi attualmente presenti presso Roma Marchiafava e Roma Forlanini, è stata effettuata una opportuna replica parziale, in quanto a livello macroscopico i nodi sono interconnessi tra loro in una wan magliata mentre la connessione internet di questa wan viene gestita complessivamente dal nodo di Pesaro.

Zona Lan Utenti

I client sono stati tutti acquisiti con configurazione allo stato dell'arte (al giugno 2003) per l'utilizzo in ambito aziendale, pertanto relativamente alla postazioni fisse, le postazioni utilizzate hanno i seguenti requisiti minimi:

- processore di tipo pentium IV con velocità di almeno 2.4GHz, per garantire la massima compatibilità con software attuali e futuri
- ram almeno 512Kbyte
- dischi fissi da almeno 30 GByte
- lettore DVD-Rom quale nuovo standard di diffusione del software
- masterizzatore CD-Rom quale supporto standard di scambio documenti alternativo al floppy disk
- sistema operativo MS-Windows XP Professional, vista la rete e le caratteristiche dei server
- monitor LCD Flat 15"
- web cam e sistema audio 2 vie per l'implementazione della videoconferenza

Per quanto riguarda le postazioni mobili ed i criteri di selezione dei pc notebook, tenuto conto del chipset Intel Centrino, si è scelto di utilizzare detta tecnologia per le garanzie di massima leggerezza e durata delle batterie. Tuttavia, viste le necessità indicate nel paragrafo relativo alle connessioni wireless, si è selezionato un notebook che non implementasse nativamente le connessioni Wi-Fi (tutte, al giugno 2003, legate al solo standard 802.11b). Tali connessioni sono attivate invece via scheda aggiuntiva pc-card estraibile ed aggiornabile, con il fine di avere sempre l'ultima release in fatto di banda utilizzabile e standard di protocollo.
In questa zona sono state anche poste le stampanti di rete, comunque controllate dai server, ed il sistema telefonico integrato sulla rete informatica.

Zona Lan Server / Lan Demilitarizzata

Nella zona definita "lan server" e "lan demilitarizzata" sono collocati i server multifunzione relativi al nodo della sede. Detti server devono avere sufficienti requisiti di affidabilità, scalabilità, sicurezza dei dati a garanzia di un funzionamento (quasi) continuativo.
In particolare i server interni si occupano della gestione della sicurezza e monitoraggio della rete e degli accessi, dell'immagazzinamento di dati e documenti (compresi i backup giornalieri), della gestione operativa del workflow dei vari progetti e delle attività di segreteria. Questi server risultano isolati in una zona separata ad opera del firewall e risultano interrogabili dalle postazioni presenti sulla lan interna e dalla VPN esterna esclusivamente nei servizi strettamente necessari.
I server esterni (dmz) si occupano della gestione dei dati e documenti esposti ad internet, con particolare riferimento ai servizi di posta elettronica, alla navigazione web e al web hosting; anche in questo caso i servizi fruibili sono esclusivamente quelli strettamente necessari ad opera del firewall.

Per quanto riguarda le caratteristiche dei server, questi sono stati selezionati rispetto alle diverse esigenze delle due tipologie di nodi, gestionale e clinico.
Per i nodi di tipo gestionale i server hanno le seguenti caratteristiche minime (da riferirsi agli standard di mercato al giugno 2003):

- processore Pentium 4 2.4GHz
- slot pci con presenza di slot 64bit

- memoria 512MB (1GB ove necessario)
- dischi (RAID 1 o 5 ove necessario) con capacità utile di almeno 30GB
- formato tower

Per i nodi di tipo clinico i server hanno le seguenti caratteristiche minime (da riferirsi agli standard di mercato al settembre 2003):

- processore Pentium Xeon 2.8GHz (doppio ove necessario)
- slot pci con presenza di slot 64bit
- memoria 1GB (2GB ove necessario)
- doppio alimentatore ridondante
- dischi (RAID 1 o 5 ove necessario) con capacità utile di almeno 30GB
- doppia scheda di rete
- formato rack 19" con sistema di estrazione rapido

Detti sistemi sono stati alloggiati in armadi standard rack 19" da 42U, dotati di opportuna console di controllo rack mount 1U.

Tutti i server sono dotati di sistema operativo MS-Windows 2003 (per il primo installato SBS2000).

I server hanno a protezione dell'alimentazione elettrica sistemi UPS di opportuna potenza in grado di erogare energia elettrica per 10 minuti a pieno carico e capaci di essere interrogati via software tramite connessione seriale, usb o ethernet, per ottenere i parametri rilevati ed effettuare lo shutdown sicuro dei server ad essi connessi.

Nel dettaglio al momento risultano operativi:

n. 2 server multifunzione per la sede di Pesaro
n. 1 server dmz per l'interconnessione internet complessiva della wan
n. 2 server multifunzione per la sede di Roma

Sono in fase di allestimento n. 4 server per l'attivazione degli altri nodi e per funzionalità specifiche o di ridondanza.

Zona Internet / Tunnel

Questa zona è dedicata all'accesso internet tramite carrier esterni su protocollo TCP/IP; in questa zona fra l'altro vengono effettuati gli accessi dei client non direttamente appartenenti alla rete IME.
Di fatto questa zona ha diverse finalità:

1. gestire la connessione internet ai fini della navigazione web e della gestione della posta elettronica;
2. gestire l'interconnessione tramite VPN (tunnel IPSEC) con altri nodi appartenenti alla rete IME;
3. gestire l'interconnessione con postazioni mobili di IME, a loro volta connessi alla rete GPRS del paese su cui sono ubicati in quel momento (vedere di seguito), anch'essi tramite tunnel IPSEC;
4. gestire gli accessi di utenti esterni verso i servizi resi fruibili.

Attualmente ogni singolo nodo dispone di questa zona che viene gestita alla stregua di una qualunque altra zona fisica. Le uniche differenze si basano sulla necessità di creazione di interfacce virtuali di entrata verso il tunnel (funzionalità che sostituisce la presenza di una interfaccia fisica che connette una lan effettiva) e sull'assegnazione di range ip fittizi per gli utenti mobili che si collegano via tunnel su internet (identificati quindi

sia da un indirizzo ip fisico di volta in volta assegnato dal carter utilizzato, sia da un indirizzo ip virtuale assegnato una tantum all'interno della wan Ime).

Rete Wireless

La zona lan utenti, per rispettare i vincoli di progettazione, risulta composta ove possibile da una rete wireless per la connessione sia delle postazioni desktop che delle postazioni mobili (laddove le postazioni mobili sono all'interno dell'edificio entro copertura o nelle sue immediate vicinanze). Detta connessione per questioni di sicurezza e riservatezza dei dati deve necessariamente utilizzare una politica di cifratura del traffico più sicura possibile (al giugno 2003 lo standard di riferimento è il Wep (Wired Equivalent Privacy), attualmente in fase di migrazione verso WPA (Wi-Fi Protected Access).
Lo standard utilizzato è identificato dalla sigla 802.11g che, rispetto allo standard precedente 802.11b, consente un netto miglioramento in termini di velocità di trasmissione pur mantenendo una compatibilità degli apparati verso il basso. Detto nuovo standard prevede sulla medesima frequenza di 2.4GHz una banda nominale di 54Mb/s che, in caso di utilizzo di una chiave di cifratura di 128 bit, effettivamente attivata, consente un throughput reale di oltre 19Mb/s.

Gprs

L'evidente necessità di mobilità sul territorio fa sì che oltre alla connettività WiFi, utilizzabile in ambito LAN, si sia reso necessario una modalità di collegamento remoto nella più ampia libertà di movimento. Oltre quindi alla soluzione di un linea telefonica cablata, si è optato per l'utilizzo della tecnologia GPRS che si appoggia alla rete cellulare GSM con una banda massima paragonabile a quella di un modem telefonico (56Kb/s). In alternativa a questo tipo di connessione rimane comunque possibile veicolare il traffico generato dalle postazioni client utilizzando la rete fissa (Dial-Up, ADSL). In prospettiva si tenderà verso l'utilizzo dello standard emergente UMTS.
L'accesso alla rete IME avviene comunque tramite opportune politiche di VPN via IPSEC tunnelling con applicativi installati sui client stessi; in particolare l'applicativo utilizzato è Netscreen Remote Secure Client, che consente la configurazione di dettaglio di tutti i parametri connessi alle fasi 1 e 2 della negoziazione del tunnel in coerenza con i firewall presenti. Fra l'altro il tunnelling è trasparente per gli applicativi lato client, pertanto non è stato necessario effettuare modifiche o riconfigurazioni su questi client mobili. In questa situazione è fondamentale considerare la scarsa larghezza di banda disponibile, la discontinuità della connessione stessa: sarà fondamentale quindi applicare politiche di sincronizzazione cartelle relativamente ai dati semplici (documenti, tabelle, ecc..) ed utilizzare applicativi specificatamente progettati per connessioni con banda scarsa o fluttuante, oltre che considerare RDBMS affidabili su connessioni e transazioni complesse. Ad esempio Outlook 2003 utilizzato in abbinamento con Exchange 2003 supporta proprio connessioni di questo tipo e garantisce l'utilizzo di funzionalità che minimizzano la richiesta di banda e tempo di connessione.

Rete Powerline

Per quanto riguarda le postazioni telefoniche utilizzanti tecnologia VoIP e le stampanti di rete, le prime non possono utilizzare la rete wireless in quanto non sono garantiti i requisiti di stabilità temporale del sistema (le connessioni wireless possono avere brevi interruzioni di connettività legate ad una serie di fattori ambientali quali oggetti o persone in movimento, onde riflesse da differenti configurazioni della stanza, ecc.) indispensabili per veicolare fonia, mentre per quanto riguarda le stampanti di rete ad oggi ancora non sono presenti interfacce native in standard 802.11g.

Pertanto, laddove non è presente un cablaggio wired, i suddetti apparati sono connessi utilizzando la tecnologia definita powerline, che utilizza il cablaggio della rete elettrica quale supporto fisico per creare un bus condiviso, in base ad uno standard internazionale denominato HomePlug 1.0.1. Detto standard prevede una banda nominale condivisa di 14Mb/s (per ogni linea elettrica, ovvero per ogni fase su cui le varie prese elettriche insistono), cifratura a 56 bit DES (da attivare con considerazioni analoghe a quanto indicato nella parte wireless), una lunghezza della linea elettrica fino a 200m, la possibilità di definire dei livelli QoS (necessari per prioritizzare il traffico fonia su quello dati).
Al giugno 2003 il sito ufficiale dello standard HomePlug prevedeva una serie di costruttori, per la maggior parte ubicati negli Stati Uniti; in conseguenza di ciò e della relativa novità della tecnologia le apparecchiature proposte certificate per l'utilizzo con tensioni a 220V sono risultate quelle prodotte dalla società Corinex, distribuita anche in Italia. Non è stato considerato il sistema proposto al tempo da Enel, in quanto al tempo utilizzante una variante dello standard con capacità inferiori.
La verifica sul campo ha dimostrato che l'impanto elettrico esistente è elemento determinate in termine di affidabilità di questa infrastruttura di trasporto, il cui utilizzo rimane pertanto confinato a modeste necessità di banda quali appunto il traffico di fonia ovvero le necessità di stampa a livello di Small Office.

Apparati Attivi

Per ogni nodo di rete è stato necessario dotarsi di uno o piu' switch con i seguenti requisiti:

- sufficiente capacità di switching di livello 2
- porte ethernet / fastethernet
- eparazione logica delle prese di rete in sottoreti mediante assegnazione fisica e vlan tagging 802.11q, per evitare l'acquisto di switch separati e disporre di sottoreti eventualmente distribuite
- gestione della prioritarizzazione del traffico (costituito da dati, voce, multimedia, ecc) QoS via DSCP, in particolare con riconoscimento del sistema di telefonia NBX layer 2 (cfr. relativo paragrafo)
- gestione remota via web / telnet
- possibilità di upgrade del firmware
- controllo via snmp
- auto mdi/mdix
- capacità di stacking
- porte di espansione verso uplink su differenti media
- predisposizione per alimentazione ridondata

Firewall

La separazione logica delle zone individuate deve essere effettuato da un sistema firewall che prevede le seguenti caratteristiche:

- almeno 4 porte fastethernet relative a zone diverse
- throughput di almeno 100Mb/s
- almeno 20 tunnel vpn
- gestione client dial-up su vpn
- logica di routing
- politiche liberamente definibili

Struttura e distribuzione delle informazioni circolanti

Le informazioni devono essere ove possibile in formato elettronico (si punta ad escludere o ridurre al minimo la necessità della copia e della firma cartacea) e devono essere fruibili sia all'interno della rete IME (rete cablata o WiFi) che all'esterno (rete GPRS o internet).
Le informazioni ed i dati che giuridicamente devono essere in formato cartaceo devono essere comunque fruibili e ricercabili (tramite barcone), e indicizzate tramite sistema di archiviazione ottica.
La collocazione dei documenti elettronici è decentrata fisicamente (in una serie di Master Server) ma logicamente centralizzata ed organizzata gerarchicamente utilizzando la tecnologia Microsoft Active Directory, con le politiche di seguito specificate.
Dato l'ampio raggio d'azione dell'IME e la possibile situazione di temporaneo o forzato scollegamento dalla rete informatica, sono attivi sistemi di sincronizzazione dei dati (nell'ambito di cartelle condivise) affinché anche gli utenti scollegati possano avere nel proprio dispositivo fisso/portatile l'ultima versione di ogni proprio documento/cartella di lavoro aggiornata all'ultimo contatto on-line.
Ogni utente può accedere ad un'area personale in cui collocare tutti i documenti di propria proprietà e competenza (in senso informatico). Ognuna di queste aree può a richiesta essere suddivisa in due sottoaree, di cui una ad uso esclusivo e riservato dell'utente proprietario (sottoarea privata), mentre l'altra ad uso dell'utente proprietario con possibilità di consultazione (e quindi non modifica) da parte di altri gruppi di utenti da definire in base alle necessità (sottoarea pubblica).
Per la condivisione di insiemi di documenti (possibilità di modifica da parte di più utenti) a richiesta vengono create delle aree di scambio con accesso riservato a gruppi di utenti.
Importante inoltre la condivisione delle Rubriche e delle Agende, tutte centralizzate e consultabili o comunque sincronizzabili da remoto (notebook, cellulare, palmare), mantenute a livello aziendale dalla segreteria della Fondazione.
Sono incoraggiati gli scambi di messaggi, dati, video tramite protocollo SIP (Microsoft Conference Server e Microsoft Messenger).

Il sistema di Office Automation

Il sistema di organizzazione delle informazioni da e verso la Fondazione IME deve garantire una elevata dinamicità strutturale, capillare distribuzione verso i soggetti interagenti, mantenendo una alta recettibiltà nei diversi mezzi e formati di comunicazione. Necessita quindi di una piattaforma che unisca trasversalmente tutte le tipologie di sorgenti di dati (audio,video, immagini, fax, MMS, SMS, voice mail, email, ecc...) verso un rapido ed efficace utilizzo di questi all'interno/esterno dell' IME (informative ufficiali, scambio documenti, controllo, ricerca e sviluppo, formazione, CRM). Tale piattaforma, vista la mission di caratura internazionale della Fondazione, deve assicurare inoltre un'ampia portabilità e compatibiltà con i più diffusi network e sistemi di gestione dati ed una scalalabiltà sul traffico dati generato e generabile molto elevata. E' stata scelta la piattaforma Microsoft per la sua ormai nota caratteristica di standard "de facto" a livello mondiale. Il diffuso utilizzo della piattaforma Microsoft implica inoltre un minor sforzo formativo verso i possibili produttori e utilizzatori di informazioni/applicazioni lungo i nodi del network IME, producendo così un'infrastruttura informatica duttile ed adattabile a qualsiasi flusso informativo senza sbarramenti né strutturali né operativi.
Scegliendo come base di partenza Microsoft Small Business Server 2000, si sposa un'idea poli-funzionale mono-tecnologica non eccessivamente dispendiosa a livello di risorse hardware necessarie, altamente integrata e testata, integrando in maniera nativa:

- Sistema operativo (Windows 2000)

- Sistema di gestione messaggistica integrata (fax,sms,email,voice – Exchange 2000)
- Web server (IIS)
- Gestione database (SQL Server 2000)
- Controllo traffico internet (Internet security & acceleration server 2000)
- Servizio fax

Coerentemente dal lato client si è scelto di dotare tutte le postazioni di sistema operativo Microsoft XP Professional e del pacchetto Office XP professional.

Per quanto riguarda la produzione di documenti su carta, si è scelto di utilizzare stampanti laser con le seguenti caratteristiche

- formato A4
- direttamente connesso alla rete lan
- più cassetti di alimentazione
- sistema di gestione del fronte-retro
- risoluzione almeno 1200 dpi
- velocità di almeno 18 ppm

Per quanto riguarda le stampanti a getto d'inchiostro le caratteristiche risultano le seguenti:

- formato A4
- almeno 15 ppm nero, 12 ppm per il colore
- connessione usb

Infine per quanto riguarda la scansione di documenti esistenti, gli scanner dovranno avere le seguenti caratteristiche:

- risoluzione 1200dpi
- formato A4
- profondità colore 48bit
- connessione usb2

Sistema Antivirus

A protezione di tutto il sistema informatico risulta installato un prodotto antivirus a livello aziendale in grado di controllare capillarmente ogni possibile punto di infiltrazione di virus. In particolare il prodotto selezionato prevede:

- la scansione dei file locali tra cui i documenti di produttività individuale presenti sui client e sui server
- la scansione dei sistemi operativi
- la scansione del traffico email in ingresso/uscita in ogni livello gerarchico
- la scansione del traffico internet
- l'aggiornamento automatico via internet dei file impronta
- la gestione centralizzata di tutto il sistema e la supervisione e reportistica dello status

Tra i vari prodotti è stata selezionata la suite prodotta da Trend Micro, pertanto su tutti i sistemi server sono stati installati gli applicativi ServerProtect per il controllo delle condivisioni del file system, gli applicativi interscan per quanto riguarda il controllo del traffico snmp, ftp e http verso internet, gli applicativi Scanmail for Exchange per il controllo della posta elettronica. Sui client è stato installato l'applicativo Officescan controllato da un

sistema server centralizzato. Infine il sistema viene supervisionato dall'applicativo Control Manager per effettuare reportistica, per distribuire gli aggiornamenti a tutta la piattaforma ed eventualmente applicate automaticament politiche di Outbreak, ovvero di chiusura temporanea del sistema, in casi di particolari e localizzate diffusioni di virus su internet.

Sistema di Backup

L'architettura precedentemente indicata che comporta la centralizzazione di tutte le informazioni (sia i documenti prodotti da pacchetti di office automation, sia la messaggistica elettronica e via fax, sia le banche dati), richiede di sviluppare un'opportuna strategia di backup in grado di garantire un recupero dei contenuti in caso di fail di un singolo server.

In particolare la strategia di backup è effettuata sulla base delle seguenti regole:

- ogni backup (con verifica) avviene durante la notte a partire dalle ore 20.00 sul disco fisso in modalità raid 1 o 5 di un server apposito di stoccaggio ubicato in luogo differente dai server di produzione (ovvero un opportuno pc / server alternativo nella fase iniziale);
- ogni operazione di backup deve essere riportato su apposito log;
- ogni domenica viene effettuato un backup completo di tutte le suddette informazioni; detto backup viene ubicato su file differenti nominati Domenica1, Domenica2, Domenica3, Domenica4, soprascritti a rotazione; pertanto è possibile ottenere un ripristino on-line di file perduti fino a 4 settimane prima;
- ogni giorno della settimana (da lunedì a sabato) viene fatto un backup (detto backup incrementale) delle informazioni modificate rispetto all'ultimo backup (completo o incrementale), in file nominati opportunamente (lunedì, martedì, ecc.); il contenuto precedente viene cancellato. Detto backup consente a partire dal backup della domenica precedente e dai backup dei giorni della settimana precedenti di risalire comunque ad una situazione completamente aggiornata alla notte precedente;
- ogni primo lunedì del mese viene comunque effettuata una copia del backup della domenica precedente su un supporto rimovibile (cd-r ovvero dvd-r quando il volume dei dati raggiungerà una capacità non più gestibile su supporti cd) ed archiviata in luogo sicuro e differente.

Detto backup in questa prima fase di avvio è stato impostato per avvenire in maniera incrociata tra le server farm attive del network Ime (Pesaro e Roma), garantendo in questo modo la presenza di una copia di riserva su un nodo ubicato geograficamente in una posizione differente per poter far fronte ad una sitazione di disaster recovery.

Sistema di Supervisione

Per poter controllare le performance di una infrastruttura multisito e diagnosticare eventuali guasti o malfunzionamenti sulle singole connessioni, è stato necessario attivare un sistema di supervisione e monitoraggio costante di tutti i parametri caratteristici degli apparati presenti sulla rete.

Lo standard de-facto in questo campo prevede l'utilizzo della messaggistica SNMP nelle varie versioni (v1, v2c, v3), quantomeno limitatamente alle funzionalità di interrogazione dei parametri e generazione in caso di eventi caratteristici verso "trappole" opportunamente poste. Non sono state attivate le funzionalità di gestione e quindi modifica dei parametri dei parametri degli apparati via messaggistica SNMP per noti motivi legati alla scarsa sicurezza di questo approccio (le configurazioni verranno quindi svolte utilizzando altri protocolli più sicuri quali SSL).