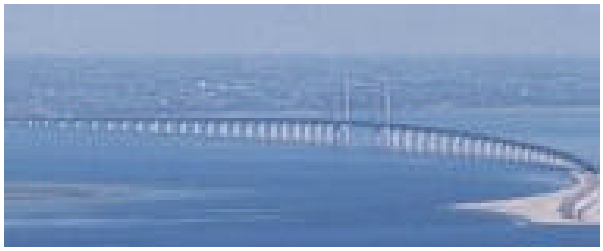
NORDUnet 2002: Serving the End User

Enrico Cavalli, Gianpiero Limongiello
CILEA, Segrate

Abstract
In aprile si è tenuta, a Copenhagen, la ventesima edizione della conferenza NORDUnet. Impressioni e riflessioni suscitatate dal convegno.

Keywords: Telematica, NORDUnet 2002, Networking, Ipv6, Fibre ottiche.



Premessa

Dal 15 al 17 Aprile 2002 si è tenuta a Copenhagen la ventesima edizione della NORDUnet Networking Conference. Tema dell'edizione di quest'anno: "Serving the End User" - servire l'utente finale. Forse troppo spesso chi lavora nel settore delle telecomunicazioni o del *networking*, si dimentica che in fondo ai cavi di fibra ottica ci sono persone che devono utilizzare servizi.
Molti sono stati i temi trattati in questa intensa tre giorni, ed è praticamente impossibile riassumere tutto in poche righe, ma basta visitare il sito www.nordunet2002.dk/ per scaricarsi le presentazioni in formato PDF. Cercheremo allora di mettere in luce alcuni temi particolarmente interessanti per suscitare qualche riflessione.

Il Nome della Rete

NORDUnet è il nome della rete posseduta, gestita ed utilizzata dai paesi scandinavi per i loro accessi internazionali.
Non per niente NORDUnet, nel senso invece di conferenza annuale, viene ospitata a turno, dai cinque paesi "proprietari" della rete: Danimarca, Finlandia, Islanda, Norvegia e Svezia; ognuno di essi possiede e controlla a sua volta una singola rete di ricerca di ambito nazionale[1]. L'evoluzione tecnologica delle reti scandinave è storicamente sempre stata molto veloce ed in genere qualche passo avanti rispetto alla media europea; di molti rispetto la realtà italiana. Volgendo ottimisticamente questo in un vantaggio, cerchiamo di descrivere quale sia la loro situazione attuale, per capire meglio dove, con tutta probabilità, andremo anche noi nei prossimi anni.

Con scelta perfetta per riprendere il discorso concluso due anni prima, tra le0 *slide* iniziali della presentazione **Nordic Networks** di Peter Villemoes[2], General Manager di NORDUnet, vi era l'ultima, intitolata "Plan for next year", della sessione di NORDUnet 2000. I piani prevedevano per la fine del 2000 velocità di 2.5 Gbit per il backbone nordico, per la connessione a quello europeo (il neonato Gèant) ed anche per le connessioni da e verso gli USA, mantenendo

[1] Forskningsnet (DK), FUNET (FI), RHnet (IS), UNINETT (NO), SUNET (SE)
[2] www.nordunet2002.dk/sessions_a/#

su questo una banda garantita per il traffico di ricerca.
I piani sono stati più che rispettati (vedi Fig. 1), grazie anche alla crollo generalizzato dei costi di connettività avutosi negli ultimi tre anni: l'attuale backbone a 2.5Gbit per la rete scandinava, ottimizzato con quasi tutti i cammini ridondati, passerà a breve ad una velocità complessiva di 5Gbit[3] con un raddoppio, relativamente semplice, degli ultimi due link NO-SE e DK-SE ancora a *solo* 2.5Gbit. Il concetto di ridondanza è applicato intensivamente su questa infrastruttura di rete: link, circuiti, apparati di rete e persino le locazioni fisiche, mantenute, per i link doppi tra due nazioni, a vari chilometri di distanza tra di loro, per sopportare anche eventi di natura potenzialmente catastrofica. Forse anche per un'attenzione innata tipica di questi paesi a cautelarsi da condizioni particolarmente avverse, un approccio del genere fornisce una garanzia intrinseca di buon funzionamento, oltre alle disponibilità di notevolissima banda trasmissiva.

Chi paga?

Grazie al crollo dei prezzi della connettività, i costi di NORDUnet pare abbiano imboccato un circolo virtuoso che ha consentito di incrementare le risorse, diminuendo i budget: i costi sono infatti passati dai venti milioni di Euro annui, superati nel 2000, ai quindici pianificati per il 2005: indubbiamente un notevolissimo risparmio. I costi di connettività internazionale sono sostenuti anche da organizzazioni con cui NORDUnet ha accordi di *partnership*; in particolare la Comunità Europea sostiene il 50% dei costi di connettività a Géant ed il 50% del backbone 6NET[4] (backbone sperimentale del nuovo protocollo IPv6), mentre la ***N**ational **S**cience **F**oundation* sostiene il 35% dei costi di connettività alle reti della ricerca statunitensi.

Ma per cosa?

Come nel resto del mondo, anche qui l'utilizzo dei *backbone* nazionali è dedicato sia alle attività classiche del mondo della ricerca (scambio dati, accessi remoti) sia a tutte quelle emergenti degli ultimi anni, molto più affamate di banda trasmissiva di un semplice *file transfer*.
Con una rapida panoramica, partendo dalla struttura danese, a 622Mb già dal 2000, dove si caratterizzano attività sia legate a 6NET che dedicate al video digitale, si passa alla Finlandia dove ad esempio, grazie anche ad un backbone nazionale a 2.5Gb, tutte le sessioni del Parlamento nazionale sono trasmesse (con tecnica *multicast*) da FUNET-TV. Di rilevanza notevole, inoltre un progetto di identificazione personale, via PKI, legato al mondo dell'istruzione superiore (università, politecnici, scuole di specializzazione). L'Islanda, fisicamente così distante e paesaggisticamente ostile, dispone comunque di un backbone ad 1Gb nella capitale e di connettività in fibra ottica in via di completamento in varie città. La rete nazionale della ricerca, RHnet, è operativamente gestita nell'ambito dell'università di Reykjavik. Norvegia e Svezia completano adeguatamente con progetti che spaziano dall'educazione a distanza della *"NET University"* svedese ai campus universitari completamente *wireless* della Norvegia.
Il bilancio finale tra costi e benefici, in ogni caso, racconta di circa 39.5 milioni di Euro all'anno suddivisi tra 573 istituzioni, con oltre 1.010.000 utenti finali. Cioè circa 39 Euro a testa all'anno. Per quanto descritto, che non è nemmeno tutto, voi non li spendereste?

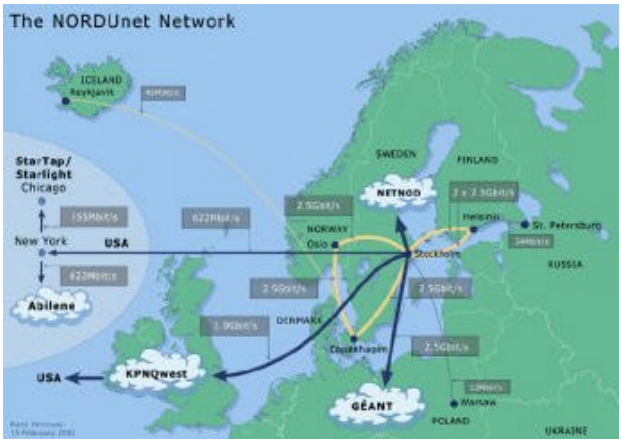


Fig. 1 - L'attuale rete Nordunet

IPv6 e l'IP everywhere

Brian Carpenter, Distinguished Engineer di IBM, ha evidenziato alcuni dei problemi che affliggono Internet. Se l'enorme successo della "rete" è sotto gli occhi di tutti, non possiamo nasconderci di fronte ad alcune questioni tuttora aperte, prima tra tutte la famosa mancanza di scalabilità di IPv4. Nel 1992 ci si è accorti che presto lo spazio di indirizzamento a 32 bit di IPv4 sarebbe finito, ed era chiaro che sarebbe stato necessario "inventarsi" un nuovo standard. La risposta esiste già, per lo meno è standardizzata dal 1997, si chiama IPv6 ed è la

[3] Rimane fuori l'Islanda, attualmente collegata solo a 45Mbit
[4] www.6net.org

chiave per avere finalmente l'IP *everywhere*, dal PC alla lavatrice.
Certo è che IPv6 stenta a decollare, vuoi perché la migrazione ha dei costi notevoli, vuoi per l'inerzia mentale degli operatori del settore. Siamo in molti ad essere ostinati conservatori, non c'è dubbio, anche al CILEA, forse perché forti di un'intera classe B di indirizzi IP non siamo afflitti e quindi sensibilizzati dai problemi che il sempre più diffuso NAT si porta dietro. Molte aziende non vogliono implementare il nuovo protocollo: d'altra parte di quali incentivi strategici dispongono per compiere questo utile ma faticoso passo? Sarebbe un po' come cambiare numero di telefono: nessuno lo farebbe se non costretto o incentivato.
Nel corso della conferenza è emerso questo punto chiave: i governi dovrebbero in qualche modo incentivare il passaggio ad IPv6. Forse questo è l'unico modo per smuovere le acque.
Col nuovo protocollo IP finalmente anche il mostro frigorifero potrà connettersi ad Internet e collegarsi al supermercato per ordinare le cose che mancano in casa. Questo scenario fa riflettere perché porta con sé ovvie problematiche di sicurezza. Cosa accadrebbe se il vicino di casa decidesse di riconfigurare il nostro il frigo tramite SNMP? E se il figlio aspirante hacker del dirimpettaio volesse sperimentare sul nostro asciugacapelli il firmware di un'aspirapolvere?

La questione sicurezza

Proprio la sicurezza è stato tema caldo del convegno e tanti sono stati gli interventi interessanti, cito tra gli altri quelli di Ingrid Melve[5] e un'interessante discussione sulle PKI di Pekka Linna[6]. In sostanza è ormai diffusa la consapevolezza che un Firewall non è necessariamente sinonimo di sicurezza, così come avere la propria Intranet nascosta dietro un NAT non è vera sicurezza, nonostante le promesse di alcuni *vendor*. Ad esempio si possono scaricare comunque virus da siti web o dalle mail e trasmetterli verso altre reti. Se ci pensiamo bene, il NAT per sua natura impedisce molti controlli di autorizzazione al livello network, oltre a rendere difficoltosi alcuni protocolli applicativi non propriamente *client/server*. La sicurezza è un altro paio di maniche, è un processo più che un prodotto che si acquista da qualche *vendor* blasonato, per citare una famoso motto. Se da un lato c'è questa consapevolezza negli operatori del settore, bisogna anche dire che dalla conferenza non sono uscite soluzioni del problema sicurezza.
Si può però fare un'interessante considerazione: se è vero che Internet diventerà un bene di *commodity* - paragonabile per intenderci a luce, acqua, gas e telefono - allora gli ingegneri di Internet dovrebbero essere in grado di assumersi responsabilità che vanno ben al di là del breve termine: dovrebbero progettare i protocolli con maggiore lungimiranza rispetto al passato. Dovrebbero essere in grado di dare garanzie, così come un ingegnere civile ha certi obblighi quando progetta un edificio. Tanto per ricordare un famoso protocollo che usiamo tutti i giorni, consideriamo SMTP utilizzato per spedire mail: è stato un grave errore non dotarlo fin dall'inizio di una parte di autenticazione del mittente. Oggi conosciamo molto bene i problemi generati dallo SPAM o dai vari virus in circolazione che abusano sì di bachi di alcuni programmi di posta, ma sfruttando anche questa intrinseca mancanza di autenticazione di SMTP.
Tanto per capirci sulla difficoltà di modificare a posteriori i protocolli, immaginiamo di trasportare il problema alla posta ordinaria. Cosa succederebbe se, per motivi di autenticazione e di sicurezza, si decidesse di apporre l'impronta digitale del mittente su un piccolo rettangolo, sporgente per due centimetri da ogni busta?
La scusa citata sempre è nota e comprensibile: finché Internet era per pochi enti accademici o di ricerca, ci si "conosceva tutti" e non era fondamentale inserire la sicurezza all'interno della rete o dei protocolli che ci viaggiano sopra. Forse chiamarla scusa è persino irriverente nei confronti dei pionieri di Internet. Ma ora che l'epoca del Far West è finita occorre essere più lungimiranti e responsabili nel disegno dei protocolli e nella scrittura dei programmi che poi li utilizzeranno.

Fantasia al potere

Immaginate ora per un attimo la pubblicità più avveniristica che vi viene in mente. Adesso passate allo spot più futuribile. Per finire, pensate al videogioco più tosto. Lasciate perdere, non avete fantasia. Non ci credete? Provate ad ascoltare il prof. Gerald Q. Maguire Jr.[7] del KTH svedese e poi ne riparliamo…

Partendo da solidissime basi teoriche, un certo numero di anni di studio, un titolo apparentemente privo di *appeal* come *"Personal Compu-*

[5] Resource Control the AAA way: Ingrid Melve, Uninett (slide non disponibili nel momento in cui scriviamo)
[6] PKI: Pekka Linna, CSC/FUNET
www.nordunet2002.dk/powerpoint/b_janne_erstattesaf_pekka_linna.pdf

[7] www.it.kth.se/~maguire/

ting and Communication: It is more than just networking of mobile devices" e da un inizio ingannevolmente noioso, la presentazione è esplosa nella seconda metà su idee e concetti, forse non nuovissimi, ma quasi banalizzati qui nella loro fattibilità tecnica con, a dimostrarlo, le foto nei prototipi costruiti. Cinque anni fa.
La teoria presentata nelle prime diapositive, serviva a gettare delle solide basi, come un buon primo piatto va giudicato anche nell'ottica della portata principale.
Partiamo quindi dalla Legge di Cooper[8]: la banda delle trasmissioni radio è, di fatto, raddoppiata ogni due anni e mezzo dal 1896[9] ad oggi; la regola vale quindi da più di cent'anni. Continuando di questo passo potremmo superare velocità trasmissive dell'ordine dei 10^{18}bps intorno al 2091. Gli standard della sottoclasse IEEE 801.11x prevedono già oggi, per le Radio-LAN (WLAN) velocità tra i 23 ed i 54 Mbps (a titolo di esempio ricordiamo che la vecchia, cara, buona rete Ethernet su mezzo condiviso ha un limite fisico nei 10Mbps, 10^{7}bps). A ciò aggiungiamo che un singolo chip radio costa intorno ai 10 dollari e che lo standard UWB, Ultrawideband, ha già avuto negli States una regolamentazione in questo febbraio; non solo: Intel ha già dimostrato la fattibilità pratica dei 100 Mbps, confidando a breve di poter raggiungere i 500, con un consumo elettrico atteso bassissimo.
La prima idea è quindi quella di estendere il *concetto* di radio, facendone un oggetto di minimo consumo elettrico, di architettura essenziale, fisicamente delocalizzato; in qualche senso ubiquo. La seconda idea alla base proviene dal *Mobile IP*: un modo per fornire connettività Internet non fissa; che sopravviva al movimento, ai cambi di sottorete e di luogo. Una rete *Mobile IPv6*, inoltre, garantirebbe come già visto, IP davvero per tutti (verrebbe quasi da dire IP-IP, IP-IP, Urrà!).

Antropocentrico

Ora comincia il bello. Partiamo da un punto di vista, lo smontiamo, prendiamo i pezzi e li rimontiamo diversamente. L'attuale interazione uomo-macchina è in realtà focalizzata sulla macchina piuttosto che sull'uomo. Le macchine, inoltre, hanno solo una vaghissima idea (diciamo così) di dove esse siano, di chi le stia usando o se, per esempio, l'utente e "padrone" sia "ancora lì". L'idea di Maguire è di capovolgere il concetto: diamo alle macchine dei sensi (o meglio, dei sensori) e la consapevolezza della presenza umana. Non basta, ampliamo l'idea. L'uomo indossa la propria interfaccia, ma la macchina rende tale interfaccia coerente attraverso tutte le applicazioni, non perché ogni applicativo supporti quella interfaccia, ma piuttosto perché l'interfaccia (cioè la presenza umana) fornisce la consistenza necessaria. Per quel poco che è stato dato di comprendere dal geniale professore, il senso dovrebbe essere di mettere l'uomo al centro dell'attenzione della macchina e non viceversa. Inviare poi, come nei fatti è avvenuto, dei sistemisti ad ascoltare questa teoria oscilla tra il dantesco contrappasso e la cattiveria informatica.

Ma concentratevi, che adesso arriva la parte divertente. Dare ad una macchina la consapevolezza della presenza o dell'assenza di una persona, del suo interagire qui ed ora, potrebbe fare esplodere il concetto di "personalizzazione del contesto" (ricordate che al centro mettiamo la persona, non la macchina). Una semplice banalizzazione, ma nota e sotto gli occhi di tutti, è rappresentata dai controlli di accesso basati su computer: in qualche modo la macchina "sa" chi, quando e da dove sia entrato o uscito da un ambito ben definito. Riuscite ad immaginare invece un *badge* dotato di telecamera, audio bidirezionale, sensore di luce, misuratori di temperatura ed umidità, di accelerazione lungo i tre assi, connessione infrarossi, completo di 1MByte di *flash memory* ed uno di SRAM? Maguire non si è limitato ad immaginarlo, l'ha fatto; nel '97. E dalla foto presentate l'oggetto era grande come un pacchetto di sigarette *light*. Non di più.
L'idea del 2002 è quella di estendere questo "oggetto" (non è chiarissimo come chiamarlo se non ricorrendo all'anglicismo di recupero *device*), personalizzarlo e farlo diventare qualcosa che conosciamo, di cui non abbiamo paura alcuna, visto che lo indossiamo da almeno una cinquantina d'anni: un orologio da polso. Lo metti la mattina e lo dimentichi; non lo punti, non lo clicchi, non lo trascini ne' tantomeno lo configuri. Funziona e basta; al limite si ricarica. Tecnicamente il progetto prevede invece *display* multimediale, processore a 32 bit, *memory file system*, connessione *wireless*, audio, microfono, sistema operativo *multithread*, XML/HTTP/TCP/IP. Nelle versioni a seguire aggiungeteci sensori di

[8] Si veda, a tale proposito:
www.arraycomm.com/Technology/coopers_law.html
[9] Anno in cui Marconi ricevette il primo brevetto per il telegrafo senza fili

movimento, di parametri biologici[10] o biometrici, la sicurezza della crittografia e di *smart* SIM.
Certo, in molti posti dove la sicurezza è un obbligo questi concetti sono come manna dal cielo. Ma parliamo invece di vita più comoda: che direste di soggiornare in albergo senza la necessità delle operazioni di *check-in* o *check-out*? Della possibilità che ad usare la vostra telecamera digitale siate solo voi? Solo voi davvero, perché anche se vi rubassero il *badge*, (domani orologio e magari dopodomani orecchino) i parametri biologici per l'accesso sono solo i vostri?

La solita zuppa? No, Internet a barre

Bene, capito di cosa stiamo parlando, adesso voi avete indossato uno o più *device*; aprite il frigo e il vostro *scanner* legge il codice a barre della scatola Campbell che risiede lì ormai da mesi. Si collega (il *device*, non la zuppa) a www.airclic.com per ottenere tre nuove ricette possibili con la Zuppa Campbell, oltre alla conferma che con questa scatola i punti Campbell accumulati vi danno diritto ad una confezione da 12 bicchierini da rosolio (che peraltro nessuno beve più). Il sistema si accorge ovviamente che la vostra zuppa comunque è scaduta da tempo e vi avvisa che se è ancora lì settimana prossima, vi manda direttamente i NAS).
Le uniche due cose vere di questo paragrafo sono il sito web; e che tutto si possa già fare a costi perfettamente accettabili e senza nessun problema tecnico.
Lo scenario è così forte che è molto più facile chiedersi quali siano gli svantaggi che i vantaggi di un mondo simile. Se nella vostra vita avete letto almeno tre romanzi di fantascienza, sapete già tutte le risposte. Ma anche il professor Maguire che, al contrario di come potrebbe sembrare, non è affatto un fautore del Grande Fratello ovunque, tutt'altro. Crittografia e sicurezza per tutti sembrano essere le sue parole d'ordine (tra l'altro native nel protocollo IPv6), oltre a *traffic pattern hiding*, *location hiding*. Ancora il controllo all'individuo, non alla macchina.
Dopo tutto, avendo appena illustrato il concetto di "polvere intelligente" (*Smart Dust*) cioè ricevitori radio di dimensioni paragonabili a granelli di polvere e come tali fluttuanti a tempo indefinito, connessi ad una *wireless* LAN, la frase "anche i muri hanno orecchie" comincia ad assumere più nuovi e sinistramente reali significati. E se questo non riguarda il potere …

[10] Immaginate di fare un esame medico senza accorgervene e di avere i risultati in mezz'ora, già valutati dal vostro medico e completi di prescrizione.

La crisi delle telecom

Il futuro non ci riserva solo queste belle ed astratte considerazioni. Stando ad Yves Poppe di BCE Teleglobe[11], nel futuro dovremo non solo disegnare protocolli più sicuri, ma anche scavare e stenderci la fibra da soli. Ve le immaginate le riunioni condominiali che potrebbero scaturirne? Questo perché le telecom di tutto il mondo sono in crisi, e non possono a breve portarci la fibra in ogni casa. Avremo quindi il forno con IPv6 - forse - ma non avremo un cavo per collegarlo ad Internet. O meglio: avremo i soliti doppini telefonici, le linee ISDN, le varie xDSL, ma la fibra in ogni casa ce la sogneremo ancora per un po'. A meno di affittare una ruspa per scavare, si intende.
Ricordate l'epoca della gallina dalle uova d'oro? Quando bastava mettere un che di tecnologico nel nome della propria azienda per essere quotati in borsa e fare miliardi delle allora Lire o milioni di Dollari? Purtroppo, o per fortuna - dipende dai punti di vista - quei giorni sono finiti. Anche le telecom hanno ovviamente approfittato dell'euforia generale per espandersi. Tutti gli analisti dicevano che bisognava espandersi, che la capacità di Internet era sempre insufficiente. Così i vari operatori hanno iniziato a stendere cavi transoceanici, a cablare cittadine e metropoli. E ora? Ora non ci sono dati che passano per tutti questi cavi, ecco qual è la realtà.
La domanda è di gran lunga inferiore all'offerta: addirittura una stima di Merrill Lynch & Co. comparsa su Business Week del 9/4/2001 affermerebbe che viene sfruttato solo un misero 2.5% dell'intera capacità di questa enorme rete che si è venuta a creare. In realtà studi più recenti attestano questo utilizzo intorno al 5%/10%. In ogni caso le telecom hanno investito molto negli anni passati e ora si trovano costrette a svendere la propria capacità per ragioni di mercato.
Un altro fattore che ha giocato a sfavore delle telecom è stato l'ignorare la multipolarità che avrebbe avuto Internet. Agli albori della sua diffusione commerciale, Internet era vista come un mondo USA-centrico. Oggi sappiamo che non è così: in Giappone ad esempio l'80% delle informazioni cui si accede in Internet è locale. Quindi forse non serviva investire in grandi capacità transcontinentali quanto ampliare l'infrastruttura locale.

Conclusioni

Insomma, finora non abbiamo detto niente di positivo: è più facile distruggere che costruire.

[11] www.nordunet2002.dk/powerpoint/a_yves_poppe.pdf

Speriamo però di aver dato qualche spunto di riflessione ai pazienti lettori che ci hanno seguito fin qui. Trovate tutto nelle presentazioni sul sito della conferenza e speriamo di incontrare quelli che abbiamo incuriosito alla prossima edizione, in Islanda. Niente paura: l'appuntamento è per Agosto 2003, così forse non gelereremo.