Packet Radio in TCP/IP

di A.Tiziano Demaria – IW2MLN –

(Prima Parte)

Dopo qualche anno di "fermo" dell'attività radio in TCP/IP, torniamo a parlarne ora, in quanto non soltanto sono riprese le sperimentazioni ma si è anche messa in moto l'attività di riprogettazione e miglioramento della rete radio digitale TCP/IP.
Per comprendere meglio in cosa consiste tutto ciò, è forse bene fare un briefing al fine di chiarire sia le terminologie usate, che comprendere le scelte che si sono fatte. E per farlo è necessario conoscere almeno i principi che governano una rete.
Anzitutto un po' di Storia recente.
Pino Zollo I2KFX era il Coordinatore Nazionale della rete TCP/IP. Abdicò in quanto si trasferì definitivamente, con famiglia, in Paraguay. Il sottoscritto, che già si era attivato molto fortemente, ne prese l'incarico per sua diretta nomina, al fine di continuare l'opera condotta da lui e dai suoi collaboratori: i Numeratori Regionali, cioè quella schiera di persone addetta all'assegnazione ed alla gestione della numerazione IP.
Una sera ci incontrammo a casa sua, in quel di Monza, ed ebbi modo di esporgli il progetto di ristrutturazione della rete, che in queste pagine vi espliciterò.
Fu entusiasta della cosa ed iniziai così il mio lungo e tortuoso cammino in questa avventura, insieme agli altri numeratori zonali.

PRELIMINARI

Iniziai dalla Lombardia. L'allora rete era costituita da una serie di server (pochi, in verità) e da un certo numero di nodi. La numerazione era stata assegnata in modo sequenziale e senza nessuna particolare politica, a causa del ridotto numero di utenti e di bassissimo traffico.
Una struttura del genere però, sebbene soddisfacente le esigenze dei tempi, non era e non è assolutamente in grado di soddisfare le esigenze attuali. Non solo: essa non era costituita affatto con una struttura vera di rete, ma come una posa in opera di oggetti "linkati" tra loro in modo casuale e secondo le politiche della rete classica packet, giammai secondo le più esigenti e logiche politiche di una rete IP.
Decisi allora di applicare le politiche di rete cassando la vecchia rete e riorganizzandola in toto, applicando il tutto ad una sola regione al fine di testare le apparecchiature ed ottimizzare i percorsi risolvendo tutti i problemi che si fossero presentati. Dopo aver fatto ciò, se gli esiti si fossero mostrati positivi, avrei contattato tutti gli altri numeratori regionali esponendo loro tutti i dati ed avrei concordato così l'estensione della politica di Zona 2 a tutte le altre regioni.
Iniziai pertanto a coinvolgere i maggiori SysOp della già presente rete packet, quelle persone che hanno dimostrato un certo grado di serietà e di competenza tecnica in materia di reti, tale da riuscire a supportare la nascita della nuova rete.
Contattai pertanto il gestore del sistema principale lombardo: Paolo IK2NHL, con il quale decidemmo di riunirci con altre persone del mestiere: Stefano IW2KXA, Matteo IW2NAW.
In seguito si unirono al progetto: Claudio IW2FER e Valentino IW2GUR.
Ci suddividemmo i compiti su chi di noi avrebbe dovuto aprire i servers e su chi, invece, si sarebbe occupato della gestione.
Sfortunatamente IW2KXA lasciò il gruppetto circa sei mesi più tardi a causa di suoi pressanti impegni di QRL. Idem dicasi per IW2NAW che comunque continua a seguire con estremo interesse l'andamento della rete.

Dopo avervi "narrato" brevemente come nacque l'organizzazione di rete in zona 2 Lombardia, vediamo nel dettaglio COSA È una rete, com'è costituita, come funziona, come abbiamo applicato le tecniche/tecnologie al Packet Radio, quali sono le modifiche introdotte rispetto alla rete pre-esistente, sino a giungere a capire: **cosa debbono fare gli utenti per connettersi ad essa.**
Credo sia estremamente necessario per tutti voi, avere un'infarinatura sui concetti di rete di modo che possiate quantomeno "intuire" le ragioni che portarono a determinate scelte che si sono rivelate piuttosto interessanti oltre che valide, come quella inerente la suddivisione zonale.
Vediamo il significato di alcuni termini che userò sovente e alcune nozioni fondamentali sulla costituzione di una rete. Non descriverò l'intera terminologia, ma solo quella più comune che sicuramente avrete già sentito.

TERMINOLOGIA

OSI – Open Systems Interconnection.
Interconnessione di sistemi aperti.
È lo standard deciso dall'ISO (International Standards Organizzation)

TCP – Transfer Control Protocol, Protocollo di Controllo Trasferimento.
É il protocollo che cura l'arrivo integro a destinazione dei dati.

IP – Internetworking Protocol, Protocollo di intercomunicabilità tra reti.
È il protocollo che si occupa di effettuare l'interconnessione dei dati (DataLink) tra le macchine. Si avvale di indirizzi numerici IP.

DNS – Domain Name Service, Servizio dei Nomi di Dominio.
È il servizio che consente di capire quale numero IP è associato ad un determinato dominio. Consente, ad esempio, all'utente di poter effettuare una chiamata (call) ad un indirizzo detto URL (Uniform Resource Locator). Ad esempio se si effettua una query al dominio http://iw2mln.2.it.ampr.org, il DNS converte questo nome in un numero IP che è: 44.134.160.9.
Il Domain name è nome dominio e indica la parte destra di un nome completamente qualificato (FQDN = Fully Qualified Domain Name), costituita a partire da destra, dal dominio internet, dall'eventuale sottodominio e dal gruppo o rete a cui il computer è collegato.

Esempio di nome_domino_completamente_qualificato:

iv3ium.3.it.ampr.org

Dove: *iv3ium* è il nome_host

Mentre: 3.it.ampr.org è il nome di dominio

GATEWAY o ROUTER – Letteralmente: Porta di Transito.
È il sistema che permette a più sottoreti (subnets) di tipo diverso di colloquiare tra loro, ossia permette l'interscambio di dati.

REPEATER – Ripetitore digitale di dati.
Serve unicamente per rigenerare la qualità del segnale in modo da servire altre zone altrimenti non raggiungibili.
Mentre per il Gateway (abbreviato: GW) necessita un numero IP per ogni interfaccia configurata, per il repeater non è in alcun modo prevista l'assegnazione di un IP.

SMTP – Simple Mail Transfer Protocol. Protocollo di Trasferimento ed Invio della Posta.
È appunto quel protocollo che gestisce ad interim (l'invio) della posta elettronica (E-MAIL). Esso si avvale di un MTA (Mail Transport Agent) quale Sendmail, Smail, Qmail ed altri, per inoltrare la messaggistica generata con un MUA (Mail User Agent) quali: Outlook Express, Eudora, Il messenger di Netscape, Pine e così via.

POP – Postal Office Protocol.
Protocollo di recapito della posta in arrivo. Attualmente il uso la versione 3 ,(POP3).

HTTP – HyperText Transfer Protocol.
Protocollo di trasferimento di testo ipertestuale.
È il protocollo che si occupa della gestione delle pagine HTML (HyperText Markup Language), ossia delle pagine note come "pagine WEB", che costituiscono tutti i siti Internet.

FTP – File Transfer Protocol.
Protocollo di trasferimento dei files.
In breve è quel protocollo che permette di prelevare files e programmi. Per intenderci: è l'equivalente del vetusto YAPP (Yet Another Packet Program).

INTRANET
Rete del tutto simile ad Internet ma direttamente **non** connessa a quest'ultima (tipo le reti aziendali).

LAN – Local Area Network, Area di rete Locale
Si indica una rete non estesa geograficamente ma definita in genere in un unico stabile o in un isolato.

MAN – Metropolitan Area Network, Area di Rete Metropolitana.
Si indica una rete estesa entro i confini cittadini.

WAN – Wide Area Network, Area di Rete Geografica.
Si indica una rete geograficamente estesa: regionale, nazionale, mondiale.

LIVELLI OSI

Si sente spesso parlare di questi "livelli" (Layers), avendo già detto cosa significa la parolina: OSI, vediamo nel dettaglio di cosa si tratta.
Lo standard OSI è stato sviluppato dall'ISO (International Standard Organization) con lo scopo di definire le regole con cui i produttori debbono implementare i protocolli hardware e software. Il modello OSI è composto da sette livelli.
Ciascun livello è gestito da protocolli, che vedremo poi riassunti in una tabellina. Codesti protocolli comunicano tra loro seguendo una precisa gerarchia.
Partendo dal primo livello sino al settimo, in ordine crescente ed in particolare riferimento all'uso radioamatoriale, essi sono così descritti:

Livello 1: FISICO.
Definisce la modalità con cui si deve inviare i dati su una linea, cioè trasformare ciò che giunge dagli altri livelli in impulsi elettrici od ottici: TNC, BayCom, Radio, L.A.S.E.R., nonché le modalità con cui comunicano: livelli di tensione, eventuali frequenze, modalità d'emissione e così via. Un esempio sono: l'RS-232, AFSK, G3RUH, GMSK etc…

Livello 2: LINK DATI.
È la famiglia di protocolli che consente la connessione fisica tra le macchine. AX.25 ad esempio, è un protocollo che si cura di questa fase. Esso si premura solo di realizzare il "condotto fisico" in cui fluiranno i dati. Metaforicamente, diciamo che esso è il binario di una ferrovia, su cui viaggerà un treno carico di dati.

Livello 3: RETE.
Famiglia di protocolli che cura il DataLink tra i sistemi. IP è il protocollo che, sempre in base alla precedente metafora, funge da "treno" in cui i dati viaggiano.

Livello 4: TRASPORTO.
È la famiglia di protocolli che si occupa di assicurare l'integrità dei dati. Essi ne garantiscono l'arrivo a destinazione. A questa famiglia appartengono: TCP e UDP.
Qui è necessario effettuare una piccola digressione.
A differenza di AX.25, TCP non necessita del pacchetto di NACK (Not Aknowledge cioè: non riconosciuto). In pratica, mentre nelle trasmissioni AX.25 classiche per ogni pacchetto trasmesso e mai giunto a destinazione, il destinatario invia al mittente un "avviso" di non avvenuta ricezione, in TCP ciò non succede. Esso riceve solo pacchetti di ACK, cioè di avvenuta ricezione.
Come può allora, il mittente, sapere se un pacchetto non giunge a destinazione e quindi reinviarlo ?
È abbastanza semplice: se entro un certo periodo di tempo, da quando ha inviato il pacchetto al destinatario, non riceve da esso l'ACK, allora provvede ad inviarlo nuovamente.
Questo "periodo di tempo" si chiama RTT: Round Trip Time.

Livello 5: SESSIONE.
È il protocollo che consente di effettuare la connessione logica tra due applicativi che debbono comunicare per gestire/controllare il data transfer.

Livello 6: PRESENTAZIONE.
Definisce un formato comune dei dati. È necessario allorquando i computers che comunicano usano formati dati differenti. Ad esempio tra un mainframe ed un PC.
I protocolli di questo livello trasformano i dati in un formato comprensibile agli utenti finali. Questo livello si occupa quindi di:

- Codifica dei dati;
- Compressione dei testi;
- Crittografia;
- Conversione di formato;
- Gestione di terminali virtuali;
- Gestione di files virtuali;

Quindi si rende un dispositivo il più possibile indipendente da un altro. Ad esempio se un terminale usa il formato VT100 ed un altro il formato VT52, essi comunque possono comunicare tra loro in modo intelligibile

Livello 7: APPLICATIVO.
Questo livello è quello a diretto contatto con i programmi applicativi (applicazioni). Cioè ciò che gli utenti normalmente usano per poter esercitare la loro attività in rete.
Esso comprende i protocolli tipo FTAM per il trasferimento dei files e X.400 CCITT per lo scambio di messaggi.

PRINCIPIO DI FUNZIONAMENTO.

Dò qui una breve spiegazione di come funziona una rete dal punto di vista dei protocolli in uso.
Già dalla precedente specifica sui livelli OSI si nota che, contrariamente a quanto da molti asserito, NON si può trasmettere dati in "tcpip puro". Tal concetto è solo un'eresia.

TCP/IP va incapsulato in un protocollo di livello più basso, un protocollo di link dati. Nel caso radioamatoriale, detto protocollo è il ben noto AX.25, che significa Amateur X.25. Vi furono degli improovments del ben noto X.25 che ne permisero l'utilizzo per gli scopi radioamatoriali.
Implementando TCPIP in AX.25, è possibile creare una rete radioamatoriale Intranet, cioè una rete del tutto simile ad internet ma da essa disconnessa per questioni legali. È infatti proibito dal D.p.R. che regola nostra attività radioamatoriale, la comunicazione con stazioni non autorizzate, per cui è proibito comunicare tramite radio con: siti internet, persone che non sono O.M., e così via.
Ciò significa che un radioamatore utente di questa rete, può connettersi e "navigare" in essa con un comune browser. I più diffusi programmi di navigazione sono: Netscape, Internet Explorer, Opera, Lynx. Si hanno pertanto i vantaggi ed i servizi offerti sulla rete delle reti: Internet.
Anche la messaggistica viene trattata come la si tratta in Internet. Pertanto i messaggi possono essere inviati/ricevuti tramite un server di posta con i più comuni programmi client: Eudora, Messenger di Netscape, Pine, Outlook Express. Lo stesso dicasi per i NEWSGROUP, che sono l'equivalente dei bollettini.

NUMERO IP

Cerchiamo di capire cosa è questo "misterioso" numero IP ed a cosa serve.
Per indirizzare correttamente i dati, si fa' uso di un sistema numerico costituito in modo simile alla numerazione della rete telefonica nazionale.
Questa numerazione è parte integrante del protocollo che si occupa di porre in comunicazione DATI le macchine.
Il protocollo è il protocollo IP e la numerazione vien così detta: Numerazione IP.
Gli indirizzi IP sono costituiti da una stringa di testo ASCII di quattro numeri decimali disposti in quattro ottetti separati l'un dall'altro da un punto e corrispondenti all'indirizzo IP di quattro bytes. I quattro numeri sono indicati come segue:

nnn.hhh.lll.iii

n = rete
h = host
l = indirizzo logico
i = processore per i messaggi d'interfaccia o nodo dei pacchetti

Le reti sono suddivise in CLASSI. Un indirizzo di classe A è rappresentato come: n.h.l.i
Un indirizzo di classe B è rappresentato come: n.n.h.i.
Un indirizzo di classe C è rappresentato come: n.n.n.h.
Un esempio di indirizzo di classe A è: 16.9.0.122, dove n=16, h=9, l=0 e i=122

Un dispositivo di un utente può generare un indirizzo di dodici o quattordici cifre. Le ultime due cifre dell'indirizzo di quattordici cifre sono un sotto indirizzo e non vengono utilizzate.
In pratica oltre la sequenza n.h.l.i esiste un'altra cifra (sempre da 0 a 255), che non viene usata.
Un esempio di indirizzo di una rete di classe C, tipica per l'utente in rete e comunque nelle reti LAN, è ad esempio: 192.168.1.2. Questo numero indica che la macchina 2 è nella sotto rete 1, della rete intermedia 168 che fa parte della rete principale 192. Al fine di "isolare" il traffico su una rete da quella presente su un'altra rete, si rende necessario informare il GW di quali pacchetti far passare da una parte e quali dall'altra.
Per far ciò, si fa uso delle SubNet Masks (maschere di sotto rete).
Con esse è possibile interdire la comunicazione tra due reti differenti, in modo che sulle rispettive isole non si abbia il fluire dei dati reciproci.
Un'isola è un segmento di rete collegato da una medesima tratta fisica, ad esempio un gruppo di PC interconnessi da un cavo di rete (come RG-58 nel caso di reti piccole Ethernet), che vien poi connesso al server.
Ad esempio la rete: 192.168.1.0 (con lo "0" com'ultimo numero viene indicata una rete. Il "255" indica il canale di broadcast (vedremo più avanti) e con 254 in genere il GW. Il ".1" ed il ".2" generalmente, ma non sempre, indicano rispettivamente: DNS Primario e DNS Secondario.
L'indirizzo di Broadcast indica una porta sulla quale tutte le macchine della sottorete a cui appartengono, sono costantemente in ascolto. Pertanto un qualsiasi tipo di informazione che viene inviata a quest'indirizzo, è recepita dalla totalità delle macchine.
È appunto a questo indirizzo che, in internet, si fanno puntare le informazioni quali: diffusione radio, TV ed altro.
Lo stesso tipo di servizio può esser dato sulla rete Intranet radioamatoriale, velocità permettendo.
Le informazioni presenti sull'indirizzo di Broadcast non necessitano di ACK da parte di chi ascolta. Per tal ragione il flusso dati (Data Flow) risulta più veloce.
La maschera di rete è formata anch'essa da quattro gruppi di tre cifre ciascuno (da 0 a 255). Funziona con logica "AND" bit-a-bit. Per non "mischiare" i dati di entrambe le reti citate prima come esempio, dobbiamo impostare le subnetmasks come segue:

255.255.255.0

Significa che: il passaggio É APERTO SOLO per tutte le macchine della rete 192.168.1.0.
Idem per la rete 192.168.2.0…..e tra esse NON può esservi comunicazione se NON attraverso un ROUTER.
Tenere SEMPRE BEN PRESENTE che quando si parla di TCP/IP: dire ROUTER, ha lo stesso significato del dire: GATEWAY.
È anche importante specificare però che con il termine GATEWAY o ROUTER non si indica affatto un REPEATER ! Questa è fonte di confusione in ambito radioamatoriale, al riguardo sono in molti ad avere le idee non molto chiare.
Un repeater (più noto con l'abbreviativo: DIGI, che deriva dal termine *digipeater* ossia: ripetitore per segnali digitali) ha il solo compito di rigenerare un segnale e/o, nel caso delle reti AX.25, di reindirizzarlo SOLO a livello 2 OSI, su opportune porte.
Quindi mentre un ROUTER necessita di un numero IP su ogni interfaccia, in quanto indica al pacchetto (datagramma) TCP dove dirigersi, un DIGI non ha nessunissima necessità di avere un IP. E non deve proprio averlo, in quanto l'eventuale "re-addressing" avviene a livello di puro AX.25 (livello 2 OSI) senza in alcun modo coinvolgere TCP.
Una domanda che a questo punto viene spontanea e che diversi OM mi hanno già posto è: un repeater generico ha un ingresso ed un'uscita. Un repeater classico radioamatoriale può avere più di un ingresso e più di un'uscita. In questo caso l'indirizzamento opportuno come viene gestito ?
In questo caso è il livello OSI 2 vale a dire AX.25 che se ne occupa senza coinvolgimento dei layers superiori, come IP.
Ritornando alla nostra subnetmask dell'esempio che vi stavo proponendo, traducendola in codice binario 255.255.255.0 e traducendo anche l'indirizzo di rete 192.168.1.0, si ha:

```
11111111.11111111.11111111.00000000 = 255.255.255.0
11000000.10101000.00000001.00000000 = 192.168.1.0

11000000.10101000.00000001.00000000
└──── RETE ────┘└SUBNET┘└HOST┘
```

La logica di funzionamento indica: Se l'indirizzo di destinazione IP e la maschera di sottorete equivalgono al mio indirizzo IP e alla mia maschera di sottorete, inviare il datagramma alla rete locale, altrimenti inviarlo al Gateway.
Come detto, l'impiego delle maschere consente di gestire i percorsi per raggiungere le convenzioni dirette, i percorsi specificati dell'host e i percorsi predefiniti.
A proposito delle subnets, è opportuno che i progettisti si attengano alle seguenti indicazioni:

- L'algoritmo IP deve essere attuato su tutte le macchine presenti in una subnet.
- Le subnetmasks devono essere uguali per tutte le macchine.
- Se una o più macchine non supportano le maschere, è possibile utilizzare un proxy ARP per ottenere le subnets.

Le politiche di gestione dei gateways sono gestite da appositi protocolli, che qui vediamo per sommi capi, che servono per scoprire quale percorso far seguire ai datagrammi in caso di congestione rete od in caso di rottura delle isole.
A tal fine essi effettuano un test ciclico sulle tratte detto: Polling.
Ciascun sistema testa quello adiacente (neighbor) ed invia sul canale di broadcasting la tabella dei tempi di connessione
Questa tabella si unisce a quella creata dagli altri sistemi e così via.

In questo modo ciascun Gateway di neighbor (vicino) sa dove inviare i datagrammi al fine di far loro percorrere la tratta migliore.
Questa fase è gestita da IGP (Internal Gateway Protocol, Protocollo di Gateway Interno). In Internet non ha un IGP preponderante, a causa della mancanza di sistematicità che ha contraddistinto lo sviluppo e la promulgazione di questi protocolli.

I quattro IGP correlati alle internet sono: RIP (Routing Information Protocol, Protocollo per l'instradamento delle Informazioni), OSPF (Open Shortest Path First; Apri per primo il percorso più breve, non il migliore), HELLO e GATEd.

L'uso dei vari protocolli è subordinata all'efficienza che ciascuno di essi offre in base alla banda passante della rete in cui debbono essere impiegati.
In figura 1, osserviamo un classico sistema configurato per l'internetworking tra diverse reti.

Nella figura 2 è rappresentata la tabella di routing, ossia lo schema di instradamento di base dei datagrammi, necessario per far conoscere al Gateway quali sono le porte (interfacce) su cui inviare i datagrammi indirizzati verso determinate reti.

LE TRE CLASSI PRIMARIE DI INDIRIZZI IP

CLASSE A

0	1 2 3 4 5 6 7 8	16	24	31
0	NETID	HOSTID		

CLASSE B

0	1 2 3 4 5 6 7 8	16	24	31
1	0	NETID	HOSTID	

CLASSE C

0	1 2 3 4 5 6 7 8	16	24	31
1	1	0	NETID	HOSTID

Le sottoreti per ogni classe sono:

Classe A	da	1	a	127
Classe B	da	128	a	192
Classe C	da	193	a	223

Una piccola precisazione sull'interfaccia che di norma è numerata con: 127.0.0.0. Essa è l'"interfaccia di loopback" cioè quell'interfaccia "virtuale" che serve al sistema per comunicare con se stesso ossia comunicare con i propri servizi.

Destinazioni Dirette ed Indirette

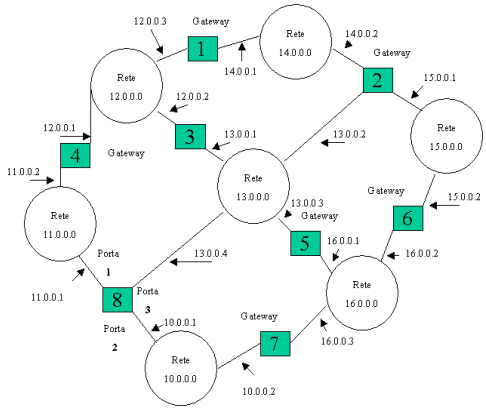

Figura 1

Tabella di routing del Gateway 8

Agli HOST Sulla rete	Percorso del datagramma	Attraverso questa porta fisica
10.0.0.0	*Diretto*	*2*
11.0.0.0	*Diretto*	*1*
12.0.0.0	*11.0.0.2*	*1*
13.0.0.0	*Diretto*	*3*
14.0.0.0	*13.0.0.2*	*3*
15.0.0.0	*10.0.0.2*	*2*
16.0.0.0	*10.0.0.2*	*2*

Figura 2

Nel prossimo articolo analizzeremo il sistema di gestione FlexNet, ne vedremo quindi le caratteristiche tecniche e le motivazioni che ci hanno suggerito di sceglierla come sistema predefinito ed unico per la gestione di rete. Inizieremo poi ad analizzare i "come ed i perché" delle nuove politiche di gestione-rete Nazionale.

(Fine Prima Parte)