1. Fondamenti di Net Bios
2. Principi di SMB
3. I protocolli: SMB e TCP/IP
4. Funzionamento delle reti Microsoft

1. Fondamenti di NetBios

Quando si parla di NetBios, NetBEUI e SMB si rischia spesso di far confusione fra protocolli, livelli di applicazione, definizione e contesti. Non è un caso, questi sono argomenti di fatto anomali, nel mondo del networking, che si trascinano dietro due decenni di utilizzi in rete e relative implementazioni.
Cerchiamo di chiarire le cose a grandi linee, in modo da poter meglio individuare gli argomenti che ci interessano e contestualizzarli correttamente.

1.2 NetBios strettamente parlando più che un protocollo è un interfaccia di programmazione (API) fatta sviluppare da IBM nel 1983 per permettere a delle applicazioni di comunicare scambiandosi file e messaggi sui PC network del tempo, che avevano un basso numero di host e non prevedevano ancora l'uso del protocollo IP (già presente ma usato più su WAN che in LAN) per le comunicazioni di rete.
Con l'introduzione di Token Ring, IBM nel 1985 definì delle estensioni a NetBios (NetBIOS Extended User Interface **NetBEUI**) che permettevano di appoggiarsi ad un data-link 802.2 (Token Ring o Ethernet).
Microsoft ha iniziato ad usare NetBEUI come protocollo di rete su Windows for Workgroup (Windows 3.1) e poi su tutte le versioni successive ma, al contempo, con la diffusione di Novell IPX e di IP, si è iniziato a veicolare NetBios anche su IPX e IP, oltre che su altri protocolli.
E' quindi possibile trovare NetBios (tipicamente proposto come protocollo a livello di sessione) nella sua incarnazione originaria, come NetBIOS Frames Protocol (NBF) detto anche semplicemente NetBios o NetBEUI, che copre i livelli di network e trasporto, oppure incapsulato su IPX o TCP/IP con questi ultimi a gestire il network e transport layer e NetBios posizionato come session layer.
Il protocollo Server Message Block (**SMB**) e il suo derivato Common Internet File System (**CIFS**) agiscono a livello applicativo, direttamente su NetBEUI, NetBios su IPX o NetBios su IP (chiamato anche NBT o NetBT), CIFS, invece, nelle sue recenti versioni può anche essere trasportato direttamente dal TCP/IP, senza layer NetBios intermedio.

1.3 Caratteristiche di NetBios

L'indirizzamento di NetBios è flat, basato sul semplice nome di un host (generalmente fino a 15 caratteri) e senza elementi gerarchici (come il DNS) che di fatto lo rendono inadatto per gestire il routing fra network diversi. Il nome NetBios è lo stesso che viene utilizzato dai procotolli superiori come SMB/CIFS.
Per impedire che due host nella stessa rete abbiamo lo stesso nome viene utilizzato il protocollo Name Management Protocol (NMP), tramite il quale, a colpi di broadcast, un host annuncia la sua presenza in rete e avverte quando un nuovo host con lo stesso nome prova ad apparire.
Nella comunicazione fra host si usano lo User Datagram Protocol (UDP, diverso dall'UDP usato su IP), unreliable e basato su datagrammi fino a 512 byte e il Session Management Protocol (SMP), bidirenzionale, reliable e basato su sessioni che vengono stabilite fra due host. Meccanismi di controllo e di monitoring vengono gestiti dal Diagnostic and Monitoring Protocol (DMP).
Attualmente la forma maggiormente utilizzata è quella di NetBios incapsulato su TCP/IP (NetBios over TCP/IP o NBT). Questo standard è definito nelle RFC 1001 e RFC 1002 dove si affrontano le problematiche relative all'associazione di un nome di host ad un indirizzo IP (broadcast o server di nomi centralizzato) e i metodi di comunicazione (a datagrammi o a sessioni).Le porte utilizzate per questi servizi sono:

netbios-ns **137/udp** # NETBIOS Name Service
netbios-dgm **138/udp** # NETBIOS Datagram Service
netbios-ssn **139/tcp** # NETBIOS Session Service

1.4 Gestione dei nomi su NetBios

I nomi di host di NetBios su TCP/IP (che coincidono con i nomi SMB) possono essere registrati (annunciati) e risolti (trovati) sul network locale sia tramite broadcast che tramite un server di nomi centralizzato (NBNS NetBios Name Server, su sistemi Windows l'implementazione di un NBNS è il WINS server) che risulta, soprattutto su reti affollate, molto più efficace.
A seconda di come un host è configurato per gestire i nomi assume un tipo di nodo diverso:
b-node - Host che usa solo broadcast per la risoluzione e la registrazione degli host name.
p-node - Host che usa un server centrale (comunicazione point-to-point) per risoluzione e registrazione
m-node - Host che usa broadcast per la registrazione e la risoluzione, inoltre se porta a termine con successo una registrazione lo notifica ad un server NBNS, che viene usato anche quando la risoluzione via broadcast non ha successo.
h-node (hybrid) - Host che usa un server NBNS per risoluzione e registrazione dei nomi e, nel caso in cui il server NBNS non sia disponibile utilizza i broadcast. Questa modalità è stata introdotta da Microsoft, non appare nelle RFC 1001 e 1002.
Il tipo di nodo, su Windows, è visibile nell'output del comando `ipconfig /all` dove si parla di `NodeType`

I nomi possono essere lunghi 15 caratteri (byte) e contenere caratteri alfanumerici standard (a-z, A-Z, 0-9, ! @ # $ % ^ & ( ) - '). Il sedicesimo e ultimo byte indica il tipo di risorsa, a seconda del valore esadecimale indicato corrisponde una diversa risorsa, alcuni esempi:
00 - Normale workstation
03 - Servizio di messaggistica (WinPopup)
1B - Domain Master Browser
20 - Fileserver
NetBios inoltre prevede il concetto di **gruppo** (i Workgroup in ambiente Windows).

2. Principi di SMB

SMB è un protocollo di livello applicativo utilizzato per la condivisione di directory fra computer, la stampa via rete e lo scambio di file e messaggi. Si basa su una struttura client-server ed ha una logica di tipo request-response. Dalla sua introduzione originaria ha subito varie modifiche e varianti che modificano e aggiungono nuovi SMB (Server Message Blocks, di fatto i "comandi" utilizzabili). Su Windows 95 e NT per esempio viene utilizzata la variante NT LM 0.12, che viene supportata, fra gli altri, anche da Samba, un implementazione OpenSource del protocollo che è utilizzabile su gran parte degli Unix in circolazione.

Opzioni smb.conf per il browsing di rete

2.1 Local master - Domain master

Queste opzioni servono per spingere Samba a cercare di diventare rispettivamente Local Master Browser (il server che mantiene la browse list per una rete IP) e Domain Master Browser (il server che mantiene la browse list per un intero workgroup, anche esteso su più reti IP, nel qual caso raccoglie e coordina lo scambio di browse list dai Local Master Browser remoti). Di default Samba ha attivata l'opzione Local Master (con cui semplicemente gli viene detto di partecipare alle elezioni, senza la certezza di vincerle) e non ha attivata l'opzione Domain Master (è bene che il Domain Master Browser sia la stessa macchina che fa eventualmente da Primary Domain Controller, sia esso un Samba o un Windows server). Le impostazioni di default sono quindi:

```
local master = yes
domain master = no
```

2.2 Preferred Master - OS Level

Con queste opzioni si gestisce il comportamento di Samba nelle elezioni e la sua possibilità di vincerle.
La prima impone a Samba di chiamare un'elezione ogni volta che entra in rete e gli imposta una probabilità leggermente superiore di vincerle rispetto ad altre macchine con

lo stesso livello. E' bene impostarla a yes quando si configura Samba come Domain Master Browser o Local Master Browser:

```
preferred master = yes
domain master = yes
```

E' comunque raccomandabile non avere troppe macchine in rete (Windows o Samba) che cercano di partecipare alle elezioni per evitare inutili e ripetuti broadcast e possibili incongrenze sulla browse list di riferimento.
L'opzione OS Master, invece setta esplicitamente il livello con cui Samba si presenta alle elezioni. Può avere valore da 0 a 255, più è alto e maggiore la possibilità di diventare Master Browser. Un valore di 34 basta per far vincere tutte le elezioni con server Windows ad eccezione di un PDC. Il valore di default è 20. Il seguente esempio dovrebbe bastare per vincere ogni elezione (ovviamente ad eccezione di altri server Samba con un OS level superiore):

```
os level = 65.
```

2.3 Risoluzione dei nomi con samba

E' possibile utilizzare una o più delle seguenti modalità di risoluzione dei nomi:

- Broadcasting
- LMHOST file
- Unix /etc/host o NIS
- WINS (Windows Internet Name Service), samba ha la facoltà di appoggiarsi ad un WINS server esterno oppure configurare lo stesso SAMBA per fungere da WINS server.

3 I protocolli: SMB e TCP/IP

La grande popolarità di Samba risiede nell'ottima compatibilità del server con le reti Microsoft grazie al comune utilizzo del protocollo SMB (Server Message Block). Per affrontare con la dovuta preparazione l'argomento, è doveroso analizzare i concetti che stanno alla base di una rete SMB: il NetBIOS di IBM e il successivo NBT.
Il primo venne creato da IBM nel 1984 per affrontare in modo rudimentale il problema della connessione e della condivisione di dati tra computer; consisteva in una semplice interfaccia API (application programming interface) il cui acronimo significava per esteso Network Basic Input/Output System. L'anno successivo ne venne rilasciata una versione migliorata definita NetBEUI che permetteva di creare piccole reti locali (LAN) dove ciascuna macchina possedeva un unico nome di riconoscimento di 15 caratteri per un totale massimo di 255 nodi.
La fondamentale differenza che intercorre tra protocollo NetBIOS e TCP/IP consiste nella rappresentazione dei client sulla rete: il primo si avvale esclusivamente di nomi sotto forma di un range di caratteri alfanumerici; il secondo di un gruppo di triplette numeriche come ad esempio 192.168.1.100. Da qui nacque l'esigenza di unire i due protocolli e nel 1987, l'Internet Engineering Task Force (IETF) pubblicò una serie di documenti (RFC 1001-1002) che esponevano come adattare NetBIOS a reti TCP/UDP; il

risultato fu l'implementazione di NetBIOS over TCP/IP (NBT). Il protocollo NBT consiste di tre servizi di rete:
-- un servizio di risoluzione nome-indirizzo
-- un servizio Datagram che si incarica di spedire pacchetti di dati direttamente o in broadcast senza accertarsi dell'arrivo a destinazione (UDP)
-- un servizio Session che instaura una comunicazione che permette di rilevare problemi o inoperabilità di connessione (TCP).
Nel sistema di connessione NetBIOS ogni volta che una macchina accede alla rete, cerca di identificarsi con un nome; questa operazione viene anche definita name registration (fig. 1-2)..

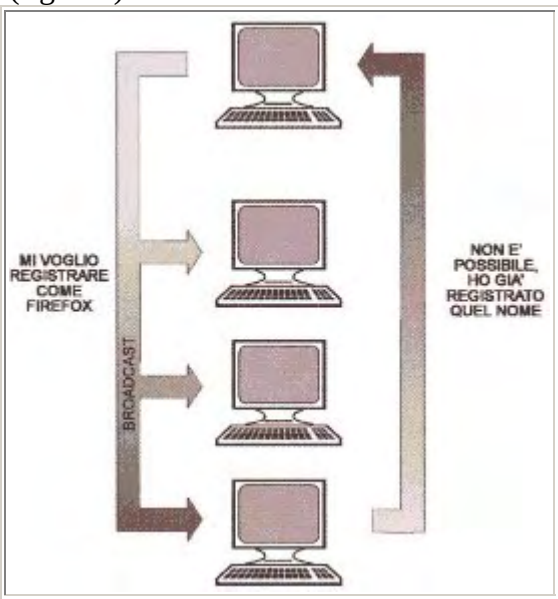

Fig 1: Registrazione del nome senza un NetBIOS Name server.

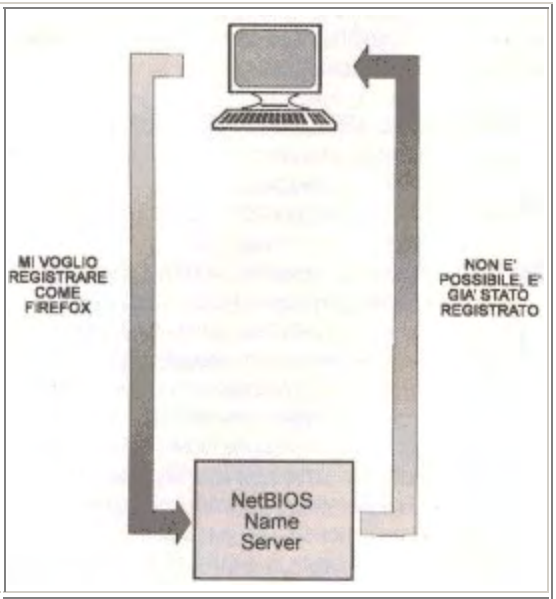

Fig 2: Registrazione del nome con un NetBIOS Name Server.

Ovviamente il maggiore problema che si può riscontrare in questa fase è nella verifica che non esistano due macchine con lo stesso nome in un dato momento. Due sono le soluzioni utilizzabili: avvalersi di un NetBIOS Name Server (NBNS) che tenga traccia delle differenti identità nomemacchina, oppure lasciare che sia compito del client “difendere” il proprio nome. Oltre al problema sopra esposto si deve garantire l'abbinamento tra un nome NetBIOS a uno specifico indirizzo IP; questa fase è anche conosciuta con il termine name resolution (fig. 3-4).

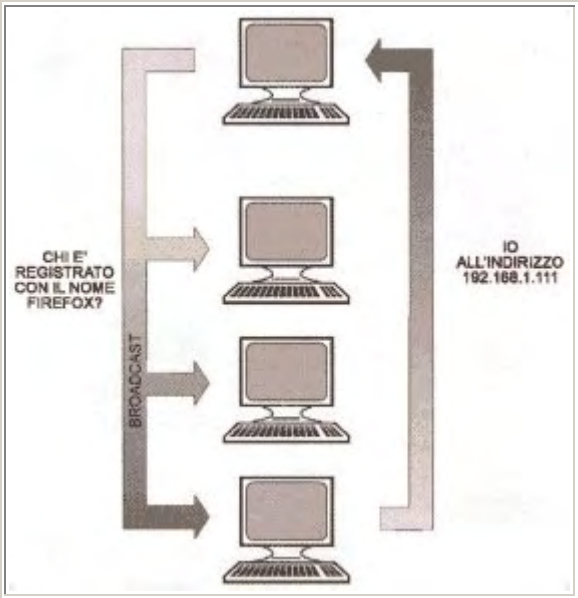

Fig 3: Risoluzione del nome senza un NetBIOS Name Server.

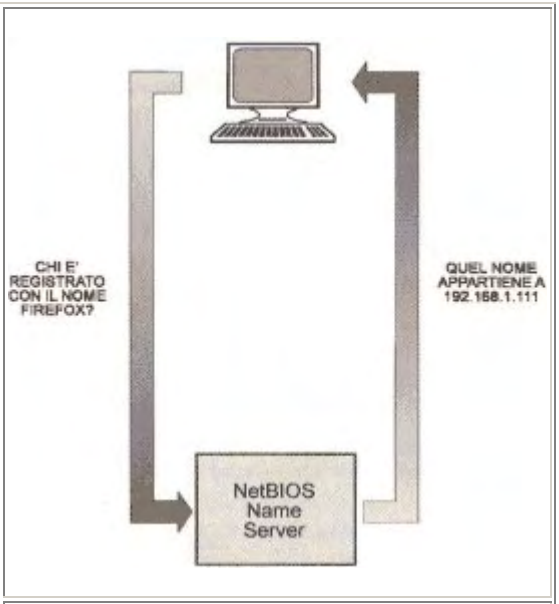

Fig 4 Risoluzione del nome con un NetBIOS Name Server.

NBT affronta il problema permettendo a ciascuna macchina di rispondere a una richiesta in broadcast del nome NetBIOS con il proprio indirizzo IP o, in alternativa, awalendosi di un NBNS nella risoluzione nomi NetBIOS/indirizzi IP.
Di seguito si può vedere la tabella dei tipi di nodi NBT:

Tabella 1: tipi di nodi NBT

Tipo	Valore
b-node	registrazione in broadcast e risoluzione diretta
p-node	registrazione point-to-point e risoluzione diretta
m-node	registrazione in broadcast e notifica a **NBNS**; risoluzione in broadcast e notifica a **NBNS** in caso di errore
h-node (hybrid)	registrazione e risoluzione via **NBNS**; broadcast se **NBNS** non è disponibile

Se si desidera verificare il tipo di nodo utilizzato
da una macchina Windows, digitare al prompt dei comandi MSDOS

C:\>ipconfig /all

La finestra restituita dovrebbe mostrare alla voce "tipo di nodo" il termine ibrido (scelta usuale nelle reti Microsoft).

4. Funzionamento delle reti Microsoft

Quanto detto fino ad ora permette di descrivere il funzionamento tipico di una rete Microsoft fornendo le necessarie informazioni per il successivo approfondimento dei parametri di configurazione smb.conf.

4.1 Windows Domains

È possibile definire un gruppo di lavoro (workgroup) come un insieme di computer SMB che risiedono in una sottorete (subnet) e che accedono allo stesso gruppo SMB. Un dominio Windows consiste in un workgroup con un server in qualità
di domain controller.
Questa mansione è di fondamentale importanza dal momento che:
-- gestisce il processo di autenticazione (garantire o negare l'accesso a risorse condivise attraverso l'uso di password)
-- gestisce il sistema di controllo username-password per mezzo di un security account manager (SAM)
Una volta che un client viene autenticato, non necessita
più di una seconda verifica e viene considerato collegato
al workgroup; (riferirsi alla figura 5 per lo schema di funzionamento).
Il domain controller attivo in un dominio viene anche dèfinito Primary Domain Controller (PDC); esiste anche la possibilità di configurare una seconda macchina in qualità di Backup Domain Controller (BDC) nel caso (non così infrequente) che il PDC diventi inaccessibile.
Questa lunga disgressione ci permette di asserire che Samba può assumere il ruolo di PDC in luogo di soluzioni ben più costose.

4.2 Sistema di Browsing

Ogni volta che una macchina collegata a un workgroup ricerca le risorse condivise, effettua una operazione di browsing.
In un network SMB ne esistono di due tipi:
-- browsing di una lista di macchine (con delle risorse condivise)
-- browsing di risorse condivise di una particolare macchina.
In un workgroup Windows, la macchina adibita al mantenimento di una lista aggiornata di macchine si chiama
Local Master Browser.

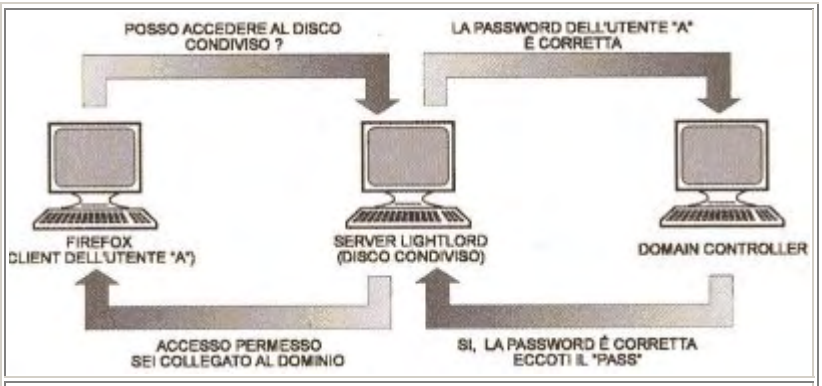

Fig 5: Autenticazione con un domain controller

L'accesso alle risorse di una singola macchina awiene invece attraverso il collegamento diretto alla stessa. Il ruolo del Local Master Browser è di grande importanza poiché ogni volta che un server si autentica in workgroup con un nome NetBIOS, lo comunica al LMB. In una rete Microsoft praticamente tutti i S.O. Windows possono ricoprire tale mansione, quindi per decidere il responsabile di questo compito si deve effettuare un'elezione (election). Una "elezione" consiste nell'invio in broadcast del proprio ruolo ricoperto nella rete attraverso il servizio datagram; questa informazione consiste in un valore numerico (si entrerà nel dettaglio più avanti). Ovviamente anche Samba vi partecipa attivamente. Accanto al ruolo di LMB è possibile trovare quello di Domain Master Browser. Quest'ultimo entra in gioco quando si hanno più subnet collegate tra loro: i vari LMB comunicano e si sincronizzano con il DMB permettendo l'aggiornamento delle liste delle risorse a disposizione di tutto il dominio Windows (spesso impossibile con un semplice broadcast dal momento che molti amministratori di rete bloccano questa operazione sui router).

La figura 6 riassume quanto esposto.

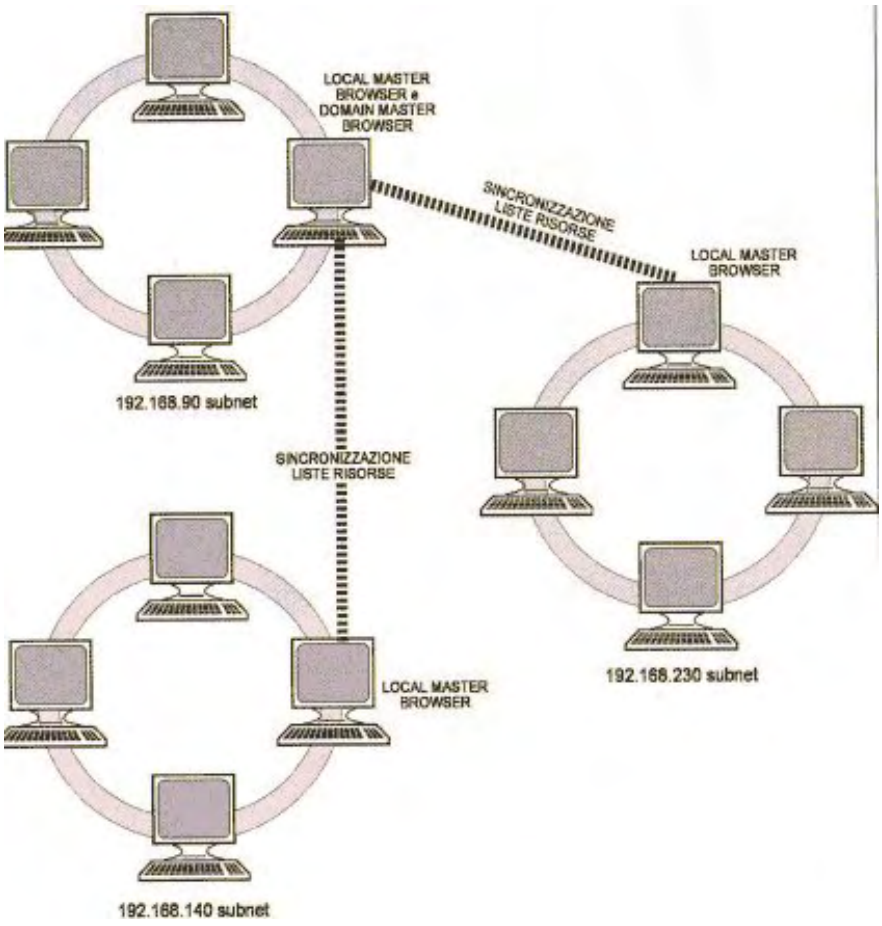

Fig 6: Wins Server

4.3 Il server WINS

Ultimo argomento da trattare a sommario completamento della panoramica sulle reti Microsoft è il Windows Internet Name Service (WINS). Questo servizio è la risposta Microsoft a NBNS, grazie ad esso è possibile gestire i client con i loro nomi, indirizzi e workgroup di appartenenza. Anche in questo caso esiste un WINS server attivo definito col nome di Primary WINS Server; accanto a esso si può collocare un server secondario che entra in azione nel caso che il principale non sia più disponibile. Samba può rivestire il ruolo di primary WINS Server come vedremo più avanti nell'analisi del file di configurazione.