

Capitolo 5: NetBIOS over TCP/IP

5.1 - NetBEUI e NetBIOS

NetBEUI è l'acronimo di NetBIOS Extended User Interface (interfaccia utente estesa di NetBIOS). NetBIOS, a sua volta, significa Network Basic Input Output System (sistema input/output di base per le reti). SMB, infine, sta per Server Message Block.

Modello OSI	NetBEUI	NetBIOS over TCP/IP	TCP/IP
applicazione	SMB	SMB	TELNET, FTP, SMTP...
presentazione			
sessione	NetBEUI	NetBIOS	TCP, UDP
trasporto		TCP, UDP	
network		IP ICMP	
data link	<i>indipendente dai protocolli superiori</i>		
fisico			

Più che un protocollo, il NetBIOS, che nel modello OSI lavora al livello sessione, è paragonabile ad una API, cioè ad un'interfaccia di programmazione che, attraverso un set di comandi standard, unisce l'SMB con i protocolli di trasporto ed instradamento sottostanti (come il TCP/IP o l'IPX/SPX). NetBEUI è invece un protocollo vero e proprio (o meglio, come il TCP/IP, un'insieme di protocolli), che ingloba in modo nativo sia l'interfaccia NetBIOS, sia una semplice funzionalità di trasporto. Il livello di trasporto del NetBEUI implementa il protocollo OSI LLC2. Quindi, mentre il NetBIOS può lavorare solo se abbinato ad un protocollo di trasporto, NetBEUI è del tutto indipendente, non avendo bisogno né di protocolli di trasporto, né di interfacce verso l'SMB.

5.1.1 - Il protocollo SMB

Creato dalla IBM a metà degli anni 80 e sufficientemente adattato e modificato dalla Microsoft, l'SMB è un importante protocollo, la cui implementazione è presente in quasi tutti i sistemi Windows. Come si può vedere nella figura precedente, si tratta del protocollo di più alto livello, al di sotto del quale si può trovare il NetBEUI oppure il NetBIOS (se corredato, come già detto, di un adeguato protocollo di trasporto). Il suo funzionamento è di tipo client/server, del tipo richiesta-risposta, dove il server è quel sistema che rende disponibili le proprie risorse condivise al client. I messaggi di richiesta e di risposta tra il client ed il server, sono detti appunto SMB. Essenzialmente, il lavoro di questo protocollo è quello di rendere

possibile la condivisione di files e stampanti, incluse tutte le operazioni che comunemente vengono fatte su queste risorse (ad esempio, leggere, scrivere, cancellare, creare, stampare, ecc...). Come ricordato prima, ad ognuna di queste operazioni corrisponde un certo messaggio SMB (ad esempio read, write, delete, new, print, ecc...). SMB é anche il responsabile del tanto comodo quanto problematico "browsing" delle risorse di rete. All'interno del protocollo SMB esiste infatti quel particolare elemento che permette di disporre delle risorse remote come se fossero locali. Il nome di questo componente é redirector ed esso permette, ad esempio, di vedere il disco fisso di un altro computer come se fosse il proprio. Per adattare meglio l'SMB ai vari ambienti sotto cui può lavorare, sono state create diverse varianti di questo protocollo. Per questo, quando due computer instaurano una connessione SMB, la prima operazione che viene effettuata é quella di stabilire quale variante utilizzare. Se entrambi gli host supportano la variante scelta dal client, si passa alla fase di autenticazione, che avviene inviando al server un nome utente ed una password. Se il login ha successo, al client viene inviato come risposta un numero, l'UID, che funge da identificatore e che dovrà essere reinviato al server in tutte le successive connessioni con esso. Il protocollo SMB é in grado di gestire due livelli distinti di sicurezza: share e user. In modalità share, ad ogni risorsa condivisa viene associata una password, che una volta superata permette il pieno accesso alla risorsa in questione. In modalità user, invece, il client deve essere innanzitutto autenticato dal server tramite una coppia utente-password indipendenti dalle risorse di cui l'utente vorrà usufruire. L'accesso alla risorsa é deciso in base ai privilegi posseduti dal client. Si definisce dominio un insieme di computer in cui la gestione della sicurezza é affidata ad una entità centrale, chiamata PDC (primary domain controller). Al suo fianco possono esserci spesso controller secondari di backup. Un PDC contiene ad esempio l'elenco dei nomi dei client, le rispettive password, il gruppo di appartenenza, ecc...

Le comunicazioni con il livello inferiore (NetBEUI o NetBIOS) avvengono tramite particolari strutture dati a 64 byte, chiamate NCB (network control block). Attraverso le NCB passano le richieste e le risposte SMB. Il metodo consiste nel caricare opportunamente queste strutture dati con tutte le informazioni necessarie, come il codice del comando, i nomi NetBIOS o altri parametri. L'accesso alle NCB può essere asincrono, se il controllo ritorna subito al programma, o sincrono, se invece il programma attende il completamento dell'operazione specificata.

5.1.2 - I nomi NetBIOS

Ogni host Windows, riceve un nome NetBIOS nel corso dell'installazione del sistema operativo. Questo nome viene usato per identificare in modo univoco la macchina sulla rete. Il nome NetBIOS però non viene utilizzato in sé per identificare un host:

viene invece usato dalle applicazioni e dai processi NetBIOS per stabilire comunicazioni con altre applicazioni NetBIOS su di host remoti. Un nome NetBIOS è costituito da 15 caratteri alfanumerici. Se un nome NetBIOS non contiene 15 caratteri, Windows aggiunge il numero opportuno di caratteri nulli per portarlo alla lunghezza standard. A tutti i nomi NetBIOS viene aggiunto un sedicesimo carattere (chiamato nodo), che solitamente non è visibile. Si tratta di un valore esadecimale che indica il tipo di nome, servizio o gruppo rappresentato dal nome NetBIOS.

Name	Number	Type	Service
<computername>	00	U	Workstation Service
<computername>	01	U	Messenger Service
< MSBROWSE >	01	G	Master Browser
<computername>	03	U	Messenger Service
<computername>	06	U	RAS Server Service
<computername>	1F	U	NetDDE Service
<computername>	20	U	File Server Service
<computername>	21	U	RAS Client Service
<computername>	22	U	Exchange Interchange
<computername>	23	U	Exchange Store
<computername>	24	U	Exchange Directory
<computername>	30	U	Modem Sharing Server Service
<computername>	31	U	Modem Sharing Client Service
<computername>	43	U	SMS Client Remote Control
<computername>	44	U	SMS Admin Remote Control Tool
<computername>	45	U	SMS Client Remote Chat
<computername>	46	U	SMS Client Remote Transfer
<computername>	4C	U	DEC Pathworks TCP/IP Service
<computername>	52	U	DEC Pathworks TCP/IP Service
<computername>	87	U	Exchange MTA
<computername>	6A	U	Exchange IMC
<computername>	BE	U	Network Monitor Agent
<computername>	BF	U	Network Monitor Apps
<username>	03	U	Messenger Service
<domain>	00	G	Domain Name
<domain>	1B	U	Domain Master Browse
<domain>	1C	G	Domain Controllers
<domain>	1D	U	Master Browser
<domain>	1E	G	Browser Service Elections
<INET~Services>	1C	G	Internet Information Server
<IS~Computer name>	00	U	Internet Information Server
<computername>	[2B]	U	Lotus Notes Server
IRISMULTICAST	[2F]	G	Lotus Notes
IRISNAMESERVER	[33]	G	Lotus Notes
Forte \$ND800ZA	[20]	U	DCA Iramalan Gateway Service

Nella tabella qui sopra, il sedicesimo carattere (esadecimale) è rappresentato nella colonna number. La colonna type, invece, indica se il nome NetBIOS è unico (U) oppure di gruppo (G).

5.2 - I limiti di NetBIOS e NetBEUI

La diffusione di Internet, ha messo subito in luce tutti i limiti di NetBIOS e del suo "socio" NetBEUI, quando la rete cresce di dimensioni. Tralasciando problemi seri, ma non insormontabili, quale il degrado prestazione sulle WAN dovuto all'uso dei broadcast, rimangono tuttavia altri problemi di non facile soluzione. Innanzitutto c'è il problema dell'unicità dei nomi. Dato che due computer non possono utilizzare due nomi uguali nella stessa rete, occorrerebbe individuare un nome diverso per ogni computer connesso. Operazione non banale in una rete geografica con milioni di host collegati. In secondo luogo, sempre a causa dei nomi, NetBEUI non permette il routing. Cioè, dato un nome NetBIOS, è impossibile sapere quale sia la strada per raggiungerlo. Ciò porta a complicazioni assurde: per esempio, un host si comporterebbe nello stesso modo per spedire un pacchetto ad un host distante da lui 100 metri, oppure situato in un altro continente. Il problema, in questo caso, risiede nel fatto che i nomi NetBIOS non contengono alcuna informazione gerarchica. A differenza degli indirizzi IP, che possono essere visti come indirizzi postali del tipo stato.città.via.casa, i nomi NetBIOS non forniscono indicazioni di nessun tipo. Un ultimo problema, forse il più importante, è che i router di Internet non permettono il propagarsi dei broadcast, tanto cari al NetBIOS quando cerca di localizzare un nodo. Per dire tutto in poche parole, NetBIOS ed Internet sono incompatibili. Tuttavia, per evitare che il NetBIOS venisse definitivamente abbandonato, Microsoft ebbe la brillante idea di abbinare l'interfaccia NetBIOS ad un protocollo molto più flessibile del NetBEUI, ovvero il TCP/IP. In questo modo, ogni messaggio elaborato da NetBIOS viene incapsulato in un messaggio TCP/IP, che non soffre delle limitazioni di cui sopra.

5.3 - NetBIOS over TCP/IP (NBT)

Per rendere possibile l'interfacciamento tra NetBIOS e TCP/IP era necessario che anche NetBIOS iniziasse ad interpretare degli indirizzi IP. E' da questa considerazione che nasce il NetBIOS over TCP/IP, chiamato anche NBT e descritto nelle RFC 1001 e 1002. Esso è in grado di lavorare su reti geografiche, basandosi su associazioni tra nomi NetBIOS ed indirizzi IP ricevute dall'esterno.

Iniziamo col dire che i singoli host (che in ambiente NBT sono detti nodi), possono operare secondo cinque modalità standard:

- nodi b (broadcast nodes): utilizzano broadcast sia per la registrazione che per la risoluzione dei nomi in indirizzi IP. I nodi b soffrono ancora del problema dei broadcast di NetBIOS: se essi sono separati da router, non riusciranno a vedersi;
- nodi eb (enhanced broadcast nodes): è la configurazione di default per gli host basati su Windows NT, che non sono

configurati per accedere ad un server WINS. Questa versione modificata dei nodi b, permette di consultare il file LMHOSTS nell'eventualità in cui la risoluzione via broadcast fallisca;

- nodi p (point-to-point nodes): scoprono l'IP delle risorse, interrogando con richieste unicast un server WINS noto. WINS (Windows Internet Name Service) , un server che, imitando i DNS, fornisce una lista di coppie nome NetBIOS - indirizzo IP;
- nodi m (multi nodes): utilizzano prima il broadcast (come i nodi b) e poi, in caso di risposta negativa, inoltrano le richieste ad un server WINS (come i nodi p);
- nodi h (hybrid nodes): funzionano al contrario dei nodi m, cioè, prima contattano un server WINS noto, poi passano eventualmente al broadcast;

I clients Microsoft, per la risoluzione di un nome NetBIOS, utilizzano dunque un procedimento che si suddivide in sei passaggi:

- controllo della cache interna, dove sono memorizzati gli ultimi indirizzi risolti;
- interrogazione del server WINS;
- broadcast;
- controllo del file LMHOSTS;
- controllo del file HOSTS;
- interrogazione del server DNS;

Il file LMHOSTS é il corrispondente Windows di quello che negli ambienti UNIX é solitamente HOSTS. Si tratta di un file da editare manualmente e che contiene, come una sorta di server WINS statico, una lista di coppie nome netbios - indirizzo IP. Può risultare molto utile nel caso in cui alcuni nodi non riescano a vedersi (per la presenza, ad esempio, di un router) e non vi sia un server WINS disponibile.

5.3.1 - Le porte dell'NBT

Il protocollo NBT, utilizza tre porte del TCP/IP per la comunicazione:

- porta 137 UDP: risoluzione nomi NetBIOS;
- porte 138 e 139 UDP: datagrammi;
- porta 139 TCP: sessioni;

Per gli amministratori di rete, queste porte sono spesso problematiche da gestire. Il rischio concreto, infatti, è che qualche errore di configurazione renda accessibili le risorse condivise del computer, tramite una connessione NetBIOS effettuata da un utente privo di autorizzazione. Si tratta di una operazione di hacking molto diffusa, anche da coloro che sono considerati semplici lamer (un termine dispregiativo, che gli hackers usano per indicare chi vuole diventare come loro, ma senza essere disposto a passare giorni e giorni davanti al computer). E' infatti sufficiente un semplice portscanner (ottimo il SuperScan 2.04, prelevabile freeware da Internet) per trovare un sistema "netbiosato", su cui tentare l'accesso. Un pc con il NetBIOS attivo è riconoscibile proprio dalle porte 137, 138 e 139 che risultano aperte, in quanto vi sono in ascolto i demoni predisposti da Microsoft.

5.4 - NBT: la sua funzione oggi

Al giorno d'oggi, Internet è basata quasi esclusivamente sul TCP/IP e potrebbe benissimo andare avanti senza NetBIOS e NetBEUI. Nell'ambito delle reti locali, invece, il discorso è diverso. Microsoft ha infatti sviluppato un protocollo chiamato NBF (NetBIOS Frame), che presenta alcune migliorie rispetto al NetBEUI da cui prende spunto. Tra queste, invece di interfacciarsi con i livelli superiori tramite il consueto NetBIOS, l'NBF utilizza un'altra interfaccia più flessibile, denominata TDI (Transport Driver Interface). Nelle reti di piccole/medie dimensioni (diciamo fino a circa 200 host), l'NBF resta una delle soluzioni migliori, in quanto il broadcast non è molto problematico ed è piuttosto veloce.