

Problematiche di rete su sistemi Windows

Introduzione

Esistono molti strumenti per analizzare e risolvere le problematiche relative alle connessioni di rete, sia in ambiente Windows NT che in ambiente Windows 95 e Windows 98. La maggior parte di tali strumenti sono inclusi all'interno del prodotto o in pacchetti aggiuntivi come il *Network Monitor* incluso nel *Microsoft System Management Server*.

Quando si cerca di risolvere un problema di rete, è utile ricorrere ad un approccio logico.

Ecco alcune domande da porsi:

- Che cosa funziona?
- Che cosa non funziona?
- Come sono collegati gli elementi funzionanti con quelli non funzionanti?
- Gli elementi che non funzionano hanno mai funzionato su questo computer o su questa rete?
- Se sì, che cosa è cambiato dall'ultima volta che non funzionavano?

Per isolare un problema un sistema valido consiste nel farne un'analisi dal basso verso l'alto. Nei prossimi paragrafi vedremo alcuni problemi nei quali è possibile imbattersi all'interno delle reti Windows e i migliori modi per analizzarli e risolverli.

Il logon alla rete

Per analizzare i problemi connessi al processo di **logon** alla rete, innanzitutto è necessario conoscere il funzionamento e come si diversifica tale processo in tutti i sistemi operativi della famiglia Windows (vedi 4.4.2).

Normalmente, in un ambiente di rete, un utente viene autenticato per mezzo di **username** e **password**, da un server detto **domain controller**. Se il domain controller non viene trovato, allora l'utente può comunque eseguire il **logon** utilizzando una copia in cache delle proprie credenziali.

Il Processo di User Logon in NT rispetto a 9x

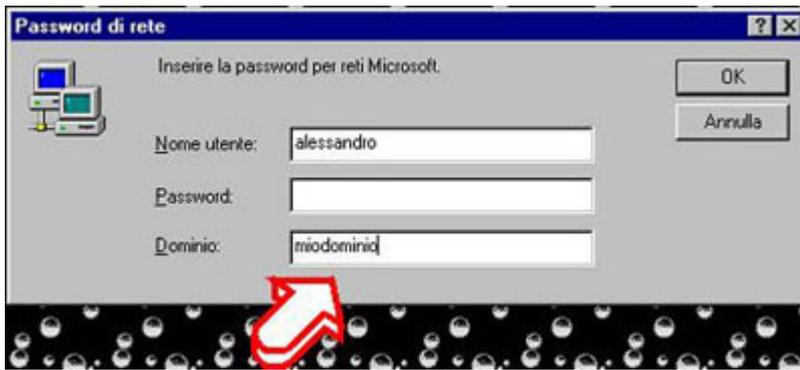
Il processo di **logon** in ambiente Windows 95 e Windows 98 differisce dal processo di logon in ambiente Windows NT (Windows NT 4, Windows 2000, Windows Xp Professional). Capire il funzionamento del processo di logon in questi due ambienti aiuta nell'affrontare e risolvere molte delle problematiche che si riscontrano nell'utilizzo quotidiano di una rete Windows.

Processo di Logon in Windows 95 e Windows 98

Quando un computer con sistema operativo Windows 95 o Windows 98 esegue il **boot**, il calcolatore non appartiene a nessun dominio e non detiene nessun **computer account**, quindi il calcolatore non ha bisogno di autenticazione ad un **domain controller**.

Si può configurare il sistema in modo che appaia una finestra di **logon** che permette di inserire le proprie credenziali locali, è altresì possibile configurare il sistema in modo da inserire username e password valide per l'autenticazione nel dominio come indicato successivamente.



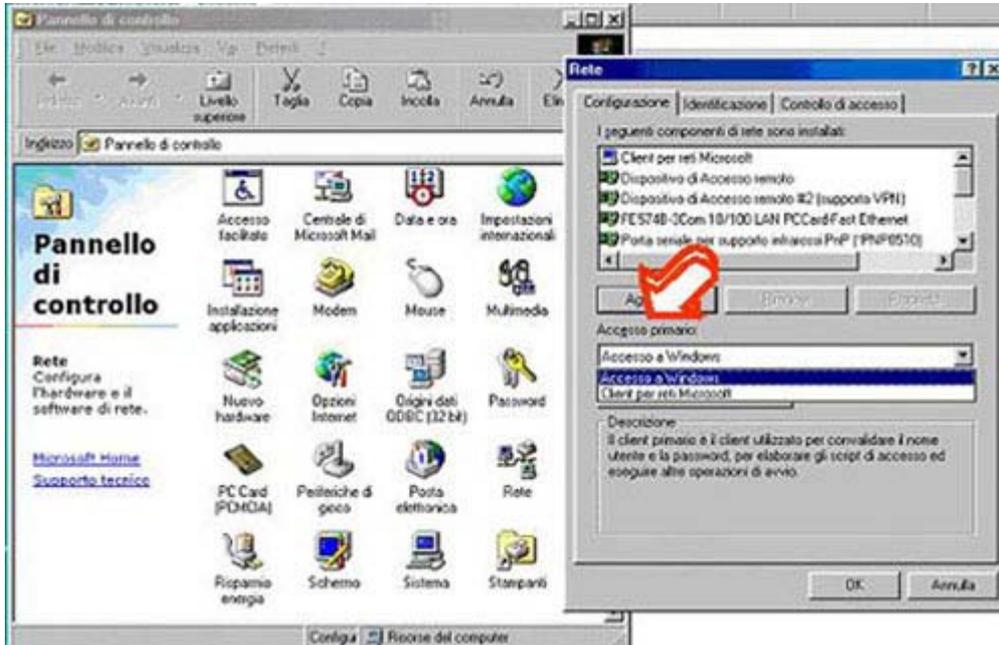


Quando un utente si autentica, le informazioni sono validate dal dominio, e il computer può accedere alle risorse della rete. Se questa validazione non va a buon fine per qualche ragione, l'utente non riesce a usufruire di parte o di tutte le condivisioni di rete gestite dai **domain controller**.



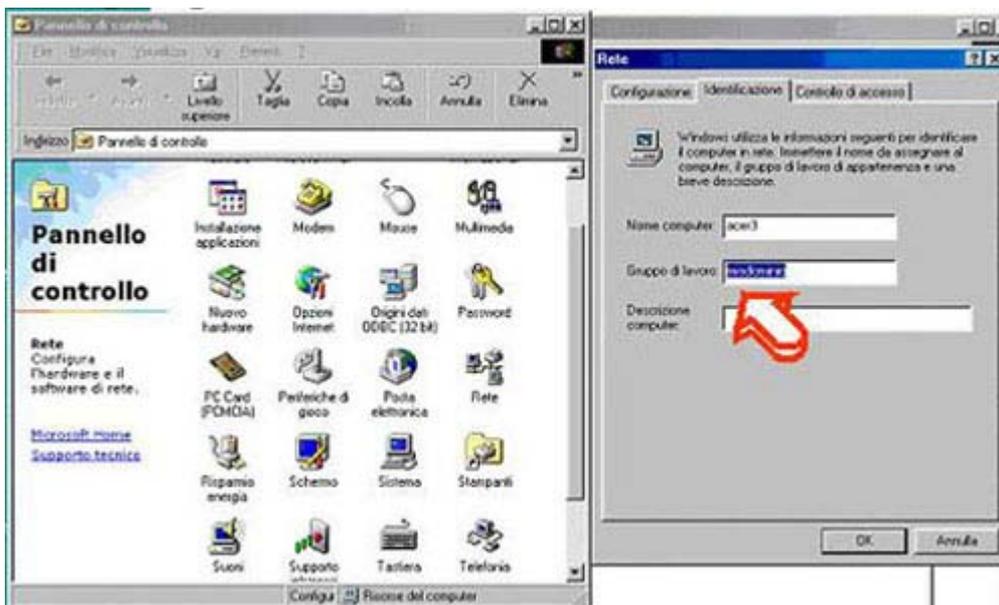
Di seguito vediamo le operazioni da compiere per la corretta configurazione della sezione rete di Windows 9x per lavorare nel dominio.

Definizione del metodo di accesso primario:

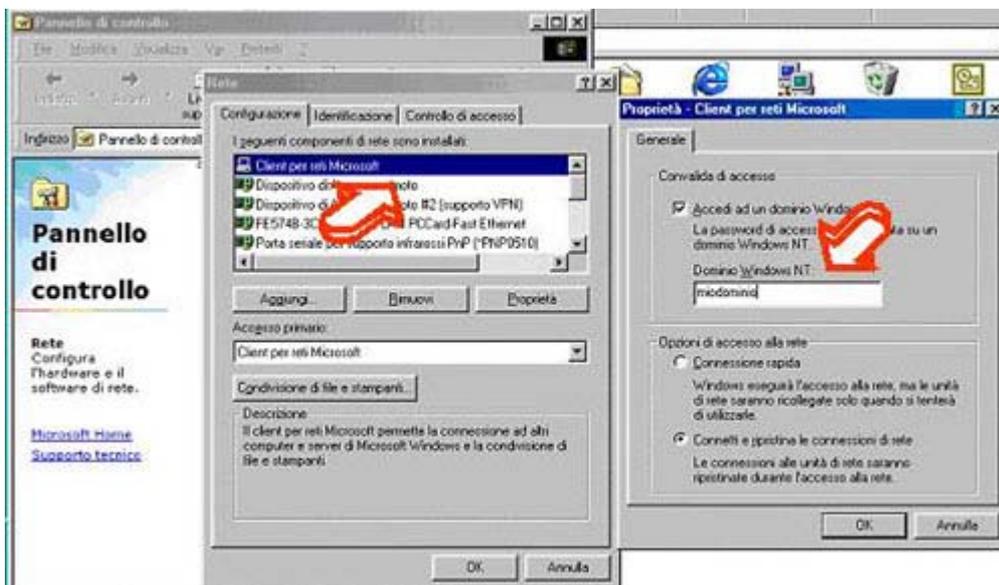


Si seleziona Client per reti Microsoft come accesso primario.

Definizione del nome di gruppo di lavoro uguale al dominio:



Definizione del nome del dominio al quale il sistema operativo deve eseguire l'autenticazione:



Processo di logon nella famiglia Windows NT

Quando un computer con un sistema operativo della famiglia Windows NT esegue il **boot**, il calcolatore è membro del dominio, quindi possiede un **account** di computer. Questo comporta che il computer si deve prima autenticare a un **domain controller**, poi permette all'utente di inserire le credenziali per autenticarsi al dominio.

I computer che eseguono Windows NT, Windows 2000 e Windows Xp, supportano la **cache** delle credenziali utente per tutti gli account utilizzati precedentemente, quando il domain controller era attivo. Avendo in **cache** le credenziali, un utente può essere validato anche se il computer non trova un domain controller, potendo così utilizzare le risorse locali della macchina.

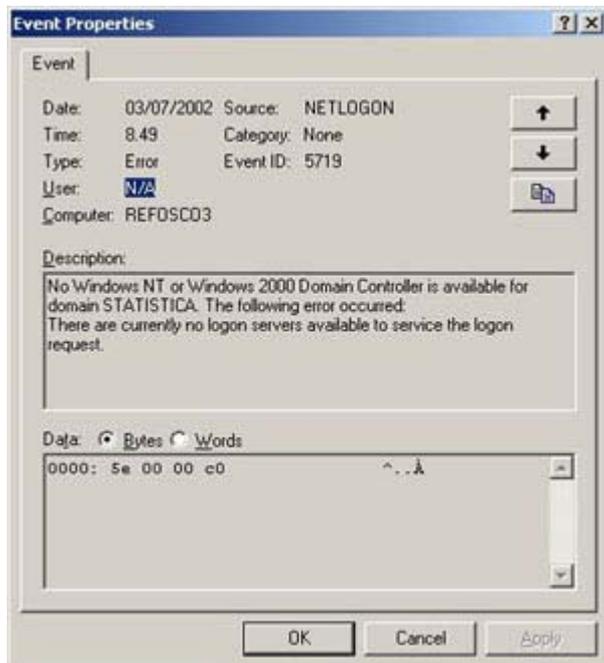
Se si riesce a compiere il **logon** con le credenziali residenti su un **domain controller** l'utente può utilizzare tutte le risorse, autorizzate per quell'account, gestite dai server e le **workstation** del dominio.

Eseguendo il **logon** con la rete scollegata, il sistema Windows NT riconosce che le credenziali immesse coincidono con quelle in **cache** e apparirà l'avviso

Windows cannot connect to a server to confirm your log on setting. You have been logged on using previously stored account information.

o un messaggio equivalente.

Nel visualizzatore degli eventi si trova la seguente segnalazione di errore con codice 5719. Notiamo che il codice di errore rimane inalterato al variare della lingua e della versione del sistema operativo. Di seguito vediamo il codice di errore di un Windows NT 4 Workstation e di un Windows 2000 Professional appartenenti allo stesso dominio:



oppure

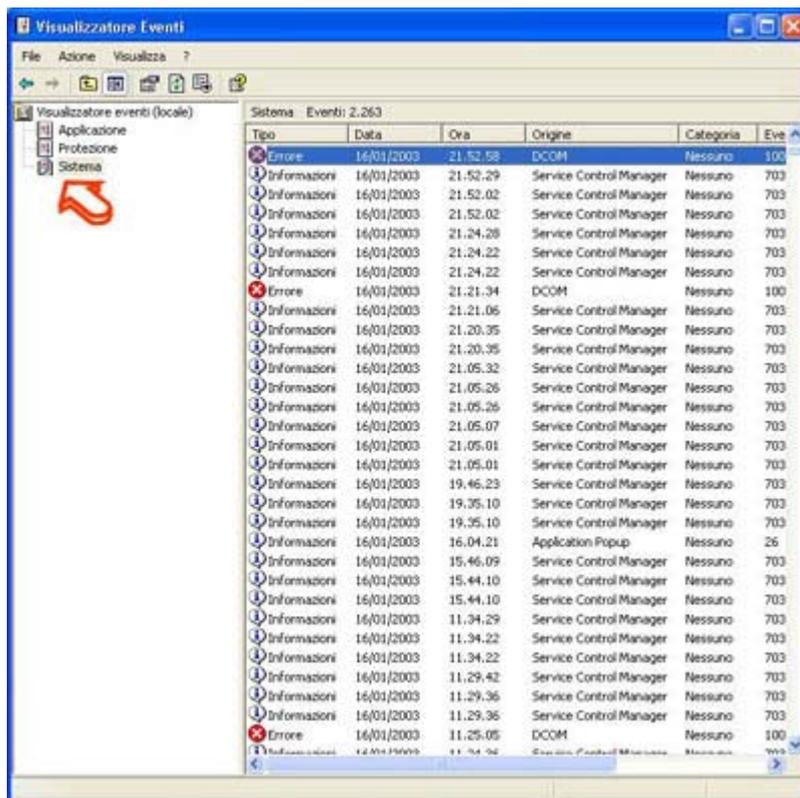


Appena il problema di collegamento con il **domain controller** viene risolto, le credenziali in **cache** vengono mandate al dominio e l'utente può usufruire di tutte le risorse di rete senza reinserire nuovamente la **password**.

Se si utilizza un dominio di tipo Active Directory (Windows 2000 o .NET) è possibile creare politiche di gruppo che disabilitino, per determinati utenti, la caratteristica del **caching** delle credenziali. Questa possibilità è utilizzata in particolari contesti dove sono richiesti livelli di sicurezza elevati.

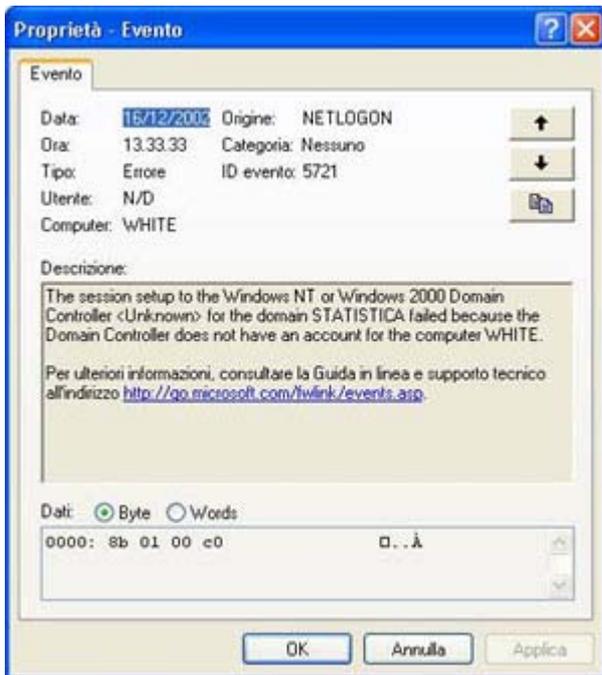
Problemi nella gestione degli account computer

Un particolare problema che si può presentare al momento del **logon**, nei sistemi della famiglia Windows NT, consiste nel disallineamento dell'account computer con il dominio. Infatti, in alcuni casi, l'utente non può collegarsi alla rete anche se le sue credenziali utente sono corrette. Questa eventualità si controlla attraverso il programma Visualizzatore Eventi, nella sezione sistema.



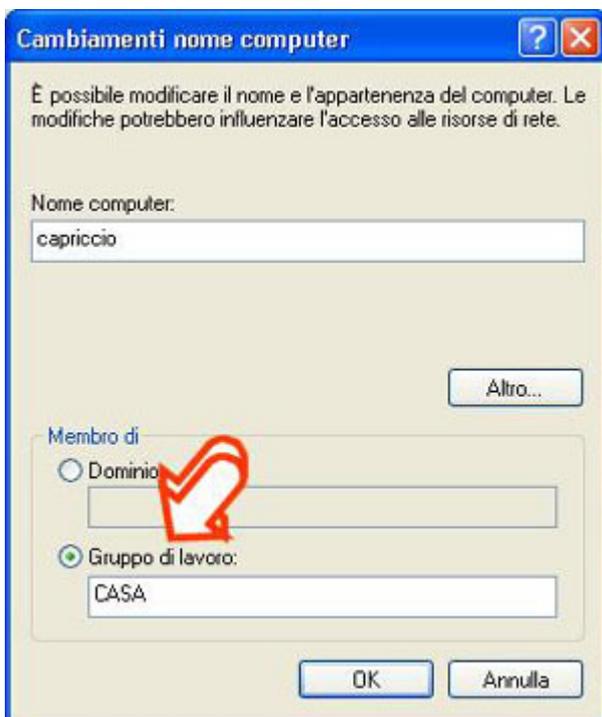
Come già precisato, il processo di **logon** per funzionare correttamente necessita di **username** e **password** sia per l'**account** computer che per l'**account** utente, ma può avvenire che le credenziali del computer siano disallineate con il dominio, in quanto le password vengono cambiate dinamicamente dal sistema al fine di aumentare la sicurezza.

Un evento che ci permette di capire l'esistenza di questo problema è il seguente:



Un amministratore del dominio Windows NT, con permessi di **join** al dominio, o un utente del dominio con privilegi di amministratore della **Workstation** in ambiente **Active Directory**, deve eseguire di nuovo la procedura di **join** al dominio, quindi togliere la **Workstation** dal dominio inserendola in un **Workgroup**, riavviare il computer ed infine reinserirla nel dominio utilizzando le opportune credenziali.

Vediamo la procedura:



Per esempio, un computer basato su windows NT viene configurato automaticamente per usare uno dei quattro diversi metodi di risoluzione del nome Netbios, basati sul modo in cui è configurato il TCP/IP sul computer. La tabella seguente descrive la configurazione del computer (nodo) e il relativo modo di risoluzione del nome Netbios.

Tipo di nodo della risoluzione del Nome	Descrizione
b-node	Utilizza dei messaggi a tutta la rete locale (Broadcast) per registrare e risolvere i nomi netbios in indirizzi IP. Soluzione utilizzata dai client che non hanno definito alcun server dei nomi, alto impatto di traffico adatto a reti di piccole dimensioni.
p-node	Utilizza le comunicazioni punto a punto con un server di risoluzione dei nomi per registrare e risolvere i nomi di computer in indirizzi IP (in NT 4 è un server WINS , in Windows 2000 è preferenzialmente il DDNS)
m-node	Utilizza una combinazione mista tra b-node e p-node. Inizialmente utilizza il metodo b-node, se non trova la soluzione voluta, utilizza il metodo p-node.
h-node	Utilizza una combinazione ibrida di b-node e p-node. Quando è configurato per utilizzare h-node, un computer prova sempre a connettersi con il server dei nomi per gestire la risoluzione (p-node) e solo se fallisce utilizza la modalità broadcast.

Di seguito vediamo una tipica configurazione dello **stack TCP/IP**, in cui il tipo di nodo identifica il metodo di ricerca dei nomi appena definita.

Per fare ciò si utilizza il comando Ipconfig, in ambiente Windows NT, e Winipcfg, in ambiente Windows 95 e Windows 98. Il primo è un'utility a riga di comando, il secondo è grafico ed entrambi stampano la configurazione connessa al protocollo **TCP/IP** del computer locale.

```
C:\>ipconfig /all
Configurazione IP di Windows
Nome host . . . . . : baule
Suffisso DNS primario . . . . . : unibo.it
Tipo nodo . . . . . : Ibrido
Routing IP abilitato. . . . . : No
Proxy WINS abilitato . . . . . : No
Elenco di ricerca suffissi DNS. . . . : unibo.it

Scheda Ethernet Connessione alla rete locale (LAN):
Suffisso DNS specifico per connessione: unibo.it
Descrizione . . . . . : Connessione di rete Intel(R) /100
Indirizzo fisico. . . . . : 10-01-23-1C-C0-9C
DHCP abilitato. . . . . : No
Indirizzo IP. . . . . : 10.10.10.1
Subnet mask . . . . . : 255.255.255.0
Gateway predefinito . . . . . : 10.10.10.254
ID classe DHCP . . . . . :
Server DNS . . . . . : 10.10.10.5
10.1.10.7
```

I tipi di server a cui i **client** chiedono la transcodifica dei nomi **netbios** in numeri IP sono principalmente due: server DNS e server WINS.

I server WINS, all'interno di una rete Microsoft basata su TCP/IP, vengono utilizzati per registrare le informazioni riguardanti i nomi macchina, i numeri IP ad essi associati ed i servizi ospitati, in modo da poter fornire tali informazioni ai client che le richiedono.

Avendo configurato tutti i client della rete in modo da utilizzare i server WINS, si ottiene una

diminuzione significativa del traffico generato da broadcast. Inoltre, è il client che, così configurato, autonomamente al boot, si prende carico di registrare le informazioni che lo riguardano sul server WINS.

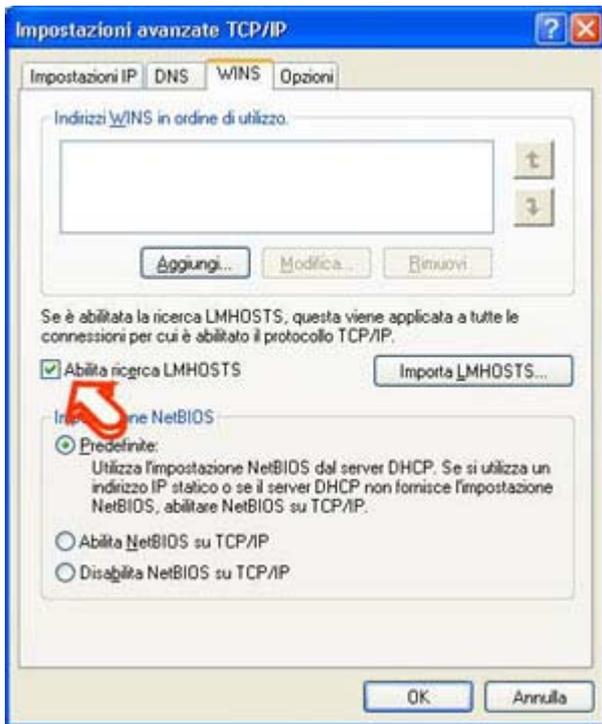
Il servizio DNS è utilizzato universalmente per la risoluzione dei nomi Internet (es.: <http://www.mamma.it> corrisponde al numero ip 66.71.161.93) e, solo da poco, ne usufruiscono anche i sistemi Microsoft per la ricerca dei server che si occupano della gestione del dominio (es. server di autenticazione).

Questo è possibile da quando, con l'implementazione del servizio DNS sui sistemi Windows 2000, si è utilizzata la registrazione dinamica, che permette, a un client o ad un server, di registrare non solo la macchina e il proprio IP, ma anche quali servizi ospita. Questo sistema viene detto Dynamic DNS (DDNS).

Come per i sistemi che utilizzano Wins, anche i client Windows 2000 e Windows Xp che utilizzano il DDNS, devono essere configurati opportunamente sia per l'uso sia per la corretta registrazione delle proprie informazioni sul server.



Un ulteriore metodo per connettersi a un server di rete è basato sull'uso del file lmhost. In questo caso se nel computer è presente il file lmhosts e nello stack TCP/IP ne è definito l'uso, i vari metodi utilizzeranno in modo preferenziale i dati presenti nel file lmhosts.



Tale file non è da confondere con il file hosts, il quale viene utilizzato per la risoluzione dei nomi di tipo Internet (<http://www.3com.com>) e, preferenzialmente, per la diagnostica interna (es: ping nomemacchina) o per risolvere indirizzi di macchine che non svolgono le tipiche funzioni di una rete Microsoft.

Nel caso in cui non venga individuato, per esempio, il **domain controller**, allora verranno applicati uno dopo l'altro i vari metodi fino al ritrovamento di un **domain controller** disponibile per autenticare le credenziali fornite.

Esempio di file lmhosts residente nella directory `systemroot\system32\drivers\etc`

```
#
102.54.94.97 chianti #PRE #DOM:miodominio #Domain Controller del dominio Italia
102.54.94.123 Verona #PRE #server origine
102.54.94.117 localsrv
#
```

L'aggiunta del carattere #PRE ad ogni voce nel file causerà il caricamento anticipato della voce nella cache del nome. Per impostazione predefinita le voci non vengono caricate prima, ma vengono interpretate solo se fallisce la risoluzione dinamica dei nomi.

L'aggiunta della sigla #DOM: <dominio> assocerà la voce con il dominio specificato da <dominio>. Ciò riguarda le modalità di funzionamento dei servizi elenco computer e di ricerca dei domain controller per l'autenticazione in ambiente TCP/IP. Per caricare prima una voce #DOM, è necessario inoltre aggiungere #PRE alla riga.

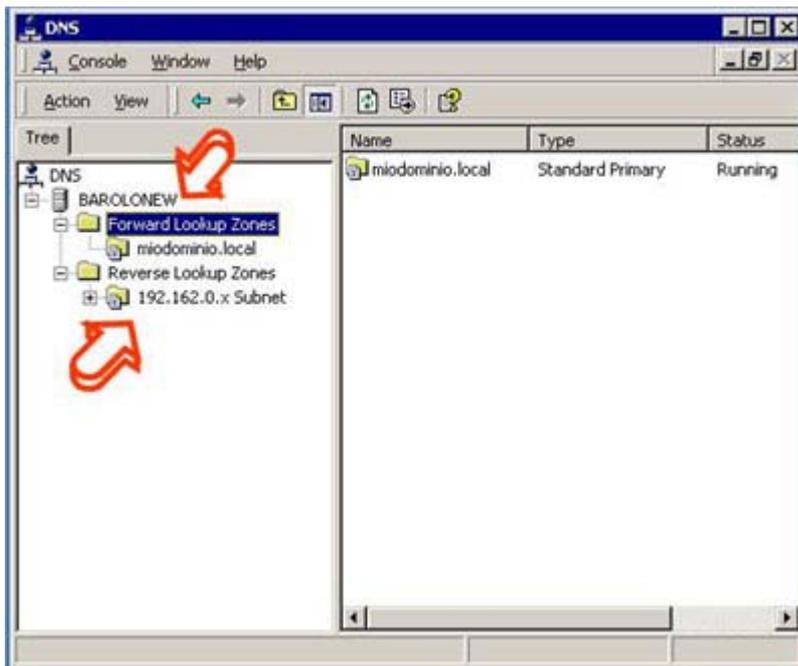
È chiaro che, essendo il file lmhosts un archivio statico residente su ogni client della rete, è estremamente oneroso dal punto di vista del costo di gestione e ne è sconsigliabile il suo utilizzo anche in piccole realtà.

È possibile che si verifichino i seguenti tipi di problemi a causa degli errori connessi al file lmhosts quali:

- Il file lmhosts non contiene il nome del calcolatore.
- Il nome del calcolatore nel file lmhosts o nel comando è errato o vi è un errore di sintassi.

- Viene inserito un indirizzo IP non valido per il nome del calcolatore nel file lmhosts.
- Il file lmhosts contiene più voci per lo stesso calcolatore su linee separate; in tale caso la prima voce è quella utilizzata.
- È stata aggiunta per errore una corrispondenza per un nome di calcolatore con un indirizzo IP nel file hosts (invece che in lmhosts).

Se siamo in presenza di sistemi Windows 2000 o Windows Xp Professional appartenenti a un dominio Active directory, la ricerca avviene attraverso il server DNS e di conseguenza anche il servizio DDNS sul server deve essere opportunamente configurato. Come vedremo nella sezione seguente, in un server correttamente configurato deve esistere la zona diretta miominio.local del dominio e una zona inversa per ogni subnet IP esistente nella rete Windows (es: 192.168.0.x).



Strumenti per la diagnostica e soluzioni di problemi nell'ambiente Netbios

Come abbiamo già detto, NetBios su TCP/IP (NetBT) risolve i nomi netbios in indirizzi IP. L'implementazione di Microsoft di TCP/IP offre molte opzioni per la risoluzione del nome NetBIOS, compresa la ricerca della cache locale dei nomi, l'interrogazione del server WINS, i broadcast, l'interrogazione del server DNS e, infine, la ricerca nel file LMHOSTS e HOSTS.

Nbtstat

Nbtstat è uno strumento utile per la soluzione dei problemi di transcodifica dei nomi NetBIOS. Il comando **nbtstat** consente l'eliminazione o la correzione delle voci precaricate. Di seguito vediamo i più interessanti usi del comando:

- **nbtstat -n** visualizza i nomi che sono stati registrati localmente sul sistema tramite applicazioni come il **servizio** server (programma che tra l'altro gestisce la condivisione dei dischi in ambiente NT);
- **nbtstat -c** mostra la cache del nome NetBIOS che contiene le corrispondenze del nome con l'indirizzo per altri computer;
- **nbtstat -R** pulisce la cache del nome e la ricarica dal file LMHOSTS;
- **nbtstat -a <nome>** visualizza la tabella dei nomi NetBIOS di un computer remoto;
- **nbtstat -S** visualizza le sessioni client e server NetBIOS, elencando i computer remoti solo in base all'indirizzo IP di destinazione.

Esempio di output del comando nbtstat -s :

```
C:\WINNT\Profiles\Administrator>nbtstat -s
```

```
Local Area Connection 2:
Node IpAddress: [130.204.10.1] Scope Id: []
NetBIOS Connection Table
```

```
Local Name State In/Out Remote Host Input Output
-----
ALA Connected In ALEATICO <00> 1KB 2KB
ALA Connected In MEDALEANICO <00> 1KB 2KB
ALA Connected In GHEMME <00> 1KB 2KB
ALA Connected In CARSO <00> 1KB 2KB
ALA Listening
```

Nella tabella seguente vengono descritte le intestazioni di colonna generate da **nbtstat -s**

Intestazione	Descrizione
Input	Il numero di byte ricevuti.
Output	Il numero di byte inviati.
In/Out	Indica se la connessione proviene dal computer (in uscita) o se è diretta al computer locale (in ingresso) da un altro sistema.
Life	L'intervallo di tempo prima dell'eliminazione della voce cache della tabella nomi.
Local Name	Il nome NetBIOS locale associato alla connessione.
Remote Host	Il nome o l'indirizzo IP associato al computer remoto.
<00>	L'ultimo byte di un nome NetBIOS convertito in valore esadecimale. I nomi NetBIOS comprendono 16 caratteri. L'ultimo byte è in genere particolarmente importante, in quanto uno stesso nome potrebbe essere presente più volte nello stesso computer e differenziarsi solo per l'ultimo byte. Nei testi ASCII, ad esempio, <20> indica uno spazio.
Type	Il tipo di nome. Può essere un nome univoco o un nome di gruppo.
Status	Indica se il servizio NetBIOS del computer remoto è in esecuzione (<i>Registered</i>) o se un nome di computer duplicato ha registrato lo stesso servizio (<i>Conflict</i>).
State	Stato delle connessioni NetBIOS.

Netstat

Netstat visualizza le statistiche di protocollo e i collegamenti TCP/IP attuali. Questo comando ci permette di analizzare lo stato di tutte le connessioni di rete, per comprendere come e con chi il calcolatore interagisce sulla rete.

Di seguito vediamo i più interessanti switch del comando:

- **Netstat -a** visualizza tutte le connessioni TCP attive e le porte TCP e UDP su cui il computer è in attesa di connessione.
- **Netstat -n** visualizza le connessioni TCP attive, gli indirizzi e i numeri di porta vengono espressi numericamente e non viene effettuato alcun tentativo di determinare i nomi.

Esempio di output del comando netstat -a

```
C:\>netstat -a
```

Connessioni attive

```
Proto Indirizzo locale Indirizzo esterno Stato
```

```
TCP capriccio:1064 chianti.unibo.it:microsoft-ds ESTABLISHED
TCP capriccio:1555 ala.unibo.it:3389 ESTABLISHED
TCP capriccio:1676 ala.unibo.it:microsoft-ds ESTABLISHED
TCP capriccio:epmap capriccio.unibo.it:0 LISTENING
TCP capriccio:microsoft-ds capriccio.unibo.it:0 LISTENING
TCP capriccio:1025 capriccio:0 LISTENING
TCP capriccio:1064 capriccio.unibo.it:0 LISTENING
TCP capriccio:5000 capriccio.unibo.it:0 LISTENING
TCP capriccio:netbios-ssn capriccio.unibo.it:0 LISTENING
```

Netdiag

Netdiag è uno strumento, presente solo in Windows 2000 e Xp, molto utile per la diagnostica e per la risoluzione di molti problemi che si possono presentare nelle reti basate sull'ultimo sistema operativo di rete della Microsoft.

Questa utility non è presente di default nelle installazioni di Windows 2000, ma deve essere aggiunta lanciando l'apposito programma di setup che risiede nei Compact Disc di Windows 2000

Professional o Windows Xp Pro e Windows 2000 Server, nella directory `\support\tools\`.

L'utility crea un report diagnostico sullo stato del calcolatore e delle connessioni di rete a vari livelli, lanciando una serie di test che permettono di verificare dove risiedono e di quale natura sono i problemi di connettività.

Le funzionalità che vengono analizzate quando si esegue l'utility NETDIAG, comprendono:

- *Scheda di rete.* NETDIAG esegue un test su tutte le interfacce di rete configurate per verificare problemi sui cablaggi di rete.
- *Default gateway.* L'utility cerca di contattare il default gateway per verificarne l'efficienza. Se ad esempio il router non è disponibile e il domain controller risiede al di là del router, l'utente sarà incapace di eseguire il **logon** alla rete o qualsiasi connessione a file server non residenti nella stessa sottorete.
- *Domain Name System (DNS).* L'utility esegue query di test al DNS server configurato nello stack TCP/IP. Se il sistema è configurato in un dominio Active Directory e il DNS server non viene raggiunto, il calcolatore non potrà conoscere né il nome del domain controller né il suo IP.
- *Domain Controller Discovery Test.* Netdiag cerca di contattare il domain controller del dominio Active Directory di cui fa parte il calcolatore. Se non viene trovato l'autenticazione dell'utente non potrà avvenire.
- *LDAP test.* Infine l'utility cerca di eseguire una particolare query LDAP sul domain controller del dominio per verificare il corretto funzionamento dell'Active Directory.

Di seguito vediamo i parametri opzionali del comando netdiag:

```
/q - Quiet output, visualizza solo gli errori
/v - Visualizza tutte le informazioni in modo dettagliato
/l - Invece di visualizzare le informazioni crea un file dal nome NetDiag.log
/debug - Visualizza ancora più informazioni dello switch /v
/d:<DomainName> - Cerca di contattare il domain controller del dominio
specificato
/fix - Se il programma trova degli errori prova a risolverli in maniera
automatica.
/DcAccountEnum - Esegue il controllo sui computer account dei domain controller.
/test:<test name> - Esegue esclusivamente il test specificato,dalla lista:
IpConfig - IP config Test
Autonet - Autonet address Test
IpLoopBk - IP loopback ping Test
```

DefGw - Default gateway Test
NbtNm - NetBT name Test
WINS - WINS service Test
Winsock - Winsock Test
DNS - DNS Test
Browser - Redir and Browser Test
DsGetDc - DC discovery Test
DcList - DC list Test
Trust - Trust relationship Test
Kerberos - Kerberos Test
Ldap - LDAP Test
Route - Routing table Test
Netstat - Netstat information Test
Bindings - Bindings Test
WAN - WAN configuration Test
Modem - Modem diagnostics Test
Netware - Netware Test
IPX - IPX Test
IPSec - IP Security Test

Vediamo e analizziamo un esempio di output del comando NETDIAG:

```
C:\Documents and Settings\Administrator>netdiag
```

```
.....  
  
Computer Name: BAROLONEW  
DNS Host Name: barolonew.miodominio.local  
System info : Windows 2000 Server (Build 2195)  
Processor : x86 Family 6 Model 4 Stepping 2, AuthenticAMD  
List of installed hotfixes :  
Q147222  
Q295688  
Q320206  
q323172  
Q323255  
Q324096  
Q324380  
Q326830  
Q326886  
Q328310  
Q329115  
Q329170  
Q329834  
Q810030  
Q810649  
  
Netcard queries test . . . . . : Passed  
  
Per interface results:  
  
Adapter : Local Area Connection  
  
Netcard queries test . . . : Passed  
  
Host Name . . . . . : barolonew.miodominio.local  
IP Address . . . . . : 192.168.0.1  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . : 192.168.0.254  
Primary WINS Server . . . . : 192.168.2.5  
Dns Servers . . . . . : 192.168.2.6
```

AutoConfiguration results. : Passed

Default gateway test . . . : Passed

NetBT name test. : Passed

WINS service test. : Passed

Global results:

Domain membership test : Passed

NetBT transports test. : Passed

List of NetBt transports currently configured:

NetBT_Tcpip_{7294CBF9-FDF5-438A-9692-D19A5B5D7109}

1 NetBt transport currently configured.

Autonet address test : Passed

IP loopback ping test. : Passed

Default gateway test : Passed

NetBT name test. : Passed

Winsock test : Passed

DNS test : Passed

Redir and Browser test : Passed

List of NetBt transports currently bound to the Redir

NetBT_Tcpip_{7294CBF9-FDF5-438A-9692-D19A5B5D7109}

The redir is bound to 1 NetBt transport.

List of NetBt transports currently bound to the browser

NetBT_Tcpip_{7294CBF9-FDF5-438A-9692-D19A5B5D7109}

The browser is bound to 1 NetBt transport.

DC discovery test. : Passed

DC list test : Failed

[WARNING] Cannot call DsBind to ala.miodominio.local (192.168.2.6).

[SEC_E_SECURITY_QOS_FAILED]

Trust relationship test. : Failed

Secure channel for domain 'miodominio' is to '\\ALA'.

[FATAL] Cannot test secure channel for domain 'miodominio' to DC 'ala'.

[ERROR_NO_LOGON_SERVERS]

Kerberos test. : Skipped

```
LDAP test. . . . . : Passed
[FATAL] Cannot open an LDAP session to 'ala.miodominio.local at '192.168.2.6'.
[WARNING] Failed to query SPN registration on DC 'ala.miodominio.local'.
[FATAL] Cannot open an LDAP session to 'chianti.miodominio.local' at
'192.168.2.5'.
[WARNING] Failed to query SPN registration on DC 'chianti.miodominio.local'
.
```

```
Bindings test. . . . . : Passed
```

```
WAN configuration test . . . . . : Skipped
No active remote access connections.
```

```
Modem diagnostics test . . . . . : Passed
```

```
IP Security test . . . . . : Passed
IPSec policy service is active, but no policy is assigned.
```

```
The command completed successfully
```

Come si può evincere dall'output di questo comando, esistono alcuni problemi di connessione con i due server Domain controller del dominio miodominio.local ALA e CHIANTI, di cui uno è un DNS server e l'altro è un WINS server, che non risiedono nella stessa sottorete. Il malfunzionamento può ricercarsi in:

- rallentamento della rete;
- presenza di firewall che sezionano la rete mal configurati.

Microsoft Performance Monitor

Il Microsoft Performance Monitor incluso nei prodotti Windows NT, Windows 2000 e Windows Xp, è uno strumento grafico che ci permette di visualizzare lo stato del sistema attraverso l'analisi di determinati parametri nell'unità di tempo. Questi dati vengono ricavati dai componenti del computer. Quando un componente di sistema esegue un'operazione sul sistema, vengono generati dei dati sulle prestazioni. Tali dati costituiscono un oggetto prestazione e ad essi verrà solitamente assegnato il nome del componente che li ha generati. L'oggetto Processore, ad esempio, è una raccolta di dati sulle prestazioni relative ai processori del sistema.

Nel sistema operativo sono incorporati diversi **oggetti prestazioni** che in genere corrispondono ai principali componenti hardware, ad esempio memoria, processori e così via. È possibile che alcune applicazioni installino oggetti prestazioni propri. Servizi come WINS e applicazioni server come Microsoft Sql Server, ad esempio, includono oggetti prestazioni, che possono essere monitorati utilizzando registri e grafici di prestazioni.

Ad ogni oggetto prestazione sono associati **contatori** che rappresentano dati su aspetti specifici di un sistema o di un servizio. Il contatore Pagine/sec associato all'oggetto Memoria, ad esempio, tiene traccia dell'indice di paging della memoria.

Il sistema può rendere disponibili molti oggetti, ma gli oggetti predefiniti utilizzati con maggiore frequenza per il monitoraggio dei componenti del sistema sono:

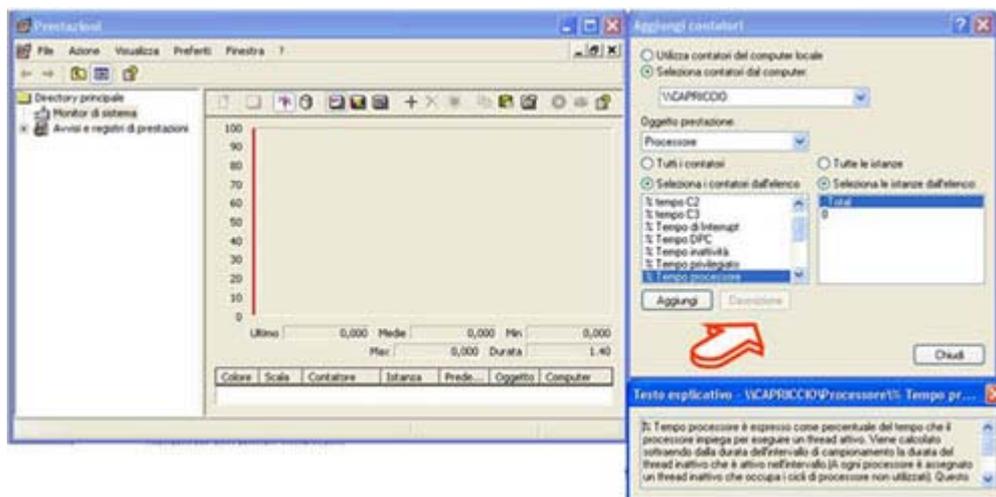
- Cache.

- Memoria.
- File di pagin.
- Disco fisico.
- Processo.
- Processore.
- Server.
- Sistema.
- Thread.

Di seguito sono riportati servizi o funzioni di Windows in grado di aiutarci nell'analisi delle problematiche di rete nell'ambiente Microsoft:

Funzione o servizio da monitorare	Oggetto prestazione disponibile
TCP/IP	Oggetti ICMP (Internet Control Message Protocol), IP (Internet Protocol), NetBT (NetBios su TCP/IP), TCP (Transmission Control Protocol) e UDP (User Datagram Protocol)
Servizi Browser, Workstation e Server	Oggetti Browser, Redirector e Server
WINS	Oggetto WINS
Servizio directory	Oggetto NTDS (servizio directory di NT)
Attività server di stampa	Oggetto coda di stampa

Per una descrizione dettagliata dei dati forniti da un particolare contatore associato ad un oggetto prestazione, fare clic sul pulsante **Descrizione** nella finestra di dialogo **Aggiungi contatori**.



Anche se alcuni oggetti come Memoria e Server possiedono una sola **istanza**, altri oggetti prestazione possono disporre di più istanze. Se un oggetto ha più istanze, sarà possibile aggiungere dei contatori per tenere traccia delle statistiche di ciascuna istanza o di tutte le istanze contemporaneamente.

A seconda di come è stato definito, il contatore può avere i valori seguenti:

- La misurazione più recente di un aspetto dell'utilizzazione delle risorse. Questi sono detti anche contatori istantanei. Un esempio è il contatore Memoria\Mbyte_disponibili, ovvero la dimensione della memoria fisica, espressa in Megabyte, disponibile per i processi in

esecuzione.

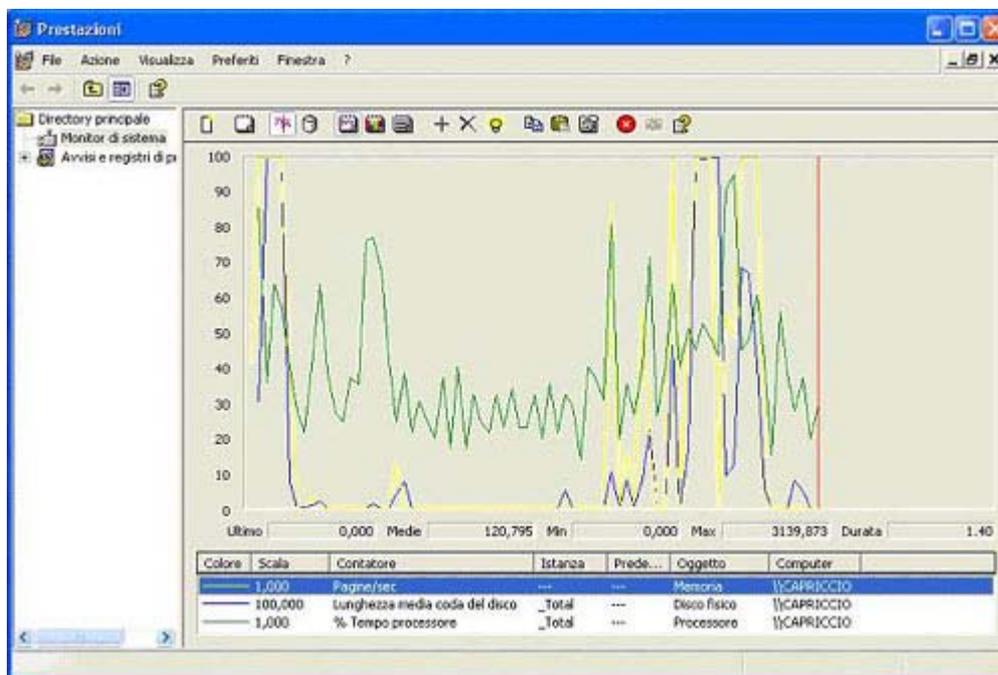
- La media delle ultime due misurazioni per il periodo tra i campionamenti. Dato che i contatori non sono mai cancellati, questa è in realtà una media della differenza tra le misurazioni. Un esempio è il contatore Memoria\Pagine/sec, che riporta la frequenza al secondo sulla base del numero medio di pagine di memoria, facendo riferimento agli ultimi due campionamenti.

La combinazione di nome computer, oggetto, contatore, istanza e indice dell'istanza è chiamata percorso del contatore. In genere il percorso del contatore è visualizzato negli strumenti nel modo seguente:

Nome_computer\Nome_oggetto(Nome_istanza#Numero_indice)\Nome_contatore

Se volessimo tracciare i byte inviati al secondo dell'interfaccia di rete Intel Pro 100 del computer capriccio il percorso visualizzato sarebbe: Capriccio\Interfaccia_di_rete (Connessione_di_rete_Intel_PRO100)\Byte_inviati/sec.

Lanciando il programma perfmon da linea di comando o dall'icona Performance monitor negli strumenti amministrativi possiamo avere il seguente output da analizzare:



Microsoft Network Monitor

Microsoft Network Monitor è uno strumento sviluppato da Microsoft per rendere più agevole e conveniente il compito di soluzione dei problemi di rete complessi. Viene fornito in versione completa nel prodotto *Microsoft System Management Server* (prodotto che serve per gestire e monitorare integralmente i client in modo centralizzato) e in versione ridotta come parte di Windows NT4 server e Windows 2000 server. Inoltre, in tutti i sistemi operativi della famiglia Microsoft, partendo da Windows 95, è presente il software *Network Monitor Agent*. Le stazioni che eseguono Network Monitor possono collegarsi alle stazioni che eseguono il software agente, attraverso la rete o con un collegamento **dial-up** per eseguire il tracciamento o la cattura dei dati che attraversano la rete. Questo può essere uno strumento molto utile, anche se molto complesso, per la risoluzione dei problemi.

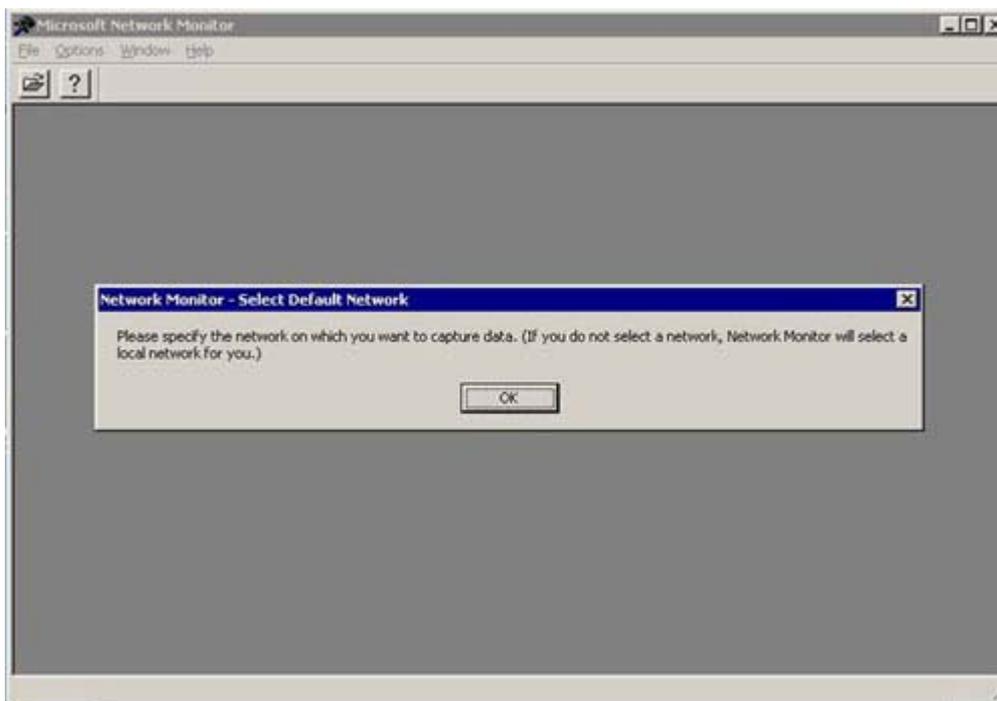
Network Monitor funziona impostando la scheda di rete per consentire la cattura del traffico da e verso il computer locale. I filtri di cattura possono essere definiti in modo che vengano salvati solo **frame** specifici per l'analisi. I filtri possono essere definiti in base a veri parametri quali: indirizzi di

origine e di destinazione della scheda di rete, indirizzi di protocollo di origine e destinazione e molto altro. Una volta ottenuta la cattura del traffico di rete, può essere utilizzata una visualizzazione filtrata per selezionare maggiormente il problema. La visualizzazione filtrata consente di selezionare i singoli protocolli (es: Ethernet, IP, TCP, NetBT, SMB).

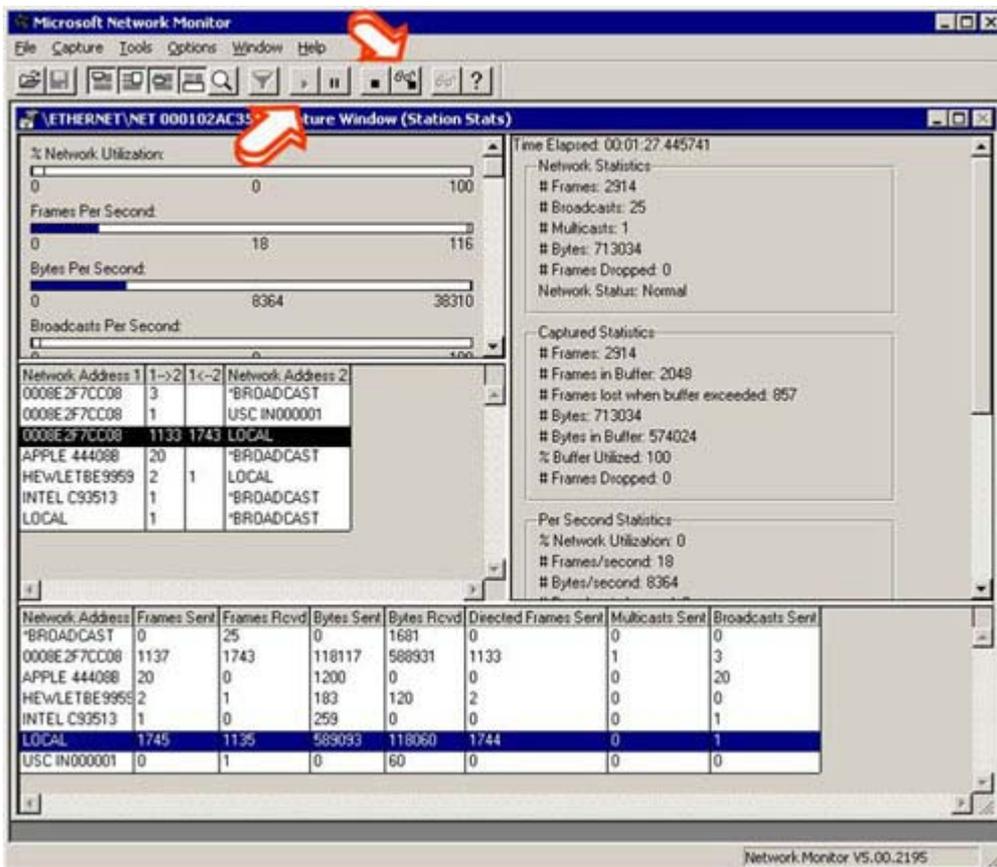
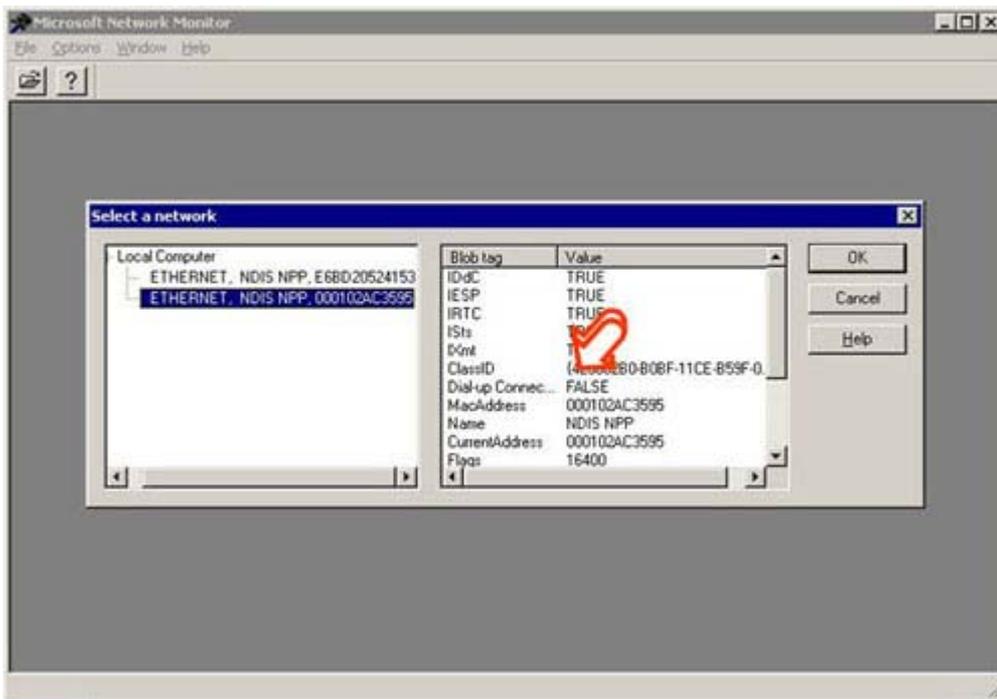
Filtrata una cattura, *Network Monitor* interpreta i dati di traccia binari in termini leggibili ricorrendo a opportuni programmi di analisi. L'Output di uscita è composto da tre sezioni:

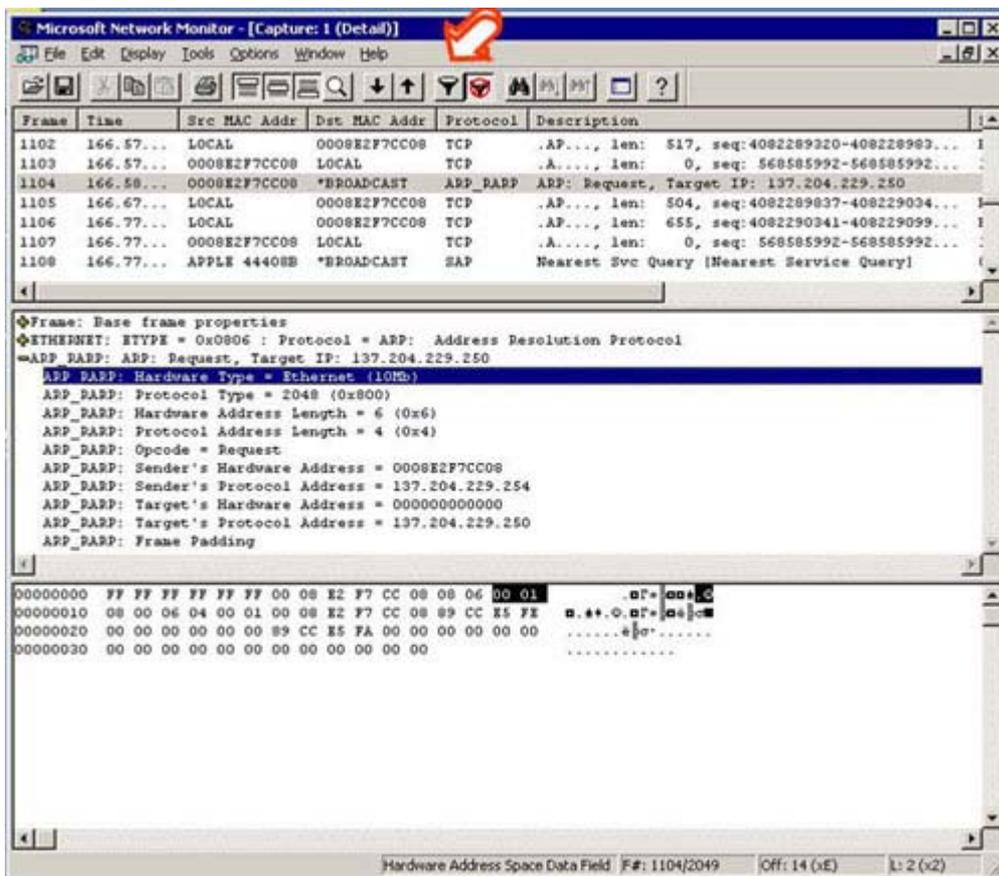
- Finestra di riassunto.
- Finestra di descrizione dettagliata.
- Output esadecimale.

Ora vediamo la sequenza di operazioni per una cattura di traffico da e verso un calcolatore:



Per analizzare il traffico che risiede sulla scheda di rete locale è necessario selezionare la scheda Ethernet con la caratteristica Dial-up connection = FALSE.





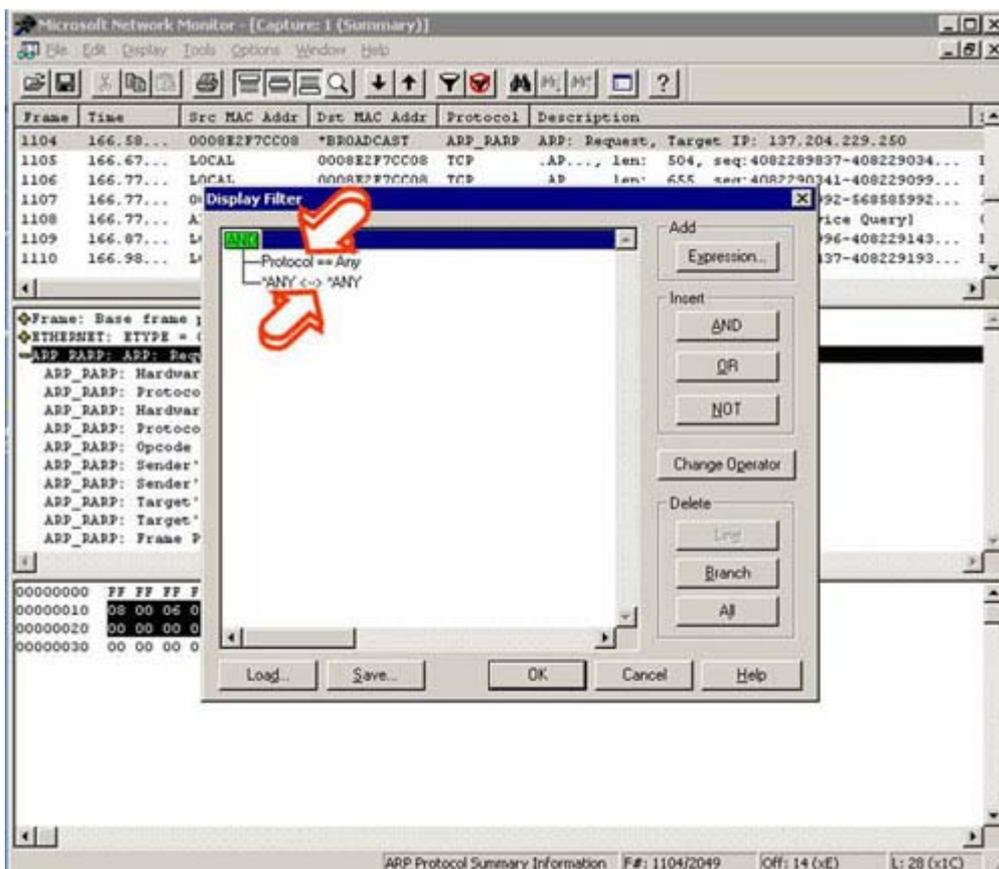
Microsoft Network Monitor - [Capture: 1 (Detail)]

Frame	Time	Src MAC Addr	Dst MAC Addr	Protocol	Description
1102	166.57...	LOCAL	0008E2F7CC08	TCP	.AP..., len: 517, seq: 4082289320-408228982...
1103	166.57...	0008E2F7CC08	LOCAL	TCP	.A..., len: 0, seq: 568585992-568585992...
1104	166.58...	0008E2F7CC08	*BROADCAST	ARP_RARP	ARP: Request, Target IP: 137.204.229.250
1105	166.67...	LOCAL	0008E2F7CC08	TCP	.AP..., len: 504, seq: 4082289837-408229034...
1106	166.77...	LOCAL	0008E2F7CC08	TCP	.AP..., len: 655, seq: 4082290341-408229099...
1107	166.77...	0008E2F7CC08	LOCAL	TCP	.A..., len: 0, seq: 568585992-568585992...
1108	166.77...	APPLE 44408B	*BROADCAST	SAP	Nearest Svc Query (Nearest Service Query)

Frame: Base frame properties
ETHERNET: ETYP = 0x0806 : Protocol = ARP: Address Resolution Protocol
ARP_RARP: ARP: Request, Target IP: 137.204.229.250
ARP_RARP: Hardware Type = Ethernet (10Mb)
ARP_RARP: Protocol Type = 2048 (0x800)
ARP_RARP: Hardware Address Length = 6 (0x6)
ARP_RARP: Protocol Address Length = 4 (0x4)
ARP_RARP: Opcode = Request
ARP_RARP: Sender's Hardware Address = 0008E2F7CC08
ARP_RARP: Sender's Protocol Address = 137.204.229.254
ARP_RARP: Target's Hardware Address = 000000000000
ARP_RARP: Target's Protocol Address = 137.204.229.250
ARP_RARP: Frame Padding

00000000 FF FF FF FF FF FF 00 08 E2 F7 CC 08 08 06 00 01
00000010 08 00 06 04 00 01 00 08 E2 F7 CC 08 09 CC E5 FX
00000020 00 00 00 00 00 00 09 CC E5 FA 00 00 00 00 00
00000030 00 00 00 00 00 00 00 00 00 00 00 00 00

Hardware Address Space Data Field F#: 1104/2049 Off: 14 (xE) L: 2 (x2)



Microsoft Network Monitor - [Capture: 1 (Summary)]

Frame	Time	Src MAC Addr	Dst MAC Addr	Protocol	Description
1104	166.58...	0008E2F7CC08	*BROADCAST	ARP_RARP	ARP: Request, Target IP: 137.204.229.250
1105	166.67...	LOCAL	0008E2F7CC08	TCP	.AP..., len: 504, seq: 4082289837-408229034...
1106	166.77...	LOCAL	0008E2F7CC08	TCP	.AP..., len: 655, seq: 4082290341-408229099...
1107	166.77...	0008E2F7CC08	LOCAL	TCP	.A..., len: 0, seq: 568585992-568585992...
1108	166.77...	APPLE 44408B	*BROADCAST	SAP	Nearest Svc Query (Nearest Service Query)
1109	166.87...	LOCAL	0008E2F7CC08	TCP	.AP..., len: 504, seq: 408229143-408229193...
1110	166.98...	LOCAL	0008E2F7CC08	TCP	.AP..., len: 504, seq: 408229193-408229243...

Frame: Base frame properties
ETHERNET: ETYP = 0x0806 : Protocol = ARP: Address Resolution Protocol
ARP_RARP: ARP: Request, Target IP: 137.204.229.250
ARP_RARP: Hardware Type = Ethernet (10Mb)
ARP_RARP: Protocol Type = 2048 (0x800)
ARP_RARP: Hardware Address Length = 6 (0x6)
ARP_RARP: Protocol Address Length = 4 (0x4)
ARP_RARP: Opcode = Request
ARP_RARP: Sender's Hardware Address = 0008E2F7CC08
ARP_RARP: Sender's Protocol Address = 137.204.229.254
ARP_RARP: Target's Hardware Address = 000000000000
ARP_RARP: Target's Protocol Address = 137.204.229.250
ARP_RARP: Frame Padding

00000000 FF FF FF FF FF FF 00 08 E2 F7 CC 08 08 06 00 01
00000010 08 00 06 04 00 01 00 08 E2 F7 CC 08 09 CC E5 FX
00000020 00 00 00 00 00 00 09 CC E5 FA 00 00 00 00 00
00000030 00 00 00 00 00 00 00 00 00 00 00 00 00

Display Filter
Add
Expression...
Insert
AND
OR
NOT
Change Operator
Delete
Line
Branch
All
Load... Save... OK Cancel Help

Protocol == Any
"ANY" <-> "ANY"

ARP Protocol Summary Information F#: 1104/2049 Off: 14 (xE) L: 28 (x1C)

Lo strumento descritto richiede conoscenze molto elevate sulle reti e sui sistemi operativi di rete, quindi in molti casi il suo uso richiede l'assistenza di un tecnico con know-how approfondito del sistema informatico presente.

Infine, se si stanno inviando tracce di traffico di rete, ottenute con il Network Monitor, a personale altamente qualificato per una diagnostica avanzata, è utile che queste siano in forma elettronica anziché in forma stampata, perché possono essere manipolate e vagliate elettronicamente.

Microsoft Knowledge Base

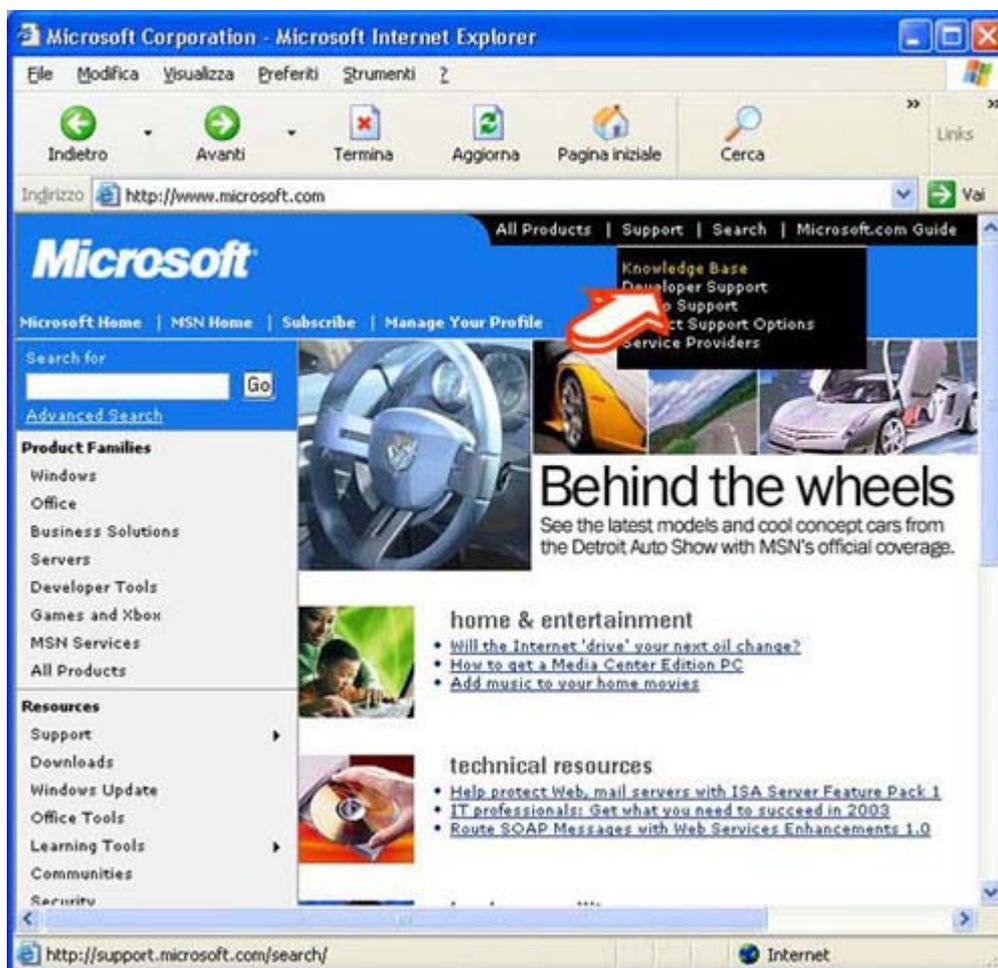
Microsoft Knowledge Base (KB) è un'eccellente fonte di informazioni su tutti gli aspetti legati ai prodotti e ai sistemi operativi di Microsoft. Contiene migliaia di articoli scritti da professionisti del supporto dell'unità *Compare Systems di Microsoft*. Gli articoli vengono aggiornati quotidianamente e comprendono i seguenti argomenti:

- Informazioni sull'installazione e la configurazione dei sistemi operativi Microsoft.
- Lo stato dei problemi conosciuti e delle soluzioni.
- Aggiornamenti dei sistemi operativi (*Service Pack, Hot fix*).
- Discussione sulla tecnologia implementata.
- Informazione specifiche sull'hardware.

Microsoft KB è disponibile per mezzo di svariate fonti, compresa Internet, diversi servizi in linea e attraverso abbonamenti educational a CD-Rom come Microsoft Tech-Net.

È possibile ricercare la risoluzione di un problema attraverso ricerche *full text* utilizzando un Browser Web sul sito <http://www.microsoft.com> o anche sul sito <http://msdn.microsoft.com>.

Vediamo un esempio che ci permette di trovare informazioni utili su problemi di risoluzione dei nomi basata su LMHOSTS in ambiente Windows 98. Quindi interroghiamo la Microsoft Knowledge Base con le seguenti parole chiavi *LMHOSTS and Windows and 98*.



Ricerca nella Knowledge Base - Microsoft Internet Explorer

File Modifica Visualizza Preferiti Strumenti ?

Indietro Avanti Termina Aggiorna Pagina iniziale Cerca Preferiti Links

Ingrasso http://support.microsoft.com/default.aspx?scid=fh;[n];kbhowto

Microsoft Product Support Services Italia Microsoft

Home Cerca Domande e Risposte Download Contattaci Newsgroup Invia Stampa Aiuto

Cerca (KB)

Inserisci le chiavi di ricerca

KB italiana
KB italiana
KB inglese

Assistenza Tecnica

Supporto assistito
Supporto in autonomia
Utenti Final
Utenti Education
Soluzioni per aziende
Partner e Rivenditori
Sviluppatori
Professionisti IT

Supporto Internazionale

Ricerca nella Knowledge Base

← ← ←

Gracie ai vostri suggerimenti abbiamo ridisegnato l'interfaccia di ricerca rendendola più facile da utilizzare e raggiungibile in qualsiasi momento.

Con questo nuovo strumento potrete consultare più di 250.000 articoli creati per voi dai nostri tecnici.

La Knowledge Base è costantemente aggiornata, espansa e perfezionata per assicurarvi informazioni sempre aggiornate.

Cerca (KB)

Per soluzioni contenenti... KB italiana
 KB inglese

Seleziona un prodotto - Tutti I Prodotti Microsoft -

Per soluzioni contenenti... Imhosts and windows and 98

Utilizzando... Tutte le parole

Limite risultati 25 articoli

Cerca Tutto il testo
 Solo titolo

Data massima Qualsiasi data

Val

The screenshot shows the Microsoft Help and Support website in Italian, accessed via Microsoft Internet Explorer. The browser's address bar contains the search query: `INtBQuery=inhosts+and+windows+and+98&Query=inhosts+and+windows+and+98&keywordType=ALL&na:Results=25&Tites=false&runDays=`. The page displays search results for the query "inhosts and windows and 98".

The search results section indicates: "I risultati della ricerca includono solo gli articoli che contengono il testo inhosts and windows and 98." It shows a summary of 4 articles:

- Accesso remoto, attivazione e esplorazione in WinNT/WinNT tramite TCP/IP, IPX/SPX e NetBEUI**
Accesso remoto, attivazione e esplorazione in WinNT/WinNT tramite TCP/IP, IPX/SPX o NetBEUI. L'obiettivo di questo articolo è quello di chiarire la modalità di configurazione dei client Windows NT, ad esempio Windows 95, Windows 98 e Windows NT...
- Come aggiornare manualmente computer alla Risorse di Rete**
Questo articolo descrive le funzioni di browsing in Risorse di Rete. Si possono avere macchine con Windows NT Server o Windows NT Workstation che richiedono una costante enumerazione nelle Risorse di Rete. E' possibile ottenere questa funzionalità...
- elenco dei bug corretti in Windows NT 4.0 Service Pack 5 (Parte 2)**
Questo articolo è la seconda parte di un elenco completo dei numeri degli articoli relativi ai bug corretti nel Service Pack 5 per Windows NT 4.0. I Service Pack sono cumulativi. Ciò significa che i bug fissati in un Service Pack sono fissati anche...
- elenco dei bug corretti in Windows NT 4.0 e in Terminal Server Service Pack 4 (Parte 2)**
Questo articolo è la terza parte di un elenco di numeri di articoli relativi ai bug corretti nel Service Pack 4 per Windows NT 4.0 e Windows NT Server 4.0, Terminal Server Edition. I Service Pack sono cumulativi. Ciò significa che i bug corretti in un...

Additional resources include:

- Contatta Microsoft**
Support Options and Pricing, Phone Numbers and Online Support
- Webcast**
Presentazioni Online su prodotti microsoft

The page footer shows the date "Ultima Revisione: sabato 10 gennaio 2003" and the status "Operazione completata".

Si ottengono molti più risultati ripetendo la stessa ricerca nella base di conoscenza (*Knowledge Base*, KB) inglese:

The screenshot shows the Microsoft Support website in Italian. The search bar at the top contains the query "inhosts and windows and 90". The search results section displays "Risultati della ricerca: 25 articoli". A red arrow points to the search bar, and another red arrow points to the first search result, which is a link to "Microsoft Knowledge Base article 901154: How to troubleshoot slow startup of Microsoft Exchange Server 2003".

Microsoft Help and Support - Microsoft Internet Explorer

Microsoft Product Support Services Italia

Cerca (00)

Inserisci la chiave di ricerca

it inglese

Visualizza le opzioni

Assistenza Tecnica

Supporto assistito

Supporto in autonomia

Utenti Finali

Utenti Education

Soluzioni per aziende

Partner e rivenditori

Sviluppatori

Professionisti IT

Supporto Internazionale

Migliora la tua ricerca

Anteprima

Visualizza solo i risultati

Seleziona un prodotto Microsoft

- All Microsoft Products -

Cerca nei risultati

inhosts and windows and 90

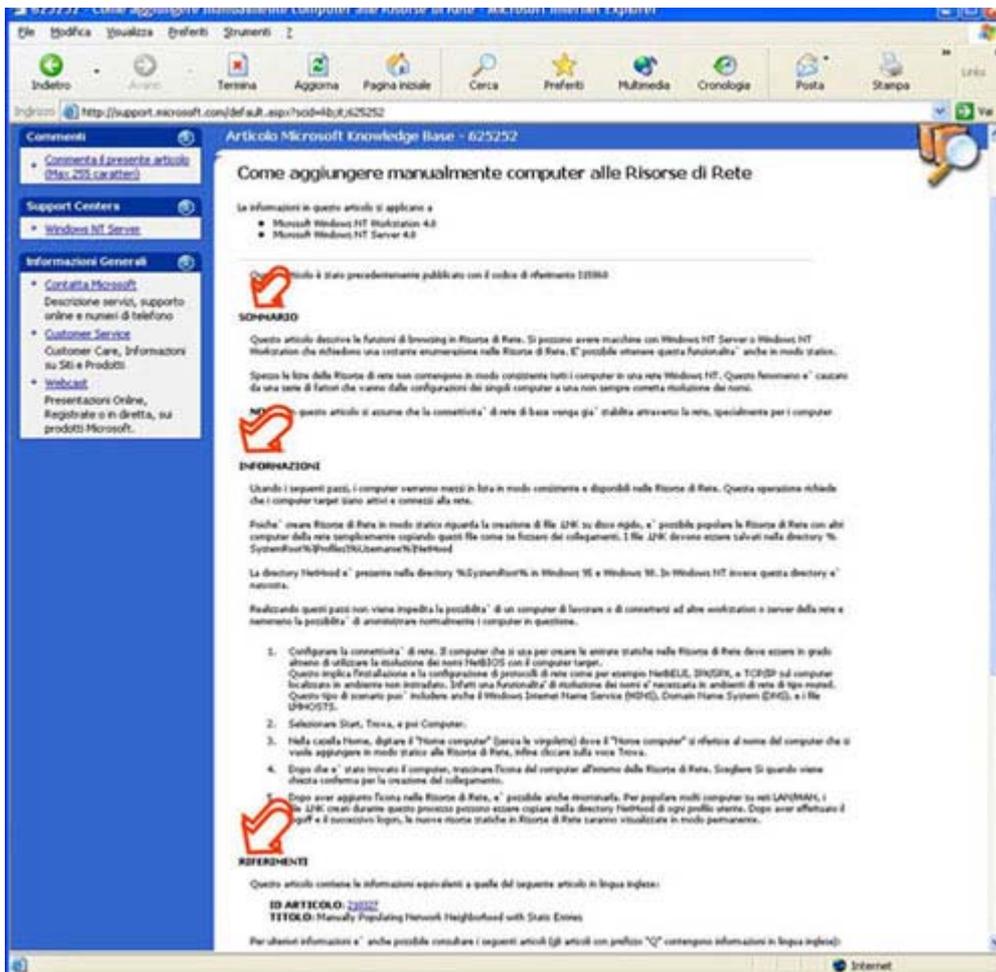
Vai

Scenario

Risultati della ricerca: 25 articoli

- Microsoft Exchange Authentication, Resolving Using TCP/IP, DNS, or NetBIOS**
Microsoft Exchange Authentication, Resolving Using TCP/IP, DNS, or NetBIOS This article has been written to help clarify how Windows NT clients, such as Windows 95, Windows 98, and Windows NT Workstation/Windows NT Server are supposed to be...
- UPHOSTS File Referenced in MSDN/GUIDE Is Not Parted at Startup by Windows NT/9x Clients**
The UPHOSTS or test file referenced in MSDN/GUIDE is not parted at startup by Windows NT/9x clients. This may occur when the remote file does not have at least CHANGE permission for the Network or E-veryone group.
- Requirements to Remote Network with Windows WinMta Dial-Up Networking Client**
This article describes the requirements to view (or browse) other computers on the network from a Microsoft Windows 9x, Windows 98, or Windows Millennium Edition (Me) client using a Dial-Up Networking connection.
- Windows WinMta RAS Client Cannot Log on to the Domain**
When you try to use a client running Microsoft Windows 9x, Windows 98, Windows Millennium Edition (Me) to connect to a Microsoft Windows NT Server 4.0-based domain through Remote Access Server (RAS), you may receive the following error message: No...
- MSN-040: NetBIOS Vulnerability May Cause Disruption to the Network Config**
Microsoft has released a patch that improves the ability of an administrator to protect against denial-of-service attacks against Windows NT 4.0 and Windows 2000-based computers. The NetBIOS over TCP/IP (NB-T) protocols are, by design, unauthenticated.
- Error Message Occurs When Attempting to Log on to a Remote Access Server**
When a Windows 95- or Windows 98-based client computer attempts to log on to the domain when it is connecting to a remote access server, the client may receive the following error message: The domain password you supplied is not correct, or access to...
- Error 53 When Changing Password with NET PASSWORD Command**
If you use the NET PASSWORD command to change your password on your Microsoft Windows 9x/NT client computer, you may receive the following error message: Error 53: An unexpected network error has occurred. Quit all network programs, restart your...
- Information About the TCP/IP Option Dialing Box**
This article provides information about the Transmission Control Protocol/Internet Protocol (TCP/IP) options in the Network Dialing box.
- File List for Dial-Up Networking 1.6 Upgrade**
NOTE: This article is for informational use only. It does not contain any troubleshooting information. If you are searching for troubleshooting information that is not mentioned in this article, search the Microsoft Knowledge Base again by using...
- Audio or Video Unavailable in NetMeeting Conference**
Audio and video may be unavailable during a NetMeeting conference.
- Windows TCP/IP Registry Entries**
This article documents the Windows registry entries for the TCP/IP Admin\Work\Profile folder on the Windows 9x CD-ROM. For more information about Windows TCP/IP settings, see the WinSx3 file in the Admin\Work\Profile folder on the Windows 9x CD-ROM.
- Windows Does Not Part the UPHOSTS File with DNS Enabled**
Windows does not part the UPHOSTS file if DNS (Domain Name System) is enabled.
- NTLIS Troubleshooting Startup of Windows Client Using TCP/IP**
When you start the Microsoft Exchange client, one of the more common reasons for slow startup is the failure to resolve the Microsoft Exchange Server TCP/IP host name. This document discusses the steps for eliminating host name resolution issues on...
- Windows 9x CD-ROM Directory Items C of 146**
This article lists the directory contents of the Windows 9x CD-ROM (part 2 of 146).
- Offline Services Are Not Removed from the Services Table**
The Cabinet\msi\Server\services.msi file is documented in the Microsoft Knowledge Base. This file does not remove an installed service when you use the Microsoft

Vediamo infine il rinvio a una delle pagine individuate:



Esempi di diagnosi e risoluzione di problemi di collegamento

Questo capitolo presenta alcuni possibili sintomi e relative risoluzioni di problemi di rete correlati al protocollo TCP/IP.



- ERROR 53 o impossibile trovare il server. Questi messaggi vengono visualizzati quando la risoluzione del nome fallisce per un particolare computer. Per determinare la causa dell'errore 53 quando ci si collega a un server dobbiamo compiere le seguenti operazioni:
 1. Se il computer si trova nella subnet locale, si controlli che il nome sia scritto correttamente, che il computer di destinazione sia acceso e che il suo stack TCP/IP sia configurato correttamente. Se il computer non si trova sulla subnet locale, assicurarsi che la corrispondenza del suo nome con il suo indirizzo IP sia disponibile nel file LMHOSTS o nei database WINS o DNS se utilizzati.
 2. Se tutti gli elementi TCP/IP sembrano installati e configurati correttamente, utilizzare il comando ping <<nome macchina remota>> per assicurarsi che il protocollo TCP/IP stia funzionando.
- Tempi di collegamento lunghi durante l'uso di LMHOSTS per la risoluzione di un nome macchina. Per determinare la causa di tempi di collegamento lunghi, dopo aver aggiunto una voce al file LMHOSTS, possiamo compiere le seguenti operazioni. Segnare la voce come

precaricata, ovvero inserita in modo automatico all'avvio, aggiungendo l'etichetta #PRE alla fine della voce. Quindi utilizzare il comando NBTSTAT -R per aggiornare immediatamente la cache dei nomi locali. Questo poiché un tempo di collegamento lungo può verificarsi a causa di file LMHOSTS di grandi dimensioni con la voce interessata inserita alla fine del file. In alternativa si può posizionare la voce più in alto nel file LMHOSTS. Il file LMHOSTS viene analizzato sequenzialmente per localizzare le voci senza la parola chiave #PRE, quindi occorre posizionare le voci di uso frequente nei pressi della parte alta del file e posizionare le #PRE nella parte bassa del file.

- Impossibile collegarsi a un server specifico. Per determinare la causa dei problemi di collegamento quando si specifica il nome di un server dobbiamo utilizzare il comando NBTSTAT -n per scoprire quale nome il server ha registrato sulla rete. L'output di questo comando elenca numerosi nomi registrati dal computer. Deve essere presente un nome che ha iniziali uguali al nome del computer, in caso contrario provare uno degli altri nomi visualizzati da NBTSTAT. L'utility NBTSTAT può anche essere utilizzata per visualizzare le voci di cache di computer remoti. Se il nome che i computer remoti stanno utilizzando è lo stesso e gli altri computer si trovano su una subnet remota, assicurarsi che abbiano la corrispondenza del server nei loro file LMHOSTS.

Conclusioni

In questa breve trattazione delle problematiche di rete in ambiente Windows, abbiamo cercato di offrire gli strumenti diagnostici opportuni per analizzare e quindi risolvere nel modo più semplice e rapido eventuali problemi. Dato che la complessità di tali problematiche cresce con l'eterogeneità degli ambienti presenti, è consigliato, dove possibile, creare realtà informatiche quanto più omogenee. Per esempio: un unico tipo di cablaggio, uno o al massimo due versioni di sistemi operativi operanti nella struttura con la stessa versione di service pack e con le stesse versioni di software applicativo.

Questa situazione, sembrerebbe di impossibile attuazione, visti i costi di aggiornamento di hardware e di licenze software. In realtà dobbiamo tenere conto del costo totale, detto **TCO** (*Total Cost of Ownership*), composto dal costo di acquisto e dal costo di manutenzione ordinaria e straordinaria, di un sistema informatico complesso. Un esempio di come può diventare costoso un sistema informatico eterogeneo in termini di tempo lavorativo perso, di chiamate di tecnici esterni, ecc, è possibile constatarlo svolgendo l'esercizio aperto.

I **referimenti bibliografici** on line consentono di svolgere ulteriori attività di approfondimento.