CAPITOLO 5

Il progetto della nostra LAN

A questo punto del libro, conoscendo i fondamenti teorici ed i componenti da impiegare nelle reti locali, siamo in grado di passare alla realizzazione di una LAN di medie dimensioni. Nella prima parte di questo capitolo sarà redatto un progetto che descrive il tipo di rete da realizzare, la sua destinazione d'uso ed i componenti necessari. La seconda parte è una dettagliata guida per la configurazione della LAN in ambiente Windows Server 2003, sistema operativo certamente indicato per utilizzi di questo tipo. E' bene precisare come nel proseguo non ci occuperemo di alcune operazioni, quali ad esempio l'installazione del sistema operativo, ampiamente documentata e peraltro semplice da portare a termine.

5.1 Schema della rete

La LAN che stiamo realizzando sia divisa in tre ambienti, ognuno dei quali abbia un certo numero di host. Supponiamo, inoltre, che la rete locale sia connessa ad Internet, per mezzo di connessione ADSL, abbastanza veloce da potere supportare tutti gli utenti.

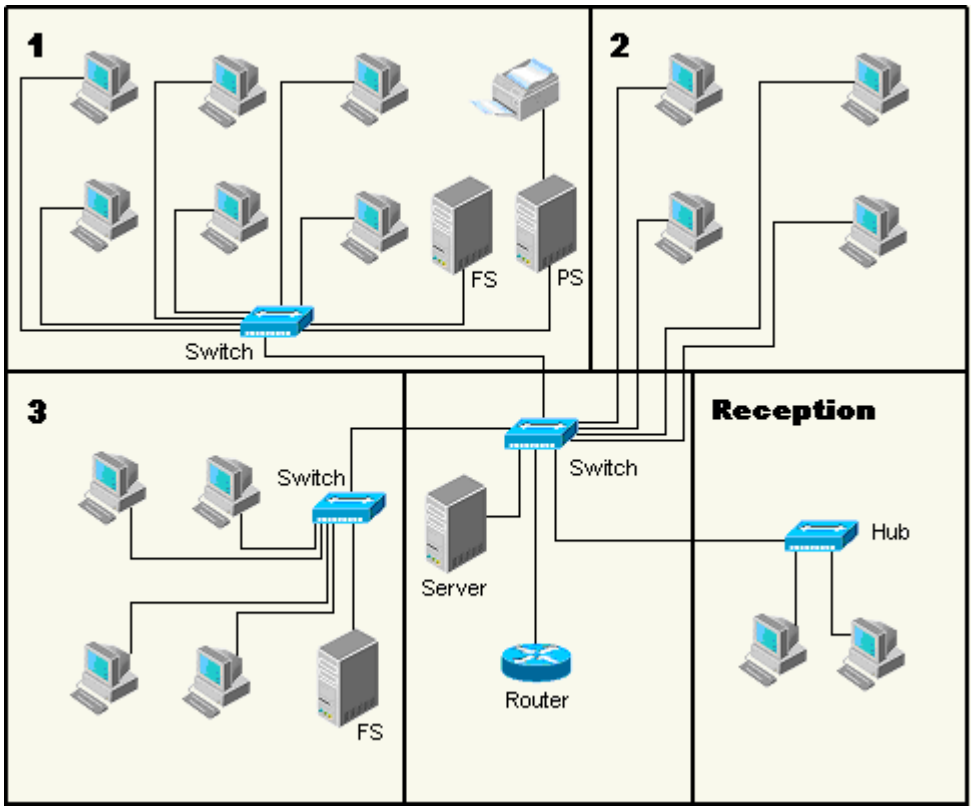

FOTO 5.1.1: Schema dell'ambiente in cui sarà realizzata la nostra rete locale

I tre ambienti della LAN abbiano caratteristiche diverse: la sala 1 contiene più postazioni di lavoro, che fanno grande utilizzo di una stampante dedicata, per cui è importante che tale sala sia dotata di un print server; la sala 2 contiene solo 4 host, i quali necessitano di velocità elevata nell'utilizzo della rete per manipolare file di grandi dimensioni quali video ed immagini, e per questo motivo sono collegati direttamente allo switch principale; la sala 3 fa uso prevalentemente di applicazioni client-server, per cui non richiede attenzioni particolari. Nella reception, inoltre, si trovano due PC che servono per registrazioni di clienti e gestione di appuntamenti ed impegni. E' prevista inoltre

una sala che contiene gli apparati di rete: in realtà nel nostro caso non è necessario avere uno spazio di questo tipo, ma in previsione di sviluppi futuri è meglio dotarsi sin dall'inizio di uno spazio dedicato al contenimento dei dispositivi di rete.

5.2 I dispositivi utilizzati

Il collegamento della LAN ad Internet avviene per mezzo di un router, che risulta molto più efficiente di una soluzione PC con modem. L'utilizzo del router come gateway mette a disposizione di tutti i dipendenti una larghezza di banda superiore ed offre la possibilità di effettuare contemporaneamente collegamenti multipli a Internet attraverso un'unica linea. Il nostro progetto prevede l'utilizzo di un router che incorpori funzioni di firewall, per evitare attacchi indesiderati dall'esterno. In alternativa è possibile anche acquistare un dispositivo firewall separato, da installare tra il router-gateway e la LAN. A monte del router-firewall troviamo lo switch principale, di tipo Fast Ethernet, che gestisce i diversi ambienti della rete. Gli utenti ad elevato consumo di banda (sala 2) sono direttamente connessi allo switch principale, per disporre di elevate prestazioni di rete. La sala 1 è dotata, oltre che del print-server (PS), di un file-server (FS) per i file che sono manipolati all'interno dell'ambiente. Anche la sala 3 è dotata di un file-server, per la gestione dei file maggiormente utilizzati.

La scelta di dotare le sale 1 e 3 di file-server, permette un numero minore di "uscite" dal proprio ambiente, mantenendo quindi la rete poco occupata. Nella sala che contiene gli apparati è presente un ulteriore server, che si occupa della gestione e del controllo dell'intera LAN. I due PC della reception saranno serviti da un hub invece dello switch, data la leggera interazione con la rete. La lista dei componenti, quindi, è la seguente:

- Router con firewall incorporato
- 3 Switch Fast Ethernet
- 1 Hub
- 3 Server
- 1 Print Server
- 19 schede di rete di tipo 10/100 (si suppone che i File Server siano normali PC che necessitano di scheda di rete, mentre il Print Server sia un dispositivo dedicato, già munito di scheda Fast Ethernet)
- cavo UTP categoria 5
- sistema operativo di rete, che nel nostro caso sarà Windows Server 2003

5.3 Il sistema operativo

Windows Server 2003 è prodotto in quattro versioni, pensate per esigenze diverse. Quella da noi utilizzata è la versione Standard Edition, in grado di fornire tutte le caratteristiche di base per la realizzazione di server e per il controllo completo della LAN. Le altre versioni sono la Enterprise Edition e Datacenter Edition, entrambe a 32 o 64 bit, e la Web Edition. Le principali innovazioni di questo sistema operativo riguardano principalmente le Active Directory, e le funzionalità IntelliMirror attraverso cui l'amministratore dispone di funzionalità avanzate per il controllo degli utenti e dei gruppi di lavoro, per l'installazione del software e il backup dei dati. Molto curato è il discorso della sicurezza, con particolare attenzione rivolta all'ambito delle reti. Queste sono assimilate a strutture che coesistono con altri livelli e tipi di rete, come le wireless, Internet, le WAN. Proprio a proposito di reti wireless, Windows Server 2003 dispone di caratteristiche, assenti nel precedente Windows 2000 Server, per l'implementazione e la migliore gestione delle reti wireless.

5.4 Le impostazioni per l'accesso a Internet

Secondo le impostazioni di default, Windows Server 2003 prevede una configurazione molto sicura per il web, che però penalizza la navigazione in Internet. Questo, però, non è un difetto visto che questo sistema operativo è dedicato prevalente all'utilizzo su server e nelle reti. Le impostazioni, naturalmente possono essere modificate dall'amministratore. Vediamo come fare!

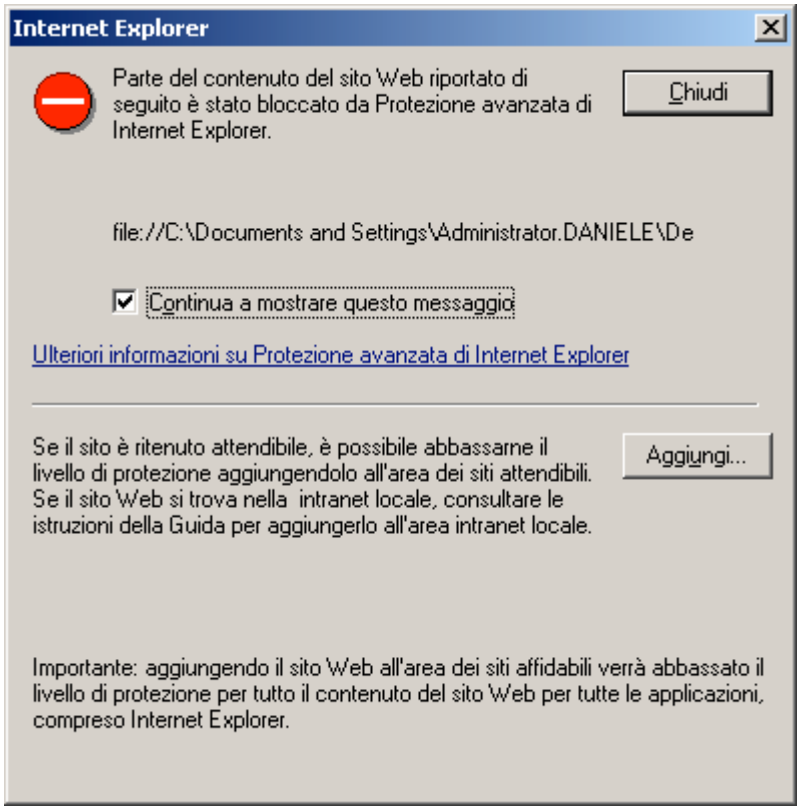

FOTO 5.4.1: Ogni sito sconosciuto deve essere inserito in una lista di siti "attendibili" per poter essere visitato

Quando si accede ad un sito mai visitato, il sistema blocca l'accesso e mostra una maschera in cui chiede se si desidera includerlo in una lista di siti noti. Cliccando sul pulsante *Aggiungi* della maschera in figura 5.4.1 è possibile inserire il sito nella lista e visitarlo. Questa impostazione può essere modificata dal browser Internet Explorer: andando nel menù Strumenti – opzioni Internet, e poi nella cartella *Protezione*.

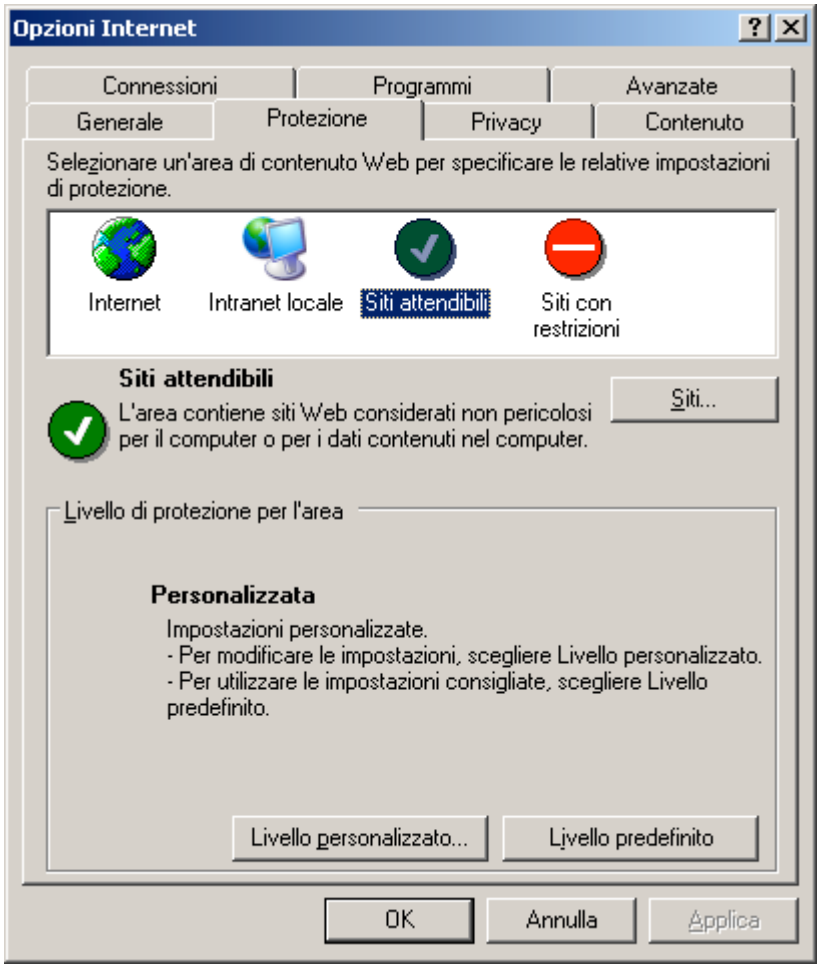

FOTO 5.4.2: Dalla cartella protezione è possibile modificare le impostazioni di sicurezza per i diversi livelli di rete

I siti inseriti nella lista "attendibili" possono essere rimossi o modificati selezionando nell'apposita finestra di figura 5.4.2 l'icona Siti attendibili e poi cliccando sul pulsante *Siti*. Dalla cartella *Privacy*, inoltre, è possibile modificare le impostazioni sulle informazioni utente durante la navigazione, quindi sulla gestione dei cookie: il livello di default è quello medio, che permette la navigazione sicura e senza troppe interruzioni.

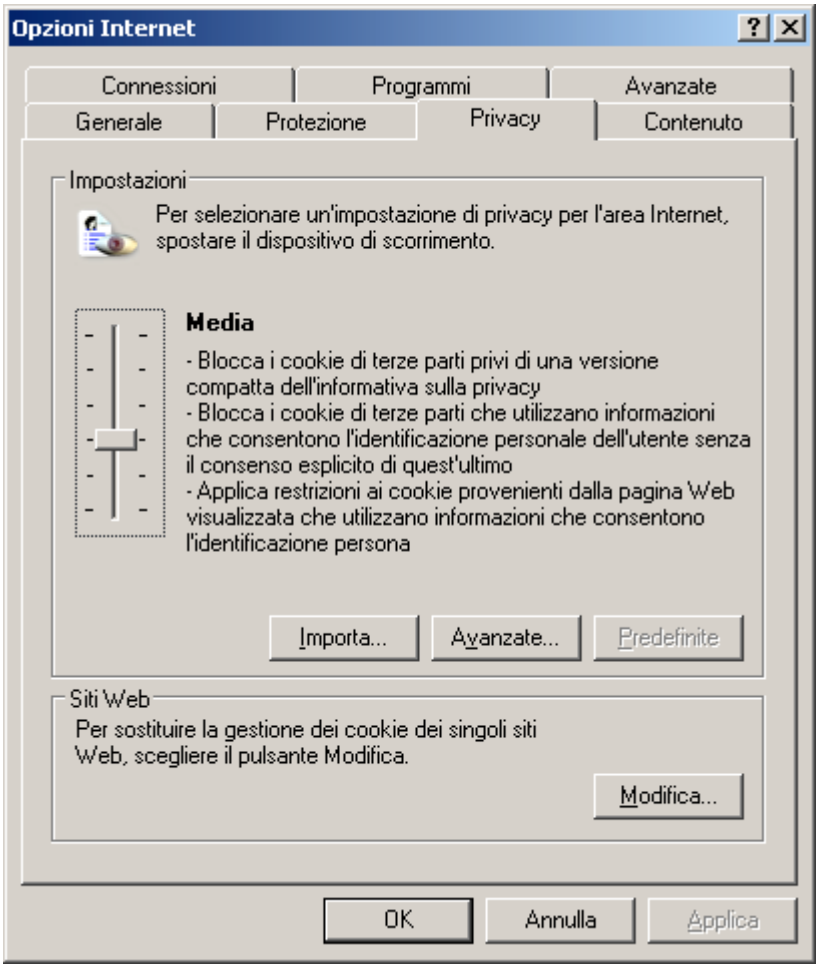

FOTO 5.4.3: I cookie vengono bloccati dal sistema se provengono da siti incerti, per evitare che essi possano richiede informazioni private

Approfondimento:

I cookie, in inglese biscottini, sono dei file che memorizzano informazioni sull'utente per facilitare la navigazione. Purtroppo però contengono informazioni spesso di carattere privato quali username e password, quindi devono essere bloccati se di provenienza incerta

E' conveniente tuttavia, se si utilizza Windows Server 2003 per gli host di una rete locale, non modificare tale impostazioni per avere il massimo della sicurezza.

5.5 Configurazione dei server

In questo paragrafo vedremo come configurare i server presenti nella nostra LAN, che come ricorderemo sono:

- server centrale, posto nella sala degli apparati di rete
- 2 file-server, posti nelle sale 1 e 3.

Il print-server è, invece, un dispositivo dedicato, per cui non richiede la configurazione del sistema operativo. In alternativa è possibile affidare tale ruolo ad un altro PC configurato in Windows Server 2003 come print-server.
Ad ogni avvio del sistema operativo appare la finestra per l'amministrazione del server. Questa importante funzionalità di Windows 2003 permette di configurare diversi tipi di server in modo automatico e veloce, utilizzando un wizard apposito.

Tips: se non si desidera visualizzare il wizard all'avvio basta spuntare la casella in basso: "Non visualizzare questa pagina all'accesso"

FOTO 5.5.1: La configurazione dei vari server avviene in modo semplice grazie al wizard di configurazione automatica

Il pulsante *Aggiungi o rimuovi un ruolo* presenta una finestra in cui sono elencate le operazioni che saranno effettuate durante la configurazione. In questa finestra è necessario solo premere il pulsante *Avanti* perche Windows avvi il rilevamento della LAN per la configurazione guidata.

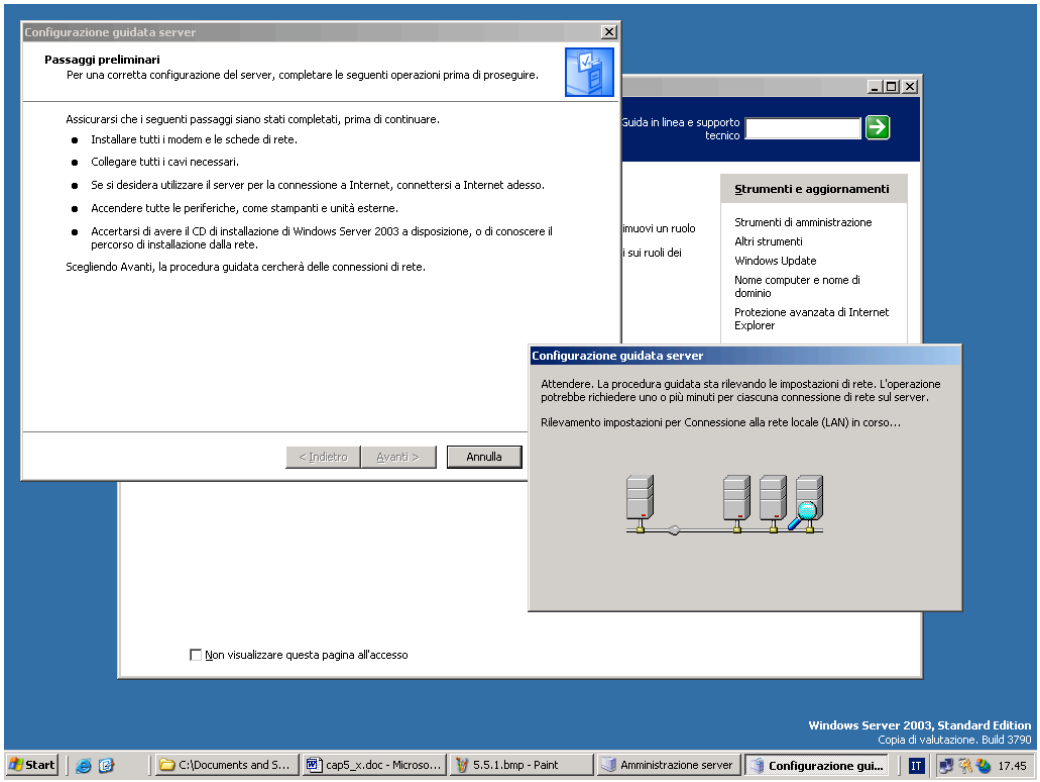

FOTO 5.5.2:

Dopo aver letto la lista delle operazioni di configurazione basta cliccare su *Avanti* per iniziare la configurazione del server

5.5.1 Configurazione del server primario

Terminata la scansione della LAN, ci viene posta di fronte la maschera in cui si sceglie quale tipo di server si deve configurare. La configurazione tipica per un primo server è adatta alla configurazione del server che abbiamo sistemato nella sala dei dispositivi, che si occupa della gestione dei domini e della risoluzione degli indirizzi IP nei nomi degli host. Cliccando sul pulsante *Avanti* apparirà una finestra in cui si richiede di inserire il nome del dominio Active Directory. Facciamo attenzione a lasciare invariata l'estensione ".local", per fare in modo che il dominio interno resti separato dal dominio Internet, come spiegato nella stessa maschera.

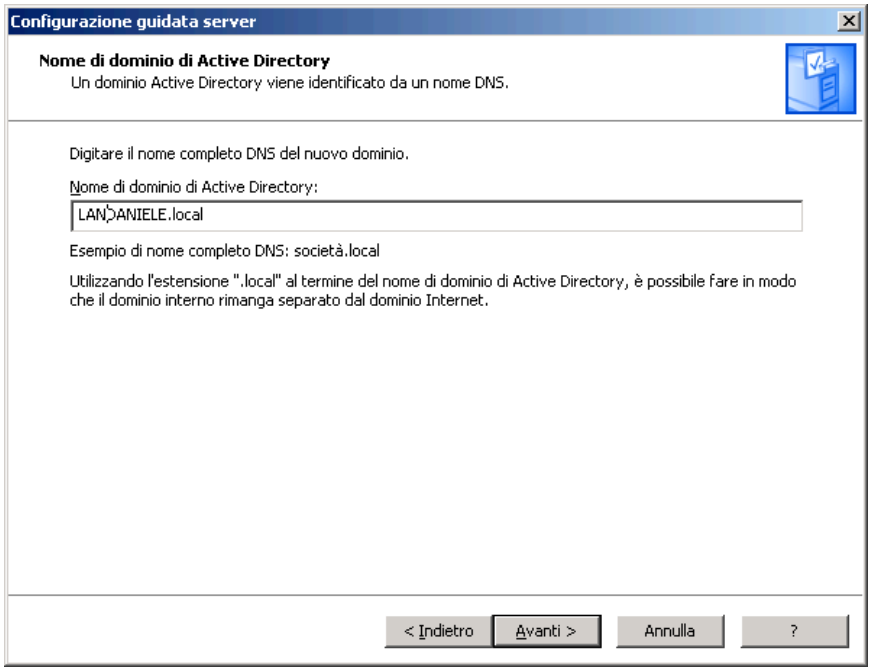

FOTO 5.5.1.1: Avviando la configurazione del server primario verrà chiesto di inserire il nome del dominio Active Directory

Andiamo sul pulsante *Avanti* per proseguire.

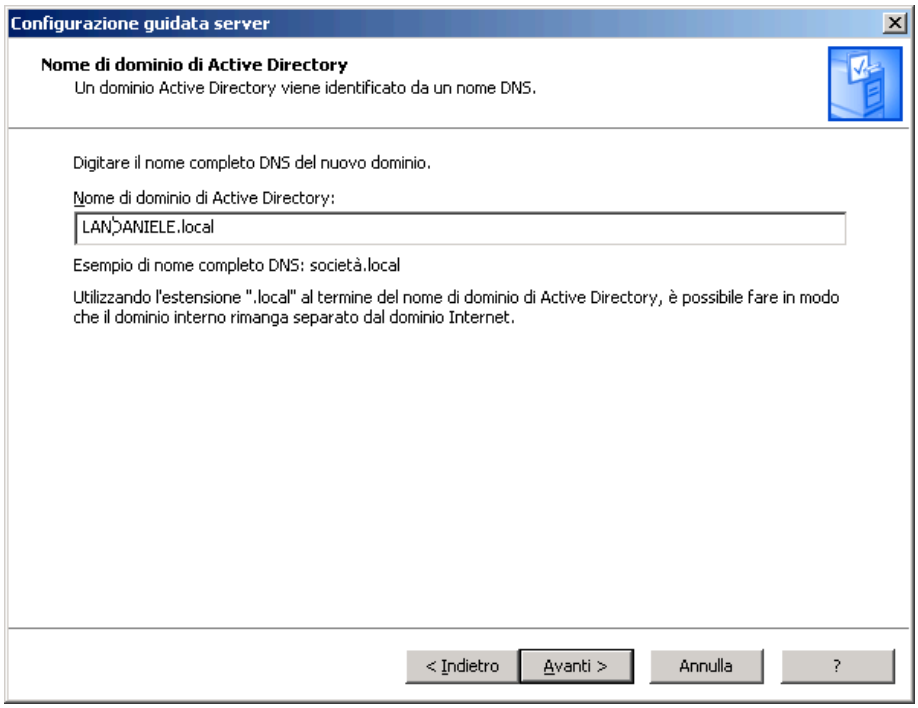

FOTO 5.5.1.2: Alla richiesta di modificare il nome predefinito per il dominio NetBIOS si può lasciare tutto invariato e proseguire

Il questa finestra ci viene chiesto se desideriamo modificare il nome predefinito del dominio NetBIOS, ma noi possiamo lasciarlo invariato e cliccare su *Avanti*. Nella maschera successiva si chiede di specificare l'indirizzo di un eventuale server a cui inviare le interrogazioni di DNS sconosciuti. Possiamo scegliere di non indicare tale server opzionale ed andare avanti.

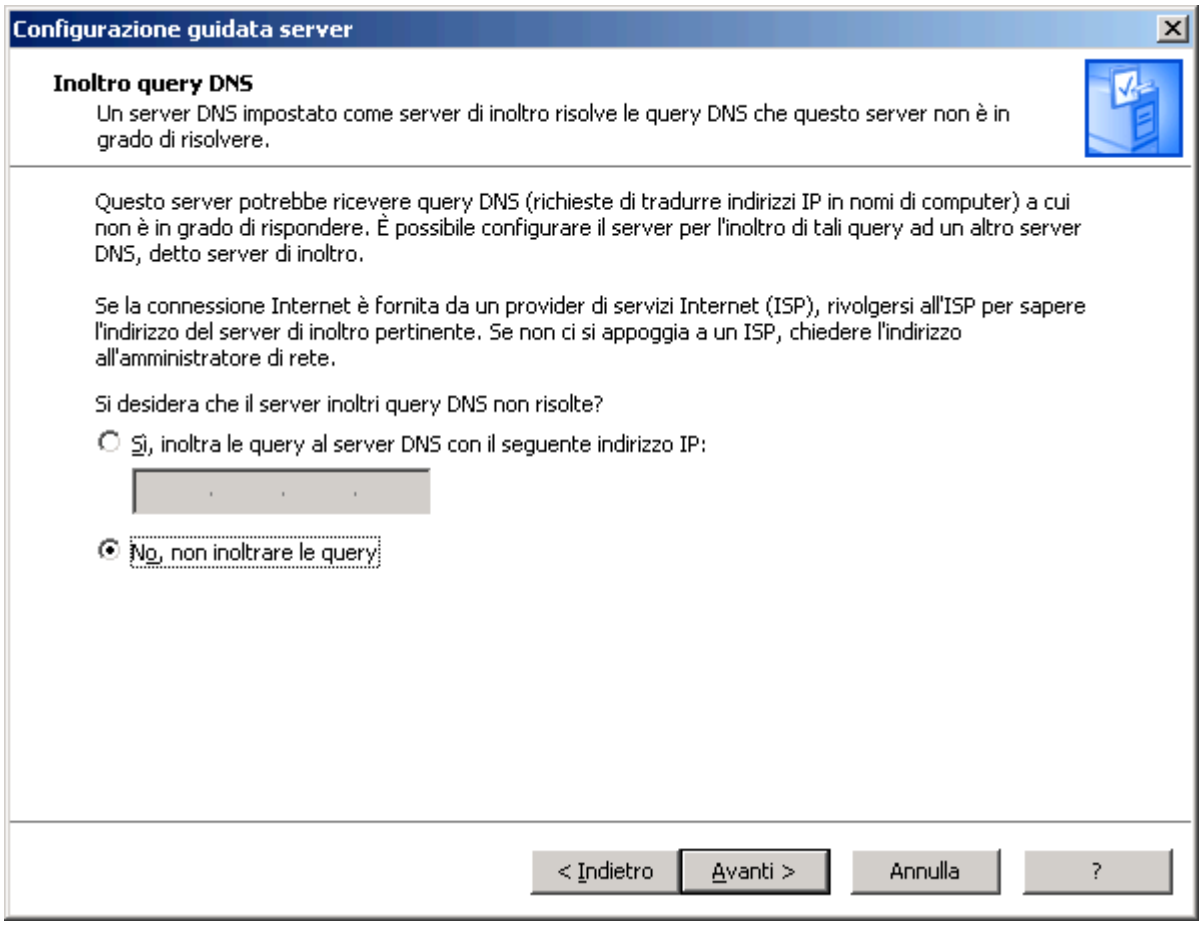

FOTO 5.5.1.3: E' possibile indicare l'indirizzo di un server a cui inviare le query DNS non risolte

La maschera successiva mostra un semplice riepilogo delle modifiche apportate al server.

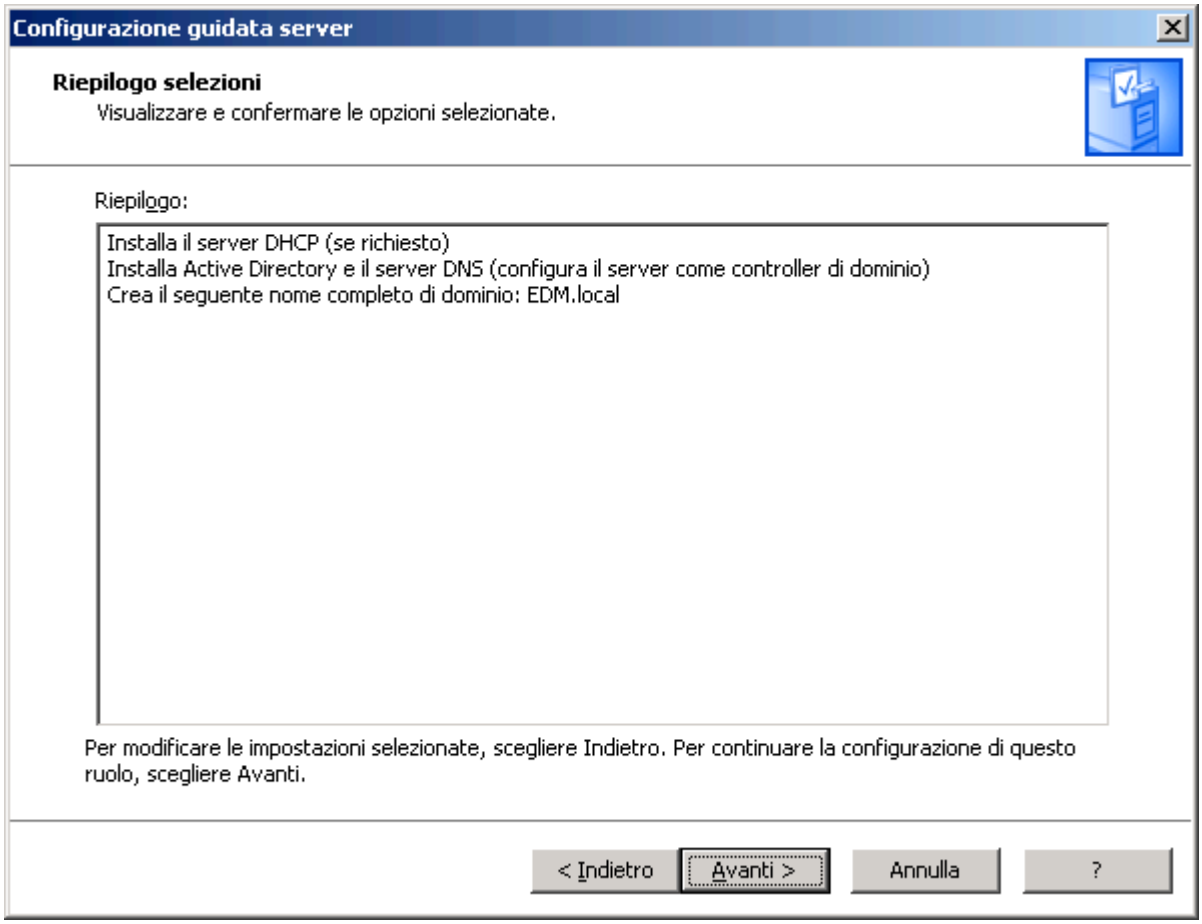

FOTO 5.5.1.4:
La maschera di riepilogo delle operazioni effettuate

Cliccare su *Avanti* per terminare e poi su OK per riavviare il PC e salvare le impostazioni.

Tips: Per la configurazione del server primario ricordate di tenere a portata di mano il CD di installazione che sarà chiesto alla fine della procedura per installare i nuovi componenti prima del riavvio

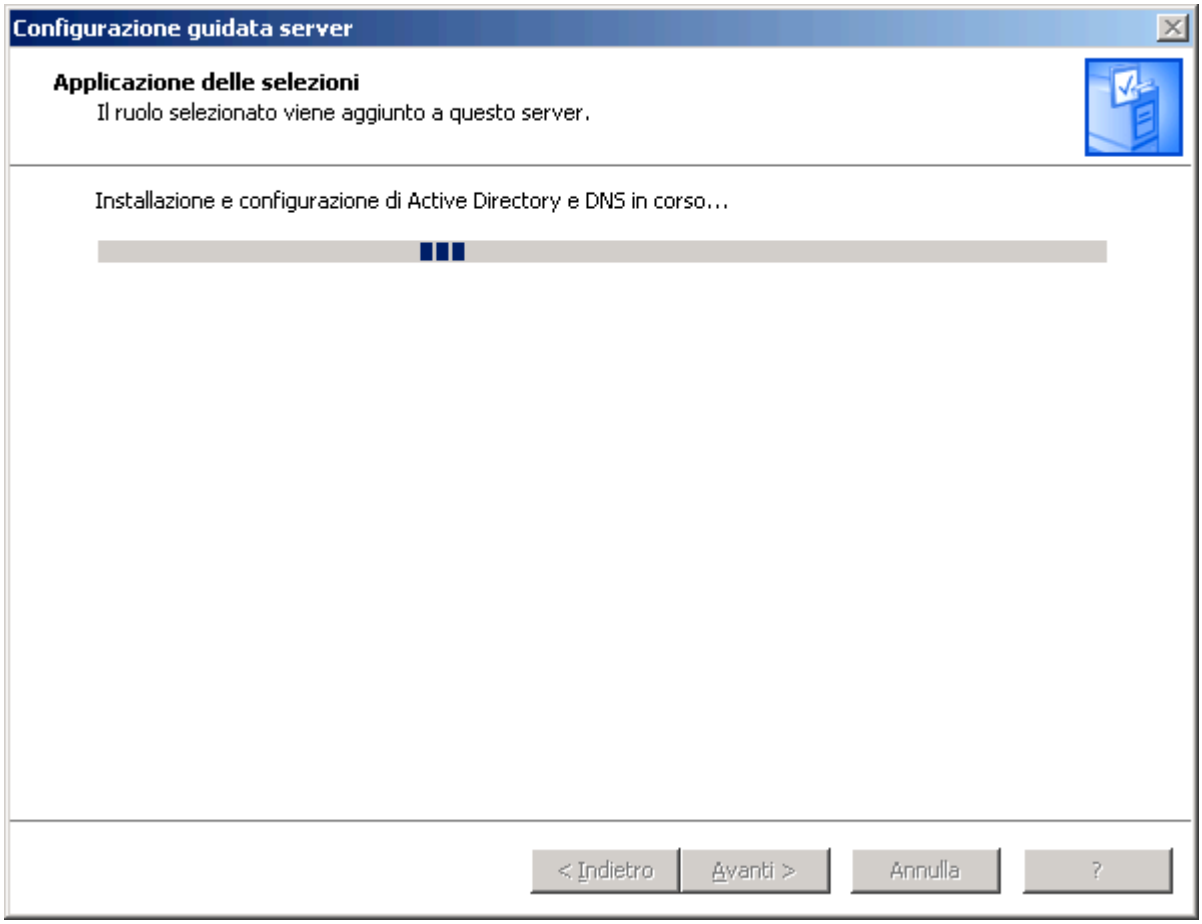

FOTO 5.5.1.5: L'installazione dei nuovi componenti per il server primario, prima del riavvio

La procedura di installazione e configurazione di Active Directory e DNS è abbastanza lunga e pesante per cui non preoccupatevi se il vostro PC non risponde.

Al riavvio di Windows appare una maschera che ci mostra tutte le modifiche apportate al nostro server. Si noti che la prima operazione, quella per l'assegnamento dell'indirizzo IP statico, appare in rosso perché non è stata effettuata, visto che l'IP era già stato assegnato in precedenza.

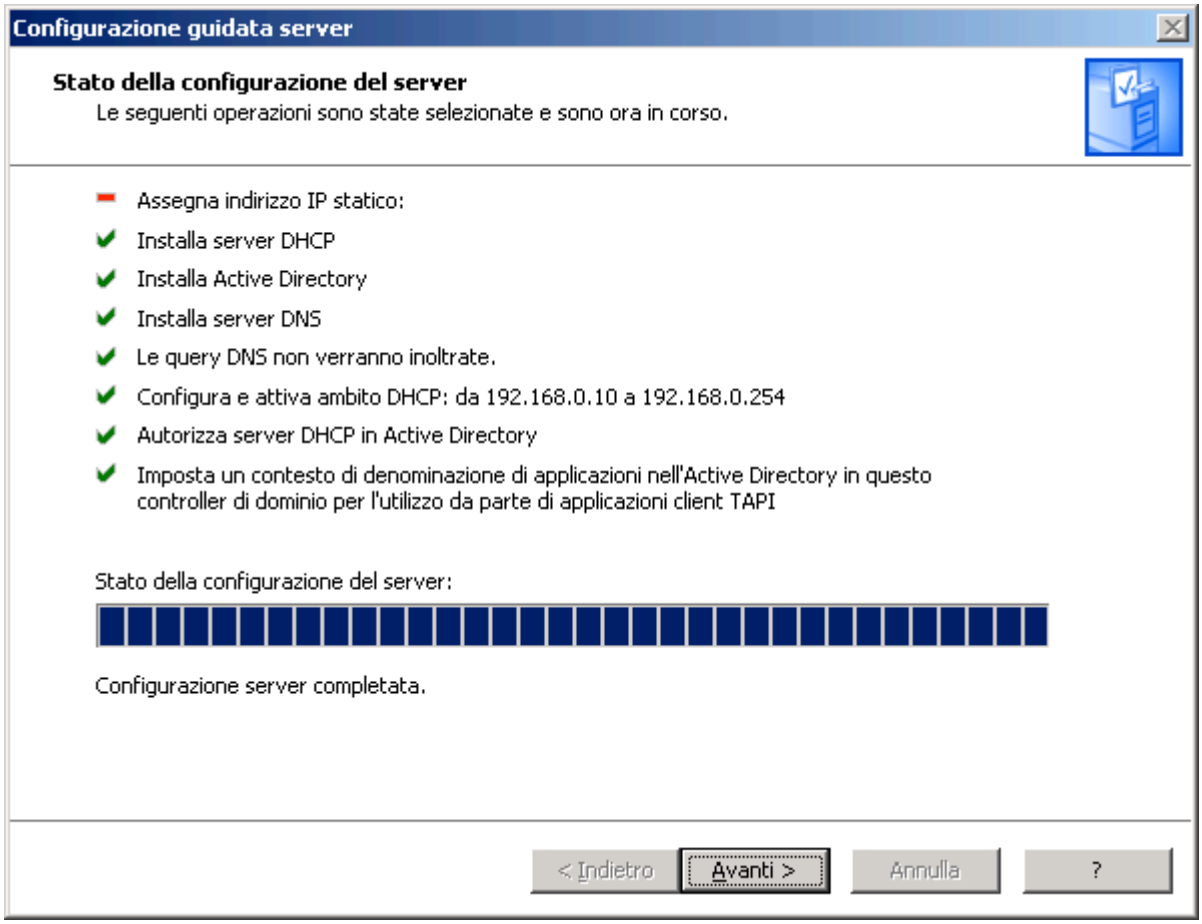

FOTO 5.5.1.6:
La maschera che mostra il completamento delle operazioni sul server primario

Tips: Ai server abbiamo assegnato IP superiori a quelli dei client: nel nostro caso, per esempio, avremo gli IP da 192.168.0.2 fino a 192.168.0.16 per i client, mentre dall'IP 192.168.0.17 saranno gli indirizzi dei server. Se si prevede che la rete possa avere una grande espansione nel numero di host conviene lasciare alcuni IP liberi tra client e server oppure numerare con gli IP più bassi (magari fino a 10) i server e con gli IP più alti i client, per offrire a questi ultimi maggiori possibilità di aumento

A questo punto, se andiamo nella finestra di configurazione del protocollo TCP/IP, quindi *Start /Pannello di controllo/Connessioni di rete/Connessione alla rete locale (LAN)*, poi clic su *Proprietà*, ed ancora selezioniamo *Protocollo Internet (TCP/IP)* e di nuovo clic su *Proprietà*, vedremo che anche l'IP del server DNS è abilitato, come appunto ci aspettavamo.

Tips nel testo: Ricordiamo che per accedere velocemente alla finestra di configurazione è possibile cliccare sull'icona della rete vicino all'orologio e poi su *Proprietà*

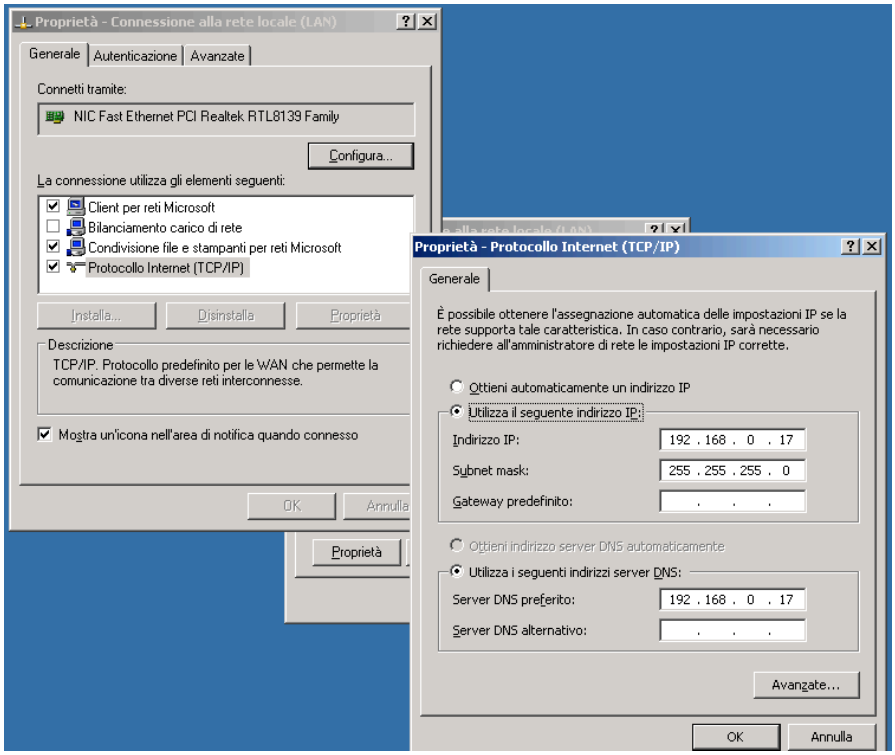

FOTO: 5.5.1.7: L'indirizzo al server DNS è stato assegnato automaticamente dopo la configurazione

Se nella finestra dell'immagine sopra clicchiamo su *Avanzate* possiamo vedere una maschera con diverse cartelle che sintetizzano e ci permettono di modificare gli IP, i DNS ed altro.

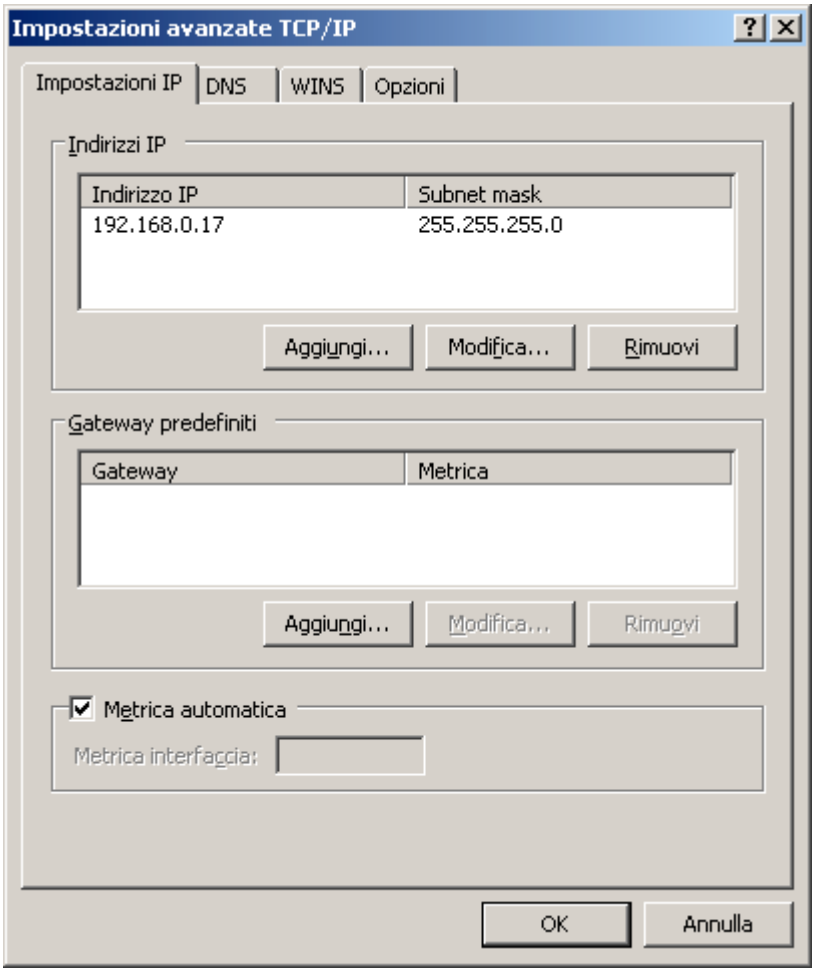

FOTO 5.5.1.8: In avanzate è possibile modificare tutti i parametri impostati per la LAN

Per il momento trascuriamo tutte le altre possibilità offerte dalla finestra di connessione alla rete locale per vederle più avanti.

5.5.2 Configurazione dei file server

I passi iniziali sono uguali a quanto visto nel precedente paragrafo. Alla maschera di scelta del tipo di server bisogna scegliere stavolta la seconda opzione: configurazione personalizzata.

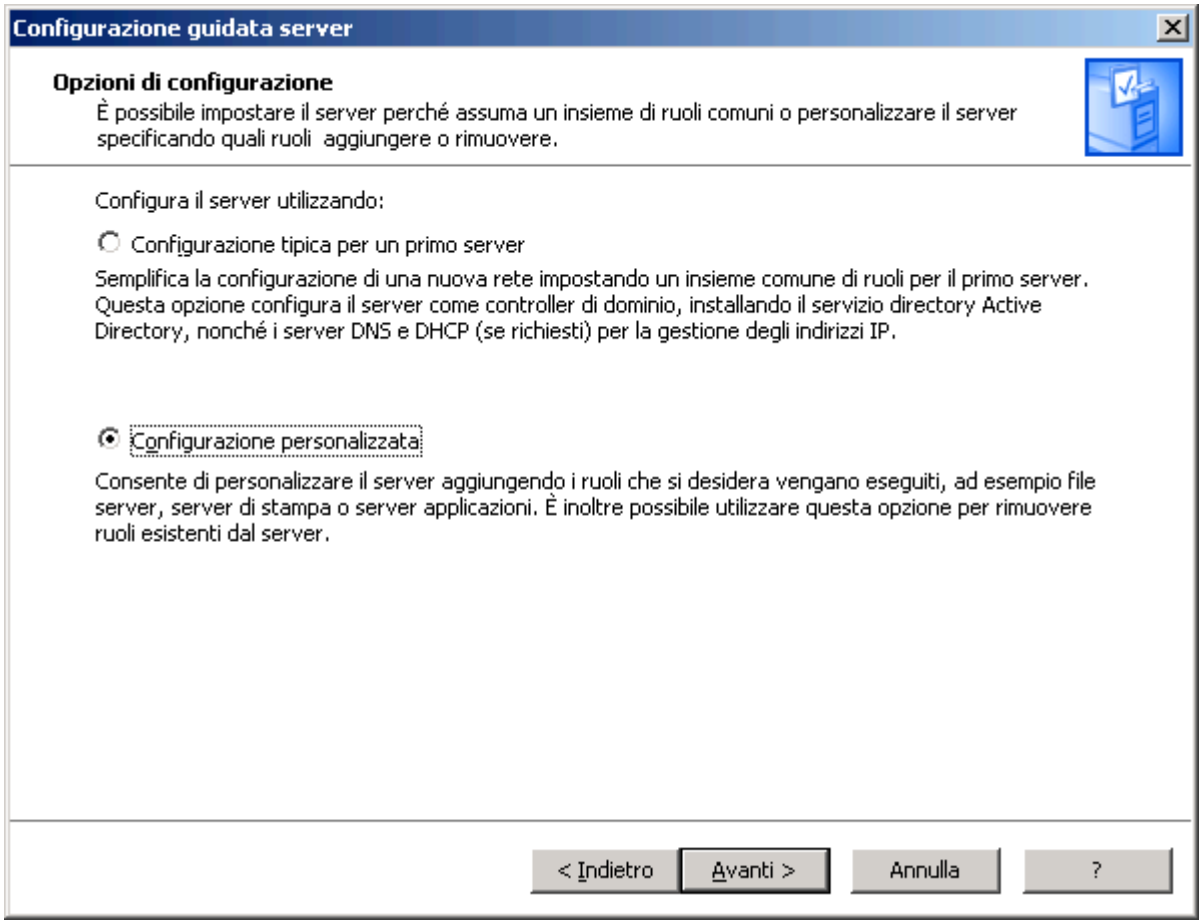

FOTO 5.5.2.1: Stavolta selezioniamo la seconda opzione per configurare i file server

La prossima maschera mostra una lista di ruoli che il server può assumere e che dovranno essere configurati. Tra tutti i ruoli a noi interessa solo quello di file server, dato che questo è il compito cui il server è destinato, quindi selezioniamo il ruolo e premiamo il pulsante *Avanti* per iniziare la configurazione.

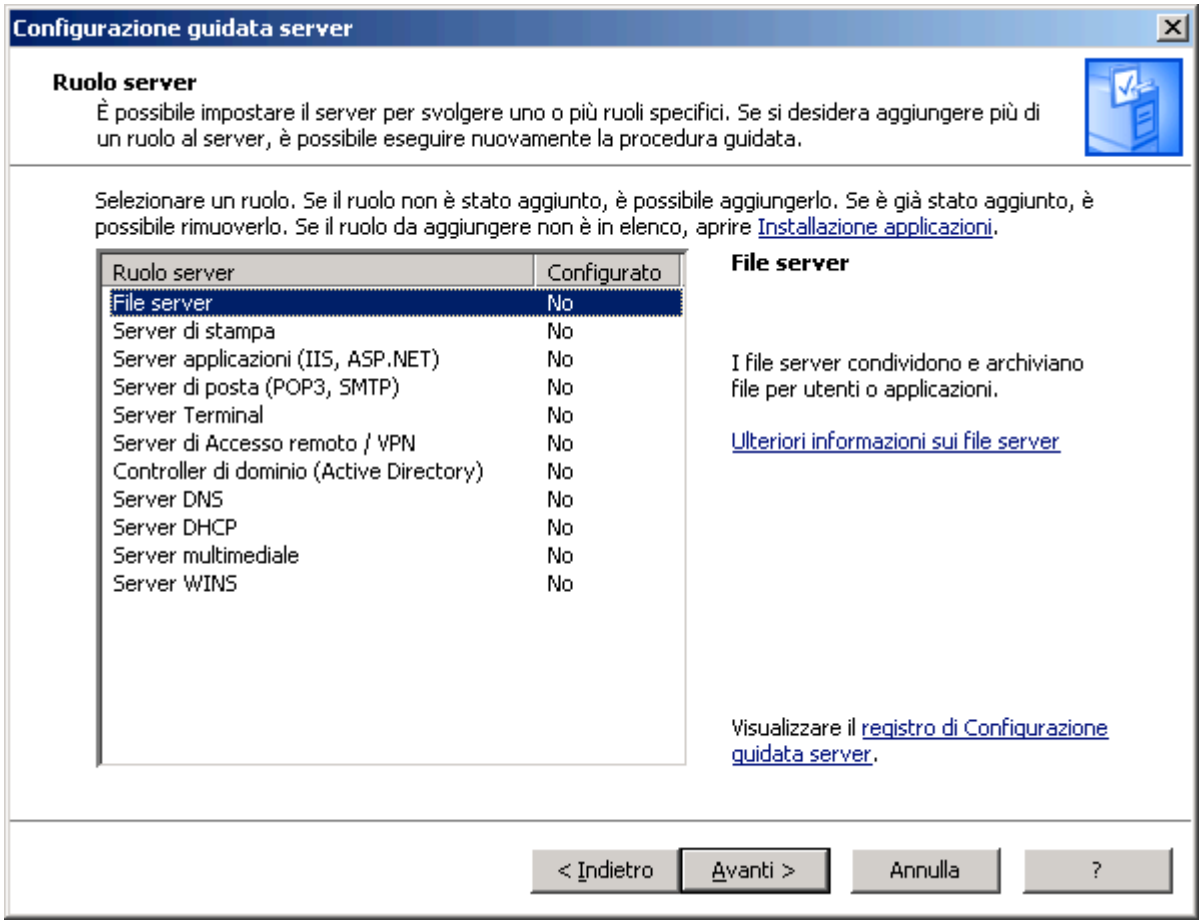

FOTO 5.5.2.2: Tra i vari ruoli che si possono attribuire al server noi scegliamo il primo

La finestra di impostazione delle quote di hard disk, in cui si specifica quanto spazio dell'hard disk riservare ai vari utenti, sarà lasciata sui valori di default.

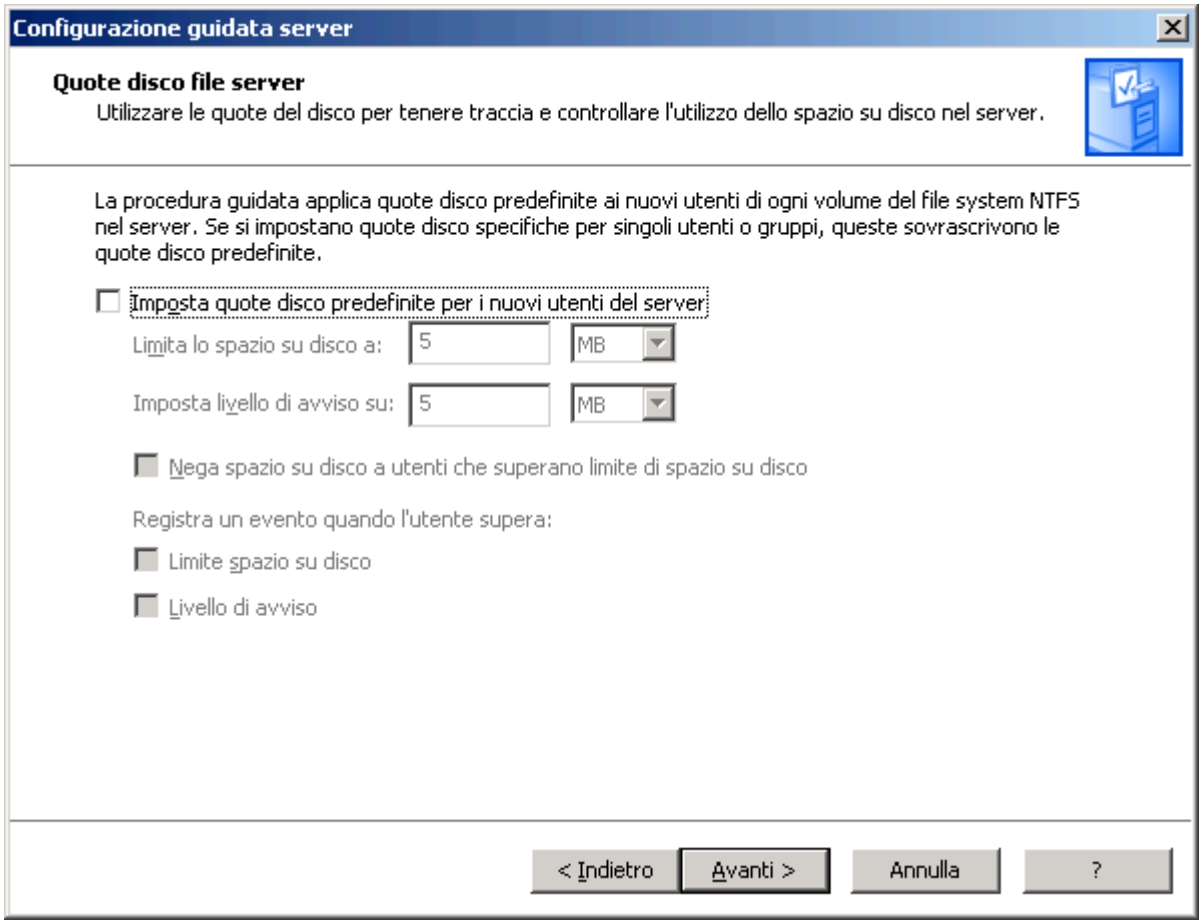

FOTO 5.5.2.3: La finestra di impostazione delle quote di hard disk ai vari utenti

Possiamo quindi proseguire senza altre modifiche fino alla maschera di riepilogo e poi a quella finale.
Terminata la configurazione ci verrà chiesto di indicare una cartella condivisa alla quale gli utenti potranno accedere per l'utilizzo del file server

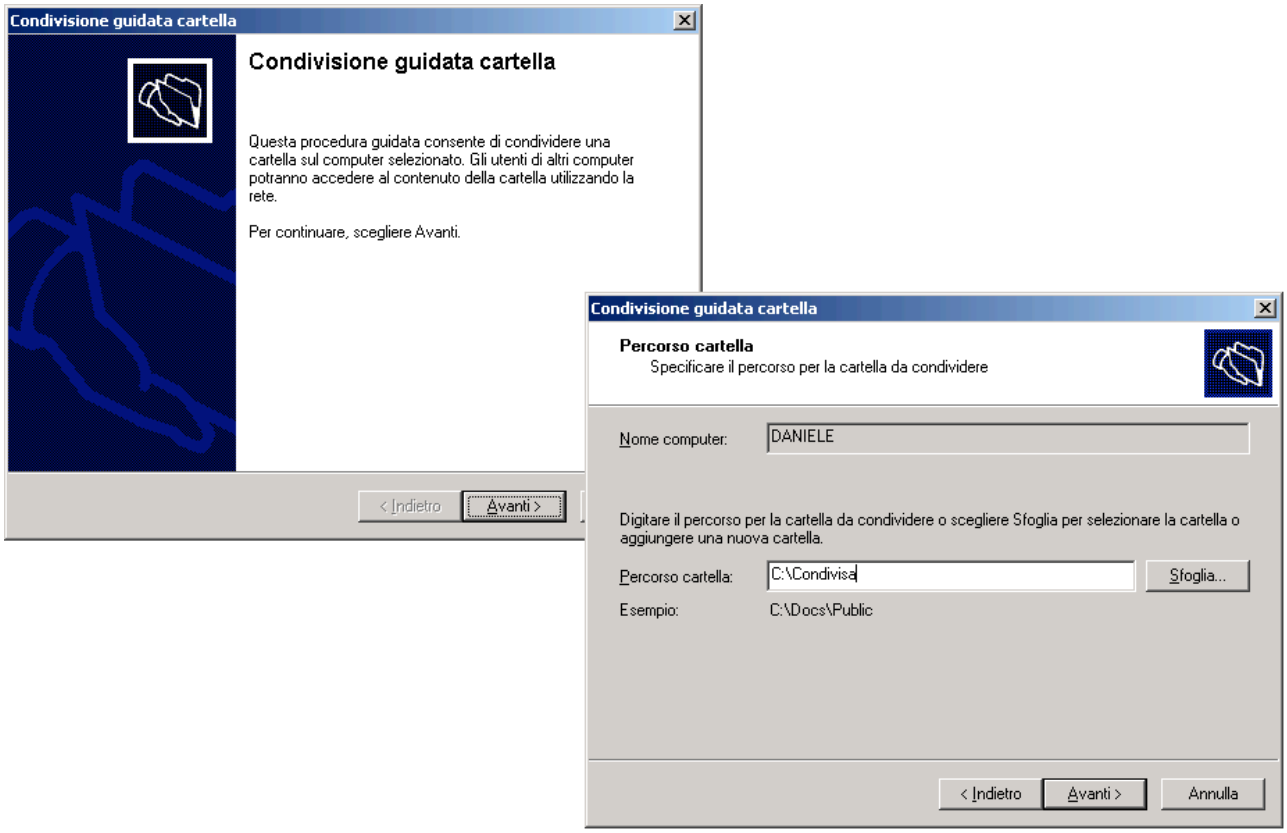

FOTO 5.5.2.4: E' necessario indicare la cartella da condividere agli utenti

Lasciare tutto invariato nella finestra di riepilogo delle proprietà della cartella condivisa e andare avanti

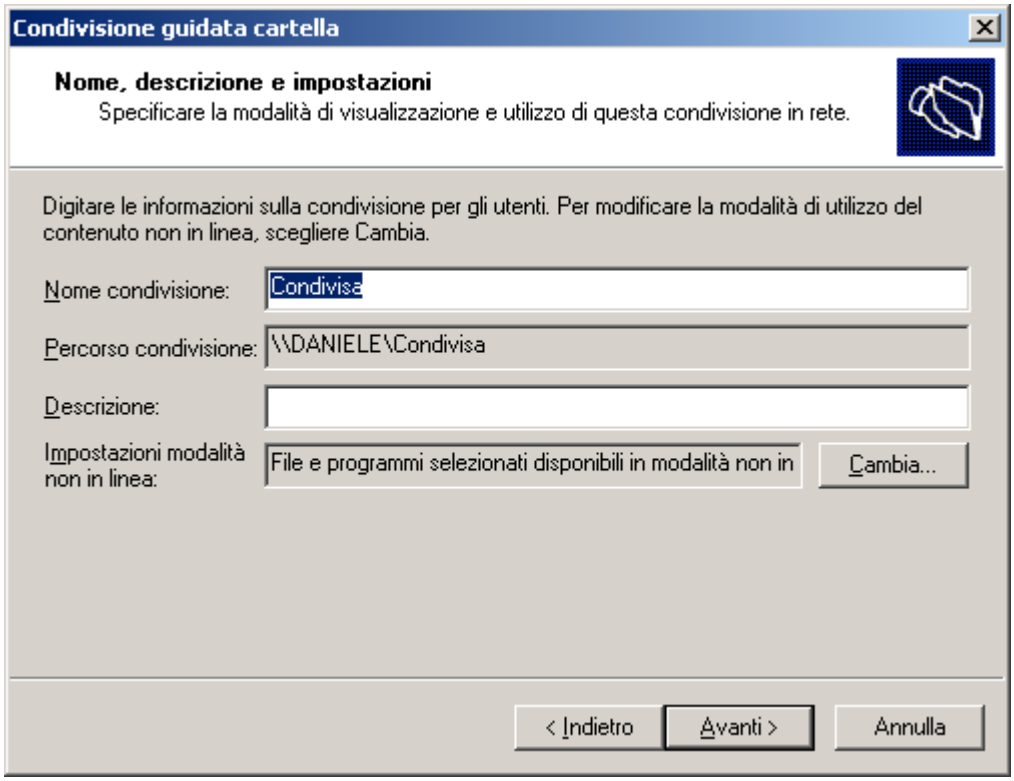

FOTO 5.5.2.5: Il riepilogo delle proprietà della cartella condivisa

Nella maschera successiva è possibile impostare le autorizzazioni: l'accesso in lettura a tutti gli utenti è la scelta più sicura. E' possibile tuttavia utilizzare autorizzazioni personalizzate per i diversi utenti.

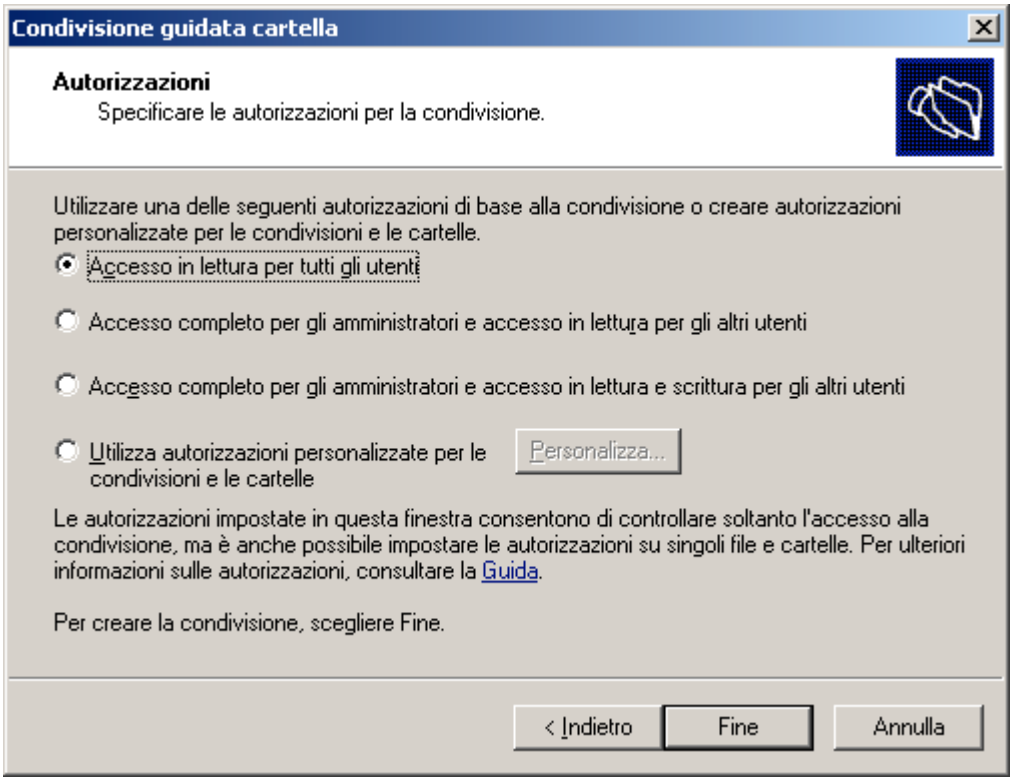

FOTO 5.5.2.6: Impostiamo le autorizzazioni per gli utenti. La scelta di fornire accesso in sola lettura è quella più sicura

Clicchiamo sul pulsante *Fine* per terminare la configurazione del file server.
Dopo aver completato la configurazione di qualsiasi server, la maschera iniziale del wizard apparirà diversa ed è possibile riconfigurare quanto appena fatto, utilizzando i pulsanti nella sezione inferiore della maschera

FOTO 5.5.2.7: Dopo aver impostato il ruolo del server è possibile modificarlo dalla maschera iniziale

Tips: La maschera iniziale può essere visualizzata in qualsiasi momento andando nel menù Start e poi su *Amministrazione server*

Nel caso in cui la LAN abbia dimensioni minori o si decida di utilizzare un solo server, questo può essere utilizzato sia come server primario che come file server. In questo caso la finestra dei ruoli indica i diversi ruoli attivi

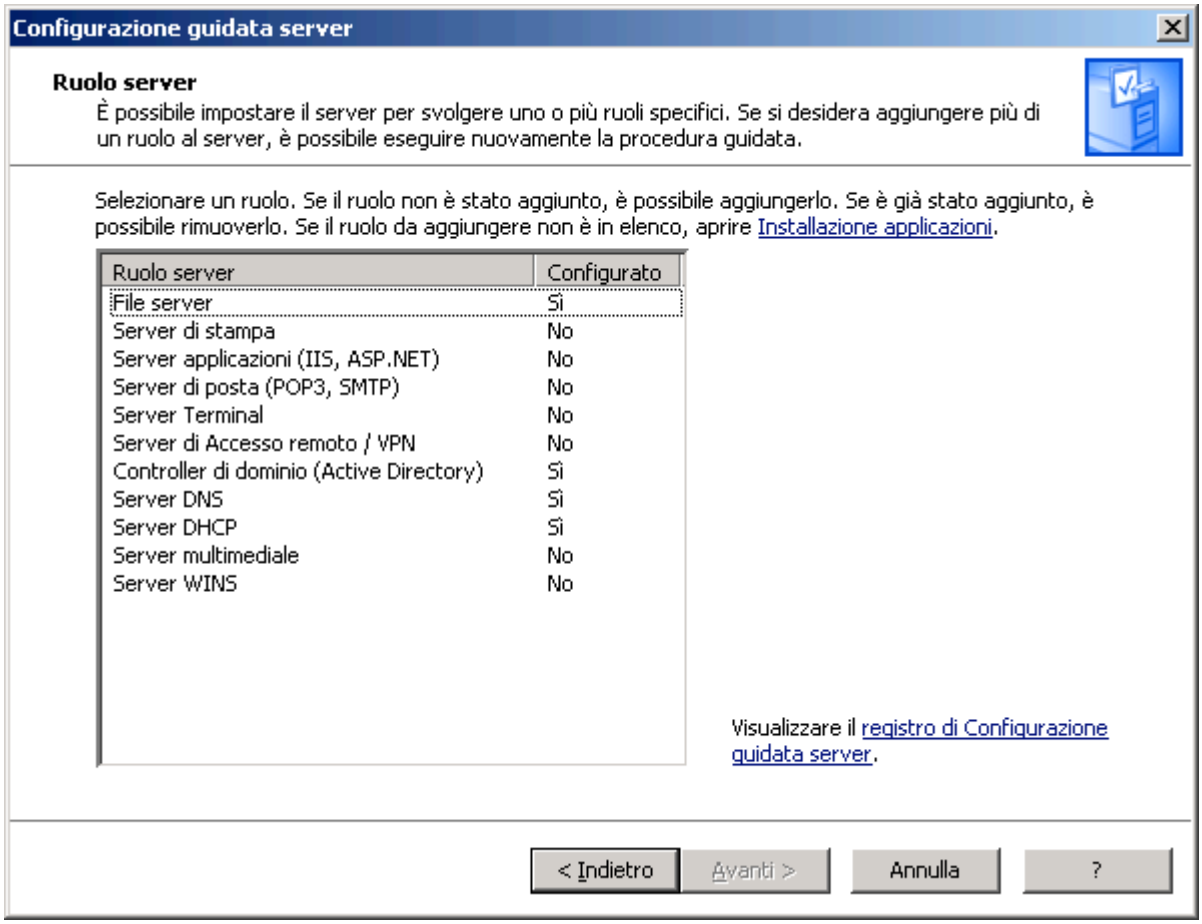

FOTO 5.5.2.8: I ruoli assegnati ad un server possono essere molteplici

Anche la maschera iniziale di gestione dei ruoli mostrerà in questo caso più possibilità di scelta

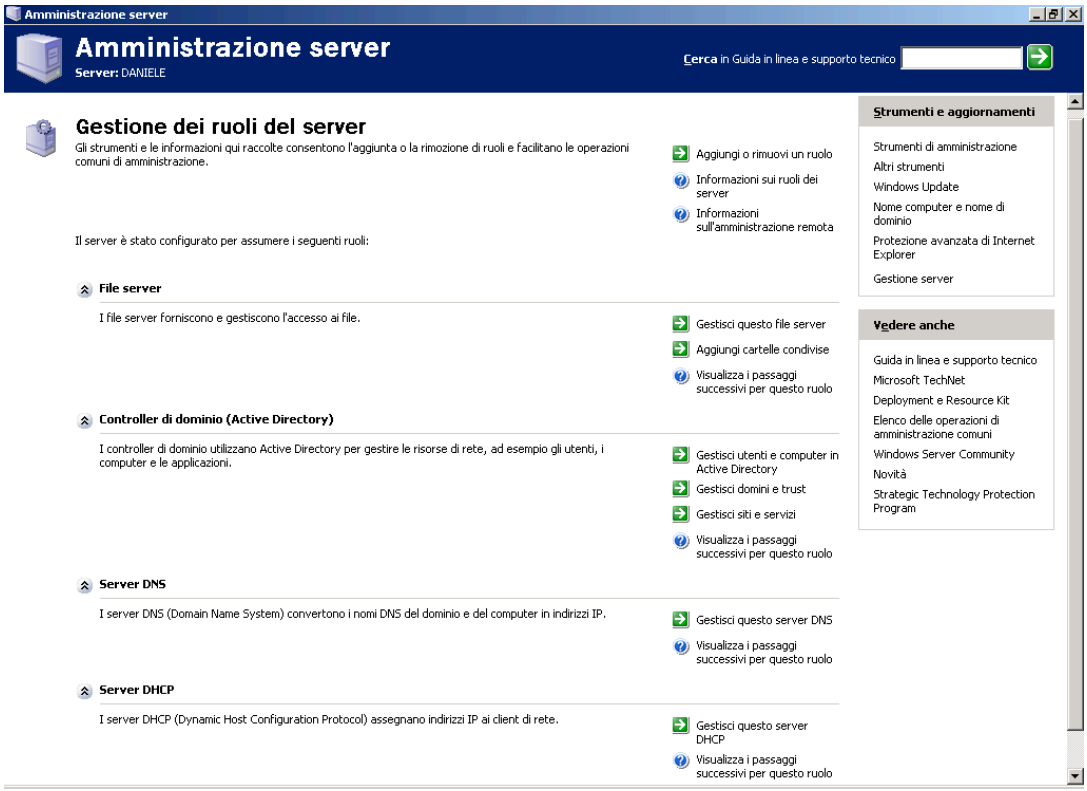

FOTO 5.5.2.9: La maschera di gestione mostra i diversi ruoli assegnati al server ed offre la possibilità di modificarli

Naturalmente la configurazione appena vista per i file server va effettuata su ciascuno dei PC che avranno questo compito nella nostra LAN, quindi sui server nelle sale 1 e 3.

5.6 Rimozione di un ruolo del server

Se si decide che un server abbia un ruolo inutile, è possibile rimuoverlo dalla finestra di gestione ruoli, mostrata nel precedente paragrafo. Tra i ruoli assegnati al server scegliere quello che riteniamo inutile e cliccare sul pulsante verde di gestione. Supponiamo di voler rimuovere dai ruoli quello del file server. Clicchiamo su *Aggiungi o rimuovi un ruolo* nella sezione *Gestione ruoli del server*. Apparirà la finestra di riepilogo già vista. Clicchiamo su *Avanti* per andare nella lista dei ruoli del server.

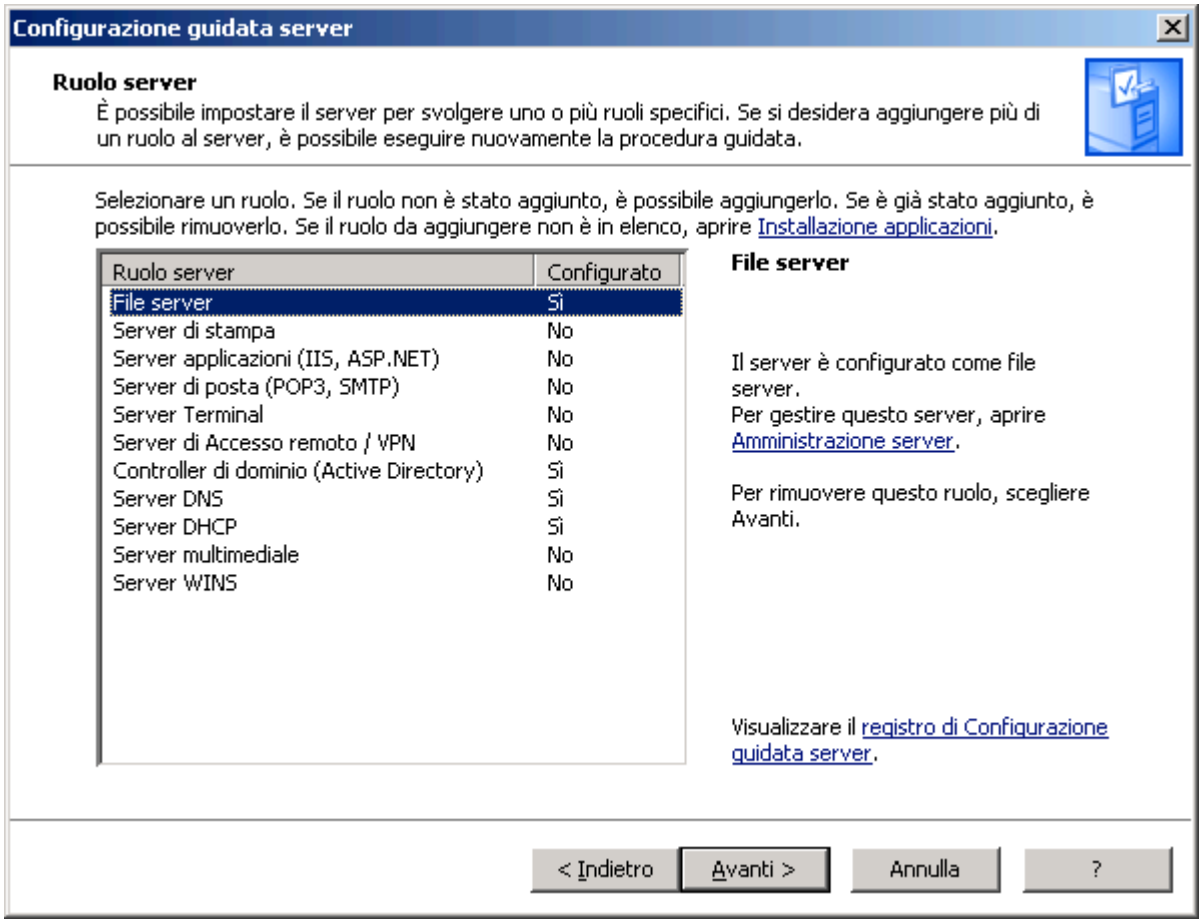

FOTO 5.6.1: La lista dei ruoli da cui possiamo rimuovere quelli già esistenti

Come possiamo vedere, il ruolo file server è configurato, infatti nella casella apposita appare la voce *Si.* Selezioniamo questo ruolo e clicchiamo sul pulsante *Avanti*. Appare una finestra che chiede conferma per la rimozione del ruolo scelto. Per fare ciò è necessario spuntare la casella in basso, *Rimuovi ruolo file server*. La finestra di riepilogo mostra tutte le operazioni che saranno effettuate, ed i cambiamenti dopo la rimozione del ruolo.

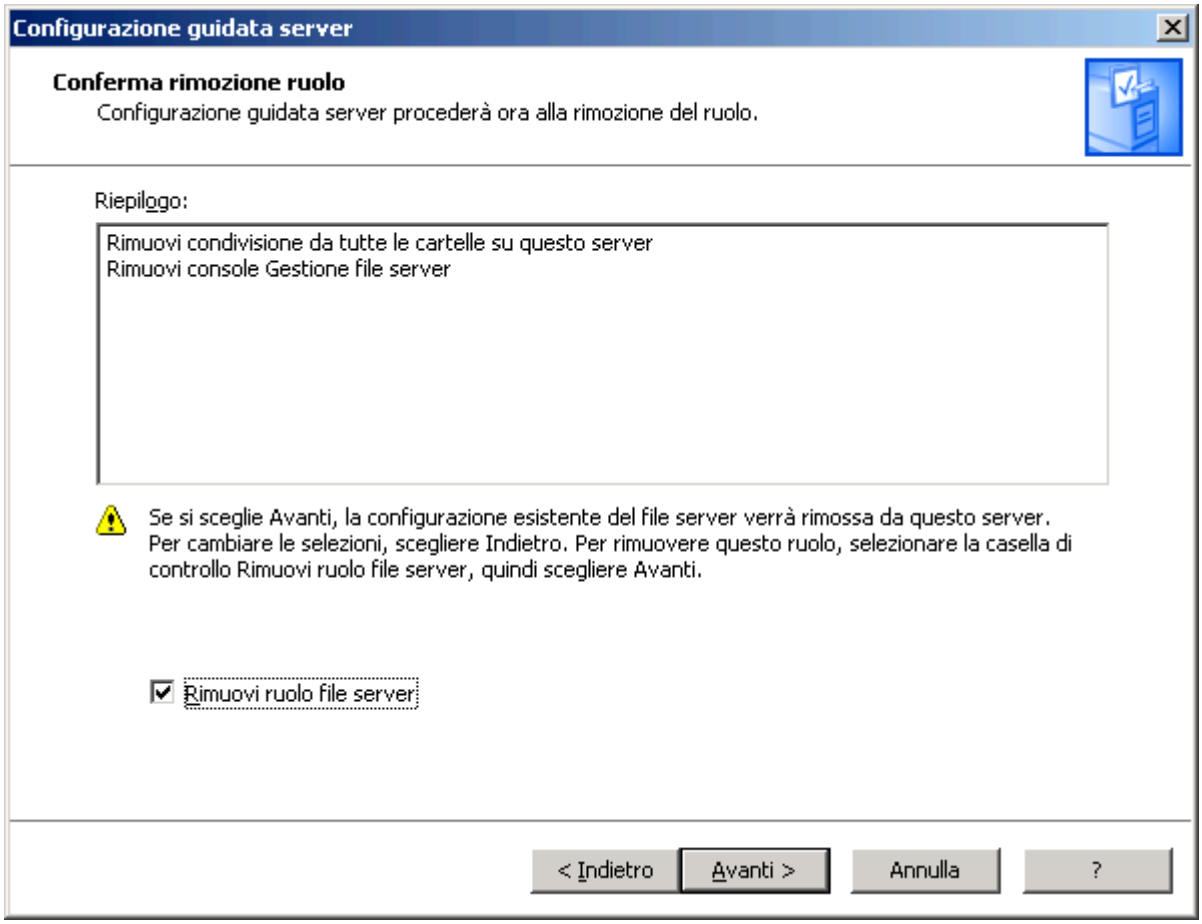

FOTO 5.6.2: Prima di rimuovere un ruolo è opportuno leggere la lista delle modifiche che avverranno

Dopo aver spuntato la suddetta casella si attiva il pulsante *Avanti* che ci permette di proseguire. La prossima finestra conferma la rimozione del ruolo file server. Cliccare su *Fine* per concludere il processo.

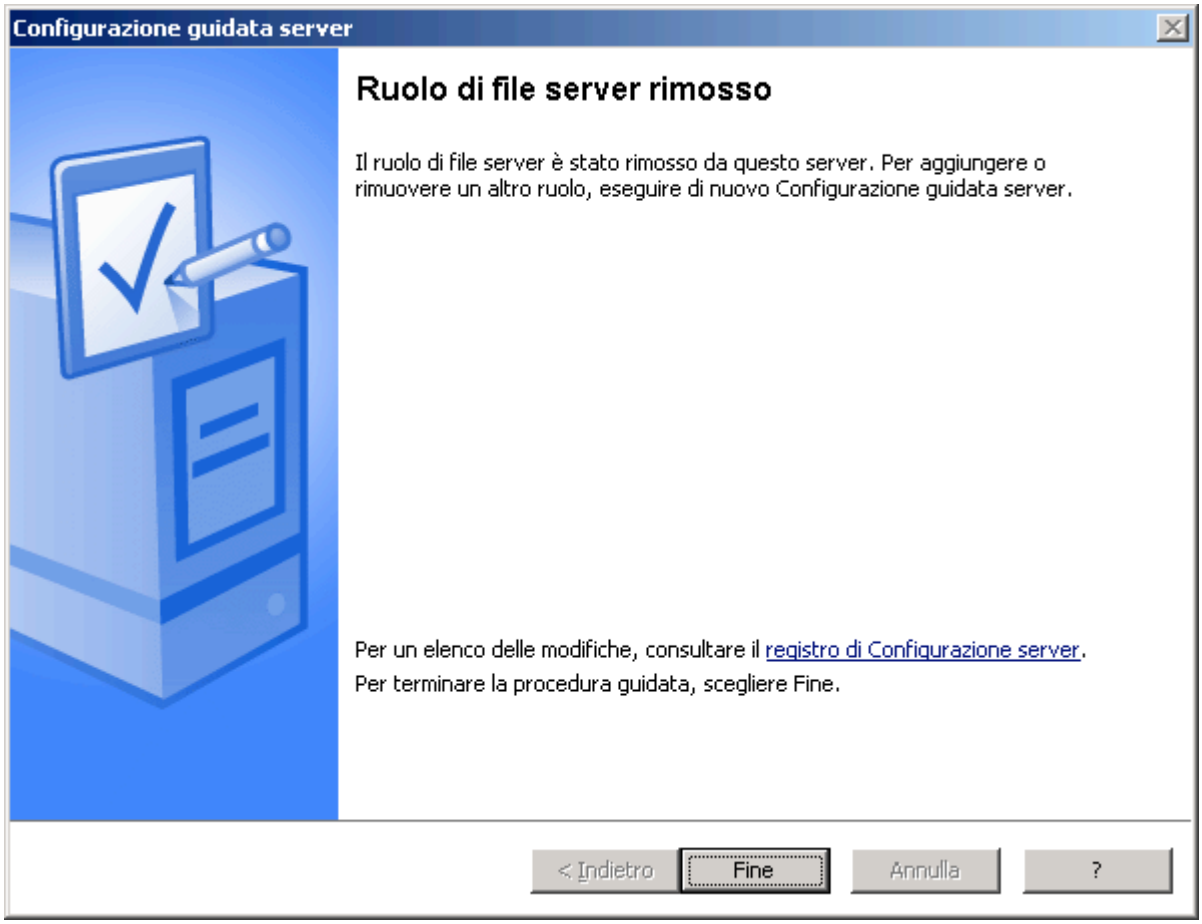

FOTO 5.6.3: La rimozione del ruolo è avvenuta con successo

Dopo la rimozione, un ruolo può essere nuovamente creato utilizzando sempre la finestra di gestione ruoli del server.
Se proviamo ad aprirla, vedremo che stavolta tra i ruoli non appare più quello di file server.

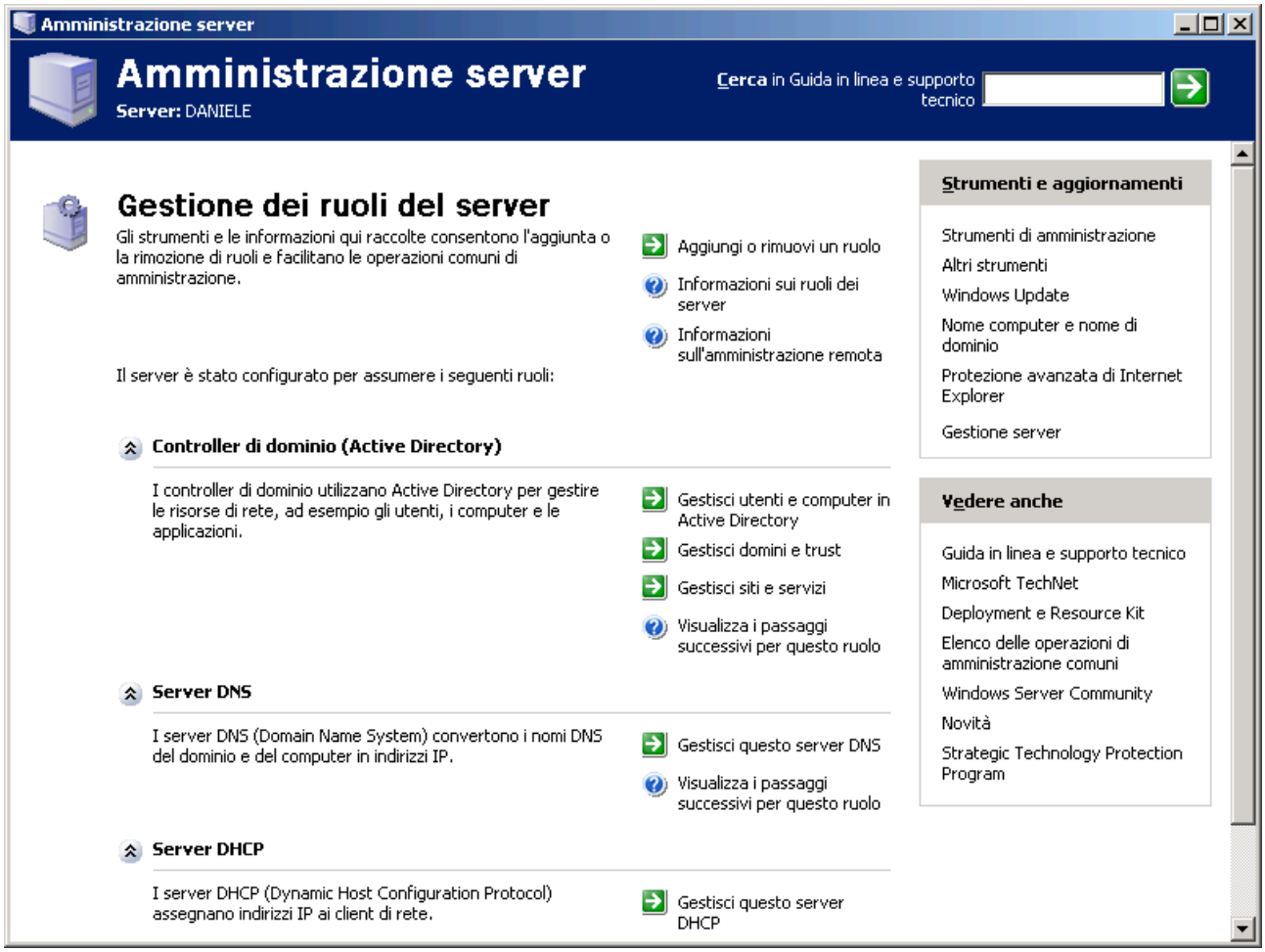

FOTO 5.6.4: Dopo la rimozione di un ruolo, questo effettivamente non compare più nella finestra dei ruoli del server

5.7 Configurazione dei client

Dopo aver configurato il server primario e i due file server, non ci resta altro che passare ai client. La procedura che vedremo tra poco deve essere effettuata su tutti i PC della rete allo stesso modo, con l'unica differenza riguardante l'indirizzo IP della macchina stessa, dato che, come abbiamo già evidenziato, gli IP degli host di una LAN devono obbligatoriamente essere diversi se appartengono ad una stessa sottorete. Nel nostro caso possiamo scegliere di utilizzare appunto una unica subnet, visto che il numero degli host è contenuto. In questo modo semplifichiamo la configurazione e rendiamo più "visibili" tra loro gli host.

Come per i server, supponiamo che siano perfettamente installati sia il sistema operativo che le schede Fast Ethernet.

Cliccando sull'icona della LAN vicino all'orologio e poi su *Proprietà*, apriamo la solita finestra di configurazione della connessione alla rete locale.

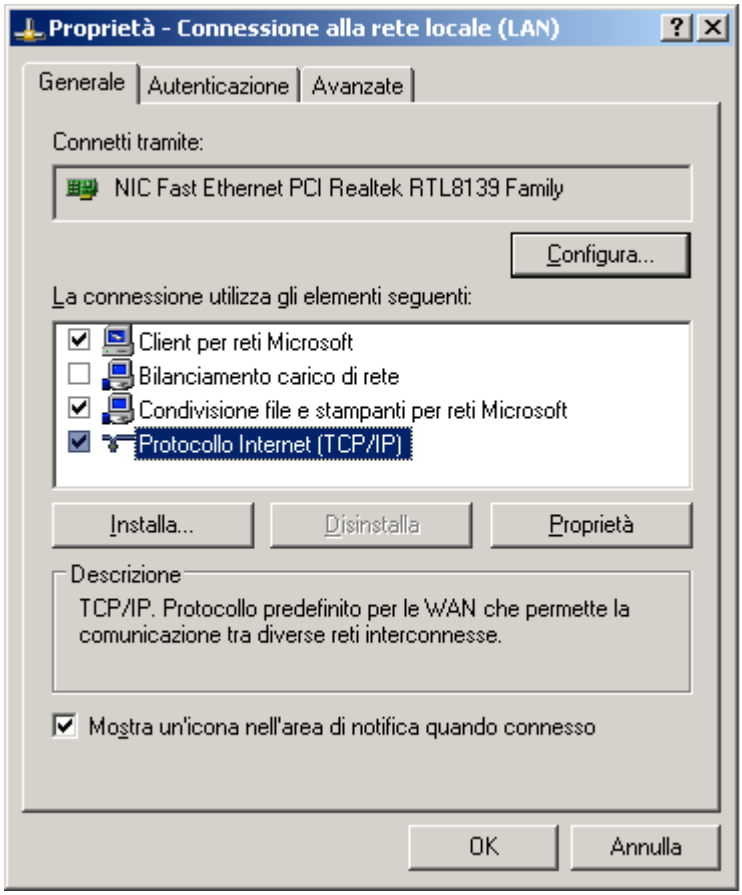

FOTO 5.7.1: Stavolta configuriamo i client

Selezioniamo il protocollo TCP/IP e poi andiamo su *Proprietà* per inserire l'indirizzo IP del client.

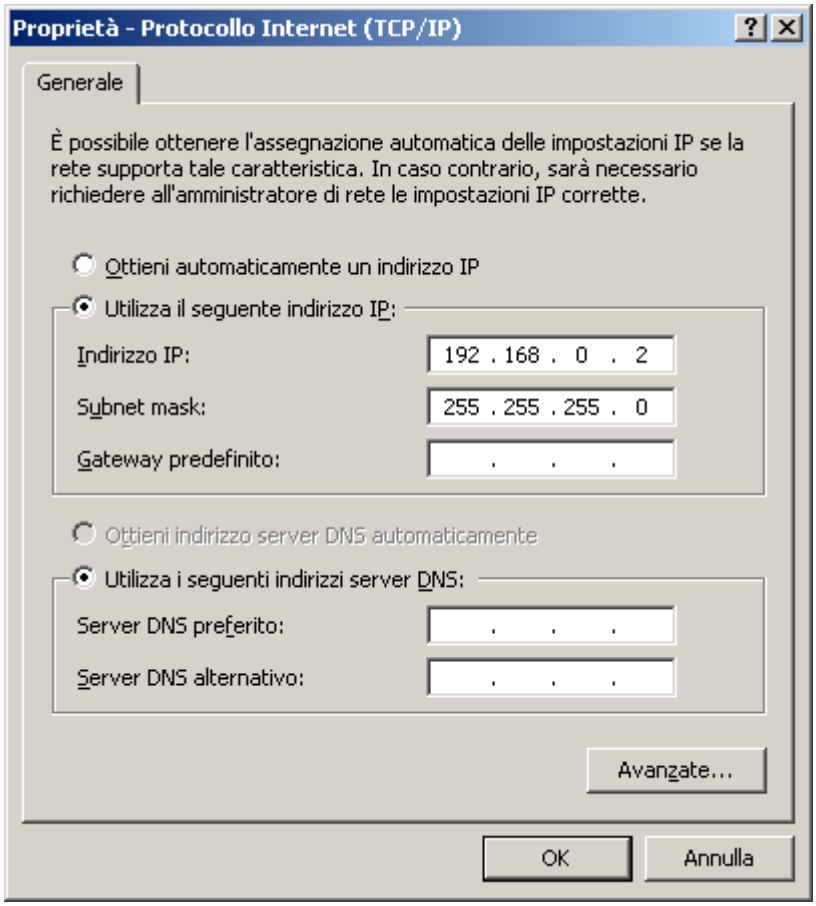

FOTO 5.7.2: Partiamo dall'indirizzo 192.168.0.2 e proseguiamo per gli altri client

Selezioniamo la casella *Utilizza il seguente indirizzo IP* e inseriamo il primo indirizzo permesso, quindi 192.168.0.2.

Tips: per gli altri client useremo IP crescenti: 192.168.0.3, 192.168.0.3, …, 192.168.0.16

Nella casella *Subnet mask* lasciamo invariato il valore impostato da Windows, quindi 255.255.255.0. Dobbiamo ora indicare al client qual è l'indirizzo del server primario, che avevamo configurato in precedenza, che fa da server DNS. Nella sezione inferiore della maschera degli indirizzi è necessario selezionare la casella *Utilizza i seguenti indirizzi server DNS* per inserire l'IP del server DNS, che nel nostro caso era 192.168.0.17.

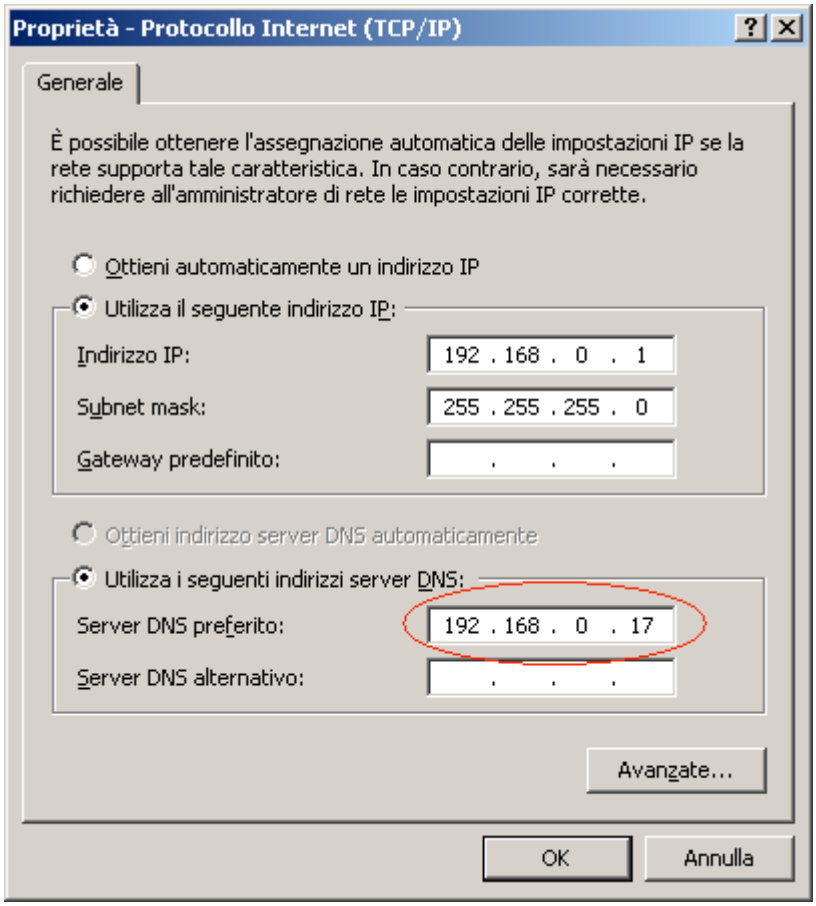

FOTO 5.7.3: L'indirizzo del server DNS corrisponde all'IP scelto nella configurazione ruolo del server primario

Dopo aver inserito i vari indirizzi IP spostiamoci nella finestra delle impostazioni avanzate del TCP/IP per mezzo del pulsante *Avanzate*. Nelle varie sottocartelle possiamo controllare che tutti i parametri da noi impostati siano a posto ed eventualmente apportare delle modifiche agli indirizzi IP, selezionando l'IP desiderato e cliccando su *Modifica.*

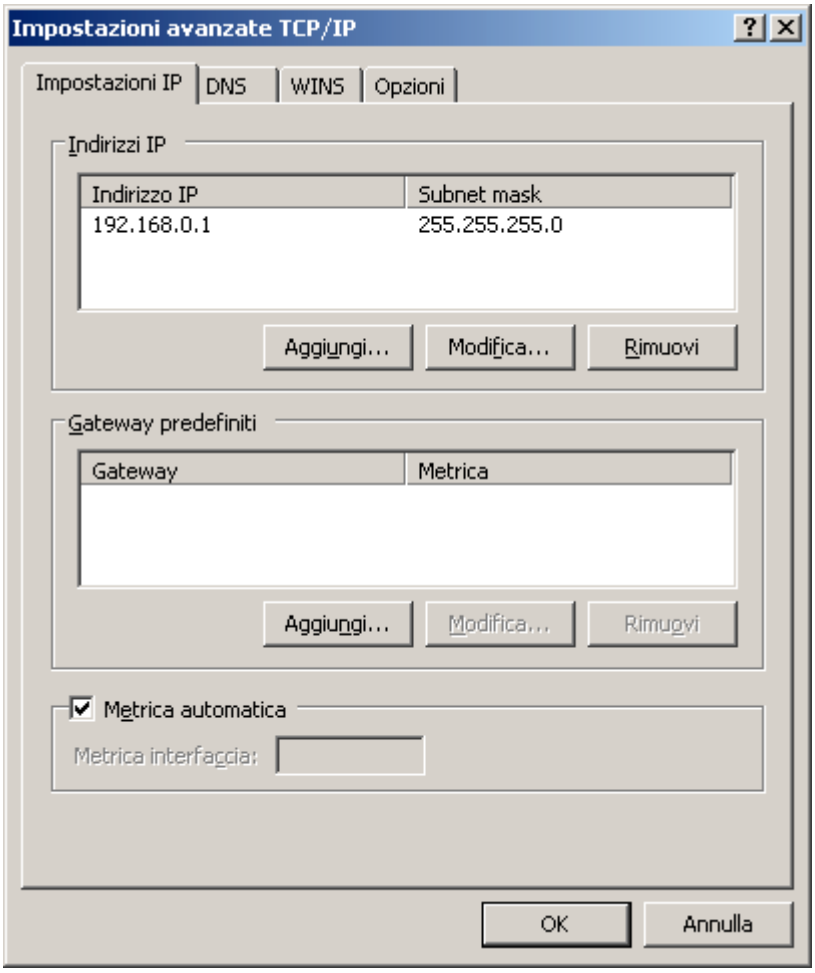

FOTO 5.7.4: Le impostazioni avanzate del TCP/IP. Da questa finestra è anche possibile modificare gli indirizzi impostati

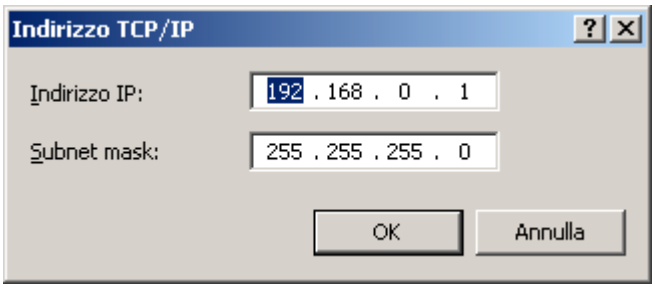

FOTO 5.7.5: Selezionando un indirizzo e cliccando su Modifica si apre la finestra in cui è possibile modificare gli IP impostati

5.8 Connessione della LAN a Internet: le VPN

L'ultima cosa che ci resta da fare è fornire a tutti gli host della nostra LAN una connessione ad Internet. Il motivo di tale scelta è ovvio: oggi Internet è diventato uno strumento così importante, sia nel lavoro che nella vita privata, che è molto difficile farne a meno dopo averlo utilizzato. Il reperimento di informazioni di qualsiasi tipo è immediato, così come l'invio di dati ad utenti esterni alla LAN. Connettere una LAN ad Internet significa aumentarne le capacità di espansione: è possibile in questo modo che la nostra LAN lavori insieme ad una LAN esterna grazie al collegamento fornito da un provider per mezzo della linea telefonica. Le reti di questo tipo sono chiamate VPN (Virtual Private Network) e sono l'alternative alle WAN private. Come abbiamo visto, le reti locali si possono collegare fra loro anche se sono distanti e si crea così una rete

geografica. Per il collegamento geografico (da città a città, per esempio) le aziende hanno tradizionalmente utilizzato apposite linee dedicate, fornite da una società telefonica. La 'congiunzione' tra sede e filiale, o tra la sede e la casa di un dipendente, in passato richiedeva perciò una costosa linea 'privata', appositamente noleggiata dall'azienda per il servizio. Per un'azienda di medie o piccole dimensioni, una WAN rappresentava perciò una risorsa impegnativa. Ora però è disponibile un'alternativa: la rete privata virtuale. La VPN è una connessione che utilizza una rete pubblica (come Internet) per offrire gli stessi vantaggi delle linee dedicate: sicurezza e efficienza nel trasferimento dei dati. In pratica:

- Maggiore convenienza: gli utenti remoti e le filiali possono collegarsi alle risorse della rete centrale chiamando un Internet Service Provider locale, al costo di una chiamata urbana. Un metodo decisamente più conveniente rispetto alle linee dedicate da città a città.
- Maggiore flessibilità. Spostarsi o aprire nuove filiali in altre località non richiede l'installazione di nuove linee dedicate per la trasmissione dati. Inoltre le VPN semplificano anche la creazione di una extranet, ovvero una rete 'protetta' e riservata a cui accedono clienti o fornitori, per esempio, per ordinare prodotti, verificare lo stato delle forniture, inviare fatture.

5.8.1 La sicurezza nelle VPN

Sfruttare Internet per la propria rete WAN può sembrare pericoloso: qualcuno potrebbe vedere i dati privati dell'azienda senza autorizzazione. In realtà le VPN proteggono i dati da accessi non autorizzati in molteplici modi. Innanzitutto creano una specie di "tunnel" riservato all'interno della rete pubblica: i dati non si mescolano a quelli di tutte le altre aziende e utenti. Inoltre particolari tecnologie di cifratura rendono i dati leggibili solo dal mittente e dal destinatario: quindi, nessun pericolo.

5.8.2 Gli elementi necessari per creare una VPN

Una azienda di medie o piccole dimensioni può creare e gestire una propria VPN, ma è sicuramente più semplice affidarsi a un Internet Service Provider. In tal caso l'azienda si collega alla rete del Provider, il quale farà da "ponte" verso la filiale o l'utente remoto che si desidera connettere. È ovviamente necessario che il Provider scelto sia in grado di garantire un efficace livello di servizio (tra cui un funzionamento ininterrotto per almeno il 99% del tempo) e di prestazioni. È anche utile scegliere un Provider che abbia molti punti di connessione sparsi sul territorio (POP) per facilitare la creazione di nuove VPN in altre città mantenendo le chiamate telefoniche sulla tariffa urbana. Con una rete VPN è anche consigliabile disporre di un firewall, che controlla e protegge ulteriormente la rete dagli utenti non autorizzati. Le funzionalità firewall possono anche essere svolte dai dispositivi di rete esistenti, aggiungendo un apposito software.

Linee analogiche

La soluzione standard per collegarsi ad altre reti o a Internet, o per permettere agli utenti remoti di collegarsi alla propria rete centralizzata, è la normale linea telefonica analogica. Basta quindi collegare un modem al computer e alla presa del telefono per collegarsi ad un Internet Service Provider o ad una filiale. Attualmente, i modem analogici più veloci per il trasferimento di dati operano a 56 Kbps.

Le dimensioni sempre più consistenti dei file e l'uso sempre maggiore della rete rende tale velocità spesso insufficiente. Inoltre un modem può supportare solo una "conversazione" remota alla volta e ogni computer che vuole collegarsi con l'esterno deve disporre di un proprio modem. In questo caso, però, vi è una soluzione più efficiente per una connessione WAN: il router. Il router utilizza linee ISDN (digitali) e collega tutti i computer della rete locale: basta un router e molti computer possono navigare sul web o collegarsi ad una filiale. Inoltre il router offre maggior protezione da

accessi indesiderati, è più rapido nell'effettuare la connessione e nello staccare la linea telefonica quando l'attività di rete cessa.

ISDN

Le nuove linee ISDN si stanno diffondendo notevolmente in tutto il mondo. Dal punto di vista telefonico sono convenienti perchè offrono servizi aggiuntivi basati sulle tecnologie digitali a costi ridotti. Dal punto di vista dei dati di rete sono efficienti perché sono digitali e non analogiche, che invece utilizzano un "linguaggio" meno efficiente e con maggior rischio di errore. La tecnologia digitale, usata dalla linea ISDN e dai router, trasmette puri dati (e non "rumorosi" segnali da decodificare), non è afflitta dai "disturbi" della linea, opera a 64 oppure a 128 Kbps, e quindi offre maggiore velocità rispetto ai modem, e consente numerose funzionalità in più. I costi per i collegamenti ISDN sono paragonabili a quelli per le linee analogiche, ma la convenienza deriva dalla maggior velocità. Tecnicamente, una linea ISDN comprende due canali da 64 Kbps che operano separatamente o insieme. Potete usarne uno per telefonare e l'altro per i dati, oppure usare tutti e due i canali per la trasmissione dati, o addirittura usarli per l'una o per l'altra attività a seconda del bisogno del momento. Va sottolineato inoltre che le linee ISDN sono in grado di farvi usare anche i vostri vecchi dispositivi analogici (un vecchio fax, un telefono non digitale, un modem analogico): ovviamente non sfrutterete tutti i benefici del digitale, ma salverete i vostri investimenti. Alla linea ISDN è possibile collegare un router (del tipo predisposto per ISDN), in grado di "convogliare" tutta la rete locale sulla linea esterna in modo digitale.

Linee ADSL

La tecnologia ADSL (Digital Subscriber Line Asincrona) è un servizio ad alta velocità che, come ISDN, opera attraverso i normali cavi telefonici (il doppino in rame che siamo abituati a vedere nelle case) e fornisce i servizi telefonici ad abitazioni e aziende. È una tecnologia asimmetrica, ovvero la capacità di trasmettere dati è maggiore da Internet verso l'utente, ed inferiore quando è l'utente a inviare dati verso Internet. Per sfruttarla dovrete avere un modem o un router di tipo ADSL, solitamente fornito dall'ISP a cui ci si appoggia per il servizio. Questa tecnologia garantisce una trasmissione dei dati più rapida sia rispetto ai modem analogici sia al servizio ISDN.
Le offerte ADSL sul mercato spesso comprendono una connessione ininterrotta per 24 ore al giorno senza scatti, in cambio di un canone fisso e danno anche la possibilità di utilizzare contemporaneamente la linea per telefonare. In breve, ADSL si sta rivelando molto vantaggiosa, in particolare per le aziende di minori dimensioni.

Linee dedicate

Le società telefoniche offrono numerosi servizi con linee dedicate, ovvero linee digitali, permanenti, "aperte" 24 ore al giorno, sette giorni la settimana, dedicate all'utente richedente, sulla tratta richiesta (passando per una centrale della società telefonica). Invece di pagare un costo "a scatti", si paga una cifra fissa mensile senza limiti d'uso, basata sulla velocità e/o sulla distanza. Le linee dedicate migliori per le medie e piccole aziende hanno velocità variabili da 56 Kbps a 45 Mbps. La scelta della velocità dovrebbe dipende ovviamente dal traffico e dal numero di utenti della rete. Le aziende con un uso considerevole della WAN, generalmente, scelgono una linea con larghezza di banda di 1,5 Mbps, ma per molti è sufficiente una larghezza di banda decisamente inferiore (con costi ridotti).

Il servizio ideale per ogni esigenza

La scelta del servizio migliore dipende dalle opportunità offerte nell'area del cliente, dal tipo di utilizzo e dai costi. I servizi analogici tradizionali (le consuete linee telefoniche di vecchio tipo) sono i meno costosi, i più disponibili e i più facili da usare. Le linee ISDN e ADSL sono leggermente più costose ma offrono prestazioni e servizi migliori. Le linee dedicate sono le più

costose ma offrono un servizio digitale dedicato per situazioni complesse e impegnative. Per scegliere la soluzione migliore e più adatta alle proprie esigenze basta porsi le seguenti domande:

- gli utilizzatori della rete utilizzeranno Internet di frequente per e-mail, navigazione web, scambio di file, o per quantità di dati significative con file di grandi dimensioni?
- Internet verrà utilizzata per attività aziendali importanti, come gestione dell'inventario, vendita on-line da catalogo, informazioni contabili, ricerca di personale?
- Si prevede un traffico intenso tra gli uffici di filiale e l'azienda?
- Chi utilizzerà la connessione principale verso Internet? I singoli dipendenti della sede centrale, i dipendenti in telelavoro che chiamano da casa, i dipendenti mobili che chiamano mentre sono in viaggio?

Maggiori sono i sì alle risposte, maggiore è la necessità di passare a soluzioni più potenti, partendo dalle linee analogiche per arrivare a ISDN, ADSL o alle linee dedicate. È comunque possibile combinare servizi diversi. Per esempio, i piccoli uffici di filiale o i singoli dipendenti che chiamano da casa potrebbero collegarsi alla sede centrale tramite ISDN o ADSL, mentre la connessione principale dalla sede centrale a Internet potrebbe essere di tipo dedicato.
La scelta del servizio dipende anche dall'Internet Service Provider (ISP) utilizzato: si consiglia di analizzare la sua offerta anche i termini di servizi e di evoluzione successiva e non solo di economicità dei servizi di base offerti. Si deve inoltre considerare che una rete VPN può offrire le stesse funzionalità di una linea dedicata con costi inferiori, estendendo la rete aziendale e l'accesso a Internet agli uffici remoti e ai singoli utenti, con risparmi significativi. Vale quindi la pena di porsi anche le seguenti domande:

- è prevista l'aggiunta di filiali o utenti remoti a breve termine?
- Gli attuali costi di linea per l'accesso remoto aumentano rapidamente?
- L'azienda preferirebbe focalizzare il proprio interesse sulle attività strategiche piuttosto che sulla creazione di una WAN?
- E' prevista la creazione di una extranet per collegare in modo sicuro fornitori, partner o clienti alla rete aziendale?

Se la risposta è sì a una o più domande, la VPN potrebbe essere la soluzione corretta.

5.8.3 Impostazione dell'indirizzo del router

Come dicevamo, il router da noi scelto è un dispositivo dedicato che connette la LAN con l'esterno. Tale tipo di componente di rete è facilmente reperibile nei negozi di informatica a prezzi molto contenuti, purchè non si pretenda la qualità di prodotti di fascia "professionale". Tuttavia anche un prodotto di tipo economico può reggere senza alcun problema il carico di lavoro di una LAN come quella da noi realizzata.
Generalmente i router hanno un indirizzo IP assegnato di default: per molte marche questo indirizzo è 192.168.0.1, per altre è 192.168.1.1. Spesso questo indirizzo può essere variato da un pannello di controllo del router, ma conviene sempre lasciarlo invariato.
Apriamo la solita finestra di configurazione del protocollo TCP/IP, cliccando sull'icona della rete in basso nel desktop e poi su *Proprietà*. Selezioniamo il TCP/IP ed ancora clic su *Proprietà* per andare nella finestra di assegnazione degli indirizzi.

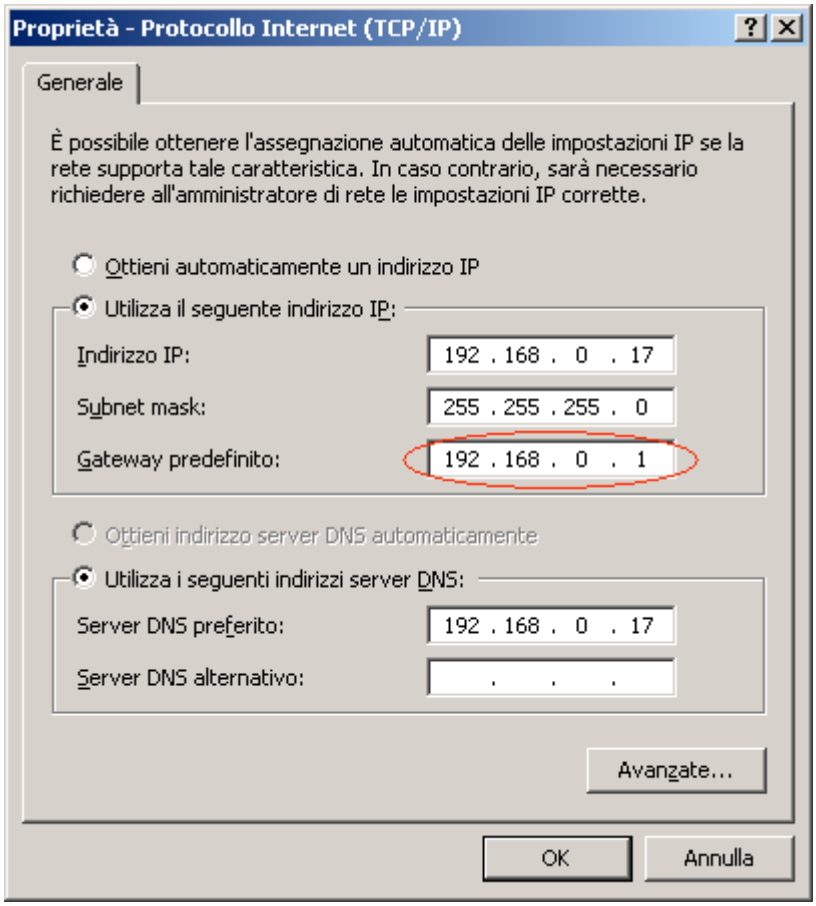

FOTO 5.8.3.1:
L'indirizzo del gateway è quello che il router possiede di default

Nella casella *Gateway predefinito*, che era rimasta vuota, dobbiamo scrivere l'indirizzo IP del nostro router-gateway. Confermiamo la scelta con il pulsante OK e di nuovo sulla finestra precedente. In questo modo ogni host conosce il dispositivo a cui rivolgersi per la connessione ad Internet.

Tips: L'indirizzo IP del router va impostato in tutti i computer appartenenti alla LAN, per fare in modo che questi abbiano accesso ad Internet

5.9 La LAN è pronta!

A questo punto le impostazioni per i server e per tutti gli host sono complete e la nostra rete dovrebbe funzionare. Per provare che tutto sia a posto verifichiamo dalle varie postazioni che tutti gli host siano visibili: in *Start /Esplora risorse*, apriamo la finestra di gestione delle risorse di Windows.

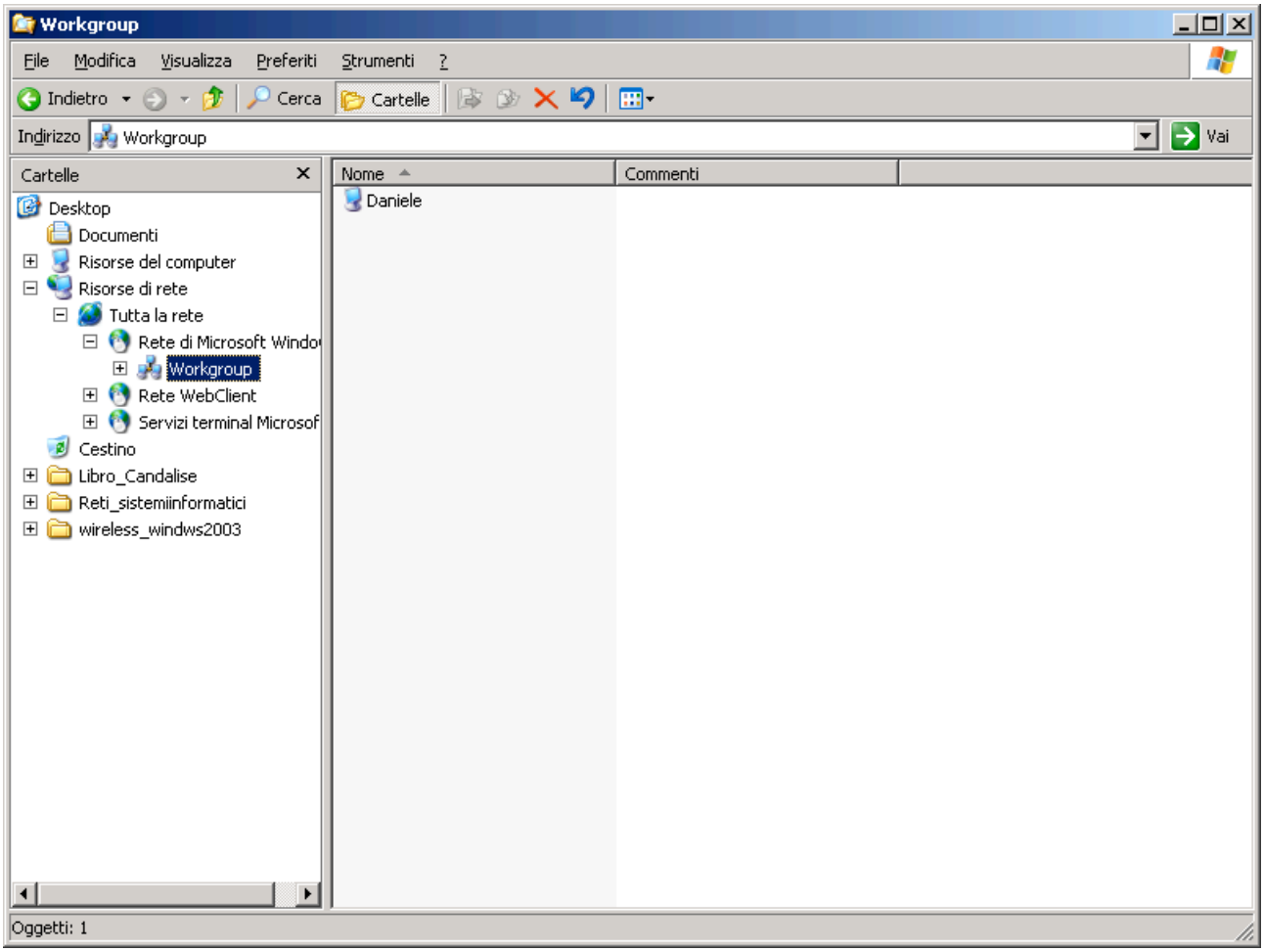

FOTO 5.9.1:
In Esplora risorse possiamo navigare le Risorse di rete per visualizzare gli host della LAN

Nella sezione *Risorse di rete* saranno visibili tutti gli host della LAN appena realizzata. Il percorso preciso è: *Risorse di rete/Tutta la rete/Rete di Microsoft Windows* – e poi il nome del gruppo di lavoro da voi assegnato, all'interno del quale troverete i nomi (nella destra della finestra di Esplora risorse) degli host della vostra rete.
Un modo più sicuro e "professionale" per il testing delle stazioni della LAN è dal prompt del DOS, utilizzando il comando *ping*, tanto noto agli esperti di reti. Questo comando permette di verificare se un host riesce a connettersi alla rete TCP/IP ed utilizzare le risorse di rete. Il comando verifica la connettività a livello IP inviando dei pacchetti ad un determinato indirizzo ed attendendo la risposta. Durante la conversazione tra le macchine viene calcolato il tempo di risposta e gli eventuali pacchetti perduti durante la trasmissione dei dati. Ecco un esempio dell'utilizzo del comando ping sulla nostra rete: abbiamo "pingato" il server, che ha indirizzo 192.168.0.17 e la risposta è stata positiva. Questa prova è stata effettuata in effetti sulla stessa macchina, solo per mostrare il funzionamento del comando, per cui i tempi di risposta sono nulli.

Tips: Il comando *Ping* riferito al proprio PC può essere utile per verificare il perfetto funzionamento della scheda Ethernet

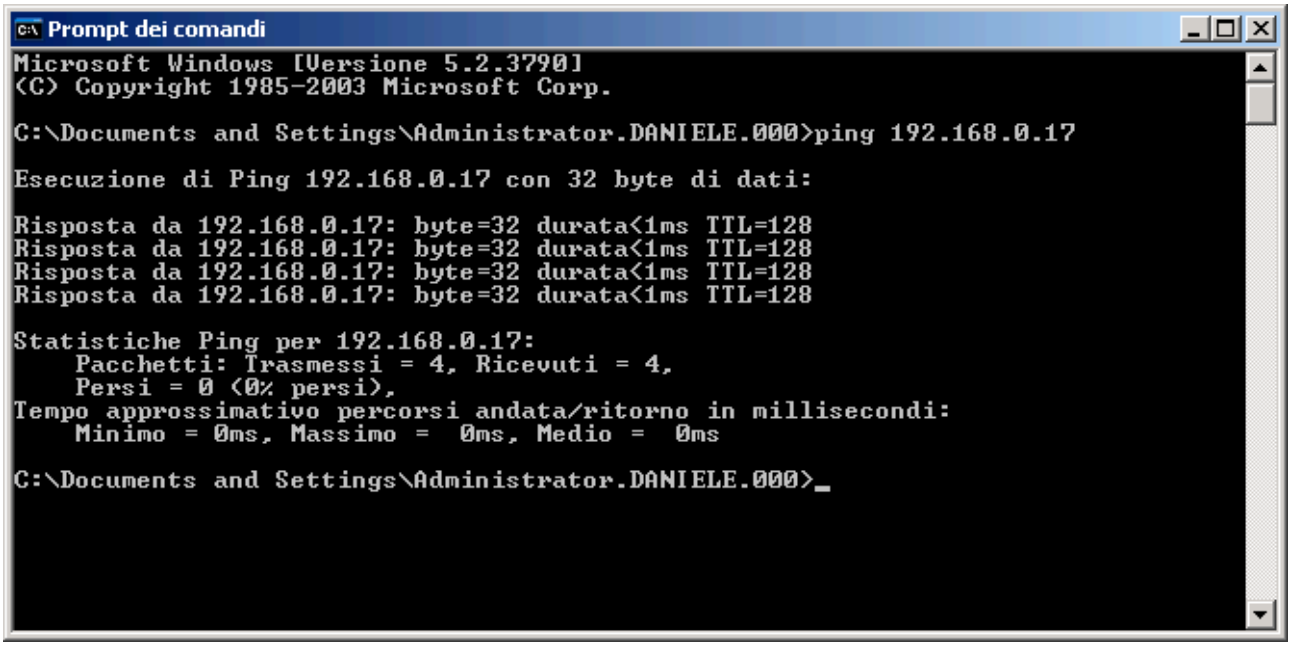

FOTO 5.9.2:
Il comando *ping* verifica che l'host ad un certo indirizzo sia connesso alla LAN

Avendo nella nostra LAN un server DNS, che come ricorderemo serve per risolvere gli indirizzi IP in nomi, possiamo utilizzare il comando ping scrivendo il nome invece dell'indirizzo. In questo caso la sintassi è identica ma al posto dell'IP scriviamo il nome della macchina.

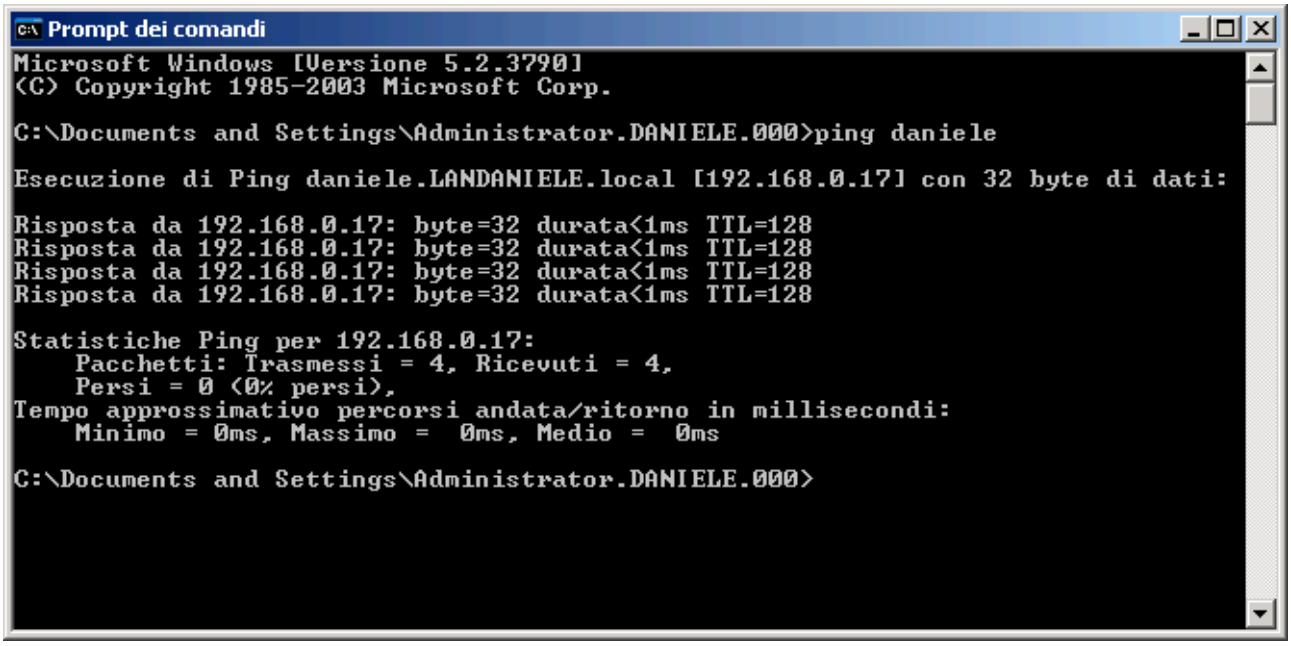

FOTO 5.9.3:
La presenza di un server DNS permette di utilizzare il comando ping con il nome della macchina invece che con l'IP

Se si desidera ottenere informazioni più dettagliate sulla propria macchina è possibile utilizzare il comando *ipconfig* o *ipconfig/all*. Quest'ultimo fornisce indicazioni dettagliate sulla configurazione di tutte le interfacce, incluse le eventuali porte seriali.

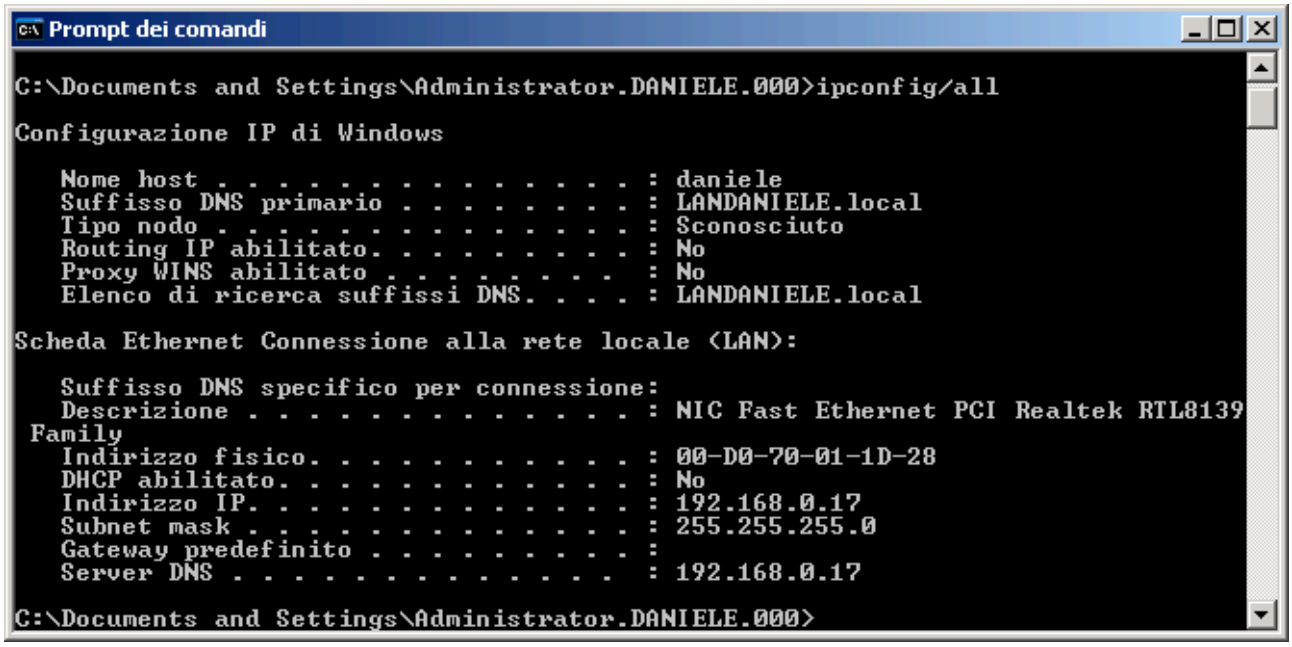

FOTO 5.9.4: Il comando *ipconfig/all* fornisce un rapporto dettagliato sulle interfacce

5.10 Alcuni dettagli per la sicurezza della rete

Come altri sistemi Windows, anche Server 2003 dispone di molti strumenti per la sicurezza dei dati e l'affidabilità della rete. In realtà Windows Server 2003 fornisce agli amministratori di rete strumenti avanzati che noi non tratteremo in questa sede perché sarebbero inutili in un piccolo ambiente di rete: lo spazio limitato, inoltre, sarebbe un grande ostacolo per l'analisi di strumenti di rete così importanti.

Anche gli strumenti che analizzeremo, tuttavia, aiutano a rendere la nostra LAN più solida ed immune da attacchi esterni.

Windows Server 2003 dispone, come Windows XP, di un firewall incorporato, che previene l'intrusione alla LAN dall'esterno. Anche se la nostra rete dispone di firewall integrato nel router (o posto tra router e LAN, in dipendenza dal prodotto da noi scelto), è sempre meglio attivarlo anche sulle singole macchine, per aumentare il livello di sicurezza.

Apriamo la finestra delle proprietà della connessione alla rete (clic sull'icona in basso nel desktop – Proprietà). In questa finestra spostarsi nella sezione *Avanzate*.

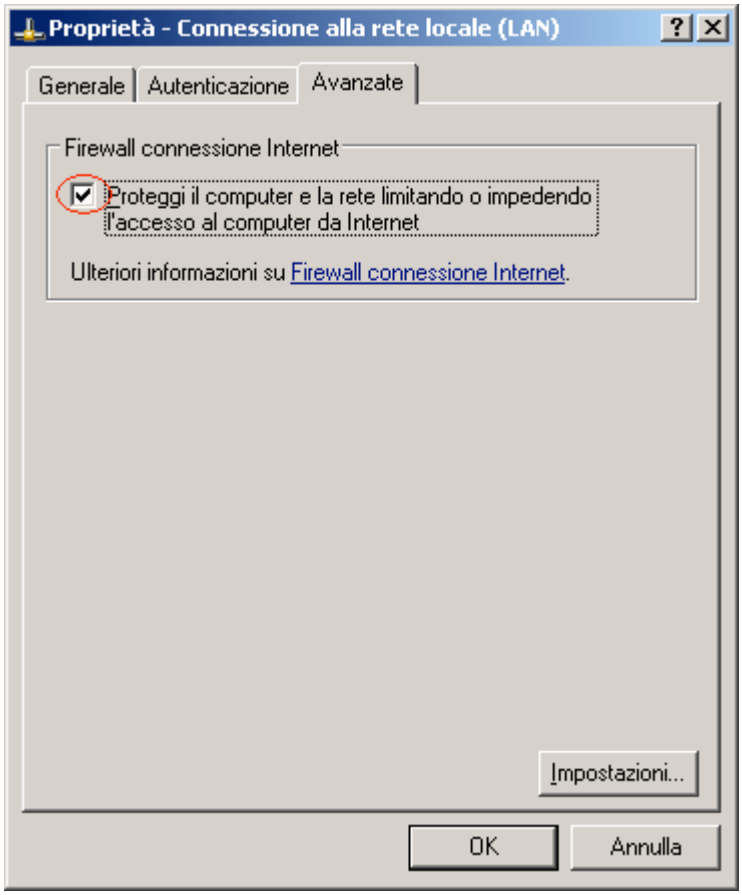

FOTO 5.10.1: Il firewall integrato in Windows Server 2003 previene intrusioni indesiderate

Come impostazione di default, il firewall è disabilitato. Per abilitarlo basta spuntare la casellina. Appena fatta questa operazione, il pulsante *Impostazioni* diventerà attivo. Clicchiamo su *Impostazioni* per configurare il firewall.

Nella cartella *Servizi* della finestra delle impostazioni avanzate, bisogna specificare in quali casi è permesso l'accesso dall'esterno della rete. Nel nostro caso i servizi Web possono essere tutti lasciati disabilitati grazie al filtraggio da parte del router.

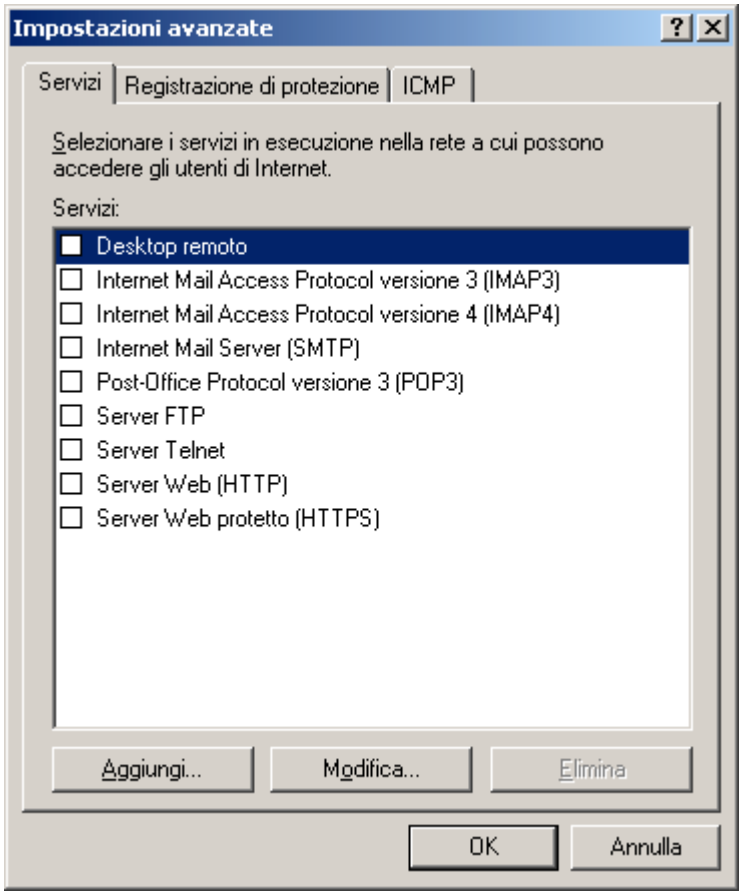

FOTO 5.10.2: I servizi permessi dal firewall vanno specificati in questa lista

Nella seconda cartella, *Registrazione di protezione*, si può specificare se registrare particolari eventi e il file in cui memorizzarli. Spuntando la casella in alto, *Registra pacchetti in ingresso ignorati*, si memorizzano i pacchetti scartati che erano stati originati all'interno della LAN o da Internet, mentre un segno di spunta sulla casella *Registra connessioni riuscite*, permette di memorizzare tutte le connessioni completate, sia interne che esterne alla LAN. Tutte queste registrazioni avvengono in un file registro, che di default è chiamato pfirewall.log ed è situato nella cartella c:\Windows.

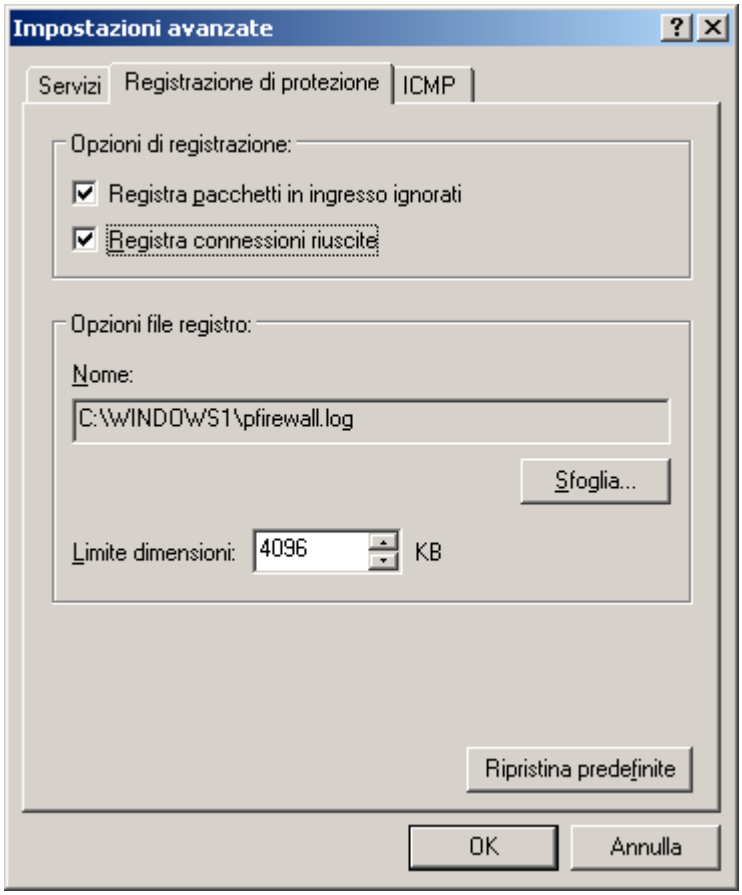

FOTO 5.10.3: E' possibile memorizzare diversi eventi "catturati" dal firewall

Cliccando sul pulsante *Sfoglia* è possibile dare un altro nome al file registro e cambiare la sua posizione, magari per motivi di comodità, nel caso in cui esso debba essere consultato frequentemente. Dalla finestra *Limita dimensioni* si può specificare la dimensione che il file può assumere per aumentare il numero delle memorizzazioni in esso contenute.
L'ultima cartella tra quelle delle impostazioni avanzate, *ICMP*, contiene una serie di box disabilitati. Queste opzioni si riferiscono alla possibilità di effettuare operazioni di ping sugli host della LAN: per potere utilizzare il comando ping sulla rete è necessario spuntare le caselle di questa lista, per consentire ai pacchetti di "viaggiare" all'interno della rete senza impedimenti.

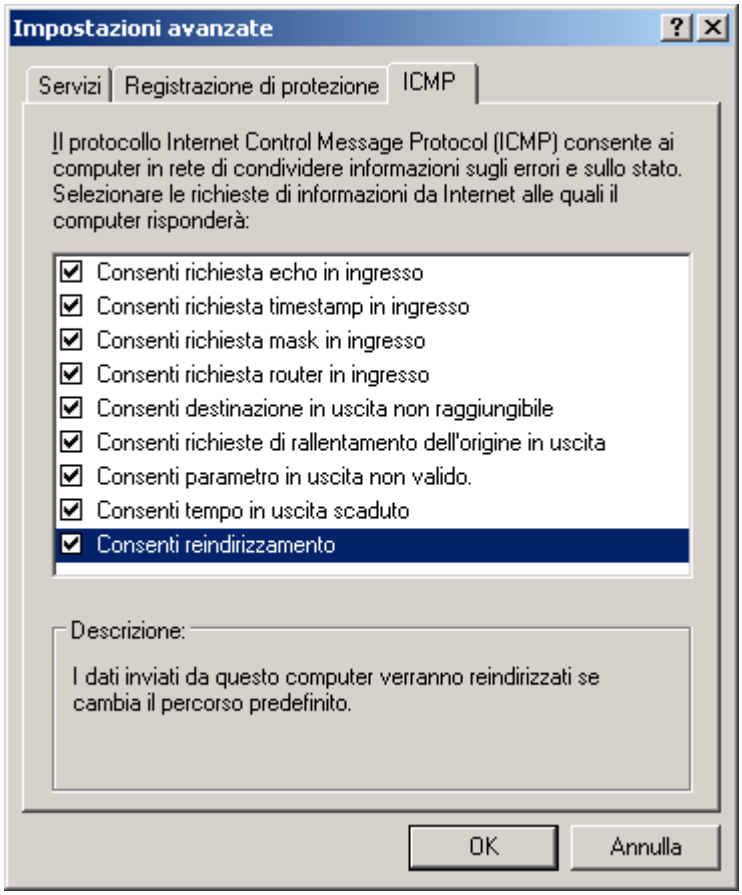

FOTO 5.10.4: La lista dei permessi per effettuare operazioni di verifica sulla LAN

Spuntando le varie caselle si otterrà in basso nella finestra una breve guida da cui è possibile decidere se attivare o meno i vari permessi. Dato che la nostra LAN è già protetta da un firewall, è possibile abilitare tutte le voci della lista.
Altra importante funzionalità è la possibilità di settare le impostazioni del filtro TCP/IP. Vediamo cosa è e come si modifica.
Apriamo la solita finestra del TCP/IP, selezioniamo questo protocollo e clicchiamo su *Proprietà*. Nella finestra degli indirizzi IP cliccare su *Avanzate* e spostarsi nella cartella *Opzioni.*

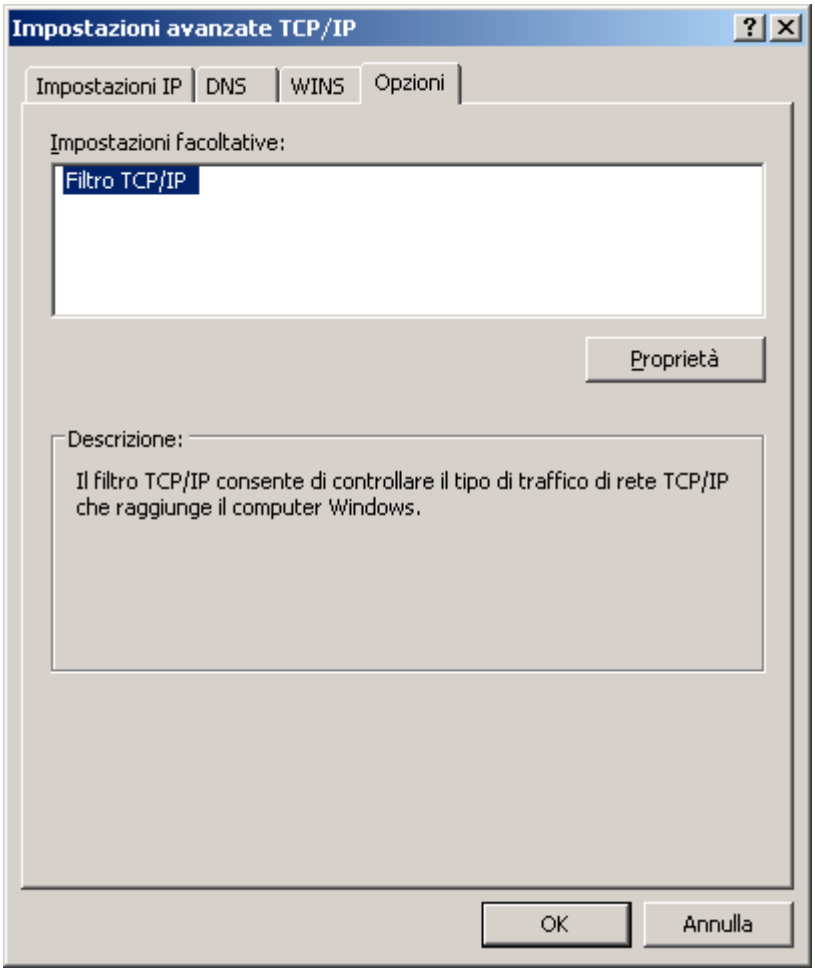

FOTO 5.10.5: La finestra per il settaggio del filtro TCP/IP

Il pulsante proprietà, riferito al filtro TCP/IP selezionato ci permette di aprire la seguente maschera:

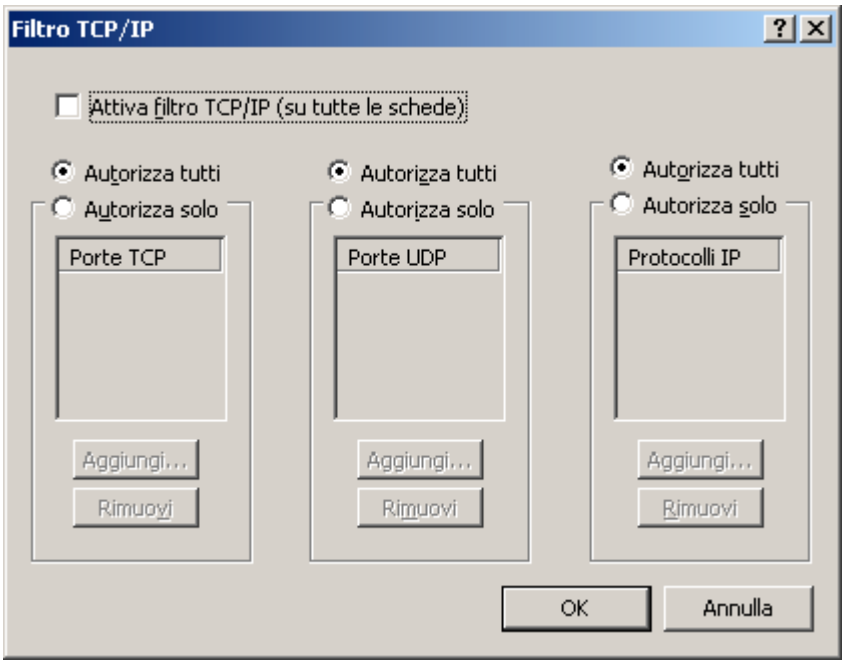

FOTO 5.10.6: E' possibile autorizzare solo alcune porte o protocolli all'accesso

Normalmente tutti sono autorizzati dal protocollo ad entrare, ma è possibile limitare l'ingresso ad alcuni elementi della rete se necessario. Supponiamo di volere fornire l'accesso al nostro host solo a determinati indirizzi IP, magari i nostri collaboratori o amici: nella casella a destra selezioniamo la voce *Autorizza solo* e poi clicchiamo sul pulsante *Aggiungi*.
Nella casella di testo della finestrella *Aggiungi filtro* è possibile indicare il protocollo IP a cui l'accesso è permesso. Analogamente è possibile autorizzare l'ingresso da porte TCP o UDP. Nella nostra rete possiamo trascurare tali impostazioni e lasciarle immodificate rispetto a quelle di default.

5.11 Chiusura sessione di Windows Server 2003
Windows Server è un sistema progettato quasi esclusivamente per l'utilizzo su macchine che, essendo server, stanno quasi sempre accese. La chiusura di un sistema si questo tipo è perciò interpretata da Windows come un evento eccezionale, per cui va richiesta una motivazione. Se terminiamo la sessione da Start – Chiudi sessione o con CTRL – ALT – CANC e poi Arresta il sistema, avremo di fronte una finestra di questo tipo:
Nella tendina delle opzioni, in basso nella finestra, si sceglie il motivo per cui si chiude la sessione. L'operazione può essere classificata come pianificata o meno, in base al segno di spunta della casella. Affinché il pulsante OK si attivi è necessario scrivere un commento nell'apposita casella.
Queste operazioni sono necessarie non solo per la chiusura della sessione ma anche per il riavvio, lo standby e la disconnessione.