TITOLO: **Progetto di una rete LAN CLIENT/SERVER**
MATERIE: **Sistemi e Reti, Telecomunicazioni**
OBIETTIVI: **Analizzare un problema di configurazione di una rete LAN CLIENT/SERVER cablata**

■ ESPOSIZIONE DEL PROBLEMA DI ANALISI/PROGETTAZIONE

Questo elaborato illustra la realizzazione di una rete LAN aziendale di tipo CLIENT/SERVER con accesso ad Internet. Il modello client-server è un insieme di processi in esecuzione su diversi host: i processi che gestiscono una o più risorse sono detti server, quelli che richiedono l'accesso ad alcune di tali risorse client.
Un processo server può a sua volta diventare client ed essere contemporaneamente sia client sia server.
É importante non fare confusione tra server e servizio, infatti:

- il Servizio è l'entità astratta fornita da uno o più server;
- il server è l'insieme di macchine, spesso eterogenee, che ospitano diversi servizi.

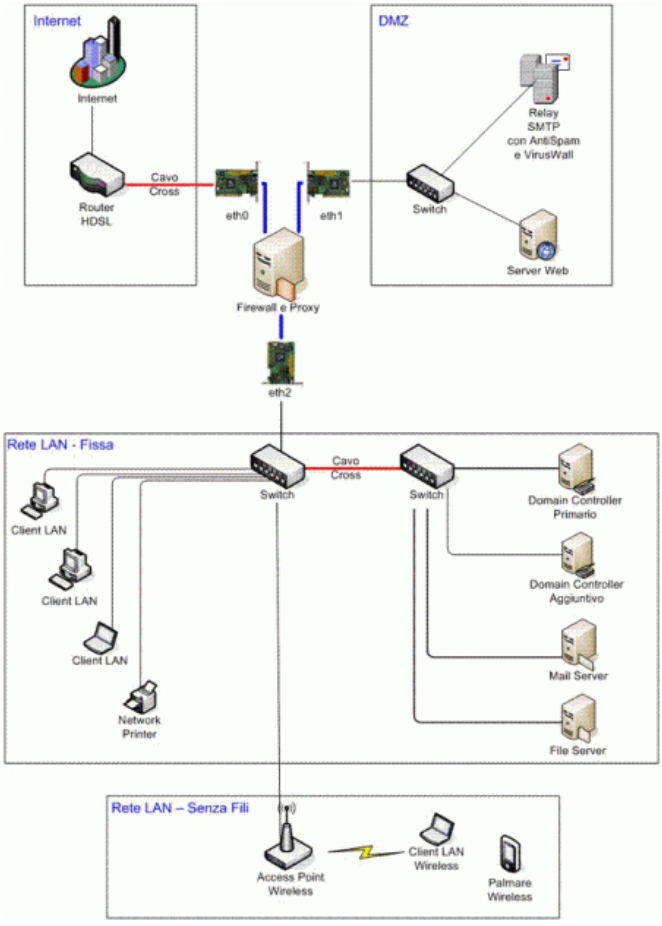
Alcuni esempi di servizi tipici delle architetture client-server sono:

- HTTP (Porta 80) e HTTPS (Porta 443), utilizzati per la trasmissione d'informazioni sul web;
- FTP (Porte 21/20), utilizzato per il trasferimento di dati tra diversi host;
- Telnet (Porta 23), utilizzato per il controllo di computer da remoto.

Schema di funzionamento di un modello client-server:

1) Il client manda una richiesta al server;
2) Il server (in stato di ascolto, listening) riceve la richiesta;
3) Il server esegue il servizio richiesto (mediante un thread concorrente);
4) Il server invia una risposta al client;
5) il client riceve la risposta.

Queste attività avvengono in maniera trasparente sia per i processi server sia per quelli client.
La seguente figura mostra la struttura logica di una tipica Rete di PC di un'azienda da configurare in modalità CLIENT/SERVER



D. Tomassini, L. Borzetta © Copyright Ulrico Hoepli Editore Spa

■ SVILUPPO DELLA SOLUZIONE CON SPIEGAZIONI E SCHEMI

La società per la quale occorre realizzare la LAN è “Azienda S.p.A.”, e quindi il nome di dominio utilizzato sia per Active Directory sia per Internet è “azienda.it”.

Caratteristiche

La rete deve presentare le seguenti caratteristiche:

- connessione verso Internet a 4 Mbit/s;
- disporre di un proprio server Web che ospita il sito Internet aziendale;
- disporre di un proprio server interno di posta elettronica;
- 70 postazioni client.

Prerequisiti

Occorre:

- un contratto aziendale per connessione Internet in HDSL a 4Mbit/s e possibilmente con Router a noleggio;
- almeno 8 indirizzi IP pubblici statici dal proprio Provider Internet;
- aver registrato il dominio Internet presso il NIC che nel nostro esempio sarà “azienda.it”;
- aver cablato e certificato l’edificio aziendale ed aver predisposto le relative prese a muro RJ45 per le postazioni.

Obiettivi da raggiungere

1) Creare una rete LAN formata da computer fissi e da dispositivi senza filo (Wireless).
2) Pubblicare in maniera sicura il proprio server Web su Internet e renderlo visibile a tutti.
3) I server più a rischio di attacchi (web e posta) devono risiedere in una rete DMZ.
4) La posta elettronica ed il sito web devono essere visti sia su Internet che nella rete LAN.
5) Proteggere la rete LAN da attacchi esterni.
6) Proteggere la posta da attacchi verso il mail server, evitando quanto più possibile il problema dello Spam (posta indesiderata).
7) I computer e i server della rete devono navigare in Internet con un solo indirizzo IP pubblico ed in maniera protetta.
8) Bloccare la navigazione su alcuni siti Web non autorizzati.
9) Configurare un dominio Active Directory del tipo “azienda.it”.
10) Indirizzare tutti i log degli apparati su un server Syslo.

Materiale hardware necessario

un Armadio Rack

un Server in formato Rack

due Switch da 48 porte

100 cavi RJ45 categoria 5 “dritti”
meglio ancora se categoria 5e

D. Tomassini, L. Borzetta © Copyright Ulrico Hoepli Editore Spa

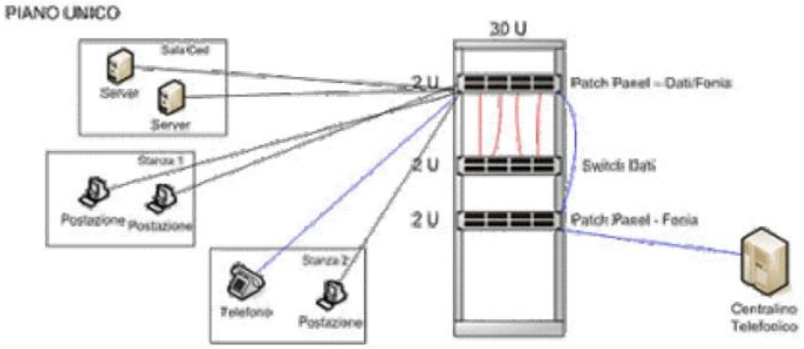
5 cavi RJ45 “incrociati”
(possono sempre servire)

1 Access Point Wireless

Realizzazione del cablaggio

La posa dei cavi e l’installazione delle prese da muro RJ45 (o colonnine da pavimento) deve essere effettuata da elettricisti specializzati nei cablaggi strutturati, che con opportuni strumenti possano “certificare” il corretto funzionamento di ogni tratto di rete (attenuazione, rumore, interferenze, ecc..). Tale certificazione, solitamente rilasciata all’utente in formato file TXT su un supporto CD-Rom, ha lo scopo di formalizzare la corretta installazione del cablaggio effettuato e rappresenta quindi una garanzia di qualità.
Essendo il cablaggio strutturato consente di utilizzare i cavi ethernet sia per il trasporto dati (rete LAN) sia per la fonia (telefoni).
In questo modo, alla presa al muro RJ45 è possibile collegare sia un computer sia un telefono.
A seconda della struttura fisica della società è necessario strutturare i collegamenti delle postazioni e degli switch in maniera diversa, come di seguito indicato.

1) **Rete estesa su un solo piano** - Se la società si estende su di un unico piano, le estremità dei singoli cavi che partono dalle prese a muro convogliano in una posizione centralizzata, che costituisce il “Centro Stella” della rete, come indicato nella figura seguente.



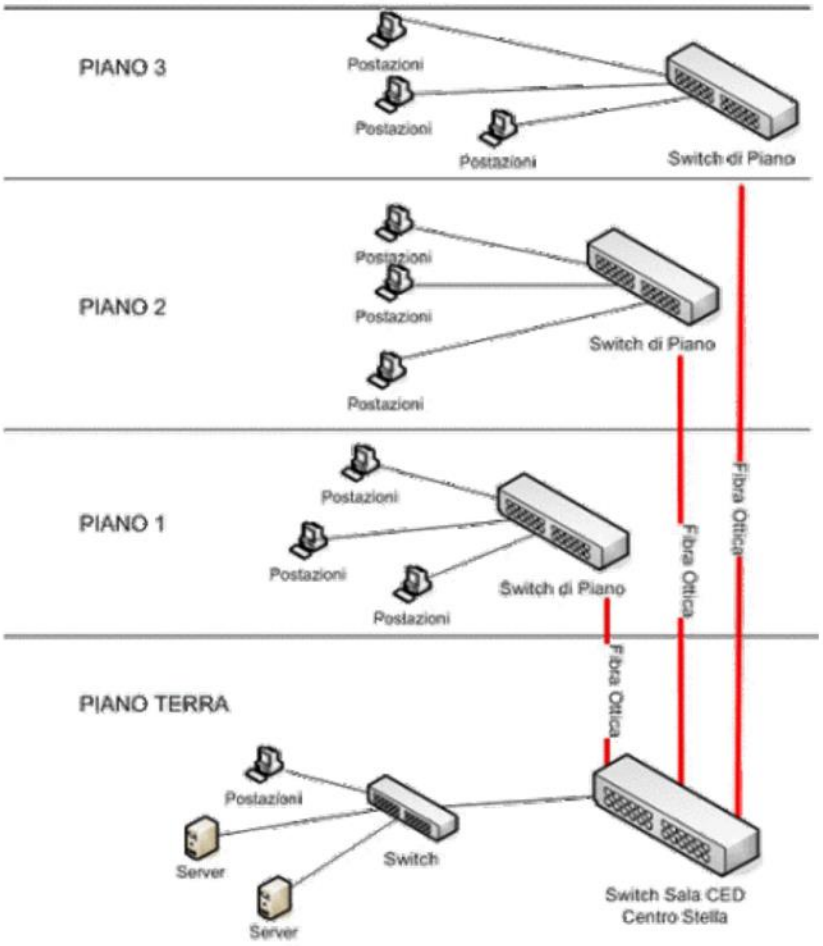
È importante ricordare che ogni cavo ha limiti di lunghezza (ad esempio il cat.5 arriva fino a 100 metri) e quindi, nel caso tale limite venga superato è necessario aggiungere ripetitori di segnale (tale funzione è oggi espletata dagli switch).
Tutti i cavi che provengono dalle prese a muro sono cablati sul retro di una base denominata “Patch Panel”, (mostrato in figura) la quale è di solito fisicamente installata in un armadio rack.

Realizzato il cablaggio occorre predisporre il collegamento dei client verso uno (o più) switch centrale, collegando la scheda di rete di ciascun PC alla presa a muro più vicina tramite un cavo di cat.5 ed annotando il numero identificativo della presa stessa. Sul patch panel, utilizzando una cavo patch cat 5, si collega la porta con il numero corrispondente alla presa dello switch più vicino (di solito presente

D. Tomassini, L. Borzetta © Copyright Ulrico Hoepli Editore Spa

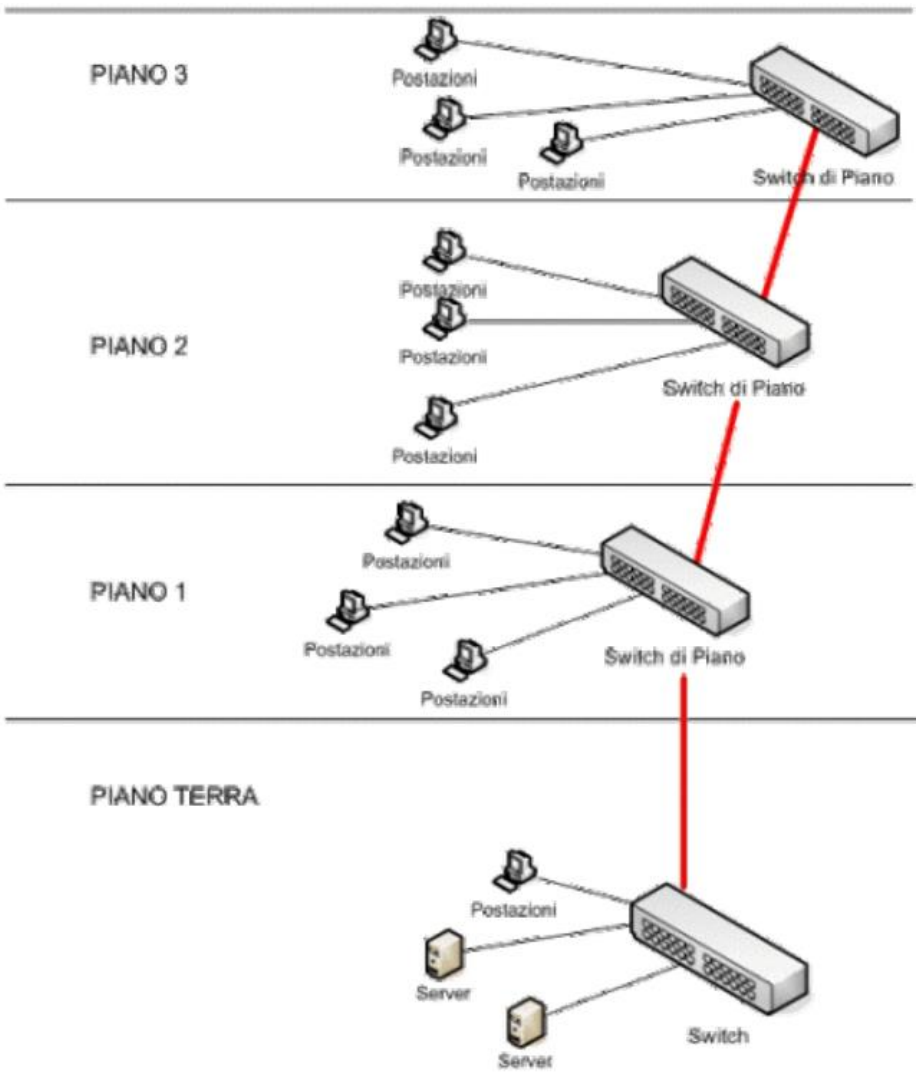
sullo stesso rack). Allo stesso modo (essendo il cablaggio di tipo strutturato), tramite un cavo telefonico a 4 fili (RJ11) è possibile collegare un telefono alla presa a muro più vicina e sul patch panel, collegando la relativa porta (tramite un altro cavo a 4 fili) al centralino telefonico anziché allo switch di rete.
Di solito sono utilizzati cavi patch di colore diverso a seconda se il tratto è telefonico o di rete.

2) Rete estesa su più piani – Nel caso l'edificio si estenda su più piani, i cavi delle prese dei vari uffici arrivano al "path panel di piano" dove, nello stesso rack, è presente uno "switch di piano". Ogni "switch di piano" ha una connessione con uno switch centrale (centro stella) posizionato in una posizione strategica (solitamente nella sala Server), realizzata mediante collegamenti in fibra ottica (figura seguente).



Nella figura che segue è mostrato un collegamento in cascata di più switch, fattibile ma sconsigliato perchè nel caso di guasto di solo switch la comunicazione verrebbe interrotta.

D. Tomassini, L. Borzetta © Copyright Ulrico Hoepli Editore Spa



Preparazione sala server

Innanzitutto occorre scegliere il Rack più idoneo alle esigenze in termini di spazio, compatibilità dei server ed espansibilità futura.

Gli armadi Rack non sono tutti uguali: esistono modelli standard e marche specifiche (ad esempio Rack IBM, Rack HP ecc.).

I parametri da tener presente per l'acquisto di un rack sono i seguenti:

- profondità dei server da installare;
- larghezza dei server;
- unità disponibili.

Per i server è consigliato un Rack da pavimento, per i patch panel di piano di solito sono sufficienti mini-rack installabili a parete.

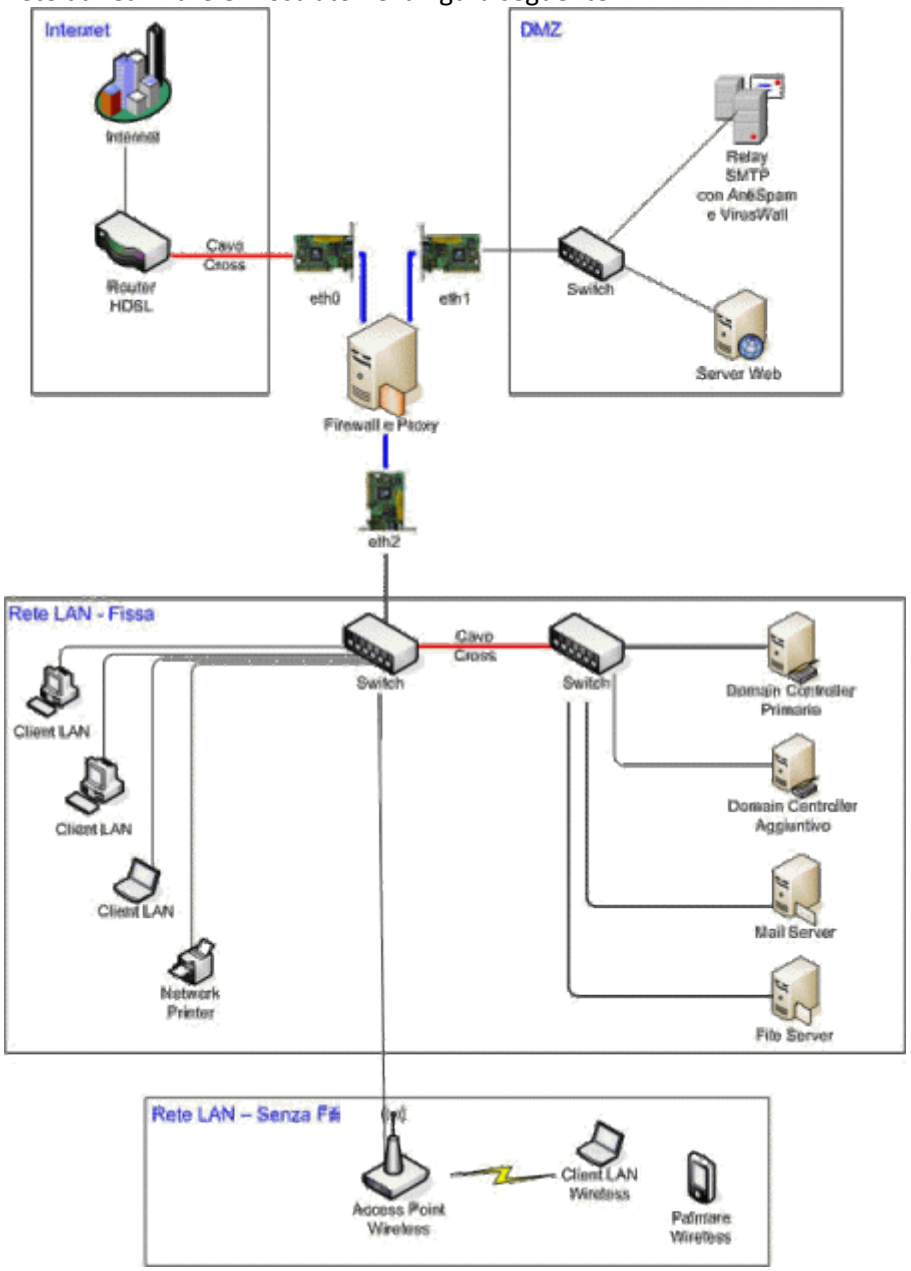
La sala server deve essere dotata di un sistema di raffreddamento adeguato, in grado di garantire una temperatura costante compresa tra 10 °C e 28 °C: il valore ottimale è 19÷20 °C.

Al riguardo è opportuno rivolgersi ad un installatore specializzato che stabilirà il totale dei KW o dei BTU che vengono "sprigionati" dai server: sommando i consumi in Watt degli apparati presenti in sala server (monitor, server, unità esterne, ecc.) possono essere determinati i BTU sono necessari (si ricorda che 1 kW/h equivale a 3412 BTU).

D. Tomassini, L. Borzetta © Copyright Ulrico Hoepli Editore Spa

Schema della rete

Lo schema della rete da realizzare è mostrato nella figura seguente.



Nella sala server sono installati i seguenti server:

- il **Primary Domain Controller** (PDC), server che in una LAN Windows gestisce il dominio sul quale viene eseguita la Active Directory;
- il **Backup Domain Controller** (BDC), sistema di backup che conserva una copia a sola lettura del PDC, allo scopo di superare eventuali guasti di quest'ultimo.
- il **Mail server,** dove risiede il software che gestisce la ricezione e lo smistamento da un computer all'altro dei messaggi di posta elettronica;
- il **File server**, macchina progettata per fornire agli utilizzatori della LAN un adeguato spazio su disco (singolo o composto da più dischi) nel quale sia possibile memorizzare, leggere, modificare, creare file e cartelle centralizzate, condivise da tutti oppure accessibili secondo regole o autorizzazioni generalmente assegnate dal gestore della rete. Tale macchina può essere un Network Attached Storage (NAS), cioè un apparecchio specificatamente studiato e costruito per tale scopo;
- il **Firewall**, che consente di filtrare ed eventualmente bloccare il traffico anomalo da e verso qualsiasi rete; il firewall agisce come una dogana che controlla il traffico proveniente dall'interno e

D. Tomassini, L. Borzetta © Copyright Ulrico Hoepli Editore Spa

dall'esterno di una rete, lasciando passare soltanto quello che rispetta regole definite; per motivi di sicurezza il firewall viene ospitato in un'apposita macchina dotata di tre schede di rete, eth0, eth1 e eth2, mediante le quali interfaccia il router, la DMZ e la LAN;

- il **router**, che collega la LAN ad Internet, il quale è fornito dall'ISP in comodato d'uso (noleggio);
- la **DMZ**, (DMZ-DeMilitarized Zone - zona demilitarizzata), ovvero la zona isolata che ospita le applicazioni a disposizione del pubblico, utilizzata per consentire ai server in essa ospitati di fornire servizi all'esterno senza compromettere la sicurezza della rete aziendale interna: per le connessioni esterne la DMZ appare infatti una sorta di "**vicolo cieco**". La politica di sicurezza attuata sulla DMZ è la seguente:
  - traffico esterno verso la DMZ **autorizzato**;
  - traffico esterno verso la rete interna **vietato**;
  - traffico della rete interna verso la DMZ **autorizzato**;
  - traffico della rete interna verso l'esterno **autorizzato**;
  - traffico della DMZ verso la rete interna **vietato**;
  - traffico della DMZ verso la rete esterna **vietato**.

  La DMZ contiene gli elementi di seguito indicati.
  - Il **Web server**, macchina contenente un insieme di applicazioni software, accessibile da parte dei client, che interpreta il linguaggio html (browser) utilizzando il protocollo di comunicazione HTTP;
  - Il **relay SMTP**, server SMTP dove vengono utilizzati software di protezione per il traffico in/out (non solo email), ovvero:
    - Antispam (SpamAssassin, DSPAM);
    - Antivirus (ClamAV, OpenAntivirus).
  - Uno **switch** a 8 porte al quale sono connessi il web service e il relay SMTP.

Piano di indirizzamento IP

A questo punto è necessario scegliere gli indirizzi IP da utilizzare.
Il seguente è un piano di indirizzamento IP composto da 4 sottoreti:

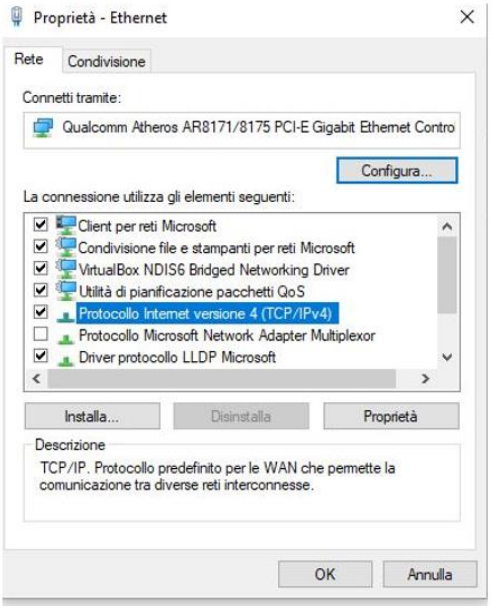
- sala server: 192.168.0.0/24 (host da 192.168.0.2 a 192.168.0.254);
- Piano 1: 192.168.1.0/24 (host da 192.168.1.2 a 192.168.1.254);
- Piano 2: 192.168.2.0/24 (host da 192.168.2.2 a 192.168.2.254);
- Piano 3: 192.168.3.0/24 (host da 192.168.3.2 a 192.168.3.254):

Gli indirizzi che terminano con .1 (es. 192.168.1.1) sono utilizzati per le interfacce del router, i .255 sono gli indirizzi di broadcast di ciascuna sottorete, non utilizzabili per essere assegnati agli host.
Queste 4 sottoreti non comunicano tra loro e quindi occorre un router per metterle in comunicazione.
La separazione è realizzata per piano, in modo tale che il traffico di broadcast di una sottorete non si diffonda anche alla altre (così facendo si hanno maggiori performance).

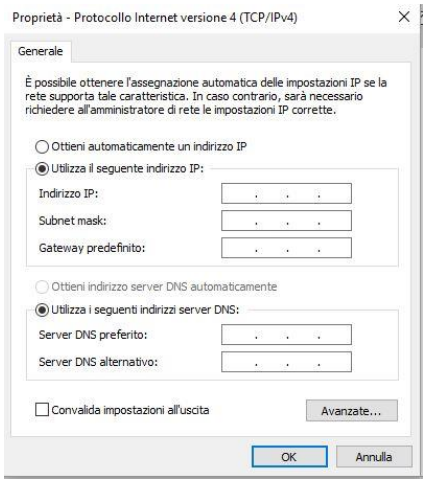
Configurazione degli indirizzi IP

Per ogni host, si seleziona "Pannello di controllo" → "Rete ed Internet"→"Connessioni di rete".
Cliccando con il tasto destro sull'icona che rappresenta la scheda di rete del PC e selezionando la voce "P**roprietà"**, compare la finestra che segue.

D. Tomassini, L. Borzetta © Copyright Ulrico Hoepli Editore Spa



Si seleziona poi “Protocollo Internet versione 4 (TCP/IPv4)”e quindi “Proprietà” (finestra seguente).



In tale finestra è specificata la configurazione della scheda di rete nella quale occorre impostare i seguenti valori (per il PC1):

- Indirizzo IP
- Subnetmask
- Gateway predefinito.

L’indirizzo IP del gateway coincide con quello del router: in questo modo tutti i pacchetti diretti a destinatari non appartenenti alla rete vengono inviati al router che provvede al loro instradamento.
Occorre infine configurare le impostazioni del DNS; al riguardo si utilizzano i seguenti indirizzi:

- Server DNS preferito: 192.168.3.230/24 (PDC); essendo i client in un dominio, come DNS preferito viene utilizzato il PDC; in questo modo i client si collegano al PDC, il quale, in base alle policy impostate, risolve i DNS dei client consentendo loro di navigare.
- Server DNS alternativo: 192.168.3.231/24; il DNS alternativo è facoltativo ed è consigliabile impostarlo con la stessa configurazione del BDC.

Per completare la configurazione della LAN si procede allo stesso modo per tutti gli altri PC e server.

D. Tomassini, L. Borzetta © Copyright Ulrico Hoepli Editore Spa

Preparazione del Dominio Active Directory e DNS

Occorre ora preparare il Controller Primario di Dominio (PDC) e quindi di Active Directory, avente nome DC1.

Installato Windows Server si esegue il comando DCPROMO da Start/Esegui per far partire la procedura guidata che consentirà al server di diventare un controller di dominio.

I parametri essenziali da configurare in questo passaggio sono il nome del dominio (aziendaspa.it) e il nome netbios (AZIENDASPA), avente la funzione di autenticare i vecchi client NT4, Win95, W3.11 e Win98.

Si procede poi alla configurazione del servizio DNS Server sullo stesso server, creando al riguardo una nuova zona primaria (diretta) integrata in AD con nome aziendaspa.it e successivamente una zona di ricerca inversa con gli IP della rete.

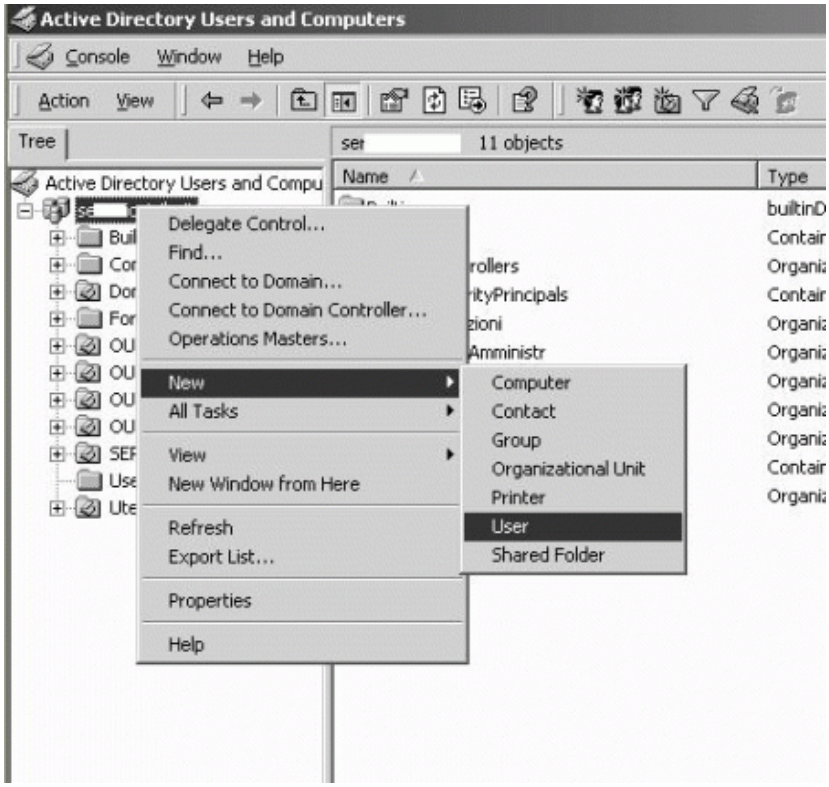
La zona diretta consente ai client di risolvere i nomi degli host nel corrispondente indirizzo IP, mentre la zona inversa, dato un IP, restituisce il nome dell'host.

Occorre creare una zona per ogni sottorete, ad esempio la zona 192.168.0 la 192.168.1 e così via. Per definire la zona inversa sono utilizzati solo gli ottetti che indicano il network.

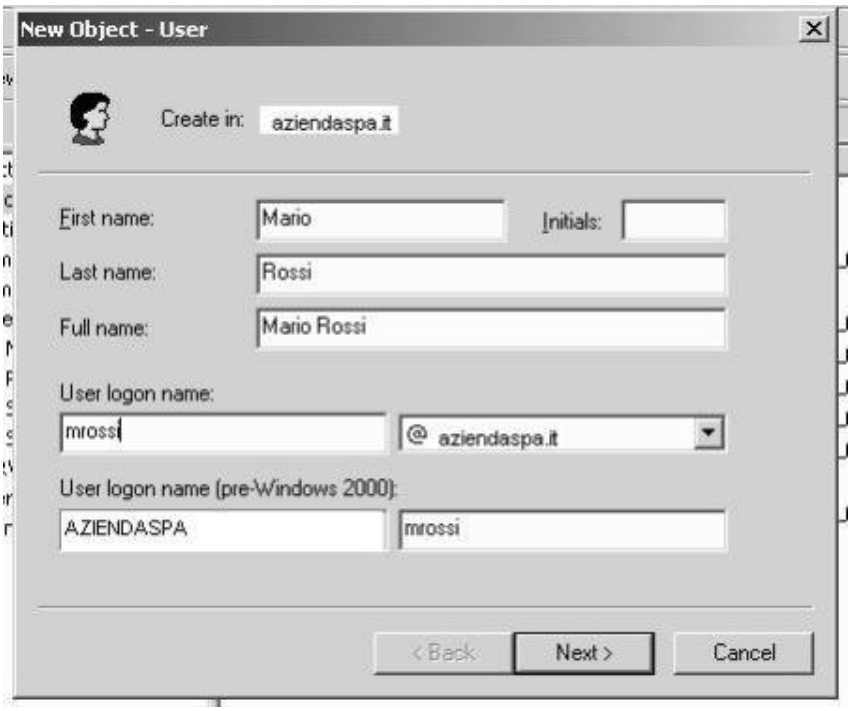
Creazione degli utenti

A questo punto occorre definire uno standard per la creazione delle login ed una politica delle password rigida. Le login (o UserName) possono essere create con l'iniziale del nome ed il cognome per esteso, ad esempio la login di Mario Rossi sarà mrossi e la password deve essere formata da almeno 8 caratteri che contengano numeri e lettere.

Per creare gli utenti occorre aprire "Utenti e Computer di Active Directory" nel menù "Strumenti di Amministrazione" sul server Doman Controller (DC1).



D. Tomassini, L. Borzetta © Copyright Ulrico Hoepli Editore Spa



Occorre inserisce una password provvisoria (ad esempio mariorossi12345) cliccando poi su "L'utente deve cambiare password al prossimo logon" in modo che il signor Mario Rossi venga istruito ad entrare nel suo PC come mrossi con password mariorossi12345; la prima volta viene richiesto di modificare la password a suo piacimento.

Collegamento degli utenti

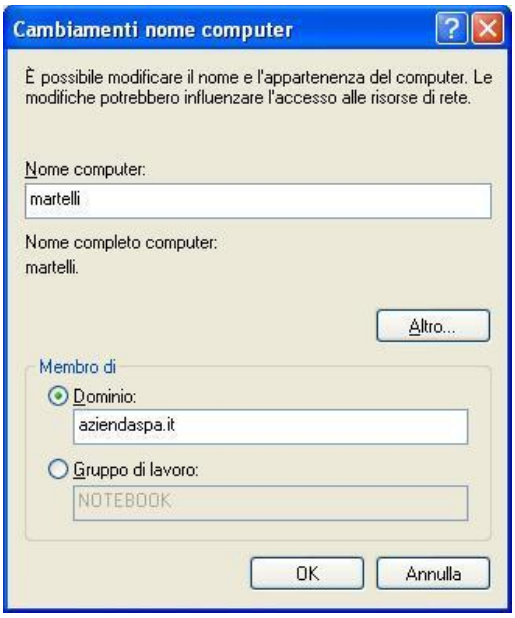
A questo punto si può iniziare a collegare i client in rete.
Dopo averli posizionati nelle stanze, si collega un cavo "dritto" dalla scheda di rete del singolo PC al punto rete sul muro, e successivamente sul rack, dove si trova lo switch, si collega un altro cavo dalla porta del patch panel (che corrisponde alla presa a muro di quella stanza) ad una porta libera dello switch.

Aggiunta (Join) dei client al dominio

Un dominio Windows è un "contesto di sicurezza" dove "girano" i client (e i server).
Tutti gli host che appartengono ad un dominio possono essere controllati centralmente attraverso le impostazioni gestite sul domain controller attraverso le Group Policy, gruppi di utenti, permessi NTFS.

D. Tomassini, L. Borzetta © Copyright Ulrico Hoepli Editore Spa

Dal domain controller è possibile impostare qualsiasi configurazione sui client che ne fanno parte, e che hanno pertanto fatto i 'Joint al Dominio').
Per Join al dominio si intende l'inserimento di un client al dominio (aziendaspa.it).
Per aggiungere un client nel dominio è necessario entrare come "Administrator Locale" della macchina e cliccare con il tasto destro su Risorse del Computer → Nome Computer → Cambia: si cambia quindi la configurazione da "Gruppo di lavoro" a "Dominio" specificando il nome (aziendaspa.it).



A questo punto occorre inserire una login e password dell'amministratore del dominio (che è l'utente Administrator creato sul server Domain Controller) che ha il permesso di "Aggiungere client nel dominio".
Si riavvia il client, si entra in rete con il nome dell'utente (ad esempio mrossi) e la sua password e si seleziona dalla lista il dominio prescelto (aziendaspa).

CONCLUSIONI

Sul domain controller è possibile configurare tutte le impostazioni di restrizione e configurazioni che si vogliono ed applicarle a tutti i computer che fanno parte di quel dominio senza agire sul singolo client.

Suggerimenti di possibili percorsi alternativi per nuovi elaborati

- Realizzazione di una rete peer-to peer.
- Sicurezza in rete.

D. Tomassini, L. Borzetta © Copyright Ulrico Hoepli Editore Spa