Installare Windows 2000 server

Riccardo Aliani & Roberto Bisceglia

Progetto di rete

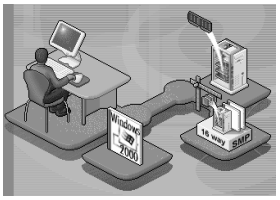
- In base al numero di client collegati e ai servizi offerti, si dovrà decidere se installare uno o due server
- Prevedendo un solo server, sarà necessario effettuare backup frequenti e pianificare procedure di ripristino rapido in caso di arresto improvviso
- Con due server, la ridondanza dei servizi consente di evitare blocchi al funzionamento della rete anche in caso di guasto ad uno dei server.

Perché Windows 2000 server

- Naturale evoluzione del progetto NT (iniziato negli anni '90 e ormai in fase di pensionamento), W2K riesce ad unire una potenza elevata ad un'estrema semplicità, derivante dall'uso dell'interfaccia dei sistemi Windows
- Disponibile in tre versioni:
  1. STANDARD SERVER
  2. ADVANCED SERVER
  3. DATACENTER SERVER

Cosa garantisce W2K

- Robustezza
- Scalabilità
- Alta affidabilità
- Sicurezza
- Capacità di Networking
- Riduzione costi di gestione



La Robustezza di W2K

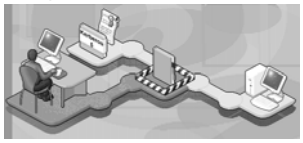
- Protezione della memoria
- File system migliorato (NTFS5)
- Diminuzione del numero di riavvii
- Protezione automatica del sistema (Windows File Protection)

La Scalabilità di W2K

- Supporto per sistemi sempre più potenti
  - 16/32 processori
  - 64 GB di RAM
- Supporto per più macchine collegate tra loro in "cluster"

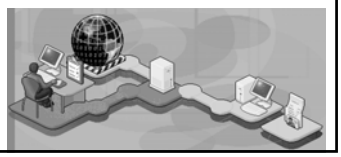
La Sicurezza di W2K

- Windows 2000 introduce un nuovo metodo per la gestione della sicurezza dei dati circolanti in rete.
- Vengono supportati tutti gli standard Internet relativi alle chiavi pubbliche / private.
- È possibile crittografare i dati su disco (EFS).



Il Networking con W2K

- Gestione semplificata delle connessioni
- Supporto migliorato per l'accesso remoto (RAS)
  - Virtual Private Networking (VPN)
  - Policy
- Connessioni ad Internet condivise
  - NAT

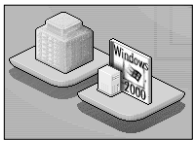


Riduzione dei costi di gestione

- L'amministrazione della rete diventa più agevole e veloce grazie ad una serie di strumenti innovativi:
  - Active Directory
  - Group Policy
  - IntelliMirror
  - Installazione e gestione remota del software
  - Microsoft Management Console

W2K versione STANDARD

- Pacchetto BASE ma già con tutti i requisiti per un'installazione completa in una piccola realtà
- È probabilmente la versione più equilibrata per un ambiente scolastico
- Supporta server multiprocessore (fino a 4 CPU) e 4 GB di memoria RAM.

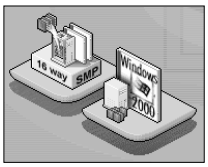


W2K versione ADVANCED

- Pacchetto destinato a reti di media dimensione con applicazioni critiche e con cospicue esigenze
- Supporta server multiprocessore (fino a 8 CPU) e 8 GB di memoria RAM.
- Gestisce il Network Load Balancing.

W2K versione DATACENTER

- Studiato per le applicazioni di portata aziendale
  - Supporta da 16 fino a 32 processori.
  - Supporta 64 GB di RAM.
- Massima affidabilità e continuità di servizio.
  - Cluster a 4 nodi con "cascading failover".
  - Network Load Balancing
- Richiede hardware certificato



Procedure di installazione

- **Munirsi di carta e penna e annotare tutti i parametri inseriti nell'iter**
- **Nel caso sia presente un controller RAID, creare da BIOS due unità logiche RAID 5 (una per il sistema da circa 4 GB e una per i dati)**
- **Ecco i vari passi:**

1. ***Boot da CD/floppy.***
2. ***Partizionamento HD.***
3. ***Scelta File system e formattazione HD.***

Boot e partizionamento

- **Usando il 1° CD (è preferibile ai floppy), si avvia la fase di setup.**
- **Eliminare eventuali partizioni presenti (escluso controller RAID) e crearne una per il sistema da almeno 4 GB e una col restante spazio per i dati**

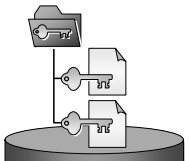
Eliminazione di ogni partizione esistente per ottenere più spazio

Creazione di una nuova partizione su una zona di HD non ancora partizionata

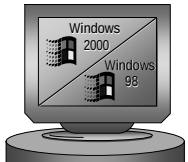
La scelta del File System

- **È il metodo col quale i sistemi operativi memorizzano i dati sulle memorie di massa (hard disk, CD, floppy, ecc.)**
- **La scelta è tra FAT (tradizionale) e NTFS (innovativa)**
- **Scegliere NTFS: garantisce prestazioni e sicurezza di alto livello in una rete di computer**

Perché scegliere NTFS



- **Sicurezza a livello di file e cartelle**
- **Compressione file**
- **Quote disco**
- **Criptazione file**



- **Supporto Dual Boot per più sistemi operativi**
- **Nessuna sicurezza a livello di file e cartelle**

I passi successivi

1. ***Configurazione TCP/IP e assegnazione di nomi e indirizzi IP statici.***
2. ***Scelta del tipo di licenza.***
3. ***Installazione DNS (fondamentale).***
4. ***Installazione DHCP e WINS (utile).***
5. ***Applicazione dell'ultimo Service Pack disponibile.***
6. ***Promozione a Domain Controller.***

Il Protocollo TCP/IP

Il protocollo TCP/IP è alla base di Active Directory e di tutti i servizi forniti dal server W2K.

In caso di reti con un numero ridotto di nodi è possibile un semplice indirizzamento, assegnando ad esempio, gli indirizzi privati:

- **Da 192.168.0.1 a 192.168.0.20 ai server**
- **Da 192.168.0.21 a 192.168.0.40 alle stampanti di rete**
- **Da 192.168.0.41 a 192.168.0.50 alle altre apparecchiature di rete (router, ecc.)**
- **Da 192.168.0.51 a 192.168.0.254 ai client**
- **Si utilizzerà la subnet mask 255.255.255.0.**

Configurare il TCP/IP

- Il nostro dominio si chiamerà NomeIstituto.local, i server ServerX (X= 1,2,3,…)
- Oltre all'indirizzo IP del server (192.168.0.1), indicheremo anche:
- L'indirizzo del DNS server (lo stesso del server).
- L'indirizzo del default gateway (se esiste un router sulla rete).

Il tipo di licenza

- Per server: con un solo server, si dovranno acquistare tante licenze client per le connessioni contemporanee (con due server, andranno raddoppiate)
- Per seat (posto di lavoro): ogni client dovrà avere la sua licenza, indipendentemente dal numero dei server presenti.

I servizi di base: DNS

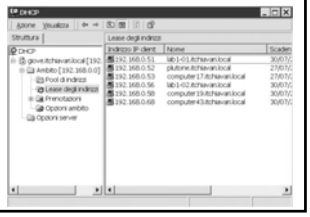
- DNS (Domain Name System) è un servizio alla base di Active Directory
- Il suo compito è di risolvere i nomi di dominio esteso (es. NomeIstituto.local) in indirizzi IP (es. 192.168.0.1) o viceversa
- Se si prevedono due server, il servizio dovrà essere configurato come Active Directory Integrated (sempre disponibile anche in caso di blocco di uno di essi)

I servizi di base: DHCP

- DHCP (Dynamic Host Configuration Protocol) permette di assegnare ai client in automatico un indirizzo IP.
- Questo evita sovrapposizioni di indirizzi involontarie, possibili in fase d'installazione.
- L'assegnazione automatica rimane valida (lease) per un tempo impostabile.
- In caso di due server DHCP, il secondo server sopperisce ad una eventuale indisponibilità del primo.

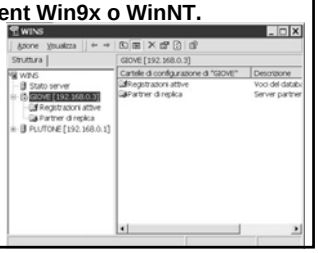
I servizi di base: DHCP

- Nel DHCP va configurato l'ambito di indirizzi (scope), entro il quale verranno assegnati gli indirizzi IP dei client
- Ne''ambito si dovranno inserire anche gli indirizzi del server DNS, WINS e del default gateway (router)
- Questo permetterà ai client di conoscere in automatico tutte le informazioni di rete necessarie al loro funzionamento



I servizi di base: WINS

- WINS (Windows Internet Name Service) era molto utilizzato su WinNT; in W2K viene completamente soppiantato dal servizio DNS.
- È quasi obbligatorio installarlo, nel caso esistano in rete client Win9x o WinNT.
- Non richiede settaggi particolari.
- In caso di due server, impostarli come *partner push pull* uno dell'altro.



I service pack e le patch

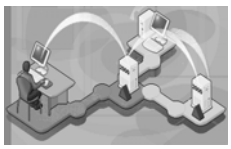
- **Permettono di aggiornare il sistema con le ultime modifiche rilasciate da Microsoft.**
- **Sono fondamentali per garantire la funzionalità e la stabilità del sistema.**
- **Sono scaricabili da Internet.**

Promozione a domain controller

- **Con la promozione a Domain Controller viene installato il servizio di Active Directory, l'organizzatore di tutte le attività della rete.**
- **Il computer che lo ospita può anche svolgere altre funzioni server, ad esempio quella di file server o di application server.**
- ***E' importanteè che il server DC svolga solo il suo compito e non sia utilizzato come una postazione di lavoro.***

Promozione a domain controller

- **W2K permette di avere un modello multimaster, cioè più server come domain controller.**
- **I vari DC si scambiano reciprocamente ed automaticamente le modifiche ad Active Directory.**
- ***La presenza di più DC è consigliata per sopperire ad eventuali guasti con inevitabile blocco della rete.***



Cos'è Active Directory

- **È un servizio installato sui Domain Controller che definisce l'organizzazione della rete.**
- **L'organizzazione avviene in base ad oggetti:**
  - ✓ **i computer**
  - ✓ **gli utenti (user)**
  - ✓ **i gruppi (group) → insiemi di user**
- **Gli oggetti sono organizzati all'interno di:**
  - ✓ **Domini (Domain)**
  - ✓ **Unità Organizzative (OU: Organizational Unit)**

Il lato logico di AD: l'Oggetto

- **È l'elemento base e permette di identificare gli utenti e le risorse della rete**
- **Ogni oggetto ha un nome e degli attributi**
- **Un oggetto può rappresentare:**
  - **Utenti**
  - **Gruppi**
  - **Contatti**
  - **Unità disco condivise**
  - **Stampanti condivise**
  - **Computer**

User Account = Oggetto	
Name	Attributi
Title	
Manager	
Office Location	
Phone	
Division	
Cost Center Code	
…	

Strutture logiche di AD

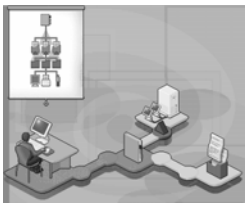
- **Domini: gruppo di computer che condividono il database di directory.**
- **Strutture di dominio (Alberi): uno o più domini con condivisione di nomi di spazio vicini.**
- **Insieme di s. di dominio (Foreste): una o più strutture di dominio che condividono informazioni di directory comuni.**
- **Unità Organizzative (UO): sottogruppi di domini che riflettono la struttura organizzativa.**

Strutture fisiche di AD

- **Subnet: gruppo della rete con intervallo di indirizzi IP specifico e maschera di sottorete.**
- **Siti: organizzazione di una o più subnet, utilizzati per l'accesso a directory o per le configurazione di replica.**

Le Unità Organizzative

- **Consentono di costruire una gerarchia di "contenitori" all'interno dei quali è possibile raggruppare gli oggetti della rete**
- **Delimitano il raggio d'azione delle policy**
- **Permettono la delega amministrativa**
- **Possono contenere sottounità**

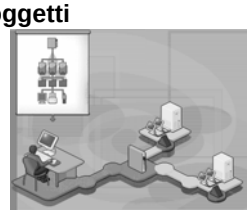


Le Unità Organizzative

- **Se è quasi scontato che in una scuola ci sarà un solo dominio (anche perché più domini imporrebbero più server), possiamo organizzare logicamente la rete in più UO.**
- **Almeno una UO deve sempre esistere.**
- **Ogni UO può contenere vari oggetti (user, group, computer).**
- **Possiamo creare anche sottounità.**
- **L'amministrazione dell'UO può essere delegata ad un utente o ad un gruppo.**

Domini

- **Costituisce il nucleo di base per l'amministrazione, la gestione della sicurezza e delle policy**
- **E' una struttura logica all'interno della quale definire UO ed oggetti**
- **I DC del dominio si scambiamo le informazioni di AD (replica multimaster)**
- **Ogni dominio richiede almeno un pc DC**



Domini

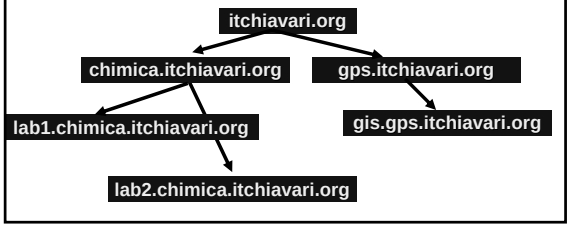
Gruppo di computer che condivide un database di directory; ad esso è assegnato un nome DNS.

I nomi di dominio devono essere univoci, ad es. non possono esistere due domini itchiavari.org, ma possono esistere domini "child" derivati dal dominio "parent":

- **chimica.itchiavari.org,**
- **gps.itchiavari.org,**
- **segreteria.itchiavari.org.**

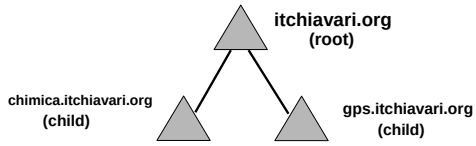
Strutture di dominio

- **Uno o più domini che condividono gli stessi dati di directory costituiscono una struttura di dominio, che appare come un *albero rovesciato.***



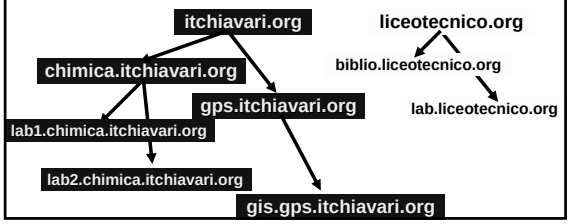
L'Albero

- **L'albero consente di:**
  - **decentralizzare l'amministrazione**
  - **avere politiche di sicurezza differenziate**
  - **mantenere la stessa radice del nome DNS**
  - **avere accesso (previa autorizzazione) a tutte le risorse disponibili sui tre domini**



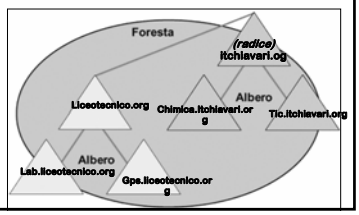
Insieme di strutture

Se la denominazione di struttura non è contigua, si costituisce un insieme di strutture (foresta), tra le quali si instaurano relazioni di fiducia.



La Foresta

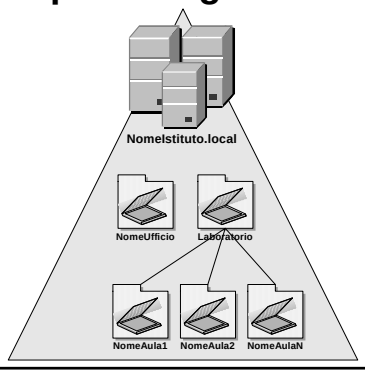
- **Costituisce il più alto livello di aggregazione tra Domini e Alberi**
- **Domini e Alberi della Foresta appartengono a nomi DNS differenti**
- **Ogni Albero della Foresta ha una sua Radice (root), la prima Radice creata è la Radice della Foresta**



Le Unità Organizzative

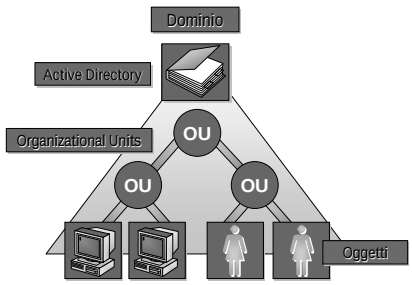
- **Nella nostra rete d'Istituto, potrà essere utile creare una UO per ogni ufficio d'amministrazione.**
- **Per i laboratori, possiamo creare una UO generale e tante sottounità, una per ogni aula di laboratorio.**

Esempio di organizzazione



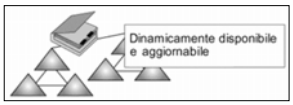
La struttura logica di AD

Oggetti, Organizational Unit, Domini



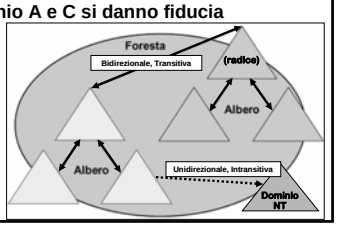
Lo Schema

- Lo Schema rappresenta quella parte di informazioni di AD condivise in una Foresta, indipendentemente dal numero di Domini e Alberi che la formano
- Questo ci garantisce che tutti gli oggetti creati sottostanno alle stesse regole. Le modifiche fatte allo Schema vengono replicate tra tutti i Controllori di Dominio della Foresta indipendentemente dal Dominio di appartenenza.

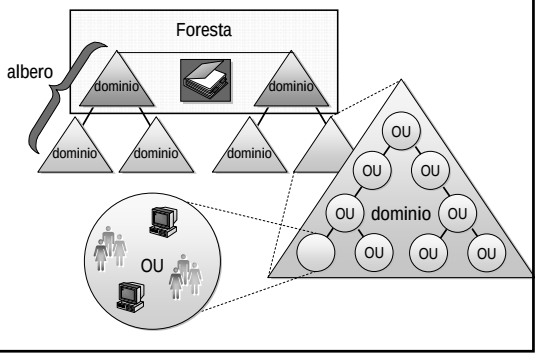


Il lato logico di AD: le relazioni di fiducia (Trust Relationship)

- In AD, la fiducia che si concedono I domini è bidirezionale e transitiva:
  - bidirezionale: se il Dominio A dà fiducia al Dominio B, quest'ultimo rende la fiducia al Dominio A
  - transitiva: se il Dominio B dà a sua volta fiducia al Dominio C, il Dominio A e C si danno fiducia
- In NT, la fiducia era unidirezionale e intransitiva, complicando non poco l'amministrazione

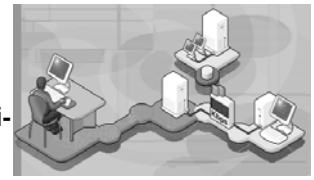


AD: struttura logica



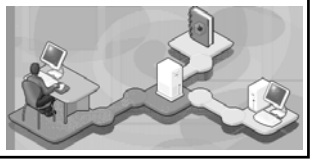
Il lato fisico di AD: il Sito

- Rappresenta il raccordo tra la struttura logica di AD e la rete fisica che la ospita
- Permette di definire una o più "sottoreti" all'interno della quale esistono collegamenti ad alta velocità
- Delimita il contesto di replica tra i vari Domain Controller, ottimizzandone il traffico



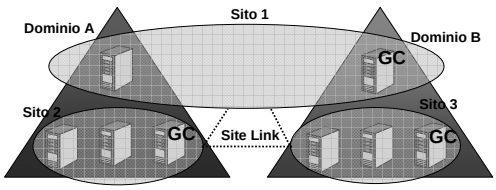
Il lato fisico di AD: Global Catalog

- Contiene un sottoinsieme delle informazioni di AD presenti nel Dominio/Albero/Foresta
- È consigliato un GC per ogni Sito, per evitare che ogni richiesta di un client (es. logon) interessi i DC dei vari Domini
- Risiede su server designati, che rispondono per informazioni presenti in strutture diverse



La struttura fisica di AD

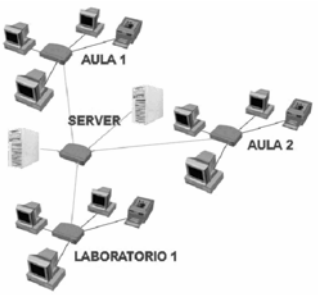
Siti e Global Catalog



- La struttura fisica è indipendente dalla struttura logica
- I siti definiscono la topologia di replica dell'Active Directory
- Il traffico di replica è ottimizzabile con il Global Catalog

Una situazione tipo in una scuola

- Un solo dominio (albero unico, foresta unica)
- Un solo segmento di rete
- Una OU per ogni aula o laboratorio
- Preferibilmente due server DC



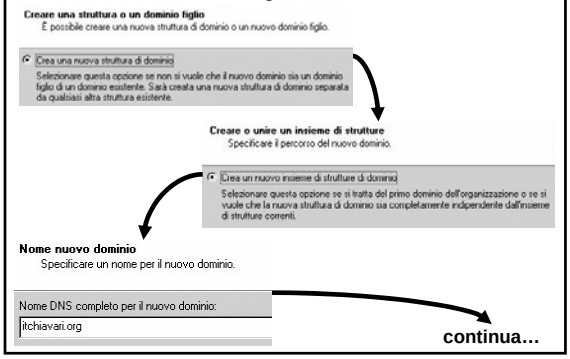
Installazione di Active Directory 1.

NB: struttura di dominio=ALBERO

insieme di strutture=FORESTA

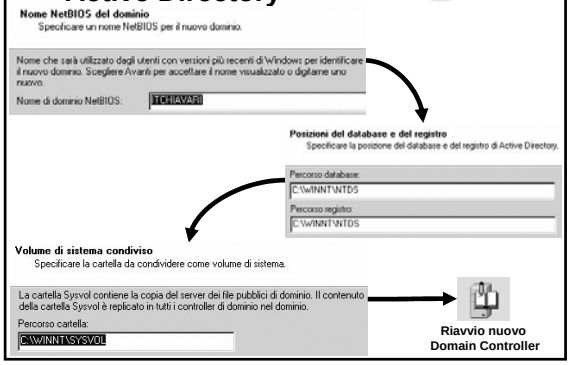
continua…

Installazione di Active Directory 2.



continua…

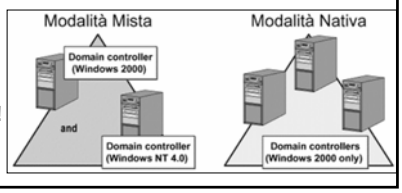
Installazione di Active Directory 3.



Riavvio nuovo Domain Controller

La modalità del Dominio

- Per facilitare la migrazione da NT a 2000, ogni dominio di AD viene creato in modalità MISTA
- Ciò permette di far convivere Domain Controller NT e 2000, ma limita le funzionalità di AD
- È consigliabile passare alla modalità NATIVA appena si sono convertiti tutti i DC
- Attenzione: il passaggio a modalità NATIVA è irreversibile!

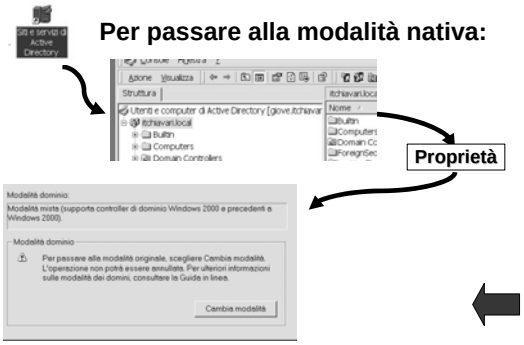


Modalità MISTA vs. Modalità NATIVA

- Modalità mista
  - Nel dominio possono essere installati BDC Windows Nt 4.0
  - L'Active Directory potrà contenere al max 40000 oggetti per le limitazioni delle dimensioni del SAM di Nt 4.0
  - Client pre-Windows 2000 non riconoscono la transitività delle relazioni di fiducia
- Modalità nativa
  - Replica multimaster
  - Nuovi tipi di gruppi:
    - Domain Local group
    - Universal group
    - Nested group
  - Supporto di client e member Server non Windows 2000
  - I client w9x necessitano di DSCLIENT.EXE

La modalità del Dominio

Per passare alla modalità nativa:



Il server è pronto

- **Installata Active Directory, il server è pronto a ricevere le richieste dei client**
- **È consigliabile testare accuratamente l'efficienza dei servizi installati**
- **Eventuali pacchetti aggiuntivi (proxy, intranet, exchange, sql, ecc.) possono essere installati tranquillamente in seguito**

Vediamo adesso come vanno configurati i client di rete.

Client Win9x

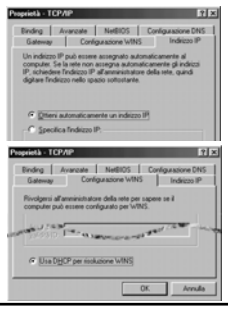
- **Dalle proprietà di Risorse di Rete:**
- **Impostare il gruppo di lavoro col nome dominio NomeIstituto**
- **Dare un nome al computer**
- **Per i nomi si può adottare la convenzione: *collocazione.xx* (con xx che va da 01 a 99)**

Client Win9x

- **Dalle proprietà di Risorse di Rete:**
- **Proprietà del Client reti Microsoft**
- **impostare l'accesso ad un dominio NT col nome dominio NomeIstituto**

Client Win9x

- **Dalle proprietà di Risorse di Rete:**
- **Proprietà del protocollo TCP/IP**
- **verificare che si ottenga automaticamente l'indirizzo IP e che si usi DHCP per risoluzione WINS**



Client Win9x

- **Dalle proprietà di Risorse di Rete:**
- **Proprietà del protocollo TCP/IP**
- **se esiste un router, aggiungere un nuovo gateway col suo indirizzo IP**

Risorse condivise

- **Tipicamente stampanti e dischi / cartelle.**
- **Determinare sempre i gruppi/utenti che possono avere accesso.**
- **L'amministratore può delegarne il controllo ad altre persone.**
- **Per i volumi condivisi, sarà opportuno impostare anche le quote disco, per evitare che alcuni utenti possano saturare lo spazio disponibile a danno degli altri utenti.**

Le quote disco

- **Permettono di limitare lo spazio occupato da ciascun utente.**
- **Sono misurate in tempo reale dal sistema per utente e per volume.**
- **Si gestiscono come proprietà del singolo volume.**
- **Il superamento di una quota genera un avvertimento.**