

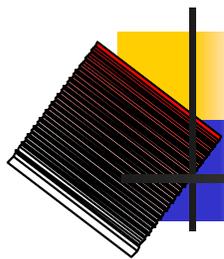
# Reti e Domini Windows 2000

---

## Corso di Amministrazione di Reti A.A. 2002/2003

Materiale preparato utilizzando dove possibile materiale AIPA

[http://www.aipa.it/attivita\[2\]/formazione\[6\]/corsi\[2\]/materiali/Reti%20di%20Calcolatori/welcome.htm](http://www.aipa.it/attivita[2]/formazione[6]/corsi[2]/materiali/Reti%20di%20Calcolatori/welcome.htm)

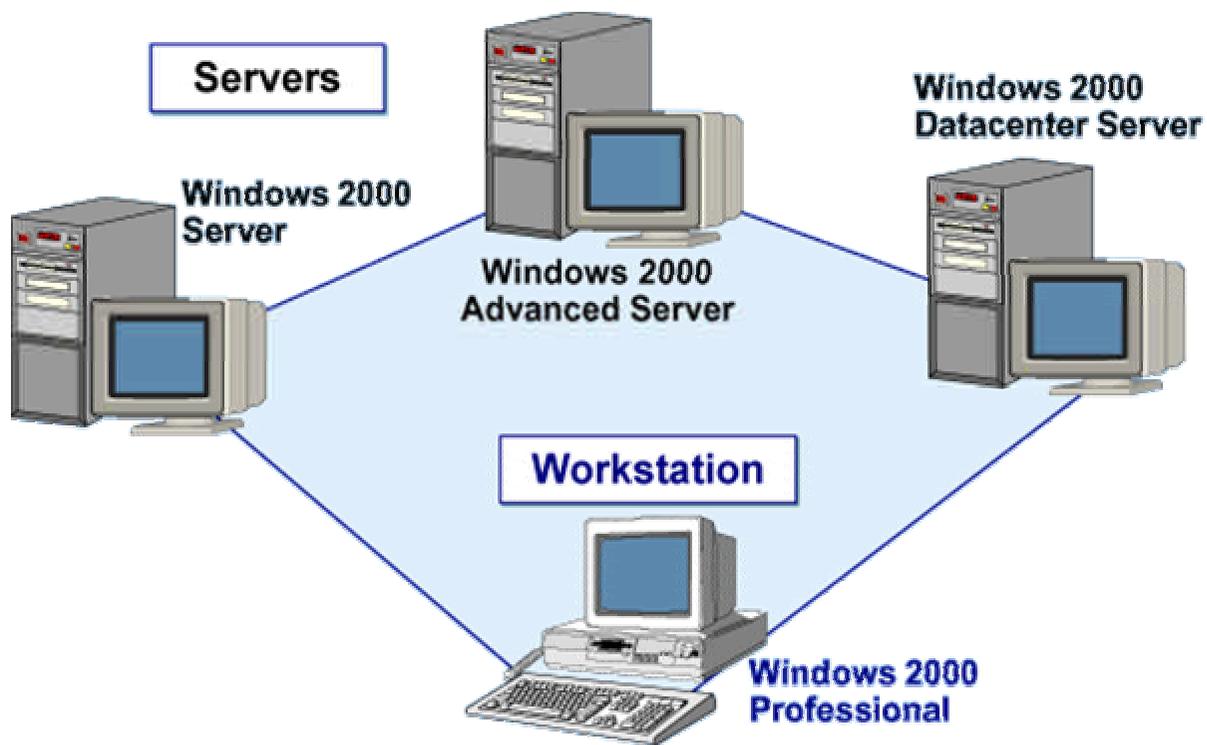


# Argomenti

---

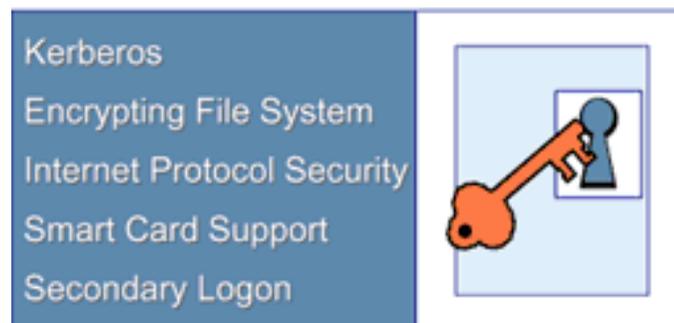
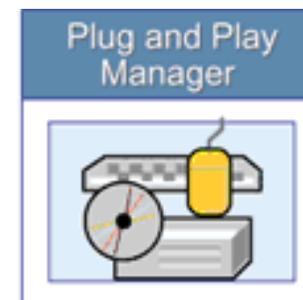
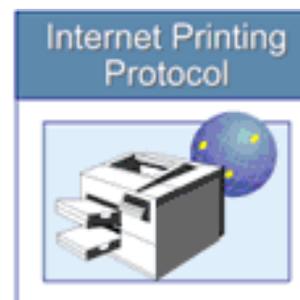
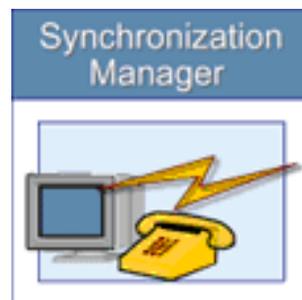
- ✎ Cenni di architettura Reti Windows 2000
  - ✎ Client e Server
  - ✎ Workgroup e Domini
- ✎ Domini Windows 2000
  - ✎ Introduzione ai Directory Services di Windows 2000
  - ✎ Active Directory
  - ✎ Supporto a protocolli standard e non proprietari
  - ✎ Spazio dei nomi
  - ✎ Active Directory e DNS

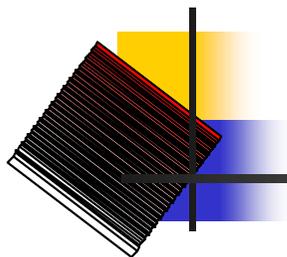
# La famiglia Microsoft Windows 2000



# Sistemi Client: Windows 2000 Professional

- ✦ **Semplicità d'Uso.** Oltre ai miglioramenti relativi all'interfaccia utente, offre il Supporto per Utenti Remoti: **Network Connection Wizard**, per configurare l'accesso remoto (connessione dial-up, connessione ad Internet, connessione VPN, connessione via cavo); Supporto per Virtual Private Network (**VPN**)
- ✦ **Gestione dei Files.** File System **NTFS**, File System **FAT32**, deframmentazione dei dischi e utility di Backup
- ✦ **Sicurezza.** Ricordiamo le seguenti funzionalità: **Kerberos 5** (protocollo standard di autenticazione), **Encrypting File System** (permette di cifrare i file memorizzati su disco), Internet Protocol Security (**IPSec**) (permette di specificare politiche di cifratura per flussi di dati sulla rete).





# Windows 2000 Server

---

- ✎ Piattaforma che offre tutte le funzionalità di Microsoft Windows 2000 Professional + le funzionalità che ne ottimizzano le performance per le funzionalità di file server, print server ed application server.
- ✎ Servizio di Active Directory: che permette di centralizzare la gestione di utenti, gruppi, sicurezza e risorse di rete.
- ✎ Buona soluzione per l'implementazione di soluzioni enterprise in realtà medio-piccole: file server, print server, web server, Terminal Services server, server di accesso remoto.
- ✎ Requisiti hardware minimi per l'installazione di Microsoft Windows 2000 Server:
  - ✎ Processor: 32-bit Pentium 133 MHz.
  - ✎ Memory: 64 MB per reti di meno di 5 computer; 128 MB è il minimo raccomandato per tutte le altre situazioni.
  - ✎ uno o più dischi con un minimo di 680 MB (raccomandati 2 GB) Sulla partizione che conterrà i file di sistema

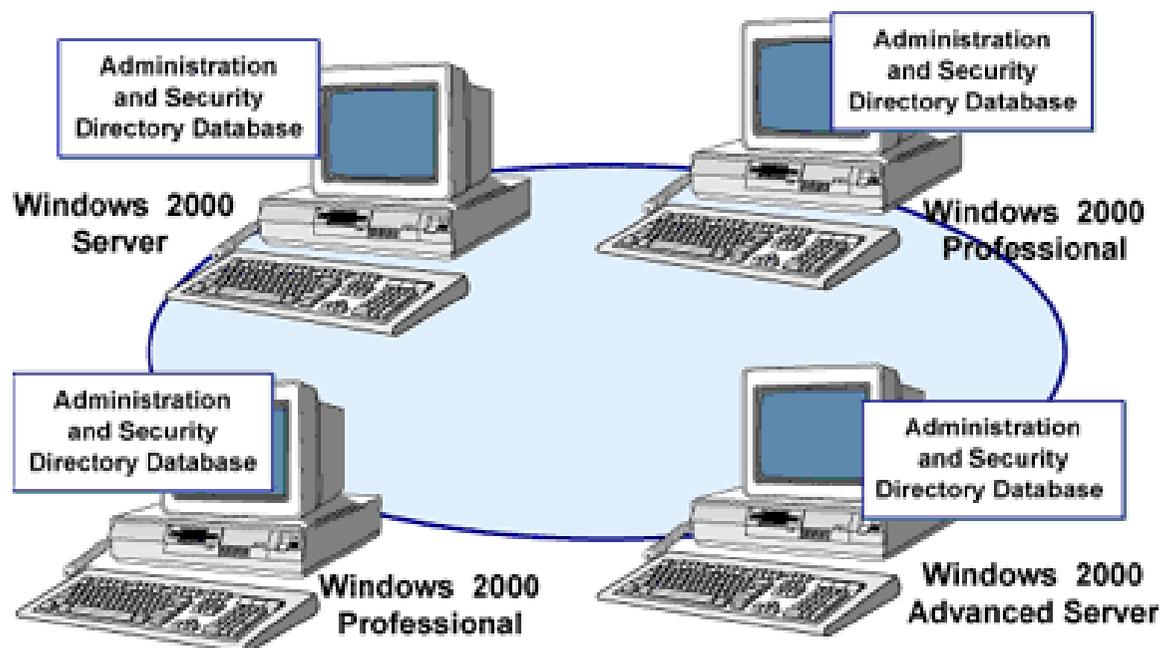
# Windows 2000 Advanced Server

- Elevata disponibilità e bilanciamento dei carichi di lavoro (**Cluster**).
- Microsoft Windows 2000 Datacenter è la soluzione server ottimizzata per data warehouse, **online transaction processing (OLTP)**, simulazioni in real-time, Web hosting. Microsoft Windows 2000 Datacenter ha tutte le caratteristiche di Microsoft Windows 2000 Advanced Server, ma supporta fino a 64 GB di memoria RAM e fino a 32 processori SMP.



# Workgroup

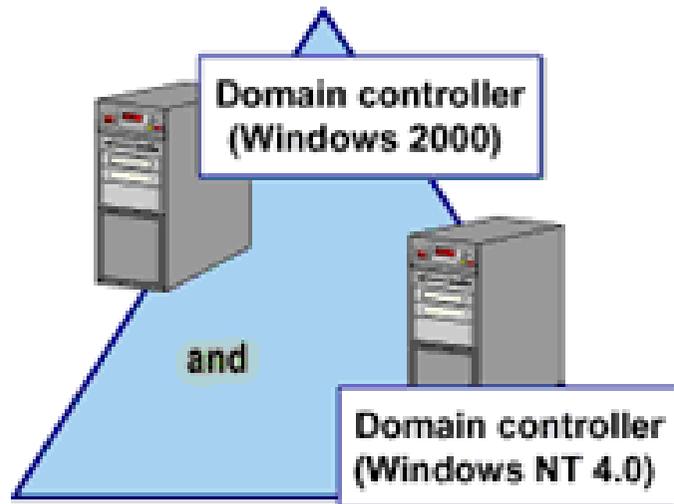
- Microsoft Windows 2000 permette di implementare **due ambienti di rete** in cui gli utenti possano condividere risorse (file, stampanti, applicazioni) indipendentemente dalle dimensioni della rete: i **workgroup** ed i **domini**.
- Un workgroup è chiamato anche rete **Peer-to-Peer** (paritetica) per evidenziare quella che è la sua caratteristica saliente: tutti i computer che appartengono ad un workgroup sono "uguali", senza che ci sia un server dedicato alla gestione della sicurezza. Ogni computer che esegua sia Microsoft Windows 2000 Professional sia Microsoft Windows 2000 Server gestisce **un proprio security database locale**, cioè una lista di utenti ed impostazioni di sicurezza inerenti il computer che ospita tale database: dunque in un workgroup la **gestione degli utenti e della sicurezza è decentralizzata**



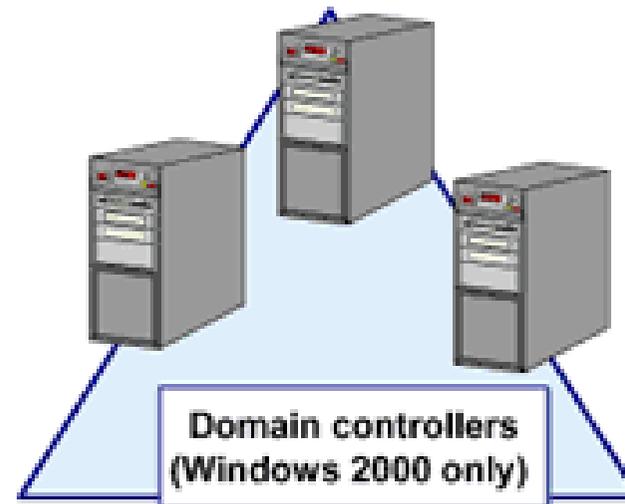
# Domini

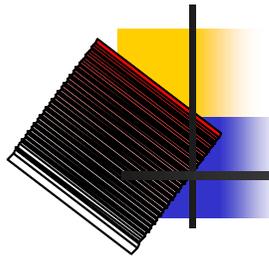
- ✎ I computer condividono un directory database centralizzato, cioè un database che contiene la definizione degli user account, dei gruppi e tutte le impostazioni inerenti la sicurezza. Tale database è chiamato "Directory" ed è una parte di Active Directory che è il directory services di Windows 2000. Tale database è contenuto su un server "particolare" denominato "**Domain Controller**".
- ✎ Vantaggi: Amministrazione Centralizzata, Accesso Universale alle Risorse, Scalabilità, One User One Account (con un unico username ed un'unica password l'utente accede al dominio da qualsiasi postazione di lavoro)

## Modalità Mista



## Modalità Nativa





# Domini Windows 2000: Active Directory

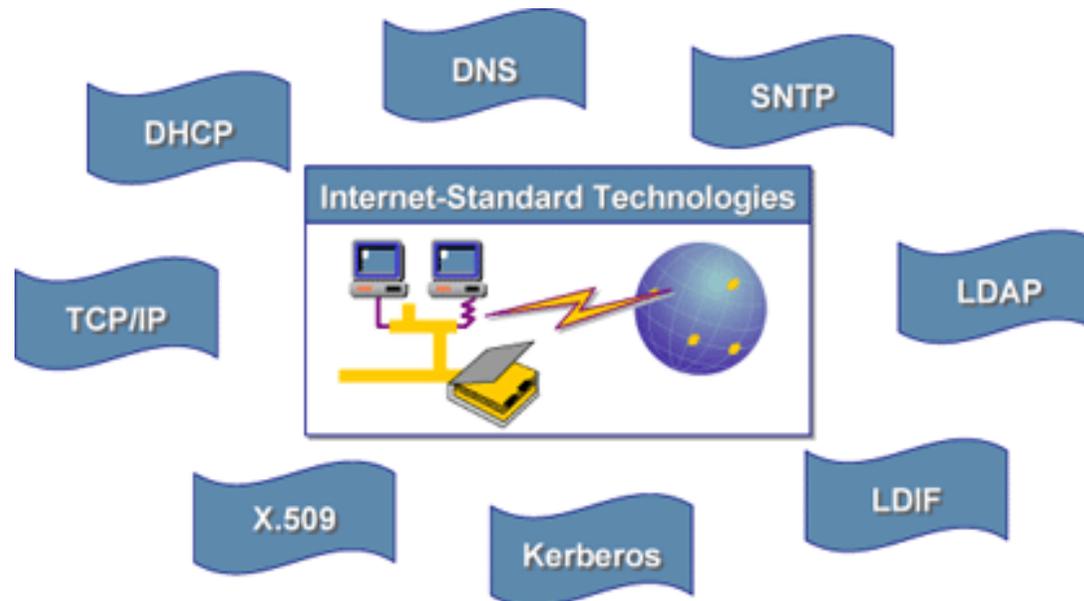
**Active Directory** è il Directory Services di Microsoft Windows 2000. Il Directory Service è un **servizio di rete** che ha lo scopo di gestire tutte le informazioni inerenti le risorse di rete per renderle accessibili agli utenti ed alle applicazioni; permette di identificare, descrivere, localizzare, accedere, gestire e rendere sicure tali risorse. Dunque Active Directory fornisce le funzionalità per **organizzare, gestire e controllare in maniera centralizzata l'accesso alle risorse di rete**, in maniera trasparente rispetto alla topologia di rete ed al protocollo utilizzato. Tramite Active Directory è possibile memorizzare ed organizzare un numero praticamente illimitato di oggetti.

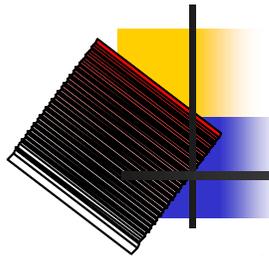


# Tecnologie Supportate

I protocolli e le tecnologie più importanti su cui Active Directory si basa:

- D**ynamic **H**ost **C**onfiguration **P**rotocol (**DHCP**): gestione centralizzata ed automatica dei parametri di indirizzamento IP;
- D**NS dynamic update protocol: creazione dinamica dei record A e PTR in una zona DNS;
- S**imple **N**etwork **T**ime **P**rotocol (**SNTP**): per la sincronizzazione dell'ora;
- L**ightweight **D**irectory **A**ccess **P**rotocol (**LDAP**): protocollo per l'accesso client al directory service;
- K**erberos **V5**: protocollo di autenticazione;
- X.509** v3 : standard per l'utilizzo di certificati digitali per la cifratura e la firma digitale;
- T**ransmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol (**TCP/IP**)





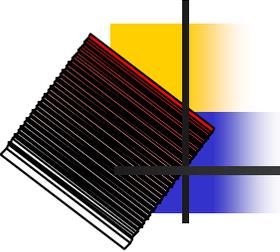
# Spazio dei nomi

- Per localizzare una risorsa, sia l'utente che le applicazioni, devono conoscerne o alcune proprietà o il nome, per cui è fondamentale conoscere la convenzione che è alla base dello spazio dei nomi di Active Directory.
- Active Directory supporta diverse convenzioni dei nomi, per cui è possibile utilizzare quella che si ritiene più conveniente.
  - Distinguished Name.** Ogni oggetto in Active Directory ha un suo "Distinguished Name" che indica il dominio in cui l'oggetto è localizzato oltre che il path completo all'interno del dominio. Ad esempio, il Distinguished Name "CN=James Smith,CN=Users,DC=contoso,DC=msft" identifica l'oggetto "James Smith" contenuti nel contenitore "Users" contenuto nel dominio "contoso.msft". In tale sintassi le abbreviazioni più utilizzate sono CN="Common Name", OU="Organizational Unit", DC="Domain Component".

CN=James Smith, CN=Users, DC=contoso, DC=msft



**Relative Distinguished Name.** E' un sottoinsieme del Distinguished Name che identifica un oggetto una volta che si sia focalizzata l'attenzione su un certo livello della gerarchia.

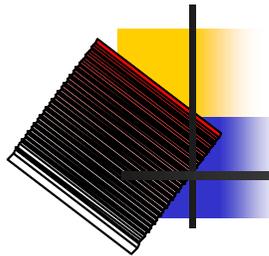


## Spazio dei nomi

- ✎ **User Principal Name.** Lo "user principal name (UPN)" di un oggetto utente è composto dal "logon name" e dal dominio in cui tale logon name risiede. Può essere utilizzato per effettuare il logon. Ad esempio , l'utente "James Smith" nel dominio "contoso.msft" ha come UPN "JamesS@contoso.msft".

JamesS@contoso.msft

- ✎ **Globally Unique Identifier.** Il "**g**lobally **u**nique **i**dentifier (GUID)" è una stringa di 128 caratteri esadecimale che Windows 2000 assegna all'oggetto all'atto della creazione. Per garantirne l'unicità l'algoritmo di creazione si basa su informazioni relative al momento della creazione (data e ora) cui vengono aggiunte informazioni di tipo casuale. Il GUID non cambia se cambia il Distinguished Name. Il GUID è unico per definizione.



# Active Directory e DNS

Active Directory utilizza il DNS per garantire principalmente tre funzionalità:

- ✗ **Risoluzione dei Nomi.** DNS fornisce ad Active Directory il servizio che permette di associare ad un nome il corrispondente indirizzo IP.
- ✗ **Definizione dello Spazio dei Nomi.** I domini Microsoft Windows 2000 vengono denominati utilizzando la convenzione dei nomi su cui si basa il DNS. Dunque un nome di dominio Windows 2000 è un nome DNS. Ad esempio "azienda.com" è sia un nome di dominio DNS valido che un nome di dominio Windows 2000 valido.
- ✗ **Localizzazione delle Componenti di Active Directory.** Per effettuare il logon sulla rete e/o eseguire ricerche in Active Directory, una macchina basata su Microsoft Windows 2000 deve innanzitutto localizzare un controllore di dominio (per il processo di autenticazione) e/o un server "global catalog" (per eseguire la ricerca). Per quanto detto ai due punti precedenti il server contiene nel proprio database tutte le informazioni necessarie ad individuare quali macchine svolgano, sulla rete, il ruolo di controllore di dominio o global catalog.