1 •Descrizione generale dell'architettura del sistema e dell'interazione tra i suoi componenti.

•Descrizione del sottosistema di sicurezza locale.

2 •Descrizione delle tecniche supportate dal sistema per l'organizzazione e la protezione delle risorse all'interno di una rete.

•Implementazione del meccanismo delle password all'interno del sistema.

L'organizzazione di rete di Windows NT e gestione delle risorse in essa

Speaker: Ricco Daniela

Windows NT dispone di due strutture di rete

•**Workgroup.**

•**Dominio**

L'appartenenza ad una delle due strutture deve essere specificata in fase di setup della macchina.

Workgroup

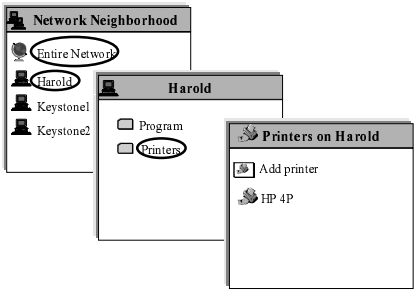
•E' un raggruppamento logico di computer che consente la localizzazione di risorse nella rete (stampanti, file, CD-ROM, modem) in quanto

•Rende possibile la visualizzazione delle directory condivise di ogni altro membro del workgroup tramite servizi di browsing (***Network Neighborhood*** e ***Windows Explorer***).

•Ogni macchina in esso funziona come **server stand-alone** per cui

–Possiede il proprio database contenente informazioni su account utenti e gruppi e non divide tali informazioni con gli altri computer del workgroup.

– L'amministratore (proprietario) del computer decide quali risorse condividere nel workgroup e con chi.



MA...

•Gestione onerosa della rete.

•Necessità di più account per avere accesso alle risorse dell'intera rete e quindi

Necessità di sottoporsi a più processi di logon.

Necessità di ricordare più password quindi

Scelta di password facili da individuare.

QUINDI...

Windows NT Server rende disponibili servizi di directory tramite i **domini.**

Domini

Gruppi di sistemi considerati come una sola situazione circoscritta in termini di sicurezza.

Organizzano le risorse localizzate in diversi sistemi in un unico complesso amministrativo comportando:

- **Una amministrazione centralizzata delle risorse del dominio.**
- **La possibilità per un utente di sottoporsi ad una unica procedura di logon per avere accesso a tutte le risorse nel dominio.**

Una rete strutturata in domini consente:

- **Una amministrazione centralizzata della rete.**
- **La possibilità per un utente di sottoporsi ad una unica procedura di logon per avere accesso alle risorse dell'intera rete.**

Un server nel dominio può essere configurato come:

- **PDC** (unico nel dominio).
- **BDC.**
- **Stand-alone server.**

Primary Domain Controller

- Mantiene il database di directory con le informazioni di account per il dominio.

- E' il server primario che tratta l'autenticazione degli utenti.

Backup Domain Controller

- Mantengono copie di backup del database di directory del dominio che **non possono essere manipolate direttamente**.

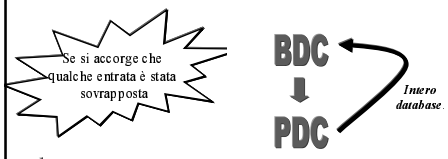
- Trattano l'autenticazione degli utenti se il PDC non è disponibile.

La memorizzazione di più copie del database di directory consente:

- Aumento del grado di fault tolerance nella struttura di rete: **maggiore è il numero di BDC e maggiore è l'efficienza della struttura di rete**.

- Diminuzione del carico di lavoro del PDC e quindi **miglioramento delle prestazioni nella struttura di rete**.

Sincronizzazione dei database di directory



N.B.

La sincronizzazione totale avviene anche quando un BDC assume il ruolo di PDC.

Sincronizzazione onerosa soprattutto se totale e se i Domain Controller coinvolti sono uniti da link lenti.

Si potrebbe

- Incrementare la taglia del Change Log.
- Diminuire i tempi per la sincronizzazione.
- Aumentare il numero di BDC da avvisare ad ogni nuovo impulso.

In Windows NT Server ***Registry***

Stand-alone server

- Non memorizza copie del database di directory del dominio.
- Memorizza e gestisce un proprio database di directory.

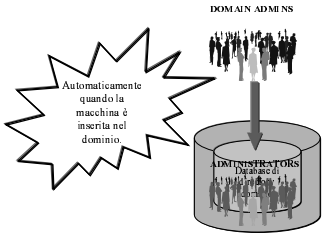
Funziona come una workstation.

Un server di dominio potrebbe essere configurato come tale poiché:

– Si potrebbe richiedere per esso una gestione locale a parte (perché dedicato ad applicazioni particolari).

– Si preferisce evitare a sever dedicati ad applicazioni onerose (gestione database SQL), il carico della gestione degli account di dominio.

Amministrazione di un dominio



L'utility ***User Manager for Domains*** **è inclusa** in Windows NT Server per gestire i database di account in maniera remota (tramite i **canali di comunicazione di sicurezza**).

Tale utility **può essere installata** anche su Windows NT Workstation.

Risorse di dominio:

Localizzazione e accesso

- La localizzazione avviene come per i workgroup (ogni sistema del dominio rende note le proprie risorse).
- Per l'accesso l'utente deve avere un account nel database di directory del dominio.

Un'organizzazione di rete richiede la costituzione di più domini per :

- Evitare la costituzione di database di account di elevate dimensioni.
- Evitare frequenti e dispendiose operazioni di sincronizzazione.
- Permettere che ogni dipartimento dell'organizzazione complessiva organizzi e gestisca le proprie risorse.

Un utente deve avere l'account in ogni dominio?

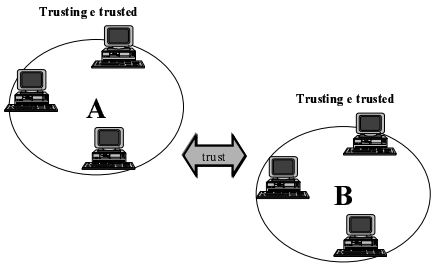
Relazioni di fiducia tra domini

Consentono:

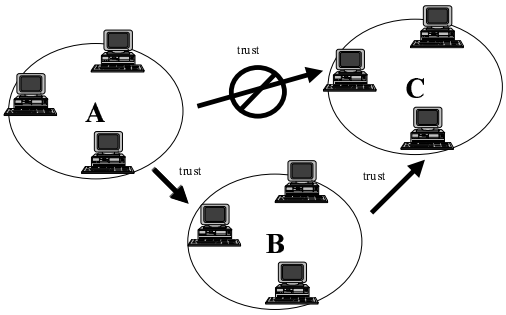
•L'accesso alle risorse dell'intera rete con un unico account di dominio e subendo un unico processo di logon .

•La fusione di amministrazione locale e centralizzata.

Possono essere **monodirezionali** o **bidirezionali**.



A concede l'accesso delle sue risorse a **B**. e **B** concede ad **A** l'accesso alle sue risorse.



Account di dominio

Il gruppo globale raggruppa gli utenti di dominio. Gli account utenti globali possono essere esportati per l'utilizzo di risorse in altri domini.

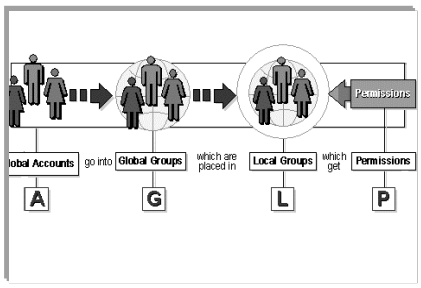
Possono essere inseriti nei gruppi locali trusted o provenienti da altri domini trusted.

Ad essi possono essere assegnati diritti nel dominio in cui creati o nei domini trusting in cui esportati.

Il gruppo globale raggruppa gli utenti di dominio. Gli account utenti globali possono essere esportati per l'utilizzo di risorse in altri domini.

Possono essere inseriti nei gruppi locali trusted o provenienti da altri domini trusted.

Ad essi possono essere assegnati diritti nel dominio in cui creati.



Logon interattivo, logon remoto,
pass_through authentication

Ricordiamo che

Il processo di logon è la prima misura di sicurezza per proteggere le risorse da accessi illeciti.

Consiste di una fase di inserimento informazioni (**user name** e **password**, **dominio**) ed una fase di autenticazione.

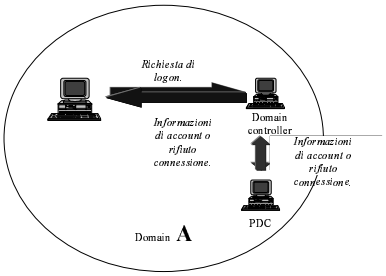
Il logon **remoto**

Avviene utilizzando le credenziali immesse per la connessione interattiva a meno che esse non vengano sovrascritte.

1

Procedura di logon effettuata in locale.

2 L'utente ha account in **A** e si collega ad una macchina in **A**.



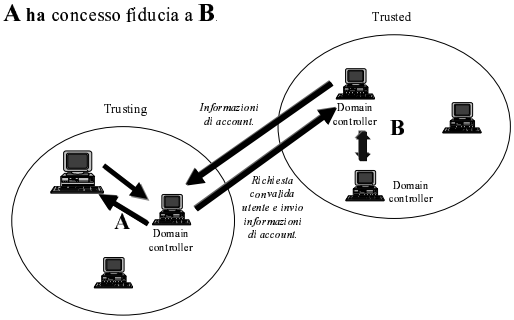
Pass-through authentication

3 L'utente ha account in **B** e si collega ad una macchina in **A**.

A non ha concesso fiducia a **B**.

Il logon procede come se l'utente si stesse collegando con un account locale alla macchina.

A ha concesso fiducia a **B**.



Pass-through authentication

Il servizio Net Logon e i canali di comunicazione di sicurezza

Net Logon gestisce:

- **Pass-through authentication.**
- **Sincronizzazione tra BDC e PDC.**

E' avviato per default all'avvio del sistema ma può anche essere avviato o interrotto dagli amministratori di rete tramite particolari servizi di controllo del sistema.

La comunicazione avviene tramite **canali di comunicazione di sicurezza**.

Ogni sistema che partecipa ad un dominio ha un **account di computer** nel database di directory del dominio.

Un account di computer:

•E' creato da un amministratore di rete quando la macchina viene inserita nella struttura di rete.

•E' utilizzato nella creazione di canali di sicurezza tra computer.

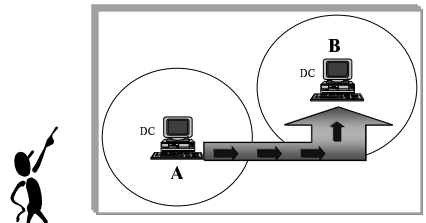
•E possibile distinguere tre tipi di account di computer:

-***Workstation trust account*** che consentono ad una stazione di lavoro interattivo di comunicare con un Domain controller per l'esecuzione della pass-through authentication.

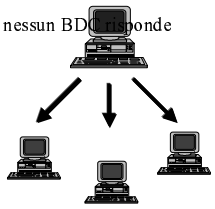
-***Server trust account***.che consentono la comunicazione tra Domain controller dello stesso dominio.

-***Interdomain trust account*** per la comunicazione tra Domain controller di domini uniti da relazioni di fiducia.

All'avvio del sistema ogni client creerà un **canale di comunicazione di sicurezza** con un domain controller dove è localizzato il suo **machine account**.



3 e nessun BDC risponde



Instaurazione del canale di comunicazione con ogni domain controller che possiede il suo machine account che risponde.

Instaurazione del canale di sicurezza

Modelli di rete

Sono determinati dalla configurazione delle relazioni di fiducia tra i domini in essa.

Ne esistono tre:

•**Master domain.**

•**Multiple-master domains.**

•**Complete trust.**

Modello Master Domain

•Assume l'esistenza di un dipartimento centrale.

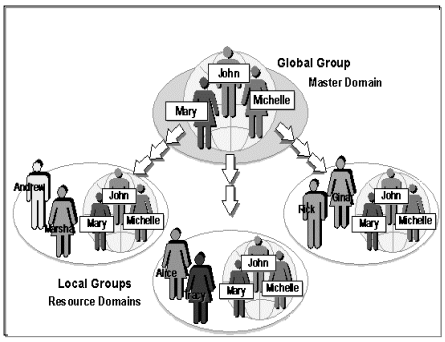
•Viene designato un unico dominio (**Master Domain**) per gestire gli account.

•Il dominio master è trusted, tutti gli altri sono trusting.

Quindi:

•Gli account utenti sono allocati e mantenuti nel dominio master.

•Le risorse sono allocate e mantenute nei domini trusting.



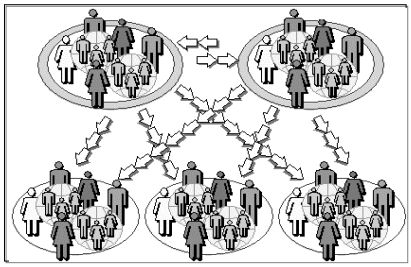
•La gestione degli account è centralizzata.

•Resource Domain possono essere utilizzati per

–Organizzare le risorse logicamente.

–Concedere ad ogni dipartimento una amministrazione centralizzata delle stesse.

Modello Multiple Master Domains



Oltre a tutti i benefici del modello Single Master Domain

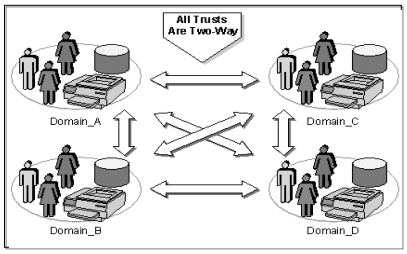
Può essere utilizzato anche per reti di grosse dimensioni.

•Il numero delle relazioni di fiducia e di gruppi cresce con il numero di master domain consolidati.

•L'allocazione degli account in domini differenti può complicare la gestione della rete.

Modello Complete Trust

Utilizzato quando ogni dipartimento vuole gestire pienamente il proprio dominio.



•Può essere utilizzato anche per reti di grosse dimensioni.

•Ogni dipartimento può gestire centralmente la sicurezza delle proprie risorse.

•Il numero delle relazioni di fiducia e di gruppi cresce con numero di master domain consolidati (**se n è il numero di domini occorrono n*(n-1) relazioni di fiducia**).

•Il controllo centralizzato della sicurezza dell'intera rete è perso.

•La gestione di un dominio praticata da un dipartimento dipende dalla gestione messa in pratica dagli altri dipartimenti.

Interazione di Windows NT con altri sistemi

Software che concede l'interoperabilità con altri sistemi (client *Windows 95, MS-DOS, Macintosh, Novell NetWare;* client e server *LAN Manager 2.x*) è incluso in Windows NT o è disponibile separatamente.

Account di dominio locali vengono utilizzati a tale scopo.

Utilizzati anche per gli utenti di domini **untrusted**.

FINE PRIMA PARTE