Reti Locali
Condivisione di risorse - Sicurezza

Lezione tenuta presso l'Istituto
I.I.S.S. "Egidio Lanoce"

Maglie, 23 Novembre 2011

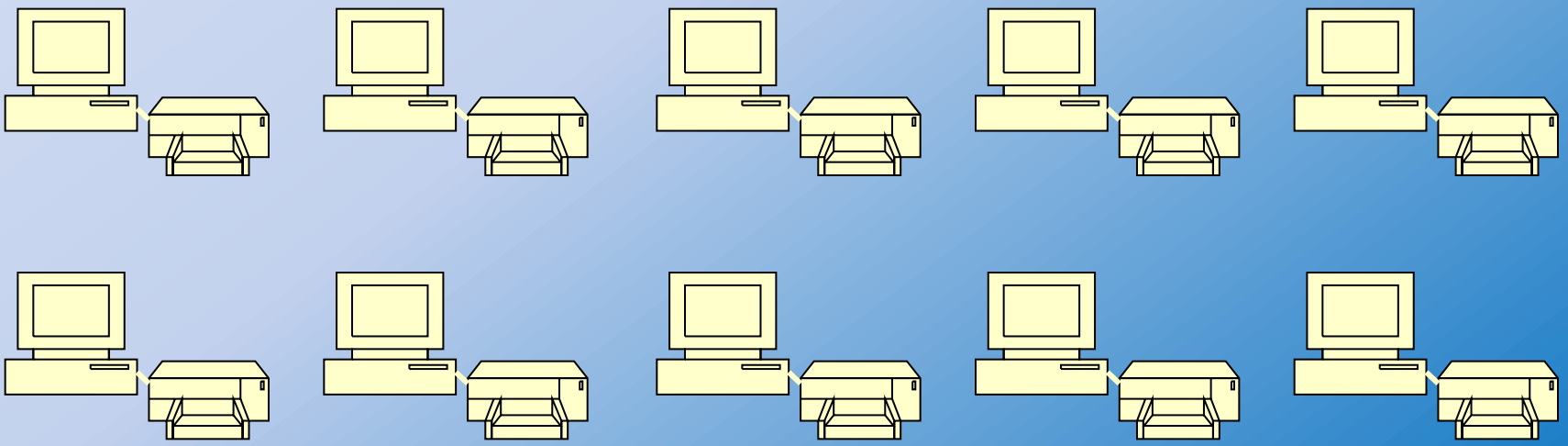
Prof Antonio Cazzato

Il computer stand-alone

- E’ più facile da gestire.
- Non subisce intrusioni dall’esterno.
- Non condivide risorse.
- Ha bisogno di un accesso singolo ad Internet.
- Non permette l’uso di software per aula didattica.

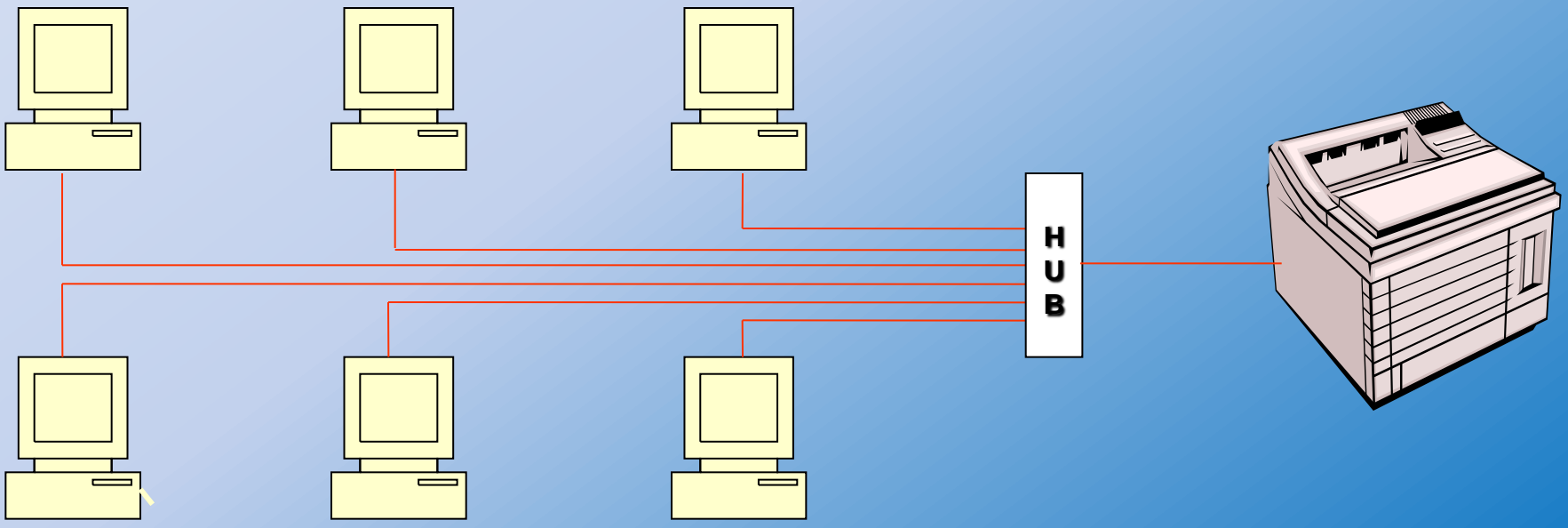
Condivisione di risorse

Il computer stand-alone non condivide risorse. Ad esempio in un aula ogni computer deve avere la propria stampante:



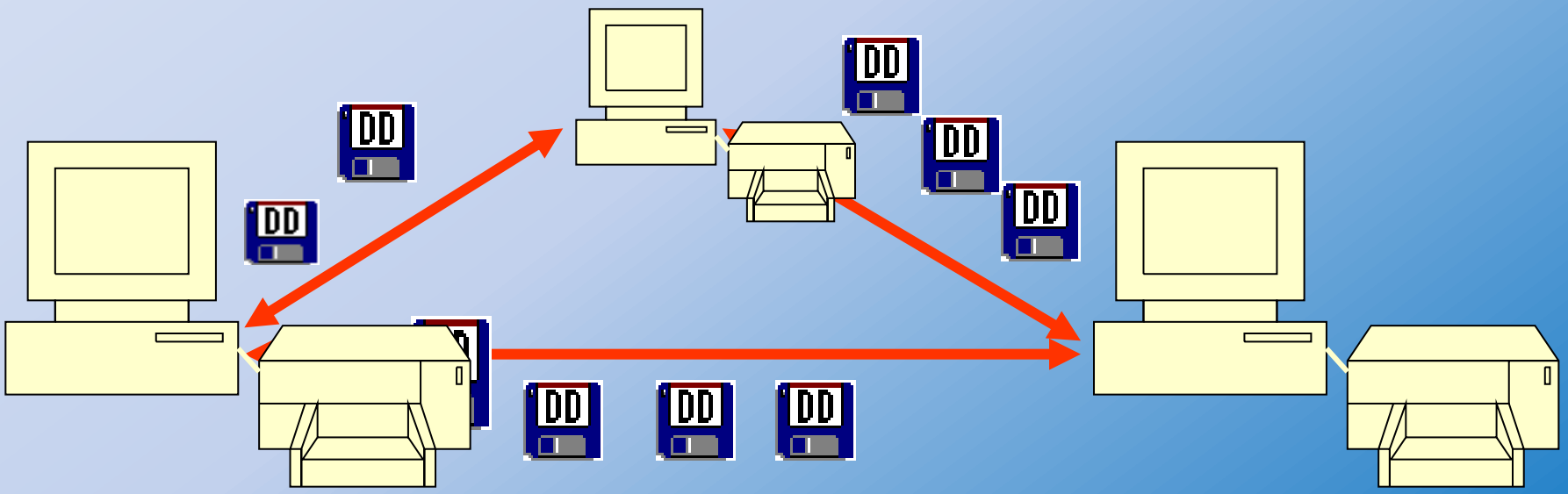
Condivisione di risorse

I computer in rete possono condividere delle risorse. In un'aula è possibile avere una sola stampante, magari di qualità migliore.



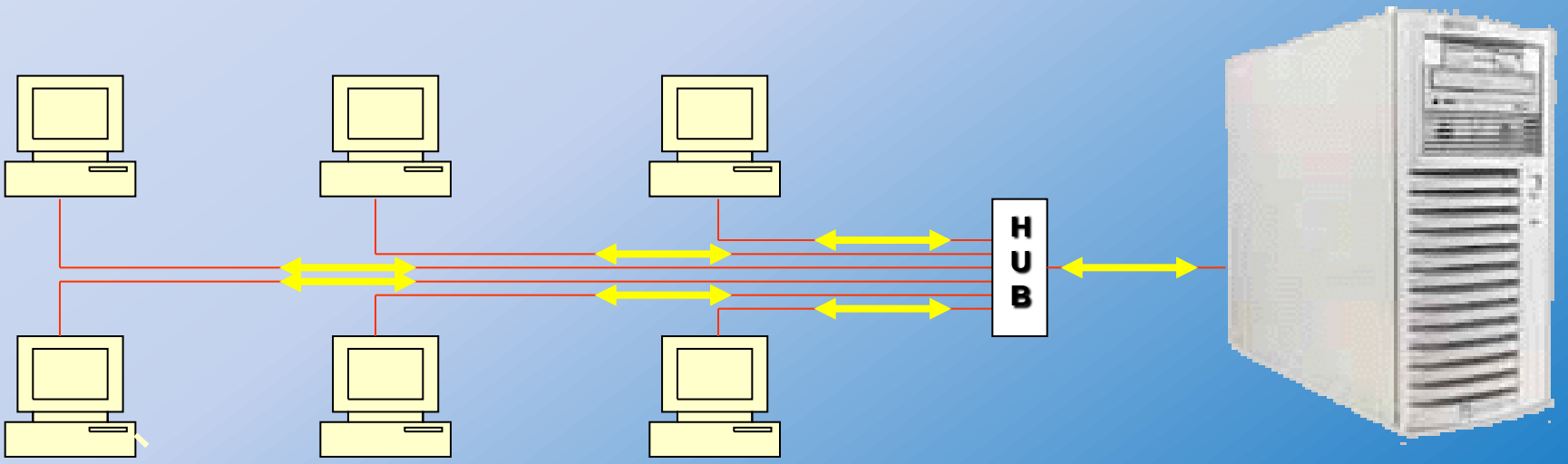
Condivisione di dati

I computer stand-alone possono scambiarsi dati solo attraverso memorie di massa rimovibili, ad es. i floppy disk ed i CDRom, ma il processo è lungo e macchinoso.



Condivisione di dati

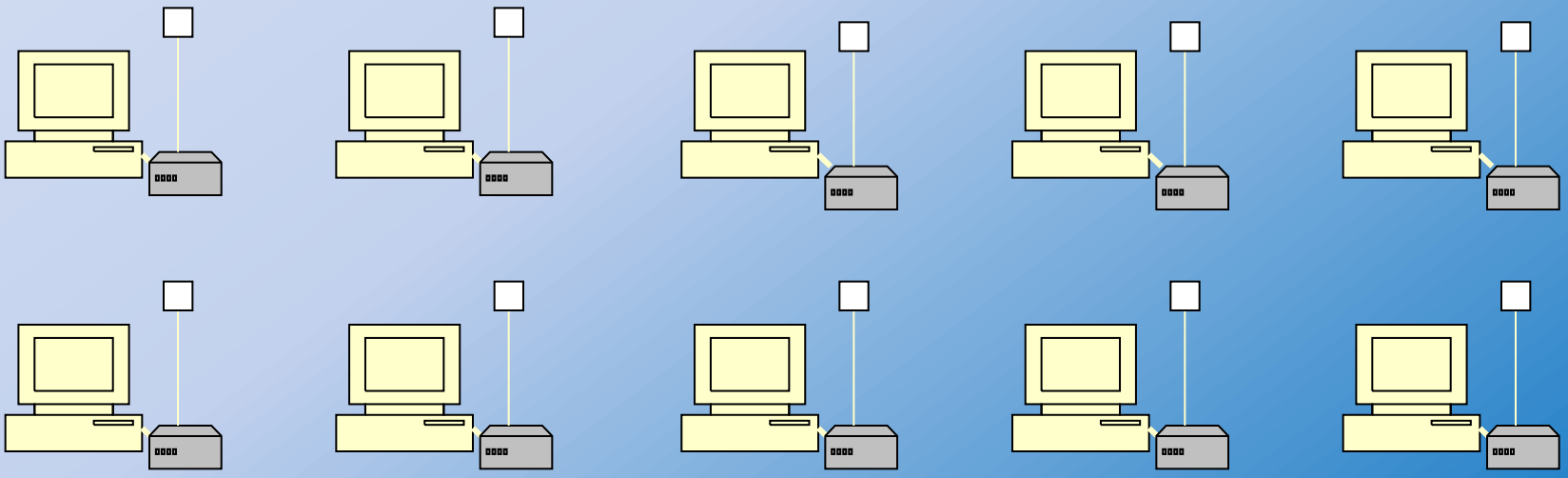
I computer in rete possono condividere i dati scambiandoseli tra di loro, avendo i relativi permessi, oppure concentrando in un computer dedicato l'archivio di tutti dati.



Accesso ad Internet

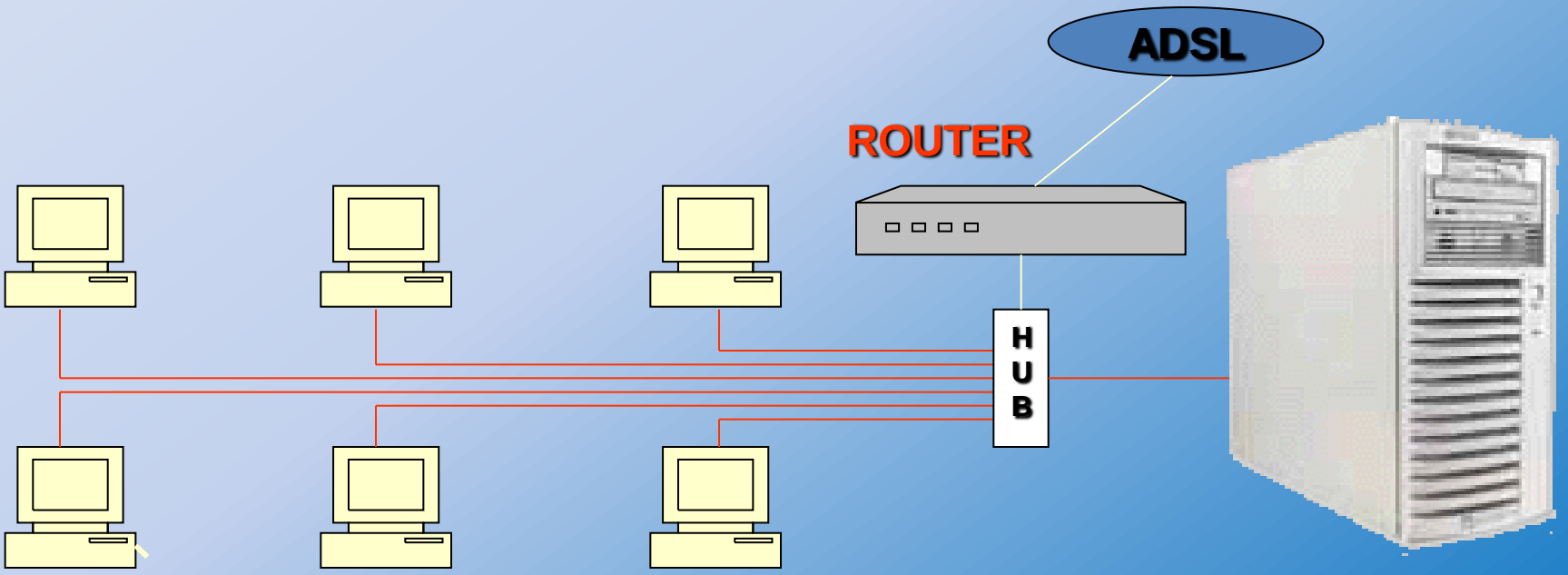
Ogni computer stand-alone deve avere un proprio accesso ad Internet e, quindi, un proprio modem ed una propria linea telefonica.

I costi di gestione sono altissimi.



Accesso ad Internet condiviso

I computer in rete possono condividere una connessione ad internet utilizzando così un solo router ed una sola linea telefonica.



Il modello centralizzato

- Negli anni settanta, si è affermato il modello time-sharing multi-utente (il modello centralizzato) che prevede il collegamento di molti utenti ad un unico elaboratore potente attraverso terminali

Il modello centralizzato

- Mediante il modello time-sharing multi-utente tutti gli utenti di un ufficio o di un centro di ricerca potevano condividere i programmi, i dati e le periferiche collegate all'elaboratore
- All'aumentare del numero di utenti e al crescere delle esigenze di calcolo, questo modello è entrato in crisi, perché era necessario usare elaboratori sempre più potenti
- L'informatica distribuita può essere vista come una naturale evoluzione del modello time-sharing multi-utente

Informatica distribuita

- Gli anni ottanta hanno visto nascere l'era dell'**informatica distribuita**
- Una nuova tendenza che consiste nel collegare in rete gli elaboratori, e quindi gli utenti, che si trovano in uno stesso ufficio o in località diverse

Il modello distribuito

- Gli elaboratori sono collegati tra di loro e possono condividere le risorse
- Ogni utente ha a disposizione una macchina su cui lavorare, ma può anche condividere le informazioni e le risorse con gli altri utenti
- L'informatica distribuita offre molteplici vantaggi rispetto al modello centralizzato

Il modello distribuito: vantaggi rispetto al modello centralizzato

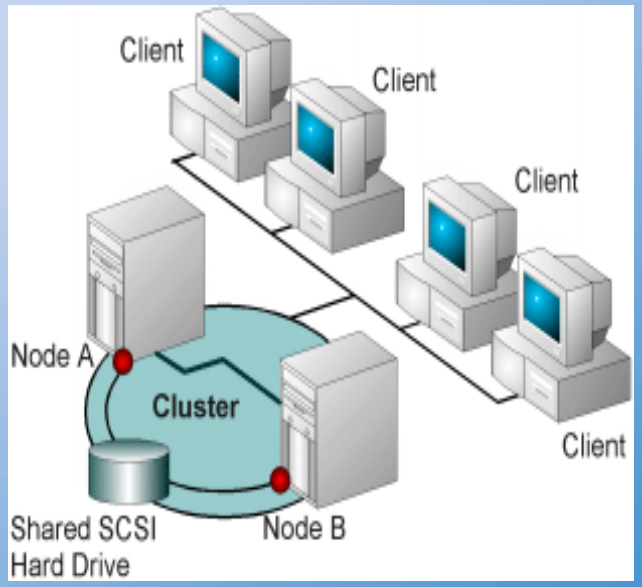
- Flessibilità:
  - In un sistema centralizzato, in caso di guasto all'elaboratore centrale nessuno può lavorare
  - Nel caso distribuito invece, la rottura di una macchina blocca un solo utente mentre gli altri possono continuare a lavorare
- Economicità:
  - In termini di costi, è più conveniente acquistare molti elaboratori personali e collegarli in rete

Il modello distribuito

- Le possibilità di connessione non si limitano agli elaboratori personal
  - Si può collegare in rete anche un elaboratore potente che gli utenti potranno utilizzare quando ne avranno bisogno
- Un altro aspetto fondamentale è dato dalla possibilità di collegarsi ad elaboratori che si trovano in diverse parti del mondo (Internet)

Caratteristiche..e Sfide

- Eterogeneità
- Openess
- Sicurezza
- Scalabilità
- Gestione dei guasti
- Concorrenza
- Trasparenza



Eterogeneità

- Networks
- Hardware
- Operating Systems
- Programming Languages
- Implementations from different Developers

Soluzioni

- **Middleware**
- Mobile code and Virtual Machine

Openess

- Caratteristica di un sistema di essere esteso e re-implementato
- Il numero a volte elevatissimo (a volte ordine di decine di migliaia) di sviluppatori di software indipendenti rende lo sviluppo di una piattaforma distribuita un lavoro molto complesso e difficile da gestire
- Esempi:
  - RFC per internet
  - JBoss per le piattaforme J2EE

Sicurezza

- Confidenzialità (protezione contro l'intercettazione di dati da parte di individui non autorizzati)
- Integrity (protezione contro l'alterazione di dati)
- Availability (protezione contro l'interferenza nell'accesso ad una risorsa)

Scalabilità

- Un sistema è scalabile se rimane operativo con adeguate prestazioni anche se il numero di risorse e di utenti aumenta sensibilmente

Computers connected to the internet

Date	*Computers*	*Web servers*
1979, Dec.	188	0
1989, July	130,000	0
1999, July	56,218,000	5,560,866

Scalabilità (2)

Il progetto di un sistema scalabile presenta quattro principali problemi:

- Estendibilità del sistema
  - Aggiungere server al volo
- Controllare le perdite di prestazioni
  - Usare algoritmi che non richiedono di dialogare con tutto il set di user di un sistema distribuito
  - Usare algoritmi che non richiedono di accedere all'intero set di dati
- Prevenire che finiscano le risorse software del sistema
  - Indirizzi IP
- Evitare i colli di bottiglia nel sistema
  - Centralizzato vs distributed DNS

Gestione dei Guasti

- Scoperta dei guasti
  - Esempio: Checksum per scoprire pacchetti corrotti
- Mascheramento dei guasti
  - Esempio: Ritrasmissione sui canali
- Tolleranza ai guasti
  - Esempio: intrusion tolerant system
- Recupero da guasti
  - Esempio: completamento di long running computation
- Ridondanza
  - Esempio: DNS

Concorrenza

- Accesso multiplo a risorse condivise
- Coordinamento
- Sincronizzazione

Trasparenza

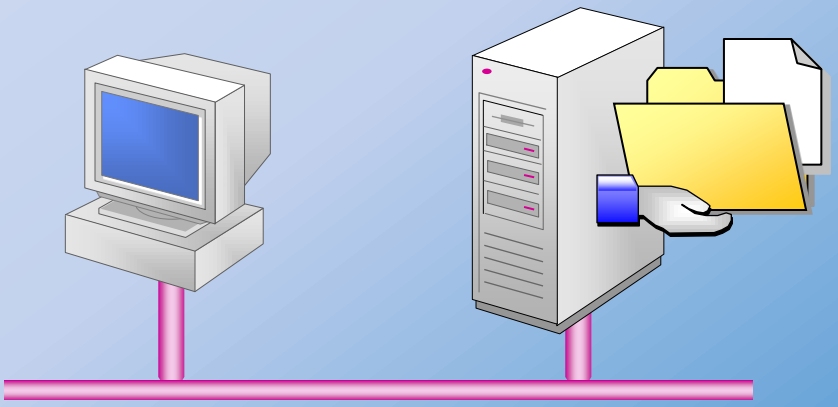
- **Accesso**: permette di accedere a risorse locali e remote con le stesse modalità
- **Locazione**: permettere di accedere alle risorse senza conoscerne la locazione
- **Concorrenza**: permette ad un insieme di processi di operare concorrentemente su risorse condivise senza interferire tra loro
- **Guasti**: permette il mascheramento dei guasti in modo che gli utenti possano completare le operazioni richieste anche se occorrono guasti hw e/o sw
- **Mobilità**: permette di spostare risorse senza influenzare le operazioni utente
- **Prestazioni**: permette di riconfigurare il sistema al variare del carico
- **Scalabilità**: permette al sistema e alle applicazioni di espandersi in modo scalabile senza modificare la struttura del sistema e degli algoritmi applicativi

- Le prestazioni di una soluzione basata su sistema distribuito *non sempre* migliorano rispetto ad una basata su sistema centralizzato. Il middleware, necessario per fornire servizi che sfruttano le caratteristiche di un sistema distribuito, in generale può diminuire le prestazioni

Ancora sull'hardware di rete

Client e Server

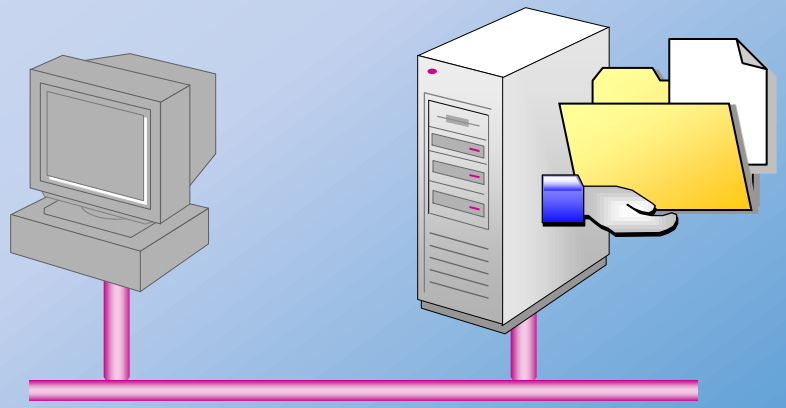
Una rete, sebbene sia usata da persone, è composta da computer. I computer sono classificabili in due categorie: *CLIENT* e *SERVER*



- I *Server* offrono una serie di servizi aggiuntivi agli altri computer della rete;
- I *Client* sfruttano la potenza dei server per ampliare le loro limitate capacità di memorizzazione e d'elaborazione

I Server di rete

- Sono computer che, possedendo maggiori risorse o capacità elaborative degli altri, le mettono a disposizione della rete

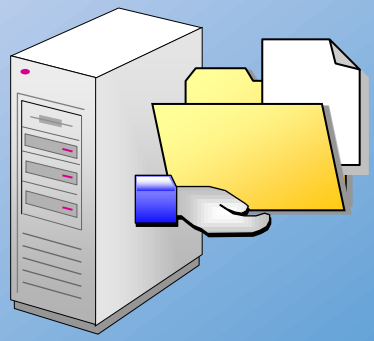


- Sono *dedicati* i server che lavorano esclusivamente per la rete, rispondendo anche a più richieste contemporanee dei client
- Sono *non dedicati* i server che, oltre ad offrire risorse alla rete, sono utilizzati correntemente anche come client

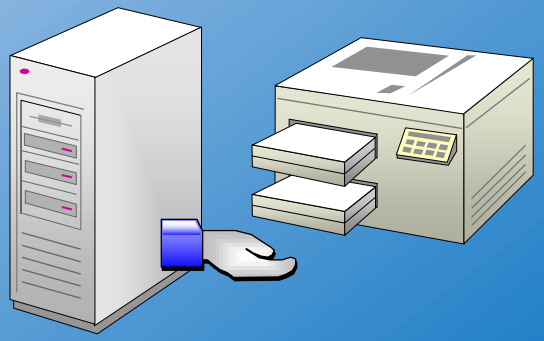
Tipi di Server di rete

A seconda dei servizi offerti, i server possono essere classificati in:

- *FILE* server; viene considerato come il gestore di una libreria di documenti, che viene messa a disposizione dei client



- *PRINT* server; si incarica di gestire i servizi e le code di stampa di una o più stampanti connesse in rete



Tipi di Server di rete

- *APPLICATION* server; esegue determinate operazioni (principalmente su database) e rende dei risultati ai client
- *MAIL/FAX* server; gestisce la corrispondenza in entrata/uscita, smistandola verso i client della rete
- *COMMUNICATION* server; gestisce il traffico di informazioni circolante nella rete/verso altre reti
- *BACKUP* server; esegue backup regolari per archiviare e proteggere i dati della rete

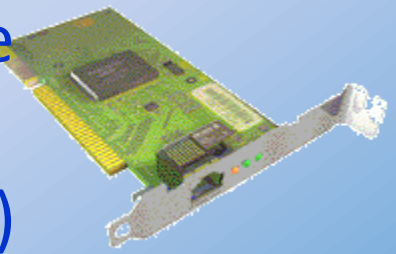
Software di rete

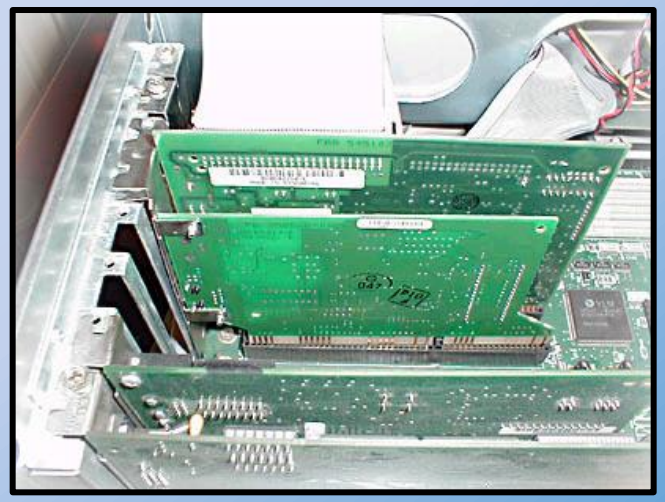
- A seconda della modalità (dedicata e non) e del tipo di servizi offerti, il server può necessitare di software specializzati e sistemi operativi di rete.
- *Windows 9x/ME/XPpro* sono sistemi operativi tipicamente adatti ai client o ai server non dedicati

- *Windows NT/2000*, *NetWare*, *UNIX* e *Linux* nascono invece come sistemi per server, offrendo una vasta gamma di utilità tipiche di un ambiente di rete

La scheda di rete

- Per poter comunicare, i computer di una rete devono essere forniti di una scheda speciale denominata *NIC* (*NetWork Interface Adapter*)
- La scheda va inserita in uno slot interno al computer o, nei portatili, nell'alloggiamento di espansione *PCMCIA*



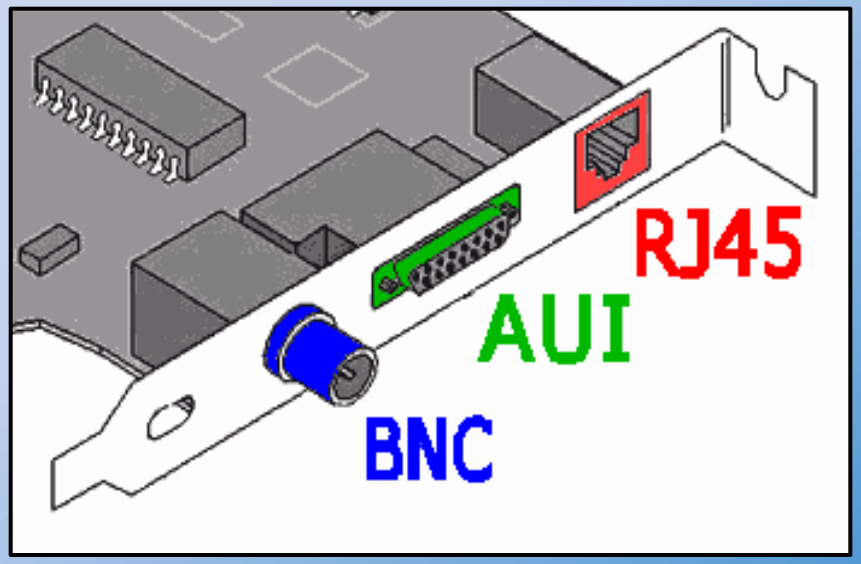


La scheda di rete

- La scheda provvede a trasformare i dati da trasmettere in rete, serializzandoli e spostandoli a pacchetti lungo il cavo a cui è collegata
- Nel computer ricevente la scheda provvede invece ad intercettare i pacchetti ad essa diretti (o di *broadcast*, diretti cioè a tutta la rete) e a ricomporli per essere letti dal calcolatore

La scheda di rete

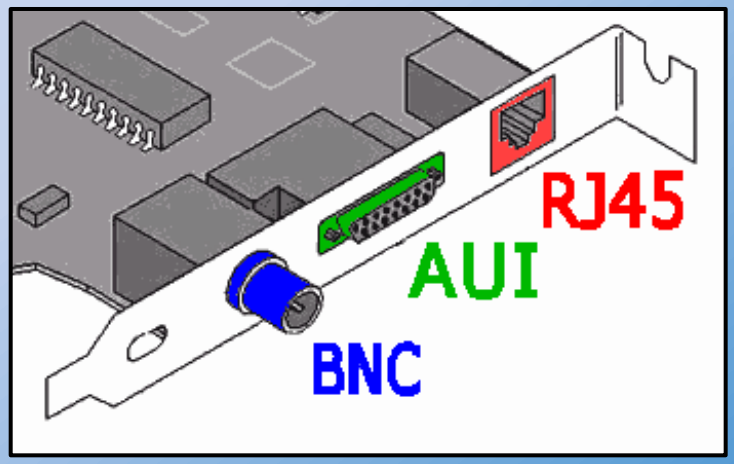
Sul retro della scheda sono presenti i connettori per il collegamento del cavo di rete. Di solito una scheda ha solamente un tipo di connettore, se ne ha più di uno viene detta “*combo*”



I connettori di una rete

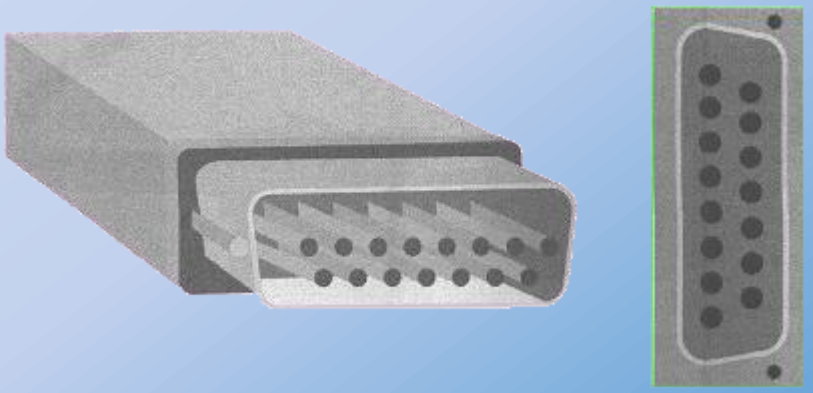
Esistono vari tipi di connettori, in relazione al cavo utilizzato:

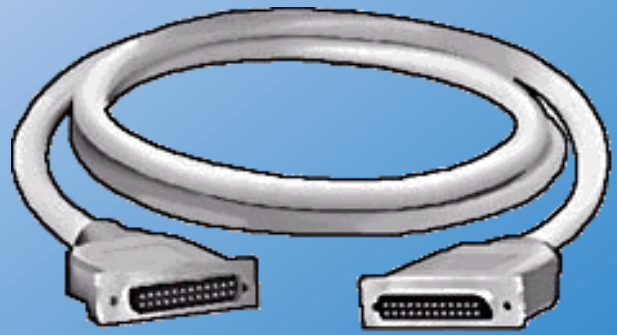
- connettore *AUI* per cavo a 15 fili
- connettore *BNC* per cavo coassiale
- connettore *RJ45* per cavo a 4 coppie intrecciate



Il connettore AUI

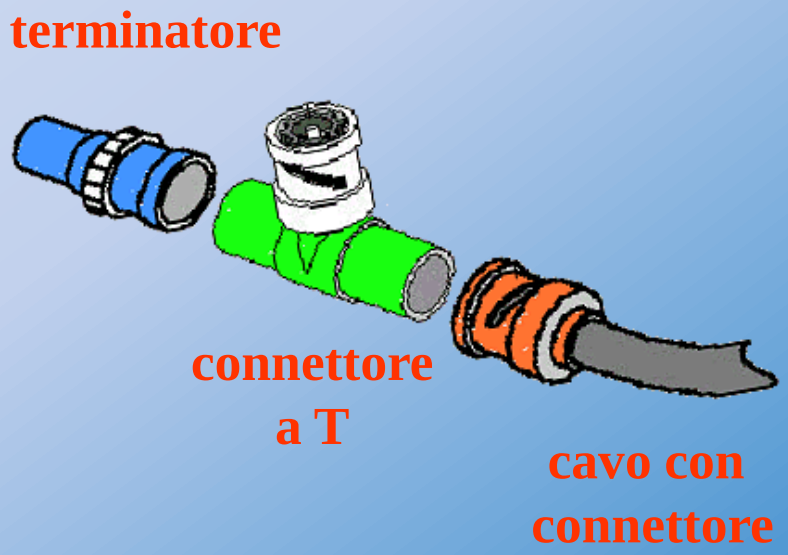
- *Attachment Unit Interface* (*AUI*) è collegato ad un cavo a 15 fili
- da molti anni è caduto in disuso, a causa del suo alto costo

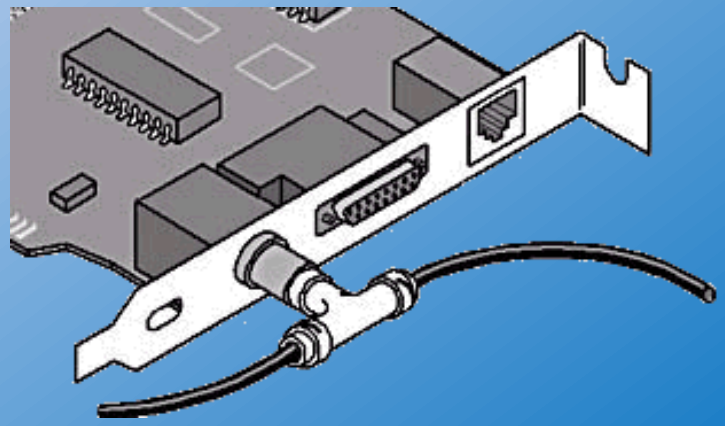




Il connettore BNC

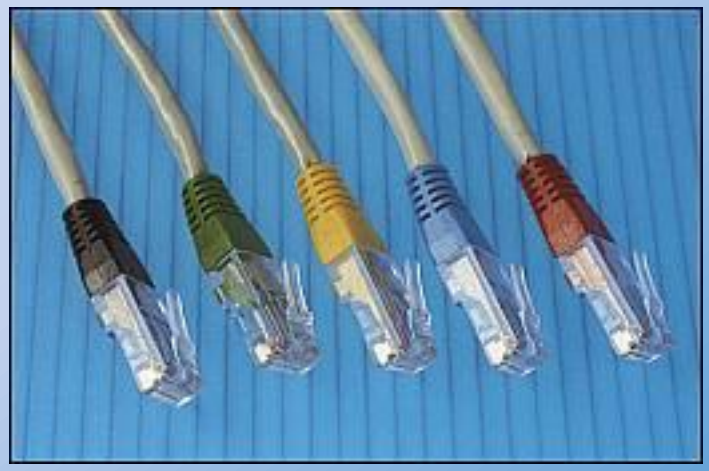
- *Bayonet Navy Connector* (*BNC*) è un connettore a baionetta metallico
- si connette ad un cavo *coassiale* (simile a quello televisivo) a due poli
- sopravvive ancora in piccole reti ed in ambienti con forti interferenze magnetiche

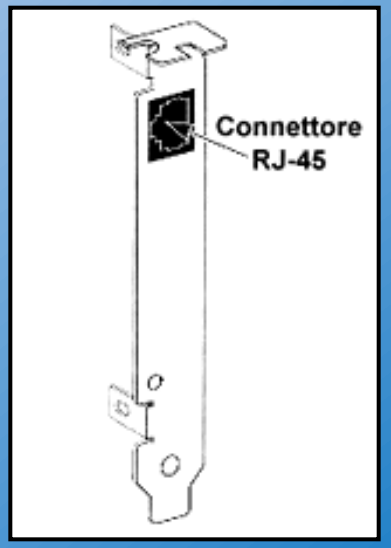




Il connettore RJ45

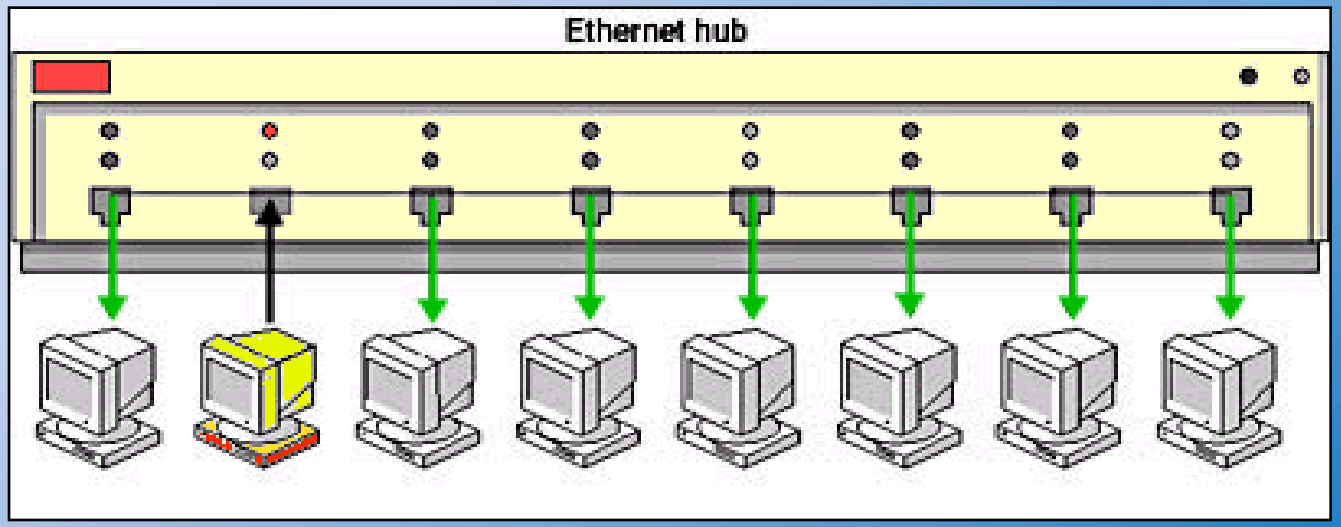
- è simile ad uno spinotto telefonico, un po' più largo
- si connette ad un cavo ad 8 fili (4 coppie intrecciate) di tipo *UTP/STP*
- è attualmente lo standard di mercato, visto che viene utilizzato per le topologie a stella





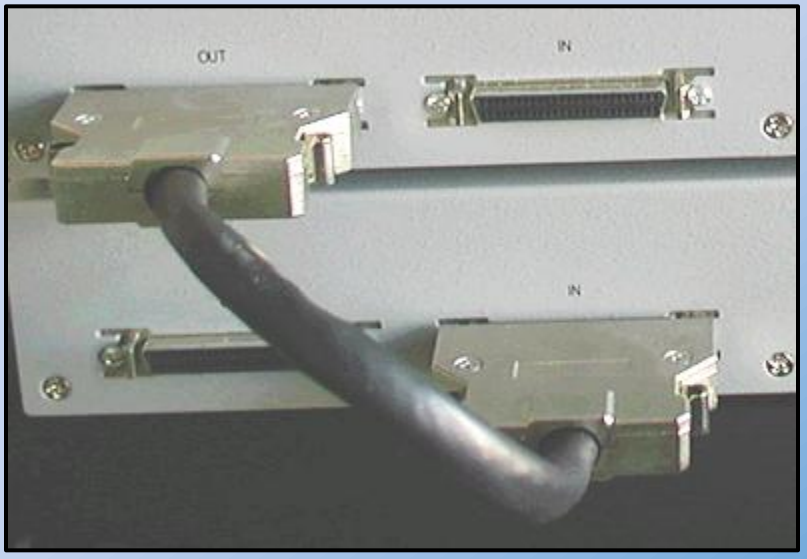
Il concentratore o HUB

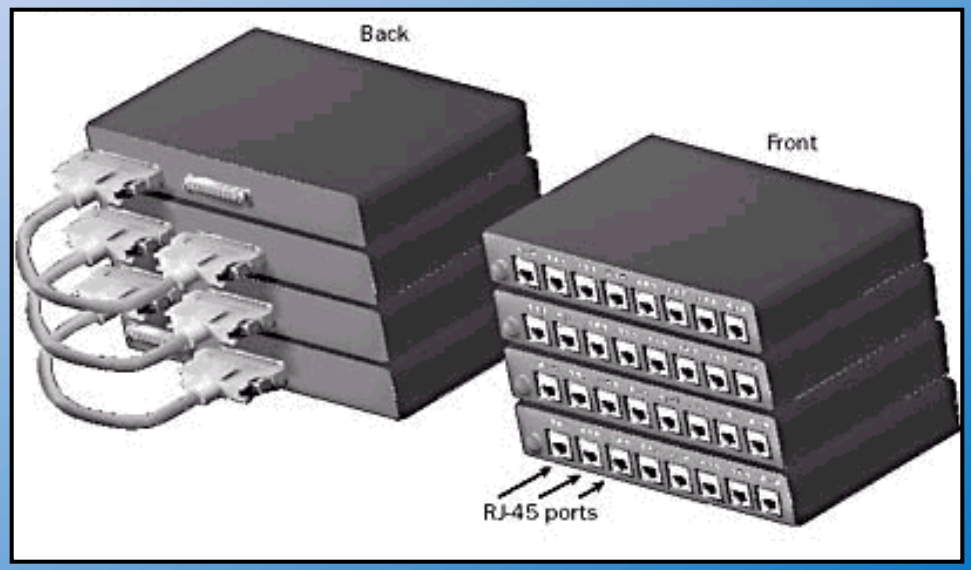
- **Mentre con l'utilizzo dei cavi coassiali non sono necessari componenti aggiuntivi, nelle reti con topologia a stella o miste spicca la presenza dei *concentratori* o *HUB*.**
- **L'hub ha lo scopo di raccogliere le informazioni trasmesse da un nodo e replicarle a tutti gli altri nodi a cui è collegato**



Il concentratore o HUB

- **Esistono hub a 4, 8, 16, 24 porte; superato questo limite è necessario connettere “in catena” più hub, per aumentare il numero di nodi collegabili**
- **Gli hub più costosi possono essere impilati a seconda delle esigenze fino a formare un unico grande hub, con oltre 144 porte**





Wireless LAN

Si tratta di reti locali senza fili, in cui i cablaggi sono sostituiti da apparecchi ricetrasmittenti che inviano e ricevono pacchetti di dati a corto raggio utilizzando tecniche protette di trasferimento delle informazioni.

Una Wireless Lan, in breve, sostituisce o gli ultimi metri del cavo Ethernet tra il portatile e la presa a muro, oppure sostituisce una tratta di cavo che collega due sottoreti.

Lo standard iniziale (2000) era siglato **802.11b** (anche detto comunemente Wi-Fi)**.** L'evoluzione di questo standard è rappresentata dal protocollo **802.11n** che, mantenendo la compatibilità verso il basso, permette un transfer rate teorico di 100 Mbps, contro gli 11 Mbps del precedente.

Componenti principali della wireless lan

- **Le schede PC card da inserire negli appositi slot di espansione dei portatili (PCM-CIA) oppure schede Wireless PCI**

- **I punti di accesso (AP, Access Point)**

L’organizzazione dei files in UNIX

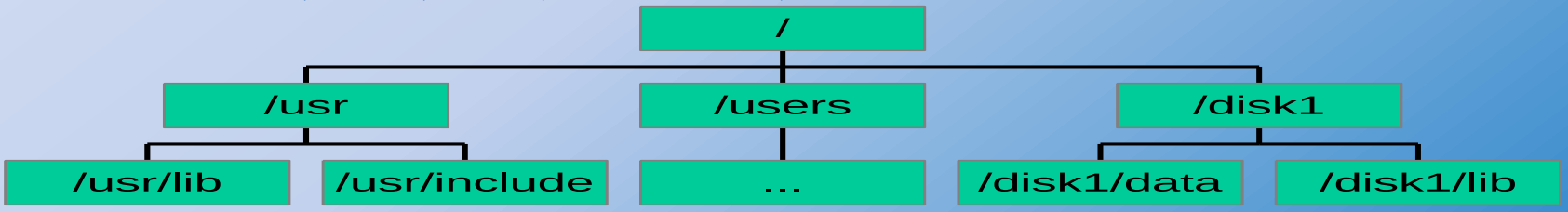
L'organizzazione dei files in UNIX

Il file system UNIX ha sempre una struttura ad albero la cui radice è *"/"*.

Dalla *root directory* si diramano diversi sotto-alberi, corrispondenti a file system locali o remoti.

I files locali possono risiedere fisicamente sul disco interno o su dischi ausiliari che vengono "*montati*" in directory nell'albero di *"/"*.

Es: `mount /dev/dsk/c0t6d0 /disk1`



Ad ogni disco corrisponde un diverso *file system:* `df` è il comando per vedere tutti *file system* montati su un sistema.

Permessi di accesso ai file UNIX

L'accesso ai file ed alle directory UNIX è differenziato per tre classi di utenti:

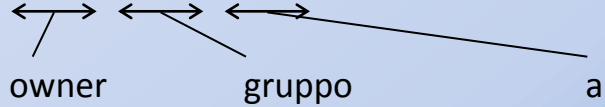
il proprietario (*owner*, che è in genere il creatore del file), il gruppo (a cui l'*owner* appartiene) e gli altri utenti.

Tre tipi di accesso sono possibili:

r - lettura, w - scrittura, x - esecuzione

```
>> ls -l filename

-rwxrw-r--  1 bob U2  3224 Sep 26 08:46 filename
```



L'owner `bob` ha tutti i permessi su `filename`,

gli utenti del gruppo U2 possono leggere e scrivere,

gli altri possono solo leggerlo.

File system distribuiti

NFS e AFS sono i sistemi più usati per realizzare l'accesso a file residenti su nodi remoti in modo trasparente, come se fossero su dischi locali. Entrambi si basano su una comunicazione in rete di tipo *client - server:*

Client è un nodo che accede ad un servizio di rete.

Server è un nodo che fornisce un servizio di rete.

NFS è utilizzato principalmente per la condivisione di gruppi di file tra un insieme di nodi su rete locale.

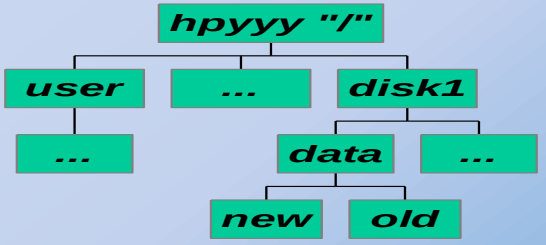
AFS consente a nodi geograficamente distribuiti di accedere con modalità uniforme ad insiemi di file messi a disposizione dai nodi *"server AFS".*

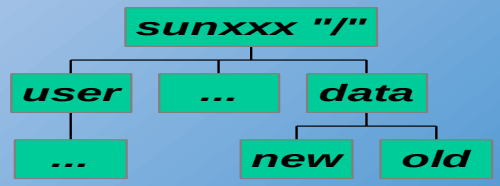
NFS - Network File System

Per NFS ogni nodo è sia *server* che *client*: può mettere a disposizione parti del proprio file system per altri nodi, sia montare parti di file system residenti su altri server.

Un *server* specifica nel file */etc/exports* quali *client* sono autorizzati ad accedere a quali dir: `/disk1/data access=sunxxx`

Se autorizzato, un client *sunxxx* può montare una directory esportata dal server *hpyyy* : `sunxxx>> mount hpyyy:/disk1/data /data`





Tutte le directory sottostanti *data* diventano accessibili, compatibilmente con le proprietà UNIX, agli utenti di *sunxxx* come se fossero locali.

NFS mount

Le operazioni di *mount* possono essere eseguite automaticamente al *boot*;

altrimenti NFS può funzionare in *automount*: quando un utente o un programma tentano di accedere ad un file remoto, il relativo file system viene automaticamente montato dal *client*.

Il path relativo ai file montati via NFS è deciso localmente, secondo una mappa di sistema.

Se per un certo tempo non si verificano accessi al file system, questo viene automaticamente smontato.

Tutto ciò avviene in modo trasparente all'utente *… se non ci sono problemi di rete!*

Tipico problema quando si tenta di accedere ad una gerarchia di files montati via NFS: dopo un lungo timeout

```
>> NFS Server not responding
```

Andrew è il nome di un progetto di CMU antenato di AFS

AFS - Andrew File System

AFS è un file system distribuito che permette la condivisione di file sia su rete locale che su WAN (Wide Area Network).

- AFS distingue tra nodi *server* e nodi *client* .
- Una cella AFS è un insieme di server (tipicamente appartenenti allo stesso dominio) raggruppati da una amministrazione centrale, che si presentano come un unico file system.

Il nome di una cella corrisponde in genere con il nome del dominio Internet

Ad esempio avremo le celle:

infn.it, cern.ch,

slac.stanford.edu

L'accesso ai file AFS

La *root* del file system AFS è */afs* per ogni client e non dipende da mappe come per NFS.
Quindi ogni client ha lo stesso path di accesso ai files sotto AFS.

Ad esempio : /afs/*infn.it/asis/cern/98/bin/paw*

Ogni cella AFS ha un proprio gruppo di utenti; il controllo dell'accesso alle directory (ACL) è più sofisticato rispetto alle proprietà UNIX:

r - read, i - insert, w - write, l - lookup , d - delete, k - lock, a - modify ACL

Il comando fs ha numerose opzioni per gestire directories, cache AFS e ACL.

```
>> fs help
```
le elenca tutte

```
>> fs listacl dirname
Access list for dirname is
  system:anyuser rl
  bob rlidwka
>> fs whereis filename
```

Token: gettone di accesso?

La login AFS

L' *autenticazione AFS* avviene mediante una password, indipendente da quella del nodo su cui l'utente è connesso.

Utilizzare la stessa password può essere utile per l'autenticazione automatica nell'account sotto AFS.

Per effettuare una login nella cella *infn.it* : `>> klog -cell infn.it`

```
Password: ********
```

Per cambiare la password AFS :

```
>> kpasswd
```

All'autenticazione l'utente riceve dal server AFS un *token*, che ha una durata limitata (25 h). Scaduto il *token* occorre rifare *klog*.

Si possono ottenere più token nella stessa sessione, per vederli:

```
>> tokens
```

Utilizzo di AFS

Tutti i comandi AFS si trovano in */usr/afsws/bin*

L'account come utente di una cella AFS va richiesta all'amministratore della cella.

- Ad ogni utente viene assegnata una *home dir* in cui si trovano le aree *public* e *private*. *Public* è utilizzata per condividere file con altri utenti.
- Oltre alle aree utenti, ogni cella può mettere a disposizione aree contenenti software pubblico.
- L'efficienza nell'accesso ad AFS è migliorata da un sistema di *caching* sui client, che riduce gli accessi in rete.

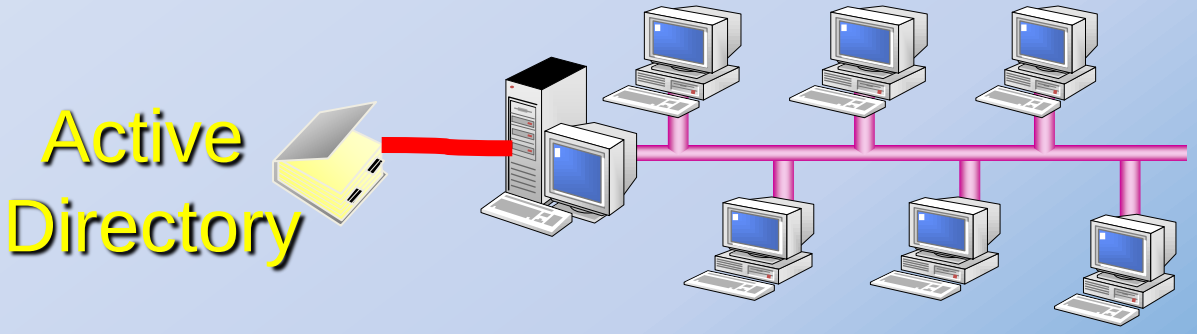
Un manuale di AFS si può trovare in:
http://www.alw.nih.gov/Docs/AFS/AFS_toc.html

Amministrazione di una rete con Active Directory

Gli oggetti di Active Directory

Active Directory organizza la rete con uno schema logico ad oggetti

Gli amministratori di una rete possono gestire le risorse hardware/software mediante oggetti.



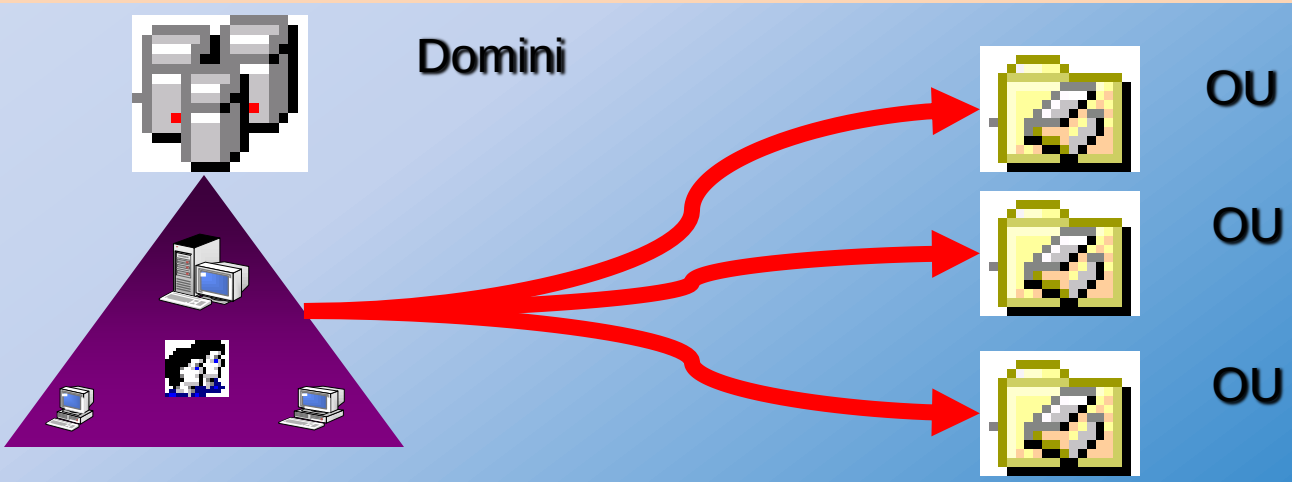
Dobbiamo però distinguere gli oggetti:

- ✓ **di base** quali: i gruppi, gli utenti e i computer;
- ✓ **contenitori** quali Domini e Organizational Unit (OU), che contengono al loro interno gli oggetti di base.

Gli oggetti di Active Directory

Gli oggetti principali di Active Directory sono…

amministrati all'interno di oggetti contenitori:



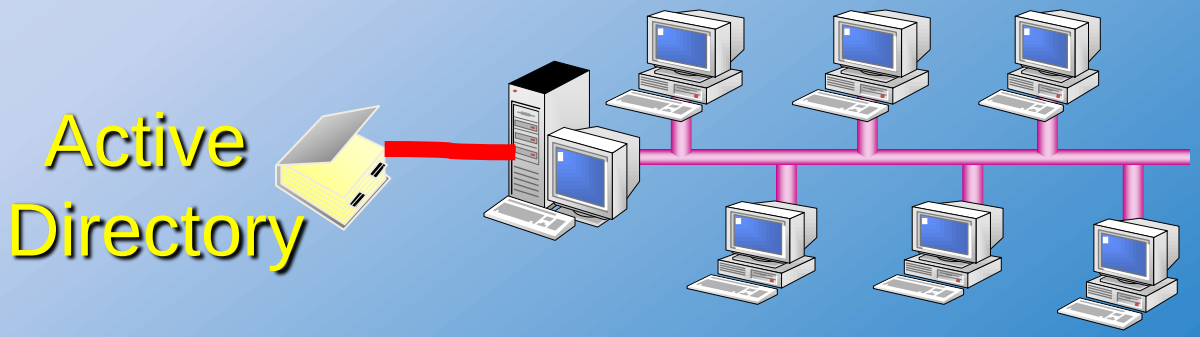
Gli utenti

Ogni utente (User) di un dominio è individuato in modo univoco mediante uno user account

Uno User Account definisce le credenziali di un utente che lo autorizzano ad entrare (log on) nella rete.

Le credenziali principali di uno user sono:

- ✓ Nome utente
- ✓ Password (parola riservata di accesso)
- ✓ Nome del dominio (in cui l'utente dispone di uno user account).



Processo di log on

Il log on è il processo di ingresso in un dominio.

Durante il log on:

1. Un utente introduce le proprie credenziali (nome utente, password e scelta del dominio).

2. Un domain controller del dominio richiesto verifica la correttezza delle credenziali in Active Directory, autorizzando l'ingresso nel dominio soltanto se *Nome Utente* e *Password* sono corrette.

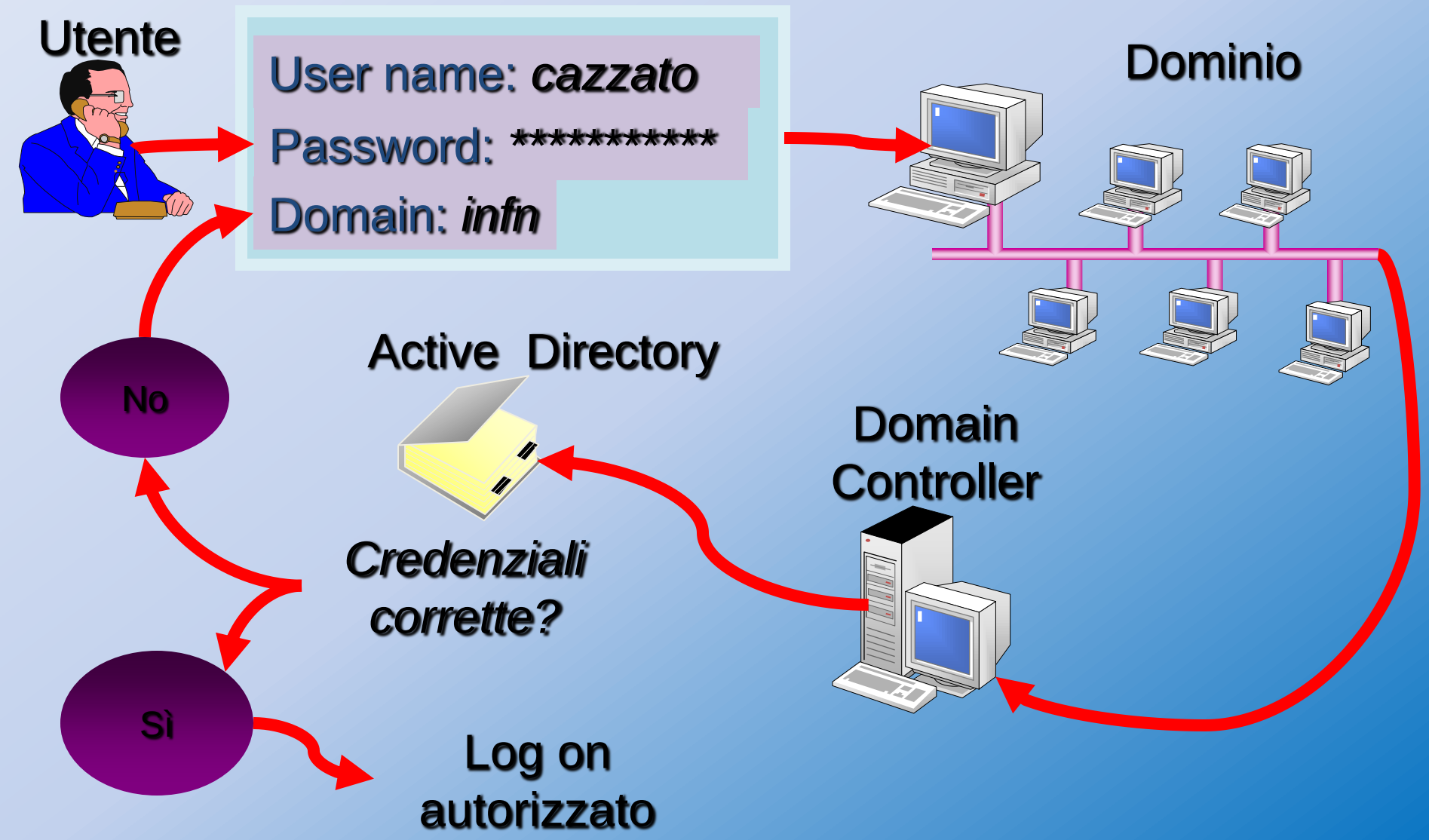
Amministratori

Il processo di uscita di un utente da un dominio è quindi denominato

Log off.

Il processo di log on

Durante il *log on* in un dominio Windows 2000…



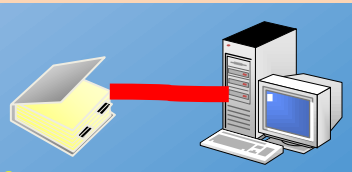
User Rights e Permission

Ogni user account è individuato da un insieme di User rights e Permission

Le user rights (diritti utente) definiscono un insieme di autorizzazioni, predefinite in Active Directory, che possono essere assegnate ad un account utente in un dominio.

Esempi di user rights sono:

- ✓ *Log on locally* → uno user può effettuare il log on in un server;
- ✓ *Shut down the system* → un utente può spegnere il server (shut down);
- ✓ *Change the system time* → un utente dispone dell'autorizzazione per la modifica dell'ora in un server.



User Rights e Permission

Ogni user account è individuato da un insieme di User rights e Permission

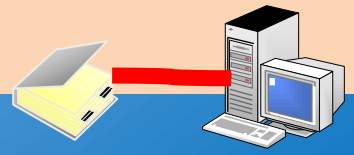
Le permission (permessi) definiscono i tipi di accesso alle risorse HW/SW che è possibile assegnare ad un utente. Le permission sono diverse e dipendono dal tipo di risorsa.

Esempi di permessi sono:

Read → permesso di lettura per le risorse file e cartelle;

Execute → permesso di eseguire un programma in una cartella;

Print → permesso per stampare su una periferica fisica di stampa.



I gruppi

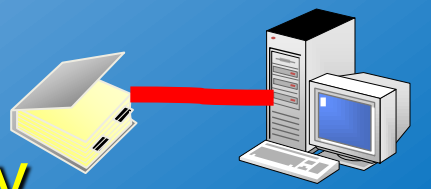
Un gruppo (Group) di un dominio contiene un insieme di utenti

Un gruppo è un insieme di user account e quindi di singoli utenti (che ogni account rappresenta).

Le autorizzazioni e i permessi assegnati ad un gruppo, sono automaticamente propagati in tutti gli user account inclusi nel gruppo stesso.

Per gli amministratori, l'utilizzo dei gruppi è essenziale, perché consente di gestire un numero elevato di utenti con un'unica azione amministrativa.

Amministratori



Active Directory

I gruppi

I gruppi possono essere di tipo diverso:

- ✓ Gruppo locale al dominio (DLG: Domain Local Group);
- ✓ Gruppo globale (GG: Global Group);
- ✓ Gruppo universale (UG: Universal Group).

Ogni tipo di gruppo si differenzia per:

- ✓ la provenienza degli utenti, che può contenere;
- ✓ l'utilizzo, nell'assegnazione di autorizzazioni e permessi di accesso alle risorse.

I gruppi

I gruppi possono essere predefiniti nel dominio oppure creati dagli amministratori

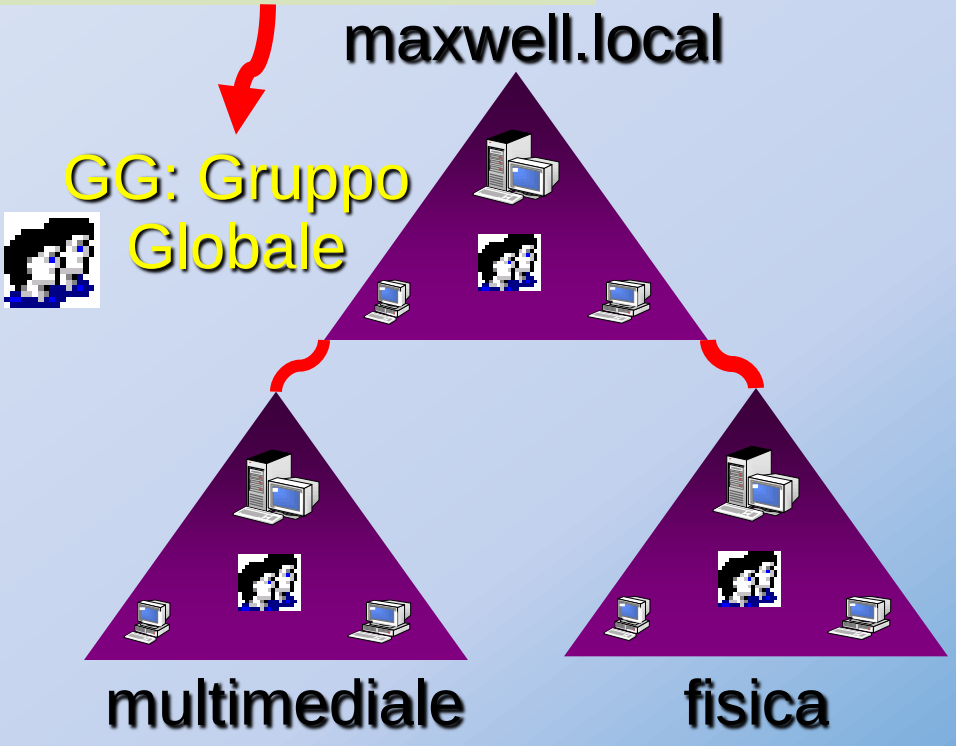
I Gruppi predefiniti nello schema logico di Active Directory dispongono di…

Gruppi Builtin	User rights e permission
Administrators	**Tutte: amministrano le rete**
Guests	**Limitate: assegnate agli utenti ospiti**
Server Operators	**Limitate alla gestione dei domain controller, in particolare, per la creazione di nuovi account**
Backup Operators	**Limitate alla gestione del processo di backup e ripristino dei dati sul server**
Print Operators	**Limitate alla gestione dei server di stampa nella rete**

Tipi di gruppi

I tipi di gruppi si differenziano per la **provenienza degli utenti** definiti nei diversi domini della foresta

Può contenere solo membri del dominio a cui appartiene



UG: Gruppo Universale

Possono contenere membri provenienti da tutti i domini della foresta

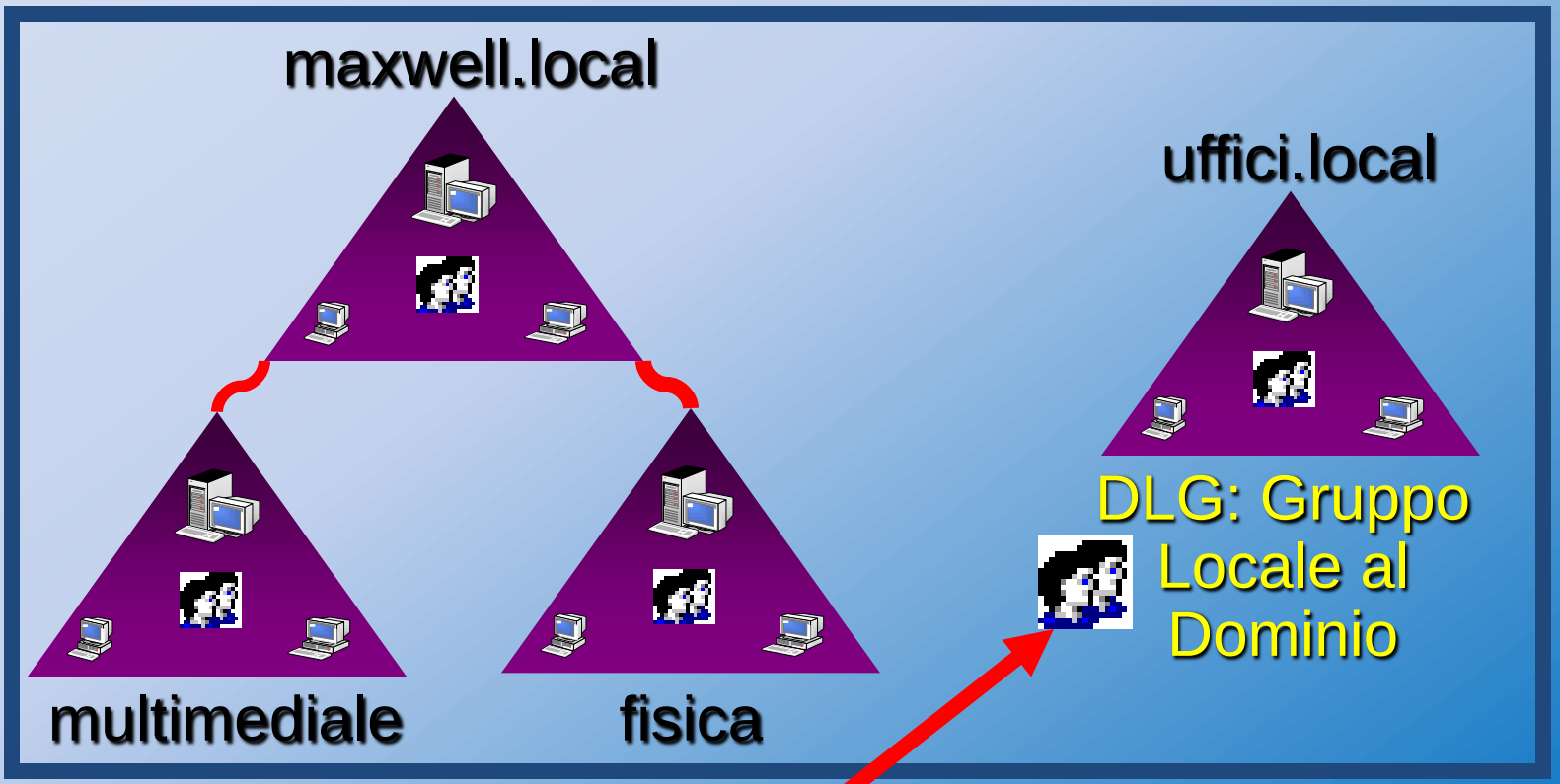
Tipi di gruppi

I tipi di gruppi si differenziano per l'utilizzo nell'assegnazione di autorizzazioni di accesso alle risorse…

Si possono assegnare autorizzazioni all'uso di tutte le risorse dei domini nella foresta

UG: Gruppo Universale

GG: Gruppo Globale



DLG: Gruppo Locale al Dominio

Si possono assegnare autorizzazioni esclusivamente all'uso delle risorse del dominio dello stesso DLG

Organizziamo in gruppi gli utenti della nostra scuola…

Dopo aver definito gli account per tutti gli utenti, possiamo creare i GG (gruppi globali):

- ✓ GGstudenti, con gli account:
  - di tutti i singoli studenti
  - delle singole classi (1A, 2A, 3A, 4A, 5A, ecc.)
- ✓ GGdocenti, con gli account dei docenti
- ✓ GGuffici, con gli user account del personale della segreteria

Amministratori

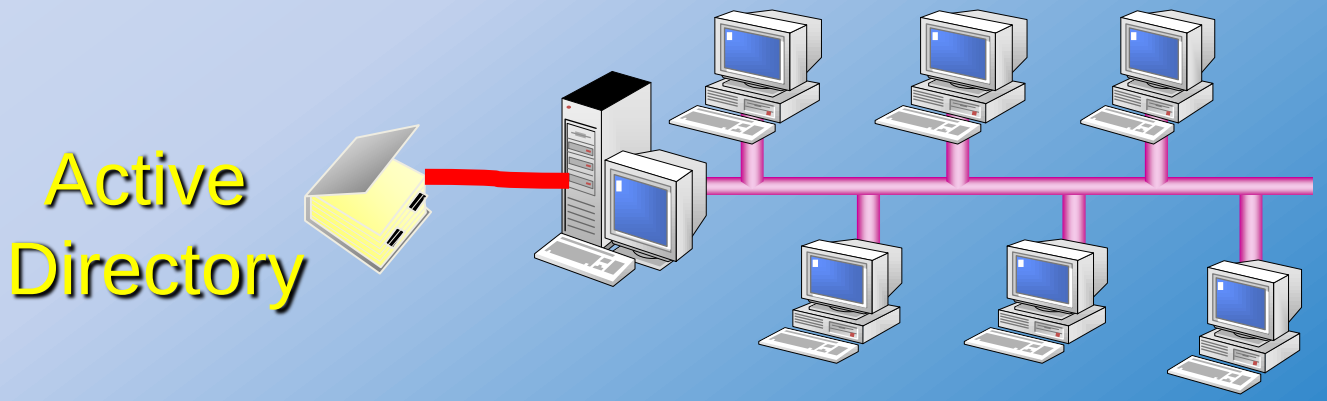
I DLG (gruppi locali del dominio) sono invece utilizzati per definire i permessi di accesso alle risorse.

I computer

Ogni computer del dominio dispone di un Account Computer

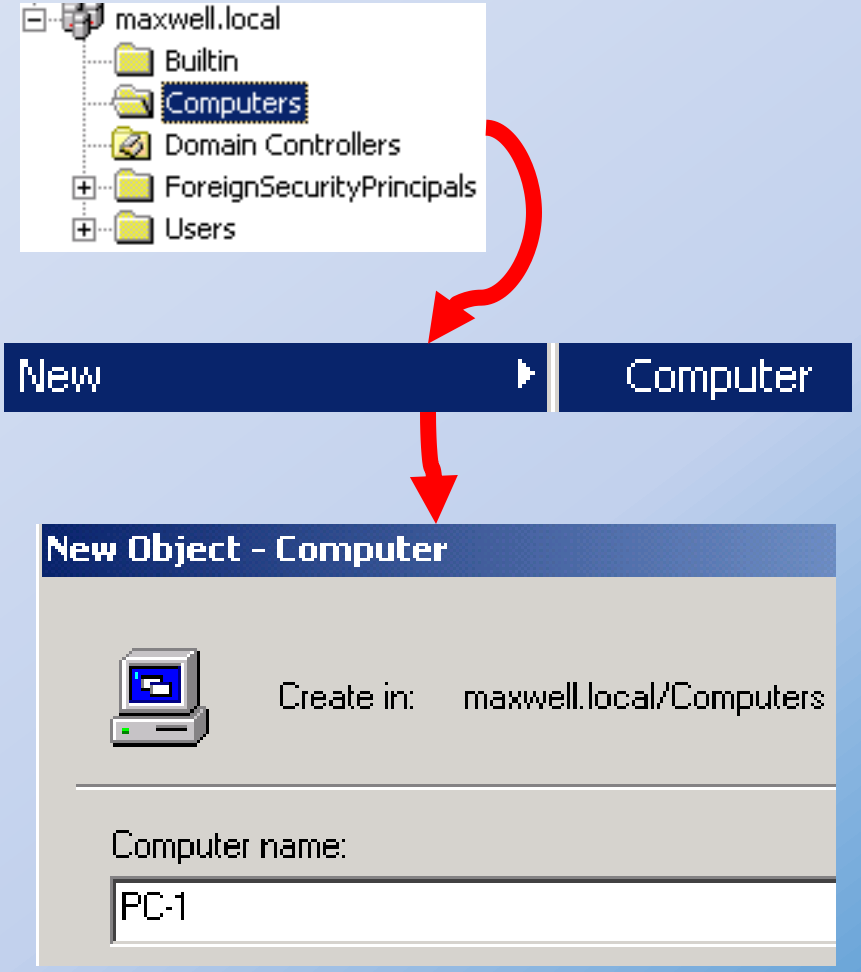
Un Account Computer rappresenta le credenziali di un computer in un dominio.

Le credenziali sono inserite una sola volta, quando si aggiunge il computer ad un dominio già esistente.

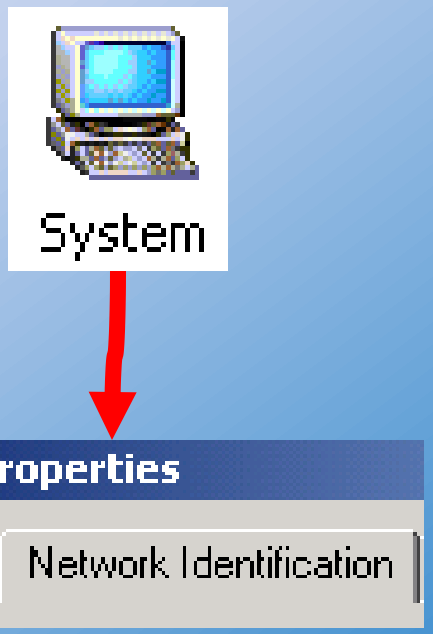


I computer Un account computer può essere aggiunto:

Direttamente in Active Directory nel domain controller:



Nel computer client:



Unità Organizzative

Le Unità Organizzative sono i contenitori logici privilegiati degli oggetti del dominio

Le Unità Organizzative permettono di realizzare uno schema logico gerarchico della nostra rete. A tal fine, una OU può includere altre OU interne.

Le unità organizzative:

- ✓ Sono completamente indipendenti dallo schema fisico di Active Directory, in Siti e Link
- ✓ Permettono di delegare l'amministrazione ai gruppi responsabili degli oggetti contenuti nella stessa OU

Sicurezza in rete

SICUREZZA???

La sicurezza (dal latino "sine cura" senza preoccupazione) può essere definita come "la conoscenza che l'evoluzione di un sistema non produrrà stati indesiderati". **In termini semplici è: sapere che quello che faremo non provocherà dei danni**

"Il problema Internet"
dove nascono i problemi

Solo in Italia Internet rappresenta un bacino di utenza stimato sopra i 25 milioni di utenti

- 1 PROBLEMA: Il mondo digitale (Internet) si rispecchia nel mondo reale
  - Anche i delinquenti usano Internet
- 2 PROBLEMA: su Internet non vi sono confini territoriali
- 3 PROBLEMA: Stiamo utilizzando una tecnologia vecchia di 30 anni che non è nata per applicazioni per esempio di E-Commerce o per garantire sicurezza

Alcuni problemi di sicurezza reali

- Intrusione dalla rete esterna
- furto o manomissione di dati
- sovraccarico di traffico anomalo
- furto di identità e codici segreti
- virus e malware
- spam

Effetti collaterali: perdita di produttività, dov
consumo di banda, sempre maggiori costi per l'amministrazione

Alcuni problemi di sicurezza reali

Il siciliano Giuseppe Russo arrestato per essersi impossessato via Internet di mille numeri di carta di credito di cittadini USA ed averli adoperati	Grossa fetta di potenziali acquirenti si rifiuta di fare acquisti online a causa di problemi di sicurezza recentemente occorsi
Un canadese di 22 anni condannato a un anno di reclusione per aver violato molti computer dei governi USA e Canada	Stanotte, qualcuno di voi potrebbe…

Minacce nuove – automazione

- Microfurti diventano una fortuna
  - *Limare 1/1000 € da ogni transazione VISA!!!*
- Violazioni quasi senza tracce
  - *Il mio PC ha fatto improvvisamente reboot!!!*

Minacce nuove – distanza

- Non esiste distanza
  - Internet non ha confini naturali
- Ci preoccupano tutti i criminali del mondo
  - *Adolescente inglese viola sistema italiano*
- Leggi versus confini nazionali
  - *Denunce contro… Internet*
  - *Trovarsi in uno stato americano con scarsa cyberlaw e mancanza di estradizione*

Minacce nuove – tecniche diffuse

- Rapidità di propagazione delle tecnologie
  - *Hacker pubblica lo script del proprio attacco*
  - *Scaricato crack slovacco per texteditor*
- Diventare hacker spesso non richiede abilità
  - *Scaricato script per attacco di negazione del servizio (DoS)*
  - *Trovato su Internet parte del codice rubato di Win2K e verificato che…*

Il d.lgs 70/2003: la responsabilità dell'ISP

L'ISP non è responsabile per le informazioni trasmesse attraverso la rete per suo tramite, né della loro memorizzazione automatica temporanea al solo scopo di rendere più efficiente il re-inoltro, né della loro memorizzazione richiesta dal destinatario del servizio.

L'ISP non è assoggettato ad un obbligo generale di sorveglianza sulle informazioni che trasmette o memorizza, né ad un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite.

Il d.lgs 70/2003: la responsabilità dell'ISP

Però è tenuto ad informare senza indugio l'autorità giudiziaria o quella amministrativa avente funzioni di vigilanza, qualora sia a conoscenza di presunte attività o informazioni illecite riguardanti un suo destinatario del servizio.

Sistemi di difesa

- Aggiornamento automatico del sistema operativo
- AntiVirus (sempre aggiornato, protegge da virus, malware, allegati di posta, attacchi durante la navigazione. Non protegge da intrusioni)
- Backdoor Cleaner o cleaner
- Malware scanner, antispyware (http://www.microsoft.com/security/malwareremove/default.mspx, http://www.lavasoftusa.com/software/adaware/)
- Firewall
- Chiusura porte e servizi pericolosi
- Certificati dei siti e sistemi di Crittografia (es. PgP)
- Antispam

Sicurezza della comunicazione

- La sicurezza di una comunicazione coinvolge una molteplicità di aspetti, tra cui assumono un ruolo centrale
  - gli attributi dell'informazione trasferita, tali da caratterizzare in primo luogo la *segretezza* dei messaggi scambiati tra le parti in comunicazione e ulteriormente le loro *integrità* , *autenticità* e *non ripudiabilità;*
  - i provvedimenti di *natura protettiva* atti ad assicurare il conseguimento degli obiettivi suddetti.

Componenti della sicurezza

- **Sono componenti di un messaggio sicuro**
  - la *segretezza*, secondo la quale il messaggio emesso deve essere di significatività informativa per il solo destinatario desiderato, mentre deve essere inintellegibile per tutti gli altri utenti; è ottenuta tramite la cifratura del testo in chiaro e la decifratura del testo cifrato;
  - l'*autenticità*, secondo la quale il ricevente ha garanzia circa l'identità dell'emittente e nei confronti di eventuali impostori;

Componenti della sicurezza

- l'*integrità*, secondo la quale il messaggio perviene al ricevente esattamente nella stessa forma con cui è stato emesso; nel trasferimento non si devono essere verificate variazioni accidentali o maliziose.
- la *non-ripudiabilità*, secondo la quale un ricevente è in grado di dimostrare che un messaggio ricevuto perviene da uno specifico emittente e quest'ultimo non deve essere in grado di negare l'invio del messaggio.

Scopo della crittografia

- La segretezza (confidenzialità) di un messaggio è conseguibile con la *crittografia*, e cioè con la scienza che ha come scopi
  - la trasformazione di un messaggio da un *testo in chiaro* (plaintext) a un *testo cifrato* (ciphertext);
  - la trasformazione in senso contrario,

  in modo da rendere il messaggio sicuro e immune da attacchi accidentali o malintenzionati.

Scopo della crittografia

- La trasformazione di un testo in chiaro in uno cifrato è chiamato *cifratura* e rende il messaggio non intellegibile a persone non autorizzate; tale trasformazione è ottenibile con un *algoritmo di cifratura* .
- La trasformazione inversa è chiamata *decifratura* e consente di passare da un testo intenzionalmente non intellegibile ad uno significativo in termini informativi; tale trasformazione è ottenibile con un *algoritmo di decifratura* .

Scopo della crittografia

- Un *cifrario* è la combinazione di un algoritmo di cifratura e del corrispondente algoritmo di decifratura.
- Un cifrario opera in funzione di una *chiave*.
- Una chiave è un'informazione segreta senza la quale è impossibile (o molto difficile) risalire al testo in chiaro dal testo cifrato.
- Gli algoritmi crittografici sono classificati in
  - metodi a *cifrario simmetrico*;
  - metodi a *cifrario asimmetrico*.

Crittografia a cifrario simmetrico

- Nella crittografia a cifrario simmetrico, la stessa chiave *segreta* è utilizzata, in modo condiviso, dall'emittente per la cifratura e dal ricevente per la decifratura su entrambe le direzioni di trasferimento.

…ma la distribuzione delle chiavi può diventare un'operazione organizzativamente complessa.

Crittografia a cifrario asimmetrico

- Nella crittografia a cifrario asimmetrico sono usate due chiavi: una *pubblica* e l'altra *privata* tra loro correlate;
- la chiave pubblica è usata dall'emittente per *cifrare* il messaggio;
- la chiave privata è usata dal ricevente per *decifrare* il messaggio.
- La chiave pubblica è di dominio pubblico (pur essendo specifica di un ricevente), mentre quella privata è nota solo al ricevente.

Crittografia a cifrario asimmetrico

Un messaggio viene quindi cifrato con la chiave pubblica del destinatario e quest'ultimo è l'unico che potrà leggerlo con la propria chiave privata.

Firma digitale

- Le componenti della sicurezza di un messaggio possono essere ottenute attraverso un metodo chiamato *firma digitale*.
- La firma digitale può essere utilizzata
  - sull'intero messaggio;
  - su un suo estratto (digest).

Firma digitale

- Una firma digitale
  - è l'equivalente elettronico di una firma convenzionale;
  - garantisce l'integrità, l'autenticazione e la non-ripudiabilità;
  - fa uso della crittografia asimmetrica;

Firma digitale

- è funzione anche del messaggio da firmare (può essere duplicata e non c'è distinzione tra quella originale e la copia)

- è separata dal messaggio firmato; quindi il mittente spedisce due messaggi: uno che contiene il documento, l'altro che contiene la firma.

- Per accettare un messaggio firmato digitalmente, il destinatario deve utilizzare un algoritmo di *verifica*, che esamina il messaggio e la firma.

Crittografia

In particolare, la maggior parte dei siti di e-commerce odierni utilizzano livelli di crittografia elevati quali, ad esempio:

- Secure Sockets Layer (SSL).
- Secure Electronic Transaction (SET).

SSL

- SSL (Secure Sockets Layer) è un protocollo progettato dalla Netscape Communications Corporation.

- Questo protocollo utilizza la crittografia per fornire sicurezza nelle comunicazioni su Internet e consentono alle applicazioni client/server di comunicare in modo tale da prevenire il 'tampering' (manomissione) dei dati, la falsificazione e l'intercettazione.

Scopo di SSL

Il protocollo SSL provvede alla sicurezza del collegamento garantendo:

- Autenticazione: l'identità nelle connessioni può essere autenticata usando la crittografia asimmetrica, ovvero a chiave pubblica (RSA, DSS, EL-Gamal). Così ogni client comunica in sicurezza con il corretto server, prevenendo ogni interposizione. È' prevista la certificazione del server e, opzionalmente, quella del client.
- Confidenzialità nella trasmissione dei dati: la crittografia è usata dopo un *handshake* (accordo) iniziale per definire una chiave segreta di sessione. In seguito, per crittografare i dati è usata la crittografia simmetrica (AES,3DES, RC4, ecc.).
- Affidabilità: il livello di trasporto include un controllo dell'integrità del messaggio basato su un apposito MAC (Message Authentication Code) che utilizza funzioni hash sicure (MD5, SHA, RIPEMP-160, ecc). In tal modo si verifica che i dati spediti tra client e server non siano stati alterati durante la trasmissione.

Fasi di SSL

SSL richiede di alcune fasi basilari:

- Negoziazione tra le parti dell‘algoritmo da utilizzare.
- Scambio di chiavi segrete tramite cifratura a chiave pubblica e identificazione tramite l'utilizzo di certificati.
- Cifratura del traffico tra le parti a chiave (segreta) simmetrica.

SSL - HTTPS

- **I protocolli di sicurezza risiedono sotto protocolli applicativi quali HTTP, SMTP e NNTP e sopra il protocollo di trasporto TCP.**
- **SSL può essere utilizzato per aggiungere sicurezza a qualsiasi protocollo che utilizza TCP, ma il suo utilizzo più comune avviene nel protocollo HTTPS.**
- **Il protocollo HTTPS viene utilizzato per aggiungere sicurezza alle pagine del WWW in modo tale da rendere possibili applicazioni quali il commercio elettronico.**
- **Il protocollo SSL utilizza metodi di cifratura a chiave pubblica e utilizza certificati a chiave pubblica per verificare l'identità delle parti coinvolte.**

HTTPS

- L'abbinamento SSL al normale HTTP permette di ottenere un nuovo protocollo: l‘HTTPS.

  Questi garantisce l'invio delle informazioni personali sottoforma di pacchetti criptati. In questo modo, la trasmissione delle informazioni avviene in maniera sicura, prevenendo intrusioni, manomissioni e falsificazioni dei messaggi da parte di terzi. Il protocollo HTTPS garantisce quindi tanto la trasmissione confidenziale dei dati, quanto la loro integrità.

- Ad oggi è sicuramente il sistema più usato, in quanto può essere supportato dai principali browser (Internet Explorer e seguenti, Netscape Navigator ecc.) e non necessita di alcun software specifico o password. Le pagine protette da questo protocollo sono facilmente riconoscibili, in quanto la scritta "https" precede l'indirizzo del sito protetto e le sue pagine vengono contrassegnate da un lucchetto, visualizzabile nella parte inferiore del proprio browser.

HTTPS

- L'HTTPS è un URI (Uniform Resource Identifier) sintatticamente identico allo schema http:// ma con la differenza che gli accessi vengono effettuati sulla porta 443 e che tra il protocollo TCP e HTTP si interpone un livello di crittografia/autenticazione.
- In pratica viene creato un canale di comunicazione criptato tra il client e il server attraverso lo scambio di certificati; una volta stabilito questo canale al suo interno viene utilizzato il protocollo HTTP per la comunicazione.
- Questo tipo di comunicazione garantisce che solamente il client e il server siano in grado di conoscere il contenuto della comunicazione.
- Questo sistema fu progettato dalla Netscape Communications Corporation che si occupa delle autenticazioni e delle comunicazioni crittografate ed è largamente usato nel World Wide Web per situazioni che richiedono particolari esigenze in ambito di sicurezza come per esempio il pagamento di transazioni online. In questo caso SSL garantisce la cifratura dei dati trasmessi e ricevuti su internet.

HTTPS

- Questo protocollo assicura una buona protezione contro attacchi del tipo man in the middle (l'attaccante è in grado di leggere, inserire o modificare a piacere, messaggi tra due parti senza che nessuna delle due sia in grado di sapere se il collegamento sia stato compromesso).
- Per impostare un web server in modo che accetti connessioni di tipo https, l'amministratore deve creare un certificato digitale ovvero un documento elettronico che associa l'identità di una persona ad una chiave pubblica. Questi certificati devono essere rilasciati da un certificate authority o comunque da un sistema che accerta la validità dello stesso in modo da definire la vera identità del possessore (i browser web sono creati in modo da poter verificare la loro validità).
- In particolari situazioni (come per esempio nel caso di aziende con una rete intranet privata) è possibile avere un proprio certificato digitale che si può rilasciare ai propri utenti.
- Questa tecnologia quindi può essere usata anche per permettere un accesso limitato ad un web server. L'amministratore spesso crea dei certificati per ogni utente che vengono caricati nei loro browser contententi informazioni come il relativo nome e indirizzo e-mail in modo tale da permettere al server di riconoscere l'utente nel momento in cui quest'ultimo tenti di riconnettersi senza immettere nome utente e/o password.

SET

- Secure Electronic Transaction (SET) è un protocollo standard per rendere sicure le transazioni con carta di credito su reti insicure e, in particolare, Internet. SET è stato sviluppato da Visa e MasterCard (con il coinvolgimento di altre aziende come GTE, IBM, Microsoft e Netscape) a partire dal 1996.
- Il protocollo impiega un algoritmo di oscuramento che, in effetti, sostituisce con un certificato il numero di carta di credito dell'utente durante le transazioni commerciali. Ciò consente agli imprenditori di accreditare i fondi dalle carte di credito degli utenti senza avere la necessità di conoscere il numero della carta.
- SET fa uso di tecniche crittografiche come i certificati digitali e la crittografia a chiave pubblica per consentire alle parti di identificarsi reciprocamente e scambiare informazioni con sicurezza.

SET

Essenzialmente, SET mette a disposizione tre servizi:

- fornisce un canale di comunicazione sicuro, condiviso da tutte le entità coinvolte nella transazione;
- fornisce fiducia, grazie all'uso di certificati digitali;
- assicura la privacy perchè le informazioni sono a disposizione delle entità in gioco, soltanto dove e quando è necessario.

Altri problemi

- Inizialmente il trasferimento dei dati tra il sito di e-commerce e il cliente avveniva in chiaro. Questo costituiva un possibile problema di sicurezza, soprattutto quando c'era un pagamento con carta di credito.

- Con l'avvento del SSL questo rischio è stato ridotto, ma sono poi comparsi altri problemi quale il Phishing e la comparsa di virus troiani che cercano di rubare informazioni utilizzabili per finalità losche.

Phishing

- Il phishing ("spillaggio (di dati sensibili)", in italiano) è una attività illegale che sfrutta una tecnica di ingegneria sociale (studio del comportamento individuale di una persona al fine di carpire informazioni), ed è utilizzata per ottenere l'accesso a informazioni personali o riservate con la finalità del furto di identità mediante l'utilizzo delle comunicazioni elettroniche, soprattutto messaggi di posta elettronica fasulli o messaggi istantanei, ma anche contatti telefonici.

- Grazie a questi messaggi, l'utente è ingannato e portato a rivelare dati personali, come numero di conto corrente, numero di carta di credito, codici di identificazione, ecc.

Metodologia di attacco

Il processo standard delle metodologie di attacco di spillaggio può riassumersi nelle seguenti fasi:

- l'utente malintenzionato (phisher) spedisce al malcapitato ed ignaro utente un messaggio email che simula, nella grafica e nel contenuto, quello di una istituzione nota al destinatario (per esempio la sua banca, il suo provider web, un sito di aste online a cui è iscritto).
- l'email contiene quasi sempre avvisi di particolari situazioni o problemi verificatesi con il proprio conto corrente/account (ad esempio un addebito enorme, la scadenza dell'account ecc.).
- l'email invita il destinatario a seguire un link, presente nel messaggio, per evitare l'addebito e/o per regolarizzare la sua posizione con l'ente o la società di cui il messaggio simula la grafica e l'impostazione.
- il link fornito, tuttavia, non porta in realtà al sito web ufficiale, ma ad una copia fittizia apparentemente simile al sito ufficiale, situata su un server controllato dal phisher, allo scopo di richiedere ed ottenere dal destinatario dati personali particolari, normalmente con la scusa di una conferma o la necessità di effettuare una autenticazione al sistema; queste informazioni vengono memorizzate dal server gestito dal phisher e quindi finiscono nelle mani del malintenzionato.
- il phisher utilizza questi dati per acquistare beni, trasferire somme di denaro o anche solo come "ponte" per ulteriori attacchi.

Difesa

- Banche, istituzioni o internet provider non fanno mai richiesta dei dati personali a mezzo di una e-mail. In caso di richiesta di dati personali, numeri di conto, password o carta di credito,è buona norma, prima di cancellare, inoltrarne una copia alle autorità competenti e avvisare la banca o gli altri interessati, in modo che possano prendere ulteriori disposizioni contro il sito falso e informare i propri utenti.
- Per eventuali comunicazioni, i soggetti sopra citati possono utilizzare un account istituzionale accessibile solo dal loro sito, ma non la e-mail personale del cittadino.
- Una preoccupazione frequente degli utenti che subiscono lo spillaggio è capire come ha fatto il malintenzionato a sapere che hanno un conto presso la banca o servizio online indicato nel messaggio-esca. Normalmente, il phisher non conosce se la sua vittima ha un account presso il servizio preso di mira dalla sua azione: si limita ad inviare lo stesso messaggio-esca a un numero molto elevato di indirizzi di email, facendo spamming, nella speranza di raggiungere per caso qualche utente che ha effettivamente un account presso il servizio citato.
- Pertanto non è necessaria alcuna azione difensiva a parte il riconoscimento e la cancellazione dell'email che contiene il tentativo di spillaggio.

Pharming

- Pharming è una tecnica di cracking, utilizzata per ottenere l'accesso ad informazioni personali e riservate, con varie finalità. Grazie a questa tecnica, l'utente è ingannato e portato a rivelare inconsapevolmente a sconosciuti i propri dati sensibili, come numero di conto corrente, nome utente, password, numero di carta di credito etc.

- L'obiettivo finale del pharming è il medesimo del phishing, ovvero indirizzare una vittima verso un server web "clone" appositamente attrezzato per carpire i dati personali della vittima.

Metodologia di attacco

- L'utente malintenzionato opera, con l'ausilio di programmi trojan o tramite altro accesso diretto, una variazione nel personal computer della vittima.
- Ad esempio, nei sistemi basati sul sistema operativo Windows, modificando il file "hosts" presente nella directory "C:\windows\system32\drivers\etc". Qui possono essere inseriti o modificati gli abbinamenti tra il dominio interessato (p.es. paypal.com) e l'indirizzo IP corrispondente a quel dominio. In questo modo la vittima che ha il file hosts modificato, pur digitando il corretto indirizzo URL nel proprio browser, verrà reindirizzata verso un server appositamente predisposto per carpire le informazioni.
- Un altro metodo consiste nel modificare direttamente nel registro di sistema i server DNS predefiniti. In questo modo l'utente, senza rendersene conto, non utilizzerà più i DNS del proprio Internet Service Provider, bensì quelli del cracker, dove ovviamente alcuni abbinamenti fra dominio e indirizzo IP saranno stati alterati.

Difesa

- **Per difendersi dal pharming non esistono ancora dei programmi specifici se non i firewall che tentano di impedire l'accesso al proprio PC da parte di utenti esterni e programmi antivirus che bloccano l'esecuzione di codice malevolo.**
- **Se il sito a cui ci si collega è un sito sicuro prima dell'accesso verrà mostrato un certificato digitale emesso da una autorità di certificazione conosciuta, che riporterà i dati esatti del sito. Questo certificato andrebbe quantomeno letto e non frettolosamente accettato.**
- **In alcuni casi il sito sicuro non appare come tale solo perché la banca utilizza una tecnica di incapsulamento delle pagine a frames che non mostra il lucchetto nell'apposita casellina del browser né l'indirizzo in modalità https.**

Difesa

- Un primo controllo per difendersi dai siti di spillaggio, è quello di visualizzare l'icona, a forma di lucchetto in tutti i browser, che segnala che sì è stabilita una connessione sicura (p. es. SSL). Tale connessione garantisce la riservatezza dei dati, mentre la loro integrità e l'autenticazione della controparte avvengono solo in presenza della firma digitale, che è opzionale e non segnalata.
- Comunque, una connessione SSL potrebbe essere stabilita con certificati non veritieri, tramite una coppia di chiave pubblica e privata valide, note a chi vuole fare phishing, ma che non sono quelle effettive del sito. Ad esempio, il certificato riporta che il sito it.wikipedia.org utilizza una chiave pubblica, che in realtà è quella del phisher. I browser piuttosto che l'utente interessato dovrebbero collegarsi al sito di una certification authority per controllare: la banca dati mostra le chiavi pubbliche e un'identificativo del possessore, come l'indirizzo IP o l'indirizzo del sito.
- Alcuni siti hanno una barra antiphishing specifica che controlla l'autenticità di ogni pagina scaricata dal sito, ad esempio tramite la firma digitale.

Keylogging

- Un'altra tecnica di spillaggio consiste nell'inserimento di applicativi di keylogging. In questo caso, i link possono rimandare al sito originale, non necessariamente a un'imitazione.

- Un keylogger è uno strumento in grado di intercettare tutto ciò che un utente digita sulla tastiera del proprio computer.
- Esistono vari tipi di keylogger:
  - hardware: vengono collegati al cavo di comunicazione tra la tastiera ed il computer o all'interno della tastiera;
  - software: programmi che controllano e salvano la sequenza di tasti che viene digitata da un utente.

- I keylogger hardware sono molto efficaci in quanto la loro installazione è molto semplice e il sistema non è in grado di accorgersi della loro presenza.

Keylogging

- I keylogger software sono semplici programmi che rimangono in esecuzione captando ogni tasto che viene digitato e poi, in alcuni casi, trasmettono tali informazioni ad un computer remoto. Spesso questi sono trasportati ed installati nel computer da worm o trojan ricevuti tramite Internet ed hanno in genere lo scopo di intercettare password e numeri di carte di credito ed inviarle tramite posta elettronica al creatore degli stessi.
- Sempre a livello software, un programma di Keylogging può sovrapporsi fra il browser e il mondo internet. In questo caso intercetta le password, comunque vengano inserite nel proprio PC. La password viene catturata indipendentemente dalla periferica di input (tastiera, mouse, microfono): sia che l'utente la digiti da tastiera, sia che l'abbia salvata in un file di testo prima di collegarsi a Internet, e poi si limiti a fare copia/incolla, in modo da evitarne la digitazione, sia questa venga inserita da un programma di dettatura vocale.
- Anche in caso di connessione sicura (cifrata), se sul computer è presente un keylogger che invia le password in remoto, tali password potranno essere utilizzate dalla persona che le riceve.

Anti-spillaggio

- Esistono, inoltre, programmi specifici come la barra anti-spillaggio di Netcraft e anche liste nere, blacklist (funzionano come un controllo degli accessi a una certa risorsa, usufruibile da tutti, ad eccezione delle entità identificate nella lista), che consentono di avvisare l'utente quando visita un sito probabilmente non autentico.
- Gli utenti di Microsoft Outlook / Outlook Express possono proteggersi anche attraverso il programma gratuito Delphish, un toolbar inserito nel MS Outlook / MS Outlook Express con il quale si possono trovare i link sospetti in un'email.
- Questi programmi e i più comuni browser non si avvalgono di whitelist (nega a priori a tutti gli utenti l'utilizzo del servizio, ad eccezione di coloro che sono inclusi nella lista) contenenti gli indirizzi logici e IP delle pagine di autenticazione di tutti gli istituti di credito, che sarebbe un filtro anti-spillaggio sicuramente utile.

Conclusioni

- Con la diffusione dell'e-commerce si sono diffuse truffe sempre più insidiose che colpiscono principalmente gli acquirenti. I principali casi sono:
  - Vendita di prodotti da siti civetta: al ricevimento del pagamento non viene inviata la merce, o viene solamente simulata la spedizione. Problema presente anche su ebay.
  - Realizzazione di siti clonati con la finalità di rubare informazioni quali il codice della carta di credito.
  - Aziende fallimentari che accumulano ordini, e introiti, senza la possibilità di evaderli.
- La normativa italiana prevede che tutti i siti di commercio elettronico riportino nella home page la partita IVA e la denominazione dell'azienda. I siti più importanti di e-commerce hanno un certificato digitale che consente di verificare l'autenticità del sito visitato.
- Il principale problema dal punto di vista delle aziende è la gestione degli ordini simulati, dove vengono indicate generalità false o non corrette per l'invio dei prodotti. Per ridurre il problema molte aziende accettano solamente pagamenti anticipati.

Arrivederci a mercoledì prossimo