Considerazioni generali nella progettazione di una rete

La tecnologia che ormai costituisce lo standard per le reti LAN è l'Ethernet per cui si sceglie di realizzare una LAN Ethernet 100BASE-TX (FastEhernet) oppure una Ethernet 10baseT le cui caratteristiche fondamentali sono :

- Adotta il metodo di accesso multiplo CSMA/CD, come indicato dallo standard IEEE 802.3u per le fastEthernet o IEEE 802.3 per le Ethernet;
- L'architettura dei protocolli comprende i primi due strati OSI : lo strato fisico e lo strato 2, che nel modello generale comprende il protocollo MAC (Medium Access Control) e l'LLC (Logical Link Control);
- Adotta la suite di protocolli TCP/IP per gli strati superiori al secondo;

Lo standard Ethernet

Con il termine Ethernet si indica l'insieme di prodotti LAN aderenti allo standard IEEE 802.3 che definisce il protocollo CSMA/CD (Carrier Sense Multiple Access/Collision Detect), ovvero la tecnica di controllo di accesso al mezzo trasmissivo. Nonostante lo sviluppo di diverse altre tecnologie, Ethernet continua ad essere la più utilizzata poiché il suo protocollo risulta facile da capire, implementare e mantenere, consente la realizzazione di reti a basso costo, consente un'estrema flessibilità topologica nella fase di installazione della rete, garantisce il successo delle interconnessioni e delle operazioni tra prodotti standard indipendentemente dalle loro caratteristiche costruttive.

Lo standard ***IEEE 802.3*** (chiamato ***Ethernet*** dove IEEE sta per *Institute of Electrical and Electronic Engineers*) è per una **rete locale broadcast**, basata su un **bus**, con arbitraggio distribuito, operante a **10** oppure **100 Mbps**.

La gestione dei conflitti di trasmissione (arbitraggio) è affidata al meccanismo CSMA/CD (Carrier Sense Multiple Access/Collision Detection) e i dati viaggiano in forma di *frame* (trama) comprensiva dell'*indirizzo* dei destinatari.

Una rete locale Ethernet si realizza avvalendosi di particolari dispositivi (**hub** o **switch**) da cui con topologia fisica a stella si dipartono i diversi collegamenti ai computer.

La **topologia fisica** di una rete è la conformazione delle linee di trasmissione, ossia il percorso dei cavi tra un'interfaccia di rete e l'altra (il cablaggio). La **topologia logica** è invece il percorso che compiono i dati

In generale, non è detto che la topologia fisica e quella logica coincidano. Le topologie più diffuse sono le seguenti : a bus, ad anello, a stella.

Ad oggi molte delle LAN sono costituite con topologia fisica a stella con al centro un hub o uno switch, ma la topologia logica è a bus poiché generalmente si utilizzano schede Ethernet.

Una LAN con hub o switch centrale ha **topologia fisica a stella**, ma **topologia logica bus.** Infatti è il dispositivo centrale (hub o switch) che funziona da bus cui sono collegate tutte le ramificazioni della rete.

Gli hub agiscono a livello fisico e si utilizzano per LAN di dimensioni ridotte (fino a una ventina di nodi), gli switch intervengono a livello datalink e la loro "intelligenza" si utilizza per LAN di dimensioni maggiori.

Una rete Ethernet è una rete con topologia logica a bus eventualmente con una gerarchia detta ad albero o gerarchica.

La rete è costruita con queste specifiche:

- E' costruita con un'architettura client / server a risorse distribuite, quindi con dei dispositivi richiedenti e altri serventi.
- Ha un topologia a stella estesa, quindi composta da concentratori o ripetitori (anche in cascata) che permettono la trasmissione delle informazioni.
- E' costruita utilizzando standard aperti e non proprietari, quindi coerente a:
    - Standard TCP / IP (livelli e protocolli).
    - Standard di cablaggio delle reti EIA / TIA 568 – A.
- Segue gli standard IEEE 802.3u Ethernet ed è precisamente di tipo Fast Ethernet con una velocità di trasmissione di 100 Mbps.
- I cavi di rete sono gli UTP (non schermati) categoria 5 che trasportano dati fino a 100 Mbps con connettore RJ45maschio.
- Il metodo di accesso al mezzo condiviso utilizzato è il CSMA/CD (Carrier Sense Multiple Access / Collision Detection).

Cavi

Il cavo UTP categoria 5 (EIA/TIA-568A) arriva fino a 100 Mbit/s. La categoria 5e (EIA/TIA-568B) invece è per le connessioni a 1000 Mbit/s.

I computer

I computer presenti nella LAN sono tutti compatibili con gli standard ISO/OSI quindi hanno:

- Un sistema operativo di rete (Microsoft Windows, Linux, MAC …).
- Stack di protocolli TCP/IP.
- Scheda di rete che gestiscono lo standard Fast Ethernet con velocità di trasmissione di 100 Mbps con presa RJ45femmina per la connessione di rete.

La **progettazione** e **realizzazione di una rete LAN** investe due problematiche:

- *la struttura trasmissiva (protocolli, modalità di gestione dei collegamenti, …) regolata dagli standard **IEEE 802**;*
- *il cablaggio della rete, regolato dalle norme **EIA/TIA 568** e **ISO/IEC 11801**.*

> Realizzare le LAN con cablaggio strutturato secondo le specifiche dello standard EIA/TIA 568-B ovvero ISO/IEC 11801, ed impiegando la tecnologia Ethernet (IEEE 802.3) o Fast Ethernet (IEEE 802.3u)

Il Cablaggio strutturato

(http://www-wsp.adckrone.com/it/productsandservices/cablaggio.jsp)

Il cablaggio strutturato è il sistema che garantisce l'interconnessione fisica di sistemi eterogenei, assicurando elevate velocità di trasmissione, modularità, espandibilità e sicurezza.

Il cablaggio strutturato consente di trasportare fonia, dati, segnali video e più in generale varie tipologie di segnali di tipo differente.

Tale sua caratteristica (non essere vincolato ad una sola tipologia di protocollo dati o più genericamente servizio) è la principale differenza tra un sistema di tipo strutturato ed un sistema di cablaggio tradizionale.

Le normative che regolano i sistemi di cablaggio sono applicabili ad un singolo edificio o ad un comprensorio (campus); esse definiscono quanto segue:

- le caratteristiche degli apparati elettrici, elettronici oppure ottici;
- le velocità di trasmissione ammesse;
- le caratteristiche dei mezzi trasmissivi e dei componenti passivi;
- le topologie di cablaggio ammesse ed eventuali livelli di gerarchia;
- le regole di installazione e le indicazioni sulla documentazione di progetto;
- i test di accettazione finale.

Topologie per il cablaggio

(http://www.grid.unina.it/Didattica/RetiDiCalcolatori/RCII/slides/RC%20II%20Parte%202%20-%20Sistemi%20di%20cablaggio%20Strutturato.pdf)

Cos'è il cablaggio

Insieme di componenti passivi posati in opera:
- » cavi
- » connettori
- » prese
- » permutatori, ecc.

Per interconnettere
- » computer
- » telefoni
- » stampanti
- » monitor
- » apparati di rete

Due tipologie

Proprietari:
- » IBM Cabling System
- » Digital DECconnect

Strutturati (conformi a standard nazionali o internazionali):
- » TIA/EIA 568A
  standard americano, approvato nel 1995, per i cablaggi di edifici commerciali di tipo **office oriented**.

- » ISO/IEC IS 11801
  standard internazionale, approvato nel 1995, per i cablaggi di edifici commerciali di tipo **office oriented**.

Normative specificate dagli standard

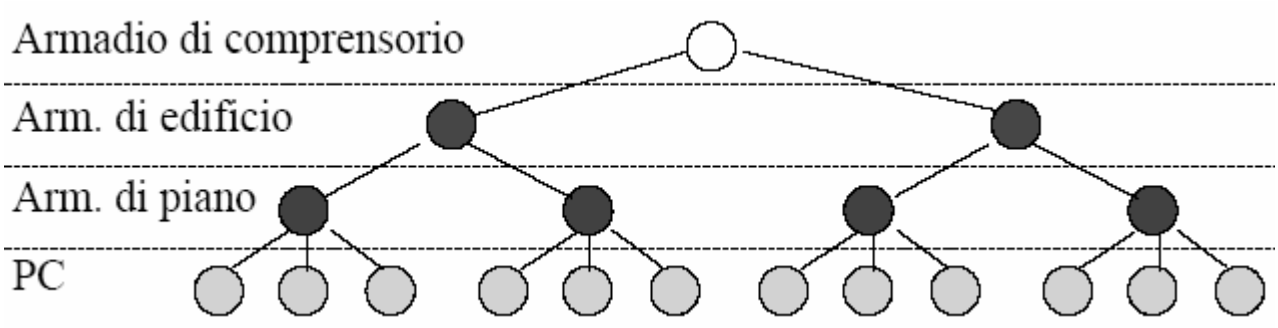
Definiscono l'ambito di adozione:
» Gruppo di edifici appartenenti ad un comprensorio (campus)

Descrivono:
» le topologie ammesse
» elementi facenti parte del cablaggio
» mezzi trasmissivi
» dorsali
» cablaggio orizzontale
» norme per l'installazione
» documentazione
» norme per il collaudo

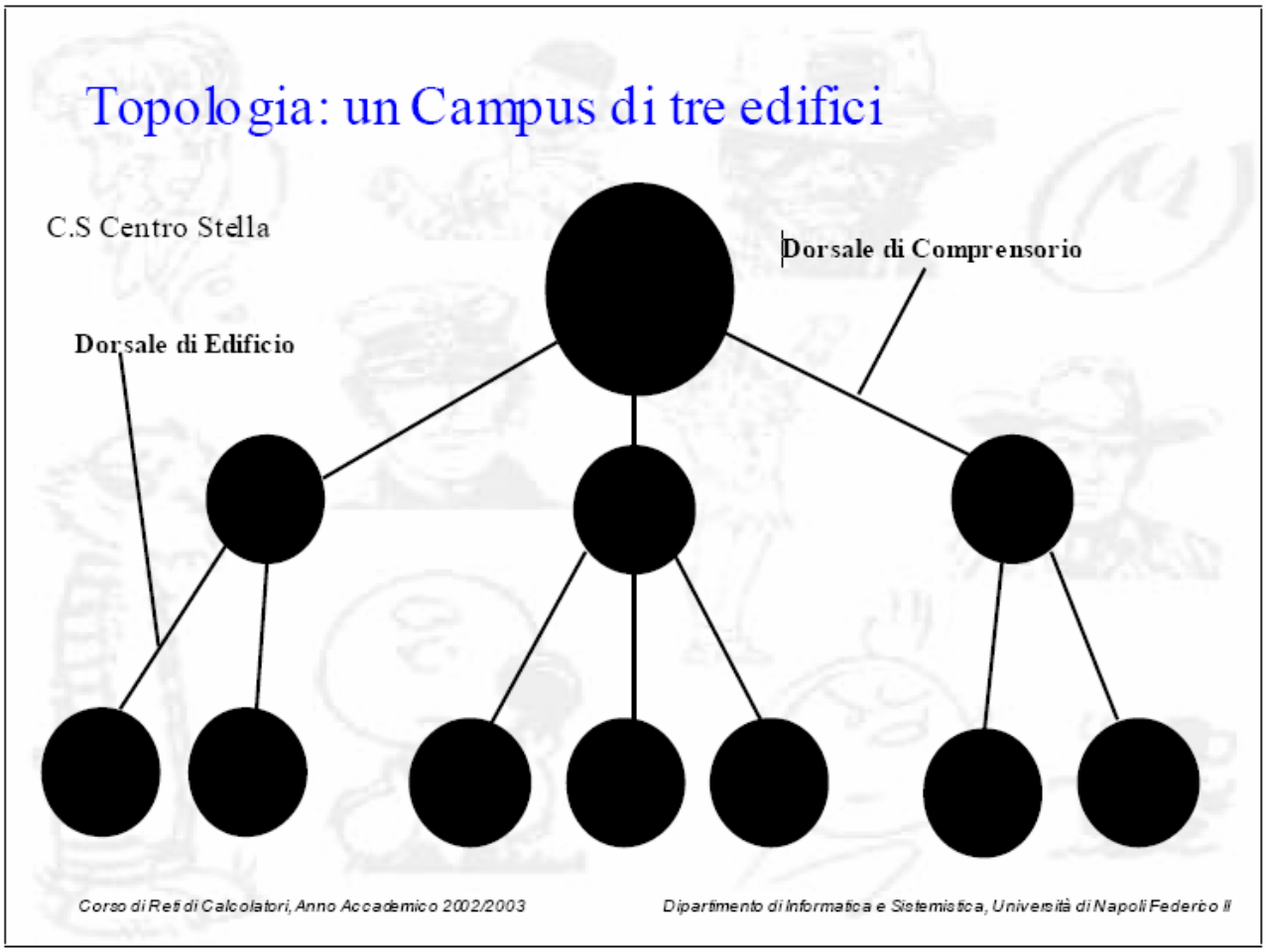
Fissano la durata minima di validità del progetto

Sia EIA/TIA 568A che ISO/IEC 11801 stabiliscono una ***topologia stellare gerarchica*** a tre livelli:

- **primo** livello : centro stella di **comprensorio**
- **secondo** livello : centro stella di **edificio**
- **terzo livello** : centro stella (o armadio) di **piano**

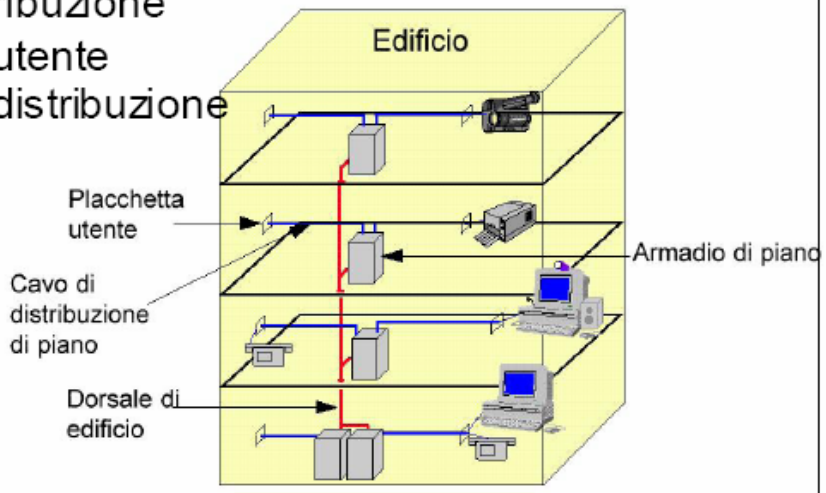


La scelta di una topologia a stella gerarchica deriva dalla necessità di mantenere la massima flessibilità (il cablaggio deve essere valido per almeno 10 anni).



Topologia: Edificio

- Per ogni edificio
  - » Un cavo dorsale di distribuzione.
- Per ogni piano
  - » Un cavo di distribuzione
  - » Più placchette utente
  - » Un armadio di distribuzione



Corso di Reti di Calcolatori, Anno Accademico 2002/2003 *Dipartimento di Informatica e Sistemistica, Università di Napoli Federico II*

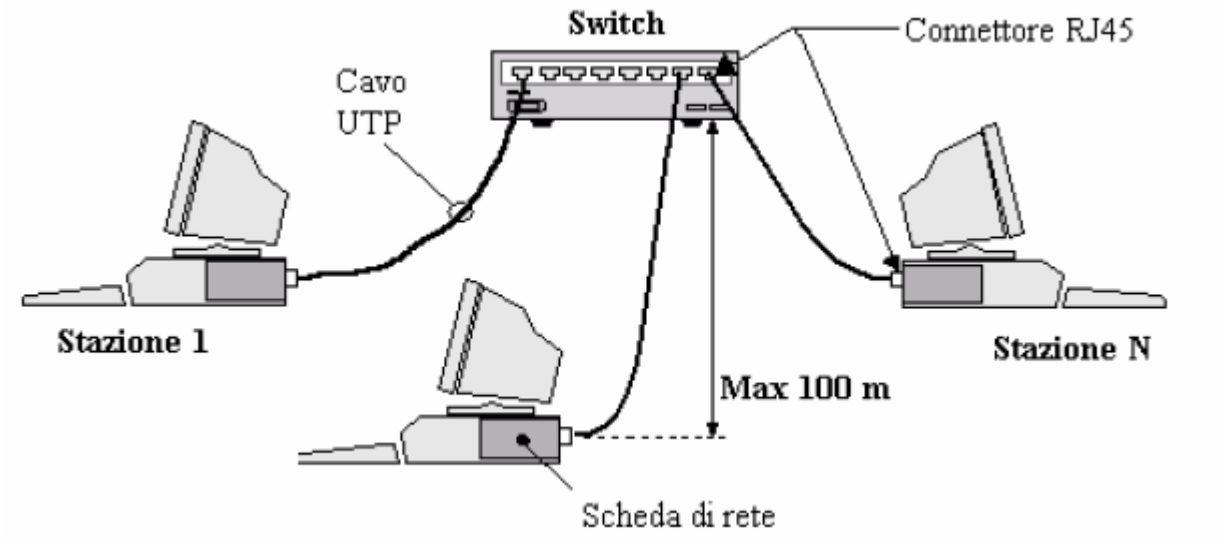
CSMA/CD

CSMA/CD (*carries sense, multiple access with collision detection*) è **un protocollo per reti lineari (a bus)** :

- Ogni nodo prima inviare un msg aspetta che il bus sia libero (carrier sense)
- Ogni computer riceve tutti i msg ma trattiene solo quelli indirizzati a se stesso
- Poiché non si può assumere che un altro nodo non inizi simultaneamente la trasmissione (multiple access), il nodo che invia deve restare in ascolto di eventuali altre trasmissioni che si sovrappongono (collision detection)
- In caso di collisione, i due nodi devono riprovare a inviare i loro messaggi

Topologia utilizzata

Si adotta la topologia a stella con l'impiego di switch come apparati di rete in quanto l'impiego di switch aumenta le prestazioni della rete in quanto riduce il numero di collisioni



Si può, quindi, proporre di installare uno switch in ciascuno dei locali da cablare; gli switch possono essere poi collegati ad uno switch principale che deve avere caratteristiche tecniche più evolute.

I dispositivi di rete

- **Repeater**: dispositivi a due porte che ripetono bit per bit il segnale in ingresso sulla porta di uscita (solo livello fisico)
- Gli **Hub**: repeater multi-porta
- **Bridge**: dispositivi a due porte che operano a livello MAC, e dunque sono capaci di leggere la trama in ingresso su una porta, leggerne gli indirizzi MAC, consultare la tabella di indirizzamento a livello MAC, e inoltrarla o meno sulla porta di uscita. Dividono domini di collisione in una LAN
- Gli **Switch**: bridge multiporta
- I **Router**: dispositivi multiporta che operano a livello Network. Sono responsabili dell'istradamento dei datagrammi IP fra subnet diverse.

(Fonte: http://it.wikipedia.org ; Autore: Luigi Freguglia; eMail: info@lutek.it Licenza: GNU FDL, http://www.gnu.org/licenses/licenses.it.html)

I dispositivi di rete sono nodi che nelle reti informatiche hanno funzionalità esclusivamente orientate a garantire il funzionamento, l'efficienza, l'affidabilità e la scalabilità (la possibilità di evolversi in modo semplice e funzionale verso una struttura di rete con dimensioni maggiori) della rete stessa. Non sono di norma dei calcolatori, anche se un calcolatore può fornire alcune di queste funzionalità, soprattutto ai livelli superiori del modello ISO/OSI.

Essendo apparati attivi, il loro funzionamento dipende da una fonte di energia, che normalmente è l'energia elettrica. Nell'elenco che segue sono indicati alcuni di questi dispositivi, insieme al livello in cui normalmente operano.

repeater (livello 1 - fisico)

Un **repeater** è un dispositivo elettronico che riceve un segnale debole e lo ritrasmette con un segnale più alto e potente, cosicché il segnale può essere garantito a lunghe distanze senza degrado.

Necessario se si devono collegare due punti distanti troppi metri, solitamente più di 50 circa.

hub (livello 1 - fisico)

Nella tecnologia delle reti informatiche, un **hub** (letteramente in inglese *fulcro*, *mozzo*) rappresenta un **concentratore**, un dispositivo di rete che funge da nodo di smistamento di una rete di comunicazione dati organizzata prevalentemente a **stella**.

Nel caso, molto diffuso, delle reti Ethernet, un hub è un dispositivo che inoltra i dati in arrivo da una qualsiasi delle sue porte su tutte le altre. Per questa ragione può essere definito anche un "repeater multiporta". Questo permette a due dispositivi di comunicare attraverso l'hub come se questo non ci fosse, a parte un piccolo ritardo nella trasmissione. La conseguenza del comportamento dell'hub è che la banda totale disponibile viene ridotta ad una frazione di quella originaria, a causa del moltiplicarsi dei dati inviati. Il ritardo introdotto da un hub è generalmente di pochi microsecondi, quindi quasi ininfluente. L'hub è un componente ormai obsoleto e viene sostituito dallo switch.

bridge (livello 2 - data link)

Un **bridge** è un semplice dispositivo di rete che si colloca al livello data link del modello ISO/OSI. Esso è quindi in grado di riconoscere, nei segnali elettrici che riceve dal mezzo trasmissivo, dei dati organizzati in strutture dette *trame* (in inglese frame). In particolare, è in grado di individuare l'indirizzo del nodo mittente e del nodo destinatario di ciascuna trama, sotto forma di indirizzi MAC (cablato nella scheda di rete).

Tipicamente un bridge è munito di porte con cui è collegato a diversi segmenti della rete. Quando riceve una trama su una porta, cerca di capire se il destinatario si trova nello stesso segmento del mittente oppure no. Nel primo caso evita di inoltrare la trama, in quanto presumibilmente il destinatario la ha già ricevuta. Nel secondo caso, invece, il bridge inoltra la trama verso il segmento in cui si trova il destinatario. Se non sa su quale segmento si trova il destinatario, il bridge inoltra la trama su tutte le porte tranne quella da cui l'ha ricevuta. Queste operazioni sono definite operazioni di **filtraggio** e **inoltro**.

switch (livello 2 - data link)

Nella tecnologia delle reti informatiche, uno **switch**, in inglese letteralmente **commutatore**, è un dispositivo di rete che inoltra selettivamente i frame ricevuti verso una porta di uscita.

A differenza di quanto farebbe un hub, uno switch inoltra i frame in arrivo da una qualsiasi delle sue porte *soltanto* a quella cui è collegato il nodo destinatario del frame. Due nodi possono comunicare attraverso uno switch come se questo non ci fosse, ovvero il suo comportamento è **trasparente**.

L'inoltro selettivo dei frame permette a più frame di attraversare contemporaneamente lo switch, e quindi la banda totale disponibile *non* viene ridotta. In una connessione di questo tipo si dice che l'host ha un **accesso dedicato** al commutatore.

La banda disponibile per Internet viene equamente frazionata fra le porte dello switch, ugualmente a quanto avviene per un hub, ed ha un'allocazione statica, per la quale banda resta la medesima anche se non tutte le porte sono collegate ad un cavo Ethernet o se alcuni computer (connessi con cavo Ethernet) non sono collegati ad Internet.

Uno switch possiede l'intelligenza necessaria a riconoscere i confini dei frame nel flusso di bit, immagazzinarli, decidere su quale porta inoltrarli, trasferirli verso una porta in uscita e trasmetterli in funzione dell'indirizzo MAC riconosciuto nella trama (cablato nella scheda di rete).

Tra uno switch e un bridge esistono le seguenti differenze:

- maggiore espandibilità in termini di numero di porte
- performance migliori

router (livello 3 - rete)

Nella tecnologia delle reti informatiche un **router**, in inglese letteralmente *instradatore*, è un dispositivo di rete che si occupa di instradare pacchetti tra reti diverse ed eterogenee.

Un Router lavora al livello 3 (rete) del modello OSI, ed è quindi in grado di interconnettere reti di livello 2 eterogenee, come ad esempio una LAN ethernet con un collegamento geografico in tecnologia ATM (Asynchronous Transfer Mode).

(L'ATM è uno dei sistemi di telecomunicazione maggiormente innovativi che permette un utilizzo delle reti informatiche efficiente, veloce e a 360° in merito alla tipologia di prodotti da poter veicolare tramite la rete. E' un sistema a banda larga che per funzionalità e possibilità di utilizzo potrebbe realizzare quella che viene spesso definita come "L'autostrada Informatica". La realizzazione dell'autostrada informatica permetterebbe, grazie alla capacità e velocità del flusso dei dati in una rete di telecomunicazione, di poter usufruire di qualunque tipo di contenuto multimediale attraverso la rete medesima con la reale possibilità di immettere qualunque tipo di contenuto.)

La funzione di instradamento è basata sugli indirizzi di livello 3 (rete) del modello OSI, a differenza dello switch che instrada sulla base degli indirizzi di livello 2 (collegamento). Gli elementi della tabella di instradamento non sono singoli calcolatori ma reti locali. Questo permette di interconnettere grandi reti, senza crescite incontrollabili della tabella di instradamento.

Rispetto ai bridge, infatti, i router operando a livello 3 non utilizzano il MAC address ma l'indirizzo IP per cui vanno configurati e non sono plug and play.

Per garantire la massima affidabilità e lo sfruttamento ottimale dei collegamenti in caso di reti complesse costituite da molte sottoreti diverse e variamente interconnesse, i router si scambiano periodicamente fra loro informazioni su come raggiungere le varie reti che collegano l'un l'altro, che poi usano per ricavare ed aggiornare delle *tabelle di instradamento* interne da consultare ogni volta che devono smistare i pacchetti di dati in arrivo.

Per fare questo sono stati messi a punto dei protocolli di routing appositi, attraverso i quali i router si scambiano informazioni sulle reti raggiungibili.

Alcuni router possiedono anche un firewall incorporato, poiché il punto di ingresso/uscita di una rete verso l'esterno è ovviamente il luogo migliore dove effettuare controlli sui pacchetti in transito.

Si vanno sempre più diffondendo router che incorporano la funzionalità di access point per reti wireless.

I router possono essere normali computer che fanno girare un software apposito (gateway), o - sempre più spesso - apparati specializzati, dedicati a questo solo scopo. I router di fascia più alta sono basati su architetture hardware specializzate per ottenere prestazioni wire speed, letteralmente alla velocità della linea. Questo significa che un router wire speed può inoltrare pacchetti alla massima velocità delle linee a cui è collegato.

I router di nuova generazione hanno la funzione **"autosensing"** che regola in automatico la velocità tra 10/100(/1000) e la Auto MDI/MDI-X che si accorge anche se il cavo è standard o crossover.

gateway (livello 7 - applicativo)

Il **gateway** (dall'inglese, portone, passaggio) è un dispositivo di rete che opera al livello di rete e superiori del modello ISO/OSI.

Il suo scopo principale è quello di veicolare i pacchetti di rete all'esterno della rete locale (LAN). Da notare che gateway è un termine generico che indica il servizio di inoltro dei pacchetti verso l'esterno; il dispositivo hardware che porterà a termine questo compito è tipicamente un router.

Nelle reti più semplici è presente un solo gateway che inoltra tutto il traffico diretto all'esterno verso la rete internet. In reti più complesse in cui sono presenti parecchie sottoreti, ognuna di queste fa riferimento ad un gateway che si occuperà di instradare il traffico dati verso le altre sottoreti o a rimbalzarlo ad altri gateway.

Spesso i gateway non si limitano a fornire la funzionalità di base di routing ma integrano altri servizi come firewall per la protezione, proxy per il filtraggio sui servizi, etc...

Riepilogo

Per creare una LAN (rete locale), collegando PC, stampanti e altri componenti di Rete che si trovino in una stanza o in stanze vicine, si utilizzano :

- **Hub**
  - Livello 1
  - accentra il segnale
  - soluzione a basso costo e basse prestazioni
- **Switch**
  - Livello 2
  - commuta il segnale in maniera mirata verso punti giusti, riconoscendo gli indirizzi MAC delle schede di rete contenuti nelle trame
  - soluzione a costo maggiore e migliori prestazioni

Per collegare tra loro più reti LAN dello stesso tipo (reti Ethernet, reti Token Ring…) e formarne una più grande, si utilizzano :

- **Bridge**
  - Livello 2
  - commuta il segnale e smista il traffico tra le reti, riconoscendo gli indirizzi MAC delle schede di rete contenuti nelle trame
  - soluzione a basso costo e basse prestazioni
- **Router**
  - Livello 3
  - commuta il segnale e smista il traffico tra le reti, riconoscendo gli indirizzi IP all'interno dei pacchetti
  - può collegare tipi di rete differenti
  - soluzione a costo maggiore e migliori prestazioni

Per collegare tra loro più reti LAN di tipo differente (Ethernet, Token Ring, ATM, Internet…) si utilizza

- **Router**
  - Livello 3
  - commuta il segnale e smista il traffico tra le reti, riconoscendo gli indirizzi IP all'interno dei pacchetti
  - può collegare tipi di rete differenti
  - soluzione a costo maggiore e migliori prestazioni

Il nodo che collega una rete LAN e l'esterno (ad esempio Internet) è genericamente detto

- **Gateway**

  - Livello 7
  - si appoggia alle funzioni del router per smistare il traffico
  - se incorpora funzioni di protezione sul contenuto dei pacchetti potenzialmente dannosi (virus, hackers…) è detto Firewall
  - se incorpora funzioni di filtraggio sul contenuto dei pacchetti in base al servizio richiesto (accesso ai siti, messaggistica istantanea, file sharing…) è detto Proxy
  - solitamente le funzioni di Router, Firewall e Proxy coesistono nello stesso dispositivo Gateway

Cos'è il routing

Per ***routing*** s'intende la funzione fondamentale di **instradamento** dei pacchetti IP, eseguita da dispositivi di rete detti **ROUTER**.

Il router opera secondo i seguenti passi:

1) Riceve su una delle interfacce di ingresso il flusso dati IP

2) Legge l'header IP di ciascun pacchetto, osservando indirizzo IP sorgente e destinazione

3) Opera una funzione decisionale, stabilendo su quale porta di uscita immettere il pacchetto in esame, in base alle informazioni contenute in un'apposita tabella.

4) Instrada il pacchetto sulla porta di uscita stabilita.

Assegnazione degli indirizzi IP ad una rete

- Gli indirizzi devono essere unici in tutta la rete (è possibile attribuire indirizzi arbitrari ad una sottorete TCP/IP solo se questa non è connessa con le altre reti).

- Un indirizzo IP identifica un host e non uno specifico utente. L'identificazione di un utente all'interno di un host è affidata ai protocolli di strato superiore**.** Lo schema d' indirizzamento IP è stato progettato per consentire un efficiente instradamento.

- Un indirizzo IP identifica prima la rete a cui un host è connesso e poi l'host all'interno di quella rete

Supponiamo di avere a disposizione una rete di classe C 192.168.10.0 con subnet mask 255.255.255.0. L'indirizzo 192.168.10.0 rappresenta l'indirizzo di rete, l'indirizzo 192.168.10.255 quello di broadcast.

- Tutti gli altri indirizzi rappresentano indirizzi di host. Con il termine host si identificano tutti i singoli apparati di una rete che sono identificabili con un indirizzo IP, per esempio PC, workstation ,stampanti e gli stessi router

- Un'interfaccia fisica è univocamente riconosciuta attraverso il suo indirizzo MAC (Medium access control), che viene codificato in hardware all'interno della scheda di rete.

- Il protocollo ARP (Address Resolution Protocol) associa ad ogni MAC address un indirizzo IP

- L'indirizzo IP è invece un indirizzo logico ed univoco a livello mondiale. Ogni host può avere più schede di rete e quindi più indirizzi IP appartenenti alla stessa rete o a sottoreti diverse.

- Un *router* è dotato di *varie interfacce di rete*, le quali sono normalmente eterogenee (interfacce di linee seriali, ATM, Ethernet, FastEthernet, FDDI etc). Un router associa a ciascuna interfaccia indirizzi IP diversi. Gli indirizzi associati alle interfacce *DEVONO* appartenere a indirizzi di rete diversi.

- Una stessa interfaccia *FISICA* può recare uno o più indirizzi IP, questo equivale ad associare ad una interfaccia *FISICA* varie interfacce *VIRTUALI*, ciascuna recante un proprio indirizzo IP.

Considerazioni generali

(http://www.pmi.it/networking/articoli/1122/progettiamo-la-rete-ideale.html)

Una rete locale o LAN (Local Area Network) è una rete di dispositivi (Pc, stampanti, Server, Storage e così via) interconnessi tra loro tipicamente tramite cablaggio elettrico o anche per mezzo di interfacce wireless. Le LAN nascono con l'intento di condividere tra i "membri" della rete informazioni, risorse ed eventualmente un accesso al mondo esterno verso altre LAN dislocate in altre parti del mondo per mezzo della rete globale ovvero Internet. Lo scopo quindi di una rete locale è quello di migliorare la fruibilità delle informazioni all'interno di una struttura aziendale al fine di migliorare ed accrescere la produttività globale. Per raggiungere lo scopo prefissato è necessario che la LAN rispetti i seguenti requisiti:

- Elevata velocità;
- Rapporto prezzo/prestazioni ottimale;
- Scalabilità;
- Affidabilità;
- Sicurezza.

Le reti normalmente utilizzate sono reti di tipo Ethernet con topologia a Stella Gerarchica.

Componenti essenziali

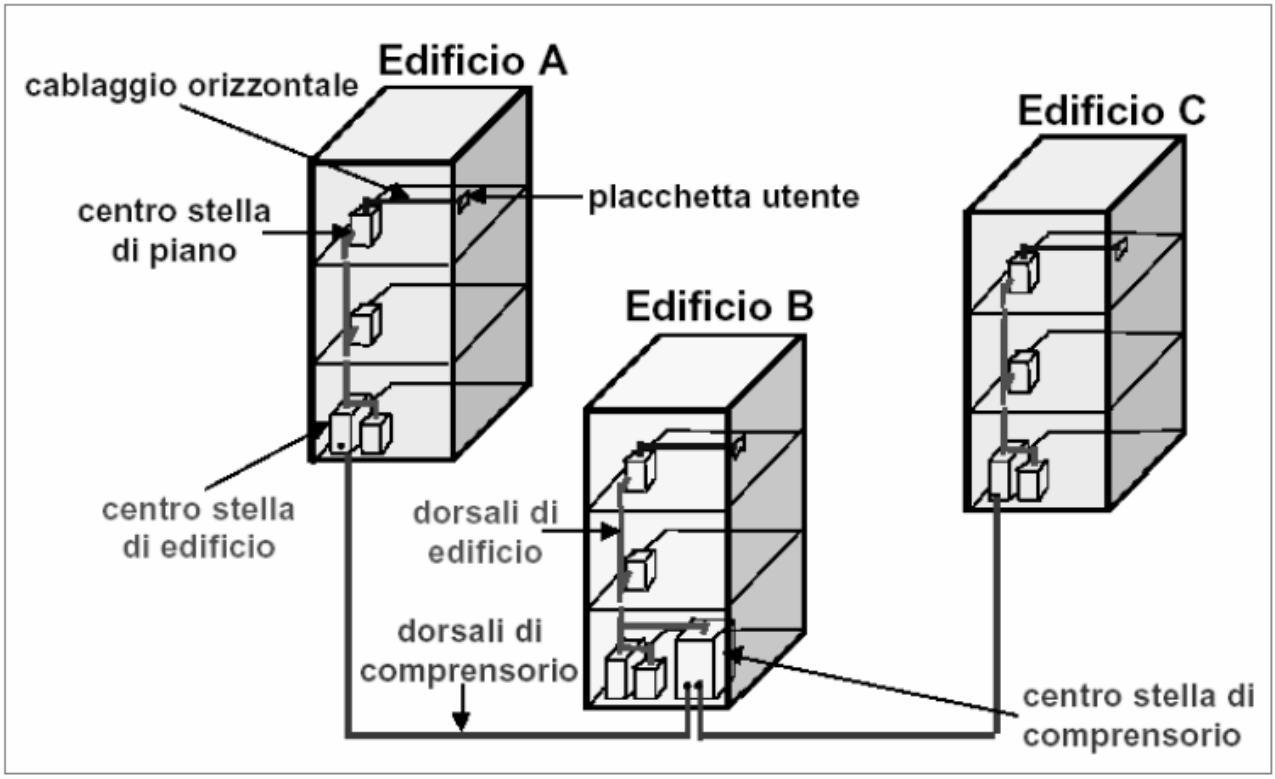
L'infrastruttura fisica di un LAN è costituita da elementi passivi (Cablaggio Strutturato) ed elementi attivi (Apparati) Dal punto di vista normativo nel 2002 sono state emanate due nuove direttive a completamento delle precedenti EN (European Norm) e EIA/TIA (Electronic Industry Association/Telecommunication Industry Association) mentre dal punto di vista legislativo occorre tenere in considerazione che tutte le installazioni devono necessariamente rispettare le normative nazionali per gli impianti tecnici. Nell'ambito delle "regole" di cablaggio si farà sempre riferimento alla norma EIA/TIA 568B-2.1 nella quale si definiscono i mezzi trasmessivi con banda passante di 250MHz ovvero di categoria 6 e alle direttive EN50173-1--ISO/IEC11801 che standardizzano le procedure generali di cablaggio per telecomunicazioni.

Le direttive precedentemente citate prevedono la suddivisione della topologia di rete in 3 livelli gerarchici

- 1° livello: centro stella di comprensorio o di campus;
- 2° livello: centro stella di edificio;
- 3° livello: centro stella di piano;

da cui è possibile derivare sottosistemi funzionali di cablaggio collegati tra loro in modo da costituire quello che viene definito sistema di cablaggio generico.

Di seguito è illustrato il modello generale per il cablaggio strutturato gerarchico a 3 livelli.



Consideriamo ora il caso di un edificio con un solo piano corrispondente ad un ufficio di medie dimensioni comprendente mediamente 10 postazioni di lavoro.

I componenti necessari per la realizzazione del cablaggio strutturato di cui sopra sono i seguenti:

1. Armadio o quadro di distribuzione di ufficio;
2. Pannello di distribuzione o Patch Panel o Permutatore;
3. Patch cord per l'interconnessione tra linee entranti e le linee uscenti del Patch Panel;
4. Patch cord per l'interconnessione tra la Presa Utente e la postazione di lavoro (PC, Stampante, etc);
5. Patch cord per l'interconnessione tra il Patch Panel e l'elemento attivo (Router, Switch, ect);
6. Bretelle per l'interconnessione tra il Patch Panel e la Presa Utente;
7. Prese Utente

La lunghezza massima del cablaggio orizzontale, ovvero dell'interconnessione tra il quadro di distribuzione e la postazione di lavoro, è di **95 metri** tenendo in considerazione che la lunghezza della bretella tra il permutatore e la presa utente non deve superare i 90 m.

Per la realizzazione di un cablaggio ottimale si deve inoltre prevedere, con opere edilizie appropriate, spazi dedicati per l'installazione degli armadi e per canalizzazioni, inoltre occorre tener presenti alcuni accorgimenti inerenti la posa in opera come il

numero massimo dei cavi, distanza minima rispetto alle linee elettriche e così via; dati che possono essere reperiti direttamente dal fornitore dei materiali. L'ultima fase del cablaggio strutturato è il collaudo per certificare che ogni singola tratta sia rispondente alle direttive previste dalle normative EIA/TIA568B-2.1 e EN50173-1.

Per completare l'infrastruttura di rete è necessario connettere le terminazioni cablate a degli elementi attivi che rappresentano l'essenza stessa della LAN. Tradizionalmente le reti locali sono state sempre implementate per lavorare con velocità di 10Mbps o 100Mbps e in tale ottica gli elementi attivi che interconnettevano i vari utilizzatori supportavano velocità fino a 100Mbps.

Attualmente però l'esigenza di scambio di informazioni tra gli utenti di una LAN è notevolmente aumentata e gli apparati in grado di supportare velocità superiori. In questo contesto è consigliabile nel progettare una LAN, considerare l'installazione di apparati di interconnessione o Switch in grado di supportare velocità multiple fino a 1Gbps (10, 100, 1000 Mbps).

Prima di acquistare lo switch è bene pianificare il numero delle stampanti di rete, degli access point, dei server, dei router, e così via presenti all'interno della struttura oltre al numero delle postazioni lavoro che era stato fissato precedentemente a 10.

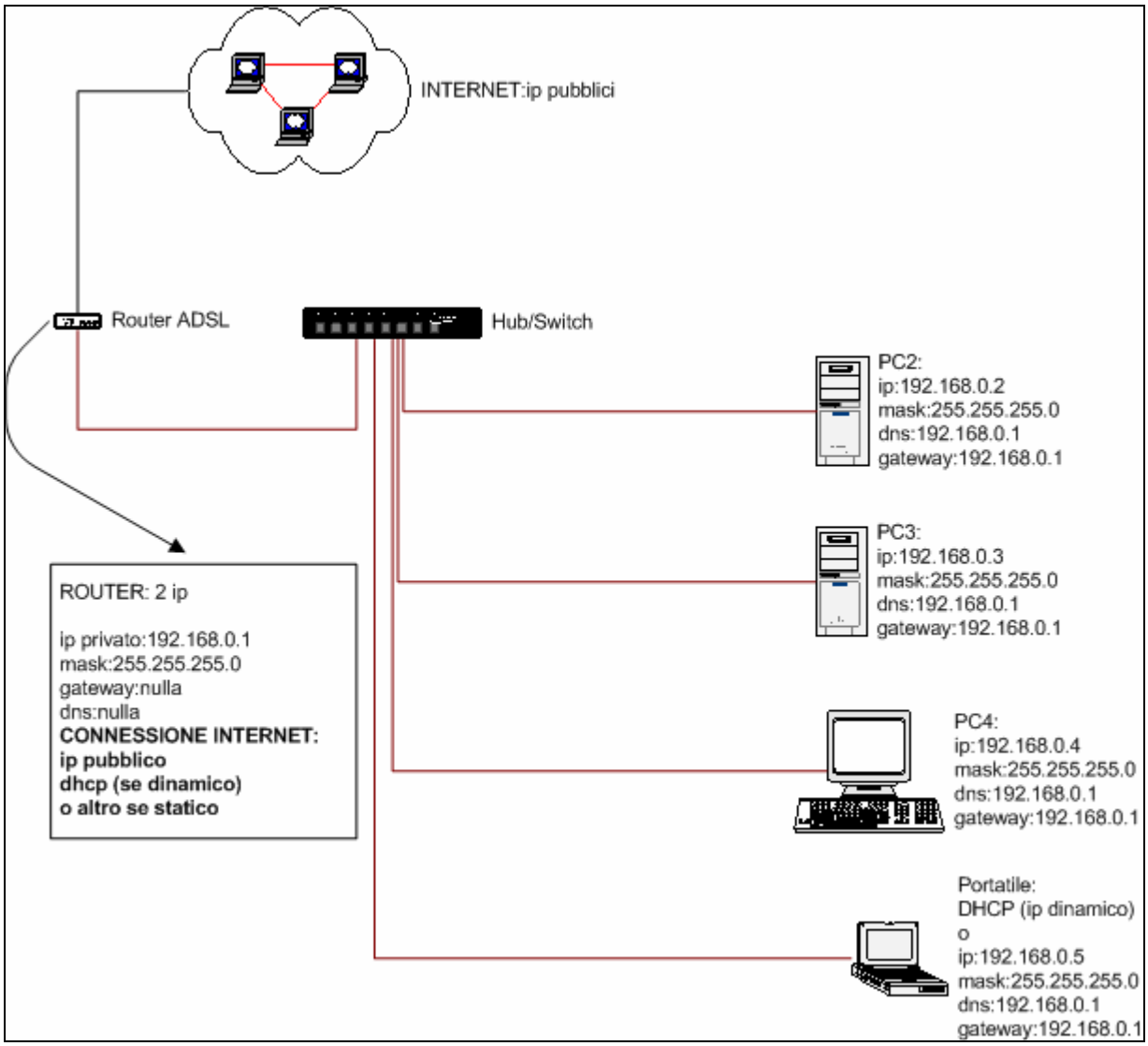
Collegamento e condivisione di una Lan ad Internet

Esempio di una rete con x PC e un Router

Schema generale per una semplice rete locale di pochi PC che condividono una connessione ad internet. I PC della rete hanno indirizzi privati (statici e/o dinamici).

Materiale necessario:

- x PC
- Router ADSL (linea ADSL attiva)
- x schede di rete
- x +1 cavi ethernet dritti
- Hub/Switch



Come funziona l'ADSL

(http://assistenza.tiscali.it/adsl/funzionamento/)

Per poter usufruire della tecnologia ADSL occorrono una linea telefonica analogica, un computer, un modem ADSL e un filtro che permette di separare il traffico voce da quello dati.

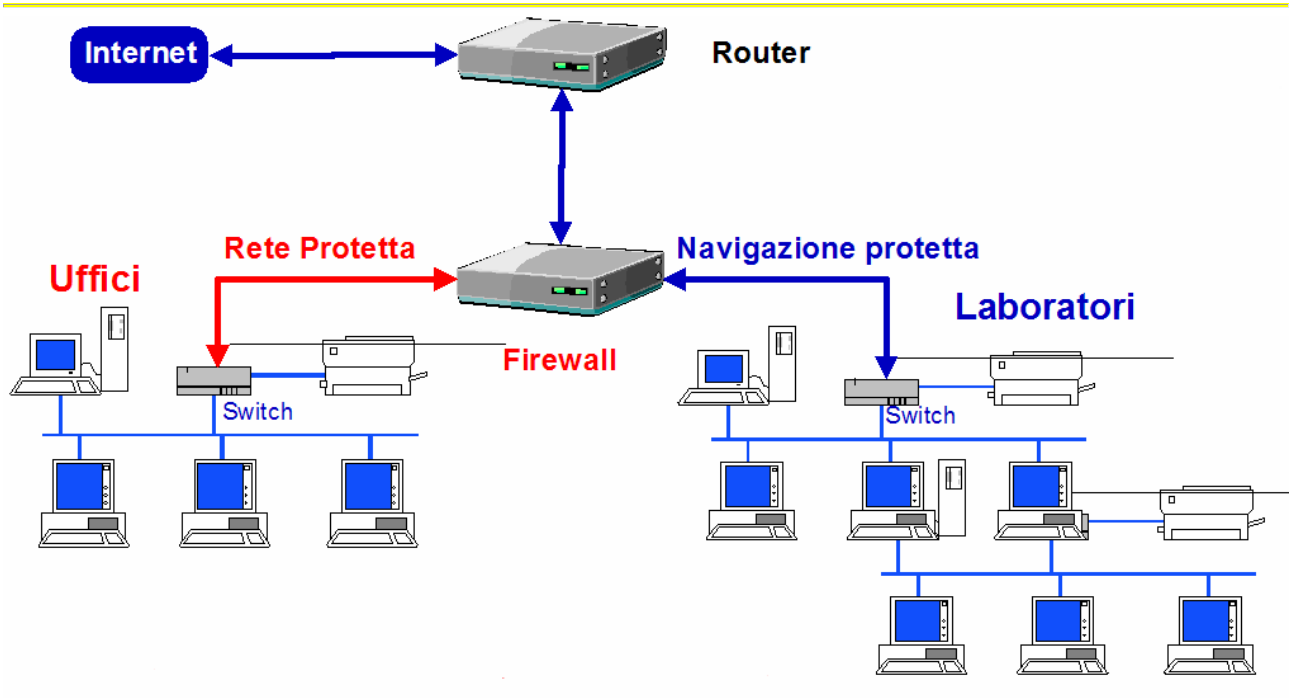
Il **modem ADSL** ha la funzione di collegare, attraverso la tradizionale linea telefonica analogica, il computer da cui parte la richiesta di connessione ad Internet al computer del provider (ad esempio Tiscali) fornitore della connettività. Il modem codifica i dati digitali emessi dal computer utilizzato per la connessione in dati analogici, affinché questi possano viaggiare lungo il normale cavo telefonico (doppino). Una volta giunti a destinazione, i dati analogici vengono poi decodificati in dati digitali.

In una comune linea analogica ad uso domestico, il **filtro** ha il compito di separare il flusso dati da quello voce. Pertanto, esso permette alla sola trasmissione voce di raggiungere il terminale telefonico collegato, bloccando a monte quella dati che altrimenti potrebbe dar luogo a disturbi e fruscii nel modem ADSL.

Velocità di download/upload: l'ADSL è un servizio a funzionamento asimmetrico, il che significa che la velocità di upload (caricamento *verso* Internet) è normalmente molto inferiore della velocità di download (scaricamento *da* Internet).

Linea ADSL

- Utilizza il classico doppino telefonico, non è necessario quindi sostenere i costi di una nuova linea nel caso già sia attiva una linea analogica;
- Permette di essere in Internet 24 ore su 24, avere la linea telefonica sempre libera e non pagare il traffico telefonico per navigare, quindi la spesa è sempre certa;
- Velocità di download 640kb/s e upload 128kb/s (velocità nominali);



da www.itismajo.it/csas/Tutorial/Liberalizzazione%20accessi%20delle%20scuole.ppt

Reti & Servizi

(http://profs.sci.univr.it/~colombar/lab_periodo_zero_2006/pdf/Lez6_Reti_e_Servizi.pdf)

TCP/IP: indirizzamento

Schema di indirizzamento generale su due livelli: **Indirizzo IP + Porta TCP**

- **Indirizzo IP**
  - Indirizzo associato a ogni calcolatore collegato a una sottorete.
  - Si tratta di un indirizzo **Internet** globale unico.
- **Porta TCP**
  - Indirizzo unico all'interno dell'host che individua un processo attivo sull'host.
  - Utilizzato da TCP per consegnare i dati al processo giusto.

Gli indirizzi IP sono machine-oriented, quindi difficili da utilizzare per un utente "umano".

- È stato definito un sistema per passare da indirizzi numerici (gli indirizzi IP) a nomi facilmente memorizzabili: il Domain Name System
- Domain Name System (DNS)
  - Associa a ogni indirizzo IP uno o più indirizzi simbolici.
  - Gestisce la conversione tra indirizzi simbolici e indirizzi IP.
- Organizzato in maniera gerarchica (domini, sotto-domini, sotto-sotto-domini, …) per semplificarne l'utilizzo.

DNS

- Il nome DNS di un calcolatore è costituito da una successione di stringhe alfanumeriche separate da punti (per esempio, server1.isttec.liuc.it)
- Ogni stringa identifica un "dominio":
  - La stringa più a destra rappresenta il dominio di primo livello (detto anche dominio generale).
  - La seconda stringa, sempre proseguendo da destra verso sinistra, indica il dominio di secondo livello.
  - Le stringhe successive indicano i domini di terzo livello (sottodomini dei domini di secondo livello), quelli di quarto livello, e così via finché non si arriva a individuare un dominio che comprende il singolo host.

Il Protocollo http

- HTTP (Hypertext Transfer Protocol) è l'insiemedi regole utilizzato per controllare l'invio e la ricezione di documenti HTML via Internet.
- Il protocollo HTTP fornisce le regole mediante le quali i browser effettuano le richieste e i server forniscono le relative risposte.
- Documentazione: RFC 2616 (http://www.freesoft.org/CIE/RFC/index.htm) versione aggiornata delle specifiche del protocollo HTTP versione 1.1.

La richiesta HTTP

Operazioni di base:

1. Un'applicazione client (browser Web) apre una connessione verso la porta HTTP del server Web (normalmente la porta 80).
2. Il client invia una richiesta attraverso la connessione aperta.
3. Il server Web analizza la richiesta ed individua la risorsa specificata.
4. Il server invia una copia della risorsa.
5. Il server chiude la connessione.

URL

- L'URL (Uniform Resource Locator) si può tradurre come localizzatore univoco di risorse
- E' lo strumento con il quale si rappresentano le coordinate di un sito o di una informazione presente su Internet
- L'URL utilizza i nomi simbolici forniti dal sistema DNS per poter localizzare file, pagine HTML, immagini, o quant'altro
- L'URL non è altro che una stringa che specifica:
  - il protocollo da seguire per richiedere la risorsa
  - l'indirizzo IP (o più semplicemente il corrispondente DNS) per localizzare la risorsa nella rete
  - Il nome della risorsa

- Esempio: **http://profs.sci.univr.it/~colombar**

  Identifica la home dell'utente colombar sulla macchina data dal DNS **profs.sci.univr.it** e http specifica il fatto che si stanno cercando documenti html, in quanto http è il protocollo che gestisce la richiesta di pagine html

Connessione al Server Web

- Normalmente un server Web riceve le richieste sulla porta 80, in questo caso l'indirizzo **http://profs.sci.univr.it/~oliboni/index.html** fa riferimento al documento **~oliboni/index.html** sul server Web in esecuzione sull'host **profs.sci.univr.it** e operante sulla porta standard 80.
- Se invece il server Web utilizzasse la porta 8080, l'indirizzo dovrebbe essere: **http://profs.sci.univr.it:8080/~oliboni/index.html**

Panoramica su altri protocolli

- **SMTP** (Simple Mail Transfer Protocol) è il protocollo standard per la trasmissione via internet di e-mail. In italiano si potrebbe tradurre come "Protocollo elementare di trasferimento postale".
  - È un protocollo relativamente semplice, testuale, nel quale vengono specificati uno o più destinatari, verificata la loro esistenza, e infine il messaggio viene trasferito.
  - SMTP era un protocollo testuale, quindi non permetteva di trasmettere direttamente file binari. Furono dunque sviluppati standard come il MIME per la codifica dei file binari ed il loro trasferimento attraverso SMTP.
  - L'SMTP è un protocollo che permette soltanto di inviare messaggi di posta, ma non di richiederli ad un server: per fare questo il client può usare POP o IMAP.

- **POP** (Post Office Protocol) (attualmente utilizzato nella versione 3 - **POP3**) è un protocollo che ha il compito di permettere, mediante autenticazione, l'accesso ad un account di posta elettronica presente su di un server per scaricare le e-mail del relativo account.
  - I messaggi di posta elettronica, per essere letti, devono essere scaricati sul computer
  - Anche se è possibile lasciarne una copia sul server
  - Password spedite in chiaro

- **IMAP** (Internet Message Access Protocol) è un protocollo di comunicazione per la ricezione di e-mail. Alternativa più moderna all'utilizzatissimo POP. Entrambi permettono ad un client di accedere, leggere e cancellare le e-mail da un server, ma con alcune differenze:
  - Accesso alla posta sia on-line che off-line
  - Più utenti possono utilizzare la stessa casella di posta
  - Supporto all'accesso a singole parti MIME di un messaggio (es: scaricare una mail senza i file allegati)
  - Supporto per attributi dei messaggi tenuti dal server (già letto, da leggere, importante, lavoro, ecc…)
  - Accesso a molteplici caselle di posta sul server
  - Possibilità di fare ricerche sul server
  - Password criptate

- **FTP** (File Transfer Protocol) è un servizio che fornisce gli elementi fondamentali per la condivisione di file tra computer interconnessi. Gli obiettivi dell'FTP sono:
  - promuovere la condivisione di file (programmi o dati)
  - incoraggiare l'uso indiretto o implicito (tramite programma) di computer remoti
  - trasferire dati in maniera affidabile ed efficiente

- **Telnet** è solitamente utilizzato per fornire all'utente sessioni di login remoto di tipo linea di comando tra computer su internet.

- **SSH** (Secure SHell, shell sicura) è una versione sicura di Telnet:
  - Sia l'autenticazione che la sessione di lavoro avviene in maniera cifrata.
  - SSH è diventato uno standard di fatto per l'amministrazione remota di sistemi unix e di dispositivi di rete

Gli schemi tipici di collegamento verso internet

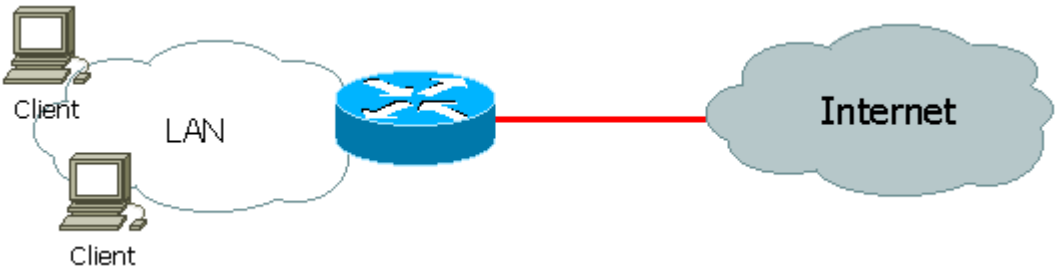
(http://www.comnet.easyict.it/1001300206/portal_ne=1001300206&cp=22975&l=1&d=MPS&pt=&pg=1&ids=0&id1=.htm)

LAN Semplice

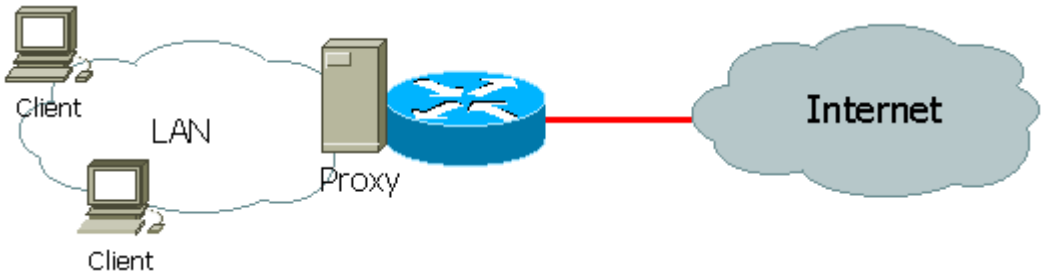
In questo scenario si possono collocare tutte quelle strutture che hanno una rete locale costituita da un piccolo numero di computer e che utilizzano un server per condividere l'accesso ad Internet tramite un modem. In tale caso il server è connesso ad un modem che si collega in dial-up (connessione tra computer realizzate con dei modem tramite la composizione di una normale numerazione telefonica) su linea ISDN o analogica e condivide la sua connessione ad Internet con tutti gli altri utenti della rete.

LAN con router di raccolta

Lo scenario descritto dallo schema seguente rappresenta una realtà con una propria rete locale, con un certo numero di computer collegati ad Internet tramite un router (collegamento di tipo ISDN oppure su linea dedicata ADSL).



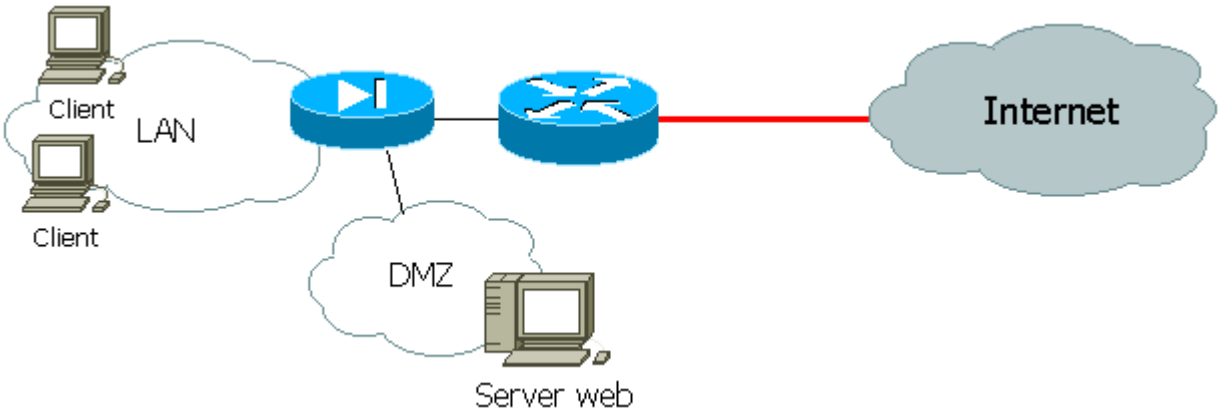
Questo scenario è un caso particolare del precedente, ma molto frequente in diverse realtà. E' soprattutto utilizzato per aumentare i livelli di sicurezza e per regolamentare gli accessi verso Internet.



In pratica si ha la stessa situazione dello scenario precedente, solo che viene utilizzato un server Proxy per permettere l'accesso sicuro, protetto e regolamentato verso Internet.

LAN con DMZ

Infine si presenta lo scenario più articolato, simbolo di realtà alquanto complesse.



Si può osservare una suddivisione della rete locale in diverse componenti: la rete interna e la zona DMZ. L'accesso ad Internet è garantito da un router ed è protetto da un firewall. In tale situazione rientrano anche le realtà ancora più complesse che prevedono una serie di uffici distaccati con le proprie reti locali e che fanno riferimento ad un unico router di raccolta.

La sicurezza nei sistemi informativi

(dal sito :http://www.villaumbra.org/resources/Documenti/Regione/sicurezza%20S.I.pdf)

Rendere un sistema informativo sicuro non significa solo attuare un insieme di contromisure specifiche (di carattere tecnologico ed organizzativo) che neutralizzi tutti gli attacchi ipotizzabili per quel sistema; significa anche collocare ciascuna contromisura in una politica organica di sicurezza che tenga conto dei vincoli (tecnici, logistici, amministrativi, politici) imposti dalla struttura in cui il sistema informativo opera, e che giustifichi ciascuna contromisura in un quadro complessivo.

1. Definizione e concetti di base

1.1. Definizione

Con il termine ***"sicurezza"***, nell'ambito dei sistemi informativi, si intende l'insieme delle misure (di carattere organizzativo e tecnologico) tese ad assicurare a ciascun utente autorizzato (e a nessun altro) tutti e soli i servizi previsti per quell'utente, nei tempi e nelle modalità previste. Più formalmente, secondo la definizione ISO, la *sicurezza* *è l'insieme delle misure atte a garantire la disponibilità, la integrità e la riservatezza delle informazioni gestite.*

1.2. Disponibilità controllata delle informazioni

Il sistema deve rendere disponibili a ciascun utente abilitato le informazioni alle quali ha diritto di accedere, nei tempi e nei modi previsti.

Nei sistemi informatici, i requisiti di disponibilità sono legati anche a quelli di prestazione e di robustezza. La disponibilità di una informazione ad un utente, infatti, deve essere assicurata in modo ininterrotto durante tutto il periodo di tempo previsto (continuità del servizio).

Il raggiungimento dell'obiettivo disponibilità dipende quindi da fattori critici come la robustezza del software di base e di quello applicativo, l'affidabilità delle apparecchiature e degli ambienti in cui sono collocati, l'esperienza e l'affidabilità degli amministratori del sistema. Non è in generale buona norma assumere che le contromisure adottate in un sistema informatico siano sufficienti a scongiurare qualsiasi attacco. Rientra quindi fra gli obiettivi di una politica di sicurezza quello di garantire il rientro in funzione in tempo utile del sistema informatico, a seguito di eventi negativi anche gravi.

1.3. Integrità delle informazioni

Il sistema deve impedire la alterazione diretta o indiretta delle informazioni, sia da parte di utenti e processi non autorizzati, che a seguito di eventi accidentali. Anche la perdita di dati (per esempio a seguito di cancellazione o danneggiamento), viene considerata come alterazione.

1.4. Riservatezza delle informazioni

Il sistema deve impedire a chiunque di ottenere o dedurre, direttamente o indirettamente, informazioni che non è autorizzato a conoscere. Vale la pena di osservare che, in determinati contesti, il fatto stesso che una informazione sia protetta, o che esista una comunicazione in atto fra due utenti o processi, può essere sufficiente per dedurre informazioni riservate.

2. Risorse di un sistema

Le ***risorse di un sistema informativo*** sono l'insieme delle entità (dagli operatori alle componenti hardware, dal software di base a quello applicativo) necessarie al suo funzionamento.

Dal punto di vista della sicurezza, non è importante distinguere fra le risorse che *costituiscono* il sistema (i.e. le sue componenti) e le risorse delle quali ha bisogno per funzionare: si tratta in ogni caso di risorse "critiche" e quindi da proteggere.

Per proteggere un sistema occorre innanzitutto identificarne le risorse e valutare il rischio legato agli eventi (indesiderati) che possano minacciarne la integrità.

Una classificazione delle tipologie di risorsa comunemente presenti in un sistema informativo è utile per procedere in modo sistematico ed esaustivo nella identificazione delle risorse stesse. Possiamo in particolare distinguere fra ***risorse fisiche*** e ***logiche.***

Le principali risorse fisiche solitamente presenti in un sistema informativo moderno sono calcolatori (server e postazioni di lavoro), periferiche (scanner, stampanti, modem), apparecchiature di rete, i locali che ospitano le apparecchiature e gli impianti di alimentazione e condizionamento di tali locali. Vale la pena osservare che anche gli operatori umani possono essere considerati per certi aspetti come risorse fisiche.

Le risorse logiche presenti in un sistema informativo moderno sono tipicamente i moduli del software applicativo e del software di base (DBMS, Sistema Operativo, Software di Rete), le basi di dati, i registri di configurazione dei dispositivi (per esempio router).

Anche in questo caso, possono essere considerate come risorse logiche anche l'insieme delle regole organizzative e comportamentali degli operatori umani.

4. Eventi indesiderati

Una volta individuate le risorse critiche, si deve stabilire quali eventi indesiderati possano determinarne un degrado nelle caratteristiche di integrità, disponibilità e riservatezza.

Una definizione precisa di "***evento indesiderato***" permette di verificare, a fronte di una analisi sistematica di tutti gli eventi che potrebbero accadere intorno al sistema, se

e quanto ciascun evento sia indesiderato rispetto alla definizione data. Un buon punto di partenza è costituito dal considerare come *evento indesiderato qualsiasi accesso* (a servizio o informazione) *che non sia esplicitamente permesso dalla politica di sicurezza del sistema.*

L'insieme degli eventi indesiderati, tuttavia, è ben più esteso, in quanto comprende eventi che non sono affatto degli attacchi deliberati, bensì dei semplici eventi accidentali.

Stando alle statistiche, anzi, gli eventi accidentali quali il guasto di un dispositivo o l'errore umano (per esempio cancellazione accidentale di file, installazione di componenti incompatibili o infettate che corrompono il software di base) restano la principale causa di perdita accidentale di dati. Per questo motivo il titolo di questa sezione fa riferimento al concetto più generale di "evento indesiderato".

Allo scopo di affrontare il problema in modo sistematico, classifichiamo quindi gli eventi indesiderati a seconda che siano accidentali o piuttosto conseguenza di un attacco deliberato. Analogamente a quanto visto per le risorse, una classificazione degli eventi indesiderati risulta utile per affrontare la loro identificazione con sistematicità.

4.1. Attacchi deliberati

Nel classificare l'insieme dei possibili attacchi al sistema, è importante partire dal presupposto che chiunque tenti di penetrarvi o danneggiarlo applicherà, in sequenza o in parallelo (sfruttando eventuali effetti combinati), tutte le tecniche di cui dispone su tutte componenti attaccabili.

4.1.1. Attacchi a livello fisico

Gli attacchi a livello fisico sono principalmente tesi a sottrarre o danneggiare risorse critiche. I principali tipi di attacco a livello fisico sono:

- **furto**: prevedibile per nastri di backup, dischi o interi server; è un attacco alla disponibilità ed alla riservatezza;
- **danneggiamento**: attacco tipicamente condotto contro apparecchiature e cavi di rete, più raramente contro calcolatori server in quanto questi sono generalmente confinati in locali sicuri; è un attacco alla disponibilità ed alla integrità.

4.1.2. Attacchi a livello logico

Gli attacchi a livello logico sono principalmente tesi a sottrarre informazione o degradare la operatività del sistema.

4.2. Eventi accidentali

Parallelamente a quanto fatto per gli attacchi deliberati, caratterizziamo un evento accidentale in funzione della componente che lo subisce e del fattore ambientale che lo scatena. Un approccio sistematico individua, per ciascuna componente fisica o logica del sistema, tutti i fattori potenzialmente pericolosi per quella componente.

Stando alle statistiche, il fattore umano (per esempio cancellazione accidentale di file, installazione di componenti incompatibili o infettate che corrompono il software di base) resta la principale causa di perdita accidentale di dati. Per quanto riguarda gli eventi accidentali di altra origine, accanto ai guasti più frequenti (dischi, alimentatori, memoria, etc.) occorre valutare anche i guasti a dispositivi di supporto come condizionatori d'aria o trasformatori di potenza, ed eventi disastrosi come l'incendio o l'allagamento della sala CED.

Considerazioni finali

I principali problemi relativi alla sicurezza dei sistemi informatici riguardano di versi aspetti :

- calamità naturali
- guasti ed interruzioni hardware
- errori del personale
- virus
- archivi

I problemi di sicurezza legati agli archivi riguardano fondamentalmente gli aspetti relativi alla perdita di dati e all'accesso alle informazioni contenute da parte di persone non autorizzate. Il primo problema si può risolvere con un'accurata politica di backup degli archivi (copie di salvataggio), la cui frequenza può essere anche giornaliera. Per quanto riguarda gli accessi alle informazioni contenute negli archivi è consigliabile associare ad ogni utente, che può accedere agli archivi, un **profilo** il cui accesso può essere controllato mediante una password. Al profilo possono essere associate diverse azioni che l'utente può compiere sui dati (sola lettura, consultazione parziale dei dati, possibilità di aggiornamento dei dati, ecc.). Tali controlli possono essere effettuati a vari livelli sistema operativo, gestore della base di dati (DBMS), applicazioni che gestiscono i database.

Problemi di sicurezza nelle reti

I problemi di sicurezza e del controllo degli accessi aumentano se i computer di una azienda sono collegati in rete e se la rete è accessibile dall'esterno della rete, come può avvenire nel caso in cui la stessa rete è collegata ad Internet.

In questo caso è opportuno proteggere eventuali attacchi ed intrusioni alla rete dell'azienda effettuando un controllo rigoroso degli ingressi nella rete e degli accessi agli archivi che costituiscono il sistema informativo dell'azienda. In tal caso occorre dotarsi di opportuni ***sistemi di identificazione*** che consentono di autenticare qualsiasi accesso alla rete ed, inoltre, di ***sistemi di log*** che consentono di tener traccia di qualsiasi operazione venga effettuata dopo l'autenticazione.

Firewall

(dal sito : http://www.osservatoriotecnologico.it/reti/sicurezza/firewall.html)

La **"Sicurezza"** è un processo che deve garantire la riservatezza delle comunicazioni, l'integrità di dati e applicazioni (modificabili solo da coloro che ne hanno la titolarità), la disponibilità continua del sistema.

Cosa vogliamo proteggere e da chi?

Il Curioso**:** vuole capire che tipo di dati e di sistema avete

Il Malizioso**:** mettere fuori uso il vostro sistema o renderlo non operante

L' Intrusore di alto profilo: usare il vostro sistema per guadagnare popolarità o fama

La Concorrenza: interesse nei dati che avete sul vostro sistema

Lo Sfruttatore: sfruttare il vostro sistema per usare le sue risorse

In altre parole possiamo dire che per mezzo delle reti locali si "trattano" dati che non vengono considerati pubblici e che di conseguenza debbono essere protetti, ovvero garantire le seguenti proprietà:

Confidenzialità

I dati devono poter essere esaminati solamente dagli addetti al loro trattamento.

Integrità

I dati non devono essere alterati, sia che risiedano stabilmente su un solo sistema (stand alone), sia che vengano trasmessi.

I dati trattati possono essere :

- **Dato anonimo**: il dato che in origine, o a seguito di trattamento, non può essere associato a un interessato identificato o identificabile.
- **Dato personale**: "qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati od identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione ivi compreso un numero di identificazione personale".
- **Dati sensibili**: i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

Da un punto di vista più generale possiamo indicare due aspetti:

Integrità dei sistemi

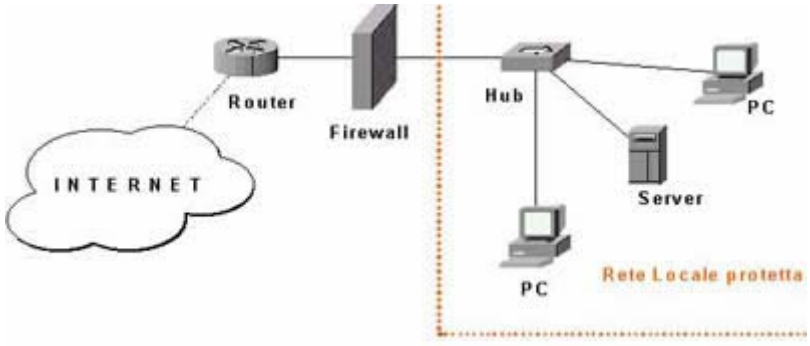
Si riferisce all'uso di un sistema così come previsto dall'amministratore, ovvero l'utilizzo da parte di un utente autorizzato con privilegi non superiori a quelli che gli sono stati assegnati; un sistema si considera compromesso quando ospita dati che non possono più essere considerati confidenziali o integri e/o quando i programmi eseguibili in esso ospitati sono stati alterati all'insaputa dell'amministratore e dell'utente abituale. In alcuni casi è possibile recuperare l'integrità del sistema, spesso è però consigliabile formattare il disco rigido (hard disk), reinstallare il sistema operativo, reinstallare i programmi applicativi dagli originali, ripristinare i dati con l'ultima copia di salvataggio antecedente la data della compromissione.

Disponibilità dei sistemi e della rete

Un sistema o una rete che non risponde agli utenti è definito/a non disponibile. Per esempio se alcuni cyber-vandali compromettono un sistema e lanciano numerosi agenti software (programmi) per attaccare un altro computer (DDoS Distributed Denial of Service) provocano una indisponibiltà, almeno parziale, del sistema compromesso. Come altro esempio se alcuni utenti di una rete aprono sessioni multiple per scaricare file di tipo musicale e/o video è possibile che saturino la banda disponibile (la quantità di informazione scaricabile nell'unità di tempo) e generino l'indisponibilità della rete.

Terminata la causa che ha generato l'indisponibiltà, in genere, il sistema e/o la rete ritornano disponibili.

La forma più diffusa di protezione è costituita dal **firewall**, ovvero un sistema che isola una rete dall'altra (p.es. la rete pubblica da quella privata). Esso può essere un router, un computer su cui è in funzione un software particolare, un dispositivo dedicato (sebbene questo possa essere assimilato a un router o a un computer dedicato). In altre parole il firewall è un dispositivo (hardware + software) utilizzato per proteggere, ovvero aumentare la sicurezza, le reti locali.

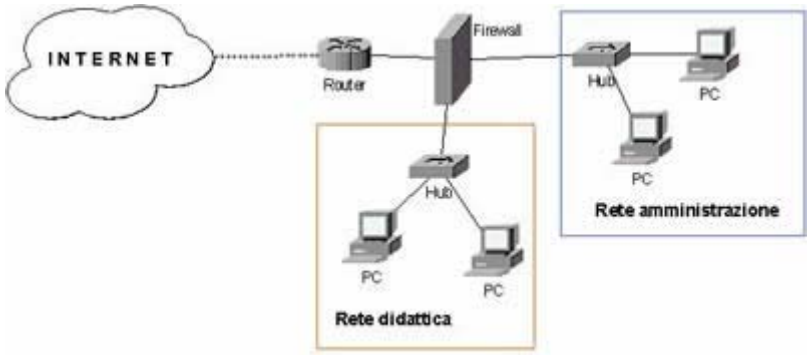


I firewall possono essere realizzati con sistemi Proprietari e/o Open Source, la configurazione di entrambi richiede conoscenze nell'ambito dei protocolli di comunicazione e dei servizi di rete.

La protezione deve essere non solo rivolta verso l'esterno (internet) ma anche verso l'interno, ovvero verso gli utenti della vostra rete locale non autorizzati al trattamento dei dati. Ad esempio in una scuola la rete didattica e quella dell'amministrazione (la segreteria) devono essere separate; nel caso di due distinte connessioni internet la separazione si ottiene semplicemente ed efficacemente non collegando fisicamente i PC della segreteria e della didattica (si hanno due reti locali distinte), nel caso di un'unica connessione (soluzione più economica con gli attuali contratti XDSL) il firewall deve svolgere le seguenti funzioni base:

1. Proteggere dall'esterno (internet)

2. Separare la didattica dalla segreteria



In questo caso un PC con software Open Source opportunamente configurato e tre schede di rete svolgono efficacemente la funzione di firewall.

Infine non dobbiamo dimenticare che *la sicurezza è un processo e non un prodotto*, il monitoraggio continuo, l'educazione alle buone pratiche, rendono "più sicura" la vostra rete.

La crittografia

(http://www.mokabyte.it/1999/06/crittografia.htm)

Il crescente utilizzo di internet come mezzo per lo scambio rapido di informazioni, ha enfatizzato la necessità di comunicazioni sicure, private, protette da sguardi indiscreti.

Sfortunatamente la rete, così come è stata concepita, non supporta un buon livello di sicurezza e di privacy. Le informazioni viaggianti sono trasmesse in chiaro e potrebbero essere intercettate e lette da qualsiasi individuo. Pertanto, è stato necessario creare dei metodi che, rendano le informazioni indecifrabili in modo che solo il mittente e il destinatario possano leggerle, che ne assicurino l'integrità e che consentano l'autenticazione degli interlocutori.

La *crittografia* si propone di ricercare algoritmi capaci di proteggere, con un considerevole grado di sicurezza, le informazioni ad alto valore contro possibili attacchi da parte di criminali, della concorrenza o di chiunque possa usarle per arrecare danno. Comprende tutti gli aspetti relativi alla sicurezza dei messaggi, all'autenticazione degli interlocutori, alla verifica dell'integrità.

La *crittografia* fornisce una serie di algoritmi e di metodi per rendere il messaggio indecifrabile. Alcuni di essi sono molto potenti ed hanno resistito ai più svariati attacchi, altri meno sicuri ma altrettanto importanti.

L'obiettivo di ogni algoritmo di cifratura è quello di rendere il più complicato possibile la decifratura di un messaggio senza la conoscenza della chiave. Se l'algoritmo di cifratura è buono, l'unica possibilità per decifrare il messaggio è di provare, una per volta, tutte le possibili chiavi fino a trovare quella giusta, ma tale numero cresce esponenzialmente con la lunghezza della chiave. Quindi, se la chiave è lunga soltanto 40 bit saranno necessari al più 240 differenti tentativi.

Se ne deduce che l'operazione più delicata in un sistema crittografico è proprio la generazione della chiave.

Affinché esso sia effettivamente sicuro, deve prevedere chiavi di considerevole lunghezza; inoltre, le chiavi devono essere generate in maniera realmente casuale e dunque assolutamente imprevedibile per un ipotetico decifratore. Per tale motivo vengono scartati i generatori di numeri pseudo-casuali forniti dal computer, di solito adottati per giochi e simulazioni, e si preferisce adottare sistemi più complessi che sfruttano il rumore di fondo del mondo fisico che non può in nessun modo essere predetto. Buone sorgenti di numeri casuali risultano essere i processi di decadimento radioattivo, il rumore di fondo in un semiconduttore, o gli intervalli di tempo che intercorrono tra le azioni dell'operatore sulla tastiera. La sorgente più comunemente utilizzata sfrutta il movimento del mouse o la misura in millisecondi del tempo di battitura dell'operatore.

Risulta tuttavia molto difficile determinare la bontà di un algoritmo. Talvolta algoritmi che sembravano molto promettenti si sono rivelati estremamente semplici da

violare lanciando l'opportuno attacco. E' comunque preferibile affidarsi a quegli algoritmi che sembrano resistere da più tempo.

Gli algoritmi di cifratura sono suddivisi in due classi:

- **algoritmi a chiave privata**, o algoritmi simmetrici;
- **algoritmi a chiave pubblica**.

La differenza tra di essi è che i primi usano la stessa chiave per la cifratura e la decifratura, mentre i secondi usano due chiavi differenti, una pubblica e una privata.

Algoritmi a chiave privata

Gli *algoritmi a chiave privata*, o algoritmi simmetrici sono i più comunemente utilizzati. Essi usano la stessa chiave per cifratura e decifratura. Entrambi gli interlocutori conoscono la chiave usata per la cifratura, detta chiave privata, o chiave simmetrica, e soltanto loro possono cifrare e decifrare il messaggio.

Algoritmi a chiave pubblica

Gli *algoritmi a chiave pubblica usano* due chiavi complementari, dette chiave pubblica e chiave privata, create in modo che la chiave privata non può assolutamente essere ricavata dalla chiave pubblica.

Il paradigma di comunicazione è il seguente: i due interlocutori A e B hanno entrambi una coppia di chiavi. A richiede a B la sua chiave pubblica con la quale cifra il messaggio e spedisce il risultante messaggio cifrato a B.

Il messaggio cifrato con una chiave pubblica può essere decifrato solo con la corrispondente chiave privata. Pertanto B, mediante la sua chiave privata, può decifrare il messaggio e leggerlo in tutta sicurezza.

Con questo metodo solo la chiave privata deve essere tenuta segreta mentre la chiave pubblica può essere distribuita a chiunque voglia spedire un messaggio al possessore della chiave. Qualora finisse nelle mani di un pirata, egli non potrà fare altro che cifrare messaggi senza poterli poi decifrare.

Note sulla crittografia (da : Centro polifunzionale di servizio: Dilos center)

L'obiettivo principale della crittografia è far si che, inviando un messaggio su un canale pubblico, il messaggio sia incomprensibile a tutte le persone non autorizzate alla sua lettura. Per far questo la crittografia utilizza un algoritmo chiamato cifrario che attraverso una chiave (chiave del cifrario) modifica il messaggio rendendolo incomprensibile a meno che non venga utilizzata la chiave di decrittazione (che nella crittografia simmetrica è la stessa della chiave di crittazione mentre in quella asimmetrica è diversa) per decrittarlo.

Nella *crittografia tradizionale* viene utilizzata un'unica chiave sia per codificare, sia per decodificare i messaggi. Le informazioni (la chiave e l'algoritmo) necessarie per chi deve inviare il messaggio sono quindi identiche a quelle necessarie a chi deve riceverlo. Per concordare una chiave con il proprio interlocutore c'è bisogno di mettersi preventivamente in contatto con lui incontrandolo di persona, telefonandogli, scrivendogli una lettera, mandandogli un messaggero o in qualsiasi altro modo. In qualsiasi caso, esiste il pericolo che la chiave venga intercettata durante il tragitto, compromettendo quindi l'intero sistema comunicativo.

La *crittografia a chiave pubblica* permette invece a due (o più) persone di comunicare in tutta riservatezza senza usare la stessa chiave e anche se non si sono mai incontrate precedentemente.

La crittografia asimmetrica, conosciuta anche come crittografia a coppia di chiavi, crittografia a chiave pubblica/privata o anche solo crittografia a chiave pubblica, è un metodo di crittografia. Come si evince dal nome, ogni attore coinvolto possiede una coppia di chiavi:

- la chiave privata, personale e segreta, viene utilizzata per decodificare un documento criptato;
- la chiave pubblica, che deve essere distribuita, serve a crittare un documento destinato alla persona che possiede la relativa chiave privata.

L'idea base della crittografia con coppia di chiavi diviene più chiara se si usa un'analogia postale:

- Il mittente A chiude il pacco con un lucchetto di cui possiede la chiave, conserva la chiave e spedisce il pacco al destinatario B.
- B riceve il pacco (che non può aprire perché non ha la chiave), lo chiude nuovamente con un lucchetto di cui conserva a sua volta la chiave e rispedisce il pacco ad A.
- A toglie il suo lucchetto e rispedisce il pacco a B, che può finalmente aprire il pacco, chiuso ormai solo con il lucchetto da lui scelto.

Questo semplice metodo condivide alcune caratteristiche con la crittografia a chiave pubblica: si tratta di un sistema che risolve efficacemente il classico problema della crittografia tradizionale. Se la sicurezza del sistema dipende dalla segretezza della chiave di codifica utilizzata, allora è necessario almeno un canale sicuro attraverso il quale trasmettere la chiave.

La firma digitale

La *firma digitale* è l'equivalente informatico della tradizionale firma apposta su carta.

La sua funzione è quella di attestare la validità, la veridicità e la paternità di un documento inteso, in senso lato, come una lettera, un atto, un messaggio o, in generale, qualunque file di dati.

La firma digitale è il risultato di una procedura informatica basata su un sistema di codifica crittografica a chiavi asimmetriche (una pubblica e una privata), che consente:

- la sottoscrizione di un documento informatico;
- la verifica, da parte dei destinatari, dell'identità del soggetto firmatario;
- la sicurezza della provenienza del documento;
- la certezza dell'integrità del documento;
- la segretezza dell'informazione contenuta nel documento.

L'utente deve disporre di una **Smart Card**, dispositivo di firma sicura, rilasciato da un Ente certificatore attraverso le "Unità di Registrazione".

Si tratta di una carta a microprocessore personalizzata e dotata di un codice segreto.

Utilizzando la propria carta, attraverso un apposito lettore e il software dedicato, l'utente è in grado di apporre la propria firma digitale su un qualsiasi documento informatico.

La firma risulterà così indissolubilmente legata, da un lato, al soggetto sottoscrittore, dall'altro, al testo sottoscritto.

Gestione di un sito web

(stralci prelevati da varie soluzioni proposte per il compito degli esami di Stato)

Fondamentalmente per gestire un sito web si possono adottare 3 soluzioni :

- Utilizzando risorse interne alla azienda fornitrice del sito web;
- Utilizzando un servizio di hosting;
- Utilizzando un servizio di housing.

Naturalmente ogni soluzione offre vantaggi e svantaggi.

Sito in sede

Proposta di svolgimento n. 1

(ipotesi di soluzione esame 2002 della casa Editrice *Tramontana*)

Questa soluzione presenta la seguente principale **problematica**: controllare che l'azienda disponga degli strumenti hardware e software necessari per rendere disponibile il sito in modo permanente su Internet.

Hardware

- un server Web per la pubblicazione del sito www.miosito;
- per essere sempre visibile in Internet e gestibile nella rete interna dell'azienda, il sito deve possedere un indirizzo IP pubblico e un nome di dominio associato, ad esempio, www.miosito.it;
- un server di database, che potrebbe coincidere con il server Web nel caso di scarse risorse finanziarie. Il server di database deve appartenere alla rete interna dell'azienda e quindi non deve essere visibile in Internet. A tal fine, per problemi di sicurezza, potrebbe essere utile disporre di un firewall ed eventualmente di un server proxy;
- il server Web, per essere sempre disponibile, deve essere collegato a Internet mediante una linea telefonica permanente possibilmente dedicata e non commutata (ad esempio, una linea ADSL permanente).

Software

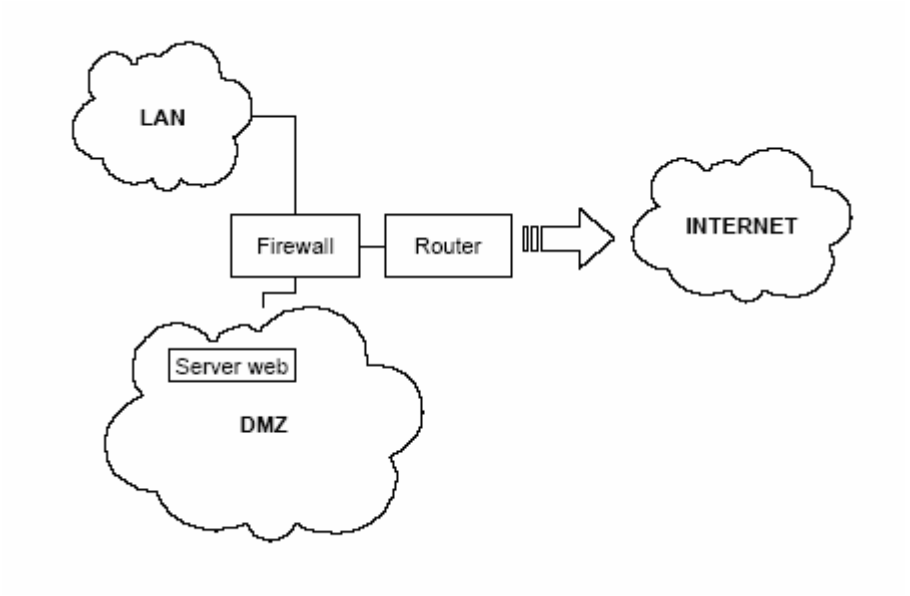
- realizzare il sito Web mediante i programmi commerciali per la progettazione dei siti stessi;
- progettare l'interfacciamento tra il sito Web e il server di database richiamando utilizzando linguaggi di script lato server quali ad esempio l'ASP (*Active Server Page*) o PHP (*Hypertext Preprocessor*).

Proposta di svolgimento n. 2

(ipotesi di soluzione esame 2006 a cura del Prof. *Vinciguerra Guido*)

La soluzione prevede che venga installato un server web presso la azienda/scuola/ditta/redazione, vi è quindi la necessità di disporre di un collegamento permanente ad internet con uno o più indirizzi IP pubblici statici da assegnare al server in questione. Il collegamento dovrà disporre di una banda minima garantita e sistemi di backup della linea in caso di guasto.

Per questioni di sicurezza il server pubblico verrà posizionato su una rete (DMZ) separata da un firewall dalla LAN. Segue schema di collegamento :



Per questioni di affidabilità è necessario che il firewall sia una macchina con sistemi di tolleranza ai guasti, in particolare è possibile indicare un sistema di ridondanza dell'alimentazione elettrica (doppio alimentatore), nonché un sistema di ridondanza delle memoria di massa (RAID).

Per quanto riguarda il software è utile orientarsi per ragioni economiche sulla scelta di un sistema basato su GNU/Linux avendo così minor costi in termini di licenze (sistema operativo server web + DBMS + firewall).

E' possibile scegliere il server web Apache, in particolare il sito on-line, si baserà su un linguaggio dinamico web-oriented, ad esempio PHP o JSP (java) ed interfacciato con un DBMS (ad esempio MySQL o Postgresql) che può inizialmente essere ospitato sulla stessa macchina del server web.

Il server web, per questioni di affidabilità, necessita di sistemi di tolleranza ai guasti in particolare un sistema di ridondanza dell'alimentazione elettrica (doppio alimentatore), nonché un sistema di ridondanza delle memoria di massa RAID (la presenza del DBMS rende importante l'affidabilità delle memorie di massa). Il sistema necessita di un buon sistema di backup.

Proposta di svolgimento n. 3

(ipotesi di soluzione esame 2003 ITC della casa Editrice *Tramontana*)

Per rendere visibile un computer in Internet è necessario disporre di uno oppure più indirizzi IP pubblici, ai quali è associato un nome di dominio di secondo livello del tipo, ad esempio,*azienda.com*. Ogni indirizzo IP pubblico è quindi associato ad un computer server che offre uno oppure più servizi. Ad esempio, il computer *www.azienda.com* può offrire i servizi WWW e FTP, mentre il server *mail.azienda.com*, può offrire i servizi di posta elettronica.

L'accesso ad una oppure più basi di dati può essere garantito installando un server di database nella rete privata dell'azienda, che può anche coincidere con lo stesso server Web.

Le apparecchiature hardware necessarie per offrire servizi on-line per Internet sono:

- server Web e di database, realizzati con computer di classe server di elevate prestazioni, in termini di CPU, RAM e velocità degli hard disk;
- un router, che permetta la connessione di tutta la rete di un'azienda (intranet) alla Rete, con indirizzi IP privati, impiegando un indirizzo IP pubblico;
- una connessione permanente a Internet con una banda garantita e quindi velocità di trasmissione elevate (ad esempio, 1-2 Mbps), realizzata ad esempio con una linea ADSL non commutata;
- un firewall, per garantire la protezione dagli attacchi esterni di persone non autorizzate da Internet nell'intranet dell'azienda.

Caratteristiche dell'applicativo da utilizzare

Per sviluppare il servizio on- line dell'Istituto sono necessari i programmi per realizzare un server Web e un server di database. Per il servizio WWW, è necessario installare in un computer di classe server un programma di sistema quale, ad esempio, Apache per i server UNIX/Linux oppure IIS per i server Windows.

Per realizzare un server di database, è necessario installare un RDBMS (*Relational DataBase Management System*) in grado di permettere la realizzazione dello schema logico relazionale della base di dati e automatizzare le sue procedure di gestione. Il server di database può essere un computer autonomo della rete aziendale oppure coincidere con il server Web.

L'accesso ai dati è realizzato sviluppando alcune pagine da inserire nel sito Web che permettono di eseguire interrogazioni sul server di database e presentare agli utenti i risultati mediante pagine HTML dinamiche di risposta. Le pagine di accesso ai dati contengono degli script server-side (eseguiti dal server) che aprono connessioni al server di database, eseguono query (anche con parametri di ingresso) e presentano i risultati agli utenti (generando pagine HTML dinamiche).

Come RDBMS si può usare Access o MySQL, mentre per realizzare le pagine per l'accesso ai dati si può utilizzare PHP o ASP.

Proposta di svolgimento n. 4

(ipotesi di soluzione esame 2006 del *Corriere della Sera*)

Per realizzare un **server web** in loco occorre innanzitutto definire la tecnologia da utilizzare per la connessione alla rete Internet. Successivamente, sulla base di un'analisi dettagliata della tipologia delle informazioni da rendere disponibili per l'utente e della distribuzione delle probabili connessioni che dovranno essere gestite nell'arco della giornata, occorrerà determinare la configurazione Hw del computer o della rete locale da adibire alla registrazione e distribuzione dei dati.

Infine si procederà alla scelta dei prodotti Sw da utilizzare non solo per la registrazione e la consultazione dei dati, ma anche per garantire un adeguato livello di sicurezza dell'intero sistema. In particolare, per quanto riguarda la connessione ad Internet possiamo ipotizzare che, trattandosi della redazione di un quotidiano locale di una piccola provincia, sia sufficiente collegare il server web alla rete tramite una connessione a banda larga tipo Adsl o a fibre ottiche.

Ovviamente, per garantire un servizio adeguato appare opportuno che questa linea sia dedicata esclusivamente al servizio di server web, demandando la gestione della posta elettronica e di eventuali connessioni provenienti dalla rete locale interna ad un router collegato ad una linea diversa dalla precedente.

Chiaramente verso l'interno della redazione il server web dovrà interfacciarsi con le varie postazioni della rete locale in modo che le pagine del sito siano modificabili in tempo reale dai vari cronisti. Per quanto riguarda la configurazione Hw del server, vista la dimensione degli HD attuali, si può ipotizzare l'utilizzo di due HD di grande capacità in modo da poter registrare su un unico supporto il software di gestione e tutte le informazioni (articoli, video e audio) da rendere disponibili.

Infine, per garantire il funzionamento del servizio verso l'esterno anche in caso di malfunzionamento del server principale, possiamo ipotizzare la presenza di un secondo server (server secondario) che, per la maggior parte del tempo funge esclusivamente da supporto di backup.

Passiamo ora ad analizzare la **parte Sw** del sistema. Innanzitutto risulta indispensabile dotare il server non solo di un sistema operativo di base adeguato (Windows 2003 server o simili), ma anche dei pacchetti necessari per una corretta gestione delle richieste (IIS, Apache, Firewall, e così via).

Infine risulta consigliabile mettere a disposizione dell'utente il software necessario per la gestione in ambiente locale dei file consultabili sul sito, tra i quali sicuramente non possono mancare un lettore di file testo compressi (ad esempio per file in formato PDF) e i pacchetti per la visualizzazione di immagini e filmati.

Se poi l'editore vuole fornire dei servizi di ricerca di articoli correnti e passati in base a criteri di selezione (argomento, data di pubblicazione e così via), è necessario realizzare una base dati a cui interfacciare le pagine web e il server deve fornire i servizi ODBC necessari.

Hosting

L'***hosting*** è un servizio fornito da un ISP (Internet Service Provider = Fornitore di Servizi Internet) che rende disponibili sistemi on-line per la fornitura di servizi Internet da parte dei clienti. Questi servizi possono essere l'archiviazione e l'accesso a informazioni, immagini o qualsiasi altro contenuto accessibile via web e in tale caso si parla di '*web hosting*' ma anche di altri servizi quali posta, ftp.

Dal punto di vista della visibilità web e degli altri servizi Internet, il cliente sembra essere un fornitore di servizi dotato di proprie risorse di connettività (host virtuali) mentre in realtà queste risorse sono allocate su un host che risiede fisicamente presso il fornitore di servizi del cliente.

Questa soluzione libera totalmente il cliente dalla responsabilità di gestire la fornitura di servizi quindi la sua connettività diventa semplicemente quella di un utilizzatore di servizi.

Ad esempio non è più responsabilità del cliente esibire un IP statico risolto via DNS e mantenere un servizio HTTP su un host con IP pubblico perché queste operazioni sono fatte dall'ISP del cliente. L'unica responsabilità del cliente è l'upload via FTP verso l'host che svolge il servizio di hosting dei documenti da pubblicare. Se si fa riferimento al servizio postale non è responsabilità del cliente gestire localmente un server SMTP perché questo risiede sull'host dell'ISP e quindi vi si accede con un normale client postale.

Tipici servizi di hosting sono:

- Registrazione del dominio: l'ISP registra il dominio presso l'autorità di registrazione ;
- Risoluzione DNS: l'ISP fornisce la risoluzione DNS per gli host virtuali del dominio;
- Servizio web: l'ISP fornisce il servizio http per gli host virtuali del dominio con web attivo;
- Servizio posta: l'ISP fornisce i servizi smtp,pop/imap per gli host virtuali del dominio;
- Servizio ftp: l'ISP fornisce il servizio ftp per gli host virtuali del dominio;
- Servizio di redirezione: l'ISP redirige le risoluzioni DNS verso altri host di altri domini.

Questa soluzione è particolarmente adatta a privati, piccole aziende o enti che vogliono avere una visibilità Internet senza avere i costi e la complessità di una connettività per fornitori di servizi

Nel caso di utilizzo di apparecchiature in hosting presso un provider ISP le problematiche sono naturalmente più semplificate, dato che occorrerà semplicemente definire le modalità per la manutenzione dinamica del sito e per l'interrogazione di un eventuale database remoto relativo agli utenti registrati. I file contenenti gli articoli, necessariamente in forma statica, vengono mandati via FTP al provider che provvede a pubblicarli. Il sito può essere suddiviso in cartelle per argomento, permettendo quindi una forma di ricerca più semplificata.

Housing

Il servizio di ***housing*** consente di effettuare la 'delocalizzazione' di tutti i servizi Internet. Consiste nella installazione un proprio server nella sede dell'ISP oppure nel noleggio di un server già completamente configurato collocato nella sede dell'ISP.

I vantaggi di una tale delocalizzazione sono:

- Fornitura di energia elettrica protetta, stabile e senza interruzioni
- Temperatura controllata e costante
- Connettività sicura ed affidabile.

A differenza del servizio di hosting in questo caso l'host non è virtuale ma è un nodo Internet fisicamente esistente ed interamente dedicato al cliente e sul quale il cliente ha diritti di accesso totali tramite una shell di accesso remoto.

L'unica differenza rispetto ad avere il server nella propria sede consiste nella connettività, routing e firewall che sono gestiti dall'ISP e non direttamente accessibili al cliente.

In comune con la soluzione hosting ci sono:

- Registrazione del dominio: l'ISP registra il dominio presso l'autorità di registrazione;
- Risoluzione DNS: l'ISP fornisce la risoluzione DNS per gli host virtuali del dominio.

Questa soluzione è particolarmente adatta ad aziende anche medie e grandi che vogliono delegare la visibilità Internet all'esterno della propria organizzazione.