

A.4 Le reti e i servizi di rete

- UdA 1 Le architetture di rete
- UdA 2 Fondamenti di networking
- UdA 3 LA STRUTTURA DI UNA RETE AZIENDALE**
- UdA 4 Hosting, housing e cloud computing

OBIETTIVI UNITÀ

- Saper classificare le reti aziendali
- Individuare i componenti di una rete aziendale
- Comprendere le funzioni del server e dei client



CURIOSITÀ

Generalmente parlando di rete aziendale si usa l'acronimo LAN Local Area Network per indicare che è "in una zona limitata di spazio", cioè con collegamento in "locale".

Tipologie di reti aziendali

Le **reti informatiche** si sono talmente diffuse da diventare di fondamentale importanza nella vita quotidiana. Fino a pochi anni fa a nessuno sarebbe venuto in mente di valutare la qualità di un albergo o di un locale pubblico in base alla presenza o meno di una rete wireless efficiente. Questo ci fa capire quanto sia diventato importante anche per un'azienda avere una **rete informatica** efficiente e sicura per migliorare la propria produttività.

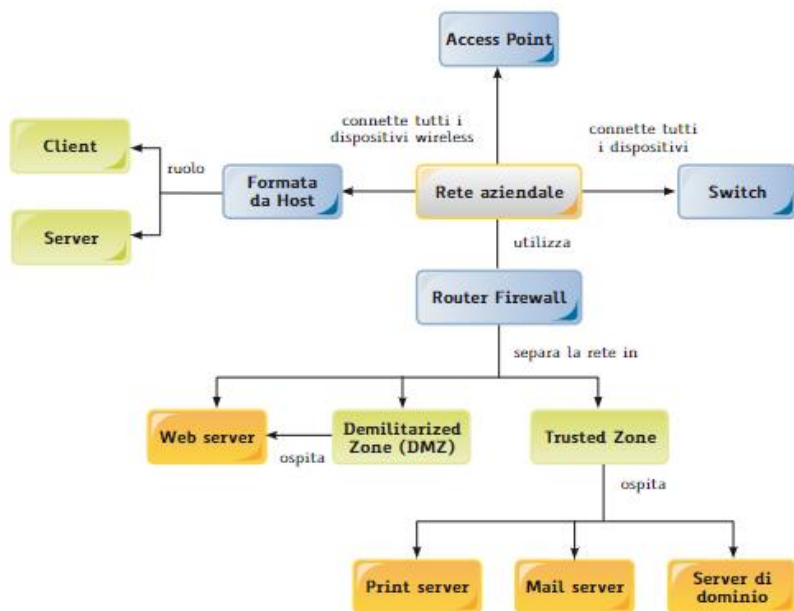
La **rete informatica aziendale** consente agli utenti di comunicare e scambiarsi informazioni in modo rapido ed efficace, senza la necessità di trovarsi fisicamente nello stesso luogo, aumentando in tal modo la **competitività del sistema**.

Vi è oggi una domanda sempre crescente di personale tecnico qualificato (**network administrator**) in grado di progettare e amministrare una rete ma, soprattutto, con conoscenze specifiche inerenti alla sicurezza dei dati e delle reti, capace di garantire riservatezza e affidabilità dei servizi.

La gestione della rete prevede il monitoraggio della stessa, l'aggiornamento, l'eventuale ampliamento, oltre alla protezione dei dati conservati in essa.

L'avvento delle reti, e in particolare di internet, ha provocato cambiamenti negli scenari industriali, nonché lo sviluppo di nuove strategie aziendali. A tal proposito, sono infatti nate nuove tecnologie e figure professionali, sia nell'ambito del **digital business** che del **social marketing**.

Cerchiamo adesso di comprendere e individuare gli elementi principali che concorrono a formare **una rete aziendale**, in particolare analizzeremo le due configurazioni tipiche presenti in azienda.



Con **RFC (Request For Comments)** si fa riferimento ad una serie di documenti contengono note tecniche e organizzative su Internet (<https://www.ietf.org/standards/rfcs/>).

Indirizzi IP privati

In ogni classe di indirizzamento, una porzione di indirizzi è riservata agli **indirizzi IP privati** appositamente dedicati da **IANA** per la configurazione delle reti private, riportati nei documenti **RFC 1597** e **RFC 1918**.

I tre range indirizzi delle rispettive classi sono i seguenti:

CLASSE DI INDIRIZZI IP	INTERVALLO DI INDIRIZZI IP RISERVATO	Subnet mask
Classe A	10.0.0.0 - 10.255.255.255	8 bit
Classe B	172.16.0.0 - 172.31.255.255	12 bit
Classe C	192.168.0.0 - 192.168.255.255	16 bit

La caratteristica degli intervalli di indirizzi IP privati è che questi non vengono instradati su Internet e possono essere utilizzati senza registrazione in altrettante reti private; inoltre ogni rete privata può utilizzare senza problema gli stessi indirizzi, dato che rimangono "all'interno della rete aziendale" e non sono visibili in Internet.

Quindi ogni rete privata può progettare un proprio piano di indirizzamento utilizzando questi particolari classi in completa autonomia, in quando non vengono instradati dal router al di fuori della rete locale.

Tipicamente, viene utilizzato l'indirizzo di **classe C 192.168.x.x**, anche perché nell'indirizzo pubblico è diversa la scomposizione tra indirizzo di rete ed indirizzo di **host**, come è possibile vedere nella tabella della pagina precedente dal numero di bit della **SubNet Mask**.

ESEMPIO

Con la **classe C** abbiamo la **SubNet Mask** a: **255.255.0.0**, ed è possibile creare, secondo le proprie esigenze:

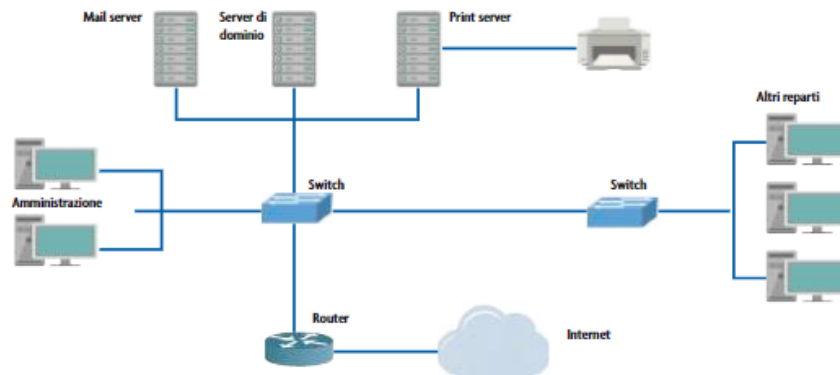
- un'unica rete che connette $(256 \times 256) - 2 = 65.534$ computer;
- due reti da $(62 \times 256) - 2 = 15.870$ PC ognuna;
- sei reti da $(30 \times 256) - 2 = 7.678$ PC ognuna;
- 254 reti da 254 computer ognuna: e questa la configurazione classica ottiene utilizzando il terzo byte come sottorete e l'ultimo byte come host (p.e. **192.168.134**).

La rete LAN per un ufficio

Ipotizziamo di voler creare una piccola rete **LAN locale**, che consenta agli utenti di comunicare internamente, di scambiarsi file e di navigare in internet.

I principali dispositivi "coinvolti" sono i seguenti:

- due (o più) **switch** usati per collegare i computer tra di loro e ad alcuni **server** necessari per condividere le risorse;
- un **router** a cui sono collegati i due **switch** per consentire la connessione a internet;
- un **server** di dominio per la gestione centralizzata degli utenti e dei file, e un mail server per la gestione della posta elettronica da parte di tutti gli utenti;
- un **print server** per la gestione della stampa dei documenti cartacei su stampante.



Data center. È un insieme di server che vengono collocati in un unico contesto, con lo scopo di favorire una centralizzazione della gestione, della sicurezza e della manutenzione dei server stessi. Per proteggere l'accesso, vengono spesso dotati di strumenti per la sicurezza sia fisica sia virtuale.

A ogni PC collegato alla rete viene assegnato un **indirizzo IP** di **classe C**, dato che, come abbiamo visto, generalmente questa dimensione risulta sufficiente per la maggior parte delle reti aziendali.

Le **reti IP aziendali** sono chiamate **reti IP private** in quanto queste non sono raggiungibili da nessun PC esterno, dato che gli **host** hanno come **indirizzi IP** proprio gli **indirizzi IP privati**. Per la **classe C** l'indirizzo ha per i primi due ottetti i valori **192.162.x.x**, mentre tutti gli altri valori fino a **223.255.x.x** sono destinati alle **reti pubbliche**.

Se osserviamo l'esempio di figura, possiamo notare che i due **switch** presenti permettono di suddividere la **rete locale** in due parti:

- sezione di rete riservata all'**amministrazione**;
- sezione di rete a disposizione per gli altri reparti dell'azienda.

Allo **switch dell'amministrazione** sono stati collegati anche i tre **server**, uno per il dominio, uno per la stampante e un mail server:

- sul **server di dominio** ipotizziamo che venga installato un sistema operativo in versione server, come ad esempio **Windows 2019**.
- sul **mail server** ipotizziamo invece che venga installata un'applicazione di gestione della posta elettronica centralizzata;
- per quanto riguarda il **print server**, non è necessario un software particolare, in quanto qualunque sistema operativo è in grado di condividere un servizio di stampa.

I **server** conservano in genere dati aziendali preziosi; l'accesso fisico del personale ai server stessi, inoltre, non avviene in modo continuativo. Per questi motivi, è bene collocare i computer che fungono da server in luoghi sicuri, come ad esempio un armadio, un locale apposito al quale possono accedere solo gli addetti del personale tecnico, oppure ancora un luogo lontano dalla sede aziendale, come i **data center**.



La rete client/server aziendale

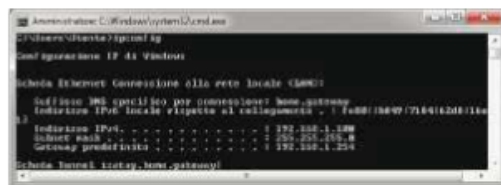
Esaminiamo adesso il caso di una **rete aziendale più complessa** rispetto all'esempio precedente, che metta a disposizione anche un sito web dell'azienda aperto in extranet a eventuali clienti e fornitori. Come operazioni preliminari, ipotizziamo di aver sottoscritto un contratto aziendale per connessione internet in ADSL, possibilmente con router a noleggio, e di disporre di almeno 4 indirizzi IP pubblici statici dal proprio provider internet, di aver acquistato un dominio internet (p.e. **www.miaAzienda.com**) e infine di aver realizzato il cablaggio dell'edificio avendo predisposto le prese a muro per le postazioni di lavoro.

Indirizzi statici e dinamici

Vi possono essere due differenti tipi di **indirizzo IP**: indirizzo **IP statico** e indirizzo **IP dinamico**.

- L'**indirizzo IP statico** è un indirizzo che è assegnato in modo definitivo da autorità riconosciute a livello internazionale all'utenza aziendale che generalmente lo richiede e lo acquista da un gestore di servizi di connessione in modo da poter lavorare in remoto, cioè per svolgere ad esempio le attività di contabilità, di gestione degli ordini, di controllo del magazzino, accedendo ai **server aziendali** dall'esterno, come se si fosse in sede.
- L'**indirizzo IP dinamico**, invece, è un indirizzo che è assegnato dalla rete al momento del collegamento e, quindi, è sempre diverso e cambia ogni volta che ci si collega alla rete.

Per visualizzare il valore dell'**indirizzo IP** assegnato a una macchina è sufficiente posizionarsi al prompt del Sistema Operativo e digitare **IPCONFIG**, ottenendo una videata simile alla seguente:



Vogliamo creare una rete **LAN** che ci consenta di rendere visibile e pubblico il sito web aziendale attraverso un **web server**. Inoltre, vogliamo mettere disposizione per i vari uffici dell'azienda un mail server per la gestione della posta sia interna sia esterna dell'azienda.

Firewall. È un dispositivo che ha l'obiettivo di creare una separazione tra Internet, intesa come rete pubblica, e la rete aziendale, ritenuta vulnerabile, al fine di preservarla da intrusioni fraudolente o non autorizzate. Il firewall può essere un computer specializzato in queste funzioni di controllo della rete, oppure un programma software installato sul server della rete.

Si vuole poi proteggere la rete **LAN** da attacchi esterni mediante **firewall** e la posta elettronica da attacchi verso il **mail server**. I computer e i server della rete **LAN** devono navigare su Internet con un solo indirizzo IP pubblico e in maniera protetta.

In una **rete aziendale** di tipo **client/server**, per aumentarne la sicurezza perimetrale, è necessario procedere alla sua suddivisione in due zone distinte, chiamate rispettivamente:

- **Trusted Zone:** è il segmento della rete non accessibile direttamente dall'esterno, se non attraverso il firewall, che bloccherà ogni tentativo di accesso non autorizzato;
- **Demilitarized Zone (DMZ):** è un segmento isolato di **LAN** che consente esclusivamente connessioni verso l'esterno; per maggiore sicurezza, gli host presenti nella **DMZ** non possono connettersi alla rete aziendale interna.

Osservando la figura, possiamo notare come nella **Trusted Zone** tutte le postazioni degli utenti, rappresentate dai computer, dalle stampanti di rete e dai dispositivi **wireless**, possono accedere al dominio interno autenticandosi con le proprie credenziali tramite il **server di dominio**, mentre il firewall, rappresentato in questo caso da un router con specifiche funzionalità di protezione, separa la rete interna (**Trusted Zone**) dalla **DMZ**, evitando in tal modo accessi non autorizzati dall'esterno.

