

Fondamenti di Networking e Reti Informatiche Aziendali

Classe 5ASI
ITCG Fermi

Prof. Montemurro

Definizione di Rete Informatica e Networking

Rete informatica: insieme di **hardware**, **software**, e **cablaggio** i quali permettono a più dispositivi di elaborazione di comunicare tra loro.

I computer collegati in rete possono (1) scambiarsi file, e (2) condividere periferiche (es. stampanti, dispositivi di archiviazione collegati alla rete NAS ecc.).

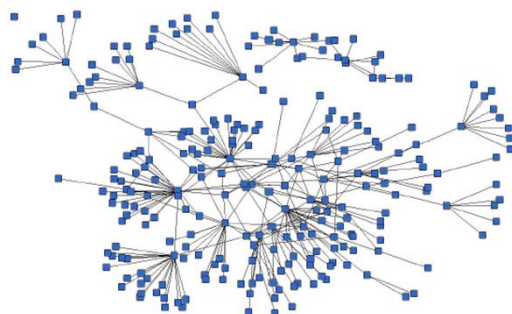
Networking: connessioni tra diverse reti informatiche.

Prof. Montemurro

Definizione di Rete Informatica e Networking

Una rete (anche non informatica) è costituita da:

1. **nodi** i quali sono le unità che costituiscono la rete. Nel caso di una rete informatica, un nodo è una qualsiasi entità che genera/smista/riceve informazioni sui canali di comunicazione della rete stessa (esempi di nodi: PC, tablet, smartphone, stampanti, switch, router ecc.);
 2. **connessioni** tra i nodi.
- Una connessione collega una coppia di nodi.
 - Ogni nodo può avere più connessioni.



Prof. Montemurro

Classificazione delle Reti in Base all'Estensione Geografica

Rete informatica	Distanza coperta (m)
LAN (Local Area Network (o rete locale))	500
CAN (Campus Area Network)	1000
MAN (Metropolitan Area Network)	Area metropolitana
WAN (Wide Area Network (o rete geografica))	Area transcontinentale

Esempio di LAN: rete informatica in un'unica sede aziendale.

Esempio di WAN: due o più reti informatiche LAN, collegate tra loro, che si trovano in sedi differenti nel mondo.

Prof. Montemurro

Componenti di Base di una Rete Aziendale

1. Almeno due host.

Host è un qualunque dispositivo dotato di CPU in grado di connettersi ad una rete (es. computer, tablet, smartphone, console per videogiochi ecc.).

2. Almeno una scheda di rete su ciascun host.

Scheda di rete: dispositivo che permette di connettere un host ad una rete.

3. Un **mezzo di collegamento**: cavi oppure connessione senza cavo (wireless).

4. Un **software di rete**.

5. Un **punto di aggregazione**, cioè un dispositivo in grado di connettere tutti i cavi; oggi i dispositivi che fanno da punto di aggregazione sono gli **switch**.

Prof. Montemurro

Modelli di Reti Informatiche Aziendali

Il sistema informatico di un sistema informativo aziendale può basarsi sui seguenti modelli di reti informatiche:

1. modello mainframe-terminale;
2. modello client-server;
3. modello peer-to-peer (P2P);
4. modelli ibridi che prevedono l'uso sia del modello client-server che P2P.

Prof. Montemurro

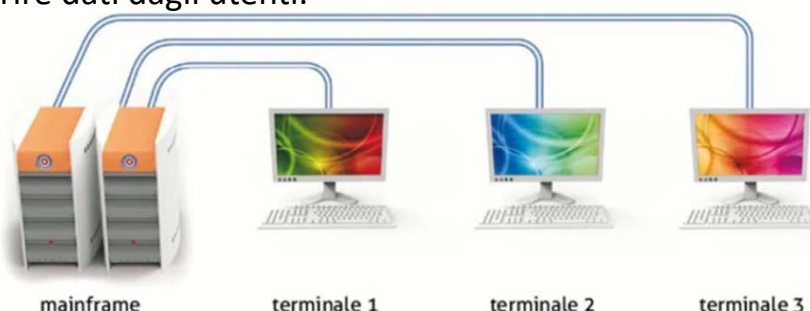
Modelli di Reti Informatiche Aziendali

Modello mainframe-terminale (di una rete informatica aziendale): questo modello prevede la presenza di:

1. una macchina chiamata **mainframe** la quale è in grado di eseguire operazioni di elaborazione e memorizzazione dei dati che poi verranno distribuiti all'utente;
2. **terminali** i quali non sono in grado di elaborare informazioni, sono usati solo visualizzare ed inserire dati dagli utenti.

Svantaggi

- i. hardware complesso e costoso;
- ii. sistema poco flessibile.

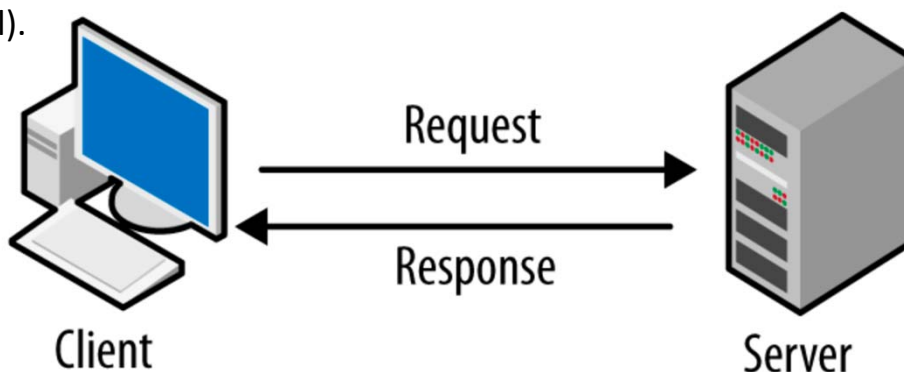


Prof. Montemurro

Modelli di Reti Informatiche Aziendali

Modello client-server (di una rete informatica aziendale): architettura software costituita da due applicazioni:

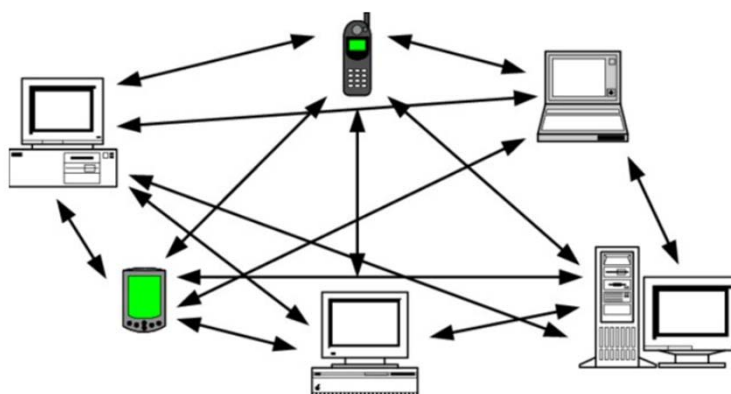
1. **client**: applicazione che richiede un servizio (es. Gmail sul browser del nostro PC);
2. **server**: applicazione che fornisce un servizio (es. server Google fornisce Gmail).



Prof. Montemurro

Modelli di Reti Informatiche Aziendali

Modello peer-to-peer (P2P) (di una rete informatica aziendale): il client ed il server risiedono entrambi su ciascun computer della rete informatica.



Prof. Montemurro

Cablaggio di Reti Informatiche Aziendali

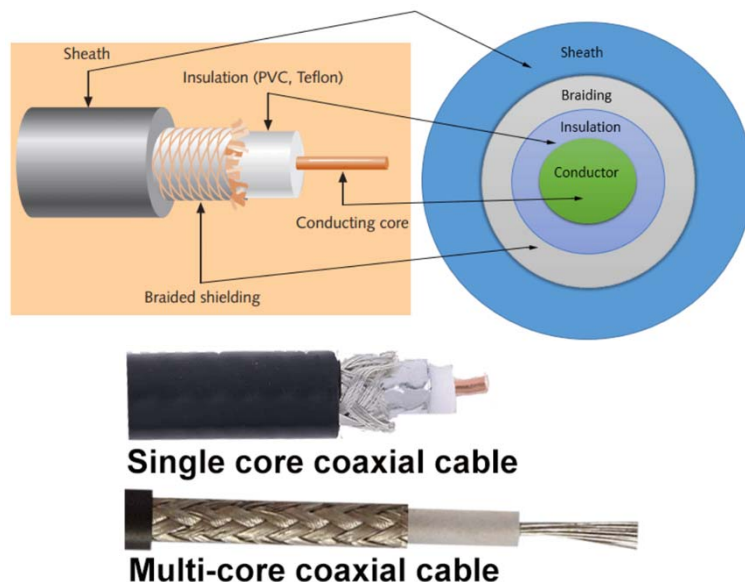
Cablaggio: modalità con le quali si effettuano i collegamenti fisici tra i dispositivi di rete.

Tipi di cavi

1. **Cavo coassiale** il quale è poco utilizzato
2. **Doppino in rame** (o **cavo Ethernet**) il quale si usa nelle reti LAN, il suo spinotto terminatore si chiama **RJ45**, è conforme a vari standard di rete (**UTP**, **FTP**, **STP**; questi si differenziano per la schermatura dalle interferenze elettromagnetiche EM), e la distanza massima coperta non supera i 100 metri
3. **Fibra ottica** la quale si usa per le linee ad alta velocità sulle quali vengono scambiate grandi quantità di dati, e la distanza massima coperta è di circa 10 chilometri

Prof. Montemurro

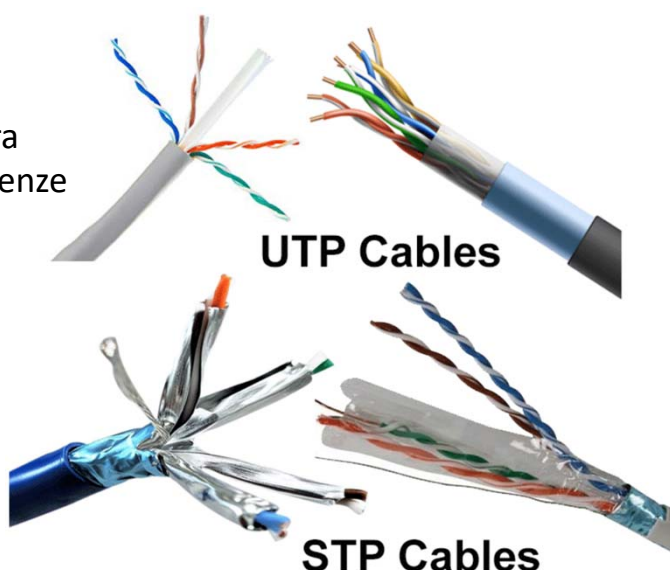
Cablaggio: Cavi Coassiali di Rete



Prof. Montemurro

Cablaggio: Doppino in Rame (o Cavo Ethernet) di Rete

- 1. Cavi Ethernet UTP (Unshielded Twisted Pair):** tutte le coppie di cavi sono avvolte in un'unica guaina di plastica (no schermatura metallica protettiva dalle interferenze elettromagnetiche).
- 2. Cavi Ethernet STP (Shielded Twisted Pair):** ogni coppia è avvolta da un ulteriore strato di protezione metallica, poi tutte le coppie sono avvolte in un'unica guaina esterna metallica e da una di plastica (schermatura massima dalle interferenze EM).



Prof. Montemurro

Cablaggio: Doppino in Rame (o Cavo Ethernet) di Rete

3. **Cavi Ethernet FPT (Foiled Twisted Pair):** tutte le coppie sono avvolte in un'unica guaina esterna metallica e da una di plastica, le singole coppie non sono schermate (schermatura intermedia dalle interferenze EM rispetto ai cavi UTP e STP).

Prof. Montemurro

Cablaggio: Spinotto Terminatore RJ45 del Doppino in Rame



Fig. 2. RJ-45 connector

Prof. Montemurro

Cablaggio: Fibra Ottica



Prof. Montemurro

Dispositivi di Rete

Dispositivi di rete: dispositivi che permettono la comunicazione tra gli host.

Tipi di dispositivi di rete

1. Schede di rete
2. Hub
3. Switch
4. Router

Prof. Montemurro

Dispositivi di Rete: Schede di Rete

Scheda di rete: dispositivo che permette di connettere un host ad una rete; in genere sono già montate sulla scheda madre, ed hanno una **porta RJ45** dove viene connesso il cavo Ethernet.

Tipi di schede di rete

1. **Schede di rete Ethernet** le quali sono obsolete; velocità massima di comunicazione pari a 10 Mbps
2. **Schede di rete Fast Ethernet** le quali permettono una velocità massima di comunicazione pari a 100 Mbps
3. **Schede di rete Gigabit Ethernet** le quali permettono una velocità massima di comunicazione pari a 1000 Mbps (1 Gbps)
4. **Schede di rete senza fili** (o **wireless**, o **Wi-Fi**)

Prof. Montemurro

Dispositivi di Rete: Schede di Rete con Porta RJ45



Prof. Montemurro

Dispositivi di Rete: Schede di Rete Wi-Fi



Prof. Montemurro

Dispositivi di Rete: Hub e Switch

Hub e **switch**: sono entrambi dispositivi elettronici in grado di connettere tutti i cavi della rete per cui permettono la comunicazione tra gli host; ciascun cavo di rete è collegato ad un host diverso.

Porta fisica: è una connessione fisica (es. porta RJ45), un'interfaccia fisica dove si può inserire un cavo di rete che in genere è il cavo Ethernet.

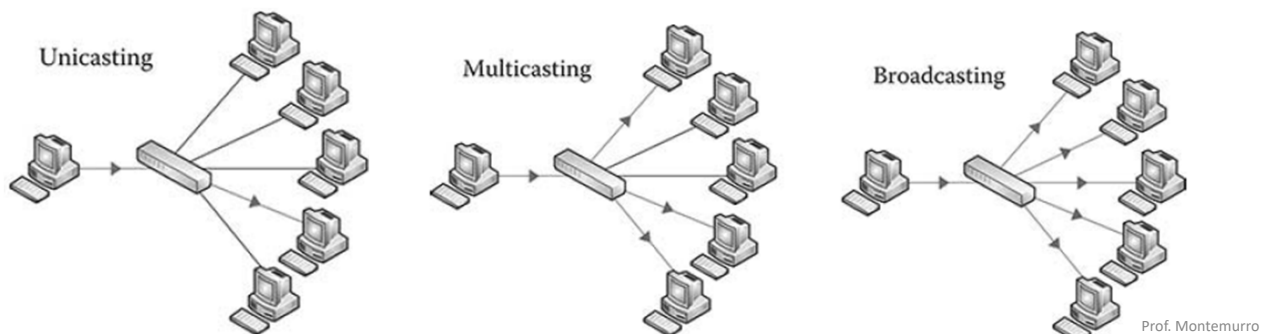
Porte RJ45



Prof. Montemurro

Digressione: Metodi di Distribuzione dei Dati

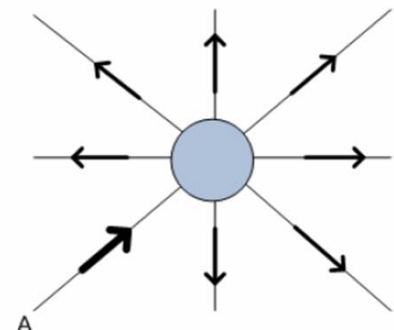
1. **Unicasting**: trasmettere dati tra una sorgente ed un destinatario (es. mando un'email ad un singolo destinatario)
2. **Multicasting**: trasmettere dati contemporaneamente ad un gruppo selezionato di destinatari (es. invio email ad un paio di amici)
3. **Broadcasting**: trasmettere dati contemporaneamente a tutti i nodi della rete (es. radio, televisione)



Dispositivi di Rete: Hub

Hub: dispositivo elettronico che riceve un messaggio su una porta e lo invia su tutte le porte, tranne alla porta sulla quale il messaggio è stato ricevuto (**operazione di flooding**). La distribuzione dei dati è di tipo broadcast.

Esempio: l'hub in figura riceve un messaggio sulla porta A, e lo invia su tutte le altre porte.

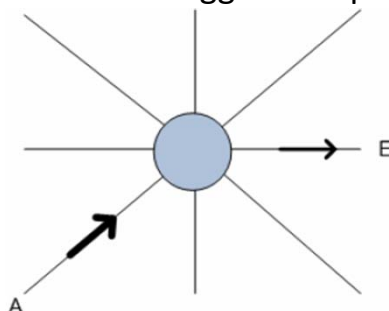


Dispositivi di Rete: Switch



Switch (o **commutatore**): dispositivo elettronico che riceve un messaggio su una porta e lo invia solo su una sola porta che viene specificata all'interno del messaggio stesso. La distribuzione dei dati è di tipo unicast.

Esempio: l'hub in figura riceve un messaggio sulla porta A, e lo invia solo sulla porta E.



Prof. Montemurro

Dispositivi di Rete: Switch



La principale caratteristica di uno switch è la sua **banda di trasmissione**, cioè quanti megabit al secondo (Mbps) riesce a trasmettere.

Esempio: switch con banda di trasmissione di 10 Mbps significa che ciascun utente potrà inviare/ricevere 10 megabit al secondo.

Patch panel



Switch

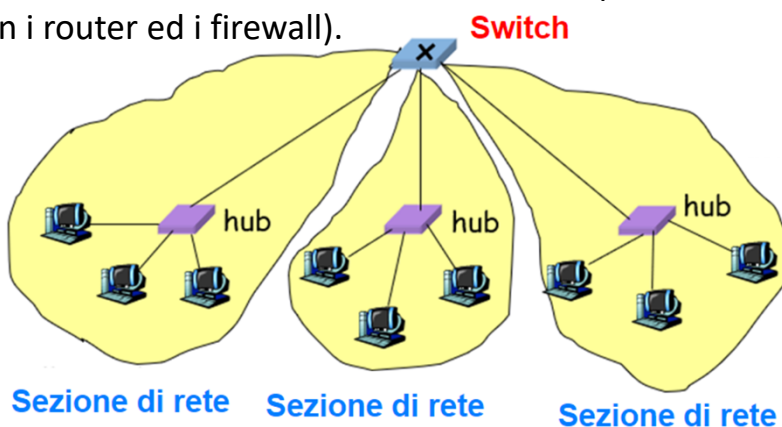
Prof. Montemurro

Dispositivi di Rete: Switch



Sezione di rete (o **segmento di rete**): insieme di dispositivi di rete che condividono lo stesso cavo di rete (se la rete è una rete cablata).

Gli switch consentono di creare e connettere tra loro più sezioni di rete (si può fare anche con i router ed i firewall).



Prof. Montemurro

Dispositivi di Rete: Router



Router: dispositivo elettronico che smista, cioè instrada i dati in genere verso l'esterno di una rete locale (LAN).

Esempio: i router sono usati per collegare due LAN tra loro oppure per collegare una LAN a internet.

Dunque i router sono usati soprattutto per collegare reti fisicamente distanti, cioè reti geografiche (WAN).

Ci sono diversi percorsi che i dati possono prendere, il router sceglie i percorsi più efficaci, cioè quelli in cui si ha il minor spreco di risorse (es. tempo). Se cade la connessione, per non interrompere il traffico, un router sorgente può definire anche un eventuale percorso alternativo.

Prof. Montemurro

Topologie di Rete

Topologia di rete: descrive (1) posizione (disposizione geometrica) di tutti i nodi che fanno parte della rete, (2) tutti i collegamenti fisici da realizzare per connettere i nodi.

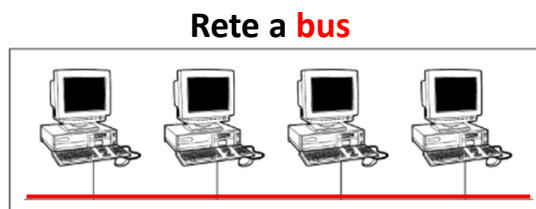
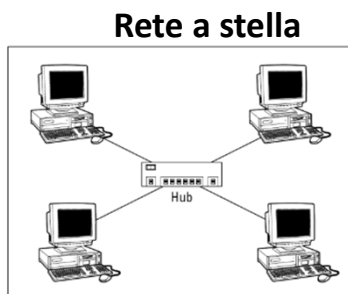
Parametri topologici di una rete

1. **Numero di nodi**
2. **Numero di canali trasmissivi**
3. **Ridondanza delle connessioni;** maggiore è il numero di connessioni alternative per raggiungere una stessa destinazione, maggiore è la **tolleranza ai guasti**. Infatti, se una connessione si rompe, ce n'è un'altra alternativa.

Prof. Montemurro

Tipi di Topologie di Rete

1. **Rete a stella**
2. **Rete ad anello**
3. **Rete a bus**

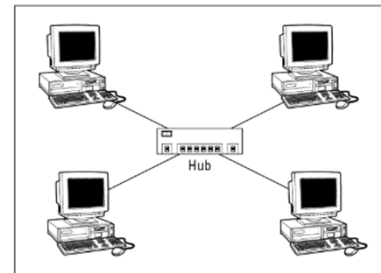


Prof. Montemurro

Topologie di Rete: Rete a Stella

Rete a stella: il numero di canali è uguale al numero di nodi meno uno ($n = c - 1$). Al centro della stella si trova un dispositivo concentratore (switch o hub).

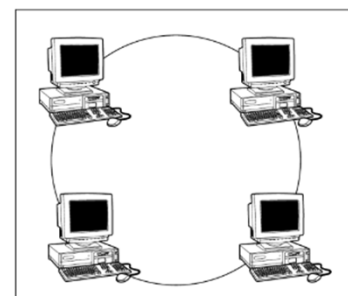
Svantaggio: tolleranza ai guasti inesistente; nel caso in cui il canale si guasti, la funzionalità della rete viene compromessa.



Prof. Montemurro

Topologie di Rete: Rete ad Anello

Rete ad anello: ogni nodo è collegato con altri nodi, in modo da formare una struttura circolare. Ci sono due percorsi alternativi per raggiungere una stessa destinazione. Ogni scambio di informazioni coinvolge anche nodi della rete che non sono direttamente interessati ai messaggi, nonostante ciò devono cooperare per permettere la trasmissione dei messaggi.

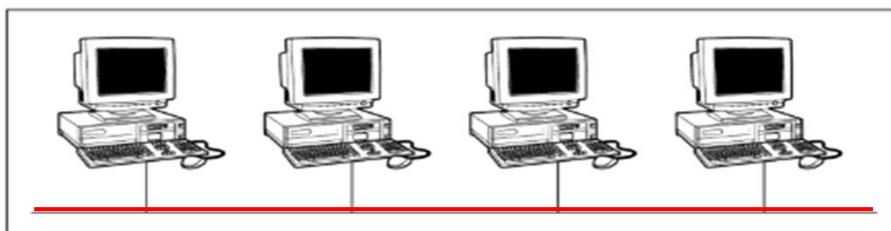


Prof. Montemurro

Topologie di Rete: Rete a Bus

Rete a bus: i computer sono connessi a un unico canale comune, condiviso da tutte le comunicazioni. Un solo nodo alla volta può trasmettere sul canale. Tutti i nodi possono valutare i messaggi, ma solo il nodo che riconosce di essere il destinatario acquisisce il messaggio.

Bus: insieme di fili ordinati che permettono la trasmissione di dati.



Prof. Montemurro

Collisioni di Rete

Collisione di rete: quando più dispositivi condividono lo stesso mezzo trasmissivo (es. cavo di rete o mezzo wireless), può accadere che due o più dispositivi tentino di inviare un messaggio contemporaneamente. Poiché su un mezzo trasmissivo può viaggiare un messaggio per volta, quando ne arriva più di uno, tali messaggi o vengono distrutti o vengono corrotti (cioè non sono più uguali ai messaggi originali) per cui vengono scartati quando raggiungono i rispettivi destinatari. Questo conflitto tra più dispositivi che si verifica quando tentano di inviare contemporaneamente un messaggio sul mezzo trasmissivo in comune si chiama collisione di rete.

Esempio: due amici usano i walkie-talkies; se tentano di comunicare contemporaneamente, quello che si sente è rumore. Questa è una collisione di rete.

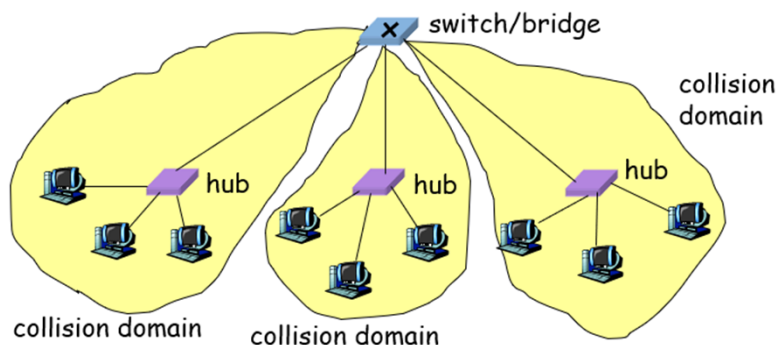
Prof. Montemurro

Dominio di Collisione

Dominio di collisione: insieme dei dispositivi che condividono lo stesso mezzo trasmissivo per cui, in fase di trasmissione del messaggio, si potrebbero verificare collisioni di rete.

Gli switch servono per creare domini di collisione; così facendo previene le eventuali collisioni tra i diversi domini di collisione grazie alla **bufferizzazione**

(memorizzazione temporanea dei messaggi provenienti contemporaneamente da più dispositivi nella **memoria interna dello switch**; ciò permette di inviare un messaggio alla volta sul mezzo trasmissivo anche se più messaggi arrivano contemporaneamente).



Prof. Montemurro

Larghezza di Banda

Larghezza di banda: quantità di dati che possono circolare in un dato periodo di tempo, in un mezzo trasmissivo; si misura in bit/s (o bps, o bitrate). La larghezza di banda dipende anche dal tipo di mezzo trasmissivo (es. cavo Ethernet, fibra ottica, wireless).

Congestione della rete: eccesso di traffico che blocca i percorsi dei dati lungo la rete.

Quando viene utilizzato più del 50% della larghezza di banda, il numero di collisioni tende ad aumentare rapidamente causando congestioni (il tempo per stampare i file si allunga, le applicazioni si aprono lentamente e gli utenti devono aspettare). Quando questo valore raggiunge e supera il 60%, la rete rallenta drasticamente o, addirittura, si ferma.

Prof. Montemurro

Linea dedicata

Linee dedicate (o **Circuito Diretto Numerico CDN**): consente la connessione fissa tra due sedi aziendali, oppure tra la sede centrale e le filiali; tali linee garantiscono sicurezza ed elevate prestazioni.

Sicurezza informatica (o **cybersicurezza**): insieme delle misure atte a garantire la disponibilità, l'integrità (dati originali, cioè non letti/modificati da persone non autorizzate) (informazione originale, non corrotta), e la riservatezza (informazioni comprensibili solo per chi è autorizzato) delle informazioni gestite dai sistemi informatici.

Svantaggio delle linee dedicate: costi di gestione elevatissimi.

Prof. Montemurro

Linea dedicata



Linea CDN



Prof. Montemurro

Reti Informatiche Aziendali

Obiettivo: scambiarsi informazioni in modo efficiente.

Gestione di una rete informatica aziendale prevede:

- i. il monitoraggio della stessa;
- ii. l'aggiornamento della stessa;
- iii. l'eventuale ampliamento della stessa;
- iv. la protezione dei dati conservati in essa.

Configurazioni tipiche di una rete informatica aziendale

1. Rete LAN per un ufficio
2. Rete client/server aziendale

Prof. Montemurro

Reti LAN per un Ufficio

Creare una rete LAN che consenta agli utenti:

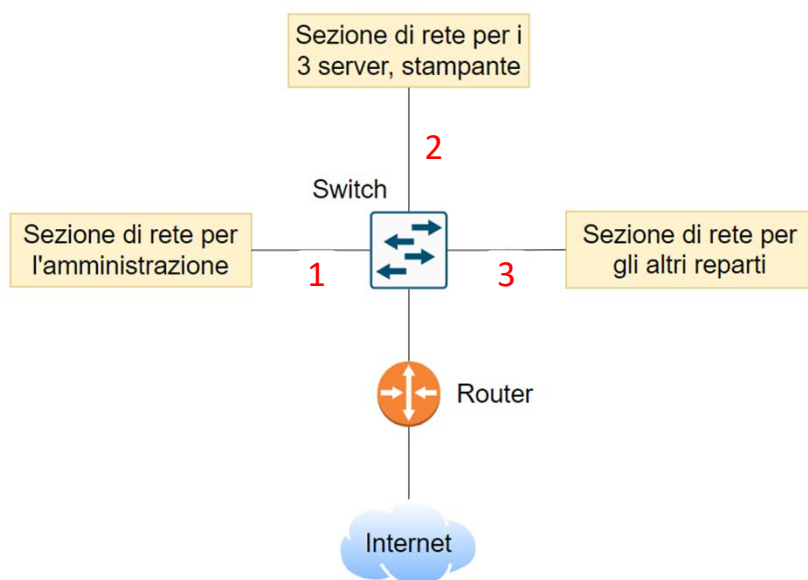
1. di comunicare internamente (servirà un server per la gestione della posta elettronica da parte di tutti gli utenti; è il **mail server**);
2. di scambiarsi file (servirà un server per la gestione centralizzata degli account degli utenti e dei file; è il **server di dominio**);
3. di navigare su internet (servirà un router);
4. di stampare documenti cartacei (servirà un **print server** ed una stampante).

Inoltre la rete deve essere suddivisa in due parti:

- i. una parte riservata all'amministrazione e ai tre server;
- ii. una parte per gli altri reparti dell'azienda.

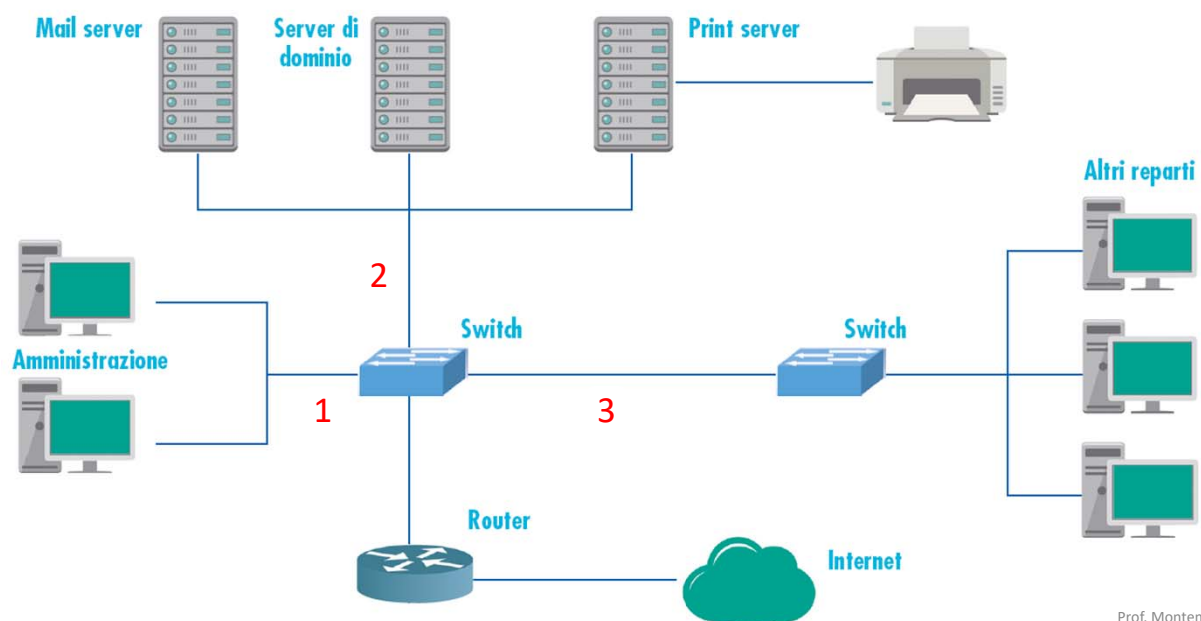
Prof. Montemurro

Reti LAN per un Ufficio: Sezioni di Rete



Prof. Montemurro

Reti LAN per un Ufficio



Prof. Montemurro

Reti Client/Server Aziendale

Rete client/server aziendale: in soldoni è come la rete LAN appena vista, in più c'è una parte della rete LAN accessibile da persone esterne all'azienda (fornitori, clienti ecc.); questa parte della rete LAN è accessibile in extranet.

Extranet: rete informatica interna a un'organizzazione (per es. un'azienda), o porzione di essa, che viene messa a disposizione anche di alcuni soggetti esterni (clienti, fornitori, partner commerciali ecc.) con un accesso regolato da password.

Prof. Montemurro

Reti Client/Server Aziendale

Vulnerabilità: debolezza in un sistema IT che può essere sfruttata da un aggressore per sferrare un attacco di successo.

Firewall di rete: è sempre un software il cui obiettivo è separare internet dalla rete aziendale in quanto quest'ultima è vulnerabile alle intrusioni non autorizzate. Si distinguono due tipi di firewall:



1. **firewall software** i quali sono firewall installati su un computer, cioè su una macchina che non si occupa solo della sicurezza della rete, ma svolge diversi compiti;
2. **firewall hardware** i quali sono software installati su una macchina il cui unico scopo è garantire la sicurezza della rete.

Prof. Montemurro

Reti Client/Server Aziendale

Politiche di default per i servizi web configurabili per il firewall

1. **Politica default deny** (è quella raccomandata): assume che tutto il traffico sia maligno per cui, di default, tutto è proibito. Quando si identifica del traffico benigno, si aggiunge una **regola di eccezione** per consentirgli l'accesso alla rete.

Vantaggio: questa politica permettere ai responsabili della sicurezza di rete di concentrarsi sul traffico benigno, invece di dover attenzionare tutte le possibili attività maligne.

2. **Politica default allow:** assume che la maggior parte del traffico sia benigno per cui, di default, tutto è concesso. Quando si identifica del traffico maligno, si aggiunge una **regola di eccezione** per bloccare il suo accesso l'accesso alla rete.

Svantaggio: questa politica obbliga i responsabili della sicurezza di rete ad attenzionare continuamente tutte le possibili attività maligne.

Prof. Montemurro

Reti Client/Server Aziendale

La rete aziendale client/server, per motivi di sicurezza perimetrale, deve essere suddivisa in due grosse sezioni di rete usando il firewall (es. router mette a disposizione la funzionalità di firewall):

1. la **trusted zone** la quale non è accessibile direttamente dall'esterno, ma indirettamente attraverso il firewall che bloccherà ogni tentativo di accesso non autorizzato. I dispositivi di rete degli utenti nella trusted zone possono accedere a tale zona autenticandosi con le proprie credenziali le quali sono gestite dal server di dominio;
2. la **DeMilitarized Zone** (o **DMZ**) la quale consente solo connessioni verso l'esterno; inoltre, per maggiore sicurezza, si fa in modo che gli host nella DMZ non possano connettersi alla trusted zone.

Prof. Montemurro

