	Corso “Progettazione e sviluppo di Data Center	Data: 02/09/2025 – 09/09/2025 A.S. 2025/2026
Docente: Prof. Roberto Fuligni	Relazione di fine corso	Autori: Davide Baldinu, Alessandro Colombo, Lorenzo Porta

I data center multi-tier web-centered

Strutture, tecnologie e implementazioni pratiche

Introduzione: Cos’è un data center?

Un **centro elaborazione dati**, abbreviato in “CED”, o in inglese “**data center**”, è l’apparato di un'organizzazione che ne coordina e ne mantiene l’infrastruttura IT e i suoi dati, mettendoli a servizio di **uno o più fruitori**. Può essere implementato sia da enti pubblici che da enti privati, e al suo interno possono essere presenti vere e proprie **server farm** anche di scala industriale.

Una **server farm** (in italiano "*fattoria di server*", chiamata anche “*webfarm*”), in informatica, è un ambiente in cui vengono collocati una serie di server in modo da poterne centralizzare la gestione, la manutenzione e la sicurezza.

Nella sua forma più semplice, un data center è una struttura fisica che le organizzazioni utilizzano per **ospitare applicazioni e dati critici**.

I data center sono importanti per le aziende per l’erogazione di una serie di **servizi**, tra i quali citiamo E-mail, condivisione di file e altri dati (database), applicazioni di produttività, desktop virtuali, servizi di comunicazione e di collaborazione, ma anche intelligenza artificiale.

La progettazione di un data center si basa su una rete di risorse di elaborazione e storage che consentono la distribuzione di applicazioni e dati condivisi e si basa su tre pilastri: **infrastruttura di rete**, **infrastruttura di storage** e **risorse di elaborazione**.

Noi analizzeremo più nel dettaglio l’infrastruttura di rete sia nei dispositivi che la compongono, sia nei protocolli che vengono impiegati per sfruttarla al meglio.

Dispositivi di rete per data center

Nei data center i dispositivi di rete sono essenziali per garantire **connettività**, **sicurezza** e **gestione del traffico** dati. Apparati come switch, router, load balancer e firewall permettono di interconnettere i sistemi, bilanciare i carichi di lavoro e proteggere le comunicazioni assicurando efficienza e continuità di servizi.

Cenni sul modello ISO/OSI

Prima di analizzare nel dettaglio i principali dispositivi di rete è importante chiarire un aspetto strettamente legato al loro funzionamento: **il modello ISO/OSI**. Al suo interno, la comunicazione viene suddivisa in 7 livelli, ciascuno con compiti ben specifici. Analizziamo, in particolare, il **livello 2** e **il livello 3**.

Il **livello 2** ("*Data Link layer*" o "*Livello di accesso in rete*") gestisce il traffico interno ad una rete permettendo a dispositivi connessi di comunicare tra loro mediante l'utilizzo del **MAC address**, un indirizzo univoco composto da 48 bit, che **identifica ogni interfaccia di rete**.

Il **livello 3** ("*Network layer*" o "*Livello di rete*"), invece, permette lo scambio di messaggi tra sottoreti e reti diverse, mediante l'uso di **indirizzi IP** (sequenze di 32 bit variamente suddivise in una parte che identifica la rete e una che identifica lo specifico host) e di protocolli di routing che permettono di instradare i pacchetti lungo il precorso più breve verso la loro destinazione.

Dispositivi di rete di base

Questi dispositivi non sono presenti unicamente nelle reti di data center, ma si possono trovare anche in contesti più piccoli (o addirittura domestici), tuttavia analizzarne il funzionamento ci aiuta a comprendere la funzione fondamentale che svolgono all'interno di reti di alto livello.

Switch

Lo **switch** (o "*switch layer 2*", abbreviato in "*switch L2*") opera a livello 2 del modello ISO/OSI. La sua funzione principale è l'**inoltro di dati** (che a livello 2 sono segmentati in frame ethernet), **sulla base degli indirizzi MAC**. Esso è in grado di imparare in maniera del tutto indipendente e dinamica le posizioni dei vari host presenti nella rete: quando riceve in ingresso un frame estrapola della sua **MAC address table**. Consultando questa tabella, lo switch è anche in grado di inoltrare i frame in ingresso al host di destinazione (**unicasting**), se il suo indirizzo fisico è già presente nella tabella, o di inviare messaggi in broadcast per localizzare destinatari che non sono presenti nella tabella (**flooding**). In questo modo è possibile eliminare traffico inutile, evitando collisioni e saturazione della rete.

Router

Il **router** opera, invece, a livello 3 del modello ISO/OSI occupandosi dell'**instradamento dei dati tra sottoreti e reti diverse**. A differenza dello switch, che si serve degli indirizzi MAC, il router **utilizza gli indirizzi IP**. Quando un router riceve un pacchetto ne analizza l'indirizzo IP di destinazione e lo confronta con le informazioni contenute nella **tabella di routing** in modo da poter individuare l'interfaccia più appropriata su cui inviare i dati per seguire il percorso stabilito. Esistono diverse possibilità per popolare la tabella di routing che verranno discusse in seguito.

Dispositivi di rete specializzati

Switch Layer 3

Lo **switch layer 3** (abbreviato in "*Switch L3*") combina le funzioni di uno **switch tradizionale** e di un **router**. È in grado sia di inoltrare i pacchetti all'interno della rete usando gli indirizzi MAC, sia instradarli tra reti diverse usando gli indirizzi IP. Un uso comune degli switch L3 è **gestire le VLAN** (*Virtual LAN*), utilizzate per dividere una rete fisica in più reti virtuali, in modo da organizzare meglio il traffico e aumentare la sicurezza. I dispositivi in VLAN diverse non possono parlare direttamente tra loro quindi lo switch L3 svolge anche la funzione di **gateway**, assegnando a ogni VLAN

un'**interfaccia virtuale** (**SVI** ovvero "*Switch Virtual Interface*") con un indirizzo IP, permettendo in questa maniera il **routing inter-VLAN**. Quando un host deve inviare dati a un altro dispositivo appartenente ad un'altra VLAN, contatterà lo switch che si comporterà come un router instradandoli verso la loro destinazione.

Il principale vantaggio di questa apparecchiatura è che con un unico dispositivo è possibile combinare i servizi di connettività in rete locale e di comunicazione con reti (virtuali) differenti. Lo switch L3 combina le **funzionalità avanzate di instradamento** di un router con l'**estrema rapidità** di uno switch per questo è molto usato nelle sottoreti di comunicazione dei campus aziendali, e quindi dei data center.

Indicazioni pratiche per gli switch layer 3

In uno switch L3 le interfacce possono lavorare in due modalità differenti: **switch-port** e **router-port**. La prima operare fino al livello 2 ISO/OSI inoltrando i pacchetti tramite indirizzo MAC, mentre la seconda si spinge fino al livello 3 instradando i pacchetti tramite IP.

Senza ulteriori configurazioni tutte le porte lavorano in modalità switchport. Per commutare lo stato di funzionamento di una porta, e assegnare all'interfaccia un indirizzo IP, è possibile operare come segue:

1. Accedere allo switch e abilitare la modalità privilegiata

```
Switch> enable
```

2. Entrare in modalità di configurazione globale

```
Switch# configure terminal
```

3. Abilitare l'instradamento IP

```
Switch(config)# ip route
```

4. Entrare in modalità di configurazione dell'interfaccia che si desidera commutare

```
Switch(config)# interface GigabitEthernet0/0
```

5. Commutare l'interfaccia

```
Switch(config-if)# no switchport
```

6. Assegnare l'indirizzo IP (ad esempio 192.168.1.1/24)

```
Switch(config-if)# ip address 192.168.1.1 255.255.255.0
```

Ipotizzando, poi, di voler utilizzare uno switch L3 come gateway predefinito della rete con indirizzo IP 192.168.1.0/24, per configurare la VLAN, assegnare ad essa un indirizzo IP e configurare la SVI è possibile procedere come segue:

1. Accedere allo switch e abilitare la modalità privilegiata

```
Switch> enable
```

2. Entrare in modalità di configurazione globale

```
Switch# configure terminal
```

3. Entrare in modalità di configurazione della VLAN specificandone l'ID (ad esempio 10)

```
Switch(config)# vlan 10
```

4. Impostare il nome della rete virtuale e uscire dalla modalità di configurazione della VLAN

```
Switch(config-vlan)# name VLAN-test
Switch(config-vlan)# exit
```

5. Entrare in modalità di configurazione della SVI indicando nuovamente l'ID della VLAN da configurare (con questo comando la SVI verrà automaticamente accesa)

```
Switch(config)# interface vlan 10
```

6. Assegnare all'interfaccia virtuale un indirizzo IP seguito dalla sua maschera di sottorete e uscire dalla modalità di configurazione dell'interfaccia

```
Switch(config-if)# ip address 192.168.1.254 255.255.255.0
Switch(config-if)# exit
```

7. Entrare in modalità di configurazione dell'interfaccia (o del range di interfacce) che apparterrà alla VLAN appena configurata

```
Switch(config)# interface GigabitEhternet1/0/1
Switch(config-if)# switchport access vlan 10
```

Altri dispositivi specializzati

All'interno dei data center è poi possibile trovare altri dispositivi di rete molto specializzati che hanno il compito di garantire maggiore efficienza e sicurezza. Tra questi citiamo i **load balancer**, dispositivi che distribuiscono in modo intelligente le richieste degli utenti, tipicamente, tra i server che compongono un cluster, ottimizzandone le prestazioni, evitando sovraccarichi e garantendo continuità del servizio in caso di guasti, e i **Router/Firewall**, speciali router equipaggiati con un firewall che monitora il traffico in ingresso e in uscita, proteggendo la rete da accessi indesiderati e attacchi informatici.

Server

In un data center tutte le tecnologie precedentemente descritte sono orientate a fornire un servizio di connettività di rete efficiente, ridondato e sicuro a degli utilizzatori particolari: i **server**. Essi rappresentano l'elemento centrale di un data center, **offrono servizi, applicazioni** e **archiviazione di dati**. Sono i nodi finali della nostra rete e hanno il compito di elaborare le richieste degli utenti, garantendo potenza di calcolo e capacità di storage.

Esistono **diverse tipologie di server** in base ai servizi che erogano, ad esempio: gli application server, che mettono a disposizione l'esecuzione di software; i database server, per lo storage e la gestione di dati; web server, che permetto la pubblicazione e l'archiviazione di siti e contenuti web; file server, per la condivisione di documenti; mail server, per la gestione e l'archiviazione della posta elettronica, e molti altri ancora.

All'interno dei data center, i server vengono, solitamente, **virtualizzati**, in modo da ottimizzare lo spazio e ridurre i costi per l'hardware, e **organizzati in cluster**, gruppi di server utili per migliorare l'affidabilità di un servizio distribuendo i carichi di lavoro e facilitare la gestione di eventuali guasti.

Il cablaggio strutturato dei campus aziendali

Il cablaggio strutturato è un **insieme di regole standardizzate**, definite nella normativa **ISO11801**, per creare una **rete di comunicazione unificata e ordinata**. Le regole di cablaggio strutturato sono

la base per la realizzazione di reti di comunicazione moderne, come quelle utilizzate in ambienti aziendali, edifici commerciali, campus universitari e data center.

Tipico schema di cablaggio strutturato per una rete di campus aziendale

Di seguito descriviamo una tipica infrastruttura di rete realizzata seguendo queste normative.

Il cablaggio strutturato prevede che venga utilizzata una **topologia ad albero**. Gli end-devices, posti su ogni postazione di lavoro, non sono direttamente collegati ai dispositivi di livello superiore, ma si connettono alla rete tramite le **Telecommunication Outlet** (**TO**), ovvero le "*prese a muro*", solitamente poste vicino alle postazioni di lavoro, alle quali è possibile collegare i dispositivi tramite cavo di rete (con connettore RJ-45 o RJ-11).

Ogni TO è collegata tramite **cablaggio orizzontale**, solitamente tramite cavi in rame, al **Telecommunication Closet** (**TC**) all'interno del quale è presente un armadio rack che contiene il **Floor Distributor** (**FD**), lo switch di piano che fornisce agli utenti l'accesso alla rete.

Questi switch sono poi collegati per **cablaggio verticale**, solitamente realizzato in fibra ottica per garantire elevate larghezze di banda, tramite i **collegamenti di uplink**, ad un **Building Distributor** (**BD**), verosimilmente uno switch layer 3, ubicato, per praticità, nel TC del piano più basso dell'edificio.

L'interconnessione tra edifici diversi è possibile grazie ad un ulteriore switch L3 ad altissime prestazioni: il **Campus Distributor** (**CD**) che funge da centro-stella per i vari BD.

Al CD è direttamente collegata una rete detta "*Campus Core*", composta da tre sezioni:

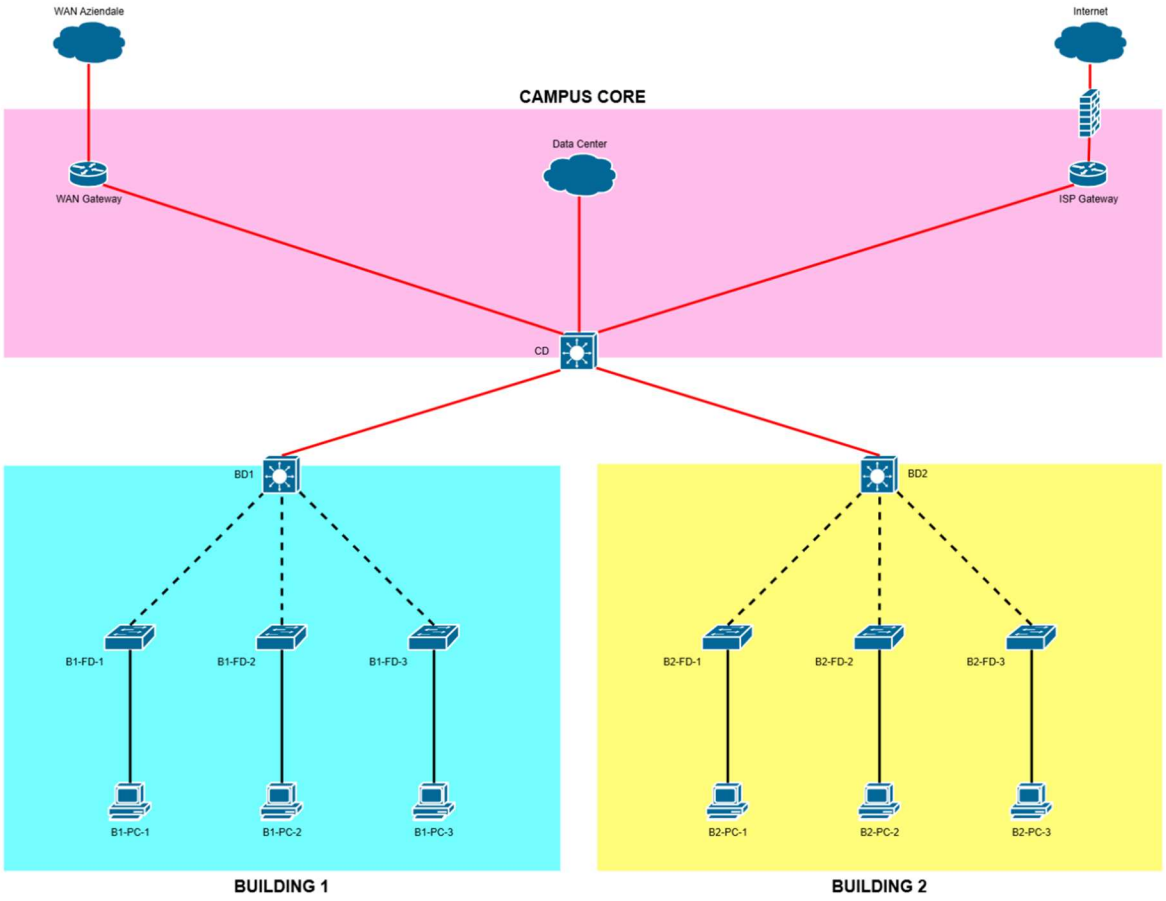
- La rete del **data center** aziendale;
- Il collegamento alla **WAN** aziendale (se presente);
- Il collegamento alla rete **Internet**;

Si va quindi a creare una infrastruttura gerarchica formata da 3 livelli:

- **Livello Access**, formato da tutti gli switch di piano presenti nei Telecommunication Closet;
- **Livello Distribution/Aggregation**, comprendente tutti gli switch che svolgono la funzione di Building Distributor;
- **Livello Core**, dove si trovano tutti gli switch che svolgono la funzione di Campus Distributor.

Nel caso di un complesso formato da soli due edifici, il livello core può essere semplificato collegando direttamente i rispettivi building distributor realizzando una infrastruttura a **Core Collassato**.

Di seguito, la topologia di una tipica rete di campus aziendale, realizzata secondo le regole del cablaggio strutturato.



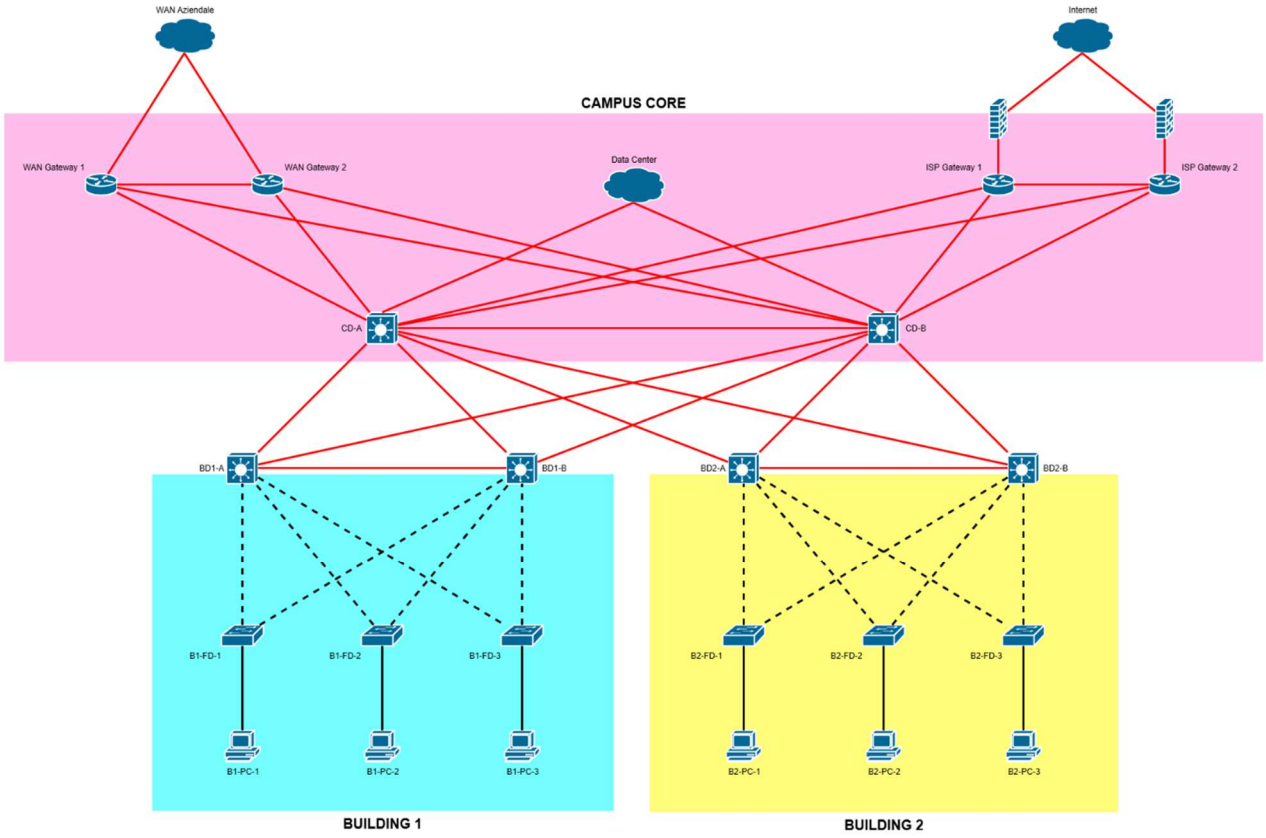
Il piano di indirizzamento per una rete come quella precedentemente descritta prevede che **ad ogni edificio sia assegnata una propria VLAN**, eventualmente partizionata per creare una rete diversa per ogni piano. Per questo motivo è utile utilizzare gli switch L3 sia a livello di building distribution, sia di core distribution.

Ridondanza

La topologia ad albero, tuttavia, porta con sé un problema: possiede una **ridotta tolleranza ai guasti**. L'interruzione di un collegamento di uplink, ad esempio, porterebbe all'isolamento di intere porzioni della rete. Per questo motivo, le regole di cablaggio strutturato prevedono l'implementazione di **sistemi di ridondanza**. Ogni dispositivo deve avere uno o più "*gemelli*", o "*dispositivi di backup*", pronti ad intervenire in caso di guasto. Grazie a specifici protocolli, vi è la garanzia che l'intervento del dispositivo di backup avvenga in appena qualche secondo in maniera completamente trasparente alla rete e agli utilizzatori, rendendo così **impercettibile il disservizio**.

Nelle reti di alto livello sono presenti anche dei **server syslog**, o sistemi analoghi, atti a segnare all'amministratore di rete la presenza di un guasto in modo che possa intervenire per ripristinare il normale funzionamento dell'infrastruttura. Questi registrano ogni messaggio di avviso o di errore prodotto dai dispositivi di rete in modo da segnalare tempestivamente i disservizi e facilitare il troubleshooting.

Di seguito, il diagramma di rete mostra come viene realizzata la ridondanza nella rete precedentemente descritta.



Protocolli di rete per data center

All'interno di un data center, la rete rappresenta **l'infrastruttura fondamentale** che garantisce la connettività, la ridondanza e l'**affidabilità** dei servizi informatici.

Per assicurare comunicazioni efficienti, sicure e continue tra i vari dispositivi di rete vengono utilizzati diversi **protocolli specializzati**, ognuno con funzioni specifiche.

Tra questi, protocolli come **STP** (Spanning Tree Protocol), **HSRP** (Hot Standby Router Protocol), **OSPF** (Open Shortest Path First) ed **Ether-Channel** svolgono un ruolo chiave nella gestione del traffico, nell'ottimizzazione dei percorsi e nella prevenzione dei guasti.

La corretta configurazione di questi protocolli è essenziale per garantire alta disponibilità, bilanciamento del carico e resilienza dell'intera infrastruttura di rete del data center.

Analizziamo ora più dettagliatamente questi protocolli.

STP: Spanning Tree Protocol

Le reti aziendali sono spesso basate su architetture **switch-based** in cui il guasto di uno switch o l'interruzione di un collegamento può causare serie ripercussioni sulla stabilità della rete.

Per ovviare a questo problema si realizzano **collegamenti ridondati tra gli switch** garantendo una maggiore affidabilità e tolleranza ai guasti: in caso di malfunzionamenti, il traffico può passare automaticamente attraverso un altro dei percorsi disponibili.

Realizzare più collegamenti tra gli switch, tuttavia, potrebbe **generare dei loop**, ovvero dei percorsi ciclici tra i dispositivi, in cui dei pacchetti potrebbero "*rimanere intrappolati*" percorrendo la rete all'infinito e causandone la saturazione. Ad esempio, se uno switch inoltrasse un messaggio in broadcast (ad esempio una richiesta ARP), questo verrebbe inoltrato a tutti i collegamenti attivi. Senza un meccanismo di controllo, lo stesso pacchetto finirebbe per circolare tra gli switch in un ciclo infinto, causando **congestione e malfunzionamenti** (questo fenomeno è detto "*Broadcast Storm*"). Per risolvere questo problema è possibile adottare lo **Spanning Tree Protocol** (STP).

STP è in grado di **rilevare la presenza di percorsi ciclici e di intervenire per "*spezzarli*"** bloccando una delle porte che generano il loop. I collegamenti sulle porte bloccate non inoltrano il traffico, pur rimanendo pronti ad essere riattivati in caso di necessità. In questo modo è possibile garantire alla rete stabilità e assenza di loop, garantendo allo stesso tempo la continuità del servizio.

Nella maggior parte degli switch moderni il protocollo **STP è già attivo di default** senza necessità di ulteriori configurazioni. La scelta delle interfacce da bloccare viene fatta dagli switch tramite lo scambio di specifici messaggi.

HSRP: Hot Standby Router Protocol

In una rete aziendale, la continuità della connessione verso reti esterne, tra cui internet, è un aspetto fondamentale. Se il router con la funzione di gateway predefinito si dovesse guastare, la rete rimarrebbe isolata dall'esterno. Per risolvere questo problema adottiamo la **ridondanza dei gateway**, offrendo alla nostra rete più router pronti ad offrire lo stesso servizio di collegamento con l'esterno, senza interrompere le comunicazioni dei client. Per poter implementare quanto descritto, è possibile utilizzare un **protocollo proprietario di Cisco**, che prende il nome di **Hot Standby Router Protocol** (HRSP).

HSRP permette a **due o più router** di **condividere un indirizzo IP virtuale** che funge da gateway per tutti i dispositivi della rete. I router partecipanti, una volta configurati, possono assumere uno di due ruoli:

- **Active router**: svolge effettivamente la funzione di gateway gestendo il traffico e inoltrando i pacchetti;
- **Standby router**: monitora l'active router e quando ne rileva il malfunzionamento gli subentra diventando il dispositivo attivo. Quando il router principale riprenderà il suo regolare funzionamento, il router di standby rilascerà la funzione di gateway tramite un meccanismo chiamato "**preemption**".

Tutti i client usano lo stesso indirizzo IP virtuale come gateway, **senza dover cambiare configurazioni** in caso di failover. Quando il gateway principale non dovesse essere operativo, tutto il traffico riuscirà a raggiungere le reti esterne attraverso uno dei gateway di backup in maniera completamente trasparente ai client.

Configurazione di HSRP su apparecchiatura Cisco

Ipotizzando di configurare HSRP su due router appartenenti alla rete con indirizzo 192.168.1.0/24 che utilizzi come gateway predefinito il dispositivo con indirizzo 192.168.1.254, è possibile procedere come segue:

a. Configurazione del router attivo:

1. Accedere al router e abilitare la modalità privilegiata

```
RouterAttivo> enable
```

2. Entrare in modalità di configurazione terminale

```
RouterAttivo# configure terminal
```

3. Entrare nella modalità di configurazione dell'interfaccia su cui si desidera abilitare HSRP

```
RouterAttivo(config)# interface GigabitEthernet0/0
```

4. Assegnare all'interfaccia il suo indirizzo IP

```
RouterAttivo(config-if)# ip address 192.168.1.252 255.255.255.0
```

5. Impostiamo l'appartenenza dell'interfaccia ad uno specifico gruppo di standby, indicato con il parametro group number (esempio: standby 1) univoco per tutta la rete, e assegniamo l'indirizzo IP all'interfaccia virtuale

```
RouterAttivo(config-if)# standby 1 ip 192.168.1.254
```

6. Stabilito che questo router sarà quello attivo di default, impostiamo un valore di priorità arbitrario (per convenzione superiore a 100) per il corretto funzionamento della preemption

```
RouterAttivo(config-if)# standby 1 priority 110
```

7. Abilitiamo la preemption

```
RouterAttivo(config-if)# standby 1 preempt
```

b. Configurazione del router di standby:

1. Accedere al router e abilitare la modalità privilegiata

```
RouterBackup> enable
```

2. Entrare in modalità di configurazione globale

```
RouterBackup# configure terminal
```

3. Entrare nella modalità di configurazione dell'interfaccia su cui si desidera abilitare HSRP

```
RouterBackup(config)# interface GigabitEthernet0/0
```

4. Assegnare all'interfaccia il suo indirizzo IP

```
RouterBackup(config-if)# ip address 192.168.1.253 255.255.255.0
```

5. Impostiamo l'appartenenza dell'interfaccia al gruppo di standby scelto per il router attivo e assegniamo l'indirizzo IP all'interfaccia virtuale.

```
RouterBackup(config-if)# standby 1 ip 192.168.1.254
```

6. Stabilito che questo sarà un router di backup, impostiamo un valore di priorità inferiore a quello impostato per il router attivo

```
RouterBackup(config-if)# standby 1 priority 100
```

7. Abilitiamo la preemption

```
RouterBackup(config-if)# standby 1 preempt
```

OSPF: Open Shortest Path First

Open Shortest Path First (OSPF) è un protocollo di **instradamento dinamico** che permette ai router di una rete di scambiarsi informazioni sulla topologia e di **calcolare automaticamente i percorsi più efficienti** per inoltrare i pacchetti.

Una rete su cui viene configurato OSPF viene **suddivisa in aree**. Ne esistono di diversi tipi con caratteristiche differenti, ma, per semplicità, ci concentreremo solo su un'area singola: la *backbone area* o *area 0*. Nel caso di una singola area, tutti i router fanno parte della stessa area e condividono tra loro **informazioni complete su tutti i collegamenti** attivi creando una mappa logica della rete.

Ogni router conosce quindi lo stato dei collegamenti di tutti gli altri router e può determinare il percorso più breve verso qualsiasi destinazione utilizzando **l'algoritmo di Dijkstra**. Questo significa che, se un collegamento diventa non disponibile o un router si guasta, OSPF rileva immediatamente il cambiamento, aggiornando la mappa della rete e **ricalcolando i percorsi alternativi senza intervento manuale**. In questo modo, i pacchetti continuano a raggiungere la loro destinazione in modo efficiente e senza interruzioni.

Questo è possibile grazie ad una analisi costante del traffico di rete svolta da una specifica routine che i router eseguono costantemente in maniera parallela al resto della loro attività chiamata "*processo OSPF*".

Anche con una singola area, OSPF garantisce quindi che la rete sia dinamica, resiliente e stabile: i router reagiscono rapidamente ai guasti, evitando percorsi inefficienti o bloccati, e assicurano che il traffico utilizzi sempre il cammino più corto disponibile.

Configurazione di OSPF a singola area su apparecchiature Cisco

Ipotizzando di configurare OSPF su un router alle cui interfacce sono collegati:

- Una rete privata con indirizzo 192.168.1.0/24;
- Un link punto-punto con indirizzo 10.0.0.0/30;
- Un link punto-punto con indirizzo 10.0.0.4/30;

è possibile procedere come segue:

1. Accedere al router e abilitare la modalità privilegiata

   ```
   Router> enable
   ```

2. Entrare in modalità di configurazione globale

   ```
   Router# configure terminal
   ```

3. Abilitare OSPF (che equivale a creare ed eseguire una nuova istanza del processo OSPF) e assegnare un ID di processo utilizzato per identificare l'istanza sul singolo router

   ```
   Router(config)# router ospf 1
   ```

4. Elencare le reti direttamente connesse la router che dovranno essere conosciute da tutti gli altri membri dell'area OSPF seguite dalla wildcard mask, in sostituzione della subnet mask, e dall'area di appartenenza (che per la configurazione a singola area sarà sempre la 0)

   ```
   Router(config-router)# network 192.168.1.0 0.0.0.255 area 0
   Router(config-router)# network 10.0.0.0 0.0.0.3 area 0
   Router(config-router)# network 10.0.0.4 0.0.0.3 area 0
   ```

   La **wildcard mask** è un modo per indicare quali parti di un indirizzo IP devono essere considerate fisse e quali possono variare. Concretamente si tratta del risultato dell'operazione di **complemento a 1 della subnet mask** e si ottiene ponendo a valore 1 tutti i bit del Host-ID di un indirizzo IP e a valore 0 tutti i bit del Net-ID.

In una wild card, **il valore 0 significa che il bit deve corrispondere esattamente** all'indirizzo specificato, mentre **il valore 1 indica che il bit è "libero"** e può assumere qualsiasi valore. Ad esempio, la wildcard 0.0.0.255 applicata all'indirizzo 192.168.1.0 significa che i primi tre ottetti devono corrispondere esattamente, mentre l'ultimo ottetto può variare da 0 a 255.

Ether-Channel

Ether-Channel è una tecnologia che permette di realizzare l'**aggregazione** (o *bonding*) **di porte su una apparecchiatura Cisco**, ovvero permette di raggruppare più interfacce fisiche, di uno switch o di un router, in un'unica interfaccia logica (detta anche "*bond di interfacce*"). In questo modo, collegandole opportunamente, esse agiscono come un singolo "canale" garantendo così una serie di benefici:

- **maggiore larghezza di banda**: la somma delle singole velocità delle interfacce fisiche;
- **ridondanza e tolleranza ai guasti**: se un collegamento dovesse cadere, il traffico verrà ridistribuito automaticamente sugli altri collegamenti;
- **semplificazione della configurazione**: più link sono gestiti come un'unica interfaccia logica.

Configurazione di Ether-Channel su apparecchiature Cisco

Ipotizzando di configurare Ether-Channel su uno switch dotato di 4 interfacce con larghezza di banda 1 gigabit nominate: GigabitEthernet0/0, GibabitEthernet0/1, GigabitEthernet0/2 e GigabitEthernet0/3 è possibile procedere come segue:

1. Accedere allo switch e abilitare la modalità privilegiata

```
Switch> enable
```

2. Entrare in modalità di configurazione globale

```
Switch# configure terminal
```

3. Selezionare le interfacce da aggregare specificando il range

```
Switch(config)# interface range GigabitEthernet0/0-3
```

4. Creare il gruppo Ether-Channel specificando l'ID da assegnare la gruppo e la modalità di aggregazione

```
Switch(config-if-range)# channel-group 1 mode active
```

Più nel dettaglio, ipotizzando di stare eseguendo la configurazione di uno switch L3 dove le quattro interfacce aggregate debbano svolgere la funzione di router-port per un link punto-punto con indirizzo 10.0.0.0/30, l'indirizzo IP è assegnabile come segue:

1. Uscire dalla modalità di configurazione del range di interfacce

```
Switch(config-if-range)# exit
```

2. Entrare nella modalità di configurazione dell'interfaccia logica associata alle porte aggregate specificando l'ID precedentemente assegnato al bond

```
Switch(config)# interface Port-channel 1
```

3. Impostare l'indirizzo IP

```
Switch(config-if)# ip address 10.0.0.1 255.255.255.252
```

4. Accendere l'interfaccia

```
Switch(config-if)# no shutdown
```

Struttura tipica di un data center multi-tier web-centered

L'architettura multi-tier

Una topologia di rete molto diffusa per i data center è **l'architettura multi-tier**. Questa, come suggerisce il nome, prevede **un'organizzazione in livelli** del centro di elaborazione. Il numero dei livelli, così come la complessità interna di ogni livello, possono variare in base al caso specifico. Come i server possono erogare un gran numero di servizi diversi, **è possibile realizzate un livello specializzato per ogni servizio**.

Ogni tier costituisce una sottorete a se stante solitamente composta da:

- **router o router/firewall** per interconnetterla con gli altri tier o con la rete di campus;
- **switch L2** che fornisce connettività ad un **cluster di server** configurati per erogare uno o più servizi specifici;
- **load balancer** per distribuire il carico di lavoro sul cluster di server e monitorarne lo stato di salute.

L'interfaccia di rete del load balancer è "*la porta di accesso*" ai servizi del data center: è lui ad essere contattato con le richieste provenienti dall'esterno che poi demanderà ad uno dei server del cluster in base al carico di lavoro in quel momento.

Tutte le apparecchiature precedentemente citate sono ovviamente **ridondate** per garantire la tolleranza ai guasti e ridurre la congestione della rete. I server, in particolare, erogando servizi essenziali sia nel data center che al di fuori, sfruttano il **bonding delle interfacce** per aumentare la larghezza di banda e fornire la ridondanza del loro collegamento fisico con gli switch in modo da ridurre al minimo le probabilità di rimanere isolati.

I tre livelli fondamentali di un data center

In generale, in un data center, anche di piccole dimensioni, troveremo sicuramente **tre livelli fondamentali**: **Web Tier**, **Application Tier** e **Database Tier**.

Web Tier

Il Web Tier è sempre **il più basso della gerarchia**: è un livello che ha la possibilità di **interfacciarsi direttamente** sia con il resto della rete di campus, sia con la WAN aziendale e addirittura, qualora fornisse anche servizi esterni, con Internet.

Al suo interno troviamo dei **server web** che possono servire sia la rete di campus (intranet), ospitando, ad esempio, un sito per la gestione delle risorse aziendali, sia la rete pubblica (extranet o internet), ospitando il sito internet dell'azienda proprietaria del data center.

Application Tier

In questo livello sono presenti degli **application server** che forniscono alla rete di campus **applicazioni specifiche** (basate, ad esempio, sul modello Client/Server puro) e/o **servizi applicativi per il Web Tier**, anche rivolti ad internet, come, ad esempio, la gestione di una transazione bancaria.

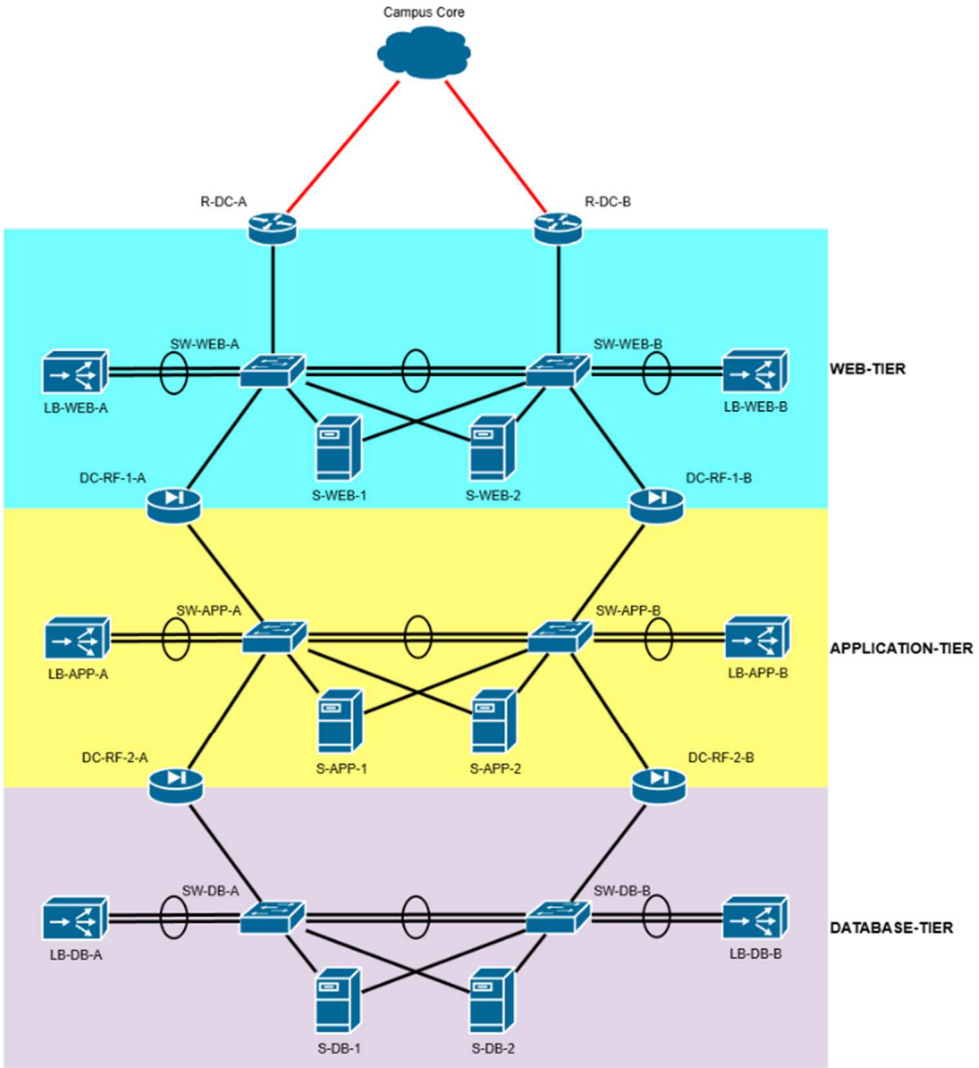
L'accesso a questo livello è **protetto da dei router firewall** in quanto le applicazioni non devono essere direttamente accessibili dall'esterno, ma devono essere raggiunte solo da alcune specifiche richieste provenienti, principalmente, dai web server.

Database Tier

I server degli altri livelli potrebbero avere la necessità di **memorizzare dati su supporti affidabili**, per questo si adotta un **Database Tier**. I server qui presenti svolgono unicamente il servizio di **archiviazione delle informazioni in basi di dati**. Si tratta di server con un'ampia capacità di storage che, di fatto, custodiscono l'intero patrimonio informativo aziendale.

Anche a questo livello l'accesso è controllato tramite router/firewall per impedire l'accesso diretto dall'esterno.

Di seguito, la topologia tipica di un data center web-centered composto dai tre tier sopra descritti.



Comunicazione tra i livelli

Per poter far comunicare i vari livelli tra loro occorre impostare delle rotte tra i router, ma usare OSPF in questo contesto non è una scelta applicabile, in quanto, è necessario che ogni tier abbia una

conoscenza limitata delle altre reti raggiungibili in modo da porre un ulteriore livello di sicurezza contro gli attacchi informatici. Possiamo raggiungere questo obbiettivo impostando delle rotte statiche sui router di collegamento tra i tier.

Impostazione di rotte statiche su apparecchiature Cisco

Ipotizzando che ad un router siano collegati due tier distinti di un data center:

- Tier 1 con indirizzo di rete 10.1.1.0/24, default gateway 10.1.1.254, gateway verso Tier 2 10.1.1.253;
- Tier 2 con indirizzo di rete 10.1.2.0/24;

e che il router con la funzione di default gateway abbia come indirizzo IP 10.1.0.254/24 (appartenente al tier inferiore, ma connesso al router che stiamo configurando), è possibile procedere come segue:

1. Accedere al router e abilitare la modalità privilegiata

```
Router> enable
```

2. Entrare in modalità di configurazione globale

```
Router# configure terminal
```

3. Inserire una nuova rotta indicando l'indirizzo della rete da raggiungere seguito dalla sua subnet mask e dall'indirizzo IP del router di Next Hop

```
Router(config)# ip route 10.1.2.0 255.255.255.0 10.1.1.253
```

4. Impostare la Default Route per instradare tutti i pacchetti destinati a reti non conosciute (Indirizzo di rete: 0.0.0.0; Subnet mask: 0.0.0.0)

```
Router(config)# ip route 0.0.0.0 0.0.0.0 10.1.0.254
```