Switch, Router e Firewall

Switch

Uno **switch** (in italiano ***commutatore***) è un dispositivo di rete che si occupa di commutazione a livello datalink, cioè il livello 2 del modello ISO/OSI. In una rete di computer, collega insieme i vari dispositivi attraverso singoli cavi per ogni dispositivo. Gli switch gestiscono il flusso di dati attraverso la rete trasmettendo un pacchetto di rete ricevuto solo a uno o più dispositivi per i quali il pacchetto è destinato.
Ogni dispositivo collegato in rete a uno switch può essere identificato dal suo indirizzo **MAC**, consentendo allo switch di dirigere il flusso del traffico massimizzando la sicurezza e l'efficienza. Lo switch dispone di una memoria volatile (**MAC table**) che viene riempita con le associazioni fra le porte e i MAC osservati su di esse, in modo da poter tracciare le connessioni fra le porte in funzione.
Internamente, uno switch è costituito da una o più schede munite di **porte**. A ogni porta può essere connesso un **nodo**, che può essere una stazione, un altro switch, uno hub o un altro dispositivo di rete.
Quando un nodo A cerca di comunicare con un nodo B, il comportamento dello switch dipende dalla scheda cui è collegato B:

- Se B è collegato a una porta sulla stessa scheda cui è collegato A, la scheda stessa inoltra i frame in arrivo su tale porta.

- Se B è collegato a una scheda diversa da quello cui è collegato A, la scheda invia i frame a un canale di trasmissione interno della backplane che provvede a consegnare il frame alla scheda giusta.

Spesso su alcune porte possono essere montati trasduttori di tipo diverso per risolvere diversi tipi di esigenze. Questa possibilità viene tipicamente utilizzata per aggiungere a uno **switch 100Base-TX** una o due porte di tipo **1000Base-X** per il collegamento verso il resto della rete (uplink) o un server veloce.
Alcuni switch hanno una costruzione modulare, ovvero le schede possono essere montate dal gestore, per modulare il numero di porte a disposizione o per utilizzare porte di tipo diverso. È possibile realizzare uno switch anche con un comune computer dotato di più interfacce di rete, anche se non è economicamente conveniente.

Lo switch agisce sull'**indirizzamento** e nell'**instradamento** all'interno delle reti LAN mediante indirizzo fisico (MAC), selezionando i frame ricevuti e dirigendosi

verso il dispositivo corretto (leggendo il MAC di destinazione). L'instradamento avviene per mezzo di una corrispondenza univoca porta-indirizzo.
Lo **switch** ha un comportamento analogo a quello del **bridge**, mentre si differenzia dal **router**, che opera a livello 3, e dall'hub che invece è solamente un ripetitore multiporta di strato fisico ovvero diffusivo senza indirizzamento.
Uno switch separa i domini di collisione connessi alle sue porte, ovvero se due computer collegati a porte diverse trasmettono in contemporanea, non si verifica una collisione tra le due trasmissioni, che attraversano lo switch contemporaneamente.
Normalmente uno switch non è in grado di interconnettere reti di livello 2 eterogenee mentre può interconnettere ad esempio reti Ethernet con velocità o tecnologia fisiche diverse.

La **funzione di instradamento** è basata sull'apprendimento passivo progressivo degli indirizzi sorgente contenuti nei frame inoltrati (**transparent learning** o **backward learning**) che lo switch associa univocamente alla rispettiva porta di provenienza: questa associazione porta-indirizzo viene poi memorizzata in un tabella di instradamento di livello 2 chiamata **forwarding database**.
Alcuni frame hanno un indirizzo destinazione particolare, denominato broadcast, che indica che sono destinati a tutti i dispositivi della rete. Lo switch provvederà ad inoltrarli su tutte le porte.
Il fatto che i frame vengano trasmessi selettivamente ha anche delle implicazioni di sicurezza informatica, in quanto evita che un computer possa facilmente intercettare (**sniffare**) il traffico instradato a un altro terminale. Sono state però sviluppate altre tecniche, come **switch flooding**, **port stealing** e **ARP poisoning**, che permettono lo sniffing, per cui uno switch non deve essere considerato come una protezione inattaccabile e bisogna dotare la rete di altri dispositivi di protezione.

Router

Il **router** è un dispositivo che si occupa di incanalare il traffico tra due o più dispositivi connessi alla stessa rete o nelle sottoreti. L'esistenza di un router in una rete non è direttamente collegata al fatto che esista o meno una connessione ad internet, dato che può essere utilizzato internamente alla rete locale LAN.
Nel caso un router abbia la possibilità di collegarsi ad internet tramite una connettività adsl, esso integrerà un modem che si occuperà della connessione tra la rete locale ed internet.

Ad oggi, si possono facilmente trovare sul mercato tipologie di router in grado di generare reti Wi-Fi, o che integrano un media server per lo streaming diretto di contenuti multimediali dalla rete e tanto altro ancora.

I router sono particolarmente *intelligenti*, infatti leggono un indirizzo più completo rispetto allo switch per determinare il punto successivo a cui inviare il pacchetto dei dati.
Basandosi su una **mappa di rete** denominata **tabella di routing**, i router possono fare in modo che i pacchetti raggiungano le loro destinazioni attraverso i percorsi più efficaci. Se cade la connessione tra due router, per non bloccare il traffico, il router sorgente può definire un percorso alternativo.
I router creano anche i collegamenti tra reti che utilizzano protocolli diversi. Possono collegare reti situate nello stesso luogo o in un gruppo di edifici ma sono usati soprattutto per il collegamento WAN tra reti fisicamente distanti.
In pratica un router è un **computer di commutazione** che prende parte all'instaurazione di un collegamento in una rete di computer con commutazione di pacchetti, come ad esempio la rete Internet. Tali computer instradano i pacchetti di dati verso la destinazione servendosi dell'indirizzo IP di un protocollo, come ad esempio il TCP/IP.
L'indirizzo IP di un pacchetto di dati comunica a quale sottorete, a quale altro router o computer si devono inviare i dati. Una volta che il router determina dove il pacchetto deve essere spedito, trova la strada più veloce per spedire, deve inoltre spedire questi dati nel formato più adatto per il trasferimento delle informazioni. Ciò significa che può *reimpacchettare* i dati o frammentarli in pezzi più piccoli, in modo tale che il destinatario li possa gestire.

Firewall

Secondo la definizione Cisco, un **firewall** è un dispositivo per la sicurezza della rete che permette di monitorare il traffico in entrata e in uscita utilizzando una serie predefinita di regole di sicurezza per consentire o bloccare gli eventi.
I firewall rappresentano la prima linea di difesa per la sicurezza della rete, costituiscono inoltre una barriera tra le reti interne, sicure e controllate, e le reti esterne. Infine, un firewall può essere costituito da un componente hardware, software o entrambi.

In rete i dati vengono trasmessi mediante alcuni protocolli, tra cui TCP/IP. Ogni insieme di dati viene suddiviso in pacchetti: il mittente contatta il destinatario e quando questo accetta la connessione, gli invia i pacchetti. Ogni pacchetto dispone

di un'etichetta (**header**) con diverse informazioni che consentono al destinatario di ricostruire i dati originali inviati, tra cui gli indirizzi IP, la porta di destinazione e il protocollo di trasmissione. Il firewall quindi analizza i dati contenuti in queste etichette, li confronta con le regole di filtro impostate e decide se bloccare o lasciar passare la connessione.

I firewall più semplici sono soggetti a minacce, come lo spoofing dell'IP, che sostituisce l'IP che verrebbe bloccato con uno invece legittimo.

Esistono diversi tipi di firewall:

- **Firewall proxy:** il firewall proxy funge da gateway tra le reti per una specifica applicazione. I server proxy possono offrire funzionalità aggiuntive come il caching e la protezione dei contenuti, che impediscono connessioni dirette dall'esterno della rete. Questa soluzione può tuttavia avere ripercussioni sulla velocità di trasmissione e sulle applicazioni supportate.

- **Firewall stateful inspection:** il firewall stateful inspection, oggi considerato il tipo "tradizionale", consente o blocca il traffico secondo regole basate sullo stato, sulle porte e sul protocollo. Monitora tutta l'attività dal momento in cui viene stabilita una connessione fino alla sua chiusura. L'applicazione del filtro viene decisa sulla base delle regola definite dall'amministratore e del contesto, ovvero su informazioni relative a connessioni precedenti e pacchetti appartenenti alla stessa connessione.

- **Firewall a livello di applicazioni:** questo tipo di firewall sono dedicati a una singola applicazione, funzionano come intermediari nella comunicazione di dati tra questa e la rete esterna o altre applicazioni. Questi firewall svolgono un'analisi molto più approfondita e possono bloccare le connessioni in tempo reale. Si tratta di soluzioni di livello aziendale, utili quando il grado di sicurezza richiesto è molto alto.

- **Firewall NG:** Oggi i firewall non si limitano più al filtro dei pacchetti e all'esecuzione di stateful inspection. La maggior parte utilizza soluzioni **Next-Generation Firewall** per bloccare le minacce più recenti come malware e gli attacchi a livello di applicazione. L'**NGFW** incentrato sulle minacce consente di:
    - Individuare le risorse più a rischio con informazioni dettagliate sul contesto

    - Reagire tempestivamente agli attacchi grazie all'automazione intelligente della sicurezza che consente di impostare le policy e rafforzare le difese in modo dinamico
    - Rilevare in modo più efficace le attività evasive o sospette tramite la correlazione degli eventi della rete e dell'endpoint
    - Ridurre notevolmente l'intervallo di tempo tra l'individuazione e l'intervento correttivo con soluzioni di sicurezza retrospettiva che monitorano costantemente la rete per rilevare attività e comportamenti sospetti anche dopo l'indagine iniziale
    - Semplificare l'amministrazione e ridurre la complessità grazie a policy unificate che proteggono la rete in tutte le fasi dell'attacco

- **Sistemi di gestione unificata delle minacce UTM:** questi sono veri e propri sistemi integrali di cybersicurezza che, tra le altre cose, contengono anche un firewall. Differiscono dai firewall NG perchè ne esistono versioni più economiche che contengono anche VPN e altre funzioni.

Il firewall è un elemento importantissimo degli strumenti di cybersicurezza, data la quantità e complessità delle nuove minacce informatiche, ogni aggiunta al nostro sistema di protezione è indispensabile.

Fonti:

https://it.wikipedia.org/wiki/Switch

https://vitolavecchia.altervista.org/cose-e-a-cosa-serve-uno-switch-di-rete-in-informatica/

https://www.robadainformatici.it/cose-un-router/

https://vitolavecchia.altervista.org/che-cosa-e-un-router-in-informatica/

https://www.cisco.com/c/it_it/products/security/firewalls/what-is-a-firewall.html

https://www.pandasecurity.com/it/mediacenter/che-cose-un-firewall/