

Verifica di sistemi

-TCP/IP ----comunicazione tcp----rip 1 e 2----subnetting-----supernetting-----ospf

-Protocollo TCP/IP

Sono fondamentali per navigare in rete. Tramite i protocolli, i pacchetti di dati vengono trasferiti nella LAN o WAN, quindi anche in Internet.

Prende il nome dai suoi protocolli più importanti, TCP e IP.

I livelli del TCP/IP contengono protocolli relativamente indipendenti che possono essere usati a seconda delle necessità. Il protocollo TCP/IP, essendo antecedente al modello OSI, doveva essere solo una soluzione transitoria ma alla fine non è stato così. Il modello OSI rimane un modello di riferimento soprattutto per i livelli bassi.

Applicativo	Realizza servizi di livello applicativo per Internet utilizzando protocolli http, ftp etc. Implementa le applicazioni di rete.
Trasporto	è detto anche livello TCP. In questo livello sono standardizzati due protocolli: TCP e UDP. Il protocollo UDP (connection less) è fatto per i flussi e funziona per mezzi che fanno pochi errori (streaming). Si usa quando si utilizza un solo pacchetto. Il protocollo TCP (connection oriented) crea un canale di comunicazione con ACK. Invia pacchetti uno alla volta e deve attendere la risposta del destinatario. Se il pacchetto non arriva a destinazione, lo rinvia.
Rete	è detto anche livello IP. Si occupa dell'instradamento dei pacchetti nella rete, dell'interconnessione delle reti e routing. Utilizza protocolli IP e include le funzioni dello strato Network del modello OSI (connectionless).
Interfaccia alla rete	è lo strato di accesso alla rete perché consente di utilizzare risorse di rete diverse tra loro. Include informazioni degli strati Physical, Data Link e Network (in parte) del modello OSI.

-Connection less: più veloce ma meno affidabile (**protocollo UDP**);

-Connection oriented: meno veloce ma più affidabile (**protocollo TCP**). Anche se il pacchetto prende strade diverse, si ha sempre la certezza dell'arrivo di esso grazie all'Ack. Questa verifica però rallenta il processo.

Protocollo UDP: è fatto per i flussi e funziona per mezzi affidabili e che fanno pochi errori (streaming). Si usa quando si utilizza un solo pacchetto e quando la perdita di un pacchetto non è importante.

Protocollo TCP: crea un canale di comunicazione con ACK. Invia pacchetti uno alla volta e deve attendere la risposta del destinatario. Se il pacchetto non arriva a destinazione, lo rinvia.

-AUTONOMOUS SYSTEM

Prima esisteva il single network. Successivamente si è passato agli AS, che sono dei sistemi formati da un insieme di router e LAN raggruppati secondo criteri topologici. Gli AS sono formati dagli Interior Router e, che instradano messaggi a altri router che fanno parte dello stesso AS (utilizzano Interior Protocol) e dagli Exterior Router, che instradano messaggi a un altro router che fa parte di un altro AS. Ciascun ER conosce le reti raggiungibili utilizzando i link che lo collegano agli altri ER ma non conosce il modo in cui queste reti sono connesse all'interno degli AS. Gli accordi tra i gestori di AS differenti per stabilire le politiche di transito e raggiungibilità sono detti accordi di peering (si stabilisce una relazione quando un EP viene attivato tra due AS diversi).

Gli AS hanno una propria dorsale e sono numerati. Gestiscono un insieme coerente di indirizzi (ottenuti con il supernetting o semplicemente indirizzi di una stessa classe).

La metrica varia in base ai next hop che si percorrono per raggiungere il router di destinazione. Per un router direttamente connesso la metrica sarà 0, per un router che percorre un altro router sarà 1. I salti vanno da 1 a 15 (16 è irraggiungibile).

-RIP 1

Il Rip fa parte delle reti Distance Vector (router dinamico), ovvero tiene conto del carico istantaneo della rete. Insieme all'EIGRP, è il protocollo più leggero. Ogni router misura la distanza che lo separa dai nodi adiacenti ricevendo i dati dai router vicini.

La sua metrica è il numero di hop (max 16), è la più semplice ma anche la meno efficiente: il rip non può quindi essere usato in configurazioni con più di 15 router.

Le sue tabelle di routing vengono aggiornate ogni 30 secondi.

Con il RIP il router spedisce update contenenti parte delle loro tabelle di routing (ogni 30 secondi), e di conseguenza riceverà update dai router direttamente connessi (annuncia le reti). Con il comando network stiamo istruendo il protocollo (non il router) a conoscere le reti adiacenti.

Un difetto del RIP è che funziona male in una configurazione lineare. Infatti se in presenza di n router, si interrompono dei collegamenti tra di essi (**poisoning della rete**), si crea un loop tra i pacchetti dei router in funzione (**count to infinity**) e l'**hop count** sale. Per risolvere questo problema viene utilizzato lo **split horizon** oppure il **poisoning riverse**.

Count to infinity: loop dei pacchetti tra router adiacenti (routing loops).

Split horizon: è un metodo che permette di prevenire il routing loops, infatti impedisce a un router di inviare informazioni di route al router da cui le ha apprese.

Poisoning: rende indisponibile una rete.

Poisoning riverse: è uno split horizon con update poison reverse che, a differenza dello split horizon, invia ugualmente le informazioni ma gli attribuisce una metrica infinita (16) e quindi la destinazione risulta irraggiungibile. Anche questa tecnica elimina i loops fra i router adiacenti.

Trigger update: il router invia una nuova tabella di route a seguito di un cambiamento, per far propagare le informazioni immediatamente senza aspettare il tempo standard di 30 secondi.

Hold down timer: serve quando un nodo riceve la notifica di un altro router offline (avvelenato). Esso avvia un timer di tolleranza per dare il tempo ai dispositivi offline di riprendersi senza dover aggiornare le rispettive tabelle di routing.

Flush: eliminazione di una riga della tabella di routing.

RIP V1 (broadcast); RIP V2 (multicast)

-RIP 2

In aggiunta rispetto al RIP 1, nel pacchetto è presente anche un campo chiamato Subnet Mask che contiene la subnet mask della sottorete considerata.

Inoltre viene introdotta un'altra novità che riguarda i messaggi di update. Mentre nel RIP 1 vengono inviati in broadcast, nel RIP 2 vengono inviati in multicast, interessando solo certi router e alleggerendo il numero di informazioni da trasmettere.

-OSPF

È un protocollo di routing che utilizza l'algoritmo Link State e si basa sulla creazione di database. Questo protocollo è in grado di rispondere in modo tempestivo alle variazioni topologiche dell'autonomous system con un rapido aggiornamento delle routing-information con un traffico di protocollo ridotto.

Si divide in aree: ogni area ha il suo database topologico e quindi ogni router ha quello della sua rispettiva area. Questo fa sì che si riduca il traffico di routing. Con questa organizzazione ci saranno due tipi di routing (livelli):

-routing intra-area, quando la sorgente e la destinazione dei pacchetti si trovano nella stessa area;

-routing inter-area, quando la sorgente e la destinazione dei pacchetti si trovano in aree diverse.

Backbone: area che è formata da tutte quelle reti che non appartengono a nessun'area (più i router di confine).

Classificazione dei router:

-router interni: router che sono connessi direttamente alle reti appartenenti alla stessa area (anche backbone);

-router di confine dell'area: router collegati a più aree;

-router backbone: router che hanno un'interfaccia backbone (se hanno solo interfacce backbone sono da considerare router interni);

-router di confine dell'AS: router che scambiano informazioni con altri AS (solo chi conosce i cammini può instradare l'informazione verso l'esterno).

Sotto-protocolli OSPF:

-protocollo Hello: verifica la connessione e che i link siano attivi con lo scambio di un datagramma semplice ogni hello-interval secondi.

-protocollo exchange: alimenta e crea i link state database (matrici di adiacenze);

-protocollo di flooding: invia informazioni sui cambiamenti di metrica.

Il protocollo Hello è sempre attivo.

Il protocollo Exchange quando ci sono cambiamenti topologici;

Il protocollo Flooding per alcuni eventi.

Subnetting:

è un'operazione di segmentazione della rete in sottoreti, utile per ottimizzare il traffico in una rete (2^x-2)

Supernetting:

è un sistema ideato per porre rimedio a sprechi e carenze. Crea una super rete composta da più reti.