Networking

Paolo Bettelini

Contents

1 Router

Il router è un nodo della rete che si occupa della commutazione dei pacchetti a livello 3 del modello OSI.
La communtazione è dunque basata sugli indirizzi di livello 3 del modello OSI.
Il route si occupa di instradare i pacchetti fra 2 o più sottoreti. A ciascuna delle sottoreti è assegnata un'interfaccia.

2 Switching

Con switching si intende l'instradamento effettuato a livello di collegamento.
La commutazione avviene al livello 2.
Gli switch contengono una tabella di rete contenente gli indirizzi MAC di tutti i computer collegati.

2.1 Routing protocols

Le rotte possono essere specificate manualmente (static routing), oppure possono essere utilizzati dei protocolli che permettono ai router di scambiarsi le informazioni circa la topologia della rete.

2.2 Algoritmi non adattivi

2.2.1 Dijkstra Algorithm

Permette di trovare i cammini minimi in un grafo.

2.2.2 Flooding

Consiste nell'inoltrare un pacchetto pacchetto in ingresso su tutte le linee ad eccezione di quella da cui proviene.

2.3 Algoritmi adattivi

2.3.1 Tipologia

I protocolli di instradamento sono principalmente divisi in due categorie: quelli interni al proprio sistema autonomo (**IGP**, Interior Gateway Protocol), mentre quelli fra sistemi autonomi (**EGP**, Exterior Gateway Protocol).

2.3.2 IGP

Questi protocolli possonoe ssere suddivisi in due categorie principali: **Distance Vector** e **Link State**. I protocolli Distance Vector inviano informazioni circa la topologia solo ai router adiancenti, mentre quelli di tipo Link State comunicano con tutti i router del proprio sistema autonomo.

Protocols:

- **Distance Vector**
  - **RIP** (Routing Information Protocol)
  - **IGRP** (Interior Gateway Routing Protocol)
- **Link State**
  - **IS-IS** (ntermediate System to Intermediate System)
  - **OSPF** (Open Shortest Path First)
- **Ibridi**
  - **EIGRP** (Enhanced Interior Gateway Routing Protocol)

2.3.3 EGP

Protocols:

- **EGP** (Exterior Gateway Protocol), obsolete
- **BGP** (Border Gateway Protocol)

2.4 Distance Vector

Il protocollo Distance Vector, anche noto come **Bellman-Ford** routing, è un algoritmo di routing dinamico che tiene conto del carico istantaneo della rete. Questi algoritmi sono più leggeri rispetto a quelli Link State.

Ogni router misura periodicamente la distanza (secondo vari fattori) che lo separa dai nodi adiacenti e riceve i dati dai router vicini. Utilizzando l'algoritmo di Bellman- Ford, stima *distanza* e calcola *il primo passo del percorso*.

2.5 Link State

Il protocollo Link State conosce l'intera topologia della rete e tutti i costi dei vari collegamenti.
I nodi calcolano e inviano le informazioni sulla rete agli altri nodi mediante dei pacchetti **link state broadcast**. Ognu router sfrutta un algoritmo di Dijkstra per calcolare il cammino minimo a tutti gli altri nodi della rete.

2.6 RIP Protocol

Il protocollo RIP è un protocollo Distance Vector ed utilizza il conteggio degli hop come metrica. Il massimo di hop è 15 e trasmette ogni 30 secondi la propria tabella di routing.

Ci sono 3 versioni di RIP: RIPv1, RIPv2, e RIPng

- **RIPv1**: Gli aggiornamenti delle tabelle di routing non contengono la maschera di sottorete rendendo impossibile la creazione di sottoreti di dimensione diversa all'interno della stessa rete. Non c'è autenticazione.
- **RIPv2** Include il trasporto delle informazioni sulla maschera di sottorete, supportando così il Classless Inter-Domain Routing, CIDR. Autenticazione semplice con testo in chiaro e MD5
- **RIPng** È un'estensione del protocollo originale RIPv1 per supportare IPv6.

2.7 IGRP Protocol

L'Interior Gateway Routing Protocol (IGRP) è un protocollo di routing di tipo Distance Vector.
Supporta metriche multiple quali *larghezza di banda*, *carico della linea*, *ritardo e affidabilità*.
Il massimo di hop è 255 e la trasmissione della tabella di routing avviene ogni 90 secondi.

2.8 EIGRP Protocol

L'Enhanced Interior Gateway Routing Protocol è il successore dell'IGRP.
L'aggiornamento delle informazioni del network avviene solo quando c'è un cambiamento di stato. Il massimo numero di hop è 244.

2.9 IS-IS Protocol

L'Intermediate System To Intermediate System è un protocollo di routing di tipo Link State che permette agli Intermediate System (IS) all'interno di un dominio di Routing di scambiarsi configurazioni e informazioni di Routing.

2.10 OSPF Protocol

Il protocollo Open Shortest Path First è uno dei protocolli più diffusi (Link State).
L'aggiornamento delle informazioni del network avviene solo quando c'è un cambiamento di stato.

3 Hub

L'hub è un dispositivo di rete che funga da nodo si smistamento. L'hub è un ripetitore multiporta, questo significa che inoltre i pacchetti su tutte le sue porte.

Vi sono tre categorie di Hub:

- **Attivi**: più diffusi, essi necessitano di alimentazione per amplificare il segnale.
- **Passivi**: Non amplificano il segnale, quindi non necessitano di alimentazione. Si limitano a connettere fisicamente i cavi.
- **Ibridi**: Sono particolari ed avanzati hub che permettono il collegamento tra più tipologie di cavo.

4 Bridge

Un bridge è un dispositivo di rete che si colloca al livello (2) datalink del modello ISO/OSI e che traduce da un mezzo fisico ad un altro all'interno di una stessa rete locale.
Il bridge è in grado di leggere i frame dei vari pacchetti ed individuare mittente e destinatario.
Il bridge differisce dallo switch in quanto ha generalmente meno porte ed è spesso usato per connettere diversi segmenti di rete, piuttosto che i singoli host.
Quando riceve un frame identifica il destinatario.

- Se si trova nello stesso segmento del mittente evita di inoltrare il messaggio
- Se non si trova nello stesso segmento inoltra il messaggio verso il segmento del destinatario
- Se il segmento del destinatario è sconosciuto, inoltra il messaggio su tutte le sue porte eccetto quella del mittente

4.1 Collisions

Ogni segmento di rete collegato ad una porta di un bridge costituisce un dominio di collisione. Il bridge applica l'algoritmo **CSMA/CD** se individua un problema di collisione su un segmento di rete.

4.2 Spanning Tree

Per questioni di affidabilità è possibile creare delle connessioni ridondanti fra i segmenti di rete. Questo potrebbe portare ad un loop di moltiplicazione del messaggio.

Il problema si evita con la creazione automatica di uno spanning tree, cioè di un sottogruppo della rete privo di anelli.

Le porte del bridge (e switch) possono essere in 5 stati

1. Blocking
2. Listening
3. Learning
4. Forwarding
5. Disabled

Da ogni stato si può solamente passare ad uno degli stati successivi.

4.3 Switch

Lo switch è un commutatore di pacchetti del livello 2 (Data-Link del modello ISO/OSI) che si occupa di instradare i pacchetti all'interno di una rete locale. Esistono tuttavia switch che lavorano al livello 3. A differenza dell'hub, i pacchetti vengono letti e inoltrati solamente sulla porta collegata al destinatario.

Esistono 3 tipologie di instradamento che possono essere utilizzate da uno switch:

- **cut-through** Legge l'indirizzo MAC del destinatario e comincia immediatamente la trasmissione durante la lettura dello stesso.
- **store-and-forward** Viene letto l'intero frame e viene calcolato il **CRC** (Cyclic redundancy check) e lo confronta con il campo **FCS**. Se i due non combaciano non viene inoltrato.
- **fragment-free** Vengono controllati solo i primi 64 byte del frame

5 Access Point

5.1 Definition

Un Access Point (AP) è un dispositivo che permette all'utente mobile di collegarsi ad una rete *wireless*. Esso agisce da gateway per i client wireless.

L'AP comunica alle stazioni riceventi nel proprio raggio di copertura l'**SSID** (Service Set Identifier) della rete o delle reti locali wireless che sta servendo.

5.2 Wireless security

La procedura più semplice è quella di permettere l'accesso solo ad alcuni indirizzi **MAC**. Tuttavia, essi possono essere clonati.

Un'altra tecnica è quella di non annunciare l'**SSID**. Tuttavia, è comunque possibile individuare la rete sniffando i segnali.

La maggior parte degli Access Point implementava un sistema di cifratura dei dati denominato **WEP** Wired Equivalent Privacy, ma è ora diventato insicuro. Attualmente vengono utilizzati i protocolli **WPA** e **WPA2** (WI-FI Protected Access).

5.2.1 WEP

Il Wired Equivalent Privacy è l'implementazione dello standard *IEEE 802.11*. La comunicazione è cifrata simmetricamente utilizzando l'algoritmo **RC4**. Questo protocollo utilizza una chiave a 40/64 bit (10 hex digits) oppure 104/128 (26 hex digits). A queste vengono aggiunti 24 bit per l'**IV** (Initialization Vector).

5.2.2 WAP

Il Wi-Fi Protected Access è l'implementazione dello standard *IEEE 802.11i*. L'architettura *IEEE 802.11i* utilizza lo standard *IEEE 802.1x* per l'autenticazione dei client, server e la distribuzione delle chiavi per ogni utente. Può inoltre supportare la **PDK** (Pre-Shared Key).
WAP implementa il protocollo **TKIP** (Tempora Key Integrity Protocol), il quale cambia dinamicamente al chiave ogni pochi minuti e la combina con un **IV** di 48-bit.
Viene utilizzato l'algoritmo **RC4** per la cifratura.
L'algoritmo per verificare l'integrità pacchetti è **Michael** (A differenza di **CRC nel WEP**), che include un contatore per evitare le ristramissioni malevoli.

This protocol is no longer secure.

5.2.3 WAP2

Wi-Fi Protected Access 2 sostituisce WAP e si differenzia dall'algoritmo di cifrature **CCMP** (Counter-Mode/CBC-Mac Protocol) per la gestione delle chiavi e dell'integrità dei messaggi.
CCMP è basato sull'algoritmo di cifratura simmetrica **AES**/128-bit (Advanced Encryption Standard).

5.2.4 WAP and WAP2

Con i protocolli **WAP/WAP2** sono supportate le modalità **WPA-PSK** (il client deve conoscere la **PSK** per associarsi ad un **SSID**) e la modalità **WPA-EAP** (il client si autentica con username e password o certificato **X.509**), anche nota come **WPA Enterprise**.
I certificati **X.509** sono autenticati da un server **RADIUS** (Remote Authentication Dial-In User Service).

6 VLAN

Le **VLAN** (Virtual LAN) sono delle tecnologie che permettono di segmentare un dominio di broadcast. Le VLAN sono principalmente utilizzate per separare il traffico e applicare diverse policy di sicurezza.

6.1 Trunking

VLAN Trunking è una tecnologia che permette la comunicazione fra 2 VLAN.

6.2 Tipologia

- **Locali** Sono locali ad uno switch o ad un gruppo di switch
- **End-to-End** Si estendono per tutta la rete e molteplici switch

7 Firewall

Un firewall è un componente passivo di difesa perimetrale. Il firewall si occupa di filtrare tutti i pacchetti mediante delle policy.

7.1 NAT

Il **NAT** (Network Address Translation) è una tecnica che consnste nel modificare gli idnirizzi IP dei pacchetti in transito su un sistema che agisce da router o da firewall.

Il NAT si può distinguere in **SNAT** (Source NAT) e **DNAT** (Destination NAT), a dipendenza di se viene modificato l'indirizzo sorgente o quello di destinazione.

7.1.1 SNAT

SNAT permette ad ogni host di una rete interna di essere mappato ad un diverso IP pubblico.

7.1.2 DNAT

È un caso particolare di SNAT dove il traffico degli host della rete interna viene modificato dal router con il proprio IP pubblico. Il router si occupa di smistare le varie connessioni.

Questa tecnica è anche chiamata **PAT** (Port Address Translation) o IP masquerating e spreca meno IP pubblici.

7.1.3 Port forwarding vs IP masquerating

La differenza tra PAT e Port forwarding è che la mappatura delle porte di destinazione nel port forwarding sono le medesime, mentre nel PAT vengono cambiate. Questo permette a molteplici server all'interno della rete privata di essere direttamente contattati.

8 Common protocols

8.1 FTP

In una connessione FTP attiva, il client apre una porta e ascolta e il server si collega attivamente ad esso. In una connessione FTP passiva, il server apre una porta e ascolta (passivamente) e il client si connette ad esso.

8.1.1 Attivo

1. Il client inizia una connessione (generalmente sulla porta 21) verso il server e comunica la porta in cui si pone in ascolto (generalmente una porta random decisa dal client) per lo scambio dei dati;
2. Il server conferma la connessione (nel caso validando le credenziali)
3. Il server apre una connessione verso il client sulla porta comunicata
4. Il client conferma la connessione
5. Inizia la trasmissione dei dati

8.1.2 Passivo

1. Il client inizia una connessione (generalmente sulla porta 21) verso il server;
2. Il server conferma la connessione (nel caso validando le credenziali) e comunica la porta in cui si pone in ascolto (generalmente una porta random in un preciso range impostato lato server) per lo scambio dei dati;
3. Il client apre una connessione verso il server sulla porta comunicata x la trasmissione dei dati
4. Il server conferma la connessione

8.2 SFTPS and FTPS

L'SFTP necessita di solamente una porta per tutte le comunicazioni, mentre l'FTPS utilizza porte multiple (la prima porta per l'autenticazione/comandi, porta 990), mentre viene utilizzata sempre una nuova porta per il trasferimento di file). FTPS aggiunge un livello di sicurezza a FTP, mentre SFTP è completamente un altro protocollo basato su SSH (porta 22).

8.3 SSH

SSH (Secure Shell) è un protocollo che permette di stabilire una connessione remota cifrata. È il successore di Telnet. SSH opera sulla porta porta 22.

8.4 SSL and TLS

TLS (Transport Layer Security) è la versione più sicura del SSL (Secure Socket Layer). Entrambi sono un protocollo di sicurezza basato sui certificati. Affinché una comunicazione sia sicura con i certificati è necessario che essi vengano emessi da una CA (Certificate Authority).

9 DNS

The **Domain Name System** is a system to achieve domain name resolution through a web of DNS server.

9.1 Domain

A domain is a set of strings joined by a dot.
The DNS is separated into multiple **zones**. The root domain is `.`
A top-level domain (TLD) is the rightmost part of a domain (`.org, .com,` $\cdots$).
A second-level domain (SLD or 2LD) is a domain directly below a TLD (`google.com, wikipedia.org,` $\cdots$).
A third-level domain or subdomain is a domain directly below a SLD (`www.google.com, en.wikipedia.org,` $\cdots$).
In general, a domain could have many levels.

9.2 Authoritative Name Server

An authoritative name server (A NS) is a server that can directly resolve domains in a specific DNS zone.

9.3 TLD server

There are 13 TLD servers with the domains `[A-M].root-servers.net`.

9.4 Resolution

To resolve a domain, the client will query a DNS resolver. This server will query iteratively other DNS servers starting from the TLD. The DNS resolver will ask a random TLD server which will respond with a more specific DNS server. This process is repeated until an authoritative name server is reached and its response will include the *Authorative Answer* (AA) flag to indicate that the response is authorative for the given zone.

Both the DNS servers and client apply caches. Every DNS record has a *Time To Live* (TTL) which indicates the maximum cache time.

The operation order of a domain name resolution is as follows

- Check if it is the local hostname
- Check system cache
- Check hosts file
- Query DNS resolver

9.5 DNS Records

- **A**: Corrispondenza fra nome e uno o più IPv4
- **AAAA**: Corrispondenza fra nome e uno o più IPv6
- **MX** (Mail Exchange): Corrispondenza dominio e server di posta elettronica
- **CNAME**: Create aliases
- **PTR**: Reverse lookup
- **SOA** (Start of Authority): Zone info / Transfer zone
- **NS** (Name Server): Tells the name server of a zone