Nivelul Retea

Permite transferul de date între sistemele neadiacente (care nu partajeaza acelaşi mediu de acces). Unitatea de date utilizată este *pachetul*.

- Funcţia principală : dirijarea pachetelor între oricare două noduri de reţea.

Două categorii de servicii de transport:

- orientate pe conexiuni: înainte de transferul datelor între două echipamente trebuie stabilită o conexiune (circuit virtual), care se închide la terminarea transferului. La stabilirea conexiunii se pot negocia anumiţi parametri legaţi de calitatea serviciului (viteză, întrâziere, cost). Ruta (secvenţa de noduri intermediare) pe care vor fi trimise pachetele se stabileşte în momentul stabilirii circuitului virtual. În acest sens, circuitul virtual va primi un identificator (adresă), fiecare pachet fiind rutat pe baza acestui identificator. Exemplu : VPN
- fără conexiuni: nu este necesară stabilirea unei conexiuni prin subreţeaua de comunicaţie în vederea transferului datelor. Ruta este determinată pentru fiecare pachet în parte, iar direcţionarea (rutarea) se realizează pe baza adreselor (sursă şi destinaţie) conţinute în fiecare pachet. Deoarece nu este necesară memorarea informaţiilor de stare cu privire la conexiuni, complexitatea este redusă, fiind posibilă implementarea unor reţele mai rapide. În cazul defectării unui nod intermediar, comunicaţia poate continua pe căi alternative. Dezavantajul principal al acestor servicii constă în faptul că nu se mai poate efectua un control al congestiei traficului. Exemplu : IP

Cel mai cunoscut si utilizat protocol la acest nivel este IP (*Internet Protocol*), utilizat pentru interconectarea reţelelor din *Internet*.

- Este un protocol fără conexiune care permite transmiterea unor blocuri de date (datagrame) între surse şi destinaţii identificate prin adrese cu lungime fixă.
- IP este un protocol nefiabil, fără a însemna însă o calitate scăzută a acestuia, de tipul “best effort”, iar livrarea pachetelor se realizează într-un mod fără conexiune → pachetele pot fi pierdute, pot sosi în altă ordine decât cea de la transmisie sau chiar pot fi recepţionate de mai multe ori.
- În cazul datagramelor foarte mari, protocolul IP realizează, dacă este cazul, fragmentarea şi reasamblarea în vederea transmiterii prin orice reţea.
- Nu dispune de mecanisme care să asigure securitatea serviciului sau controlul fluxului de informaţii.

Se prezinta formatului pachetului IP :

- Structura pachetelor se bazează pe cuvinte de 32 biţi.
- *Versiune* - Identifică versiunea protocolului IP care generează pachetul.
- *Lungimea antetului* - Indică lungimea antetului măsurată în cuvinte de 32 biţi. Lungimea minimă a antetului corespunde cazului când acesta nu conţine câmpul opţiuni şi este 5 (20 octeţi).
- *Tipul serviciului* - Arată calitatea serviciului cerut pentru transportul pachetului în reţea. Acest câmp poate influenţa routerele în alegerea unei căi spre destinaţie, dar IP nu garantează calitatea cerută pentru transportul datelor. Parametrii de calitate: o prioritate, o întârziere, o eficienţă în transmisiune (referitor la debit - throughput) o fiabilitate.
- *Lungimea totală* - Acest câmp specifică lungimea totală a pachetului, măsurată în octeţi, incluzând atât antetul cât şi datele.
- *Identificare, Fanioane şi Decalajul fragmentului* - Controlează fragmentarea şi reasamblarea pachetelor. Fiecare fragment are acelaşi format ca şi un pachet complet. (se prezintă exemplul).
- *TTL – Time to live* - arată cât timp, în secunde, i se permite unui pachet să rămână în reţea. Routerele scad valoare acestui câmp cu o unitate atunci când redirectează pachetul.
- *Protocol* - Identifică protocolul de nivel superior (transport: TCP sau UDP) asociat pachetului. Pentru protocolul TCP identificatorul este 6 iar pentru UDP este 17.

- *Secvenţa de verificare a antetului* - Permite verificarea corectitudinii (integrităţii) valorilor din antet. Acest câmp este determinat prin prelucrarea antetului, considerat ca o succesiune de întregi, fiecare alcătuit din 16 biţi. Fiecare router calculează secvenţa de verificare şi o compară cu cea din antet.
- *Câmpurile de adrese* - Conţin adresele de reţea (IP) de câte 32 biţi fiecare, a sistemului sursă şi a sistemului destinaţie. Aceste câmpuri nu sunt modificate la trecerea pachetelor prin routere. *Opţiuni* - Are o lungime variabilă (maximum 40 octeţi) şi este rezervat pentru a introduce unele funcţiuni de control privind rutarea, securitatea reţelei şi altele.
- *Câmpul datelor* - Are o lungime variabilă, dar un număr întreg de octeţi. Limitele pentru dimensiunea unui pachet, inclusiv antetul, sunt 576 octeţi minimum şi 65.535 octeţi maximum.

Modul de funcţionare al protocolului IP este:
- aplicaţia pregăteşte datele şi le transmite nivelului Internet al software-ului de reţea,
- nivelul Internet adaugă acestor date un antet (header), conţinînd adresa de destinaţie,
- datagrama rezultată este transmisă interfeţei de reţea, care adaugă la rândul ei un antet şi transmite întreg cadrul către primul nod intermediar al reţelei de comunicaţii, care va efectua rutarea pachetului,
- la recepţie, un nod intermediar va decide după adresa de destinaţie prezentă în antet care este subreţeaua şi, implicit, următorul nod intermediar către care trebuie redirecţionat pachetul,
- în cadrul destinaţiei finale, antetul este înlăturat şi datagrama se transmite nivelului Internet, de unde este transmis nivelului aplicaţie.

Adresarea IP (versiunea 4 a protocolului IP = IPv4)
- Adresele IP constau în valori fără semn reprezentate cu 32 de biţi, scrişi sub forma a 4 octeţi, fiecare dintre octeţi putând fi scris sub forma unui număr zecimal luând valori intre 0 si 255, in forma p.q.r.s (dotted quad).
- În funcţie de domeniul în care se află primul octet (p), mai exact primii 4 biţi, există mai multe clase de adrese, notate A, B, C, D, etc.
- Pentru toate aceste clase, se elimină întotdeauna, atât la identificatorul de reţea cât şi la identificatorul de sistem, secvenţa cu toţi biţii 1 şi cea cu toţi biţii 0: *masca*, respectiv adresa întregii reţele din clasa respectivă.
- O adresă utilizată pentru o funcţie specială este adresa de buclă locală (loopback). Spre exemplu, reţeaua de clasă A 127.0.0.0 este definită ca adresă de reţea pentru bucle locale. Aceste interfeţe pentru bucle locale nu permit accesul în reţeaua fizică.
- Masca unei reţele este acea secvenţă de 32 biţi (de aceeaşi lungime cu adresele) care are biţi cu valoarea 1 pe toate poziţiile corespunzătoare identificatorului de reţea şi biţi cu valoarea 0 pe toate poziţiile corespunzătoare identificatorului de sistem.
- Măştile sunt utilizate în fiecare router pentru luarea deciziei asupra interfeţei de reţea a routerului pe care se va redirecta datagrama IP ce conţine adresa destinaţie. Masca permite selectarea identificatorului de reţea dintr-o anumită adresă. Identificarea reţelei pentru rutarea unei datagramei se va face pe baza operaţiei binare ŞI (AND) la nivelul biţilor de pe o anumită poziţie a adresei IP citită din datagramă şi poziţia corespunzătoare din mască.
- Adresele de difuzare (broadcast) pentru o anumită reţea sunt acele adrese care au biţi cu valoarea 1 pe toate poziţiile corespunzătoare identificatorului de sistem, iar identificatorul de reţea specifică domeniul în care se va face difuzarea.

Crearea de subreţele (subneting)
- Principiul de alocare a adreselor IP a devenit inflexibil pentru a permite modificări facile ale configuraţiilor reţelelor locale → divizare a reţelelor din fiecare clasă în subreţele (IP subnetting).
- Alocarea subreţelelor este efectuată local. Totuşi, întreaga reţea este văzută din exterior ca o singură reţea IP.
- Există două metode de divizare în subreţele: statică şi de dimensiune variabilă.

- Masca subreţelei şi adresele de difuzare în subreţele au acelaşi rol ca şi în cazul reţelelor clasificate.

Adrese IP private

- O procedură utilizată pentru a conserva spaţiul de adrese este de a relaxa regula conform căreia adresele IP trebuie să fie unice la nivel global. Astfel, o parte din spaţiul de adrese global este rezervată pentru reţele care nu sunt conectate la Internet.
- Trei mulţimi de adrese au fost rezervate pentru acest scop:
    - 10.0.0.0: o singură reţea de clasă A,
    - de la 172.16.0.0 la 172.31.0.0: 16 reţele consecutive de clasă B,
    - de la 192.168.0.0 la 192.168.255.0: 256 reţele consecutive de clasă C.
- Routerele din cadrul domeniului unei organizaţii care foloseşte adrese private vor limita referinţele la adresele private numai la nivelul unor legături interne. De asemenea, ele nu vor anunţa în exterior rute către adrese private şi nici nu vor redirecta datagrame IP conţinând adrese private către routere externe.
- Staţiile care au doar o adresă IP privată nu vor avea acces direct, prin intermediul nivelului IP, la Internet, ci numai prin intermediul unor pasarele de nivel aplicaţie (application gateways).

Translatarea adreselor de reţea (NAT)

- NAT realizează o corespondenţă între adresele IP interne şi adresele externe alocate oficial. NAT schimbă în mod dinamic adresa IP dintr-un pachet care iese din reţeaua internă cu o adresă globală alocată oficial. Pentru pachetele care se propagă pe sensul de intrare în reţeaua internă NAT de bază translatează adresa alocată oficial într-o adresă internă.
- Pentru fiecare pachet care iese din reţeaua internă, adresa sursă este verificată conform regulilor de configurare NAT. Dacă una dintre reguli se aplică pentru adresa sursă, atunci adresa este translatată într-o adresă globală din lista de adrese disponibile.
- Pentru fiecare pachet de intrare în reţeaua internă, adresa destinaţie este verificată pentru o eventuală utilizare de către NAT. Dacă se găseşte o corespondenţă NAT atunci adresa destinaţie este schimbată cu adresa internă originală.

Rutarea intre domenii fără clase (CIDR)

- Rutarea IP clasică utilizează numai adresele de reţea din clasele A, B şi C. Nu există nici o posibilitate de a stabili o anumită relaţie între mai multe reţele de clasă C, spre exemplu.
- Soluţia la această problemă este rutarea între domenii fără clase de adrese CIDR (Classless InterDomain Routing).
- CIDR nu efectuează rutarea după clasa din care face parte reţeaua (de aceea se numeşte fără clase). Această metodă se bazează numai pe biţii cei mai semnificativi ai adresei de reţea, care constituie prefixul IP.
- Fiecare locaţie din tabela de rutare CIDR conţine o adresă de 32 de biţi şi o mască de reţea de 32 de biţi, care împreună permit identificarea lungimii şi a valorii prefixului IP. Această locaţie este reprezentată ca o structură <adresă_IP mască_reţea>.
- Exemplu: pentru a adresa un grup de 8 adrese de clasă C cu o singură locaţie în tabela de rutare este suficientă următoarea reprezentare: <192.32.136.0 255.255.248.0>.
- Rutarea CIDR se efectuează pe baza unor măşti de reţea care sunt mai scurte decât măştile de reţea obişnuite pentru o adresă IP. Această metodă este total opusă divizării în subreţele, caz în care măştile subreţelelor sunt mai lungi decât măştile de reţea obişnuite.

Reguli privind mecanismele de rutare:

- fiecare datagramă este direcţionată către cel mai apropiat nod intermediar, router sau gateway,
- operaţia de rutare constă în determinarea nodului intermediar următor (adiacent) care la rândul lui poate redirecţiona datagramele către destinaţia finală. Acest tip de rutare este numit „hop-by-hop routing” şi nu permite determinarea întregii secvenţe de noduri intermediare.
- destinaţia imediat următoare poate fi un alt router sau chiar destinaţia finală.

- decizia privind destinaţia imediată este luată pe baza informaţiilor existente în cadrul tabelei de rutare. Această tabelă este menţinută de fiecare router şi conţine asocieri de tipul „destinaţie finală - destinaţie următoare” (next hop).
- la primirea unei datagrame, router-ul caută în tabela de rutare înregistrarea corespunzătoare destinaţiei finale. Dacă această înregistrare este găsită, datagrama se transmite către următoarea destinaţie specificată în ruta respectivă.

Tabela de rutare poate fi actualizată în următoarele moduri:

- prin rute statice, introduse de administratorul reţelei. Orice echipament de reţea (host sau router) conţine o aşa-numită rută statică implicită (default), utilizată pentru redirecţionarea datagramelor atunci când nu este găsită nici o înregistrare care să corespundă cu adresa finală.
- prin rute directe, care sunt create automat de echipamentul de reţea (host sau router) în momentul în care se specifică adresele IP şi măştile de subreţea pe interfeţele echipamentului. În acest mod se realizează asocierea între destinaţia imediată şi interfaţa fizică prin care poate fi atins următorul nod de rutare.
- prin rute dinamice, schimbate între router-ele adiacente prin intermediul protocoalelor specializate. Utilizînd mecanismele de rutare dinamică, un router transmite router-elor învecinate întreaga tabelă de rutare, constînd în rute statice, rute directe şi rute dinamice „învăţate” de la alte router-e. Cele mai cunoscute protocoale de rutare dinamică sunt: RIP (Routing Information Protocol), versiunile 1 şi 2, utilizat frecvent în reţele private, OSPF (Open Short Path Finding), IGRP (Internal Gateway Routing Protocol), BGP (Border Gateway Protocol, utilizat în reţeaua Internet pentru rutarea infomaţiilor între furnizorii de servicii).

Sistem autonomy

- Un sistem autonom (SA) este o porţiune logică dintr-o reţea IP. De obicei, un SA reprezintă o inter-reţea din cadrul unei organizaţii. Acesta este administrat de către o singură autoritate de management. Un SA se poate conecta cu alte SA administrate de aceeaşi organizaţie. Pe de altă parte, un SA se poate conecta cu alte reţele publice sau private.
- Unele protocoale de rutare sunt utilizate pentru a determina rutele optime dintr-un SA. Alte protocoale de rutare sunt utilizate pentru a interconecta mai multe SA. În reţelele TCP/IP sunt utilizate următoarele protocoale de rutare:
    - Protocoale de rutare în interiorul unui SA, Interior Gateway Protocol (IGP): Exemple de protocoale IGP: Open Short Path First (OSPF) and Routing Information Protocol (RIP);
    - Protocoale de rutare în exteriorul unui SA, Exterior Gateway Protocols (EGPs). Protocoalele EGP permit schimbul de informaţii de rutare între diferite SA-uri. Exemplu de protocoal EGP: Border Gateway Protocol (BGP).

Rutarea de tip vector distanţă (Distance Vector)

- Algoritmii de tip vector distanţă permit ca fiecare echipament din reţea să construiască şi să menţină, în mod automat, o tabelă locală de rutare IP.
- Fiecare router din reţea menţine o listă cu toate distanţele (costurile) asociate căilor de la el la toate destinaţiile cunoscute. Costul unei căi determină selecţia acestei căi pentru dirijarea pachetelor la destinaţie. Căile cu un cost mai mic sunt preferate căilor cu un cost mai mare. Calea cu costul minim dintre căile disponibile va fi aleasă (soluţia optimă) pentru a ajunge la destinaţie. Această informaţie este menţinută într-o tabelă vector distanţă (distance vector). Această tabelă (a unui router) este transmisă periodic către routerele vecine. Atunci când primeşte tabela, fiecare router prelucrează informaţiile din tabela primită pentru a determina cea mai bună cale prin reţea către fiecare destinaţie cunoscută.
- Avantajul principal al algoritmilor vector distanţă îl reprezintă simplitatea implementării şi depanării. Aceşti algoritmi sunt foarte eficienţi atunci când sunt utilizaţi în reţele de dimensiuni mici cu o redundanţă scăzută.
- Dezavantaje: În cazul apariţiei unei modificări în cadrul reţelei, se pune problema reconvergenţei conţinutului tabelelor de rutare pentru a reflecta modificarea de topologie. Intervalul de timp necesar fiecărui router din reţea pentru a avea o tabelă de rutare actualizată

se numeşte *timp de convergenţă*. În reţelele mari şi cu redundanţă crescută, timpul de convergenţă al algoritmilor vector distanţă poate atinge valori excesiv de mari. Este posibil ca în intervalul în care tabelele de rutare tind să conveargă, reţeaua să utilizeze informaţii de rutare eronate. Astfel se pot produce bucle de rutare sau alte tipuri de redirectări instabile de pachete;
- De obicei, pentru a reduce timpul de convergenţă se impune un număr maxim de noduri (routere sau hop-uri) care pot fi parcurse de către o singură rută. Căile valide care depăşesc această valoare limită nu sunt utilizate în reţelele de tip vector distanţă;
- Tabelele de rutare vector distanţă sunt transmise periodic către nodurile vecine. Aceste tabele sunt transmise chiar şi în cazul în care nu s-au produs modificări în conţinutul acesteia. Acest lucru poate determina o încărcare excesivă a reţelei, mai ales în reţelele de capacitate redusă.
- În ultimii ani, s-au mai adus îmbunătăţiri algoritmului vector distanţă de bază pentru a reduce timpul de convergenţă şi regimurile de instabilitate.
- O variantă foarte utilizată de protocol de tip vector distanţă este protocolul RIP (Routing Information Protocol).

Rutarea de tip stare legătură (Link state)
- Creşterea dimensiunilor şi a complexităţii reţelelelor, din ultimii ani, a determinat dezvoltarea unor algoritmi de rutare mai robuşti. La elaborarea acestor algortimi s-a urmărit eliminarea dezavantajelor observate în cazul protocoalelor de tip vector distanţă. Aceşti algoritmi utilizează principiul mesajelor de tip stare legătură (link state) pentru a determina topologia reţelei.
- Un mesaj stare legătură reprezintă o descriere a interfeţei unui router (spre exemplu, poate conţine informaţiile: adresă IP, mască subreţea, tipul reţelei), precum şi relaţiile cu routerele vecine. Baza de date de tip stare legătură conţine mai multe informaţii de tip stare legătură.
- Procesul utilizat de algoritmii de tip stare legătură pentru determinarea topologiei reţelei este:
    1. Fiecare router identifică toţi ceilalţi routeri din reţelele la care este conectat direct;
    1. Fiecare router transmite (anunţă) lista tuturor legăturilor din reţelele conectate direct şi costul asociat fiecărei legături. Aceast lucru este realizat prin transmiterea unor mesaje de anunţare a stării legăturii, LSA (Link State Advertisement) către celelalte routere din reţea;
    2. Pe baza acestor mesaje LSA, fiecare router crează o bază de date care conţine detaliile topologiei curente a reţelei. Baza de date a topologiei din fiecare router este aceeaşi;
    3. Fiecare router foloseşte informaţiile din baza de date a topologiei pentru a calcula rutele optime pentru fiecare reţea de destinaţie.

Rutarea de tip vector cale (Path vector)
- Algoritmul de rutare de tip vector cale este asemănător algoritmului de tip vector distanţă în sensul că fiecare router de graniţă (border router) transmite către routerii vecini anunţuri cu destinaţiile pe care le poate accesa. Totuşi, în loc să anunţe reţelele din punctul de vedere al destinaţiei şi al distanţei până la acea destinaţie, acestea sunt anunţate cu adresele destinaţie şi descrierile căilor (path descriptions) către acele destinaţii.
- O rută este definită de perechea formată din adresa destinaţie şi atributele căii până la acea destinaţie, de unde provine şi numele de rutare de tip vector cale, routerele primind un vector care conţine căi până la un set de destinaţii. Calea, exprimată de domeniile traversate până în acel punct, este asociată unui atribut special de cale care conţine secvenţa de domenii de rutare prin care a trecut informaţia de accesare. Calea reprezentată de cel mai mic număr de domenii traversate este aleasă pentru a direcţiona pachetele către destinaţie.
- Avantajul principal al acestui protocol este flexibilitatea.

Protocolul informaţiei de rutare (RIP)
- Protocolul RIP (Routing Information Protocol) este un exemplu de protocol de rutare în interiorul unui SA de dimensiuni mici. RIP este un protocol de tip vector distanţă.
- Protocolul RIP specifică două tipuri de pachete. Aceste pachete pot fi transmise de către orice nod în care rulează protocolul RIP:

- pachete cerere: un pachet de cerere solicită nodurilor RIP vecine să transmită tabela lor de vectori distanţă. În cerere se specifică dacă nodul vecin trebuie să transmită numai un subset de vectori sau să transmită întregul conţinut al tabelei;
- pachete răspuns: un pachet de răspuns este transmis de către un nod pentru a anunţa informaţia menţinută în tabela locală de vectori distanţă. Tabela este transmisă în următoarele situaţii:
  - În mod automat, la fiecare 30 de secunde;
  - Ca răspuns la un pachet de cerere generat de un alt nod RIP;
  - Dacă este disponibilă funcţia de actualizare declanşată (triggered update), tabela este transmisă atunci când apare o modificare a tabelei de vectori distanţă.

- Atunci când se recepţionează un pachet de răspuns la un nod, informaţia conţinută în acesta este comparată cu cea din tabela locală de vectori distanţă. Dacă pachetul de răspuns anunţă o rută către o destinaţie cu un cost mai mic, atunci tabela este actualizată cu noua cale.
- Nodurile RIP au două moduri de operare:
  - Modul activ: Nodurile care lucrează în modul activ transmit tabelele lor de vectori distanţă şi recepţionează actualizări de rutare de la nodurile RIP vecine. De obicei, routerele sunt configurate să funcţioneze implicit în modul activ.
  - Modul pasiv (silenţios): Echipamentelele care lucrează în acest mod, doar recepţionează actualizări de rutare de la nodurile RIP vecine. Aceşte echipamente nu transmit tabela de vectori distanţă. De obicei, staţiile de capăt sunt configurate să lucreze în modul pasiv.
- Algoritmul de calcul al vectorilor distanţă:
  - De fiecare dată când un nod primeşte un mesaj de anunţare a unei tabele de rutare, acesta procesează informaţiile din mesaj pentru a identifica existenţa unei căi de cost mai mic către fiecare destinaţie cunoscută. Această funcţie este realizată cu ajutorul algoritmului vector distanţă RIP.
  - La iniţializare, fiecare router conţine o tabelă de vectori distanţă care specifică fiecare reţea conectată direct şi costul configurat. În mod uzual, fiecărei reţele i se asociază costul cu valoarea 1. Acest cost reprezintă o cale cu un singur nod intermediar până la destinaţie. Numărul total de noduri intermediare (hop) dintr-o rută este egal cu costul total al rutei. Totuşi, costul poate fi modificat pentru a reflecta şi alte metrici, cum ar fi: utilizarea, viteza sau fiabilitatea.
  - Fiecare router transmite periodic (uzual, la fiecare 30 de secunde) către routerele vecine tabela proprie de vectori distanţă. Un router poate transmite tabela şi atunci când se produce o modificare a topologiei. Fiecare router utilizează aceste informaţii pentru a actualiza propria tabelă de vectori distanţă: Costul total al căii pentru o anumită destinaţie este calculat prin adunarea costului raportat în tabela transmisă de nodul vecin la costul legăturii cu acel nod. Calea cu costul minim este salvată în tabela de vectori distanţă.

Convergenţa algoritmului RIP şi numărarea la infinit

- După un interval de timp suficient de mare, algoritmul va calcula corect tabela de vectori distanţă pentru fiecare nod. Totuşi, pe durata acestui timp de convergenţă, informaţii despre rute eronate se pot propaga prin reţea.
- Maniera în care sunt incrementate costurile din tabela de vectori distanţă a condus la introducerea termenului de numărare la infinit. Astfel, costul continuă să crească, teoretic tinzând la infinit. Pentru a limita acest proces de incrementare a costului, în cazul în care o reţea este inaccesibilă trebuie să se întrerupă la un moment dat transmiterea mesajelor de anunţare a tabelelor de rutare. În cazul protocolului RIP, s-a impus o valoare limită superioară a costului de 16.
- O consecinţă a limitării metricii este că se limitează şi numărul de noduri intermediare prin care un pachet poate trece pe ruta de la reţeaua sursă la reţeaua destinaţie. Astfel, în reţelele RIP

orice rută care include peste 15 routeri intermediari este considerată invalidă. Algoritmul de rutare va elimina aceste rute.
- Există alte două metode de îmbunătăţire a algoritmului clasic vector distanţă, din perspectiva problemei numărării la infinit:
    - Despicarea orizontului cu întoarcere otrăvită (Split horizon with poison reverse)
    - Actualizări declanşate (Triggered updates)

Split horizon:
- Timpul de convergenţă excesiv de mare cauzat de numărarea la infinit poate fi redus prin metoda Split horizon. Această nouă regulă impune ca informaţia de rutare să nu fie retransmisă de un router pe aceeaşi interfaţă pe care a primit această informaţie.
- Dezavantajul acestei metode este acela că fiecare nod trebuie să aştepte să expire timpul pentru ruta către destinaţia inaccesibilă, înainte ca această rută să fie eliminată din tabela de vectori distanţă. În mediile RIP, acest timp de expirare este de cel puţin trei minute din momentul ultimei actualizări a informaţiei respective. Pe durata acestui interval, routerul continuă să transmită informaţii eronate despre destinaţia inaccesibilă către nodurile vecine. Acest fapt conduce la persistenţa buclelor de rutare şi a altor probleme de rutare.

Split horizon with poison reverse:
- Split horizon with poison reverse reprezintă o îmbunătăţire adusă implementării Split horizon. Toate reţelele cunoscute sunt anunţate în fiecare mesaj de actualizare a tabelei de rutare. Modificarea esenţială faţă de varianta anterioară este că reţelele învăţate din mesajele sosite printr-o anumită interfaţă sunt anunţate ca fiind inaccesibile în mesajele de rutare transmise prin aceea şi interfaţă.
- Această modificare reduce considerabil timpul de convergenţă în reţelele complexe, cu redundanţă mare. Atunci când un mesaj de actualizare indică o reţea ca fiind inaccesibilă, rutele sunt eliminate imediat din tabela de rutare. Astfel, se întrerup buclele de rutare, înainte ca informaţiile despre acestea să se propage în reţea.

Triggered updates:
- Algoritmii care utilizează actualizări declanşate vizează reducerea timpului de convergenţă. Un router transmite imediat tabela de vectori distanţă către nodurile vecine, de fiecare dată când se schimbă costul unei rute. Acest mecanism asigură anunţarea modificărilor de topologie cât mai repede şi nu în mod periodic, ca în varianta clasică.

Protocolul OSPF (Open Shortest Path First)
- Permite utilizarea unor metrici multiple pentru calcularea costului unei legături, cum ar fi: întârziere, debit, cost monetar şi eficienţă. Versiunea cea mai utilizată de OSPF pentru IPv4 este definită de RFC 2328.
- OSPF implementează un număr de funcţii pe care protocoalele de tip vector distanţă nu le prezintă. Astfel, OSPF a devenit cel mai utilizat protocol de rutare în reţelele de dimensiuni mari. Funcţiile care au contribuit la succesul standardului OSPF:
    - Echilibrarea încărcării reţelei pentru căi de cost egal (Equal cost load balancing): Utilizarea simultană a căilor multiple permite utilizarea mai eficient ă a resurselor reţelei.
    - Divizarea logică a reţelei (Logical partitioning of the network): Această funcţie reduce propagarea informaţiilor neactualizate în cazul unor condiţii defavorabile (modificări de topologie). De asemenea, permite cumularea anunţurilor de rutare (aggregate routing announcements) care limitează anunţarea informaţiilor inutile.
    - Mecanisme de autentificare: OSPF permite autentificarea fiecărui nod care transmite mesaje de anunţare a rutelor. Aceasta previne ca surse frauduloase (routeri neautorizaţi) să modifice conţinutul tabelelor de rutare.

    - Timp de convergenţă mai mic: OSPF permite propagarea instantanee a informaţiilor despre modificarea rutelor. Astfel, actualizarea informaţiilor de topologie se realizează mult mai rapid.
- OSPF este un protocol de tip stare a legăturii (link state). Fiecare router OSPF execută algoritmul SPF (Shortest-Path First), pentru a procesa informaţiile salvate în baza de date a stărilor legăturilor (link state database). Algoritmul generează arborele de căi minime (shortest-path tree) care prezintă rutele optime către toate reţelele de destinaţie.

- Reţelele OSPF sunt divizate în mai multe arii. O arie reprezintă o grupare logică de reţele şi routere. O arie poate coincide cu o zonă geografică sau administrativă. Fiecare arie este identificată unic prin intermediul unui identificator de 32 de biţi, denumit ID arie.
    - Într-o arie, fiecare router menţine o bază de date a topologiei (topology database) care descrie routerele şi legăturile din această arie. Aceste routere nu deţin informaţii despre topologii aflate în exteriorul ariei, ci deţin numai rutele către aceste destinaţii externe. Astfel, se reduc considerabil dimensiunile bazei de date a topologiei, deţinute de fiecare router.
    - Divizarea în arii reduce posibila creştere a numărului de actualizări de stare a legăturilor. Astfel, cele mai multe LSA sunt distribuite numai în interiorul unei arii.
    - Se reduce timpul de procesare CPU necesar pentru a menţine baza de date a topologiei. Algoritmul SPF se limitează la a administra modificările numai dintr-o arie.

Aria coloană vertebrală (Backbone) şi aria 0
- Toate reţelele OSPF conţin cel puţin o singură arie. Această arie este aria 0 sau aria coloană vertebrală (backbone). Se pot adăuga şi alte arii, în funcţie de topologia reală a reţelei sau de alte cerinţe de proiectare.
- În reţelele care conţin mai multe arii, aria backbone se conectează fizic cu toate celelalte arii. Toate ariile vor anunţa informaţiile de rutare, direct în backbone. Apoi, din backbone se vor transmite aceste informaţii către celelalte arii.
- În funcţie de amplasarea şi rolul unui router în reţea există trei tipuri de routeri într-o reţea OSPF:
    - Router de interior de arie, IA (Intra-area routers) - Aceste routere sunt amplasate, d.p.d.v. logic, în interiorul unei arii OSPF. Fiecare router de interior de arie menţine o bază de date a topologiei, corespunzătoare numai ariei locale a acestuia.
    - Routere de extremitate de arie, ABR (Area border routers) - Acestei routere se conectează, d.p.d.v. logic, cu una sau mai multe arii, dintre care una trebuie să fie aria backbone. Astfel, un router ABR este utilizat pentru interconectarea mai multor arii. Fiecare router ABR menţine o bază de date a topologiei, separat pentru fiecare arie la care se conectează.
    - Router de extremitate de SA, ASBR (AS boundary routers) – Aceste routere sunt plasate, d.p.d.v. logic, la periferia unui sistem autonom OSPF. Astfel, un router ASBR funcţionează ca o poartă de acces (gateway), care anunţă căile de acces dintre reţeaua OSPF şi alte domenii de rutare. Routerele ASBR transmit spre interiorul SA, mesajele de anunţare a rutelor LSA externe.

Routere vecini şi adiacenţe
- Routerele care împart un segment comun de reţea pot stabili o relaţie de învecinare la nivel logic. În acest caz, pentru a stabili o relaţie de învecinare, routerele trebuie să convină asupra următoarelor informaţii:
    - ID arie: Routerii trebuie să aparţină aceleiaşi arii OSPF.
    - Autentificare: Dacă se defineşte o autentificare, atunci routerele trebuie să utilizeze aceeaşi parolă.
    - Intervalele Hello şi intervalele moarte (dead): Routerele trebuie să utilizeze aceleaşi intervale de timp pentru funcţionarea protocolului Hello.
    - Stub: Routerele trebuie să convină că aria este configurată ca arie stub.

- După ce două routere au stabilit o relaţie de învecinare, se poate stabili o relaţie de adiacenţă între aceştia. Routerele vecin sunt considerate adiacente după ce şi-au sincronizat reciproc bazele de date de topologie. Sincronizarea bazelor de date se realizează prin schimbul de mesaje de stare a legăturii.

Anunţurile de stare a legăturii şi inundarea
- Conţinutul unui mesaj LSA descrie o componentă a reţelei, care poate fi: un router, un segment sau o destinaţie externă. Mesajele LSA sunt schimbate de către routerele OSPF adiacente pentru a sincroniza între ele bazele de date ale stărilor legăturilor.
- Atunci când un router generează sau modifică un mesaj LSA, acesta trebuie să comunice această modificare în cadrul reţelei. Mai întâi, routerul transmite mesajul LSA fiecărui sistem adiacent. La recepţionarea LSA-ului, aceşti vecini salvează informaţia în propriile baze de date a stărilor legăturilor şi la rândul lor, comunică LSA-ul vecinilor lor. Această activitate de tipul "salvează şi trimite mai departe" (store and forward) continuă până când toate sistemele primesc acest LSA.
- Acest proces poartă numele de inundare eficientă (reliable flooding), deoarece se parcurg următorii doi paşi pentru a asigura transmiterea LSA în toată reţeaua fără a o supraîncărca cu trafic de volum mare:
- Fiecare router salvează mesajul LSA pentru un interval de timp înainte de a propaga informaţia către vecinii săi. Dacă pe durata acestui interval de timp, routerul primeşte o nouă versiune a LSA, acesta înlocuieşte versiunea salvată.

Tipuri de pachete OSPF:
- Pachetele OSPF sunt transmise în datagramele IP si nu sunt incaptulate în pachetele TCP sau UDP. Antetul IP contine în câmpul de identificare a protocolului valoarea 89. De asemenea, valoarea câmpului care defineşte tipul serviciului (type of service) are valoarea 0. Acest mecanism este utilizat pentru a impune o procesare specială a pachetelor.
- Atunci când este posibil, un router OSPF utilizează transmisia multiplă (multicast) pentru a comunica cu routerele vecin.

PROTOCOLUL INTERNET – Versiunea 6 (IPv6)
- Varianta IP care a fost introdusă pentru a înlocui IPv4.
- Experimentând IPv4 s-au constatat 3 tendinţe în Internet:
    - Integrarea hardware şi software şi dezvoltarea unor algoritmi cât mai simplu de implementat hardware;
    - Procesarea rapidă a pachetelor la routere – routerele trebuie să proceseze şi să clasifice pachetele la o viteză comparabilă cu cea a conexiunilor fizice (conexiunile fizice, dintre routeri, au devenit din ce în ce mai rapide, de debite mari) → soluţie: nu se memorează pachetele înainte să fie clasificate QoS. Astfel, se respectă cerinţele QoS ale fluxului din care face parte pachetul;
    - Creşterea dimensiunilor Internet-ului + management defectuos al spaţiului de adrese ↔ epuizarea adreselor IPv4.
- Soluţii IPv6
    - modificarea (prin simplificare) a antetului pachetului: Se elimină fragmentarea şi reasamblarea, dimensiunea pachetului fiind controlată la niveluri superioare
    - Se adaugă câmpurile "clasă de trafic" şi "etichetă flux" → suport QoS îmbunătăţit;
    - Nu se mai face verificarea erorilor (erori de antet) → se elimină câmpul "checksum" → problemă rezolvată la nivelurile superioare;
    - Dimensiunea adreselor creşte de 4 ori (dimensiunea spaţiului de adrese creşte de $2^{3 \cdot 32} \approx 7{,}9 \cdot 10^{28}$ ori) → nu mai este necesară utilizarea metodelor de reutilizare a unor subspaţii de adrese, spre exemplu, NAT, CIDR, VLSM, etc.;
    - Securitate sporită a reţelei → IPv6 specifică utilizarea obligativitatea utilizării protocolului de securitate IPSec, printr-un antet opţional.
- Dezavantaje (probleme încă nerezolvate integral) ale IPv6:

- Nu implementează interoperabilitatea cu IPv4 → introducere lentă a IPv6; se dezvoltă ca reţele paralele, independente → este necesară utilizarea unor soluţii de translatare de protocol: Gateway translatoare IP; Tunelare.

Se prezintă formatul pachetelor IPv6:

- Structura pachetelor se bazează pe cuvinte de 32 biţi.
- Versiune – Identifică versiunea protocolului IP care generează pachetul.
- Clasă de trafic şi Etichetă flux – câmpuri pentru definirea politicilor de QoS; deşi nu s-au definit utilizări explicite ale acestor două câmpuri, s-a intenţionat utilizarea acestora într-un context asemănător "multiplexării" de fluxuri.
- Lungime date – Acest câmp specifică lungimea câmpului de date, măsurată în octeţi.
- Următorul antet – dimensiunea antetului implicit este fixă (40 octeţi, inclusiv adresele), dar prin intermediul acestui câmp se pot introduce opţiuni ca extensii adiţionale la antetul implicit (după antetul implicit) → servicii suplimentare: QoS, securitate, mobilitate, etc.; Următorul antet reprezintă un pointer către (următorul eventual) antet opţional; fiecare extensie include un câmp Următorul antet, care localizează următoarea extensie; câmpul Următorul antet din ultima extensie localizează datele utile;
- Limită de hop-uri – (rol asemănător câmpului TTL din antetul pachetului IPv4);
- Câmpurile de adrese - Conţin adresele de reţea (IPv6) de câte 128 biţi fiecare, a sistemului sursă şi sistemului destinaţie. Aceste câmpuri nu sunt modificate la trecerea pachetelor prin routeri.
- Câmpul datelor - Are o lungime variabilă, dar un număr întreg de octeţi. Limitele pentru dimensiunea datelor sunt 64 kilo-octeţi minimum şi 232-1 octeţi maximum (dimensiunea maximă a pachetelor Jumbograms, pentru legături de debit mare).

Adresarea IPv6

- Adresele IP constau în valori fără semn reprezentate cu 128 de biţi folosite pentru identificarea unui singur sistem în Internet;
- Cei 128 de biti ai adresei IPv6 se scriu sub forma a 8 cuvinte de câte 16 biţi (1 cuvânt de 16 biţi = 4 caractere/digiţi hexazecimale) separate cu ":".
- Nu se folosesc adrese de broadcast → reţelele sunt atât de mari încât conceptul de multicast este suficient (un domeniu de MC de tip IPv6 >> un domeniu de BC de tip IPv4);
- Adresele IPv6 sunt de trei tipuri: unicast, anycast şi multicast (roluri identice cu ale celor din IPv4);
- Alocarea adreselor se poate face dinamic prin autoconfigurare → SLAAC (StateLess Address AutoConfiguration) → sistemele IPv6 se pot autoconfigura atunci când se conectează la un router IPv6 folosind mesajele de descoperire a routerilor (ICMPv6); sistemul foloseşte în cerere o adresă de tip multicast (cunoscută routerului), iar routerul răspunde cu adresa alocată;
- Problema renumerotării adreselor de la IPv4 (la schimbarea IP provider, cu mesaje "prefix and router announcements") → la IPv6 problema e rezolvată implicit, deoarece se schimbă numai prefixul reţelei (anunţat de routeri), identificatorul sistemului (ultimii 64 biţi) fiind (auto)configurat de sistem;

Rutare IPv6. Reţele şi subreţele

- Adresele dintr-o reţea IPv6 sunt definite pe principiul CIDR: <adresă reţea IPv6/mască>, unde adresa reţelei reprezintă prefixul reţelei (cu toţi biţii identificatorului de sistem = 0) şi masca specifică dimensiunea prefixului;

Formatul adresei IPv6 care mapează o adresă IPv4:

- Primii 80 biţi setaţi cu "0";
- Următorii 16 biţi setaţi cu "1";
- Ultimii 32 biţi sunt cei ai adresei IPv4.