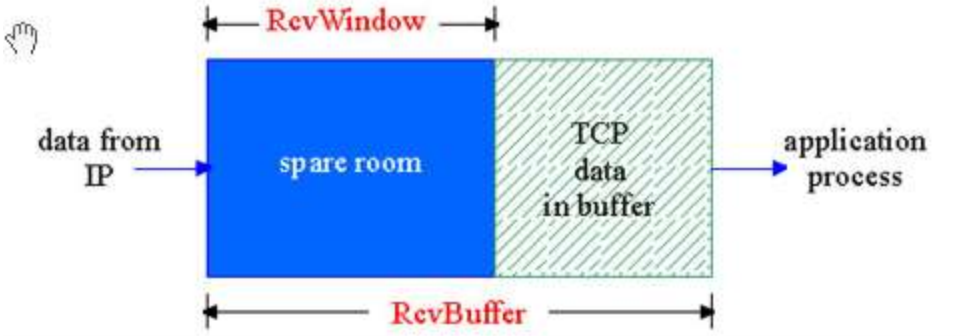
Ôn tập mạng máy tính

I. TCP

I.1. Flow control vs Congestion control

- Flow control: (Điều khiển luồng) là quy trình quản lý tốc độ truyền dữ liệu giữa 2 host của mạng. Đảm bảo:
  - Kiểm soát không để cho receiver buffer bị tràn vì sender gửi quá nhiều gói tin.
  - Receiver: Thông báo cho sender biết kích thước của rcvWindow (free buffer) có thể nhận.
  - Sender: luôn biết được kích thước tối đa có thể được gửi tiếp.



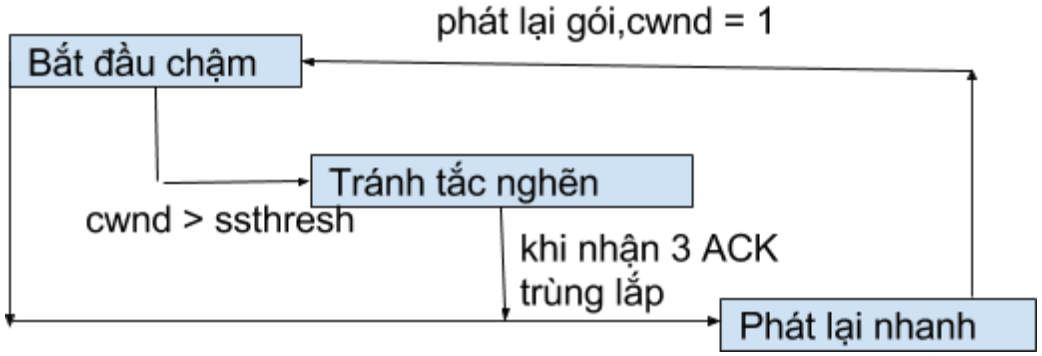
- Congestion control:(Điều khiển tắc nghẽn): điều khiển luồng dữ liệu khi tắc nghẽn sảy ra.
  - Có 2 dạng:
    - Dạng 1: "End – end congestion control" điều khiển tắc nghẽn giữa 2 host với nhau. Thông tin về mức độ tắc nghẽn trên đường truyền sẽ được suy ra từ số lượng gói tin bị mất mát trong qua trình truyền.
    - Dạng 2: "Network – assited congestion control" - Router là nhiệm vụ cung cấp các thông tin phản hồi về tình trạng nghẽn mạng tới end systems.
      - Bit thông báo nghẽn mạng: thông báo tình trạng mạng đang bị nghẽn và yêu cầu host ngừng đẩy dữ liệu xuống đường truyền.
      - Thông báo tốc độ tốt đa cho phép gửi (maximum rate allowed) tới các host.

I.2. Các giải pháp tránh tắc nghẽn mạng.

- **Slow tart:**
  - Ban đầu: bên gửi sẽ gửi đi một segment (datagram), thiết lập cửa sổ cwnd =1 và chờ tín hiệu báo nhận (ACK). Khi nhận được lời đáp đầu tiên, nó tăng kích thước cửa sổ nghẽn mạch "cwnd" lên thành 2. Qua trình cứ tiếp tục như vậy và cửa sổ nghẽn mạch "cwnd" sẽ tăng theo hàm số mũ khi nhận được các ack phản hồi cho tất cả các gói tin gửi đi, VD: cwnd = 2,4,8,…
  - Bên gửi sẽ giữ nguyên trạng thái slow start tới khi kích thước của cwnd đạt tới một ngưỡng (ssthresh – slow start threshold).
  - TCP nhận biết tình trạng tắc nghẽn mạng bằng thời gian chờ (RTO) và việc nhận các gói ACK lặp lại.
  - Thuật toán:
    - **Ssthresh:** ngưỡng cwnd do TCP quản lý ➔ cwnd < ssthresh

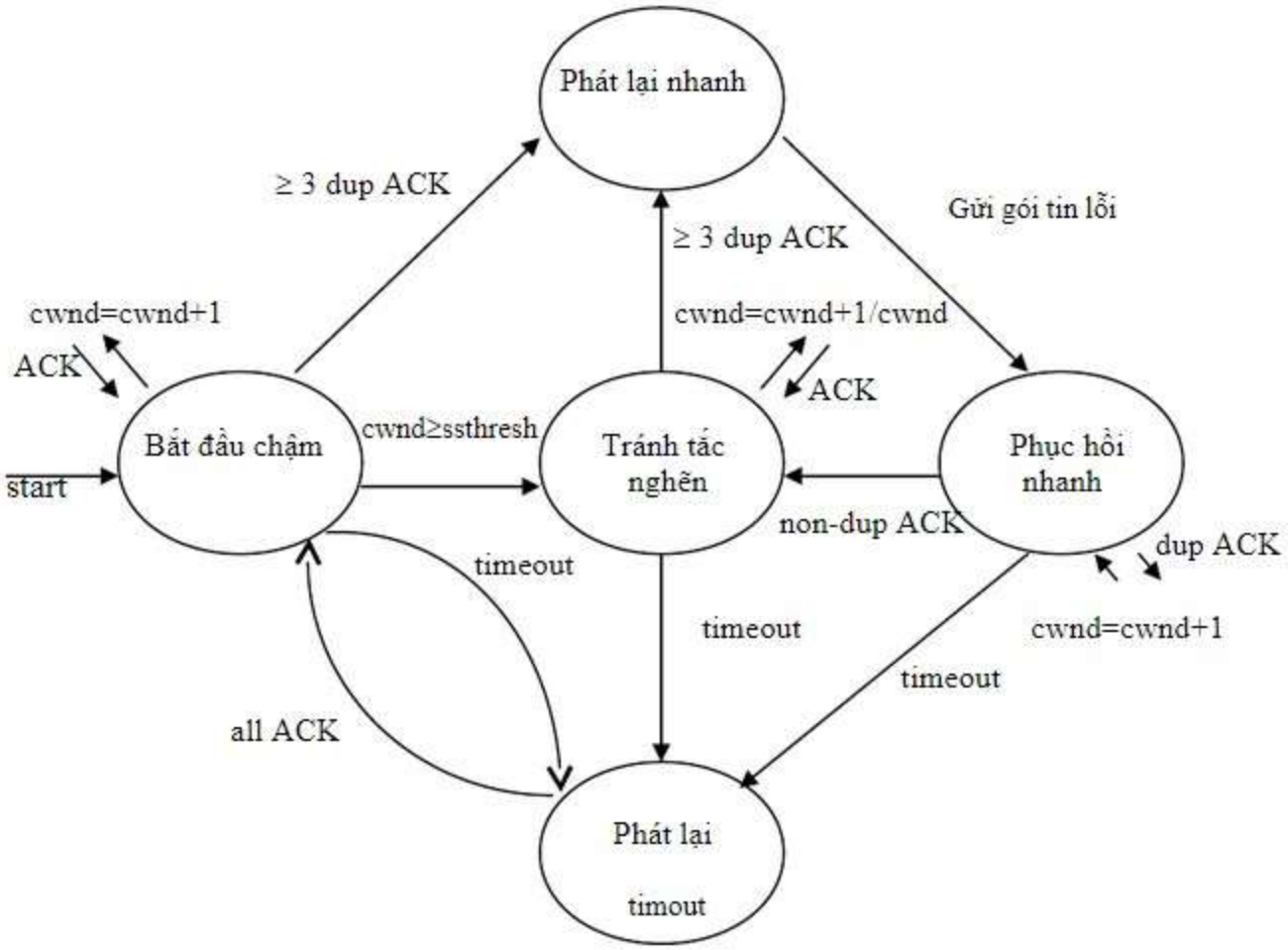
- **Time out:** Ssthresh = cwnd / 2; Cwnd = 1 MSS
- **Cwnd >= ssthresh:** Slow start *chuyển sang* Congestion avoidance
- **Nhận 3 ACK trùng:** Slow start *chuyển sang* Fast recovery

- **Congestion avoidance**
  - Giải thuật congestion avoidance được sử dụng khi kích thước cwnd >= ssthresh.
  - Trong pha congestion avoidance: kích thước cửa sổ cwnd tăng lên tuyến tính và chầm hơn so với trong pha slow start, do cwnd được tăng lên một segment cho mỗi round – trip time, tức là với mỗi ACK không lặp (non-duplicate), cwnd được tăng thêm 1 cho mỗi lần nhận đủ ACK cho các gói tin gửi đi.
- **Fast Restransmit:**
  - Thường thì một segment được truyền lại khi vượt quá thời gian chờ gửi lại (thực chất là khoảng thời gian chờ gói tin hồi đáp).
  - Với Fast Retramsmit: Khi bên gửi nhận được 3 gói ACK phản hồi giống nhau thì bên gửi sẽ lập tức truyền lại segment bị mất mà không cần phải chờ cho tới khi hết time – out.
- **Fast Recovery:**
  - Khi nhận được một gói tin ACK hồi đáp cho dữ liệu đã gửi. Lúc này kích thước cwnd = ssthresh.
  - Thuật toán Fast Recovery quy định việc thực hiện thuật toán tránh tắc nghen ngay khi thực hiện phát lại nhanh.
- **TCP Tahoe**
  - Giao thức điều khiển tắc nghẽn TCP Tahoe là giao thức TCP kết hợp với ba cơ chế "bắt đầu chậm", "tránh tắc nghẽn" và "phát lại nhanh". Đặc trưng của TCP Tahoe là khi phát hiện mất góidữ liệu thông qua việc nhận 3 gói ACK lặp lại, trạm gửi phát lại gói dữ liệu bị mất đặt cwnd bằng 1 gói dữ liệu và khởi động quá trình "bắt đầu chậm".Cơ chế "phát lại nhanh" khôi phục chờ "time-out", cho phép tăng đáng kể thông lượng và hiệu suất sử dụngkênh kết nối TCP. Hoạt động của TCP Tahoe như sau:



- **TCP Reno**
  - TCP Reno là cải tiến tiếp của TCP Tahoe, ở đây sau "phát lại nhanh" là "hồi phục nhanh" (giảm cwnd xuống còn một nửa), chứ không phải là "bắt đầu chậm"(cwnd=1). Như vậy tránh được "đường ống" khỏi bị rỗng sau khi phát lại

nhanh và cần quá trình "bắt đầu chậm" để đổ đầy đường ống. Theo chuẩn TCP Reno khi độ lớn cửa sổ phát đặt về 1, giá trị ngưỡng threshold bằng W(t)/2, ta thấy trong giai đoạn này cửa sổ phát tăng rất chậm nhưng giảm rất nhanh theo cấp số nhân.



- Khi dữ liệu bị mất hay quá thời gian chờ ACK, TCP Reno đặt lại cửa sổ phát bằng 1, sử dụng cơ chế phát lại nhanh (Fast retransmission) và khôi phục nhanh (Fast recovery), trạm gửi sẽ đi vào giai đoạn khôi phục nhanh (xét trường hợp một gói lỗi) sau khi nhận được một giá trị ngưỡng của số báo nhận ACK lặp bằng 3. Khi số báo nhận lặp đạt đến ngưỡng trạm gửi sẽ phát lại 1 gói dữ liệu, sau đó giảm cửa sổ tắc nghẽn cwnd xuống còn một nửa. Sau đó cứ mỗi lần nhận được 1 ACK, trạm gửi lại gửi đi 1 gói dữ liệu.
- So sánh 2 loại: So với TCP Tahoe, TCP Reno cải thiện đáng kể hiệu năng về thông lượng nếu chỉ có nhiều nhất là 1 gói dữ liệu bị loại trong các gói dữ liệu của một cửa sổ. Tuy nhiên, hiệu năng của TCP Reno sẽ giảm trầm trọng nếu trong một cửa sổ có trên một gói dữ liệu bị loại.

II. Routing

II.1. Distance Vector, linkstate

a. Distance Vector

- Distance Vecter sử dụng metric và next-hop để tới mạng đích.
- Các router trao đổi thông tin định tuyến theo chu kỳ.
- Thông tin định tuyến trao đổi giữa các router là toàn bộ bảng định tuyến.
- Chu kỳ trao đổi bảng định tuyến xảy ra là bắt buộc ngay cả khi khong có sự thay đổi nào trong hệ thống, dẫn đến hiện tượng routing overhead.
- Các router hoàn toàn không biết được sơ đồ tổng quan mạng của toàn bộ hệ thống. Router chỉ biết được thông tin của các đường mạng khác trong hệ thống thông qua Router láng giềng (neighbor) kết nối trực tiếp với nó mà thui.
- Các giao thức định tuyến tiêu biểu: Ripv1, Ripv2, IGRP…
- Ưu điểm:
  - Dễ cấu hình hình.
  - Router tốn ít CPU và bộ nhớ.
- Nhược điểm:
  - Cập nhật theo chu kỳ nên gây tốn băng thông mạng.
  - Hội tụ chậm dẫn đến dễ bị hiện tượng loop.

b. Link State

- Giao thức định tuyến theo trạng thái đường liên kết thu thập thông tin về đường đi từ tất cả các router khác trong cùng hệ thống mạng hay trong cùng một vùng đã được xác định. Khi tất cả các thông tin đã được thu thập đầy đủ thì sau đó mỗi router sẽ tự tính toán để chọn ra đường đi tốt nhất cho nó đến các mạng đích trong hệ thống. Như vậy mỗi router có một cái nhìn riêng và đầy đủ về hệ thông mạng, khi đó chúng sẽ không còn truyền đi các thông tin sai lệch mà chúng nhận được từ các router láng giềng.
- Một số đặc điểm chính:
  - Đáp ứng nhanh theo sự thay đổi của hệ thống mạng.
  - Gửi cập nhật khi hệ thống có sự thay đổi.
  - Gửi cập nhật định kì để kiểm tra trạng thái đường liên kết.
  - Sử dụng cơ chế hello để xác định router láng giềng và còn kết nối hay không.
  - Update thông tin mạng theo địa chỉ multicast
- Nguyên lý hoạt động:
  - Các router tìm neighbors của mình từ các Router nối trực tiếp.
  - Sau khi tìm được neighber xong Router gửi các LSA "xác thực trạng thái liên kết" tới neighbor của nó.
  - Tất cả các Router lưu LSA trong database của nó.
  - Mỗi router sử dụng thuật toán Dijtra để tính toán đường đi tốt nhất để đưa vào Routing Table.
- Ưu điểm:
  - Thích hợp với những hệ thống mạng thường sảy ra thay đổi.
  - Ít tốn băng thông.
- Nhược điểm:
  - Tốn performance của Router.
  - Khó cấu hình và troubleshoot khi có sự cố.

II.2. Intradomain routing, Interdomain routing

- **Intradomain routing**
  - Giao thức định tuyến Intradomain là giao thức tìm đường trong một vùng Autonomous System. Giao thức định tuyến Intradomain cung cấp thông tin cần thiết cho việc quyết định và chọn đường đi đến đích dựa vào các số liệu như: số hop, delay, băng thông. Các giao thức định tuyến Intradomain routing điển hình đang được sử dụng hiện nay là:RIP,OSPF, IS-IS, EIGRP
  - Trong các giao thức này 3 giao thức đầu tiên là chuẩn mở của Internet Engineering Task Force. Chuẩn EIGRP là giao thức độc quyền của Cisco.
- **Interdomain routing**
  - Giao thức định tuyến Interdomain là giao thức định tuyến giữa các AS (Autonomous System) với nhau. Việc định tuyến Interdomain còn bị chi phối bởi chính sách định tuyến dựa trên các mối quan hệ kinh doanh. Interdomain không hạn chế số metric nhưng hạn chế sự kết nối giữa các AS vì liên quan đến các chính sách hợp tác kinh doanh.
  - Giao thức tiêu biểu của Interdomain là BGP.

II.3. Hoạt động của RIP, OSPF, BGP

a. RIP

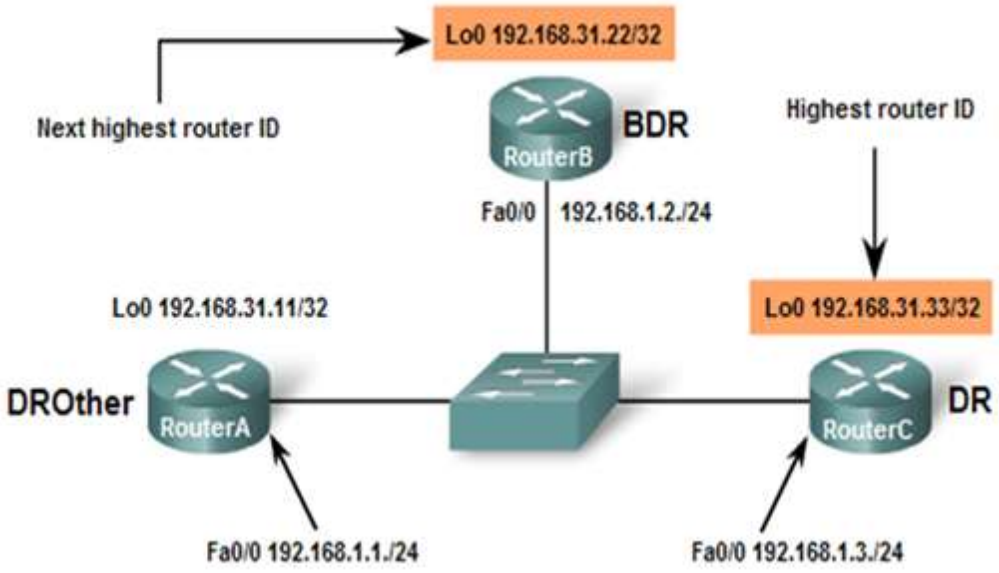
- Là giao thức định tuyến theo Distance-vector
- Sử dụng hop-count (đếm số router phải đi qua để đến đích) làm Metric nhằm xác định đường đi tới mạng đích.
- Nếu số lượng hop để tới được tới mạng đích > 15 thì gói dữ liệu đó sẽ bị hủy.
- Cập nhật bảng định tuyến định kỳ 30s một lần.
- Administrative distrance (AD) là 120.
- Có 2 phiên bản RIP:
  - RIPv1: chạy giao thức định tuyến Classfull. Gửi Update theo địa chỉ Broadcast.
  - RIPv2: chạy giao thức định tuyến Classless. Gửi update theo địa chỉ multicast: 224.0.0.9

b. OSPF (Open Shortest Path First)

- **Tổng Quan:**
  - OSPF là một giao thức link – state điển hình. Mỗi router khi chạy giao thức OSPF sẽ gửi các trạng thái đường link của nó cho tất cả các router trong vùng (area). Sau một thời gian trao đổi, các router sẽ đồng nhất được bảng cơ sở dữ liệu trạng thái đường link (Link State Database – LSDB) với nhau, mỗi router đều có được "bản đồ mạng" của cả vùng. Từ đó mỗi router sẽ chạy giải thuật Dijkstra tính toán ra một cây đường đi ngắn nhất (Shortest Path Tree) và dựa vào cây này để xây dựng nên bảng định tuyến.
  - OSPF sử dụng địa chỉ multicast 224.0.0.5 và 224.0.0.6 để gửi thông điệp Hello và Update.
  - Metric của OSPF còn được gọi là cost, được tính theo bandwidth trên interface chạy OSPF.
  - Hỗ trợ VLSM.
  - Hỗ trợ chứng thực authentication

- Tốc độ hội tụ nhanh.
- Chỉ cập nhật khi cấu trúc mạng có thay đổi.
- Adminsitrator distrance AD là 110

- **Bầu chọn DR/BDR**
- Việc bầu chọn ra DR/BDR được thược hiện trong hệ thống mạng Broadcast – Multi Access "BMA".
- Trong mô hình mạng BMA thường sảy ra tình trạng quá tải do các router thực hiện quá trình thiết lập quan hệ và trao đổi thông tin trạng thái.
- Giải pháp cho vấn đề trên là bầu ra một router làm đại diện cho BMA. Router đó được gọi là Designated Router (DR). DR sẽ thiết lập mối quan hệ với mọi router khác trong mạng quảng bá. Các router còn lại sẽ chỉ gửi thông tin về trạng thái liên kết cho DR. Sau đó DR sẽ gửi thông tin này cho mọi router khác trong mạng sử dụng địa chỉ multicast 224.0.0.5. Rõ ràng DR đóng vai trò như một người phát ngôn chung. Việc bầu ra DR rất có hiệu quả nhưng cũng có một nhược điểm. DR trở thành một tâm điểm nhạy cảm đối với sự cố. Do đó, cần một Router thứ hai được bầu ra để làm đại diện dự phòng – Backup DR (BDR), Router này sẽ đảm trách vai trò của DR nếu DR bị sự cố. Địa chỉ multicast 224.0.0.6 được sử dụng để truyền thông giữa các DR và BDR.
- Lựa chọn DR và BDR: quá trình bầu chọn DR và BDR được tiến hành ngay sau khi cổng của Router đầu tiên được kết nối vào mạng đa truy cập và được cấu hình giao thức OSPF. Quá trình này có thể mất vài phút, sau khi tất các Router được bật, Router có chỉ số ID lớn nhất có thể là DR.
- Quá trình lựa chọn DR và BDR sẽ theo qui tắc sau:
  - DR: Router có chỉ số Priority lớn nhất.
  - BDR: Router có chỉ số Priority lớn thứ hai.
  - Trong trường hợp các Router có chỉ số Priority bằng nhau thì Router nào có chỉ số ID (Router ID) cao nhất làm DR.



- Router ID: dùng để chọn DR và BDR trong mạng. Router ID đơn giản là Địa chỉ IP, nó là duy nhất với mỗi Router. Nó được chọn như sau:
  - Người quản trị mạng cấu hình trực tiếp.
  - Nếu không được cấu hình, sẽ chọn địa chỉ IP lớn nhất của cổng mạng ảo (Loopback interface)
  - Nếu không có Loopback interface, Địa chỉ IP lớn nhất của cổng vật lí (đang hoạt động) sẽ được chọn làm Router ID.

c. BGP

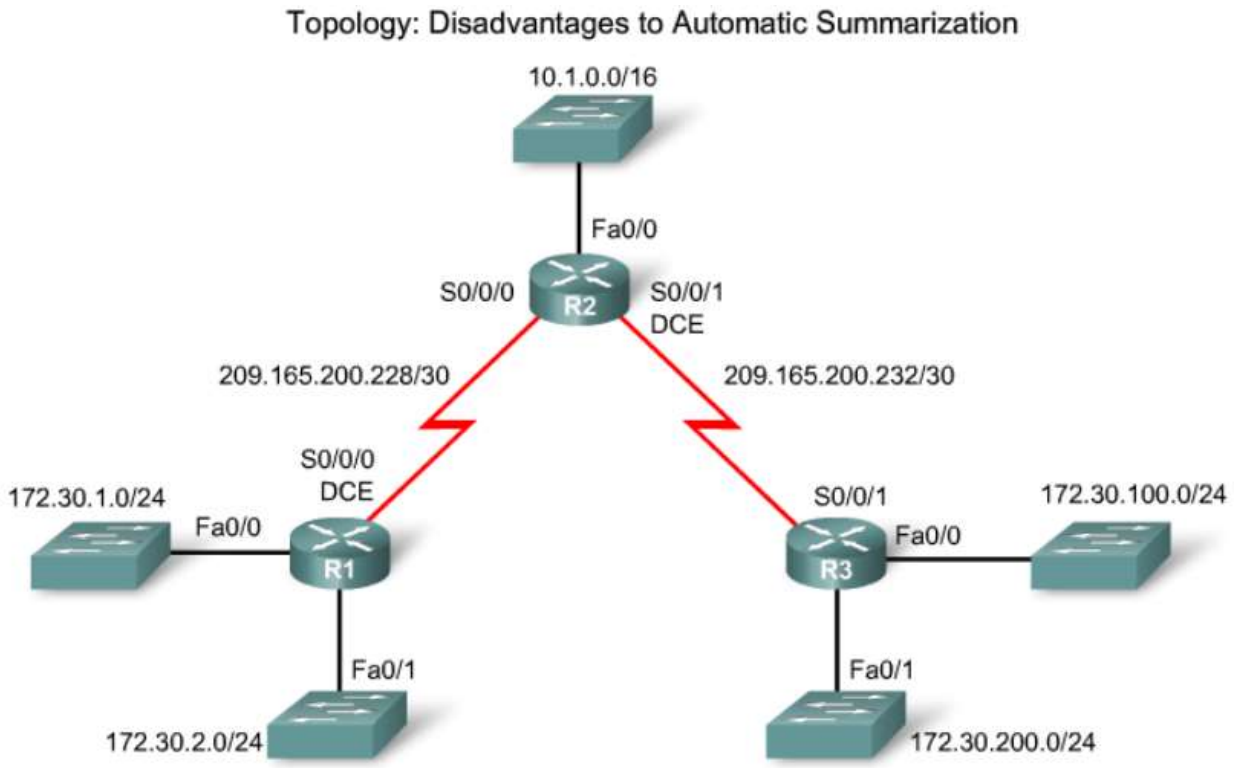
- **Tổng quan:**
  - BGP là một giao thức định tuyến dạng path-vector và việc chọn đường đi tốt nhất thông thường dựa vào một tập hợp các thuộc tính (attribute).
  - Nhiệm vụ của BGP là đảm bảo thông tin liên lạc trao đổi thông tin định tuyến giữa các AS.
  - BGP sử dụng giao thức TCP 179.
  - BGP chỉ ra chính xác danh sách toàn bộ đường dẫn đến đích
  - Chống vòng lặp rất hiệu quả nhờ vào cơ chế xem xét các tuyến đường mà router gửi về xem có chính bản thân AS trong đó hay không, nếu có route sẽ biết được ngay là đã bị lặp và sẽ loại bỏ thông tin đó.
  - Trong giai đoạn đầu tiên thiết lập mối quan hệ BGP thì toàn bộ thông tin cập nhật sẽ được trao đổi và sau đó sẽ chuyển sang cơ chế trigger-update.
  - Một điểm khác biệt rõ thấy nhất của BGP so với các giao thức định tuyến loại IGP (như OSP, RIP, EIGRP, IGRP,…) đó là nó không quan tâm đến các subnet cụ thể trong một công ty, cơ quan,…mà nó quan tâm đến việc chuyển tải đầy đủ thông tin đến 1 AS khác với các chính sách định tuyến (policy) cần thiết.
  - BGP có thể sử dụng giữa các router trong cùng 1 AS và khác AS. Khi BGP được dùng trong cùng 1 AS thì được gọi là iBGP, còn dùng để kết nối các AS khác nhau thì gọi là eBGP.
- **Hoạt động của BGP:**
  - Cập nhật bảng định tuyến: Chức năng của BGP là để trao đổi định tuyến giữa các AS khác nhau và đảm bảo chọn lựa tuyến thông suốt không bị loop. Do BGP sử dụng giao thức TCP nên nó thừa kế tính tin cậy và kết nối có hướng của TCP. BGP xây dựng một biểu đồ hình cây các AS dựa trên thông tin giữa các BGP neighbor để đảm bảo lựa chọn tuyến không loop. Kết nối giữa hai AS bất kỳ được thể hiện bởi đường Path.
  - Thiết lập mỗi quan hệ BGP Neighbor: Để chạy giao thức BGP thì đầu tiên các router phải thiết lập mối quan hệ neighbor hay peer (có nghĩa là kết nối TCP phải được đảm bảo). Sau khi đã thiết lập được mối quan hệ này, các router neighbor sẽ trao đổi thông tin bằng nhiều bản tin để mở và xác nhận các thông số kết nối. Tiếp theo chúng sẽ trao đổi các thông tin về các tuyến đường BGP. Sau khi việc trao đổi thông tin này được hoàn tất thì các cập nhật thành phần (incremental update) sẽ được gửi đi khi có sự cố trong mạng chứ không truyền toàn bộ bảng định tuyến (hoạt động theo cơ chế trigger-update). Nếu như không có thông tin định tuyến

nào được trao đổi thì sau thời gian keepalive (mặc định là 60s) các router chạy BGP sẽ tự động ngắt kết nối.

- **Thứ tự yêu tiên trong thuật toán tìm đường đi tốt nhất:** BGP sẽ chọn đường đi tốt nhất từ danh sách các đường đi hợp lệ dựa vào thứ tự ưu tiên của các luật sau "ưu tiên từ trên xuống dưới".
  - Ưu tiên đường đi có trọng số Weight cao nhất. Đây là một thông số do Cisco đưa ra, nó chỉ mang tính local trong một router.
  - Ưu tiên đường đi có Local Preference cao nhất. Có giá trị mặc định là 100.
  - Ưu tiên đường đi có nguồn gốc từ lệnh Network hoặc aggregate hoặc thông qua quá trình Redistribute từ một IGP. Các đương đi có nguồn gốc từ lệnh Network hay redistribute có độ ưu tiên cao hơn từ lệnh aggregate.
  - Ưu tiên đường đi có AS path ngắn nhất.
  - Ưu tiên đường đi có nguồn gốc thấp nhất. IGP < EGP < INCOMPLETE.
  - Ưu tiên đường đi có giá trị MED nhỏ nhất. Mặc định bằng 0.
  - Ưu tiên đường đi eBGP hơn so với iBGP.
  - Ưu tiên đường đi có IGP thấp nhất đến BGP next-hop.
  - Nếu có hai đường đi đến đích mà có tất cả các thuộc tính trên là giống nhau thì nó sẽ ưu tiên đường đi được nhận trước (đường đi cũ nhất).
  - Ưu tiên đường đi đến BGP router có router ID nhỏ nhất. Giá trị router ID là địa chỉ IP cao nhất trên Router. Cũng có thể gán bằng lệnh bgp router-id.
  - Ưu tiên cho đường đi có số cluster là ít nhất.
  - Ưu tiên đường đi đến từ những láng giềng có địa chỉ thấp nhất. Địa chỉ này là địa chỉ được dùng trong lệnh neighbor
- **Import /Export Rules (Policies).**

II.4. Mạng không liên tục.

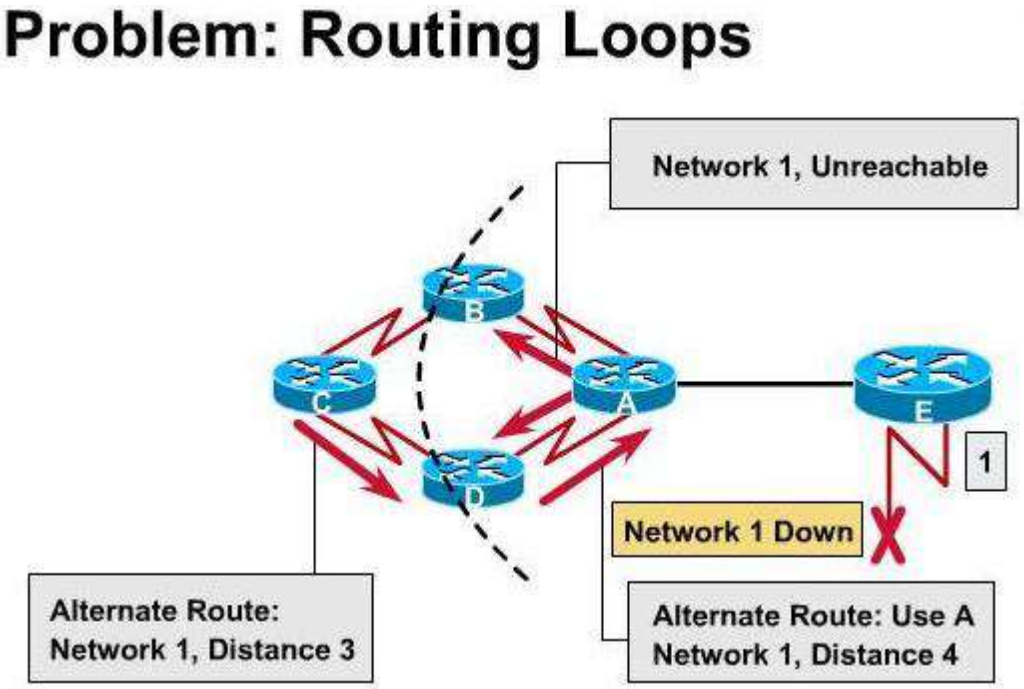
- Mạng không liên tục "Discontigous Network": là một mạng chính "Major Network" bị chia cắt bởi một hay nhiều Major netwrok khác.



- RIPv1 không hoạt động được trong hệ thống mạng không liên tục vì:
  - RIPv1 là phương thức định tuyến theo dạng classful. Nó sẽ tự động summarize địa chỉ mạng thành lớp mạng mặc định A, B, C.
  - RIPv1 chỉ quảng bá đường route, không kèm theo địa chỉ subnet mask.

II.5. Routing Loop

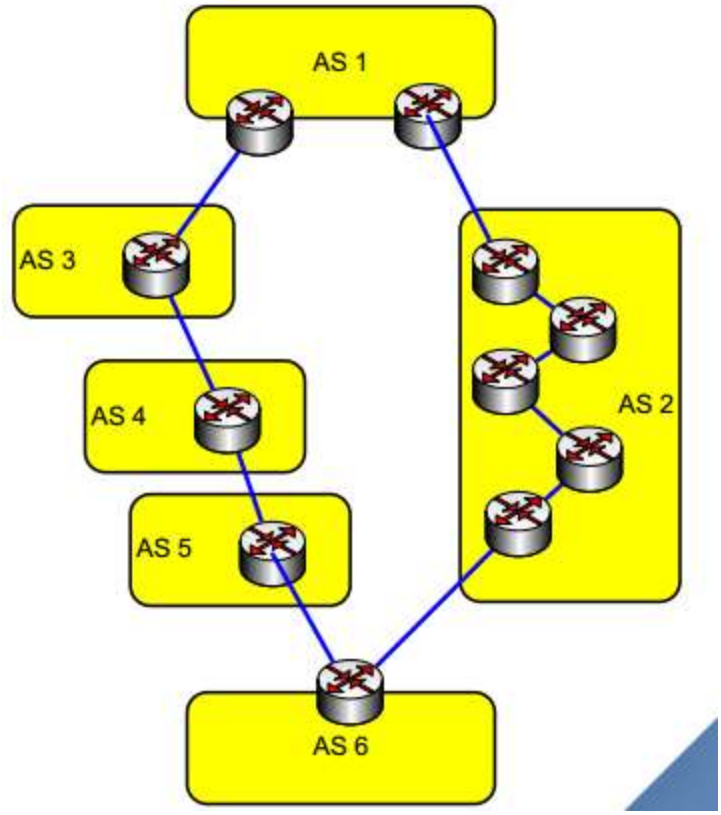
- **Khái niệm**:Routing loops là tình trạng gói tin truyền đi qua nhiều Router (lặp đi lặp lại, thành vòng)mà không đến được đích.



- **Giải pháp chống loop:**
  - Split Horizon: Khi router nhận được cập nhật định tuyến của một mạng từ phía cổng nào thì nó không gửi ngược lại cập nhật cho mạng ấy về phía cổng mà nó nhận được nữa.
  - Routing Poisoning: Khi một thông tin Network nào đó trên Router bị mất đi, thì nó sẽ gởi cập nhật cho các Router láng giềng của nó về thông tin đường mạng đã chết trên với Metric là Infinity 16.
  - Poison – reverse: khi Router nhận được thông tin của láng giềng của nó báo về một đường mạng đã chết => Router sẽ gởi gói Poison Reverse (giống như 1 thông tin Ack) khẳng định là Router đã biết về việc đó.
  - Triggered updates: khi Router có sự thay đổi thông tin về 1 Network nào đó thì ngay lập tức nó sẽ gửi cập nhật về sự thay đổi đó cho các láng giềng của nó mà không cần phải đợi đến đúng chu kỳ.
  - Hold-down timer: khi Router B nhận được thông tin từ Router A báo về một Network X đã mất, thì Router B vẫn giữ thông tin về đường mạng X trong bảng định tuyến trong khoảng thời gian Holddown Timers là 180s. Trong khoảng thời gian trên nếu như Router B nhận được thông tin về đường mạng X từ các Router khác Router A với Metric = hoặc kém tốt hơn Metric từ Router A, thì Router B sẽ không học thông tin về đường mạng X từ các Router trên. Nhưng nếu tốt hơn thì học ngay. Sau thời gian Holddown Timers, nếu như có 1 Router nào đó báo cho Router B thông tin về đường mạng X với bất kỳ Metric nào thì Router B sẽ học thông tin về đường mạng X qua Router trên, tuy nhiên vẫn giữ thông tin về đường mạng X qua Router A thêm 60s.

II.6. Trong BGP đường đi được chọn sử dụng AS - PATH có phải là đường đi ngắn nhất? Giải thích?

- Trong BGP đường đi được chọn sử dụng AS - PATH chưa chắc là đường đi ngắn nhất. Vì độ ưu tiên chọn lựa AS-PATH của "Đường đi AS ngắn nhất" lớn hơn "đường đi có chi phí thấp nhất" , nên khi AS-PATH đi qua số AS ít hơn nhưng có chi phí nhiều hơn thì quãng đường là dài hơn so với một AS-PATH đi qua nhiều AS hơn nhưng chi phí ngắn hơn.
- VD:Ta có {AS2, AS1} là ngắn hơn so với {AS5, AS4, AS3, AS1}, tuy nhiên ở đường đi thứ nhất số router đi qua là nhiều hơn khi sử dụng AS-PATH đường đi ngắn nhất.

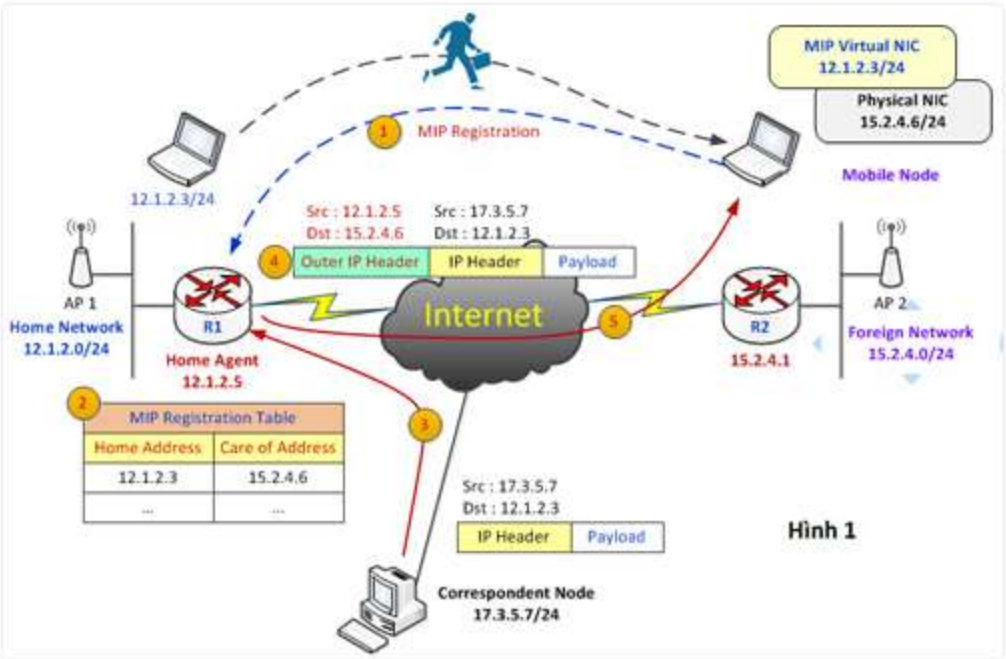


III. Mobile Ipv4

III.1. Care-of Address (CoA)

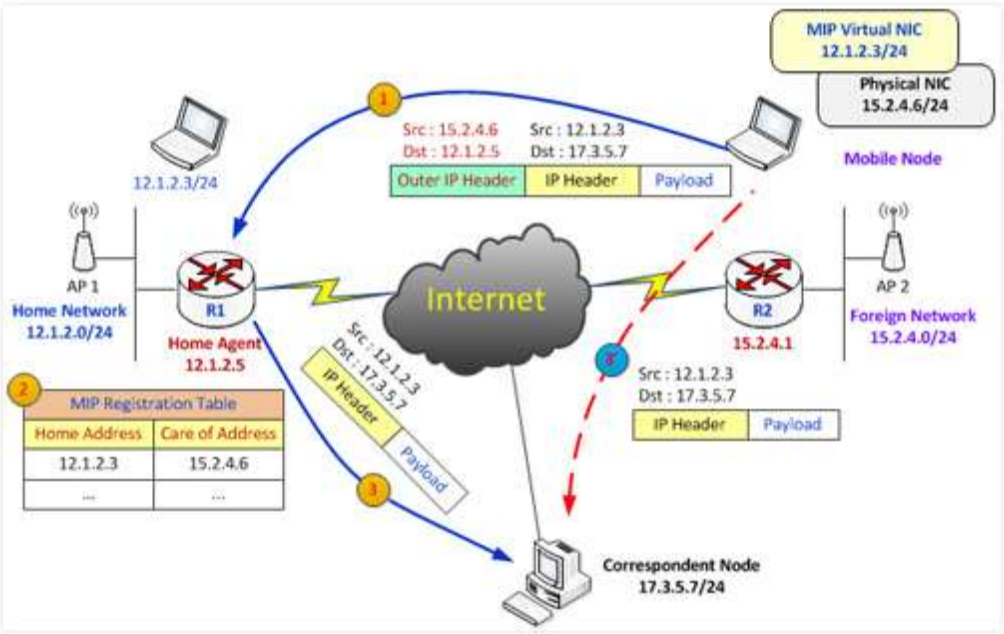
- ***Địa chỉ Care of Address***"địa chỉ tạm trú": là địa chỉ mà khi mobile node di chuyển từ mạng thường trú đến mạng tạm trú (Foreign network). Mobile node "MN" có nhiệm vụ đăng ký với HA địa chỉ CoA mới này. MN có thể nhận địa chỉ này là từ máy chủ DHCP hoặc sử dụng IP của đại diện tạm trú FA (Foreign Agent).

III.2. Hoạt động của mobile IP.



- "1" Theo như trong hình này, router R1 đóng vai trò như một HA cho nút di động. Khi MN di chuyển sang mạng tạm trú, nó sẽ thực hiện việc đăng ký địa chỉ CoA bằng cách gửi gói tin "MIP registration" đến cho đại diện thường trú HA.
- "2" HA sử dụng địa chỉ CoA nhận được ở bước 1 để tiến hành cập nhật bảng đăng ký (MIP Registration Table). Bảng đăng ký này lưu trữ ánh xạ giữa địa chỉ thường trú, tạm trú và một số thông tin liên quan như thời hạn đăng ký.
- "3" Khi gói tin được gửi từ CN đến địa chỉ thường trú của MN, đại diện thường trú HA sẽ đứng ra làm trung gian tiếp nhận gói tin này sau đó chuyển hướng chúng đến vị trí hiện tại của MN.
- "4" HA dùng phương pháp "đóng gói" gói để chuyển thông tin cho MN bằng cách dùng thêm phần mào đầu IP bên ngoài (Outer IP header) vào gói tin gốc và chuyển theo đường hầm (IP-in-IP tunelling) đến địa chỉ CoA mà MN đã đăng ký. Trong ví dụ minh họa đường hầm được hình thành giữa HA và MN.
- "5" - Card mạng vật lý (Physical NIC) thực hiện tháo bỏ IP header ngoài để khôi phục gói tin gốc và chuyển giao cho card mạng ảo (Virtual NIC). Các ứng dụng đang thực thi trên MN vốn chỉ gắn kết với địa chỉ thường trú trên card mạng ảo, do vậy việc thay đổi của CoA của thiết bị sẽ không làm gián đoạn luồng thông tin giữa hai thiết bị.
- Quá trình tiếp diễn cho đến khi hết thời hạn đã đăng ký (hoặc MN chuyển đến vị trí mới). Khi điều này xảy ra, MN sẽ tiến hành đăng ký lại với HA. Khi MN trở về mạng thường trú, nó không cần di động nữa, vì thế MN sẽ gửi một yêu cầu hủy bỏ đăng ký lưu động đến HA, nói rõ rằng nó đang "ở nhà" để HA không thực hiện đường hầm và dọn bỏ các địa chỉ tạm trú trong bảng đăng ký trước đó.

III.3. Vấn đề định tuyến tám giác.



- MN sau khi nhận được gói tin gốc sẽ biết được chính xác địa chỉ IP của CN. Vì thế, MN có thể gửi các gói tin trực tiếp đến CN hoặc thông qua đường hầm đến HA nhờ chuyển giúp. Việc gửi trực tiếp gói tin đến CN sẽ là giải pháp tối ưu giúp giảm thiểu delay khi gửi/nhận thông tin giữa MN và CN. Quá trình này được gọi là định tuyến tam giác. Tuy nhiên, thực tế một số router và firewall thường được cấu hình với chức năng "ingress filtering" nhằm mục đích ngăn chặn các cuộc tấn công giả mạo địa chỉ. Chức năng này sẽ chặn các gói tin có địa chỉ IP nguồn không thuộc subnet mạng cục bộ. Trong hình minh họa số 2 thì gói tin gửi từ MN đến CN sẽ có IP source là 12.1.2.3, không thuộc về subnet 15.2.4.0/24, do đó nó sẽ bị loại bỏ. Để giải quyết vấn đề này IP di động đưa ra giải pháp đường hầm nghịch (Reverse Tunneling). Theo đó MN sẽ chuyển gói tin thông qua đường hầm đến HA trước khi HA chuyển tiếp chúng cho CN (xem các bước 1, 2, 3 trong hình minh họa số 2).
- Để cải thiện hiệu quả định tuyến, người ta đưa ra giải pháp cho phép MN sau khi xác định được địa chỉ IP của CN thì MN sẽ gửi trực tiếp thông tin CoA hiện hành đến CN. CN sẽ duy trì ánh xạ liên kết giữa địa chỉ thường trú và CoA của MN (tương tự như HA) trong một khoảng thời gian nhất định. Nếu ánh xạ này vẫn còn hợp lệ thì CN và MN sẽ trao đổi dữ liệu trực tiếp với nhau mà không cần qua HA. Nếu ánh xạ không tồn tại hoặc bị expired thì CN sẽ tiến hành gửi các gói tin đến HA, rồi từ HA sẽ chuyển đến MN như bình thường, sau đó MN có thể gửi lại CoA cho CN
- Khi MN di chuyển từ FN này qua FN khác, tức sẽ chuyển từ FA cũ sang FA mới thì trong quá trình chuyển từ FA cũ sang FA mới, các gói tin vẫn được chuyển tới FA cũ gây ra tình trạng mất thông tin và để giảm việc thông tin bị mất do vấn đề này thì chúng ta có giải pháp forwarding để cho phép FA cũ chuyển tiếp thông tin đến FA mới.

IV. Content Delivery Network

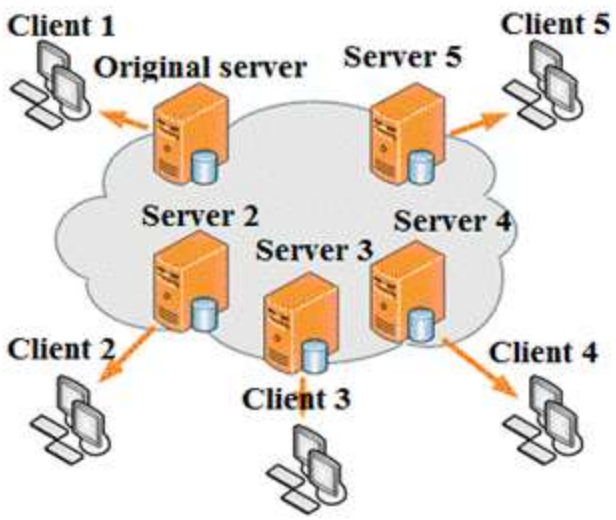
IV.1. Hạn chế của kiến trúc Client Server

- Một trong những vấn đề nảy sinh trong mô hình này đó là tính an toàn và bảo mật thông tin trên mạng. Do phải trao đổi dữ liệu giữa 2 máy ở 2 khu vực khác nhau cho nên dễ dàng xảy ra hiện tượng thông tin truyền trên mạng bị lộ.
- Hệ thống nhưng hoạt động nếu server gặp vấn đề "trong giải pháp 1 server"
- Dễ dàng lợi dụng các lỗ hổng bảo mật của server.
- Vấn đề cân bằng tải trong mô hình nhiều server.
- Hỏng địa chỉ URL khi server thay đổi.
- Gặp vẫn đề nghẽn cổ chai khi truyền dữ liệu giữa client và server.

IV.2. Các cơ chế để support scalability về hạ tầng đối với các ứng dụng Client Server

IV.3. Mạng CDN là gì? Cách hoạt động? Ứng dụng?

- **Tổng Quan:**
  - CDN "Content Delivery Network": được tạm hiểu là một hệ thống máy chủ được đặt ở nhiều nơi khác nhau trên thế giới và chứa những bản sao dữ liệu của nội dung website trong hệ thống và khi người dùng truy cập vào thì các bản sao đó nằm tại một máy chủ gần với người dùng nhất sẽ được thay thế với dữ liệu nội dung gốc của website. Giả sử như máy chủ website bạn ở Châu Âu nhưng khi một người dùng ở Việt Nam truy cập vào thì những dữ liệu mà người dùng nhận được là bản sao của máy chủ gốc được lưu trữ tại những máy chủ trong hệ thống CDN ở khu vực Đông Nam Á hoặc tại Việt Nam nơi gần người dùng nhất.
- **Nguyên lý hoạt động:**



  - Mô hình mạng phân phối nội dung (CDN) sử dụng một mạng các máy chủ được đặt ở nhiều vị trí khác nhau. Nội dung của nhà cung cấp được lưu trữ trong máy chủ gốc (Original server), các máy chủ khác trong mạng CDN sẽ thực hiện sao lưu, đồng bộ dữ liệu với máy chủ gốc.
  - Khi khách hàng gửi yêu cầu truy cập nội dung, mạng CDN sẽ tự động tìm kiếm máy chủ tốt nhất để cung cấp nội dung cho khách hàng. Do đó sẽ tránh được việc

quá nhiều khách hàng cùng yêu cầu truy cập đồng thời vào một máy chủ gây tắc nghẽn đường truyền.
  - Số lượng máy chủ trong mạng CDN càng lớn, mạng càng thể hiện được những ưu điểm của nó so với mô hình truyền thống.
- **Ứng dụng:**
  - Khai thác các ứng dụng nội dung số: video, audio…
  - Hệ thống tìm kiếm toàn cầu…

IV.4. Akamai

- Akamai là một nhà cung cấp dịch vụ CDN hàng đầu thế giới.
- Akamai sử dụng 2 cơ chế DNS và Cache Hit.

Topic 5: P2P Networks

1/ P2P và Client Server

- Client Server:

Server là một máy chủ web, đây là nơi lưu trữ nội dung của một trang web, và máy tính của bạn được gọi là Client, nó sẽ lấy thông tin từ Server để hiển thị lại trên máy tính của bạn. Mỗi Server độc lập có thể lưu hàng trăm nghìn dữ liệu khác nhau và chịu tải bơi hàng trăm Client cùng lúc và đó là vấn đề của mô hình Client Server vì nó phụ thuộc quá nhiều vào phần cứng của Server. Ví dụ như bạn muốn đọc bài A thì Server phải xử lí và cho ra nội dung A, một bạn khác muốn đọc bài B thì Server phải xử lí và cho ra nội dung B mỗi lần như vậy sẽ khiến cho Server tốn một phần CPU và RAM để xử lý. Server sẽ phải nâng cấp nếu không đáp ứng được nhu cầu của Client. Đó cũng chính là giới hạn về phần cứng của Server.

MỖi Client sử dụng một phần nhỏ đường truyền mạng của Server. Ví dụ như Server có đường truyền mạng khoảng 100MB/s, nếu bạn có 100 client cùng sử dụng thì mỗi ng` sẽ có 1 MB/s để sử dụng, nếu 100 client cùng sử dụng thì mỗi ng` còn sử dụng được 100KB/s. Đây là giới hạn về đường truyền Server.

Và nhà quản trị web sẽ phải trả một số tiền lớn cho dung lượng mà Client sử dụng.

- P2P

Mô hình này sẽ giúp mọi Client trở thành Server. Và ta chỉ cần một Server để điều khiển hoạt động cho từng Client khác nhau. Voi mô hình này, Client không chỉ lấy dữ liệu mà còn có thể chia sẻ dữ liệu cho các Client khác và việc chia sẻ dữ liệu này đươc gọi là seeding. Việc seeding rất quan trọng trong mô hình này, nếu không có seeding thì P2P chỉ giống như mô hình Client-Server. Không giống như Client-Server hiệu suất sẽ giảm đi khi có quá đông Client tham gia vào mạng. Hiệu suất của P2P sẽ tăng lên nếu số lượng Client càng đông.

Trong P2P tốc độ download càng nhanh khi có nhiều người seeding tập tin đó cho bạn.

2/ Pros và Cons của P2P

- Pros của P2P:

Các peer tham gia vào mạng có thể đóng góp tài nguyên để chia sẻ với nhau, tài nguyên có thể riêng lẻ hoặc có thể truy cập ở bất kì các node nào trong mạng.

Các peer đóng vai trò như cả Client khi truy vấn thông tin và Server khi cung cấp thông tin.

Không cần Server riêng, khi hệ thống mở rộng thì khả năng hoạt động càng tốt.

Chi phí thấp, dễ cài đặt và bảo trì.

- Cons của P2P

Liên quan đến văn hóa trong chia sẻ về các tài nguyên có bản quyền.

Không đáng tin cậy và không tốt cho các ứng dụng CSDL cần bảo mật cao.

3/ Napster, Gunutella, Kazza

- Napster:

Napster là mạng ngang hàng không cấu trúc đầu tiên thu hút được đông đảo người sử dụng trên mạng. Đây là sự kết hợp của một mạng ngang hàng peer to peer và một số máy chủ trung tâm để duy trì kết nối hệ thống và danh sách dữ liệu được chia sẻ trong mạng. Ngoài việc là một mạng peer to peer, Napster cũng giống như một mạng với các máy chủ. Chính các máy chủ này làm cho việc tìm kiếm dữ liệu và chia sẻ giữa các máy tính trong mạng tốt hơn, tạo nên mô hình mạng peer to peer đầu tiên được ưu chuộng với các dịch vụ chia sẻ file dữ liệu, file nhạc trên mạng Internet. Napster gồm 2 thành phần, thứ nhất là máy chủ trung tâm và thứ hai là các ứng dụng trên các máy tính kết nối với nhau. Một máy tính tham gia vào mạng sẽ kết nối với máy chủ trung tâm và đưa danh sách file chia sẻ trong máy tính lên máy chủ này. Những máy tính khi tìm kiếm dữ liệu sẽ tìm kiếm thông tin về từ khóa trên máy chủ trung tâm để biết máy tính nào hiện đang giữ file chia sẻ đó. Để tìm kiếm một file, một truy vấn sẽ được gửi đi tới máy chủ trung tâm cùng với từ khóa tìm kiếm. Máy chủ trung tâm sẽ tìm trong danh sách các file chia sẻ được đưa lên bởi các máy tính và trả về địa chỉ IP của máy tính lưu giữ file chia sẻ này. Sau đó sẽ là kết nối trực tiếp giữa máy tính yêu cầu và máy tính giữ file chia sẻ, dữ liệu được truyền giữa hai máy tính giống như trong một mạng ngang hàng.

Gunutella:

Gnutella là một mạng peer to peer thuần và chủ yếu dựa trên mạng peer to peer không có cấu trúc. Một phiên bản thương mại của Gnutella là Limewire. Các máy tính trong Gnutella được mô tả như là những "servent", những thành viên trong mạng và được chia sẻ file trong mạng. Các máy tính khác có thể lấy được những file chia sẻ này. Khi một máy tính A tìm kiếm file X, nó sẽ gửi một truy vấn broadcast tới tất cả các máy tính nó biết, được coi là hàng xóm của nó. Truy vấn sau đó sẽ được chuyển dần qua các bước và tới được máy tính có chứa file X.

Kazaa:

Kazaa sử dụng mô hình peer to peer chia sẻ file cùng 1 mô hình với Napster. Nhưng không giống như Napster, mà phân phối nội dung thông qua một máy chủ trung tâm, Kazaa sử dụng một hệ thống phân cấp. Người sử dụng Kazaa liên hệ trực tiếp với nhau để chia sẻ nội dung. Để chuyển đổi dữ liệu giữa những người sử dụng thì Kazaa sử dụng phương thức FastTrack. FastTrack được gọi là thế hệ thứ 2 của giao thức P2P.

4/ Bittorrent và Skype

- Bittorrent:

BitTorrent là một giao thức P2P, đồng nghĩa với mỗi máy tính tham gia trong mạng lưới BitTorrent sẽ đảm nhận cả việc download lẫn upload dữ liệu mà không cần có sự có mặt của một server trung tâm. Thường thì một máy tính sẽ tham gia vào một mạng lưới BitTorrent bằng cách sử dụng thông tin chứa trong một file .torrent. Các phần mềm

BitTorrent client, ví dụ như uTorrent hay BitComet sẽ sử dụng thông tin từ file này để liên lạc với một máy đảm nhiệm vai trò "tracker" trong mạng lưới. Tracker cũng là một dạng máy chủ, nhưng không trực tiếp cung cấp dữ liệu cho các máy khác trong mạng lưới BitTorrent mà chỉ chịu trách nhiệm giám sát và theo dõi tình trạng các máy tính đang tham gia vào mạng lưới. Thông qua giao tiếp và sử dụng các thông tin mà Tracker cung cấp, máy tính của bạn lúc này sẽ có thể thực hiện kết nối trực tiếp đến các máy khác trong mạng lưới để bắt đầu gửi/nhận dữ liệu.

Khi đã kết nối vào mạng lưới, máy tính của người dùng có thể bắt đầu thực hiện tải dữ liệu về theo từng phần nhỏ. Dữ liệu này do các máy khác trong mạng lưới cung cấp. Và dĩ nhiên, những phần dữ liệu đã được tải về cũng sẽ lại tiếp tục được máy của người dùng chia sẻ cho những máy chưa có phần đó. Với cơ chế này, cho dù 10000 máy cùng download một file tại một thời điểm cũng sẽ không gây quá tải cho máy chủ nào hết. Thay vào đó gánh nặng trên băng thông upload được chia sẻ đều cho các máy trong mạng lưới.

- Skype:

Skype hoạt động theo mô hình P2P. Thư mục người dùng của Skype hoàn toàn phân rã và phân bố trên các node mạng, điều đó có nghĩa là mạng có thể mở rộng dễ dàng mà không đòi hỏi một cơ sở hạ tầng tập trung phức tạp và đắt tiền.