**TRƯỜNG ĐẠI HỌC ĐÀ LẠT**

**KHOA CÔNG NGHỆ THÔNG TIN**



**BÁO CÁO ĐỒ ÁN CHUYÊN NGÀNH**

**TÌM HIỂU VỀ ĐỊNH TUYẾN BGP**

**Giáo viên hướng dẫn: Vũ Minh Quan**

**Sinh viên thực hiện: 2011438 – Hoàng Ngọc Minh Thắng**

**2012366 – Nguyễn Quang Minh**

**Đà lạt, …/2023**

**NHẬN XÉT CỦA GIÁO VIÊN HƯỚNG DẪN**

………………………………………………………………………………

………………………………………………………………………………

………………………………………………………………………………

………………………………………………………………………………

………………………………………………………………………………

………………………………………………………………………………

………………………………………………………………………………

………………………………………………………………………………

………………………………………………………………………………

………………………………………………………………………………

………………………………………………………………………………

………………………………………………………………………………

………………………………………………………………………………

………………………………………………………………………………

………………………………………………………………………………

………………………………………………………………………………

………………………………………………………………………………

………………………………………………………………………………

………………………………………………………………………………

Đà Lạt, ngày ….. tháng …… năm ……

Giáo viên hướng dẫn

[Ký tên và ghi rõ họ tên]

**LỜI CẢM ƠN**

Trước hết, tụi em xin phép gửi lời cảm ơn đến thầy Vũ Minh Quan. Người đã từng bước hướng dẫn, giúp đỡ tụi em trong quá trình thực hiện đồ án của tụi em.

Em xin chân thành cảm ơn các thầy cô giáo khoa công nghệ thông tin của trường Đại Học Đà Lạt đã góp ý và giúp đỡ tụi em có thêm những ý tưởng mới trong quá trình thực hiện đồ án.

Tuy rằng tụi em có cố gắng trong quá trình làm đồ án nhưng không thể tránh khỏi những thiếu sót , tụi em rất mong có được sự góp ý của tất cả các quý thầy cô giáo để kết quả của em được hoàn thiện hơn.

Một lần nữa em xin chân thành cảm ơn, chúc quý thầy cô thật nhiều sức khỏe.

**MỞ ĐẦU**

BGP (Border Gateway Protocol) là một trong những giao thức định tuyến phổ biến nhất được sử dụng trong hệ thống mạng lớn như Internet. Nó đóng vai trò quan trọng trong việc kết nối các mạng con với nhau để tạo thành một hệ thống mạng lưới toàn cầu.

Mục tiêu của đồ án là tìm hiểu và nghiên cứu về BGP, cách thức hoạt động của giao thức, các thuật toán định tuyến, các tính năng, cơ chế bảo mật và ứng dụng của nó. Đồ án cũng sẽ tập trung vào cách cấu hình và vận hành BGP trong môi trường mạng thực tế, bao gồm các vấn đề liên quan đến kết nối với các nhà cung cấp dịch vụ Internet (ISP) và xử lý các vấn đề định tuyến như hỗ trợ đa đường tuyến (multihoming) và tránh các vấn đề liên quan đến đường đi còn sót lại (route flapping).

Ngoài ra, đồ án cũng sẽ đề cập đến những thách thức và vấn đề thường gặp trong quá trình triển khai và vận hành BGP, và cung cấp các giải pháp để giải quyết chúng. Việc tìm hiểu và nghiên cứu về BGP sẽ giúp người đọc có được kiến thức vững chắc về giao thức định tuyến này và có thể áp dụng nó trong thực tế để xây dựng một hệ thống mạng lưới ổn định và an toàn.

**MỤC LỤC**

[**Chương 1: Tổng quan về BGP :** 7](#_Toc138623088)

[**I.** **Khái niệm** 7](#_Toc138623089)

[**II.** **Lịch sử ra đời của BGP** 12](#_Toc138623090)

[**III.** **Đặc điểm của BGP** 13](#_Toc138623091)

[**Chương 2: Tìm hiểu về các cấu trúc và cách thức hoạt động của BGP** 15](#_Toc138623092)

[I. **Cấu trúc của BGP** 16](#_Toc138623093)

[**II.** **Cách thức hoạt động của BGP** 16](#_Toc138623094)

[**III.** **BGP trong mô hình mạng doanh nghiệp** 17](#_Toc138623095)

[**IV.** **Tiến trình chọn đường đi của BGP** 19](#_Toc138623096)

[**Chương 3: Triển khai giao thức BGP trên phần mềm giả lập** 38](#_Toc138623097)

[**Chương 4: Kết luận và hướng phát triển của đề tài** 41](#_Toc138623098)

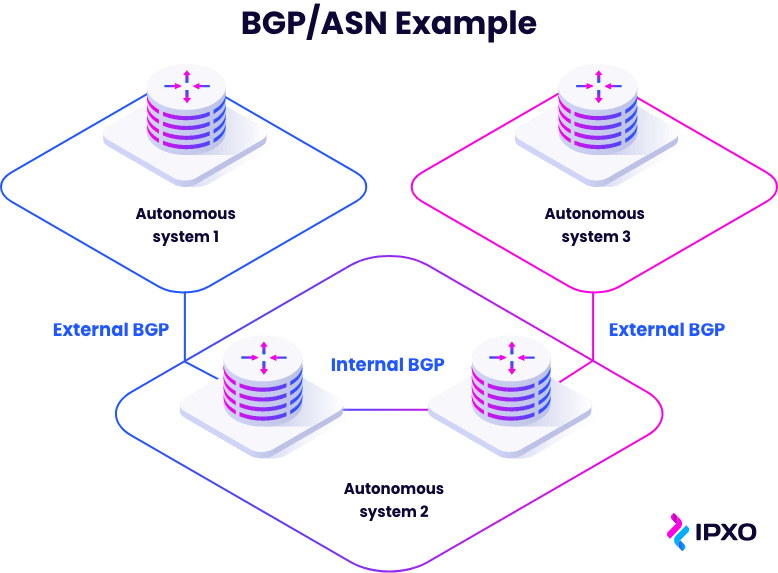
[***4.1*** ***Kết luận*** 41](#_Toc138623099)

[**4.2** ***Hướng phát triển*** 41](#_Toc138623100)

[***4.3*** ***Tổng kết*** 43](#_Toc138623101)

[**TÀI LIỆU THAM KHẢO** 45](#_Toc138623102)

# **Chương 1: Tổng quan về BGP :**



1. **Khái niệm**

BGP (Border Gateway Protocol) là giao thức tìm đường nòng cốt trên Internet, nó được thiết kế để cung cấp khả năng định tuyến không vòng lặp giữa các miền định tuyến riêng biệt chứa các chính sách định tuyến độc lập (hệ thống tự trị). Cisco triển khai phần mềm của BGP phiên bản 4 bao gồm hỗ trợ cho số hệ thống tự trị 4 byte và tiện ích mở rộng đa giao thức để cho phép BGP mang thông tin định tuyến cho các tuyến IP multicast và nhiều lớp, địa chỉ giao thức bao gồm IP Phiên bản 4 (IPv4), IP Phiên bản 6 (IPv6), Mạng riêng ảo Phiên bản 4 (VPNv4), Dịch vụ mạng không kết nối (CLNS) và VPN lớp 2 (L2VPN). Nó hoạt động dựa trên việc cập nhật một bảng chứa các địa chỉ mạng (prefix) cho biết mối liên kết giữa các hệ thống tự trị (autonomous system, tập hợp các hệ thống mạng dưới cùng sự điều hành của một nhà quản trị mạng, thông thường là một nhà cung cấp dịch vụ Internet, ISP). BGP là một giao thức vector đường đi (path vector). Khác với các giao thức tìm đường khác như RIP (vector độ dài), OSPF (trạng thái liên kết), BGP chọn đường bằng một tập các chính sách và luật. Phiên bản BGP hiện nay là phiên bản 4, dựa trên RFC 4271.

Một bộ định tuyến chạy phần mềm của Cisco có thể được cấu hình để chỉ chạy một quy trình định tuyến BGP và là thành viên của chỉ một hệ thống tự trị BGP. Tuy nhiên, quy trình định tuyến BGP và hệ thống tự trị có thể hỗ trợ nhiều cấu hình họ địa chỉ BGP và họ địa chỉ con đồng thời.

BGP được thiết kế để chạy trên một giao thức vận chuyển đáng tin cậy; nó sử dụng TCP (cổng 179) làm giao thức vận chuyển bởi vì TCP là một giao thức hướng kết nối. Cổng TCP đích được gán 179 và cổng cục bộ được gán một số cổng ngẫu nhiên. Phần mềm của Cisco hỗ trợ BGP phiên bản 4 và phiên bản này đã được được các nhà cung cấp dịch vụ Internet (ISP) sử dụng để giúp xây dựng Internet. RFC 1771 đã giới thiệu và thảo luận về một số tính năng BGP mới để cho phép giao thức mở rộng quy mô để sử dụng Internet. RFC 2858 giới thiệu đa giao thức tiện ích mở rộng để cho phép BGP mang thông tin định tuyến cho các tuyến IP multicast và nhiều giao thức Lớp 3 họ địa chỉ, bao gồm IPv4, IPv6 và CLNS.

BGP hỗ trợ tìm đường liên vùng phi lớp (CIDR Classless Inter-Domain Routing) và dùng kỹ thuật kết hợp đường đi để giảm kích thước bảng tìm đường (ví dụ nếu một mạng chiếm 255 địa chỉ lớp C từ 203.162.0.0/24 - 203.162.254.0/24 thì chỉ dùng 1 địa chỉ 203.162.0.0/16 để định danh mạng).

BGP chủ yếu được sử dụng để kết nối mạng cục bộ với mạng bên ngoài để truy cập Internet hoặc kết nối với các tổ chức khác. Khi kết nối với một tổ chức bên ngoài, BGP bên ngoài (eBGP) ngang hàng phiên được tạo ra. Mặc dù BGP được gọi là giao thức cổng bên ngoài (EGP), nhiều mạng trong một tổ chức đang trở nên phức tạp đến mức BGP có thể được sử dụng để đơn giản hóa mạng nội bộ được sử dụng trong tổ chức. BGPpeers trong cùng một tổ chức trao đổi thông tin định tuyến thông qua nội bộ BGP (iBGP) phiên ngang hàng.

BGP sử dụng thuật toán định tuyến vectơ đường dẫn để trao đổi thông tin về khả năng tiếp cận mạng với các mạng khác Các thiết bị mạng nói BGP. Thông tin về khả năng tiếp cận mạng được trao đổi giữa các BGP ngang hàng trong cập nhật định tuyến. Thông tin về khả năng tiếp cận mạng chứa số mạng, thuộc tính cụ thể của đường dẫn và danh sách các số hệ thống tự trị mà một tuyến đường phải chuyển để đến mạng đích. danh sách này là chứa trong thuộc tính AS-path. BGP ngăn chặn các vòng lặp định tuyến bằng cách từ chối mọi cập nhật định tuyến có chứa số hệ thống tự trị cục bộ vì điều này cho biết rằng tuyến đường đã đi qua đó hệ thống tự trị và do đó một vòng lặp sẽ được tạo ra. Thuật toán định tuyến đường dẫn-vector BGP là một sự kết hợp giữa thuật toán định tuyến theo vectơ khoảng cách và phát hiện vòng lặp AS-path.

Theo mặc định, BGP chọn một đường dẫn duy nhất làm đường dẫn tốt nhất đến máy chủ hoặc mạng đích. Lựa chọn đường đi tốt nhất thuật toán phân tích các thuộc tính đường dẫn để xác định tuyến nào được cài đặt là đường tốt nhất trong định tuyến BGP bàn. Mỗi đường dẫn mang các thuộc tính bắt buộc nổi tiếng, tùy chọn nổi tiếng và chuyển tiếp tùy chọn được sử dụng trong phân tích đường đi tốt nhất của BGP. Phần mềm của Cisco cung cấp khả năng tác động đến lựa chọn đường dẫn BGP bằng cách thay đổi một số thuộc tính này bằng cách sử dụng giao diện dòng lệnh (CLI.) Lựa chọn đường dẫn BGP cũng có thể được bị ảnh hưởng thông qua cấu hình chính sách BGP tiêu chuẩn. Để biết thêm chi tiết về việc sử dụng BGP để tác động đến đường dẫn lựa chọn và định cấu hình chính sách BGPđể lọc lưu lượng truy cập, hãy xem “BGP4PrefixFilter và Inbound Route Maps” mô-đun và mô-đun “Lọc tuyến đường đi dựa trên tiền tố BGP”.

BGP sử dụng thuật toán lựa chọn đường dẫn tốt nhất để tìm một tập hợp các tuyến đường tốt như nhau. Các tuyến đường này là tiềm năng đa đường. Trong Phiên bản Cisco IOS 12.2(33)SRD và các phiên bản mới hơn, khi có nhiều đường truyền tốt như nhau có sẵn hơn số lượng tối đa cho phép, các đường dẫn cũ nhất được chọn làm nhiều đường dẫn.

BGP được sử dụng thay thế cho EGP và xóa hẳn mạng xương sống NSFNET nhằm giúp cho Internet trở thành một hệ thống phân tán đúng nghĩa.

Ngoài việc sử dụng BGP giữa các AS, BGP cũng có thể được sử dụng trong các mạng riêng quy mô lớn do OSPF không đáp ứng được. Một lý do khác là dùng BGP để hỗ trợ multihome.

Đa số người sử dụng Internet thường không sử dụng BGP một cách trực tiếp. Chỉ có các nhà cung cấp dịch vụ Internet sử dụng BGP để trao đổi đường đi. BGP là một trong những giao thức quan trọng nhất đảm bảo tính kết nối của Internet.

**Một số khái niệm cơ bản trong BGP:**

**Autonomous System (AS)**: Autonomous System là một tập hợp các mạng, router và các thiết bị mạng khác có cùng quyền kiểm soát và định tuyến theo một chính sách chung. Mỗi AS được gán một AS Number (ASN) duy nhất để xác định nó trong hệ thống Internet. AS có thể là một nhà cung cấp dịch vụ Internet (ISP), một công ty, một tổ chức hoặc một mạng lớn.

**eBGP**: Được triển khai ngoại vùng, giữa các AS khác nhau. Khi hai BGP Speaker thuộc các AS khác nhau kết nối với nhau thông qua eBGP, chúng trao đổi thông tin định tuyến về các đường mạng giữa các AS

**iBGP**: Được triển khai trong nội vùng của một AS. Trong một AS, khi hai BGP Speaker (router) cùng AS kết nối với nhau thông qua iBGP, chúng sẽ trao đổi thông tin định tuyến về các đường mạng trong AS đó.

**AS Path**: AS Path (Đường dẫn AS) là một thuộc tính trong tin nhắn BGP, nó mô tả chuỗi các Autonomous System mà đường mạng đã đi qua trước khi đến đích. AS Path giúp xác định quảng bá và kiểm soát đường mạng trong mạng lớn.

**AS Number:** là một số duy nhất được gán cho mỗi Autonomous System trong hệ thống Internet. AS Number được sử dụng để xác định và nhận dạng các AS khác nhau khi trao đổi thông tin định tuyến qua BGP. ASN được chia thành hai loại:

**Public AS Number**: Đây là các số AS được cung cấp bởi IANA (Internet Assigned Numbers Authority) và được sử dụng rộng rãi trong mạng lớn, chẳng hạn như các nhà cung cấp dịch vụ Internet (ISP), tổ chức, công ty, v.v.

**Private AS Number**: Đây là các số AS được dành riêng cho sử dụng nội bộ trong mạng riêng. Private AS Number không được quảng bá ra bên ngoài mạng nên không gây xung đột với các số AS công cộng.

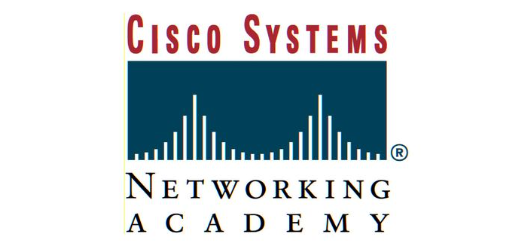
**Single-homed:** Single-homed ám chỉ rằng một tổ chức chỉ có một kết nối với một nhà cung cấp dịch vụ Internet (ISP) duy nhất. Tổ chức này chỉ kết nối với một mạng Internet thông qua một ISP. Điều này thường áp dụng cho các tổ chức nhỏ hoặc cá nhân không yêu cầu độ tin cậy và sự dự phòng cao hơn.

**Dual-Home:** Dual-Home đề cập đến việc một tổ chức có hai kết nối độc lập đến hai ISP khác nhau. Hai kết nối này được sử dụng để cung cấp tính dự phòng và độ tin cậy cao hơn cho tổ chức. Khi một ISP gặp sự cố, tổ chức vẫn có kết nối hoạt động thông qua ISP còn lại.

**Multihomed**: Multihomed đề cập đến việc một tổ chức có nhiều hơn hai kết nối đến các ISP khác nhau. Tổ chức này có thể kết nối với ba hoặc nhiều hơn ba ISP, tùy thuộc vào nhu cầu và yêu cầu của họ. Multihoming cho phép tổ chức tận dụng các đường mạng khác nhau từ các ISP khác nhau để tăng cường độ tin cậy, cải thiện hiệu suất và cung cấp sự dự phòng cao hơn.

**Dual-Multihomed**: Dual-Multihomed kết hợp cả khái niệm Dual-Home và Multihomed. Điều này ám chỉ rằng một tổ chức có hai kết nối độc lập đến hai ISP khác nhau và mỗi ISP cung cấp kết nối đa đường mạng (multihoming). Dual-Multihomed là một cách để tăng cường tính dự phòng và độ tin cậy, đồng thời tận dụng các đường mạng khác nhau từ các ISP khác nhau.

1. **Lịch sử ra đời của BGP**

****

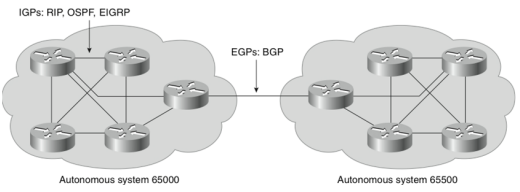
**BGP (Border Gatewave Protocol )** được giới thiệu lần đầu tiên vào năm 1989 ( Trong RFC 1105), phiên bản đầu tiên của nó được hoàn thành một năm sau đó và được giới thiệu trong RFC 1163. Sự phát triển của giao thức BGP được trải qua khá nhiều giai đoạn và tiếp tục được hoàn thiện cho đến ngày nay và trải qua tổng cộng 4 phiên bản là BGP-1, BGP-2, BGP-3 , BGP-4. Phiên bản ngày nay được sử dụng là BGP-4 được giới thiệu vào năm 1995 trong RFC 1771. BGP-4 có gì khác so với các phiên bản trước đây của nó ? Sự khác nhau rõ ràng nhất của BGP ver4 và các version trước đó là việc BGP version 4 là “classless” còn các version trước đây là “classfull”, tại sao lại có sự khác nhau căn bản này ? lý do được giải thích như sau :

+ Ban đầu trong các phiên bản trước (khởi đầu là từ năm 1989) lúc này mạng internet vẫn còn tương đối nhỏ, nó chưa thực sự “ phình” to như hiện tại, lúc bây giờ thì việc sử dụng hết dải địa chỉ của IPv4 vẫn là không tưởng và chưa được nghĩ đến, nên sử dụng “classful” và những người thiết kế không nghĩ đến việc làm sao phải tiết kiệm địa chỉ để sử dụng

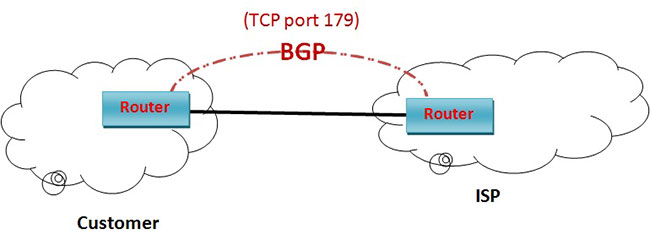
+ Khi số lượng địa chỉ IPv4 đã ngày một cạn kiệt thì việc làm sao để các giao thức chạy trên nền IP có thể tiết kiệm được dải địa chỉ IPv4 là hoàn toàn cần thiết (cách thức này là để đối phó với việc cạn kiệt địa chỉ IP trong IPv4 còn trong IPv6 thì vấn đề cạn kiệt địa chỉ IP vẫn chưa phải là một vấn đề vì số lượng rât lớn của địa chỉ IPv6). Năm 1995 khi phiên bản BGP version 4 được chính thức ban hành thì nó là một “ classless protocol”, để hiểu thêm về “classless” là gì thì ta có thể đọc trong RFC 1517 được ban hành năm 1993.

**Tại sao cần sử dụng BGP ?**

Như đã biết thì nhiệm vụ của Router là định tuyến, việc một gói tin đi đến Router, thì Router sẽ thực hiện việc xem xét gói tin đó đến từ đâu, cần chuyển qua đâu và tra trong bảng định tuyến nếu như có tuyến đường đến đích thì nó sẽ forward gói tin đó theo tuyến đường có sẵn trong bảng định tuyến. Router chạy các giao thức định tuyến như : RIP, OSPF, EIGRP, BGP. Trong đó thì RIP, OSPF và EIGRP chạy trong cùng một AS ( Autonomous System ) còn BGP chạy giữa các AS. BGP chính là một giao thức thuộc EGP (Exterior Gateway Protocol), để hiểu rõ vấn đề, ta sẽ theo dõi hình phía dưới:



1. **Đặc điểm của BGP**



1. ***Phân phối thông tin định tuyến***

BGP cho phép các nhà cung cấp dịch vụ internet trao đổi thông tin định tuyến với nhau để xác định các tuyến đường tốt nhất để chuyển tiếp gói dữ liệu.

1. ***Tính linh hoạt***

BGP cho phép các nhà cung cấp dịch vụ internet tự động cập nhật các tuyến đường định tuyến, giúp tăng tính linh hoạt của mạng lưới internet.

1. ***Độ tin cậy cao***

BGP được thiết kế để đảm bảo tính tin cậy cao trong việc phân phối thông tin định tuyến. Điều này giúp đảm bảo rằng các tuyến đường được chọn là tốt nhất và gói dữ liệu được chuyển tiếp một cách hiệu quả.

1. ***Hỗ trợ nhiều loại định tuyến***

BGP hỗ trợ nhiều loại định tuyến, bao gồm cả định tuyến theo địa chỉ IP và định tuyến theo các tiêu chí khác như AS (Autonomous System)

1. ***Quản lý lưu lượng truy cập***

BGP cho phép quản lý được lưu lượng truy cập giữa các mạng lưới khác nhau, giúp tăng cường tính bảo mật và kiểm soát lưu lượng truy cập trên mạng internet.

1. ***Khả năng mở rộng***

BGP có khả năng mở rộng, cho phép mạng lưới internet có thể mở rộng kích thước và độ phức tạp của nó một cách linh hoạt

**Thuộc tính BGP (attribute):** các thuộc tính này được sử dụng bởi BGP để quyết định đường đi tốt nhất cho gói tin:

* ***AS – Path***: được sử dụng để ngăn chặn các vòng lặp định tuyến và để tối ưu hóa đường đi
* ***Next hop***: được sử dụng để chỉ định đường đi tiếp theo và để xác định độ ưu tiên của đường đi
* ***Local Preference***: được sử dụng để lựa chọn đường đi trong cùng một mạng con
* ***MED***: được gửi từ ISP đến các khách hàng của họ, và các khách hàng sử dụng MED để lựa chọn đường đi tốt nhất
* ***Communities***: cho phép các ISP áp dụng các chính sách khác nhau cho các khách hàng khác nhau, dựa trên các yêu cầu riêng của từng khách hàng

***BGP có 4 thông điệp kết nối:***

* Open (mở phiên kết nối)
* Update (thông báo hoặc rút lại một đường đi)
* Notification (thông báo lỗi)
* Keep-alive (duy trì phiên kết nối)

Sử dụng giao thức định hướng kết nối với những cải tiến

* Bản tin cập nhật là tin cậy
* Cập nhật theo chu kì
* Nhiều thông số tính metrics
* Được dùng để thiết kế mạng có quy mô rất lớn

Cấu hình hệ thống tự trị liên kết: Vai trò chính của BGP là cung cấp thông tin liên lạc giữa hai hệ thống tự trị.

BGP hỗ trợ Next-Hop Paradigm.

Phối hợp giữa nhiều BGP speaker trong AS (Autonomous System - Hệ thống tự trị).

Thông tin đường dẫn: BGP advertisement (quảng bá) cũng bao gồm thông tin đường dẫn, cùng với cặp điểm đích có thể truy cập và điểm đến tiếp theo.

Hỗ trợ policy: BGP có thể triển khai các policy có thể được cấu hình bởi quản trị viên. Ví dụ, một router chạy BGP có thể được cấu hình để phân biệt giữa các tuyến được biết trong AS và được biết từ bên ngoài AS.

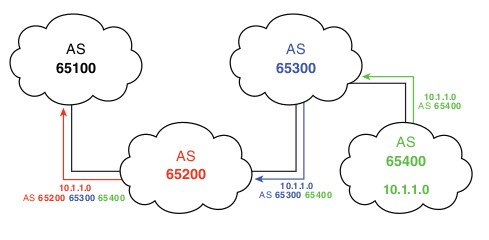
Chạy qua TCP.

BGP bảo tồn băng thông mạng.

BGP hỗ trợ CIDR.

BGP cũng hỗ trợ bảo mật.

# **Chương 2: Tìm hiểu về các cấu trúc và cách thức hoạt động của BGP**



**BGP (Border Gateway Protocol)** là một giao thức định tuyến đường lớp 4 được sử dụng trong mạng lớn, như Internet, để trao đổi thông tin định tuyến giữa các thiết bị định tuyến (router). BGP đóng vai trò quan trọng trong việc kết nối các mạng con thành một hệ thống mạng lớn.

1. **Cấu trúc của BGP**

* ***Autonomous System (AS):*** AS là một tập hợp các mạng, router và các thiết bị mạng khác có cùng quyền kiểm soát và định tuyến theo một chính sách chung. Mỗi AS được gán một số AS (ASN) duy nhất để xác định nó trong hệ thống Internet.
* ***BGP Speaker***: BGP Speaker là một thiết bị định tuyến chạy BGP và tham gia vào việc trao đổi thông tin định tuyến với các BGP Speaker khác. Một AS có thể có nhiều BGP Speaker, và chúng có thể nằm ở các điểm khác nhau trong mạng.
* ***BGP Neighbor***: BGP Neighbor là một kết nối định tuyến BGP giữa hai BGP Speaker. Các BGP Speaker lân cận trao đổi thông tin định tuyến qua BGP Neighbor và duy trì các phiên BGP để giữ cho các thông tin định tuyến được cập nhật.

1. **Cách thức hoạt động của BGP**

Như đã biết thì Internet ngày nay là tập hợp của các AS và các AS đó truyền thông với nhau sử dụng một giao thức chung. BGP cung cấp routing giữa các AS đó. Mô hình mạng ngày nay chủ yếu dựa trên giao thức TCP/IP, dựa vào đặc điểm nên khi phát minh ra BGP người ta đã sử dụng TCP như một phương tiện để các neighbor có thể thực hiện việc lập nên mối quan hệ neighbor than thiết. Để cho BGP có thể hoạt động giữa các AS ( cụ thể là cấu hình giữa các Router ) chúng phải tuân theo đúng những bước như sau:

**- Bước 1**: khi cấu hình BGP giữa các Router thì lúc này các router sẽ thành các Peer (các Router ngang hàng) của nhau, và một kết nối TCP sẽ được xem xét xem các Router ngang hàng này có thể kết nối được với nhau hay không.

**- Bước 2**: Cùng thỏa thuận các tham số : BGP có nhiều các gói tin và các gói tin này phải “matching” trước khi neighbor relationship được thiết lập, các tham số đó bao gồm như sau: AS, time…

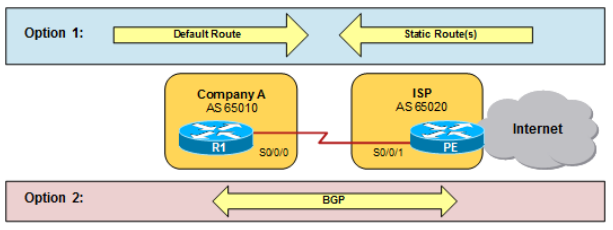
**- Bước 3**: Thiết lập Neighbor: sau khi các tham số đã thực sự “matching” thì mối quan hệ hàng xóm thân thiết sẽ được thiết lập, lúc này một kết nối BGP đã chính thức xuất hiện.

**- Bước 4**: Update thông tin: quá trình này là pha cuối cùng trong việc chạy BGP giữa các router, sau khi Neighbor được thiết lập, các router bắt đầu gửi đi những bảng tin để update thông tin về những route đến các mạng, sau khi các gói tin update này được nhận thì Router chạy BGP sẽ bắt đầu xây dựng bảng đinh tuyến của riêng mình đến các route mà nó học được.

1. **BGP trong mô hình mạng doanh nghiệp**

Việc chạy BGP giữa các AS với nhau là điều bắt buộc và nếu như không làm điều này thì các AS không thể liên lạc với bên ngoài được. Khi một doanh nghiệp, họ muốn kết nối tới 2 ISP thì sẽ sử dụng giao thức gì? Có cần thiết dùng BGP hay không hay dùng một đường default route là đủ, mỗi mô hình đều có ưu nhược điểm riêng của nó, sau đây là một số những mô hình được đưa ra:

1. ***Kết nối tới một ISP : Mô hình Single-homed***

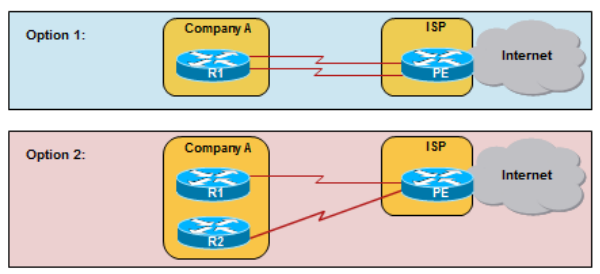
******

Trong mô hình này thì khách hành sẽ kết nối đến ISP với 2 lựa chọn đó là : một dùng default route hoặc dùng BGP:

**+ Option 1**: sử dụng Default Route: Company A muốn ra internet thì nó chỉ việc đẩy tất cả các gói tin ra một đường Default Route trỏ trực tiếp đến ISP và ISP sau khi nhận gói tín trả về thì nó có thể chuyển qua Company A với một đường Static Route. Ưu điểm của mô hình này là Router R1 của Company A sẽ không bị tốn tài nguyên vì nó không phải kiểm tra và xác định gói tin, gói tin đến nó chỉ đơn giản là đẩy hết qua ISP.

**+ Option 2**: Sử dụng BGP: BGP sẽ được thiết lập giữa Company A và ISP, thông tin về những Route giữa Company A và ISP sẽ được trao đổi với nhau rất linh hoạt do sử dụng giao thức định tuyến.

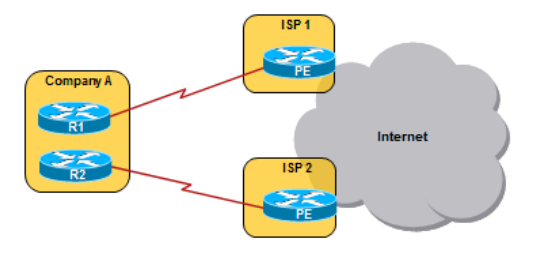
1. ***Kết nối tới một ISP : Mô hình Dual-Home***



**+ Option 1**: Cả 2 link có thể kết nối tởi ISP thông qua một router nẳm ở phía Company A (link thứ 2 mang tính chất dự phòng).

**+ Option 2**: có 2 link kết nối tới ISP thông qua 2 router nằm ở phía Company A Trong cả 2 mô hình trên có thể sử dụng Static hoặc Dynamic ( BGP).

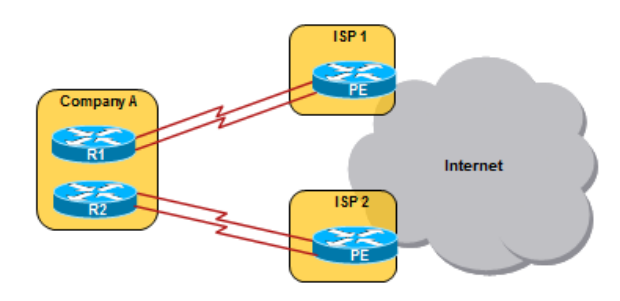
1. ***Kết nối tới nhiều ISP : Mô hình Multihomed***



Trong mô hình này thì định tuyến phải có khả năng hoặc động một cách tự động để trao đổi thông tin với nhau nên BGP là được sử dụng:

**- Ưu điểm của mô hình**: có thể chia tải giữa các ISP, tính linh động cao do sử dụng BGP nên có thể update được thông tin nhanh chóng giữa các Router.

1. ***Kết nối với nhiều ISPs: Mô hình Dual-Multihomed***

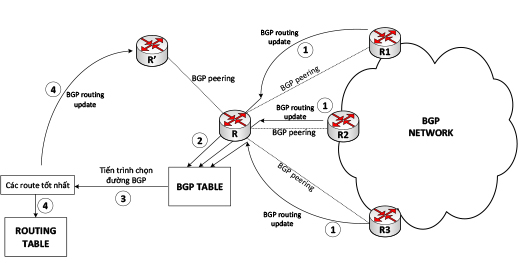


**Dual-Multihomed** có hầu hết những ưu điểm của mô hình Multihomed và chúng mở rộng về tính bền vững ( Resiliency) khi từ 1 Router có kết 2 kết nối tới 1 ISP.

1. **Tiến trình chọn đường đi của BGP**

BGP là một giao thức Path – vector, nó hoạt động theo cách thức của Distance – vector, ngoại trừ việc đường đi của BGP sẽ được đo đạc độ tối ưu bằng nhiều thuộc tính chứ không chỉ giới hạn bằng một thông số duy nhất là Metric như với các giao thức RIP và EIGRP.

Tương tự như EIGRP BGP cũng sử dụng một bộ 3 bảng dữ liệu cơ bản trong quá trình hoạt động của nó: Bảng neighbor, Bảng BGP và Bảng định tuyến. Bảng neighbor sẽ liệt kê ra danh sách các BGP router mà router đang xét đã thiết lập được quan hệ láng giềng (peering thành công); bảng BGP sẽ tập hợp tất cả các route mà các láng giềng này quảng bá cho router đang xét; và bảng định tuyến sẽ là nơi tập hợp những route tốt nhất mà giao thức BGP đã chọn ra từ bảng BGP để sử dụng làm đường đi chính thức đến các mạng đích. Quá trình vừa nêu có thể được tóm tắt trong hình vẽ dưới đây (hình 1):



***Hình 1 – Quá trình tiếp nhận và chọn lọc thông tin định tuyến của BGP***

Như mô tả trong hình 1, quá trình một router BGP tiếp nhận thông tin định tuyến và xử lý những thông tin này diễn ra theo các bước sau:

1. Router R đã peering thành công với các neighbor R1, R2 và R3. Các router R1, R2 và R3 sẽ gửi đi các BGP routing update để quảng bá cho router R các route BGP tốt nhất mà chúng đã lựa chọn được trước đó.

2. Router R khi nhận được các routing update từ các neighbor sẽ tập hợp hết lại vào một “kho chứa" route là bảng BGP. Như vậy, bảng BGP của một router là nơi tập kết tất cả thông tin định tuyến mà nó nhận được từ các láng giềng.

3. Tiếp theo, router R sẽ thực hiện “tuyển chọn” từ “kho route” trong bảng BGP ra các route tốt nhất cho từng mạng đích. Việc tuyển chọn này tuân theo một bộ quy tắc so sánh các thuộc tính đường đi của các route để từ đó chọn ra route tối ưu gọi là Tiến trình chọn đường BGP (BGP Path selection process).

4. Các route tốt nhất được chọn ra ở trên sẽ được router R cập nhật vào bảng định tuyến để sử dụng chính thức cho việc dẫn đường dữ liệu, đồng thời cũng được quảng bá đi cho router láng giềng kế tiếp (trên hình vẽ là router R). Lưu ý rằng, một router Path – vector hay Distance – vector chỉ quảng bá đến láng giềng những route tốt nhất mà nó có.

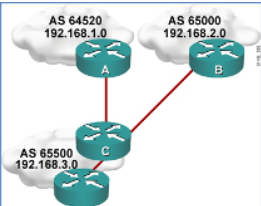
**Một số thuộc tỉnh đường đi thường gặp**

Như đã trình bày ở trên, một đường đi (route) trong BGP sẽ được đo đạc mức độ tối ưu bằng rất nhiều thông số đỉnh kèm mà người ta thường gọi là các Thuộc tính đường đi của BGP (BGP Path Attributes). Trong mục này, ta sẽ cùng điểm qua một vài thuộc tỉnh đường đi thường gặp nhất của giao thức BGP. Để có thể nắm vững và vận dụng thành thạo Tiến trình chọn đường BGP, ta cần phải nắm vững vai trò và đặc điểm của các thuộc tính này.

**Các thuộc tỉnh thường gặp được mô tả ở đây sẽ bao gồm:**

* *AS - path.*
* *Next - hop.*
* *Origin.*
* *Local Preference.*
* *MED.*
* *Weight.*

AS – path là một chuỗi ký tự liệt kê ra danh sách ASN của các AS mà một IP prefix đã lan truyền ngang qua để đến được router đang xét. Ta sẽ xem xét một ví dụ trong hình 2:



***Hình 2 – Ví dụ về thuộc tính AS – Path***

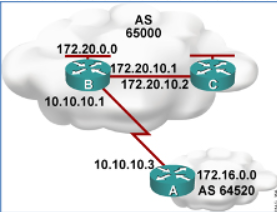
Trên hình 2, xem xét quá trình prefix 192.168.1.0 lan truyền từ AS 64520, qua AS 65500 rồi đến router B nằm trên AS 65000. Khi router B hiển thị thông tin về prefix 192.168.1.0 mà nó nhận được từ BGP, một chuỗi ký tự kèm theo sẽ xuất hiện cho biết prefix này đã đi qua các AS nào trước khi đến được router B. Chuỗi ký tự này trình bày ASN của các AS theo thứ tự từ gần nhất đến xa nhất với router B: “65500 64520".

**AS – path** là một thuộc tính quan trọng, được sử dụng rất nhiều trong việc so sánh độ tối ưu giữa các route đi đến cùng một đích đến trong Tiến trình chọn đường BGP.

**Next - hop**

Tương tự như với các giao thức IGP Distance – vector, next – hop là địa chỉ của router neighbor đã quảng bá thông tin định tuyến cho router đang xét, là router kế tiếp phải đi qua trong lộ trình đi đến một mạng đích nào đó. Tuy nhiên, trong xử lý thông tin định tuyến được quảng bá qua lại giữa các AS, vì BGP là một giao thức định tuyến ngoài, next – họp được xem như là địa chỉ IP inbound của AS kế tiếp trên đường đi đến đích.

Hãy xem xét một ví dụ (hình 3):



***Hình 3 - Ứng xử về Next – hop***

Trong ví dụ này, Router A (AS 64520) quảng bá prefix 172.16.0.0 đến router B thông qua một session eBGP với trường next – hop trong routing update được thiết lập là “10.10.10.3”. Đến lượt nó, router B lại tiếp tục quảng bá prefix này vào cho router C. Nếu giống như với các giao thức IGP thông thường. B sẽ quảng bá địa chỉ next – hop cho C là “172.20.10.1′′ –là IP của chính nó, nhưng vì đây là BGP – một giao thức định tuyến ngoài, router B sẽ vẫn đề nguyên next – hop “10.10.10.3" cho mạng 172.16.0.0 mà quảng bá đến cho router C. Kết quả là C sẽ nhận được cập nhật định tuyến cho prefix 172.16.0.0 có next – họp là 10.10.10.3, và nếu như C không được định tuyến trước đó để có thể đi đến được địa chỉ 10.10.10.3, C sẽ không thể sử dụng được cập nhật định tuyến này, từ đó không thể route dữ liệu đi đến mạng 172.16.0.0 được. Để tránh ảnh hưởng của ứng xử next – hop như next – AS như trình bày ở trên, trên các router biên như router B, khi thiết lập iBGP peering với các router BGP trong cùng AS, có thể sử dụng tùy chọn “*next-hop-self*" trong câu lệnh “*neighbor*". Ví dụ, với router B trong trường hợp này, B sẽ cấu hình thiết lập neighbor với C sử dụng “*next-hop-self*"

|  |
| --- |
| B (config) #router bgp 65000  B (config-router) #neighbor 172.20.10.2 remote-as 65000  B (config-router) #neighbor 172.20.10.2 next-hop-self  B (config-router) #exit |

Sau khi sử dụng tùy chọn này, router B khi quảng bá thông tin eBGP route vào cho các iBGP peer bên trong cùng AS sẽ không giữ địa chỉ next – hop là next – AS như trên nữa mà sẽ đổi thành địa chỉ IP của chính nó. Điều đó có nghĩa là, lần này router C sẽ nhận được cập nhật định tuyến cho mạng 172.16.0.0 với next – hop là địa chỉ 172.20.10.1 – một địa chỉ mà C có thể đi đến được, từ đó C có thể sử dụng được cập nhật định tuyến 172.16.0.0 mà nó vừa nhận được.

Thuộc tính next – hop là một thông số bắt buộc phải có trong mọi bản tin định tuyến cho mọi prefix được trao đổi giữa các router BGP.

**Origin**

Có nhiều cách để một router ban đầu quảng bá các IP Prefix vào mạng lưới BGP. Phương pháp được sử dụng là dùng câu lệnh “network” để tìm kiếm và quảng bá một IP Prefix có sẵn trước đó trong bảng định tuyến của router vào BGP.

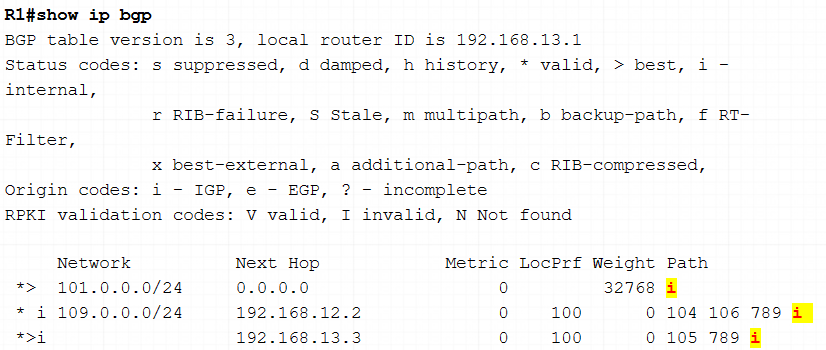
Bên cạnh phương pháp sử dụng lệnh “network”, một phương pháp khác cũng thường được sử dụng là thực hiện redistribute các route có sẵn trong bảng định tuyến của một phương thức IGP nào đó vào BGP Vi dụ, khi “redistribute ospf.”,router sẽ đem toàn bộ các route OSPF đã có trước đó quảng bá vào BGP; hay khi “redistribute eigrp.”, router sẽ đem các route EIGRP đã có trước đó quảng bá vào vào BGP. Một prefix khi được quảng bá và lan truyền trên mạng lưới BGP sẽ được đính kèm một mã hiệu cho biết nó được router gốc đưa vào BGP bằng phương pháp nào. Mã hiệu này được gọi là Origin code, và được coi là một thuộc tỉnh đường đi của BGP thuộc tỉnh Origin.

Có 3 Origin code có thể xuất hiện trong thuộc tỉnh Origin:

* ***“i” — “IGP”:*** Mã hiệu này cho biết prefix đang xét được router gốc quảng bá vào BGP bằng lệnh “network hoặc bằng thao tác summary địa chỉ.
* ***"e" – "EGE":*** Mã hiệu này cho biết prefix đang xét được router gốc quảng bá vào BGP bằng cách redistribute các route của một giao thức định tuyến ngoài khác là EGP. EGP (Exterior Gateway Protocol) là một giao thức định tuyến ngoài cũ, được sử dụng phổ biến trước khi BGP ra đời; ngày nay, BGP gần như là giao thức định tuyến ngoài duy nhất được sử dụng nên trừ phi người quản trị của router gốc có tinh thiết lập Origin code thành “c”, trong thực tế cũng sẽ ít gặp mã hiệu origin này trên các IP Prefix trong bảng BGP.
* ***“y” “Incomplete"***: Mã hiệu này cho biết IP prefix được router gốc đưa vào BGP bằng một phương pháp không xác định. Tuy nhiên, ngày nay, mã hiệu này thường được dùng để chỉ ra rằng các prefix được router gốc redistribute vào BGP từ một phương thức IGP nào đó.

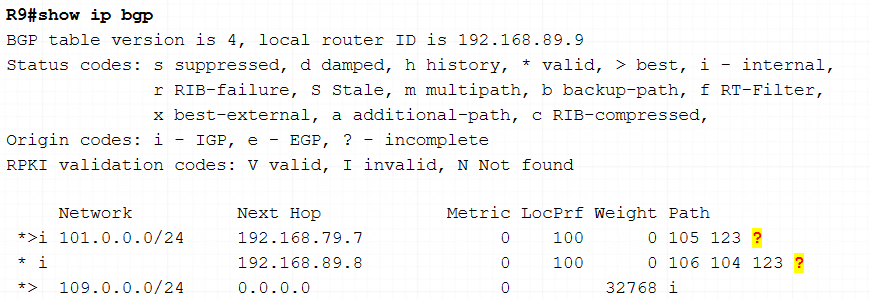
Xem xét một vài ví dụ về Origin code.

*Ví dụ 1:*



Trong kết quả hiển thị bảng BGP bằng lệnh “*show ip bgp*” của Cisco IOS, Origin code của một routing update được trình bày ở phía cuối của dòng thông tin. Với kết quả show ở trên, ta thấy các IP prefix mà R1 nhận được từ các neighbor đều có Origin code là “*i*”, điều này cho thấy các prefix này được router ban đầu đưa vào mạng lưới BGP bằng lệnh “*network*" hoặc bởi thao tác summary địa chỉ.

*Ví dụ 2*

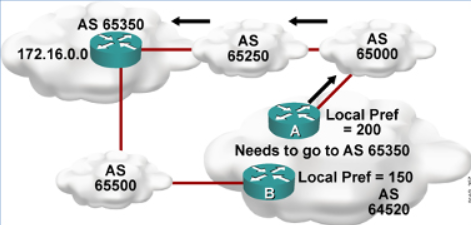


Trong kết quả show ở ví dụ thứ 2, ta thấy các Origin code của các route đi đến mạng 101.0.0.0/24 lại là “y”. Điều này cho thấy rằng mạng 101.0.0.0/24 đã được router gốc đưa vào BGP bằng cách redistribute prefi này từ một phương thức IGP nào đó.

Origin là một thuộc tính bắt buộc phải tồn tại trong mọi bản tin cập nhật cho mọi prefix BGP.

**Local Preference**

Cùng xem xét một ví dụ trong hình 4.



***Hình 4 – Ví dụ về Local Preference***

Trong ví dụ trên hình 4, mạng 172.16.0.0 được quảng bá ban đầu từ một router BGP trên AS 65350 và lan truyền qua mạng lưới BGP theo nhiều hướng để đi đến AS 64520. Ta thấy rằng AS 64520 có hai gateway là router A và router B cho phép đi ra khỏi AS này để đi đến mạng 172.16.0.0 củ AS 65350 mới đề cập ở trên.

Sau khi đã tìm hiểu về Tiến trình chọn đường BGP, ta có thể lý giải được rằng, nếu không thay đổi gì thêm, các router BGP bên trong AS 64520 (không thể hiện trên sơ đồ) sẽ chọn gateway B để chuyển đi tiếp dữ liệu muốn đi đến mạng 172.16.0.0 vì khi đi theo hướng này, dữ liệu sẽ phải trung chuyển qua it AS hơn. Tuy nhiên, có thể là do đường truyền của B nối đến AS 65500 đang quá tải nên người quản trị muốn dữ liệu xuất phát từ bên trong AS 64520 đi đến mạng 172.16.0.0 phải được chuyển tiếp theo gateway A để giảm tải bớt cho hướng gateway B. Để làm được điều này, người quản trị sẽ phải can thiệp vào một thuộc tính có độ ưu tiên cao hơn chiều dài của AS – path để lái dữ liệu theo ý mình, đó là thuộc tỉnh Local Preference.

Local Preference đơn giản là một số tự nhiên được BGP gán cho một hướng đi đến một prefix IP. Nguyên tắc một router BGP chọn đường dựa trên so sánh thuộc tính Local Prefence là: trong nhiều hướng đi đến cùng một đích đến, hướng đi nào có giá trị Local Preference đính kèm cao nhất, hướng đi đó được xem là tốt nhất và sẽ được chọn làm hướng đi chính thức đi đến đích đến đang xét. Hướng đi này sẽ được BGP cài vào bảng định tuyến để route dữ liệu đồng thời quảng bá đi cho router láng giềng kế tiếp.

Thuộc tính Local Preference chỉ có thể được quảng bá giữa các iBGP peer với nhau và sẽ bị gỡ bỏ khi prefix được quảng bá cho một eBGP peer khác. Người ta thường sử dụng Local Preference trên các router biên để định hướng cách các router BGP bên trong AS lái dữ liệu đi ra ngoài AS: router biên nào được ưu tiên làm gateway chính sẽ quảng bá route nhận được từ bên ngoài vào các iBGP router bên trong với giá trị Local Preference cao hơn, và router biên nào chỉ sử dụng làm gateway dự phòng sẽ quảng bá route nhận được từ bên ngoài vào các iBGP router bên trong với giá trị Local Preference thấp hơn.

Trở lại ví dụ đang xem xét ở trên.

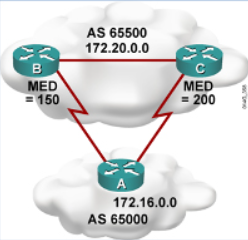
Vì người quản trị muốn rằng dữ liệu xuất phát từ bên trong AS 64520 đi đến mạng 172.16.0.0 cần phải đi ra ngoài bằng gateway A và gateway B chỉ để dự phòng, người quản trị sẽ thực hiện cấu hình để khi A nhận được mạng 172.16.0.0, nó sẽ thiết lập giá trị Local Preference là 200 cho prefix rồi mới quảng bá tiếp mạng này vào các router bên trong còn router B chỉ thiết lập Local Preference là 100 cho prefix khi quảng bá mạng nhận được vào các router bên trong. Kết quả là các router bên trong thấy rằng hướng đi đến mạng 172.16.0.0 thông qua gateway A có Local Preference cao hơn là qua gateway B sẽ ưu tiên chọn hướng Gateway A để route dữ liệu đi đến mạng 172.16.0.0, đáp ứng được yêu cầu đặt ra.

Nếu ta không cấu hình gì thêm, các iBGP peer sẽ gán giá trị Local Preference mặc định là 100 cho các prefix mà chúng quảng bá cho nhau.

**MED (Multi Exit Discriminator)**

Còn gọi là thuộc tỉnh Metric của BGP. cần phân biệt với khái niệm metric trong các IGP vì Metric (hay MED) với BGP chỉ là một thuộc tính trong số nhiều thuộc tính khác nhau được dùng để đánh giá độ tối ưu của một đường đi.

Ví dụ trên hình 5:



***Hình 5 – Ví dụ về thuộc tính MED***

Trong ví dụ trên, router A của AS 65000 thực hiện quảng bá mạng 172.16.0.0 cho các router B và C của AS 65500. Chính sách của AS 65000 (phía router A) muốn rằng AS láng giềng 65500 khi gửi dữ liệu đến mạng 172.16.0.0 cần đi vào AS 65000 theo đường link bên trái sơ đồ (đường link nối giữa A và B), còn đường link bên phải (nối giữa A và C) chỉ để dự phòng. Như vậy, trong trường hợp này. yêu cầu đặt ra là người quản trị của AS 65000 phải tác động như thế nào đó để ảnh hưởng đến quyết định chọn đường của AS láng giềng trong việc định tuyến dữ liệu đi đến mình, chứ không phải định hướng dữ liệu từ mình đi đến người ta. Một thuộc tính cũng thường được sử dụng trong tình huống này là thuộc tỉnh MED. MED cũng đơn giản chỉ là một số tự nhiên được gán cho một hướng đi nào đó. Nguyên tắc chọn đường dựa vào MED là: trong nhiều hướng đi đến cùng một đích đến, hướng đi nào có MED nhỏ nhất, hướng đi đó được xem là tốt nhất và sẽ được router chọn sử dụng làm hướng đi chính thức để đi đến đích đến này.

Mặc định, router BGP chỉ so sánh MED trên hai hướng đi có cùng neighbor AS và nếu không cấu hình gì thêm, MED sẽ mặc định được nhận giá trị là 0 với Cisco IOS.

Trở lại ví dụ trên, để thực hiện chính sách đã nêu, người quản trị của AS 65000 sẽ thực hiện thiết lập thuộc tỉnh MED cho mạng 172.16.0.0 là 150 khi quảng bá cho router B và là 200 khi quảng bá cho router C. Các router B và C tiếp tục lan truyền prefix này đến các router bên trong của AS láng giềng 65500. Các router bên trong của AS 65500 khi xem xét hai hướng đi đến mạng 172.16.0.0 thông qua hai Gateway B và C sẽ thấy rằng hướng đi qua B có MED nhỏ hơn MED của hướng đi qua C (150 < 200), nên sẽ chọn hướng qua B để lái dữ liệu đi đến 172.16.0.0. Ở phía AS 65000, khi các router bên AS 65500 láng giềng thực hiện định tuyến như vừa nêu, chính sách về định hướng dữ liệu “*đi vào*” để tới mạng 172.16.0.0 cầu người quản trị đã được thiết lập thành công.

Có thể thấy rằng MED có thứ tự ưu tiên không cao trong tiến trình này nên thiết lập MED để định hướng dữ liệu như ở trên có thể không thành công nếu AS láng giềng lại cố tình hiệu chỉnh một thuộc tỉnh có độ ưu tiên cao hơn để lái dữ liệu theo hướng ngược lại. Tuy nhiên, MED vẫn là một thuộc tỉnh thông dụng được sử dụng nhiều, đặc biệt trong việc ảnh hưởng đến quyết định chọn đường của một AS láng giềng.

**Weight**

Xem ví dụ về Weight ở hình 6:



***Hình 6 – Ví dụ về thuộc tính Weight***

Trong ví dụ ở trên, router A nhận được cập nhật định tuyến để đi đến mạng 172.20.0.0 của AS 65250 từ hai hướng là thông qua router B và router C. Với ví dụ này, người quản trị mong muốn rằng router A luôn luôn chọn hướng đi qua B để đi tới mạng 172.20.0.0, hướng qua C chỉ để dự phòng bất kể các thuộc tính trên hai hướng đi này như thế nào. Để thực hiện yêu cầu đặt ra, thuộc tỉnh Weight có thể được sử dụng. Weight là thuộc tỉnh có độ ưu tiên cao nhất trong Tiến trình chọn đường BGP Weight cũng là một số tự nhiên được gán cho một hướng đi để đến một IP prefix. Trong nhiều đường đi khác nhau cùng đi đến một đích đến, đường đi nào có Weight cao nhất, đường đi đó được xem là tốt nhất, bất kể các thuộc tính khác có giá trị như thế nào.

Weight là thuộc tính chỉ có tác dụng trong nội bộ của một router, và không được quảng bá kèm theo các prefix sang các BGP peer khác. Một đặc điểm khác đáng chú ý, Weight là thuộc tỉnh BGP do Cisco đưa ra và chỉ xuất hiện trên các thiết bị của Cisco, các phiên bản BGP của các hãng khác không có thuộc tính này.

Mặc định, một router BGP sẽ gán giá trị Weight = 0 cho mọi prefix nhận được từ các router khác và gần Weight = 32768 cho các prefix do tự nó đưa vào BGP (thường được gọi là các local route).

Với ví dụ đang xem xét, để thực hiện yêu cầu của người quản trị, router A sẽ gán giá trị Weight = 200 cho prefix 172.20.0.0 khi nhận prefix này từ router B và gán Weight = 150 cho cùng prefix ấy khi nhận từ router C từ đó, router A sẽ luôn chọn hướng B để đi đến 172.20.0.0 và hướng C chỉ để dự phòng.  
**Weight, Local Preference, Local route và AS – Path Length**

Trước hết, nhắc lại rằng khi một router peering thành công với nhiều router khác, nó sẽ được các router neighbor này quảng bá cho nó các route tốt nhất mà chúng đã tính được. Router đang xét sẽ tập trung các route nhận được vào bảng BGP rồi chạy Tiến trình chọn đường BGP trên các route này. Tiến trình chọn đường BGP sẽ lọc ra từ nhiều route đi đến cùng một đích đến một route tốt nhất sau đó đưa route tốt nhất này vào bảng định tuyến sử dụng chính thức, đồng thời quảng bá route ấy đến router neighbor kế tiếp. Mặc định, Tiến trình chọn đường BGP không hỗ trợ đa đường mà chỉ chọn ra một và chỉ một đường đi tối ưu cho từng mạng đích. Điều này có nghĩa là, nếu không cấu hình gì thêm, BGP không hỗ trợ cân bằng tải.

*Pre – check thông tin định tuyến*

Trước khi một route được đưa vào xem xét trong Tiến trình chọn đường BGP, route phải được kiểm tra trước (pre – check) xem có thỏa mãn hai điều kiện sau đây hay không, nếu một trong hai điều kiện không được thỏa mãn, route sẽ không được xem xét trong tiến trình chọn đường:

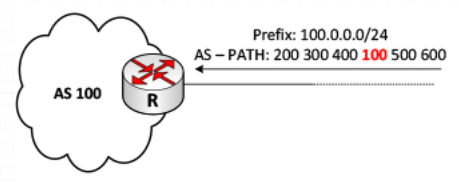
***1. Next – hop phải đi đến được:***

Mỗi route trong bảng BGP sẽ được kiểm tra xem là địa chỉ next – hop của route có thể đi đến được không. Nếu next – hop IP không thể đi đến được, route này sẽ bị loại ra khỏi hoạt động xem xét đánh giá của tiến trình chọn đường BGP.

***2. Thỏa mãn điều kiện chống loop***

Khi router BGP nhận được routing update cho một IP prefix, nó sẽ kiểm tra thuộc tỉnh AS – Path của prefix này. Nếu trong AS – Path của prefix có chứa AS Number của router đang xét, router sẽ bỏ qua không cập nhật route này vào bảng BGP, và vì vậy route sẽ không có cơ hội để tham gia vào Tiến trình chọn đường BGP. Đây là điều kiện chống loop nổi tiếng của giao thức BGP.

Để nắm được ý vừa nêu, cùng xem xét một ví dụ (hình 7):



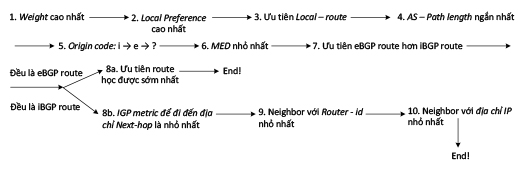
***Hình 7 – Ví dụ về điều kiện chống loop của BGP***

Trên hình 7, router R thuộc AS 100 nhận được cập nhật định tuyến cho mạng 100.0.0.0/24. Khi kiểm tra thuộc tỉnh AS – Path của prefix này, router R nhận thấy AS – Path của route có chứa ASN 100 chính là số AS của nó, khi đó, router R sẽ loại bỏ không cập nhật prefix này vào bảng BGP.

Thuộc tính AS – Path ghi lại số hiệu của các AS mà prefix đã lan truyền qua để có thể đến được router đang xét. Khi router đang xét thấy xuất hiện số AS của nó trong AS – Path của prefix nhận được, điều đó chứng tỏ prefix đã từng đi qua AS của nó rồi sau đó vòng trở lại; như vậy, loop đã xảy ra cho prefix này, router cần từ chối nhận prefix để tránh gây ra loop cho định tuyến dữ liệu.

*Tiến trình chọn đường BGP*

Tất cả các route đi đến các mạng đích sau khi trải qua hai thao tác kiểm tra ở trên và vượt qua, sẽ được tham gia Tiến trình chọn đường BGP để chọn ra từ những route này các route tốt nhất đi đến từng mạng đích. Tiến trình chọn đường BGP được mô tả như trên hình 8:



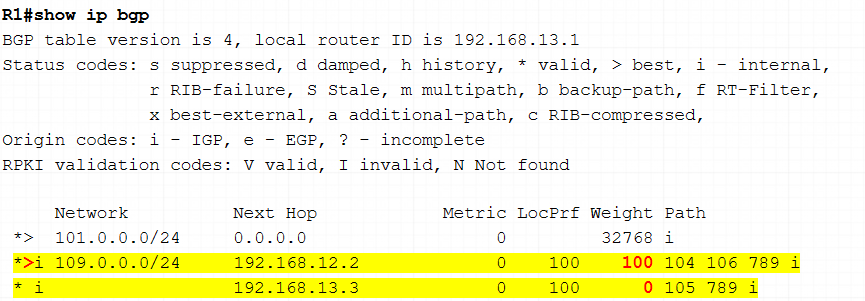
***Hình 8 – Tiến trình chọn đường BGP***

Như trình bày trên hình, tiến trình này gồm nhiều bước khác nhau xem xét so sánh các thuộc tính khác nhau giữa các route đi đến cùng một đích đến để tìm ra route tối ưu cho đích đến ấy. Nguyên tắc của việc so sánh này là khi tại một bước nào đó mà đã xác định được route tốt nhất, các bước còn lại sau đó sẽ bị bỏ qua không xem xét tiếp nữa; bước sau chỉ được xem xét nếu như bước trước đó vẫn không “phân định thắng bại” được giữa các route. Một nguyên tắc khác nữa của tiến trình chọn đường BGP là tiến trình này mặc định không hỗ trợ cân bằng tải: chỉ một route tối ưu cho mỗi đích đến được lựa chọn, tiến trình sẽ tiến hành so sánh cho đến khi tìm được một và chỉ một route tối ưu cho mỗi đích đến mà thôi.

***1. Weight cao nhất***

Thuộc tính đầu tiên được router xem xét để chọn đường tốt nhất là thuộc tỉnh Weight. Trong nhiều đường đi đến cùng một đích đến, đường đi nào có Weight cao nhất, đường đi đó sẽ được chọn làm đường đi tối ưu, được cài vào bảng định tuyến sử dụng chính thức, đồng thời quảng bá đi các router láng giềng kế tiếp.

*Ví dụ:*



Xem xét các đường đi đến mạng 109.0.0.0/24 trong bảng BGP của router R1. Ta thấy rằng hiện R1 học được hai đường đi để đi đến mạng này, một đường thông qua next – hop 192.168.12.2 và một đường thông qua next – hop 192.168.13.3. Khi so sánh các thuộc tỉnh, BGP trên R1 đã chọn đường đi qua next – hop 192.168.12.2 vì đường đi này có Weight cao hơn đường còn lại (100 so với 0).

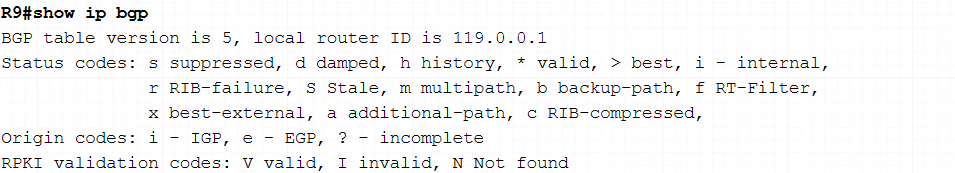
(Trong kết quả hiển thị bảng BGP với Cisco IOS, hướng đi tốt nhất là hướng đi được đánh dấu ">" ở đầu dòng thông tin)

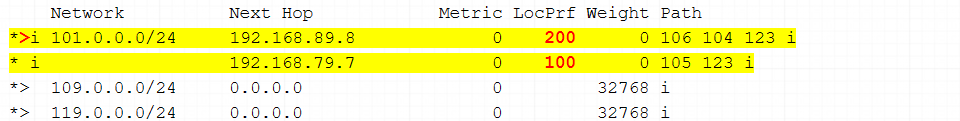
Khi làm việc với các thiết bị của Cisco, thuộc tính Weight là thuộc tính có độ ưu tiên cao nhất trong Tiến trình chọn đường BGP. Mặc định, một router BGP sẽ gán giá trị Weight = 32768 cho các local route (là các route do router tự quảng bá vào BGP) và gán trị Weight = 0 cho các route mà router nhận được từ các BGP neighbor khác.

***2. Local Preference cao nhất***

Khi các route được đem đi so sánh đều có giá trị Weight bằng nhau, bước thứ nhất của tiến trình không chọn ra được route tốt nhất, Local Preference là thông số tiếp theo sẽ được đưa ra so sánh. Trong nhiều đường đi đến cùng một đích đến, đường đi nào có Local Preference lớn nhất, đường đi đó được xem là tốt nhất.

*Ví dụ:*





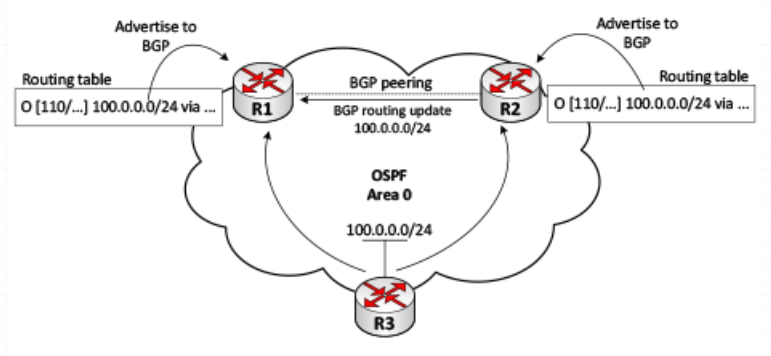
Trong kết quả show của router R9 ở trên, R9 nhận được hai đường đi để đi đến mạng 101.0.0.0/24: một đường thông qua next – hop 192.168.89.8 và một đường thông qua next – hop 192.168.79.7. Ta thấy rằng cả hai đường đi này đều có Weight bằng nhau và bằng 0 nên Local Preference được đưa ra để so sánh. Kết quả là vì đường đi thông qua next – hop 192.168.89.8 có giá trị Local Preference cao hơn nên đường đi này được chọn là đường đi tối ưu và được sử dụng chính thức làm đường đi đến mạng 101.0.0.0/24.

Nhắc lại rằng thuộc tính Local Preference chỉ lan truyền giữa các iBGP peer với nhau và thường được cấu hình hiệu chỉnh trên các router biên để định hướng cách thức các router BGP bên trong một AS lái dữ liệu ra khỏi AS ấy để đi ra bên ngoài. Mặc định, giá trị Local Preference được thiết lập là 100 cho các IP prefix trong các bản tin định tuyến BGP

***3. Ưu tiên local route***

Bước thứ 3 được xem xét sau bước thứ 2 so sánh về Local Preference là ưu tiên Local route hơn các loại route khác. Nếu tồn tại nhiều đường đi đến cùng một đích đến có các giá trị Weight và Local Preference đều bằng nhau, router sẽ ưu tiên chọn đường đi do chính nó quảng bá vào BGP hơn so với các đường đi nhận được từ các router neighbor khác.

Ta cùng xem xét một ví dụ để làm rõ ý vừa nêu (hình 3):



***Hình 9 – Ví dụ về ưu tiên Local route***

Trong ví dụ trên hình 3, cả hai router R1 và R2 đều nhận được route cho đích đến 100.0.0.0/24 từ R3 thông qua OSPF. Vì route 100.0.0.0/24 đã xuất hiện trong bảng định tuyến của hai router nên cả hai router này đều có thể quảng bá mạng này vào BGP. Vì R1 và R2 cũng thực hiện peering BGP với nhau nên chúng cũng sẽ quảng bá tiếp mạng 100.0.0.0/24 đến nhau.

Xét router R1, router này hiện có hai hướng đi để đi đến mạng 100.0.0.0/24 trong bảng BGP của nó: một hướng thông qua chính nó vì R1 là router quảng bá 100.0.0.0/24 vào BGP (ta gọi là local route), một hướng khác thông qua R2 vì R2 cũng thực hiện quảng bá mạng 100.0.0.0/24 qua cho R1. Như đã nêu ở trên, R1 sẽ ưu tiên hướng đi đến mạng 100.0.0.0/24 thông qua chính nó và coi hướng này là hướng tốt hơn hướng phải đi thông qua láng giềng R2. Ta gọi điều này là ưu tiên local route.

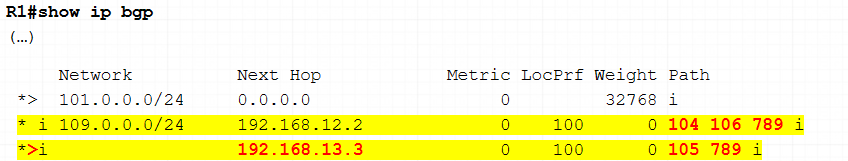
Quyết định chọn đường trên R2 để đi đến mạng 100.0.0.0/24 cũng diễn ra tương tự.

Với Cisco router, bước thứ 3 này có thể hiếm khi được xem xét. Thật vậy, như đã trình bày trong bước thứ nhất về so sánh Weight ở trên: mặc định các local route được gán Weight = 32768 và các route khác được gán Weight = 0. Do đó, ngay từ bước đầu tiên, các local route đã được ưu tiên hơn rồi, bước thứ 3 sẽ không được xem xét đến nữa. Tuy nhiên, nếu làm việc với các sản phẩm non – Cisco, bước thứ 3 là một bước quan trọng mà ta phải lưu ý.

***4. AS – Path length ngắn nhất***

Nếu tất cả các route đều không phải local route để có thể được xem xét bởi bước thứ 3 ở trên, Tiến trình chọn đường BGP sẽ xem xét đến thuộc tỉnh AS – Path của các route nhằm xác định ra route tốt nhất. Trong nhiều đường đi đến cùng một đích đến, đường đi nào có thuộc tỉnh AS – Path có chiều dài ngắn nhất, đường đi đó được xem là đường đi tối ưu cho đích đến này. Điều này có nghĩa là đường đi nào phải đi qua ít AS nhất để đến được đích đến, đường đó là tối ưu. Tất nhiên, các thông số Weight, Local Preference cần phải được xem xét trước đó và các giá trị này đều bằng nhau giữa các route khiến cho BGP chưa chọn được đường tốt nhất.

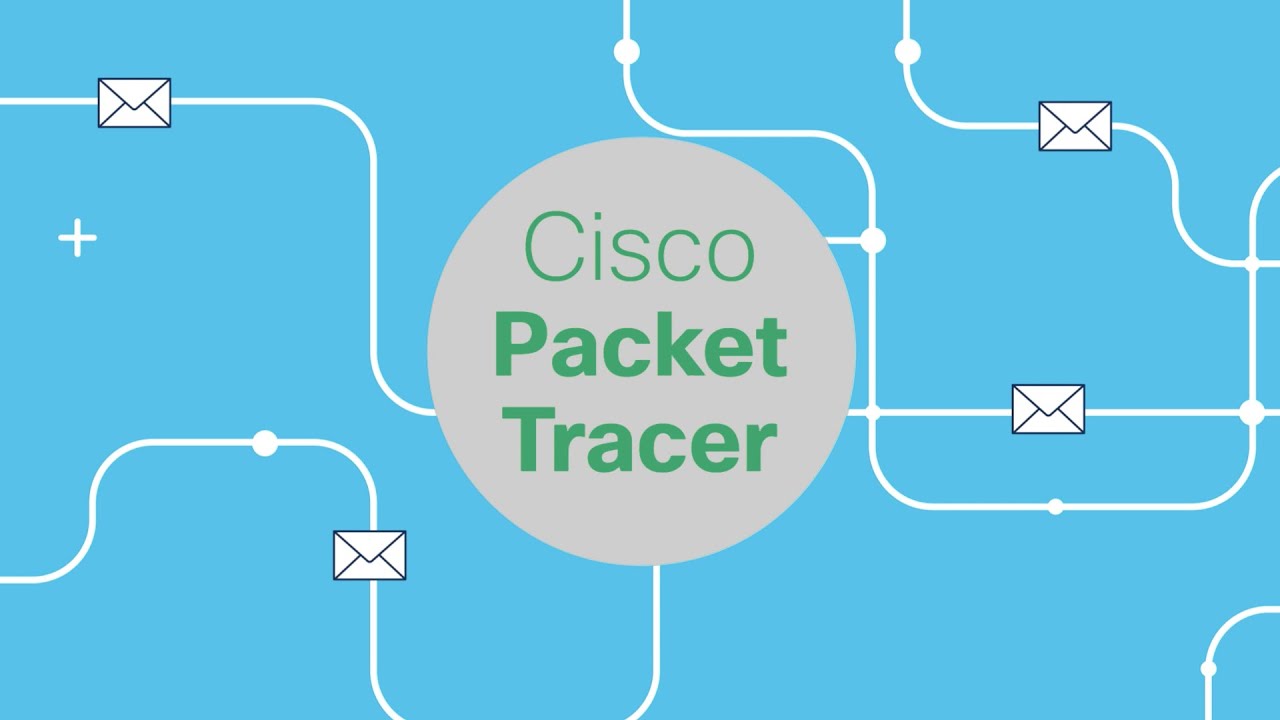
Ví dụ về việc chọn đường dựa trên AS – Path length:



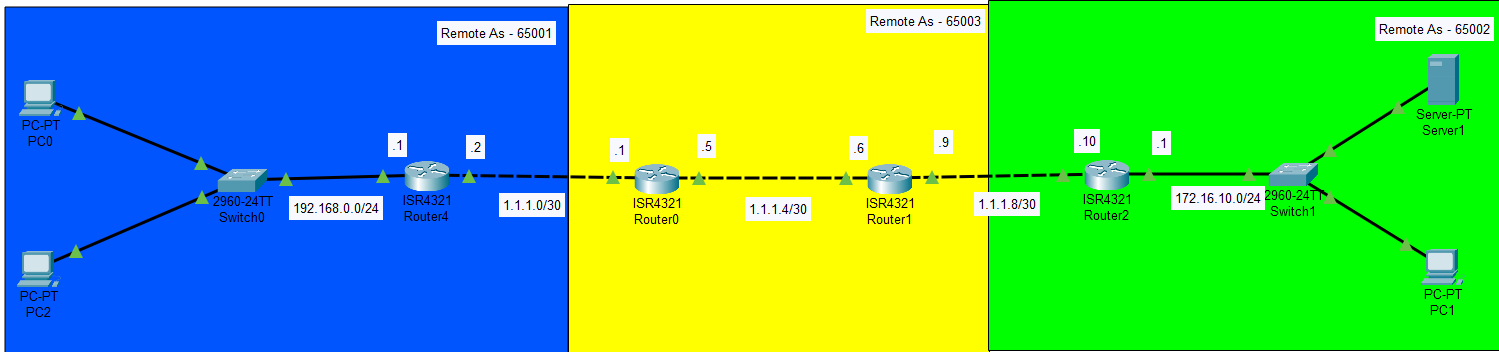
Trong kết quả show ở trên, router R1 có hai đường đi để đi đến mạng 109.0.0.0/24: một đường thông qua next – hop 192.168.12.2 và một đường thông qua next – hop 192.168.13.3. Cả hai đường này đều có các giá trị Weight, Local Preference bằng nhau và đều không phải là local route nên ba bước đầu tiên của Tiến trình chọn đường BGP chưa “phân định được thắng bại” giữa hai route này. Khi sử dụng bước thứ 4 là so sánh chiều dài AS – Path để chọn đường tối ưu, router R1 đã chọn đường đi qua next – hop 192.168.13.3 để đi đến mạng 109.0.0.0/24 vì đường đi này có AS – Path với chiều dài ngắn hơn (chỉ đi qua 2 AS là 105 và 789, so với đường còn lại phải đi qua 3 AS là 104, 106 và 789).

# **Chương 3: Triển khai giao thức BGP trên phần mềm giả lập**

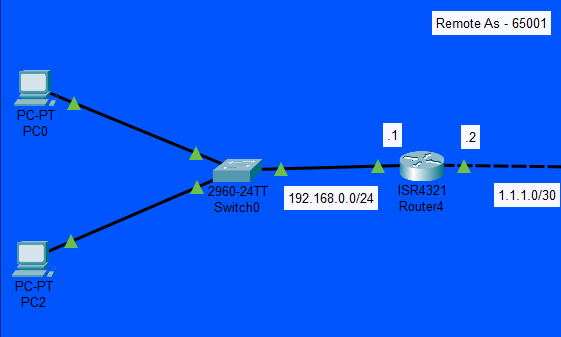
*Cisco Packet Tracer*



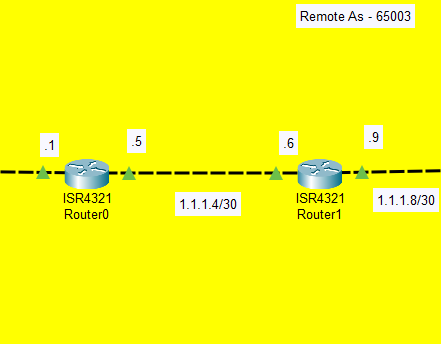
*Mô hình*

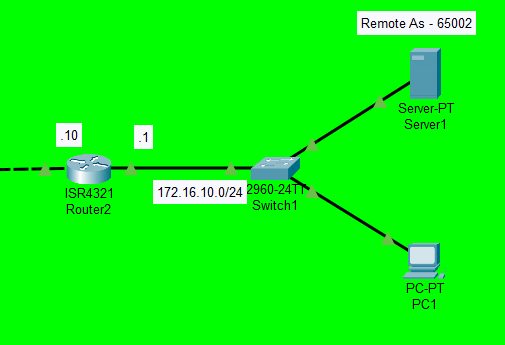


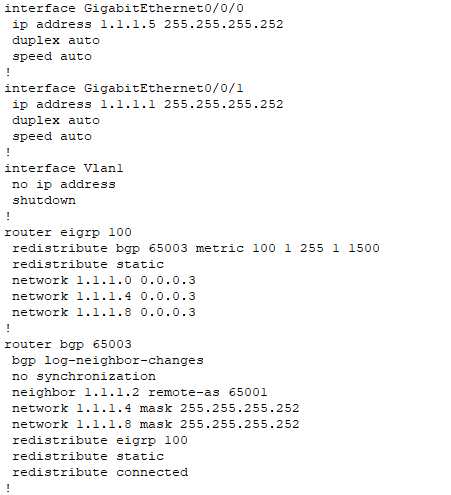
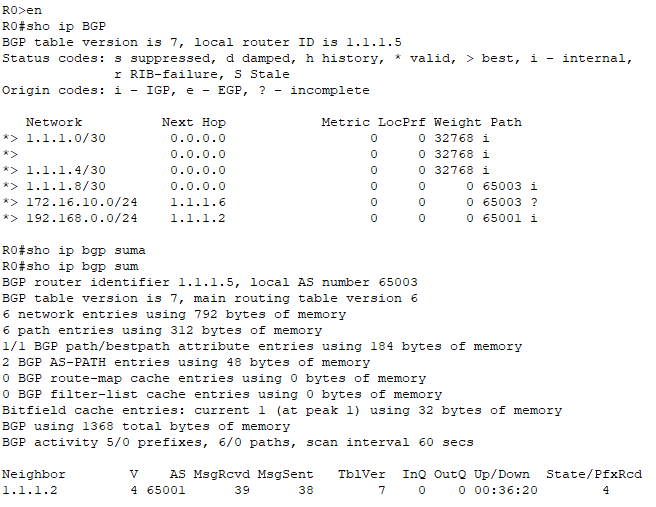
*Remote AS – 65001*



*Remote AS – 65003*



*Remote AS - 65002*

**Cấu hình của các router:**  
  


# **Chương 4: Kết luận và hướng phát triển của đề tài**

* 1. ***Kết luận***

Trong chương này, chúng ta đã xem xét về định tuyến BGP và vai trò quan trọng của nó trong mạng lưới ISP. BGP không chỉ có khả năng tích hợp giữa các AS khác nhau mà còn giúp kiểm soát lưu lượng mạng một cách hiệu quả, đặc biệt là trong các mạng lớn và phức tạp. Tuy nhiên, BGP cũng có nhược điểm, bao gồm vấn đề liên quan đến khả năng chịu lỗi của mạng và yêu cầu kỹ năng và kinh nghiệm để cấu hình và quản lý một mạng sử dụng BGP.

Qua nghiên cứu và phân tích, chúng ta nhận thấy rằng định tuyến BGP là một công nghệ quan trọng trong việc xây dựng và quản lý các mạng lớn và phức tạp. Để sử dụng BGP một cách hiệu quả, người quản trị mạng cần có đủ kỹ năng và kinh nghiệm để cấu hình và quản lý mạng của mình. Ngoài ra, việc nắm vững các nguyên tắc và phương pháp thiết lập và duy trì kết nối BGP cũng là yếu tố quan trọng trong việc đảm bảo sự ổn định và an toàn của mạng lưới.

* 1. ***Hướng phát triển***

Dựa trên nghiên cứu và kết quả đạt được trong đề tài, chúng ta nhận thấy rằng còn nhiều khía cạnh và phạm vi để phát triển và nghiên cứu thêm về định tuyến BGP. Dưới đây là một số hướng phát triển tiềm năng cho đề tài này:

* + 1. ***Mở rộng đối tượng nghiên cứu***

Trong đề tài này, chúng ta đã tập trung vào việc nghiên cứu và phân tích về định tuyến BGP trong mạng lưới ISP. Tuy nhiên, có thể mở rộng phạm vi nghiên cứu để xem xét ứng dụng của BGP trong các lĩnh vực khác như mạng doanh nghiệp, mạng truyền thông, hoặc mạng không dây. Việc tìm hiểu sâu hơn về việc triển khai BGP trong các môi trường mạng khác nhau sẽ giúp chúng ta hiểu rõ hơn về các thách thức và lợi ích của BGP trong các ngữ cảnh khác nhau.

* + 1. ***Nghiên cứu về bảo mật và an ninh BGP***

Một vấn đề quan trọng liên quan đến định tuyến BGP là bảo mật và an ninh. BGP đã trở thành một mục tiêu phổ biến cho các cuộc tấn công mạng và các hình thức tấn công như hijacking, spoofing, hoặc các cuộc tấn công Man-in-the-Middle có thể gây ra hậu quả nghiêm trọng cho mạng lưới. Do đó, nghiên cứu về các biện pháp bảo mật và công nghệ an ninh mới để ngăn chặn các cuộc tấn công này và đảm bảo tính bảo mật của định tuyến BGP là rất cần thiết.

* + 1. ***Xây dựng mô hình mô phỏng và kiểm tra***

Để nghiên cứu và kiểm tra các kịch bản định tuyến và cấu hình BGP một cách an toàn và hiệu quả, việc xây dựng các mô hình mô phỏng và kiểm tra là cần thiết. Các mô hình mô phỏng giúp chúng ta tái hiện môi trường mạng thực tế và thử nghiệm các cấu hình và kịch bản BGP khác nhau mà không ảnh hưởng đến mạng lưới thực tế. Điều này cung cấp cho chúng ta một phương pháp an toàn và tiết kiệm thời gian để tìm hiểu và thử nghiệm các tùy chọn định tuyến và cấu hình mới trước khi triển khai trên mạng lưới thực tế.

* + 1. ***Nghiên cứu về phát hiện và xử lý sự cố về BGP***

Trong mạng lưới thực tế, sự cố BGP có thể xảy ra do nhiều nguyên nhân, bao gồm lỗi cấu hình, sự cố phần cứng, hoặc các cuộc tấn công. Do đó, nghiên cứu và phát triển các phương pháp phát hiện và giải quyết sự cố BGP là một hướng phát triển tiềm năng. Các phương pháp này có thể giúp xác định và khắc phục sự cố BGP một cách nhanh chóng và đảm bảo tính liên tục của mạng lưới.

* + 1. ***Đánh giá và tối ưu hóa hiệu suất BGP***

Một khía cạnh quan trọng trong việc triển khai định tuyến BGP là đánh giá hiệu suất mạng và tối ưu hóa định tuyến. Việc đánh giá hiệu suất mạng BGP đòi hỏi khả năng đo lường các yếu tố như thời gian phản hồi, băng thông sử dụng, và tải trọng mạng. Bằng cách thu thập và phân tích dữ liệu hiệu suất mạng, chúng ta có thể xác định các vấn đề hiệu suất và áp dụng các biện pháp tối ưu hóa để cải thiện hiệu suất mạng và sử dụng tài nguyên mạng hiệu quả hơn.

* + 1. ***Tích hợp định tuyến BGP với các công nghệ mới***

Các công nghệ mới như mạng điện toán đám mây, mạng ảo hóa và IoT đang ngày càng được áp dụng rộng rãi. Để đáp ứng yêu cầu của các mô hình mạng mới này, nghiên cứu về việc tích hợp định tuyến BGP với các công nghệ mới là cần thiết. Ví dụ, việc khám phá cách thức định tuyến BGP trong môi trường đám mây, quản lý lưu lượng mạng trong mạng ảo hóa hoặc xử lý định tuyến trong mạng IoT sẽ đóng góp vào việc phát triển và mở rộng sử dụng định tuyến BGP trong các tình huống mạng mới và phức tạp.

* + 1. ***Định tuyến trong mạng không dây và mạng di động***

Mạng không dây và mạng di động đang trở nên ngày càng phổ biến và phức tạp. Việc nghiên cứu về việc triển khai BGP trong mạng không dây và mạng di động sẽ đóng vai trò quan trọng trong việc xây dựng và quản lý các hạ tầng mạng không dây và di động. Định tuyến BGP có thể được áp dụng để quản lý các mạng không dây phân tán, đảm bảo độ tin cậy và khả năng mở rộng của mạng di động, và cung cấp khả năng di động liên mạng.

* 1. ***Tổng kết***

Trên cơ sở nghiên cứu và phân tích định tuyến BGP, chúng ta đã nhận thấy vai trò quan trọng của nó trong mạng lưới ISP và các mạng lớn và phức tạp khác. Tuy nhiên, định tuyến BGP cũng mang theo những thách thức và yêu cầu đối với người quản trị mạng. Qua việc đề cập đến các hướng phát triển tiềm năng, chúng ta hy vọng rằng các nghiên cứu trong tương lai sẽ tiếp tục khám phá và cải thiện định tuyến BGP, đảm bảo tính ổn định và an toàn của mạng lưới, và đáp ứng các yêu cầu ngày càng phức tạp của mạng lưới hiện đại.

Tóm lại, đề tài đã trình bày về định tuyến BGP và vai trò quan trọng của nó trong mạng lưới ISP. Để phát triển thêm đề tài này, có thể mở rộng phạm vi nghiên cứu, tập trung vào bảo mật và an ninh BGP, xây dựng mô hình mô phỏng và kiểm tra, và nghiên cứu về phát hiện và giải quyết sự cố BGP. Những hướng phát triển này sẽ đóng góp vào việc hiểu sâu hơn về định tuyến BGP và cung cấp các giải pháp và công nghệ mới cho việc quản lý và vận hành mạng lưới ISP một cách hiệu quả.

**[[1]](#endnote-1)**

# **TÀI LIỆU THAM KHẢO**

**[1]**

[**https://www.ciscopress.com/store/border-gateway-protocol-bgp-livelessons-downloadable-9781587144899**](https://www.ciscopress.com/store/border-gateway-protocol-bgp-livelessons-downloadable-9781587144899)

**[2]**

[**https://docs.google.com/presentation/d/1xr4szqvAajMrbh1k8\_29iuFAVzD0hB-W/edit#slide=id.p1**](https://docs.google.com/presentation/d/1xr4szqvAajMrbh1k8_29iuFAVzD0hB-W/edit#slide=id.p1)

**[3]**

[**https://docs.google.com/presentation/d/1GxpaDYHIpYZ6lP3Efx6-YXWGJrEmJGSf/edit#slide=id.p1**](https://docs.google.com/presentation/d/1GxpaDYHIpYZ6lP3Efx6-YXWGJrEmJGSf/edit#slide=id.p1)

1. [↑](#endnote-ref-1)