Volume 5, Issue 11, November 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Efficient and Robust Resource Allocation in Resilient Overlay Routing Relay Node Networks using BGP Routing

D. Suguna Kuamari, Bala Veeravatnam, P. Sowmya
Department of Computer Science & Engineering in Gokaraju Rangaraju Institute of Engineering and Technology, RR Dist, Telengana, India

Abstract: Overlay routing is an efficient way to certain routing properties without long and tedious process of standardization and global deployment of a new routing protocol. Deploying overlay routing requires the placement and maintenance of overlay infrastructure rise to the optimization problem. An algorithmic framework can be efficient resource allocation in overlay routing. The actual benefit can gain from schemes namely BGP Routing, TCP Improvement and VOIP Applications. IP routing protocols compute paths based on the network topology and configuration parameters, without regard to the current traffic load on the routers and links. The responsibility for adapting the paths to the prevailing traffic falls to the network operators and management systems. We consider the problem of optimizing the inter domain routing policies that control the flow of traffic from one network to another. Optimization based on local search has proven quite effective in grappling with the complexity of the routing protocols and the diversity of the performance objectives, and tools based on local search are in wide use in today's large IP networks. A BGP Routing is up-to-date data reflecting the current BGP routing policy in internet, a small number of less than 100 relay servers is sufficient to enable routing over shortest paths from a single source to all autonomous systems(Ass), reducing the average path length of inflated paths by 40%. TCP Performance improvement is an optimal placement of overlay nodes and Voice-over-IP (VOIP) applications is a small number of overly nodes can reduce the maximal peer-to-peer delay. Optimization based on local search has proven quite effective in grappling with the complexity of the routing protocols and the diversity of the performance objectives, and tools based on local search are in wide use in today's large IP networks.

Key Terms: BGP Routing, Resilient Overlay Network (RON), Autonomous Systems (Ass).

I. INTRODUCTION

The Border Gateway Protocol (BGP) is an inter-autonomous system routing protocol. As discussed in an autonomous system (AS) is a network or group of networks under a common administration and with common routing policies. BGP is used to exchange routing information for the Internet and is the protocol used between Internet service providers (ISP), which are different ASes. One of the most important characteristics of BGP is its flexibility. The protocol can connect together any internetwork of autonomous systems using an arbitrary topology. The only requirement is that each AS have at least one router that is able to run BGP and that this router connect to at least one other AS's BGP router. Beyond that, "the sky's the limit," as they say. BGP can handle a set of ASs connected in a full mesh topology (each AS to each other AS), a partial mesh, a chain of linked one to the next, or any other configuration. It also handles changes to topology that may occur over time. The primary function of a BGP speaking system is to exchange network reach ability information with other BGP systems. This network reach ability information includes information on the list of Autonomous Systems (ASs) that reach ability information traverses. BGP constructs a graph of autonomous systems based on the information exchanged between BGP routers. As far as BGP is concerned, whole Internet is a graph of ASs, with each AS identified by a Unique AS number. Connections between two ASs together form a path and the collection of path information forms a route to reach a specific destination. BGP uses the path information to ensure the loop-free inter domain routing.

BGP is different from other routing protocols in several ways. Most important being that BGP is neither a pure distance vector protocol nor a pure link state protocol. Let's have a look at some of the characteristics that stands BGP apart from other protocols.

Inter-Autonomous System Configuration:

BGP's primary role is to provide communication between two autonomous systems.

Next-Hop paradigm:

Like RIP, BGP supplies next hop information for each destination.

Coordination among multiple BGP speakers within the autonomous system:

If an Autonomous system has multiple routers each communicating with a peer in other autonomous system, BGP can be used to coordinate among these routers, in order to ensure that they all propagate consistent information.

Path information:

BGP advertisements also include path information, along with the reachable destination and next destination pair, which allows a receiver to learn a series of autonomous system along the path to the destination.

Policy support:

Unlike most of the distance-vector based routing, BGP can implement policies that can be configured by the administrator. For Example, a router running BGP can be configured to distinguish between the routes that are known from within the Autonomous system and that which are known from outside the autonomous system.

Runs over TCP:

BGP uses TCP for all communication. So the reliability issues are taken care by TCP.

Conserve network bandwidth:

BGP doesn't pass full information in each update message. Instead full information is just passed on once and thereafter successive messages only carries the incremental changes called deltas. By doing so a lot of network Bandwidth is saved. BGP also conserves bandwidth by allowing sender to aggregate route information and send single entry to represent multiple, related destinations.

Support for CIDR:

BGP supports classless addressing(CIDR).That it supports a way to send the network mask along with the addresses.

Security:

BGP allows a receiver to authenticate messages, so that the identity of the sender can be verified.

II. SYSTEM ANALYSIS

Existing System:

Overlay Routing is to improve routing and network performance an order to evaluate and improving the network. A resilient overlay network (RON), is an application – layer overlay routing to be used on top of the existing routing infrastructure. The architecture is to replace the existing routing scheme. The work mainly focuses on the overlay infrastructure (monitoring and detecting routing problems and maintaining the overlay systems and the cost associated with the deployment of system.

Proposed System:

The minimum number of infrastructure nodes can be added to maintain a overlay routing .The shortest path routing over the Internet, BGP- based routing: to make the routing between a group of autonomous systems (ASs) use the underlying shortest path between them. The TCP performance under each TCP connection, there is a path between the connection end points for every predefined round trio time (RTT), there is an overlay node capable of TCP Piping. General optimization problem called the Overlay Routing Resource Allocation ORRA) problem and study its complexity. It turns out the problem is a nontrivial approximation algorithm.

BGP Attributes:

BGP Attributes are the properties associated with the routes that are learned from BGP and used to determine the best route to a destination, when multiple routes are available. An understanding of how BGP attributes influence route selection is required for the design of robust networks. This section describes the attributes that BGP uses in the route selection process:

- AS_path
- Next hop
- Weight

AS_path Attribute:

When a route advertisement passes through an autonomous system, the AS number is added to an ordered list of AS numbers that the route advertisement has traversed.

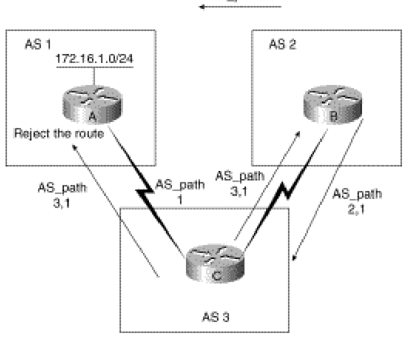

Fig: BGP Next-Hop Attribute

Next-Hop Attribute:

The EBGP next-hop attribute is the IP address that is used to reach the advertising router. For EBGP peers, the next-hop address is the IP address of the connection between the peers.

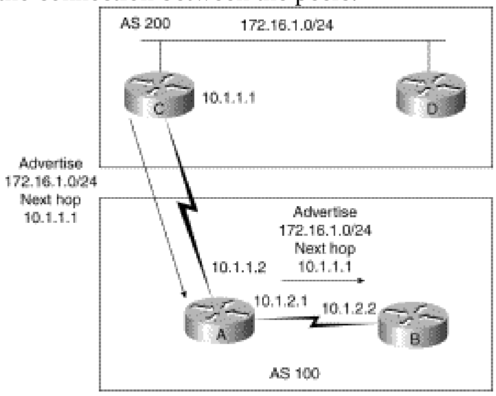

Fig: BGP Next-Hop Attribute

Weight Attribute:

Weight is a Cisco-defined attribute that is local to a router. The weight attribute is not advertised to neighbouring routers. If the router learns about more than one route to the same destination, the route with the highest weight will be preferred. Router A is receiving an advertisement for network 201.12.23.0 from routers B and C. When Router A receives the advertisement from Router B, the associated weight is set to 50. When Router A receives the advertisement from Router C, the associated weight is set to 100. Both paths for network 201.12.23.0 will be in the BGP routing table, with their respective weights. The route with the highest weight will be installed in the IP routing table.

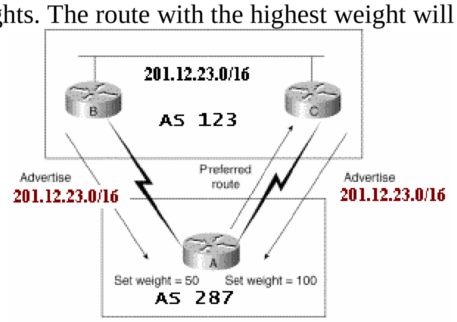

Fig: BGP Weight Attribute

III. IMPLEMENTATION

BGP Management Functions:

The overall activity of route information management can be considered to encompass four main tasks:

Route Storage:

Each BGP stores information about how to reach networks in a set of special databases. It also uses databases to hold routing information received from other devices.

Route Update: When a BGP device receives an Update from one of its peers, it must decide how to use this information. Special techniques are applied to determine when and how to use the information received from peers to properly update the device's knowledge of routes.

Route Selection:

Each BGP uses the information in its route databases to select good routes to each network on the internetwork.

Route Advertisement:

Each BGP speaker regularly tells its peers what it knows about various networks and methods to reach them. This is called route advertisement and is accomplished using BGP Update messages.

Inter domain Routing Policies:

The flow of traffic through a transit network depends on the BGP routes advertised by neighbouring ASes, as well as the local policies configured on the individual routers. We consider how tuning the BGP policies influence the forwarding of data traffic. Next, we describe how to extend the routing model from the previous section to capture the role of routing policies. Then, we discuss approaches to exploring the very large search space of BGP policy configurations, as well as fundamental limitations on the ability of models to predict the load on the links in an AS.

BGP Policies Influencing the Path-Selection Process:

The routers in an AS select BGP routes with the shortest AS path, breaking ties based on the proximity of the egress points. More generally, a router can be configured to apply a policy that assigns a local preference to a route, to select one route over another with a shorter AS path or closer Egress point. Today's routers provide an extremely flexible programming language. For specifying rules for assigning the local-preference attribute. In transit networks, the common practice is to assign a higher preference to BGP routes learned from customers than to routes learned from upstream providers, to ensure that data traffic traverses neighbours that are paying customers, even if the path through the provider is shorter.

In addition to assigning preferences based on the relationship with the neighbouring AS, operators configure policies to influence the load on the network links. For example, suppose an AS learns BGP routes to a destination from two upstream providers. By assigning a lower local preference to one route, the AS decides to direct traffic via the route learned from the other provider. Careful assignment of local preference over the range of destinations is helpful in balancing the load on the two links. In some cases, one provider might charge a higher price for sending traffic, or generally have poorer performance. To reduce minimal cost or improve performance, the AS may tend to prefer routes through the other provider, up to the point where the link becomes too heavily loaded. More generally, an AS may connect to a single AS in multiple geographic locations. If one of the links to the neighbouring AS becomes congested, the operators may reconfigure the adjacent router to assign a lower local preference value to some of the BGP routes learned at this location.

Modelling the Effects on the Flow of Traffic:

Capturing the effects of routing policies requires extensions to the model presented earlier. By changing how the local-preference attribute is set, tuning the BGP policies affects how a router at the periphery of the network selects a best route. This, in turn, affects the egress set for each destination address block (or prefix). Modelling the influence of BGP policies on the flow of traffic requires:

BGP-learned routes from neighbour ASes:

The input data for the computation is the set of BGP learned routes from neighbouring ASes. In practice, the BGP-learned routes can be captured by dumping the BGP routing table at each router, or monitoring the BGP routes as they are advertised by the neighbours.

Specification of routing policies:

A BGP routing policy is a sequence of clauses, where each clause specifies a set of routes (e.g., based on the destination prefix or the elements in the AS path) and assigns a local-preference value to the matching routes.

Model of BGP path selection:

Computing the egress set requires applying the policies to the BGP routes learned from neighbouring demands, and then selecting the best of the modified paths. In particular, the model should select routes with the highest local preference and, among those, the routes with the shortest AS path length. Ultimately, each router would select the route with the closest egress point.

IV. CONCLUSION

IP routing protocols have tenable parameters that operators can set to control the flow of traffic through their networks. Optimization based on local-search techniques plays an important role in adapting these parameters to the prevailing network conditions. In this chapter, we considered three variants of the optimization problem, with increasing complexity: When each destination connects to the network at a single location, the optimization problem consists of setting the link weights that drive how the routers direct traffic on shortest paths. The inputs to the optimization problem are the traffic matrix and the capacitated network topology. When some destinations are reachable via multiple egress points, the optimization problem becomes more complicated. Instead of the traffic matrix, the offered load is represented as a set of traffic demands. The volume of traffic entering at a certain router and travelling to a particular destination. The optimization problem must also consider the set of egress points for each destination prefix.

REFERENCES

[1] B. M. Leiner, V. G. Cerf, D. D. Clark, R. E. Kahn, L. Kleinrock, D. C. Lynch, J. Postel, L. G. Roberts, and S. S. Wolff, .The Past and Future History of the Internet,. *Communications of the ACM*, vol. 40, pp. 102.108, February 1997.

[2] D. D. Clark, .The design philosophy of the DARPA Internet protocols,. in *Proc. ACM SIGCOMM*, pp. 106.114, August 1988.

[3] W. R. Stevens, *TCP/IP Illustrated, Volume 1: The Protocols*. Addison-Wesley, January 1994. ISBN 0201633469.

[4] A. Khanna and J. Zinky, .The revised ARPANET routing metric,. in *Proc. ACM SIGCOMM*, pp. 45. 56, September 1989.

[5] S. Chen and K. Nahrstedt, .An overview of quality of service routing for next-generation high-speed networks: Problems and solutions,. *IEEE Network Magazine*, pp. 64.79, November/December 1998.

[6] E. Crawley, R. Nair, B. Rajagopalan, and H. Sandick, .A framework for QoS-based routing in the Internet,. Request For Comments 2386, IETF, August 1998.

[7] B. Fortz, J. Rexford, and M. Thorup, .Traffic engineering with traditional IP routing protocols,. *IEEE Communication Magazine*, October 2002.

[8] B. Fortz and M. Thorup, .Internet traffic engineering by optimizing OSPF weights,. in *Proc. IEEE INFOCOM*, March 2000.

[9] A. Feldmann, A. Greenberg, C. Lund, N. Reingold, and J. Rexford, .NetScope: Traf_c engineering for IP networks,. *IEEE Network Magazine*, pp. 11.19, March 2000.

[10] B. Fortz and M. Thorup, .Optimizing OSPF/IS-IS weights in a changing world,. *IEEE Journal on Selected Areas in Communications*, vol. 20, pp. 756.767, May 2002.

[11] N. Feamster, J. Borkenhagen, and J. Rexford, .Guidelines for interdomain traf_c engineering,. *ACM SIGCOMM Computer Communication Review*, vol. 33, October 2003.

[12] R. Teixeira, A. Shaikh, T. Grif_n, and J. Rexford, .Dynamics of hot-potato routing in IP networks,. In *Proc. ACM SIGMETRICS*, June 2004.

[13] G. Huston, .Interconnection, peering, and settlements,. in *Proc. INET*, June 1999.

[14] L. Gao and J. Rexford, .Stable Internet routing without global coordination,. *IEEE/ACM Trans. Networking*, vol. 9, pp. 681.692, December 2001.

[15] L. Gao, T. G. Griffan, and J. Rexford, .Inherently safe backup routing with BGP,. in *Proc. IEEE INFOCOM*, April 2001.

[16] B. Quoitin, S. Uhlig, C. Pelsser, L. Swinnen, and O. Bonaventure, .Interdomain traf_c engineering with BGP,. *IEEE Communication Magazine*, May 2004.

[17] T. Ye and S. Kalyanaraman, .A recursive random search algorithm for large-scale network parameter con_guration,. in *Proc. ACM SIGMETRICS*, June 2003.

[18] N. Feamster, J. Winick, and J. Rexford, .A model of BGP routing for network engineering,. in *Proc ACM SIGMETRICS*, June 2004.

[19] W. Fang and L. Peterson, .Inter-AS traf_c patterns and their implications,. in *Proc. IEEE Global Internet*, December 1999.

[20] J. Rexford, J. Wang, Z. Xiao, and Y. Zhang, .BGP routing stability of popular destinations,. in *Proc.Internet Measurement Workshop*, 2002.

[21] J. Fong, A. Gilbert, S. Kannan, and M. Strauss, .Better alternatives to OSPF routing,. in *Proc. Workshop on Approximation and Randomized Algorithms in Communication Networks*, 2001.

[22] R. Mahajan, D. Wetherall, and T. Anderson, .Negotiation-based routing between neighboring ISPs,. in *Proc. USENIX Symposium on Networked Systems Design and Implementation*, May 2005.

[23] J. Winick, S. Jamin, and J. Rexford, .Traf_c engineering between neighbouring domains.. http: //www.cs.princeton.edu/.jrex/papers/interAS.pdf, July 2002.

[24] J. Fong, A. Gilbert, S. Kannan, and M. Strauss, .Better alternatives to OSPF routing,. in *Proc. Workshop on Approximation and Randomized Algorithms in Communication Networks*, 2001.

[25] R. Mahajan, D. Wetherall, and T. Anderson, .Negotiation-based routing between neighboring ISPs,. in *Proc. USENIX Symposium on Networked Systems Design and Implementation*, May 2005.

[26] J. Winick, S. Jamin, and J. Rexford, .Traf_c engineering between neighboring domains,July 2002.

[27] N. Feamster, H. Balakrishnan, J. Rexford, A. Shaikh, and J. van der Merwe, .The case for separating routing from routers,. in *Proc. ACM SIGCOMM Workshop on Future Directions in Network Architecture*, August 2004.

[28] O. Bonaventure, S. Uhlig, and B. Quoitin, .The Case for More Versatile BGP Route Rectectors.. Internet Draft draft-bonaventure-bgp-route-re_ectors-00.txt, July 2004.

[29] A. Farrel, J.-P. Vasseur, and J. Ash, .Path computation element (PCE) architecture.. Internet Draftdraft-ietf-pce-architecture-00.txt, March 2005.

AUTHOR DETAILS

Mrs D.Suguna Kuamari, Post Graduated in Computer Science (M.Tech), ANU, 2010, and Graduated in Information Technology (B.Tech) From JNTU Hyderabad, 2006. She is working presently as Assistant Professor in Department of Computer Science & Engineering in Gokaraju Rangaraju Institute of Engineering and Technology, RR Dist, TS, and INDIA. She has 7+ years Experience. Her Research Interests Include Networks, Software Engineering, Cloud Computing, Operating Systems and Information Security.

Mrs Bala Veeravatnam, Post Graduated in Computer Science (M.Tech), JNTUH, 2012, M.C.A From JNTU Hyderabad, 2008. She is working presently as Assistant Professor in Department of Computer Science & Engineering in Gokaraju Rangaraju Institute of Engineering and Technology, RR Dist, TS and INDIA. She has 3 years Experience. Her Research Interests Include Networks, Software Engineering, Cloud Computing, Operating Systems and Information Security.

Mrs P.Sowmya, Post Graduated in Computer Science (M.Tech), JNTUH, 2014, and Graduated in Information Technology (B.Tech) From JNTU Kakinada, 2012. She is working presently as Assistant professor in Department of Computer Science & Engineering in Gokaraju Rangaraju Institute of Engineering and Technology, RR Dist, TS, and INDIA. She has 1year Experience. Her Research Interests Include Networks, Software Engineering, Cloud Computing, Operating Systems and Information Security.

