BGP: A protocol for the"inter domain"routing

Ledina Hoxha Karteri
Faculty of Economy and Information Technology, EUT

Abstract

Border Gateway Protocol (BGP) is the current protocol inter-domain routing applied to the Internet. BGP, originally a simple protocol path-vector is always so incrementally changing over time through a number of mechanisms to support the policy, increasing significantly the complexity Although the performance of the Border Gateway Protocol is always accepted, the size, the heterogeneity and variability that characterize the Internet today, constitute a challenge to maintain the quality of service (QoS) setting increasingly demands for BGP traffic distribution packages database. Many of the BGP mystery stems not only from the complexity of the protocol, but also by a lack of knowledge of the basic policies and the problems that ISPs face. Last security analysis obtained from research communities have reported clearly unsatisfactory characteristics of BGP such as low integrity and slow convergence through theoretical analysis and empirical measurements. Thus it is evident that Internet routing infrastructure is quite vulnerable. Misconfiguration of routers often brings injecting large routing tables in BGP routing system. In the paper are described theoretically the characteristics and the problems associated with BGP and also the expectations of today's Internet users to applications in real time.

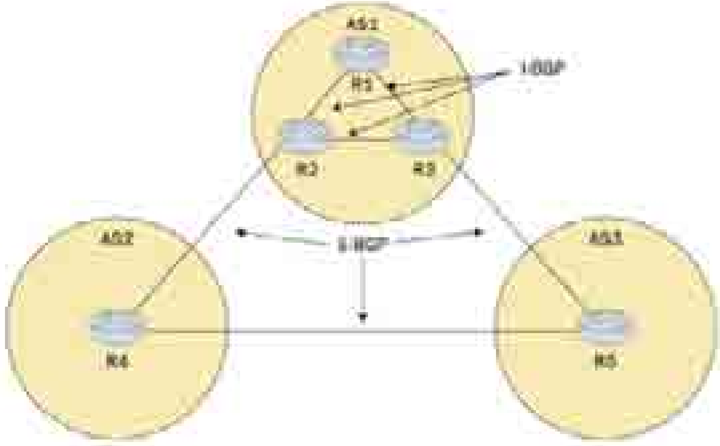
Keywords: AS, BGP, Traffic Engineering, QoS.

1. Introduction

Border Gateway Protocol (BGP) is simply another routing protocol, but with a very different role from others by serving as a connector that enables the functioning of the Internet. Moreover, the fact that each AS is managed by a different authority complicates the situation compared with intra-domain routing. BGP is implemented in a router and the messages are exchanged through a sustained TCP connection between two routers (by simplifying the complexity of implementation so the reliability of transport). Ruters executing a BGP routing process are known as a speaker BGP. Two BGP speakers that create a TCP connection with each other, in order to exchange routing information, are regarded as neighbors or pairs in communication.The local traffic running through an AS is classified as local traffic or transit traffic. The local traffic comes from or ends in the AS where is the IP address of the source or the destination. Any other traffic that crosses the AS is qualified as "transit traffic". An important goal of BGP Internet traffic is precisely reduction of the transit traffic. According to what we discussed about the traffic, we can affirm that a BGP router can communicate with a BGP router that are in the same AS with it (known as I -BGP) or other various AS-es, (known as E-BGP). All routers that "talk" I-BGP Within the same AS should establish links with each other according to the model "fully connected mesh". These links do not necessarily have to be physical it it enough only that these routers have to establish a reliable communication channel, TCP, among them. With no mechanism to detect endless cycles in I-BGP, routers that "talk" I-BGP must not convey routing information to third parties against their neighbors. E-BGP routers, contrary to the previous, can alert information to third parties to their neighbors E-BGP.

The following picture shows R1, R2, and R3 routers that use I-BGP to exchange routing information inside the same AS, and the R4-R2, R3-R5, and R4-R5 routers pairs that use E-BGP to exchange routing information between AS-es.

FIGURE 1: Internal BGP (I-BGP) towards external BGP (E-BGP)



As we discussed above, BGP is a protocol which is used to maintain the routing information between AS's. Most of the routing protocols are based on intra-domain

algorithm Dijkstra. But BGP is a protocol based on "vector path" (path-vector), which means that the routing information contains a vector with ASN (each AS-are made available to a number in order 0-65535) indicating the path of the AS-es that crosses a certain prefix (any aS also owns a sequence of IP addresses which may decide to allocate into more small groups that contain several continuous IP addresses, known as IP Prefix.). Based on the information exchanged between BGP routers is built a graph autonomous system (known and as tree).

2. BGP functionality characterstics

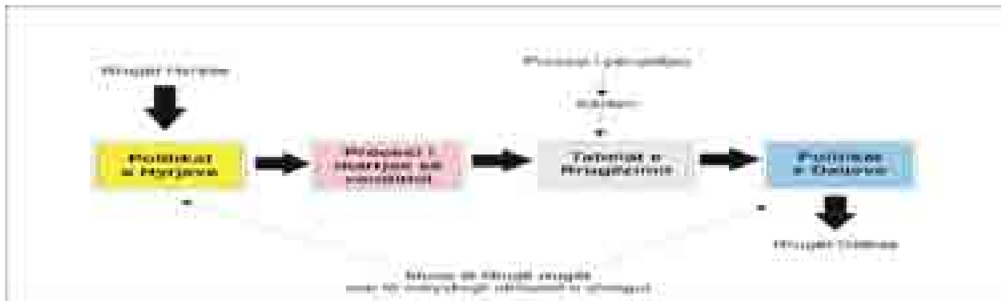
Regarding BGP: The whole Internet is a AS-s graph, connections between two AS-es form a path, the collection of information on paths forms a path to a specific destination and the routing within an autonomous system is realized through the IGP. Four types of messages are specified for BGP:

- Open message – which are the first messages that are sent and open a communication session between pairs.
- Update messages – provide updates on routing allowing the construction of a stable picture of the network topology. These messages enable the repeal of inappropriate roads and notification of new roads.
- Notification messages – Are sent in case of errors to inform the participants in the active sessin about the closure reasons of this session.
- "Keep alive" message – notifies the BGP pairs that an equipment is active dhe the session should not be closed. BGP routers don`t have a complete view of the network topology. Every router knows only how to reach the neighbours directly and especially through which neighbour in particular can a network prefix be achieved.

3. BGP routing

Most of the routing protocols which receive the routing information, use it to create routing tables and share the tables (or parts of it) with a lot of other routers on the network. What makes a protocol BGP unique is its ability to enforce policy on the information contained in the update messages, and consequently refreshing the selected information based on the attributes of the information itself. Routing policies define how are managed the paths taken by BGP nodes and sends this information to these joints. In many cases, policy routing filtering consist of paths, some paths acceptance, acceptance and modification of other roads and kunërshtimin of some. When updating messages are obtained by a BGP router, they are subject to a manufacturing process in accordance with a series of policies that determine how and where the information will be stored. In order to allow the control over the selection of the routes, the BGP announcements have added some attribute that allow changing decisions based on their values. The ruter compares the values of those attributes for each route, according to a ranking list and selects the path that has acceptable values for the attribute. If the values are the same, passes to attribute pauses. The selected way it will be used to forward packets. Through attributes is made possible that a longer route (which passes through more AS) to be selected towards a shorter one (these are very useful attribute in ISP networks). Koncepti i funksionimit të BGP mund të përmblidhet në figurën më poshtë:

FIGURE 2: Funksionimi i BGP – Politikat e rrugëzimit



A one path BGP speaker (the preferred way) can be used for a purpose and it is forbidden to spread different paths from that of the preferred in use. When a new advert is received, are used the routing implemented policies to see if the new route is better than the existing one. If this is the case, the old path is replaced with the recently received one. Later, if the policies permit it, the path is announced to the neighbors. BGP is an incremental protocol (incremental). When a router is connected for the first time with a neighbor it is broadcasted the full BGP routing table. After that, they sent regular updates on the routing information unless there are changes on the way. In theory messages should be sent only when are notified of a new path, updated (reflected changes) or revoking a path. BGP requires each router to store the information received from each neighbor and sent the information to other neighbors.

In order to route a data packet in a particular network, is needed the identification and the determination of the location of the destination network. BGP uses the routing with prefix to address the nets. The prefix of a network is based on the idea of setting an identifier for any network so that each data package to be clear if the destination is located to a certain network. Prefixes do not provide any information

on how the network reaches its destination. This information should be obtained from the use of BGP protocol. In the context of BGP, the mainting information on the connections means being able to identify how a data packet is route to the destination.

In addition to the default route will be saved also all the alternative roads that lead to a particular network prefix from other neighbors. The reason for this is the need to restore the connection as soon as the predetermined path becomes unavailable.

4. BGP convergence

BGP is executed simultaneously in routers setted in different AS and therefore, the process of choosing an Internet path is filled out and distributed in a distributed way. The result of a distributed algorithm may depend on the initial condition of the system and the order execution process. In some cases, a distributed algorithm can achieve more stable condition although stable conditions are accessible in the initial state or another execution sequence would be chosen. When a router changes his best path, they can form closed loops, temporary and can lose packets. In the process of selecting the BGP path does not converge, some routers can continue to change their path infinitely better, which can have a devastating impact on Internet traffic. For this reason, the protocol convergence is an important issue in the design of the Protocol of inter domain routing.

As most of the specifications of routing protocols, BGP includes a "stopwatch" for each ad to limit the order of BGP updates. Without limiting element, a pair would send updates to its neighbors whenever the best path changes, even if the path to a prefix changes several times within a few seconds. In BGP, the "stopwatch" is called Minimum Route Advertisement Interval-timer (MRAI).

A "stopwatch" jittered type means using values that vary randomly. MRAI typical value is 30 seconds. Whether were used exactly 30 seconds for each router, it will be transformed to self-synchronization of routers. This in its turn implies sending update messages at the same time, every 30 seconds [19]. This is an undesirable effect for BGP. This can be avoided just by modifying the range of "stopwatch" randomly for each router but implemented in a way to achieve values between 25 and 30 seconds.

MRAI can trigger sending multiple updates in a section between the lateral communication as shown in Figure 3. AS1 has added a new prefix P and therefore is sending a BGP update message ddrest AS2 and AS3 on the path P: AS1. This update is received from AS2, added to the routing tables, and sent to the AS4 bacause AS2 has not sent any update to AS4 within the last 30 seconds. AS4 receives the update, adds the code in the array and sends the updates to AS5. AS3 has also received information and updated the table, but can not send it to AS4 as long MRAI interval has not ended. Once the AS4 receives the update, it understands that this is a better path and updates the routing table for this prefix with new information and sends an update of another prefix P, AS. As noted, in a so simple example, AS1 served as a source for an update prefix P and AS4 has no need to send two updates for the same prefix.

FIGURA 3: Example for the spread of a BGP update

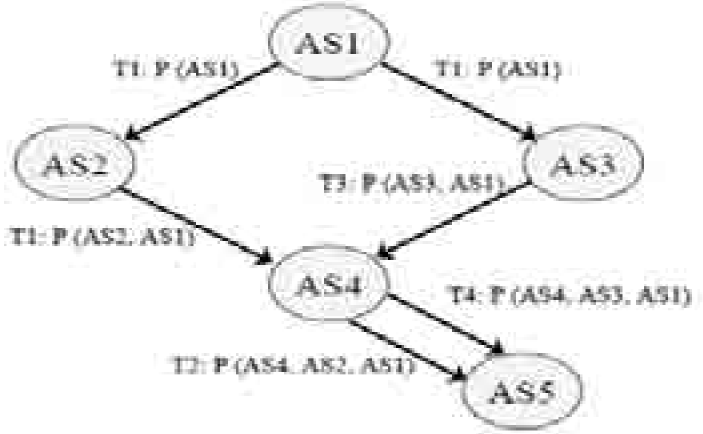


Figure 2.2: Example: BGP update propagation.

Delivering the updating messages depends mostly from the topology and on the number of alternative routes. BGP previous works has shown that if there is not any restriction, nodes tend to share a large number of updates to the unstable paths (routes flapping). Through Route flap damping mechanism [20] is attempted to avoid an unstable path to make Internet overload update messages. The main idea behind it is to keep a history of updates for a specific prefix and updates refuse to believe that exceed certain predetermined parameters. For example, a number of updates for one hour may be too high. BGP is a protocol that sends incremental updates only if there are changes about the topology and / or the achievement. In theory, the changes are followed by some updating messages sent between nodes. Once the parties have renewed their favorite routes, BGP world turns quiet again. The time between the change and the time when all pairs have chosen new favorite paths represents the concept of convergence. The convergence process ends when all pairs have established their new routes, the preferred ones. This is a naive concept. In reality, due to the size of the Internet (about 15 000 AS, 120 000 prefix) and many other factors, it has a constant traffic noise of BGP. And

therefore the process of convergence has to be studied in more details. Whenever the ability to reach a network changes, there must be a reason for this. This is known as the event of instability. A partial list of the possible reasons is as follows:

- Failure or repair of a physical link.
- Restarting the router (eg. To update the software).
- Changes in the AS's policies.
- Addition / deletion of the prefixes of the grid.

The event of instability can affect the connection within or between AS's. When the interior connection of an AS is included, it triggers the convergence process within the AS, the IGP protocol [21]. Connecting events with BGP IGP (IGP redistribution in BGP), is inconsistent with the operational practices. BGP normally should not be involved in the event of instability.

When an instability event affects the connections between AS's, it causes the repeal of a previous path or the announcement of an alternative route. If we see the effects of instability in the BGP event we distinguish moment followed by the first update sent by BGP BGP node affected by the event. This new information spreads through the achievement-at BGP router and more preferably, there will be other updates and this is where it is said that the network has converged with regard to this prefix. From the perspective of a router, this can take a number of updates from each party, a new way to calculate the best and TJA notify other parties. All this procedure will be called in BGP convergence process.

5. BGP instabilities

BGP has met many of the requirements of today‘s Internet, but there are many weaknesses. Issues as diverse as programming errors, TCP attacks or network overload can cause instability in the routing tables of BGP routers.

a. The phenomenon of “black hole” - One of the classic problems of BGP phenomenon known as the “black hole”. In this problem, a mistake, an attacker or a misconfiguration causes a BGP router to announce mistakenly through which AS where taken part, eg AS X, there are treks to several networks at low cost. This in turn causes many-a BGP routers to update their routing table with this information. As a result, a large amount of traffic will pass through AS X. This unexpected traffic turn causes instability of the routing tables, large amounts of network packets and lost resources and ultimately a decline overload to AS X.

b. The weknesses of TCP - Another important weakness of BGP is connected with the transport relevant protocol used by BGP, which is TCP. This protocol is vulnerable to some types of DOS attacks, errors in programming and network congestion on the lines used. Eg. a type attack "SYN flooding" on a server, can cause that the connections provided between the BGP parties to not lose the existing ones, if the traffic generated by the attack causes overload of the network.
c. Network overload - Network Overload can be pathological for BGP and cause instability in the routing tables. For example, if a very large amount of traffic is destined to pass through an AS-art specifically, it is likely that the links connecting the AS with the outside world to be overloaded and thus can pass messages keepalive exchanged through a TCP connection set to lose or TCP connection and detach itself. In this case will be losen the neighborhood between two BGP routers.
d. Route flapping - routing instability can be described as a rapid change of the information on the accessibility of the destination information and network topology. It occurs when a path is repealed and then renotified, in this case we say that it fluctuates. Instable paths are costly because routers should calculate new paths whenever a new message is received. This causes high load on the router and can lead to a failure (crash) of it.

Several techniques have been developed to improve the instabilities of BGP. The two most important are:

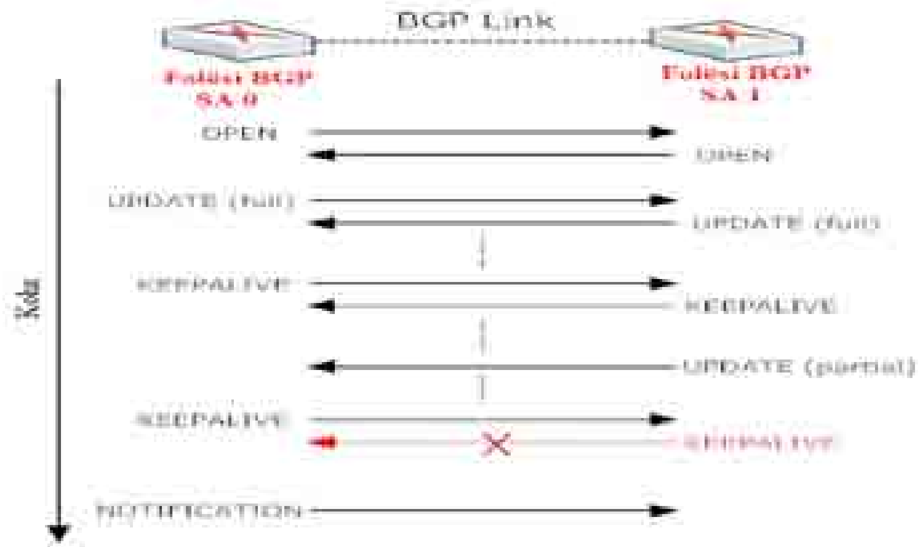
In the case of varying paths, some implementations of BGP, use a mechanism known as "path extinction" (route damping) – to a varying path is dedicated a punishment value and if that value exceeds a certain limit, this path is considered as invalid. The value of the penalty is reduced over time. Fluctuations in the path terminates, it punishment that was decided repealed.

Message aggregation often there is a link between the refresh messages and those of the revocation. Usually, when a path is repealed, repeal message directly associated with a notification message - the road may be subject to changes of behavior or a pathology. To reduce the traffic volume of that message is in our interest to not distribute it immediately after its generation, but preserve it for a long time and aggregate the information. In this way if the path it is repealed and then re-announced, it is correct to void the two messages so that the general situation remains the same. This method reduces the volume of traffic and the processing in the BGP routers. Unfortunately both of these methods brings delay in the path distribution. So regardless of the protocol and the paths stabilization, convergence time is increasing.

6. Session management between the "pairs"

When routers that support BGP want to open a communication session, then they open a TCP connection on port 179 with the match router. After the connection is established, any entity sends an opening message to negotiate the communication parameters of the session. In order to be aware of the validity of this relationship and to monitor router-at neighbors, routers often send keep-alive messages. During the opening of the exchange of the messages, BGP routers determine the waiting time, the maximum time to wait before sending a message successor. Lack of presence of a message in this interval indicates that another entity is not functioning normally. If an entity within the „couple" communication takes a wrong message, badly formatted, or you get nothing within the time waiting then sends a message type notification entity neighbor, deletes all table of routes that take him and thankfully closed TCP session. Below are shown the steps used to achieve a communication session BGP.

FIGURE 4. BGP message exchange



7. Routing information exchange

Initially, before the exchange of routing tables, 2 BGP routers establish a communication session. Then the entities can exchange all routing table that dispose, through a series of messages (UPDATE). Routers are supposed to memorize all paths offered by other entities in the session. After finishing all routers are sending updates to each other part of new paths on their tables.

Update type messages can cover 2 types of informations: 1) Announcement and 2) Retreat. An alert informs its recipient for a new path to the destination prefix, and a withdrawal cancels previously announced path. In addition to the coverage information, a message update contains a variable number of attribute paths, which describes the features of the path, from which we can mention: local preference, next-hop, Origin type, AS path and multi-exit discriminator (MED).

Let's see what describes each of them:

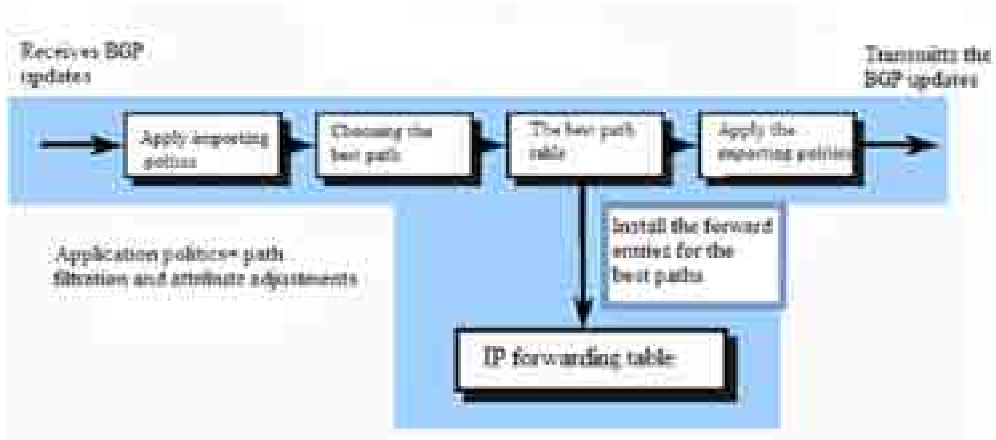
1. AS path attribute contains a list of all the autonomous systems that prefix described. AS path BGP uses to detect cycles as well as to choose the path. When a router receives a BGP update then examining whether the vector of the road and sees its number of Autonomous System then it invalidates this path.
2. Next-hop attribute represents the IP address of the router's to be used to achieve the desired network.
3. Origin type attribute identifies how AS beginners learned about the path, within the Autonomous System (static configuration), a version obsolete Exterior Gateway Protocol (EGP) or is injected by another routing protocol. Origin types are known as IGP, EGP, or unknown (incomplete).
4. Multi-Exit Discriminator attribute encourages the recipient to determine which of the exit points to guide the traffic to the neighboring autonomous system.
5. Local preference attribute may be included in iBGP messages (for which they will discuss below) to help the receiver to rank the paths taken from a different router in the same Autonomous System.

8. Path finding and processing

There are two types of BGP sessions between the entities: the external BGP (eBGP) for various entities between Autonomous Systems and the internal BGP (iBGP) for entities between the same Autonomous System. The Figure 2.3 shows the steps for BGP route finding. At first the router applies import policies to filter unwanted paths. For example, a BGP router can receive notifications from an AS path that contains a trusted set of autonomous systems. Then router calls a decision-making process to choose exactly a better path to any destination prefix, comparing the new path with all other routes previously recognized for the same

destination. The router applies a sequence of steps to tight the candidates set to 1 only. The best way of choosing this path will be installed in the distribution table, while other paths will be kept for backup purposes.

FIGURE 5. BPG path choice



In the end, the router applies export policy to manipulate attributes and decide whether to announce this path to neighboring autonomous systems. If yes, the router can modify some of the attributes of the path. It will eventually add it`s AS number to the AS path.

8.1. Path devaluation

If a router receives withdrawal information, first it removes the impaired path from his records. If the path that is removed is currently the best way, the router requires in its backups for the second best path and if that does not work then calls it as an unreachable destination. If the last on is applied, the depreciation notification must be brought to each entity that learned the path from previous announcements.

8.2. Path reflection

In the iBGP standard implementation, all BGP routers within the same autonomous system are so closely related to the routing information so that out of the distributed system among all routers within the AS. But this model can create problems with the scalability when AS has a large number of BGP speakers. Reflecting the road creates a way to reduce the BGP traffic control, this by minimizing the number of messages sent within the system update Autonomous.

The concept of route reflection is based on the idea of creating a node (router) concentration (reflective), which function as a focal point for iBGP sessions. In the paths reflection, BGP systems are organised in batches (clusters). Each cluster consists at least one router acting as a path reflector, along with any number of client entities. Entities outside the cluster entities are not considered clients. Reflector paths redistribute routing information to any entity, whether or not a customer. Because of the way Reflectors redistributes paths within the cluster, BGP routers are not required to be fully connected.

When a path reflector receives a path, he chooses the best path. Later, if the path comes from a non-entity client, the reflector sends the path to any entity within the cluster client. If the path is from a client entity, the reflectors sends path to any entity not customer and not client except that the one from which is generated. During this process, no entity client sends paths to each other.

9. Conclusions

BGP is categorized as a path vector protocol (PV), a variant protocol distance vector (DV). Rather than transfering the information about the state of connectivity and cost, it leads the information on the full path to avoid excessive cycles. BGP contains communication protocol TCP as the transport layer, which is on his side secure protocol and eliminates the need for BGP assume retransmission, approval (ACK) and secuenciality. Routers using BGP as their protocol are called BGP speakers. Two BGP speakers participating in a session are called BGP neighbors or couple. Routers couple exchange 4 types of messages: open, update, and keep-alive notification. Of all these messages contain only update routing information while 3 others serve for managing the communication session.

Based on what is mentioned above, the characteristics of routing in the Internet today can be summarized in the following general principles, about the paths between two nodes u and v:

- If u and v are in the same AS, the path between them remains entirely within the AS.
- If he is in AS v U and V AS is the path between u and v moves from u to zero or more AS transits.

Initially, before exchanging the routing tables, 2 BGP routers assign a communication session. Then the entities can exchange all routing table, through a series of messages (UPDATE). Routers are supposed to memorize all routes offered by other entities in the session. Once all is completed, routers send to each other the partial updates of the new paths in their tables. At first the router applies import policies to filter unwanted paths. Next the router calls a decision-making

process to choose exactly a better way to any destination prefix, comparing the new path with all other paths previously recognized for the same destination. The router applies a sequence of steps to narrow the candidates set to 1 only. The best way of choosing this path will be installed in the distribution table, while other routes will be kept for purposes of backup.

In conclusion, the router's export policy is applied to manipulate the attributes and to decide whether to announce this path to neighboring autonomous systems. If yes, the router can modify some of the attributes of the path. It will eventually increase it`s AS number to the AS path.

If a router receives a withdrawal information, first it removes the impaired path away from his records. If the path that is removed is currently the best way, the router requires its backups in a second best way and if that does not work as well then calls it as an unreachable destination. If the last one is applied, an impairment notification must be carried to every entity to learn the path of previous announcements. In the IBGP standard implementation, all BGP routers within the same autonomous system are so closely related to the routing information out of the distributed system among all routers within AS-es. But this model can create problems with the scalability when AS has a large number of BGP speakers. Reflecting the road creates a way to reduce the BGP traffic control, this by minimizing the number of messages sent within the system update Autonomous.

The concept of route reflection is based on the idea of creating a node (router) concentration (reflective), which function as a focal point for iBGP sessions. In reflection of the way, held in batches BGP systems (clusters). Each cluster consists of at least one router acting as a street Deliberators, along with any number of client's entities.

References

A. Bacioccola, C. Cicconetti, dhe G. Stea, User-level performance evaluation of VOIP using NS-2, në Proc. Int. Conf. Performance evaluation methodologies and tools, Brukles, Belgjikë, 2007, ICST.

F. Wang, N. Feamster, dhe L. Gao. Quantifying the Effects of Routing Dynamics on end-to-end Internet Path Failures. Raport Teknik TR-05-CSE-03, Universiteti i Massachusetts, 2006.

F. Wang, Z. M. Mao, J. W. L. Gao, dhe R. Bush. A Measurement Study on the Impact of Routing Events On End-to-End Internet Path Performance. Në SIGCOMM, 2006.

Fouad A. Tobagi, Athina P. Markopoulou dhe Mansour J.Karam. Is the Internet ready for VoIP? In Proceedings of Distributed Computing, Mobile and Wire- less Computing 4th International Workshop (IWDC), faqet 49–57. Microsoft Press, 2002.

N. Kushman, S. Kandula, and D. Katabi. Can you hear me now?! It must be bgp. Në SIGCOMM, 2007.

R. K. Rajendran et al., Performance Optimization of VoIP using an Overlay Network, Raport Teknik, NEC, 2005.
S. Tao et al. Improving VoIP Quality Through Path Switching. Në INFOCOM, 2005.
T. D. Feng, R. Ballantyne, dhe L. Trajkovi. Implementation of BGP in a network simulator. Në Proc. of Advanced imulation Technologies Conference 2004 (ASTC'04), Prill 2004.
Y. Amir, C. Danilov, S. Goose, D. Hedqvist, dhe A. Terzis. An Overlay Architecture for High Quality VoIP Streams. Në IEEE Transactions on Multimedia, Djetor 2006.

Social media and brand management (literature review)

Elvira Tabaku
Faculty of Economy & Information Technology, EUT

Abstract

Social media use has expanded greatly in the last years in Albania. The development of different networks that offer online service all over the country has contributed a lot to it. Many people, particularly young ones, are very fond of it, are using heavily and social media networks are now part of their lives. Social media have changed the way people communicate and interact with each-other and the marketing done on social media has enriched their marketing mix and has transformed the way companies communicate to their customers. Companies and brand managers have the opportunity to benefit from the use of these new communication channels and boost their profits. The purpose of this study is to offer a review of the existing literature about social media use by companies. It focuses on the marketing generated through social media channels and the specific elements related to it. Extant research evidence the significant effect that social media marketing has on the overall communications between companies and customers and the benefits and challenges associated to it.

Key words: *social media marketing, brand, consumer*

1. Introduction

Technological developments in the last decades have offered new ways of communication between people and organizations. Internet is an innovative way for individuals and companies to communicate. Internet use has become a normal phenomenon during the last decade and an essential element of everyday life (Amichai-Hamburger & Vinitzky, 2010) as it influences many human and business aspects from the way in which organizations operate to the way people