Journal of Telecommunications System & Management

Chreighvon, J Telecommun Syst Manage 2018, 7:3
DOI: 10.4172/2167-0919.1000175

Review Article Open Access

Building a MPLS Based Telecommunication Network

Chreighvon Rodgers*

East Carolina University, Greenville, 2313 August Way, Raleigh, North Carolina 27610, USA

Abstract

Broadband internet has provided a way for people to connect across the country in almost real time. People have started hosting servers and media so they can access their files anywhere. They have also given access to friends who may use their servers to stream files. The rise of broadband internet has also revived the videogame industry and has opened the door to new possibilities. Broadband internet has allowed gamers to connect and play with people all over the globe. The boon of broadband internet has also led to an increase in competitive gaming. Competitive gaming requires minimal lag time, minimum drops, and very low latency to provide a robust experience. Schools and businesses have tapped into the power of broadband internet by creating WANs and hosting their own servers and services. Building a network to provide internet services to these customers is a large and complex endeavor. Similar to a campus LAN or building LAN the telecommunication service provider must be wary of the cost of providing the services. Similar to data center network, the company will need to handle obstacles like collocation and bandwidth utilization. This paper will explore how telecommunication companies can better serve customers like the video game industry and LAN administrators, through a range of technologies and services. This paper will look at MPLS, VPLS, DWDM, and BGP technologies to see how the telecommunication companies can use them to increase customer satisfaction without straining the company's network. This paper will compare and contrast different protocols, technologies, and design modules to aid in determining what will be the best fit for the company.

Keywords: LAN; WAN; Broadband; Network; Telecommunication

Introduction

Broadband internet is the driving force of innovation. The increased internet speeds have given the public a method to connect from almost anywhere in the developed world. People use this new connectivity to share things like media, status posts, shopping, and even competitive gaming. Broadband internet has helped industries like video games become competitive events. The internet and the advancement of gaming consoles have created a growth in the popularity of tournaments and sites that allow people to stream other people playing games like Twitch. Customers in the public want a connection that is high speed, low latency, and resilient. Telecommunication companies strive to fill these requirements and provide these services to their customers. Services telecommunication companies provide include providing internet access, transporting customer data, and providing dark fiber solutions. In a traditional network, the customer relies on the telecommunication company to transport their packets across traditional IP links to their end destination. This connectivity requires a very robust network that can sustain outages and continue to grow with the demand. This paper will introduce an MPLS based network. This network is an alternate type of network that can meet the customer demands. This paper will breakdown the technology a telecommunication provider will need to use to provide a MPLS enabled backbone. This paper proposes providing a network where customers can request extended LAN services. Using extended LAN services can potentially cut down on latency, lag, and improve customer service through ease of setup. This network will require collaboration with the telecommunication company, partner telecommunication companies, and the end users. Before designing the network topology and protocols, the engineer will need to decide which model to follow. The two most widely used models are the Open Standards Institute model and the Department of Defense model.

Basics of the OSI Model

The OSI model divides the network communication process into 7 layers: Physical, Data link, network, transport, session, presentation, and application. A telecommunication company needs to be able to provide services on all seven levels to remain competitive. The first layer is the physical layer. The physical layer is the media used to connect the devices together. It can range from fiber optic, to cable, to Cat6, to wireless. The second layer is the data link layer. The data link layer uses things like mac-addresses to switch traffic. Switches or routers with switching capability typically operate at this layer. The third layer is the network layer. The network layer performs routing functions so that packets reach their destination. The fourth layer is the transport layer. This layer packages the information into packets for transmission along the infrastructure. The session layer is responsible for establishing communications between 2 pieces of equipment. The presentation layer is responsible for restoring the data to a readable format. This includes decrypting communications. The Application layer is responsible for displaying the data in a screen. The benefits of this model are the separation of duties. Each layer is responsible for its part. When the device finishes its part, it passes the information on to the next layer. The operations that occur on each level happen independently of what occurred in the previous layer. On a conceptual level, the architect can think of each layer talking to its twin layer at the other end of the destination. For example, if there is a frame problem transmitted from site A when the traffic reaches Site B the equipment responsible for that layer is responsible for generating the error. The downside to the OSI model is that new routing protocols and devices do not operate on just one particular layer. For example, routing protocols should run on the third layer however, BGP runs on layer 4,

***Corresponding author:** Chreighvon Rodgers, East Carolina University, Greenville, 2313 August Way, Raleigh, North Carolina 27610, USA, Tel: +19194459399; E-mail: rodgersch17@students.ecu.edu

Received November 27, 2018; **Accepted** November 28, 2018; **Published** December 07, 2018

Citation: Rodgers C (2018) Building a MPLS Based Telecommunication Network. J Telecommun Syst Manage 7: 175. doi: 10.4172/2167-0919.1000175

and EIGRP runs on layer 3. They provide connectivity across the link but they also provide connectivity across links that are not physically connected. Switches are another example because they can operate at layers 1, 2 and 3 [1].

Basics of DoD Model

The Department of Defense (DoD) model is a four layer model. The first layer is the link layer. The second layer is the internet layer. The third layer is the transport layer. The fourth layer is the application layer. The link layer is a combination of the physical and data link layer of the OSI model. The internet layer performs the same functions as the network layer in the OSI model. The job of the transport layer is to build and maintain sessions between devices. This layer must also handle transmitting the data between devices. The application layer is where the user interacts with the data. This model fixes some of the shortcomings of the OSI model. An advantage of this model is that things like the routing protocols all fit in one layer. This is the most widely used methodology and is the methodology used to design this network. After choosing which model to follow the architect will need to design the physical layer, choose the routing protocols, design the MPLS enabled backbone, and then provide MPLS services like VPLS [2].

Designing the Fiber Network

The first layer of the OSI and DoD model is the physical layer or link layer. For most topologies, this layer is simply cat5 cables or fiber optic patch cables that can connect equipment together that are at most a few miles from each other. The telecommunication company's layer 1 infrastructure is more complex due to the distance between pieces of equipment and the number of services on the links. In order to meet the physical layer demands telecommunication companies employ specialized equipment called optical amplifiers to send the signal via light across the fibers for long distances. Currently the core technology that allows networks to grow exponentially is the Wave Division Multiplexing technology or WDM. Between the 1990s and the 2000s, WDM capacity grew at a rate of about 80% per year. In the 2000s, the technology advanced to the point where channel spacing could be as tight as 50GHz. Each of these channels could support speeds above 40 Gb/s. In the last few years, telecommunication companies have started creating 100 Gb/s wavelength networks to backhaul their data [1]. This new technology allows for the transmission of Terabytes of data at 100 Gb/s per channel. Winzer by using this WDM technology, the telecommunication company can mux numerous channels together and use one fiber pair to carry this traffic to its core. For example, Cisco has a card system that combines 10 – 10 Gb/s signals and sends across the network on one 100Gb/s channel using only one wavelength. Protocols like Ethernet, SONET, and wireless protocols also fall into this layer [3].

OSI Data Link Layer/Link Layer in DoD Model

Before choosing which routing protocol to use the architect will need to understand the second layer of the OSI model, the data link layer. In the Department of Defense model, this technology also corresponds to the link layer. The data link layer handles communication between two neighboring pieces of equipment [2]. Data is switched using the layer 2 addresses or mac-address between devices. The layer 2 switch has a mac address table that it uses to forward traffic destined for that mac address. There are basic layer 2 protocols that networks use to forward their traffic. The first is address resolution protocol also known as ARP. ARP binds an IP address of an interface to the media access control of an interface. Before sending a packet out, the network device checks their ARP table to see if there is a MAC address for a specific IP address. If there is a MAC address for the next hop the packet is forwarded. If there is not a MAC address in the table then the device sends a broadcast to determine who has the next hop information for that IP address. In networks, this type of switching stops at the router and the router uses the layer 3 address to route the traffic [4].

OSI Network Layer/Internet DoD Layer

The fiber network is the base of the telecommunication company's network but the network cannot provide any IP services without using a layer 3 protocol to stitch connections together. Most layer 3 networks use protocols that use the IP network stack. The router uses the IP information to form forwarding tables. The router uses the table to forward traffic to its end destination. Routers forward traffic by using a static route, interior gateway protocol, or exterior gateway protocol. The IP address is the address used by routers to forward traffic. There are two types of IP address: IP version 4 and IP version 6. IP version 4 uses a 4-byte address and is the prominent addressing scheme of the internet. Administrators can assign IP version 4 address either manually or via an automation process called DHCP. The IP version 4 addresses can be either public or private. Administrators can route public space across the internet to other providers. Private space is limited to local use only. Administrators should not advertise private IP version 4 spaces to other autonomous systems. IP version 6 addresses are different from IP version 4 addresses. The underlying protocols and features are different. Instead of public and private IP space, IPv6 has global and link local addresses. Administrators can assign IPv6 addresses manually or allow the routers to negotiate their own. When choosing the interior gateway routing protocol, the architect will need to choose how much of each type of addressing they plan to employ. While the architect is deciding which address scheme to choose, the architect will also need to work on the network topology network.

Designing the Network Topology

When designing their network the telecommunication company must determine the best topology, where to locate their hardware, maximizing reliability, and planning for new technologies [5]. Similar to most LANs the telecommunication provider must plan its network according to anticipated traffic flow. However, unlike a traditional campus LAN architects must thoroughly plan equipment locations. Telecommunication networks can span thousands of miles with connected network devices being miles apart. Cisco has determined that the most efficient network design follows a hierarchical approach. This approach divides the network into 3 layers: a core, distribution, and an access layer. The core layer is the center of the network. The core layer is responsible for fast transport, high reliability, redundancy, fault tolerance, low latency, good manageability, avoidance of CPU packet manipulation, limited size, and QoS. The core layer of the network must be the most secure. If an attack compromises the core, the effects could be widespread and very damaging. The size of the core must be limited to minimize core exposure and maximize core speed. The network normally connects the distribution layer to the core layer. The distribution layer: provides redundancy and load balancing, aggregation of access sites, QoS, security filtering, address summarization, broadcast or multicast domain definition, redistribution between routing protocols, among other things. The access layer connects to the distribution layer. The access layer is responsible for providing user access to the network. Some features of the access layer includes: layer 2 switching, high availability, port security, broadcast suppression, QoS classification, rate limiting, and ARP inspection [6]. The telecommunication company can design

its network using the suggested hierarchical model but it will be on a larger scale than enterprise networks and campus networks. The majority of the connections at the access layer will be users. Each customer will need a piece of equipment called customer equipment (CE). The distribution layer is the hut or point of presence that captures all the customer connections. The connection between the two layers can be fiber optic or coaxial cable. The distribution layer combines the signals together and sends traffic to the core. The network engineer can determine how to engineer the traffic. Some of the traffic can flow around the core to alleviate core bandwidth. Unlike campus or enterprise networks, the architect does not have to follow the Cisco hierarchical model. Some customers will have direct connections to the core or distribution layer. This commonly happens when peering with other commodities or large bandwidth customers. However, the engineers should keep these connections as low as possible for security purposes. When designing the topology the architect should keep in mind what routing protocol they may want to deploy. There are four main routing protocols: EIGRP, OSPF, ISIS, and BGP. Each protocol has its advantages and disadvantages.

BGP

In order for traffic to flow between autonomous systems, engineers use an Exterior Routing Protocol. The industry standard is Border Gateway Protocol or BGP. According to the American registry for Internet Numbers (ARIN) an autonomous system is defined as a "group of routing prefixes that maintains a unique routing policy, controlled by an Internet Service Provider (ISP) ("Autonomous Systems and Autonomous System Numbers," n.d.). The network administrators of a pair of neighboring autonomous systems enable BGP so it can advertise routes to the other autonomous system [7]. After the telecommunication companies advertise its routes, the routers use updates to notify the adjoining autonomous system of routing changes. A major drawback of using BGP is the updates can be processor intensive. A study has shown that interdomain route convergence instead of congestion causes the majority of packet bursts [8]. Since BGP table refreshing can be processor intensive engineers need to take steps to protect the router from flapping interfaces and routes. BGP is the protocol of internet. The architect must be ready to enable BGP to connect to upstream peers so customer's traffic can flow to other peers.

IS-IS

Intermediate System-to-Intermediate System also known as IS-IS is a link state protocol. A link state protocol passes information along the entire path to build a routing table. In the IS-IS protocol the entire routing domain is split into subdomains with each subdomain being called an area. IS-IS differs from other protocols in how it divides its routing. Level 1 routing means that the routing is contained to the same area. When routing flows between areas it becomes a Level 2 area. The network administrator determines whether IS-IS passes Level 1, Level 2, or both. Level 1 IS-IS routers passes information to other Level 1 IS-IS routers. IS systems that operate at level 2 passes information to other level 2 routers even if the routers live in different level 1 domains. Unlike other protocols like EIGRP or OSPF IS-IS uses a completely different type of address to differentiate devices. IS-IS uses a Network Entity Title [9]. The Network Entity Title (NET) consists of the Network Service Access Point or NSAP. The NET consists of 3 parts: the area ID, the System ID, and the NSEL. The NSAP identifies the instance of IS-IS running on an intermediate system.

OSPF

Open shortest path first protocol is an open source interior gateway routing protocol. OSPF is a link state routing protocol. The link state is the description of the interface and the interface's relationship with the routers neighbors. OSPF uses a shortest path first algorithm to determine the best shortest path to all destinations. OSPF uses the concept of areas to divide the network into chunks. The backbone area is typically the core of the network. The network administrator can create other types of areas to connect to the backbone area to segment their network.

EIGRP

Enhanced Interior Gateway Routing Protocol (EIGRP) is a Cisco proprietary routing protocol. EIGRP is a distance vector protocol. EIGRP uses the Diffused Updated Algorithm to determine the best patch. This protocol uses multicast traffic to form adjacencies with its neighbors. The routers use can dynamically discover and recover adjacencies with little input from the operators. EIGRP use hello packets in order to maintain the adjacencies and to detect a link failure. EIGRP has the added benefit of being able to load balance across asymmetrical links.

MPLS

After the choosing which protocol to use, the network can use Multiprotocol Label Switching. Multiprotocol Label Switching is an extension of IP network protocol. MPLS is similar to a lightweight tunneling protocol. In the OSI model, the MPLS protocol requires both data link layer and network layer technology to operate. In the Department of defense model, it requires services at both the link and the internet levels. A MPLS network has edge label switch routers, which surround a core label switch router. The customer connects their equipment to the edge label switch routers. Engineers can aggregate multiple customer sites into the edge label switch routers. The customers typically run traditional IP networks. Thus, the MPLS network is transparent to them. MPLS networks use routing protocols used in ordinary IP networks. The routing protocols provide the router with routes to destinations outside its known networks. There are two main routing protocols in use in most MPLS networks, Open Shortest Path First (OSPF) and Interior System to Interior System (IS-IS) . Under the hood, Label switch routers (LSR) use labels to switch traffic instead of using traditional IP packet forwarding. This switching technology relies on the administrator setting up label switched paths (LSP). The process of setting up a label switch paths uses the Label Distribution Protocol (LDP) . The LSR uses the IP forwarding table set up the LSPs. This type of MPLS is known as hop-by-hop MPLS. There are a number of different ways to set up LSPs. Architects should base the method selection on the platform, network requirements, and services offered. There are two different types of MPLS networks: Packet-based or switch-based. Packet-based MPLS LSRs have the ability to handle packets and can examine the layer 3 header. Switch-based MPLS LSRs forward packets via the layer 2 header or optical switching [10]. The data flow of a packet entering an MPLS cloud is as follows: the ingress router receives the packet and appends a label to it. During each hop on the LSP, each router swaps the tag for the tag it has in its FIB that corresponds to the next hop. When the packet arrives at the egress router, it removes the tag and the payload is unaltered [11]. In order to deliver MPLS based services to customers, telecommunication providers will need to collaborate with each other.

Building an Inter-Provider MPLS Service

In order to provide MPLS services to customers the service provider will need to pass traffic onto other providers. There are traditionally three different options to pass labels onto a different provider: VRF-

to-VRF, Redistribution, and Multihop redistribution models. In the VRF-to-VRF model, providers do not exchange labels. Instead, sub-interfaces connect the routers and an EBGP peer is setup to distribute routes between them. This model is the most secure because peers do not share routing information. However, this option does not scale well because each VPN needs a sub-interface and a BGP peer. Redistribution models requires the two service providers to share BGP routing tables and VPLS information. This model improves the scalability because the provider uses one peer to exchange the labels. The Multihop redistribution model requires two autonomous systems "to share BGP routing information and MPLS routes across a provider boundary". This allows the company to build complete label switch paths from end to end across the network boundary separating the two autonomous systems. Since the autonomous system border routers do not maintain routing information for the VPNs this model is the most scalable. However, this model requires the edge routers to accept labeled packets and label bindings [12]. After setting up the MPLS network the architect can utilize overlay technologies like Virtual Private Lan Switching.

VPLS

Virtual Private LAN Switching allows a customer to connect their LANS across a telecommunication company's network. Establishing a VPLS domain will also allow people to form their own data sharing pods. Movies can eat up a lot of bandwidth especially 4K HDR so being able to provide low latency streaming services to customers could be a welcome addition. I believe the video game industry would see a huge growth of users. Putting gamers on the same LAN would reduce latency and allow for a more immersive experience. The telecommunication company must create a virtual point to point between to edge LSRs. Each VPLS has a unique Virtual Channel Label (VCL) to distinguish between VPLS data flows. Each LSR must setup a LSP to each other LSR in the VPLS mesh. After the creation of the LSPs, the label switch routers proceed learn the addresses of all the other routers in the VPLS mesh. Once the customer premise equipment (CPE) sends the first packet, the first LSR captures the mac address of the customer equipment. The routers create a learning bridge between all of the LSRs with the mac addresses of all the CPE endpoints. The nodes in the middle of the LSPs only forward according to the mac-address. The only node that pays attention to the VCL is the edge routers so it can distinguish the traffic. The downside to the VPLS is it creates an expanded broadcast domain. If an edge router does not have the destination mac address of the target CPE then it floods the mac-address out to all members in the VPLS domain [13]. Utilizing the VPLS solution to connect LANs together has a number of benefits. The first major benefit is cost. Since the customer is purchasing a LAN connection between two sites it works out being cheaper for the telecommunication company. For example if a customer ordered a traditional E-Line service for each site then the telecommunication company will have to charge for ports and optics at both ends. Then the customer will have to purchase routers and firewalls for each site to manage each link. Using a VPLS infrastructure allows the customer to reduce the equipment cost since the customer may not need as many routers and firewalls at each site. A gateway switch will be able to handle all of the switching needed to connect the LANs together. VPLS also minimizes the need for VPNs. People use VPNs to connect remote sites to the headquarters because it provides security. VPNs like IPSEC encrypt the data instead of sending the data in open text where it is vulnerable. Putting the remote site on the same LAN as the headquarters eliminates the need for this technology. All outside connections from the remote sites will go through the central firewall at the main site. After the creation of the MPLS network, the architect will need to focus on security.

Securing the MPLS Network

MPLS services like Virtual private LAN services effectively extends the LANs of customers. Extending the LAN means that there are more chances for an attacker to break into the network. Attacks can range from "intercepting sensitive data to disrupting data, voice, and multimedia services" that can cripple an organization. BGP is the protocol normally used to implement MPLS VPNs. Once the BGP is cracked then the attacker has access to the service provider and customer data. One-step a provider can take to mitigate traffic injection is to separate traffic. Engineers can use BGP communities, route distinguishing or route filtering to separate traffic. These options create a separate routing table in the PE router. When the router creates the separate routing table, the routing decision depends on the interface and not the IP address. Separating the traffic also allows the provider to protect the customer edge traffic because the label edge router makes the decision based on the interface and not any packet information. Another vulnerable spot in the network is the meeting point between the two provider networks. The VRF-to-VRF model is the most secure because it requires the least amount of sharing between providers. The redistribution model does require exchanging label information, which requires the autonomous system border routers to send labeled packets. This border provides an entry point for an attacker to inject traffic. The security policy must be sure that the ASBR only accepts packets with labels that it has advertised. The multihop redistribution model requires the providers to share the most information. Opening up this line of communication allows attackers an entry point into customer VPN information as well as provider VPN information. BGP has multiple vulnerabilities that can allow attacks like "interception of routing information, message replay, message insertion, message deletion, message modification, man-in-the-middle, and denial of service attacks". BGP attacks can be classified into three different categories: route modification, traffic injection, and denial-of-service attacks. Route modification attacks change the traffic paths of packets traversing the provider's network. The traffic path can be modified by modifying the Label edge router labels, modifying VPN labels, abusing BGP update messages, compromising route reflectors, or modifying VRF tables. Injection attacks requires the insertion of traffic into the VPNs. There are two types of injection attacks: injection based on VPN labels and injection based on label edge router labels. Denial of service attacks are attacks that aim to prevent users from using the services. There are four denial of service attacks that BGP is susceptible too. The four attacks are modifying the community attribute in BGP messages, modifying the community attribute of label edge routers, withdrawing BGP routes, and injecting capability advertisements. Mitigating the attacks require that the core be highly secure. The telecommunication provider should have the security policy that denies traffic from outside their network.

Benefits of the MPLS Solution

Utilizing the MPLS protocol opens the door for more diverse traffic engineering options and service delivery. MPLS is partially a layer 2 technology so engineers can avoid some of the downsides of traditional layer 3 protocols. One major downside to routing protocols is limited amount of IPv4 address space. Most of the internet still uses the traditional IPv4 address scheme even though IPv6 can overcome that limitation. The problem with IPv6 is that it is different from traditional IPv4. The underlying technology is different from IPv4 so it requires retraining the engineers to use this space. MPLS can allow customers to stitch their LANs together via tunnels. By stitching their LANs

together, engineers can save their public IPv4 space. Another advantage to MPLS is the router's routing table will shrink in size. MPLS can allow telecommunication companies to use less of their IP space on links to the customer premise. Instead, MPLS can tunnel that traffic at the data link layer to the core. By following this practice steps like static routes will not be necessary to reach the customer LAN.

Downside to the MPLS Solution

Implementing a MPLS solution will increase the complexity of the network when provisioning new circuits and troubleshooting current connections. For example, if a customer wants a layer 2 connection to connect his LANs together the provisioning engineer will need to know things like what protocols the customers want to use across the link and things like MTU. MTU is the maximum size a packet can be before it is subject to fragmentation or drops. MPLS also relies on layer 3 protocols to function so the engineer that is troubleshooting the connection must account for the protocol. The configuration is also more complex. For example, when standing up a layer 2 connection between 2 PE nodes tunnels must be created. If the tunnel characteristics do not match then the tunnel will not establish. Compare this to standing up a layer 3 connection on a traditional IP network. In that scenario, you add the routes into the Interior Gateway Protocol. The interior routes the traffic across the network with minimal configuration. Broadcast storms can also become a problem. VPLS solutions provide a way for customers to extend their layer 2 topology to multiple geographically diverse sites. Traditionally routers act as broadcast domain borders. By extending the layer 2 domain, you will exponentially increase the amount of broadcasts circulating the VPLS cloud. Depending on what protocol the customer is running things like routing updates can flood into the network. Increasing the LAN size will increase the neighbor topology, which in turn will increase the amount of broadcasts sent around the network. The complexity of the VPLS sites can be overwhelming when trying to troubleshoot an issue. If there is an issue at one site good documentation will be key in understanding how this cloud is put together. The administrator will need to know where the exit points are, what cloud this customer is in, etc. The complexity increases if a different provider provides the VPLS. For example, if telecommunication company A is using a VPLS cloud of telecommunication company B to transport its data. The cloud of company B is transparent to company A. If company A is experiencing problems it cannot troubleshoot company B's infrastructure. The extension of the LAN can amplify the effects of a distributed denial of service attack.

Conclusion

The success of the VPLS service package hinges on big companies working in concert with providers. One example is setting up an LAN for schools systems so that all the schools are connected requires. Another example would be if a video game tournament hosting company purchased buildings in different cities in the state and wanted to aggregate them to the same LAN. This would allow gamers to play without the site purchasing a huge pipe to the internet. Also keeping the gaming on the LAN will provide more security than having the traffic exposed to the outside world in multiple locations. In order for telecommunication companies to provide this solution it will need to have a robust fiber network, properly chosen and configured routing protocols, and a MPLS enabled infrastructure.

References

1. Gerstel O, Jinno M, Lord A, Yoo SJB (2012) Elastic optical networking: A new dawn for the optical layer? IEEE Communications Magazine 50: s12-s20.
2. White R, Donohue D (2014) The art of network architecture. Indianapolis, IN: Cisco Systems.
3. Winzer PJ (2012) Optical networking beyond WDM. IEEE Photonics Journal 4: 647-651.
4. Tian DJ, Butler KRB, Choi JI, McDaniel P, Krishnaswamy P (2017) Securing ARP/NDP from the ground up. IEEE Transactions on Information Forensics and Security 12: 2131-2143.
5. Gzara F, Erkut E (2011) Telecommunications network design with multiple technologies. Telecommunication Systems 46: 149-161.
6. Bruno A, Jordan S (2013) CCDA 640-864: Official cert guide. Indianapolis: Cisco Press.
7. Solayman N, El-Sayed A, Badawy M (2017) Improvement of border gateway protocol against failure on autonomous systems. International Journal of Computer Science Issues (IJCSI) 14: 14.
8. Godfrey P, Caesar M, Haken I, Singer Y, Shenker S et al. (2015) Stabilizing route selection in BGP. IEEE/ACM Transactions on Networking (TON) 23: 282-299.
9. Hadjioannou V (2015) On the performance comparison of RIP, OSPF, IS-IS and EIGRP routing protocols.
10. Lawrence J (2001). Designing multiprotocol label switching networks. IEEE Communications Magazine 39: 134-142.
11. Daugherty B, Metz C (2005) Multiprotocol label switching and IP. Part I. MPLS VPNs over IP tunnels. IEEE Internet Computing 9: 68-72.
12. Grayson D, Guernsey D, Butts J, Spainhower M, Shenoi S (2009) Analysis of security threats to MPLS virtual private networks. International Journal of Critical Infrastructure Protection 2: 146-153.
13. Allen D (2004) LESSON 186: Virtual private LAN service. Network Magazine 19: 58. Autonomous Systems & Autonomous System Numbers.