

MPLS-VPN Teknolojisinde Performans Analizi

Berkan Gürbüz, N. Özlem Ünverdi

Yıldız Teknik Üniversitesi

Elektronik ve Haberleşme Mühendisliği Bölümü

İstanbul

yt.ehm.berkangurbuz@gmail.com, unverdi@yildiz.edu.tr

Özet: Bu çalışmada, servis sağlayıcı MPLS (Multiprotocol Label Switching, Çok Protokollü Etiket Anahtarlama) omurgası, GNS3 (Graphical Network Simulator 3, Grafiksel Ağ Simülatörü 3) programı ile modellenerek ikinci katman ve üçüncü katman sanal özel ağlarının benzetimi gerçekleştirilmiştir. Benzetim programı aracılığı ile hizmet sınıfları dahilinde gerçekleştirilen veri haberleşmesi, Wireshark paket izleme programı ile incelenmiştir. Veri, gönderildiği düğüm noktasından ulaşacağı düğüm noktasına gidinceye kadar geçtiği iletim hatlarında incelenerek literatürde iki farklı hizmet sınıfı olarak yer alan sanal özel ağ tiplerinin, müşteri ve servis sağlayıcı açısından maliyet, kaynak ve performans parametreleri temel alınarak karşılaştırılması yapılmıştır. Elde edilen sonuçlarda, ikinci katman sanal özel ağda, omurgadaki yönlendiricilerin kaynaklarının kullanımı açısından servis sağlayıcının ve paket iletim hızı açısından ise müşterinin avantaj sağladığı gözlenmiştir.

1. Giriş

Kurumsal ve son kullanıcı internet kullanımında ortaya çıkan hizmet sınıfı ihtiyacı nedeniyle değişik türde ağ kullanıcılarının gereksinimlerini karşılamak üzere oluşturulmuş kavramsal ve teorik farklılıkları içeren sınıfların oluşumunun merkezinde, IETF (Internet Engineering Task Force, İnternet Mühendisliği Görev Gücü) tarafından geliştirilen çok protokollü etiket anahtarlama protokolü kullanılmaya başlanmıştır.

MPLS teknolojisi, günümüzde kullanılmakta olan varış adresine göre düğümünden düğüme paket iletim yöntemi yerine etiket değiştirerek iletim (label swapping & forwarding) yöntemini getirmiştir. Bu çalışma biçimi, paket iletimi işlemlerini sadeleştirdiğinden veri iletimini hızlandırmakta ve ölçeklenebilirliği artırmaktadır. Bu teknoloji, yönlendirme (routing) işlemini, iletim (forwarding) işleminden ayırdığı için iletim yolunda (forwarding path) hiçbir değişiklik yapılmadan özelleştirilmiş veya değiştirilmiş yönlendirme servislerini uygulanabilir kılmaktadır [1].

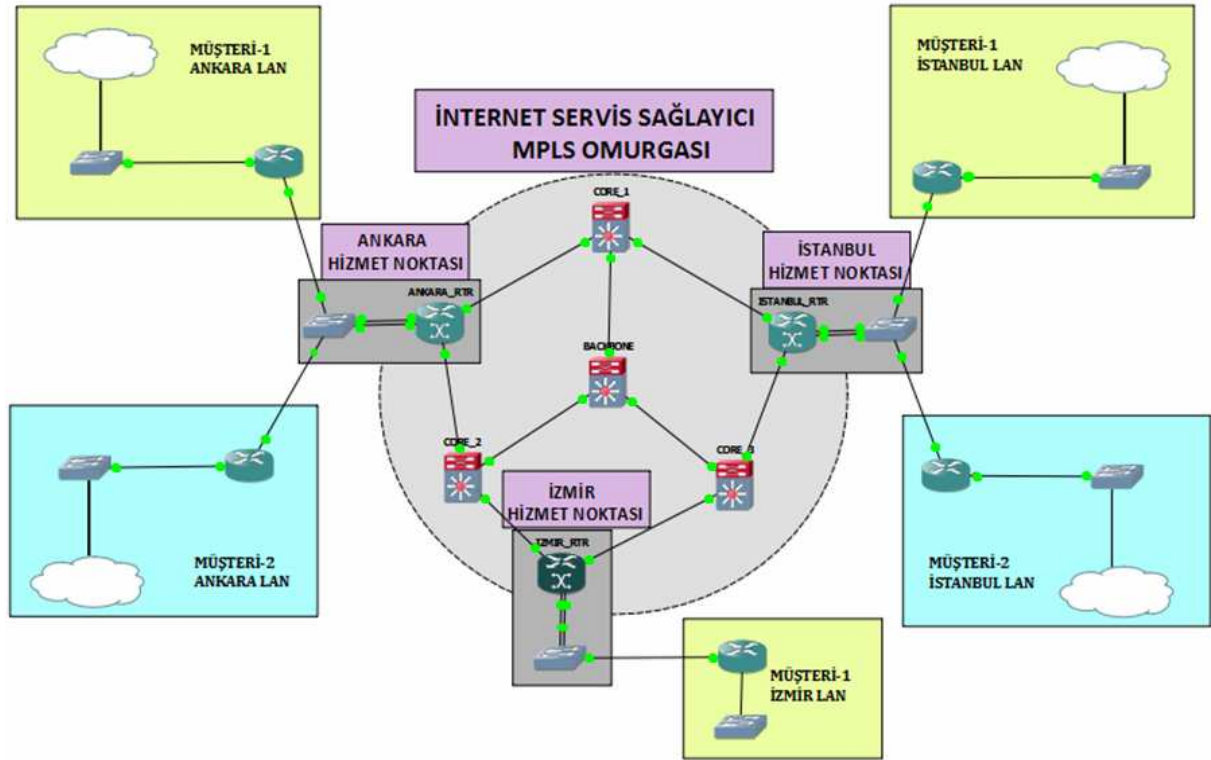
Çok protokollü etiket anahtarlama vasıtasıyla veri bağlantı katmanı ile ağ katmanı arasında bir kontrol katmanı yapısı yaratılmıştır. Bu katman ile paketler, farklı bağlantı yapılarına göre ya da farklı iletim amaçlarına göre gruplandırılmaktadır. Bu amaçla kullanılan etiketlerin birbirleriyle yer değiştirmesi, iç içe geçmesi veya yığınlaşması gibi teknikler sayesinde yönlendirme işlemleri basitleştirilmektedir [2].

Bu çalışmada, çok protokollü etiket anahtarlamanın aktarılmış olan özelliklerinden yararlanılarak oluşturulan sanal özel ağ yapısı, GNS3 programı ile modellenerek benzetimi gerçekleştirilmiştir. Çalışmanın 2. Bölümü'nde, üçüncü katman sanal özel ağ için paket analizi ve 3. Bölümü'nde, ikinci katman sanal özel ağ için paket analizi yapılmıştır. 4. Bölüm'de, elde edilen sonuçlar yorumlanarak değerlendirilmiştir.

2. Üçüncü Katman Sanal Özel Ağda Paket Analizi

Bu bölümde, GNS3 programı kullanılmış ve üç ilde hizmet noktası mevcut olduğu düşünülerek tasarlanan servis sağlayıcı MPLS omurgası, Şekil 1'de İnternet Servis Sağlayıcı MPLS Omurgası isimli çember, üçüncü katman sanal özel ağ hizmeti, Müşteri-1 isimli dikdörtgenler ve ikinci katman sanal özel ağ hizmeti, Müşteri-2 isimli dikdörtgenler ile gösterilmiştir.

Müşteri-1'in lokasyonlarında kullanmakta olduğu ağlar, RIPv2 ile servis sağlayıcının kenar yönlendiricileriyle paylaşılmıştır. Lokasyonlardaki alt ağların bilgileri, servis sağlayıcının Ankara, İstanbul ve İzmir hizmet noktaları arasında kurulmuş olan I-BGP ağıyla paylaşılarak Müşteri-1'in lokasyonlar arası internet protokolü haberleşmesi sağlanmıştır [3, 4].



Şekil 1. Servis sağlayıcı MPLS omurgası ve sanal özel ağ benzetimi.

Şekil 2, Şekil 3 ve Şekil 4’de internet servis sağlayıcının MPLS omurgasındaki kenar etiket anahtarlama yönlendiricilerinin arasında 65000 AS numarasıyla kurulmuş olunan I-BGP komşuluğu gözlenmektedir.

```
ANKARA#sh bgp ipv4 unicast sum
BGP router identifier 204.134.83.1, local AS number 65000
BGP table version is 1, main routing table version 1

Neighbor      V     AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
204.134.83.3  4  65000    79      79       1    0   0 01:14:11      0
204.134.83.101 4  65000    79      79       1    0   0 01:14:16      0
ANKARA#
```

Şekil 2. Ankara yönlendiricisinde I-BGP komşuluğunun ekran çıktısı.

```
İSTANBUL#sh bgp ipv4 unicast sum
BGP router identifier 204.134.83.3, local AS number 65000
BGP table version is 1, main routing table version 1

Neighbor      V     AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
204.134.83.1  4  65000    81      81       1    0   0 01:16:34      0
204.134.83.101 4  65000    81      81       1    0   0 01:16:37      0
İSTANBUL#
```

Şekil 3. İstanbul yönlendiricisinde I-BGP komşuluğunun ekran çıktısı.

```

IZMIR#sh bgp ipv4 unicast summary
BGP router identifier 204.134.83.101, local AS number 65000
BGP table version is 1, main routing table version 1

Neighbor      V     AS  MsgRcvd  MsgSent  TblVer  InQ  OutQ  Up/Down  State/PfxRcd
204.134.83.1   4  65000      83      83        1    0    0  01:18:10        0
204.134.83.3   4  65000      83      83        1    0    0  01:18:09        0
IZMIR#

```

Şekil 4. İzmir yönlendiricisinde I-BGP komşuluğunun ekran çıktısı.

Şekil 5’de yer alan Müşteri-1_Ankara yönlendiricisindeki RIPv2 yönlendirme protokolünün ekran çıktısında, Ankara yönlendiricisinin, İstanbul ve İzmir lokasyonlarında kullanılan yerel alan ağlarına ait internet protokolü bilgisine sahip olduğu görülmektedir.

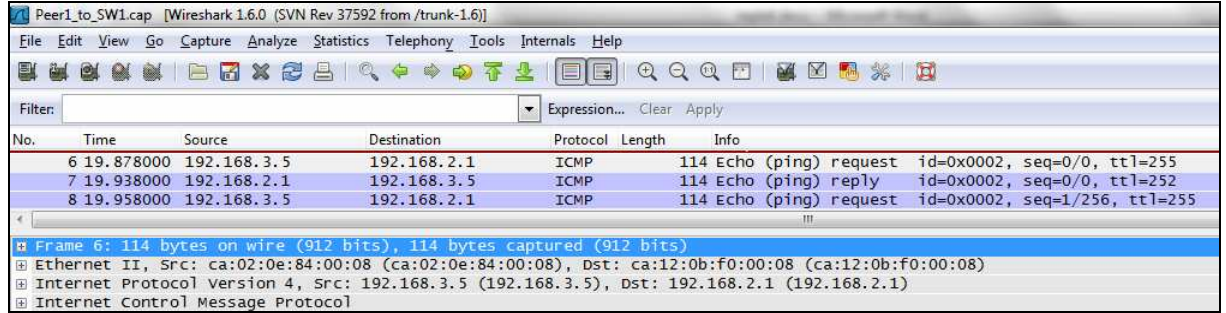
```

Musteri-1_Ank#sh ip route RIP
R    192.168.4.0/24 [120/2] via 192.168.3.6, 00:00:00, GigabitEthernet0/0
R    192.168.2.0/24 [120/2] via 192.168.3.6, 00:00:00, GigabitEthernet0/0
R    192.168.3.0/30 is subnetted, 3 subnets
R      192.168.3.8 [120/1] via 192.168.3.6, 00:00:00, GigabitEthernet0/0
R      192.168.3.12 [120/1] via 192.168.3.6, 00:00:00, GigabitEthernet0/0
Musteri-1_Ank#

```

Şekil 5. Müşteri-1_Ank isimli yönlendiricide RIPv2 yönlendirme tablosunun ekran çıktısı.

Müşteri-1_Ankara yönlendiricisinden İstanbul yönlendiricisine paket gönderilerek analizi yapılmıştır. Şekil 6’da, iletilen paketin ethernet ve internet protokolü başlıklarını alarak Ankara yönlendiricisinden 114 bayt olarak iletim hattına ulaştığı izlenmektedir. Şekil 7’de, Müşteri-1_Ank yönlendiricisinden İstanbul yönlendiricisine gönderilen paketlerin iletim süresinin ortalama olarak 69 ms olduğu gözlenmektedir.



Şekil 6. Müşteri-1_Ank yönlendiricisinden çıkan paketin Wireshark analizi.

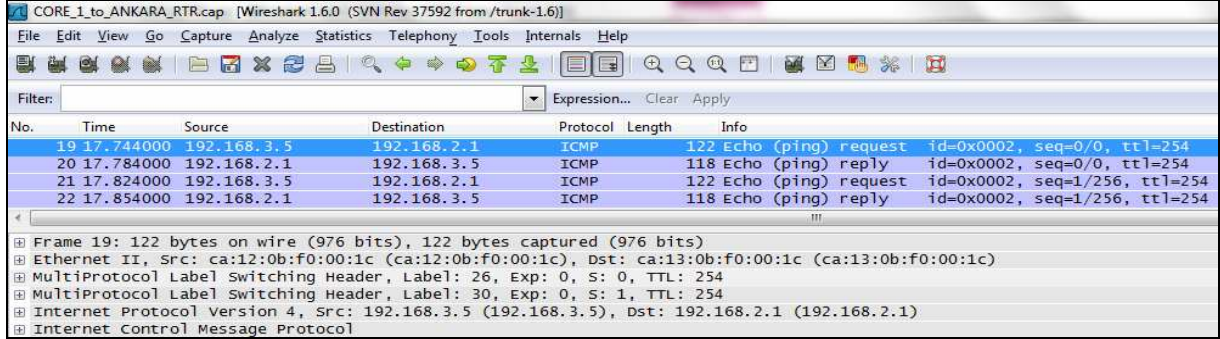
```

Musteri-1_Ank#ping 192.168.2.1 size 1000 repeat 100
Type escape sequence to abort.
Sending 100, 1000-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 40/69/160 ms
Musteri-1_Ank#

```

Şekil 7. Müşteri-1_Ank yönlendiricisinin İstanbul lokasyonuna paket gönderiminin ekran çıktısı.

Şekil 8’de, paket servis sağlayıcı, MPLS omurgasına girdiğinde, iletileceği etiket anahtarlama yolunda etiketin değiştirileceği iki adet yönlendirici bulunması nedeniyle iki adet 4 bayt’lık MPLS başlığının eklenmesiyle 122 bayt’a ulaşarak omurgada ilerlemeye başladığı görülmektedir.



Wireshark 1.6.0 (SVN Rev 37592 from /trunk-1.6) - CORE_1_to_ANKARA_RTR.cap

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
19	17.744000	192.168.3.5	192.168.2.1	ICMP	122	Echo (ping) request id=0x0002, seq=0/0, ttl=254
20	17.784000	192.168.2.1	192.168.3.5	ICMP	118	Echo (ping) reply id=0x0002, seq=0/0, ttl=254
21	17.824000	192.168.3.5	192.168.2.1	ICMP	122	Echo (ping) request id=0x0002, seq=1/256, ttl=254
22	17.854000	192.168.2.1	192.168.3.5	ICMP	118	Echo (ping) reply id=0x0002, seq=1/256, ttl=254

Frame 19: 122 bytes on wire (976 bits), 122 bytes captured (976 bits)

- Ethernet II, Src: ca:12:0b:f0:00:1c (ca:12:0b:f0:00:1c), Dst: ca:13:0b:f0:00:1c (ca:13:0b:f0:00:1c)
- MultiProtocol Label Switching Header, Label: 26, Exp: 0, S: 0, TTL: 254
- MultiProtocol Label Switching Header, Label: 30, Exp: 0, S: 1, TTL: 254
- Internet Protocol Version 4, Src: 192.168.3.5 (192.168.3.5), Dst: 192.168.2.1 (192.168.2.1)
- Internet Control Message Protocol

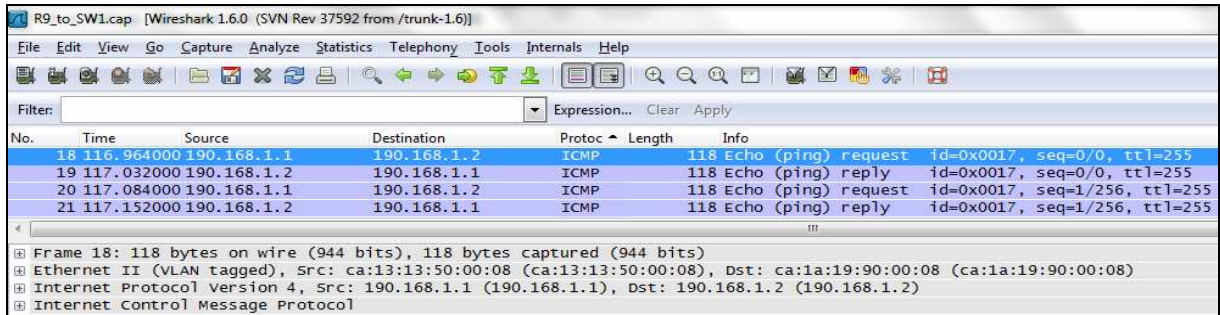
Şekil 8. Omurga Ankara_Rtr yönlendiricisinden çıkan paketin Wireshark analizi.

3. İkinci Katman Sanal Özel Ağda Paket Analizi

Müşteri-2’nin, servis sağlayıcıya fiziksel olarak bağlı bulunduğu hizmet noktalarındaki kenar yönlendiricileri olan Ankara_Rtr ve İstanbul_Rtr arasında ikinci katman sanal devre kurulmuştur [4, 5]. Şekil 9’da, Ankara_Rtr’de sanal devre çalışırılığı, sanal devreye atanmış olan etiketi ve sanal devre numarası görülmektedir.

```
ANKARA#sh mpls l2transport vc 555 detail
Local interface: Gi3/0.20 up, line protocol up, Eth VLAN 20 up
Destination address: 204.134.83.3, VC ID: 555, VC status: up
Next hop: 204.134.83.6
Output interface: Gi1/0, imposed label stack {25 31}
Create time: 01:56:17, last status change time: 01:56:11
Signaling protocol: LDP, peer 204.134.83.3:0 up
MPLS VC labels: local 31, remote 31
Group ID: local 0, remote 0
MTU: local 1500, remote 1500
Remote interface description: *** Musteri-2_VPN ***
Sequencing: receive disabled, send disabled
VC statistics:
packet totals: receive 25, send 41
byte totals: receive 3096, send 5112
packet drops: receive 0, send 0
ANKARA#
```

Şekil 9. Sanal devrenin çalışırılık kontrolünün ekran çıktısı.



Wireshark 1.6.0 (SVN Rev 37592 from /trunk-1.6) - R9_to_SW1.cap

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
18	116.964000	190.168.1.1	190.168.1.2	ICMP	118	Echo (ping) request id=0x0017, seq=0/0, ttl=255
19	117.032000	190.168.1.2	190.168.1.1	ICMP	118	Echo (ping) reply id=0x0017, seq=0/0, ttl=255
20	117.084000	190.168.1.1	190.168.1.2	ICMP	118	Echo (ping) request id=0x0017, seq=1/256, ttl=255
21	117.152000	190.168.1.2	190.168.1.1	ICMP	118	Echo (ping) reply id=0x0017, seq=1/256, ttl=255

Frame 18: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)

- Ethernet II (VLAN tagged), Src: ca:13:13:50:00:08 (ca:13:13:50:00:08), Dst: ca:1a:19:90:00:08 (ca:1a:19:90:00:08)
- Internet Protocol Version 4, Src: 190.168.1.1 (190.168.1.1), Dst: 190.168.1.2 (190.168.1.2)
- Internet Control Message Protocol

Şekil 10. Müşteri-2_Ank yönlendiricisinden çıkan paketin Wireshark analizi.

Müşteri-2_Ankara yönlendiricisinden Müşteri-2_İstanbul yönlendiricisine paket gönderilerek analizi yapılmıştır. Şekil 10'da, iletilen paketin ethernet, sanal yerel alan ağı başlığı (4 bayt) ve internet protokolü başlıklarını alarak Ankara yönlendiricisinden 118 bayt olarak iletim hattına ulaştığı izlenmektedir. Şekil 11'e göre, gönderilen paketin servis sağlayıcı MPLS omurgasına girdiğinde, iletileceği etiket anahtarlama yolunda etiket anahtarlama yapılacak iki adet yönlendirici bulunmasına bağlı olarak iki adet 4 bayt'lık MPLS başlığı ve sanal devrenin kurulduğu yönlendiricilerin arayüzlerinin ethernet başlığının (18 bayt) eklenmesiyle 144 bayt'a ulaşarak omurgada ilerlemeye başladığı belirlenmiştir.

No.	Time	Source	Destination	Protoc	Length	Info
124	101.987000	190.168.1.1	190.168.1.2	ICMP	144	Echo (ping) request id=0x0017, seq=0/0, ttl=255
125	102.037000	190.168.1.2	190.168.1.1	ICMP	140	Echo (ping) reply id=0x0017, seq=0/0, ttl=255
126	102.107000	190.168.1.1	190.168.1.2	ICMP	144	Echo (ping) request id=0x0017, seq=1/256, ttl=255
127	102.157000	190.168.1.2	190.168.1.1	ICMP	140	Echo (ping) reply id=0x0017, seq=1/256, ttl=255

Frame 124: 144 bytes on wire (1152 bits), 144 bytes captured (1152 bits)
Ethernet II, Src: ca:12:27:34:00:1c (ca:12:27:34:00:1c), Dst: ca:11:27:34:00:1c (ca:11:27:34:00:1c)
Multiprotocol Label Switching Header, Label: 25, Exp: 0, S: 0, TTL: 255
PW Ethernet Control word
Ethernet II (VLAN tagged), Src: ca:13:13:50:00:08 (ca:13:13:50:00:08), Dst: ca:1a:19:90:00:08 (ca:1a:19:90:00:08)
Internet Protocol Version 4, Src: 190.168.1.1 (190.168.1.1), Dst: 190.168.1.2 (190.168.1.2)
Internet Control Message Protocol

Şekil 11. Omurga Ankara_Rtr yönlendiricisinden çıkan paketin Wireshark analizi.

Şekil 12'de, Müşteri-2_Ank yönlendiricisinden Müşteri-2_İstanbul yönlendiricisine gönderilen paketlerin iletim süresinin ortalama olarak 64 ms olduğu gözlenmektedir.

```
Muster-2_ANK#ping 190.168.1.2 size 1000 repeat 100
Type escape sequence to abort.
Sending 100, 1000-byte ICMP Echos to 190.168.1.2, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 36/64/156 ms
Muster-2_ANK#
```

Şekil 12. Müşteri-2_Ank yönlendiricisinden Müşteri-2_İst yönlendiricisine paket gönderiminin ekran çıktısı.

4. Sonuçlar

Bu çalışmada, ikinci katman sanal özel ağda, 122 bayt olan üçüncü katman sanal özel ağ paketlerine göre 18 bayt ethernet başlığı ve 4 bayt sanal devre başlığı eklenerek 22 bayt daha büyük bir paket iletiminin gerçekleştirildiği tespit edilmiştir. Buna karşın erişim süreleri konusunda yapılan analizde, aynı düğüm noktalarından geçerek iletilen yüz adet paketin iletim hızlarının ortalamasının, üçüncü katman sanal özel ağ yapısında 69 ms olmasına karşılık ikinci katman sanal özel ağ yapısında 64 ms olduğu belirlenmiştir.

İkinci katman sanal özel ağ hizmetinde her bir pakete, sanal devrenin kurulduğu arayüzlerin ethernet başlığı ve sanal devre başlığının eklenmesiyle 22 bayt'lık ekstra veri yükünün eklendiği gözlenmiştir. Bu yükün ortaya çıkardığı dezavantaja karşın veri haberleşmesinin ikinci katmanda gerçekleşmesinin, paketlerin, hiçbir yönlendirme işlemine tabi olmadan sadece etiket anahtarlama yapıları iletilmesini sağladığı izlenmiştir. Paketlere uygulanan bu iletim biçiminin, yönlendiricinin işlemcisinde geçirilen süreyi azalttığı, ikinci katman sanal özel ağda, omurgadaki yönlendiricilerin kaynaklarının kullanımı ve yönetim kolaylığı açısından servis sağlayıcıya ve paket iletim hızı açısından ise müşteriye avantaj sağladığı görülmüştür.

Kaynaklar

[1]. Griffin T., An Introduction to MPLS, AT&T Research, November 2002.

- [2]. Alway V., Advanced MPLS Design and Implementation, Cisco Press, Indianapolis, A.B.D., September 2001.
- [3]. Yudha A. ve Kuntoro, R., Advanced Routing Introduction to MPLS, Cisco Knowledge Base, Indianapolis, A.B.D., 2003.
- [4]. Grbz B., İkinci Katman MPLS-VPN ve çnc Katman MPLS-VPN'in Karşılaştırmalı Olarak Performans Analizi, Lisans Tezi, Yıldız Teknik Üniversitesi, Elektrik-Elektronik Fakltesi, Elektronik ve Haberleşme Mhendisliği Blm, İstanbul, Trkiye, 2012.
- [5]. Pepelnjak I. ve Guichard J., MPLS and VPN Architectures, Cisco Press, Indianapolis, A.B.D., 2001.