
GAZİ ÜNİVERSİTESİ
Gazi
1926

NESNELERİN İNTERNETİ İÇİN KURUMSAL AĞLARDA İYİLEŞTİRMELER

Muhammed Fırat EREL

YÜKSEK LİSANS TEZİ
ELEKTRİK ELEKTRONİK MÜHENDİSLİĞİ ANA BİLİM DALI

GAZİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

MAYIS 2023

ETİK BEYAN

Gazi Üniversitesi Fen Bilimleri Enstitüsü Tez Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmasında;

- Tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi,
- Tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu,
- Tez çalışmasında yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi,
- Kullanılan verilerde herhangi bir değişiklik yapmadığımı,
- Bu tezde sunduğum çalışmanın özgün olduğunu,

bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

Muhammed Fırat EREL

02/05/2023

NESNELERİN İNTERNETİ İÇİN KURUMSAL AĞLARDA İYİLEŞTİRMELER

(Yüksek Lisans Tezi)

Muhammed Fırat EREL

GAZİ ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

Mayıs 2023

ÖZET

Endüstri 4.0 devrimi ile birlikte halihazırda kurumların haberleşme altyapısını sağlayan bilgisayar ağları internetin nesnelerinin haberleşmesi amacıyla da kullanılır. Bina yönetim sistemleri, akıllı üretim sistemleri, otonom araçlar, endüstriyel otomasyon ve kontrol sistemleri gibi hemen her alanda vazgeçilmez hale gelen nesnelerin interneti teknolojileri birçok farklı teknolojiyi kapsarlar. Kurulan iletişim yöntemleri kullanım ve gereksinim yönleriyle geleneksel bilgisayar iletişim yöntemlerinden farklılıklar gösterir. Nesnelerin interneti teknolojileri ürettikleri verilerle kendi aralarında ve sunucu sistemleriyle iletişim kurarlar. Nesnelerin interneti teknolojileri yapılarına ve gereksinimlerine göre kurumsal ağlara dahil olurlar. Kurumsal ağlar, bilgisayarlar için tasarlanmış ve kısıtlı işlem kapasitesi veya yüksek mobilite gibi farklı gereksinimleri olan nesnelerin interneti teknolojilerinin iletişimi hususunda belirli uyumsuzluklar görülür. Bu tez çalışmasında kurumsal ağların mevcut yapıları ile nesnelerin interneti teknolojilerinin ağ gereksinimleri iyileştirme önerileri irdelenmiştir. Çalışmanın hedefi maliyet etkin olarak mevcut ağ mimarisi ve cihaz yapılandırması konusunda önerilerde bulunmaktır. Mevcut ağ mimarisi ile önerilen mimariler nesnelerin interneti ağ gereksinimleri alanlarında karşılaştırmalı olarak incelenmiştir.

Bilim Kodu	:	90501
Anahtar Kelimeler	:	Nesnelerin İnterneti, Kurumsal Ağlar, İnternet Protokolü
Sayfa Adedi	:	69
Danışman	:	Prof. Dr. Nursel AKÇAM

INTERNET OF THINGS OPTIMIZATION IN ENTERPISE NETWORKS

(M. Sc. Thesis)

Muhammed Fırat EREL

GAZİ UNIVERSITY

GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

May 2023

ABSTRACT

With the Industry 4.0 revolution, computer networks that currently provide the communication infrastructure of enterprises are also used for the communication of things of internet. Internet of things technologies, which have become indispensable in almost every field such as building management systems, smart production systems, autonomous vehicles, industrial automation and control systems, cover many different technologies. Established communication methods differ from traditional computer communication methods in terms of usage and requirements. IoT technologies communicate with each other and with server systems with the data they produce. IoT technologies are included in corporate networks according to their structures and requirements. Certain incompatibilities exist with regard to the communication of IoT technologies that are designed for corporate networks computers and have different requirements, such as limited processing capacity or high mobility. In this thesis, the existing structures of corporate networks and the suggestions for improving the network requirements of IoT technologies are examined. The aim of the study is to make recommendations on the current network architecture and device configuration in a cost-effective manner. The current network architecture and the proposed architectures will be examined comparatively in the areas of internet of things network requirements.

Science Code	:	90501
Key Words	:	Internet of things, enterprise networks, internet protocol
Page Number	:	69
Supervisor	:	Prof. Dr. Nursel AKÇAM

TEŞEKKÜR

Çalışmalarım boyunca değerli yardım ve katkıları ile beni yönlendiren tez danışmanım Prof. Dr. Nursel AKÇAM ve bölüm hocalarıma teşekkürlerimi sunuyorum.

Hayatım boyunca akademik çalışmalarımda beni cesaretlendiren ve teşvik eden sevgili annem, babam ve kardeşim Beste'ye teşekkürlerimi sunuyorum.

Valıklarıyla, maddi ve manevi destekleri ile hep yanımda olan çok değerli eşim Şule'ye ve oğlum Mete'ye teşekkürlerimi sunuyorum.

İÇİNDEKİLER

Sayfa

ÖZET iv

ABSTRACT v

TEŞEKKÜR vi

İÇİNDEKİLER vii

ÇİZELGELERİN LİSTESİ ix

ŞEKİLLERİN LİSTESİ x

SİMGELER VE KISALTMALAR xiii

1. GİRİŞ 1

2. NESNELERİN İNTERNETİ VE KURUMSAL AĞLAR 5

2.1. Nesnelerin İnterneti 5

2.1.1. Nesnelerin internetinin tarihçesi 5

2.1.2. Nesnelerin internetinin bileşenleri 6

2.2. Temel Ağ Kavramları 6

2.2.1. İnternet protokolü 10

2.2.2. Ethernet 11

2.2.3. Wi-Fi 11

2.3. Kurumsal Ağlar 12

3. KURUMSAL AĞLARDA İYİLEŞTİRME ÖNERİLERİ 15

3.1. Kurumsal Ağlarda ile Nesnelerin İnterneti Ağları Arası Uyumsuzluklar 15

3.2. Genel İyileştirme Yöntem Önerisi 15

3.3. Kablolu Yerel Alan Ağları İçin İyileştirme Önerileri 17

3.3.1. Segmentasyon 17

3.3.2. QoS 19

Sayfa

3.3.3. NAC 20
3.3.4. Kapsayan ağaç protokolü 22
3.3.5. Tek yol kullanımı ve farklı çoklu yol kullanım karşılaştırması 24
3.4. Wi-Fi Kablosuz Ağlar için İyileştirme Önerileri 26
3.5. Yazılım Tanımlı Ağlar 27
3.5.1. SD access 29
3.5.2. SD WAN 29
3.5.3. SDDC 29
4. TEST VE BULGULAR 31
4.1. STP Simülasyonu 33
4.1.1. Tek hat STP simülasyonu 34
4.1.2. Yük dengelenmiş STP simülasyonu 41
4.2. QoS Simülasyonu 46
4.2.1. QoS yapılandırma öncesi trafik simülasyonu 48
4.2.2. QoS yapılandırma sonrası trafik simülasyonu 53
4.3. STP-QoS Birleşik Kullanım Simülasyonu 58
5. SONUÇ VE ÖNERİLER 63
KAYNAKLAR 65
ÖZGEÇMİŞ 69

ÇİZELGELERİN LİSTESİ

Çizelge **Sayfa**

Çizelge 2.1. 7 Katmanlı OSI Mimarisi 7

Çizelge 3.1. Örnek IoT Cihazları Ağ Gereksinim Listesi 17

Çizelge 3.2. Farklı IoT Trafiklerinin Bant Genişliği Tüketimi 27

Çizelge 3.3. 802.11 Kablosuz Ağ Özellikleri 27

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

Şekil 2.1. 7 Katmanlı OSI Modeli ve 4 Katmanlı TCP/IP Modeli Karşılaştırması..... 10

Şekil 2.2. IPv4 ve IPv6 Paket Yapısı Karşılaştırması..... 11

Şekil 2.3. Basitleştirilmiş Örnek Kurumsal Ağ 13

Şekil 2.4. Bilişim Teknolojileri ve Operasyon Teknolojileri Kullanım Alanları 14

Şekil 3.1. IoT Odaklı Ağ Tasarım ve Yapılandırma Çalışması..... 16

Şekil 3.2. Endüstriyel ve Kurumsal Ağ Segmentasyonu..... 18

Şekil 3.3. Servis Kalitesi Bant Genişliği Yönetimi 19

Şekil 3.4. IoT Odaklı Ağ Tasarım ve Yapılandırma Çalışması..... 20

Şekil 3.5. Örnek Yerel Alan Ağ Bağlantıları 23

Şekil 3.6. Yük Dengelenmemiş Tek Yol Kullanımı..... 24

Şekil 3.7. Otomatik Atanmış Yük Dengelenmiş Yol Kullanımı 25

Şekil 3.8. Yapılandırılmış Çoklu Yol Kullanımı..... 25

Şekil 3.9. Geleneksel Ağ ve Yazılım Tanımlı Ağ Modeli Karşılaştırması 28

Şekil 4.1. STP Simülasyon Topolojisi..... 33

Şekil 4.2. Ostinato IoT Paket Üreteci..... 34

Şekil 4.3. Ostinato Kurumsal Paket Üreteci..... 35

Şekil 4.4. Sw4 Ağ Anahtarı Vlan 1 STP Durumu..... 36

Şekil 4.5. Sw4 Ağ Anahtarı Vlan 201 STP Durumu..... 36

Şekil 4.6. STP Simülasyon İzleme Noktaları 37

Şekil 4.7. IoTGenerator ile Sw1 Arası UDP Paket Akışı..... 38

Şekil 4.8. Sw1 ile Sw2 Arası Kurumsal ve IoT Trafik Akışı 39

Şekil 4.9. Sw4 ile IoT Server Arası IoT Trafik Akışı 40

Şekil **Sayfa**

Şekil 4.10. Sw3 Vlan 201 STP Yük Dengeleme Yapılandırması 41

Şekil 4.11. Sw4 STP Yük Dengeleme Hata Ayıklama Çıktısı 41

Şekil 4.12. Yük Dengelenmiş STP Simülasyon İzleme Noktaları 42

Şekil 4.13. IoTGenerator ile Sw1 Arası Ağ Trafiği 43

Şekil 4.14. Sw1 ile Sw2 Arası Ağ Trafiği 44

Şekil 4.15. Sw1 Hız Kısıtlama İstatistik Çıktısı 45

Şekil 4.16. Sw4 ile IoT Server Arası Ağ Trafiği 45

Şekil 4.17. QoS Simülasyonu Ağ Topolojisi 46

Şekil 4.18. Ostinato IoT Paket Üreteci 47

Şekil 4.19. Ostinato Kurumsal Paket Üreteci 48

Şekil 4.20. R1 Ağ Yönlendirici QoS Politikaları 48

Şekil 4.21. R1 Ağ Anahtarı f1/0 ve f1/1 Arayüz Yapılandırması 49

Şekil 4.22. QoS Simülasyonu İzleme Noktaları 49

Şekil 4.23. Ostinato Paket Üreteçlerinin Anlık İletim Hızları 50

Şekil 4.24. R1 Ağ Yönlendiricisi f1/0 Arayüzü QoS Politika Çıktısı 51

Şekil 4.25. IoTGenerator ile Sw1 Arası Ağ Trafiği 52

Şekil 4.26. R1 ile Sw2 Arası Ağ Trafiği 53

Şekil 4.27. Ağ Tabanlı Uygulama Tanıma Yapılandırması 54

Şekil 4.28. R1 QoS Politika Yapılandırması 54

Şekil 4.29. R1 Ağ Yönlendiricisi f0/0 ve f1/0 QoS Arayüz Yapılandırması 54

Şekil 4.30. R1 QoS f1/0 Arayüz İstatistiği 55

Şekil 4.31. IoTGenerator ile Sw1 Arası İzlenen Trafik 56

Şekil 4.32. Sw1 ile Sw2 Arası Ağ Trafiği 57

Şekil 4.33. STP-QoS Bütünsel Kullanım Simülasyon Ağ Topolojisi 58

Şekil **Sayfa**

Şekil 4.34. CriticalIoTGenerator ile Sw1 Arası Ağ Trafiği 59

Şekil 4.35. IoTGenerator ile Sw2 Arası Ağ Trafiği 59

Şekil 4.36. CriticalIoTGenerator ile Sw1 Arası Ağ Trafiği 60

Şekil 4.37. Sw4 ile Server Arası Ağ Trafiği..... 60

Şekil 4.38. CriticalIoTGenerator ile Sw1 Arası Ağ Trafiği 62

Şekil 4.39. IoTGenerator ile Sw2 Arası Ağ Trafiği 62

Şekil 4.40. CriticalIoTGenerator ile Sw1 Arası Ağ Trafiği 63

Şekil 4.41. Sw4 ile Server Arası Ağ Trafiği..... 63

SİMGELER VE KISALTMALAR

Bu çalışmada kullanılmış simgeler ve kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

Simgeler	**Açıklamalar**
Gbps	Giga Bits Per Second
GHz	Gigahertz
Kbps	Kilo Bits Per Second
Mbit	Megabit
Mbps	Mega Bits Per Second
MHz	Megahertz
ms	Millisecond

Kısaltmalar	**Açıklamalar**
ACL	Access Control List
AD	Active Directory
AGV	Automatic Guided Vehicle
API	Application Programming Interface
ATM	Asynchronous Transfer Mode
Bacnet	Building Automation and Control Networks
BMS	Building Management System
CEO	Chief Executive Officer
CIP	Common Industrial Protocol
DHCP SPAN	Dynamic Host Configuration Protocol Switch Port Analyzer
DNS	Domain Name System
DSL	Digital Subscriber Line
GNS3	Graphical Network Simulator 3

Kısaltmalar	Açıklamalar
HMI	Human Machine Interface
HTTP	Hyper Text Transfer Protocol
HVAC	Heating Ventiliation and Air Conditioning
IACS	Industrial Automation and Control System
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronics Engineers
IIoT	Industrial Internet of Things
IO	Input Output
IoT	Internet of Things
IP	Internet Protocol
IPsec	Internet Protocol Security
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
IT	Information Technologies
ITU	International Telecommunication Union
L2TP	Layer Two Tunneling Protocol
LAN	Local Area Network
LLC	Link Layer Control
LLDP	Link Layer Discovery Protocol
MAC	Media Access Control
MIT	Massachusetts Institute of Technology
MPLS	Multi Protocol Label Switching
MSTP	Multi Spanning Tree Protocol
NAC	Network Access Control
NBAR	Network Based Application Recognition

Kısaltmalar	Açıklamalar
OSI	Open Systems Interconnection
OT	Operational Technologies
PLC	Programmable Logic Controller
PoE	Power Over Ethernet
PPP	Point to Point Protocol
Profinet	Process Field Network
PVST+	Enhanced Per Vlan Spanning Tree Protocol
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RSTP	Rapid Spanning Tree Protocol
SCADA	Supervisory Control and Data Acquisition
SD	Software Defined
SDDC	Software Defined Data Center
SDN	Software Defined Network
SD-WAN	Software Defined Wide Area Network
SNMP	Simple Network Management Protocol
STP	Spanning Tree Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAN	Wide Area Network
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network

1. GİRİŞ

Günümüz dünyasında insanların hayatlarının kolaylaştırılması, zaman ve enerji tasarrufu sağlanması ve katma değeri daha yüksek olan işlerin yapılabilmesi adına birçok işin makineler tarafından ya da makineler yardımıyla yapılması sağlanmaktadır. Makinelerin bu işleri daha etkin yapabilmeleri için sunucular kendi aralarında haberleşirler. Örneğin bir makine arızalanma belirtileri gösterdiği anda ilgili sunuculara göndereceği veriler anlamlandırılarak makinenin kendi bakımını yapması ve arızasını gidermesi sağlanır. Yine benzer işleri yapan birden çok makine birbirleri ile haberleşerek iş bölümü yapabilir. Endüstriyel sistemler fabrikaların kesintisiz üretim yapabilmesi esasına dayanarak tasarlanırlar. Son günlerde giderek artan üretim ihtiyaçları, endüstriyel sistemlerin birbirleri arasında ve merkezi sunucularla haberleşmesini zorunlu kılmaktadır. Örneğin endüstriyel işletmelerde mevcut olan bilgi teknolojileri ağları ile operasyon teknolojileri ağları arasında haberleşmenin sağlanması gerekliliği sık sık ortaya çıkar. Üretimde kullanılan operasyon cihazlarının daha etkin kullanımı için merkezi bir sisteme veri iletmesi, bu verilerin yorumlanarak özet bilgiler sunabilmesi ve bu veriler ışığında cihazların davranışını kontrol etmesi bir nesnelerin interneti (Internet of Things - IoT) örneğidir. Ancak IoT sistemlerinin geleneksel bilgi teknolojileri ağları üzerinden veri iletmesinde bazı önemli sorunlar ortaya çıkmaktadır. Bu tür sorunların önüne geçilmesi adına geleneksel bilgi teknolojileri ağlarında iyileştirmeler yapılması gerekir.

IoT sistemleri Internet Protokol (IP) tabanlı ve IP tabanlı olmayan olarak ikiye ayrılabilir. IP tabanlı sistemler, IP kameralar; akıllı ısıtma, havalandırma ve iklimlendirme (Heating, Ventilation & Air Conditioning – HVAC) sistemleri, akıllı batarya yönetim sistemi (Battery Management System – BMS), IP telefonlar ve akıllı aydınlatma sistemleri gibi doğrudan geleneksel IP tabanlı ağlara bağlanabilir şekilde üretilirler. IP tabanlı sistemlerin bir kısmı kablolu ethernet teknolojilerini kullanırken bir kısmı Wi-Fi teknolojisini kullanırlar. Organizasyonlar IoT sistemlerinin ağ altyapılarını oluştururken maliyeti en aza indirgemek için mevcut ağ altyapılarını kullanmayı tercih ederler. Ancak IoT sistemlerin ağ gereksinimleri mevcut kurumsal ağların yapılarına göre değişkenlikler göstermektedir. Bu gereksinimlerden en önemli olanlar düşük gecikme, yeterli bant genişliği, yüksek mobilite ve topolojik uyumluluklar olarak düşünülebilir. Örneğin uzaktan kontrol edilen bir endüstriyel otomasyon sistemi için yeterli bant genişliği ve gerçek zamanlı iletişim kurmak, diğer bir değişle düşük gecikme çok önemlidir. Böyle bir kurguda ağda yaşanabilecek

gecikmeler üretim hattının işlevsizleşmesine neden olur. Otomatik yönlendirmeli araçlar çok hızlı yer değiştirirler.

Kablosuz ağlara bağlı oldukları için bir kablosuz ağ erişim noktasından diğer kablosuz ağ erişim noktasının kapsama alanına geçerken veri kaybının olmaması önemlidir. Farklı IoT sistemler farklı ağ gereksinimlerine ihtiyaç duyar. Örneğin IP kamera sistemlerinin sayıları arttıkça ağın belli bölümlerinde daha yüksek bant genişliği kullanılır. Bu bant genişliği, düşük gecikme ve düşük gecikme değişimi gereksinimleri karşılanmadığında kamera görüntülerinde bozulma sorunları olur. Benzer biçimde, sürekli hareket halinde veri giriş işlemlerinde kullanılan kablosuz bir tablet için yeterli bant genişliği ve düşük gecikmeden daha önemli olan hareket esnasında ağ bağlantısının kesintisiz çalışması önemlidir.

Yapılan literatür araştırmalarında üretim, finans, lojistik, sağlık, eğitim, tarım gibi çok farklı alanlarda kullanılan IoT sistemleri ile ilgili yayınların son yıllarda giderek arttığı gözlemlenmiştir. Elektrik ve Elektronik Mühendisleri Enstitüsü (Institute of Electrical and Electronics Engineers – IEEE) gibi küresel yayınların yanında ülkemizde de IoT sistemleri hakkında çok sayıda bilimsel çalışma yapılmaktadır. Bu tez çalışmasının odağı olan kurumsal ağlarda IoT sistemler için yapılan iyileştirmeler ve geliştirmelerle birçok küresel ve yerli yayın incelenmiştir. Şimdiye kadar yapılan bilimsel çalışmalarda genel olarak IoT sistemler için ağ iyileştirmelerinde ağ sistemlerindeki cihazlarda ya da protokollerde geliştirilmeler önerilmiş, yoğun olarak kablosuz ağ ve güvenlik konularına odaklanılmıştır. Mevcut yerel alan ağ teknolojilerinin kullanımı ile maliyet etkin çözümlere dair kapsayıcı çalışmaların sayısı azdır. Bu tez çalışmasında gecikmeye toleransı düşük olan IoT sistemlerin yerel alan ağlarındaki mevcut teknolojilerin kullanılarak maliyet etkin ağ iyileştirme önerileri ile literatüre katkı sağlanması hedeflenmiştir.

Tez çalışmasında IoT sistemleri için kurumsal ağlarda bazı tasarımsal ve yapısal konular üzerinde incelemeler yapılmıştır. Öncelikle gereksinimleri farklılaşan cihazların farklı gruplarda ele alınması için segmentasyon konusuna değinilmiştir. Devamında bu gereksinimlerin önceliklendirilmesi için servis kalitesinde yapılabilecek iyileştirmelere değinilmiştir. İyileştirmelere güvenlik ve segmentasyon açısından katkı sağlayan ağ erişim kontrol sistemlerindeki yapılandırmalar incelenmiştir. Geleneksel kurumsal ağlarda kısırdöngü engelleme sistemi olan kapsayan ağaç protokolleri üzerinde yapılabilecek iyileştirme önerileri irdelenmiştir. İnternetin nesneleri için kablolu bağlantılara nazaran çok

yüksek esneklik sağlayan kablosuz ağlar incelenmiştir. Son olarak elle yapılan tüm değişikliklerin otomasyonunun sağlanması ve sürekli ağın izlenerek ağ yöneticisinin müdahalesine gerek kalmadan ağdaki düzenlemelerin yapılması için yaygın olarak kullanılan yazımlı tanımlı ağ teknolojilerine değinilmiştir.

Simülasyon ortamında IoT sistemlerinin kullandığı kullanıcı veribloğu iletişim kuralları (User Datagram Protocol – UDP) paketlerle IT (Information Technology) ağları üzerinde değişiklikler yapılarak performans ölçümleri yapılmıştır. Yapılan performans ölçümlerinin çıktıları karşılaştırarak önerilen yapılandırmaların doğruluğu kontrol edilmiştir.

Bu tez çalışmasında internetin nesnelerinin kurumsal ağları kullanırken daha etkin çalışmalarını sağlamak için tasarımsal ve yöntemsel önerilerde bulunulmuştur. Birinci bölümde çalışmanın amacı ve kapsamı tanımlanmıştır. Tezin ikinci bölümünde genel ağ bilgileri, kurumsal ağlar ve nesnelerin interneti hakkında temel bilgiler verilmiştir. Tezin üçüncü bölümünde kurumsal ağ yapılarında yapılabilecek tasarımsal ve yapısal değişikliklerle nesnelerin interneti teknolojilerinin ağda daha performanslı çalışmasını sağlamak amaçlanmıştır. Dördüncü bölümde önerilen yöntemlerden bazılarının simülasyon ortamında uygulama öncesi ve sonrası sonuçları karşılaştırılmıştır.

2. NESNELERİN İNTERNETİ VE KURUMSAL AĞLAR

2.1. Nesnelerin İnterneti

Günümüzde internet hayatımızın her alanına girmiş durumdadır. İnternet önceleri bilgi paylaşımı ve haberleşme aracı olarak kullanılsa da bugün eğitim, iş, bankacılık ve eğlence sektörü gibi birçok alanda vazgeçilmez durumdadır. Gelişen ağ ve taşınabilir cihaz teknolojileriyle birlikte internete bağlı olan cihaz sayısı gün geçtikçe artmaktadır.

IoT, güncel teknolojiler arasında üst sıralarda yer almakta olup, Türkçe'de "Nesnelerin İnterneti" olarak ifade edilmektedir. Buradaki nesne kavramı birçok elektronik cihazı kapsamaktadır. Elektronik nesnelerin ağ iletişimi kurarak veri alışverişinde bulunduğu ve yazılımlarla akıllandırılmış sistemlere genel olarak IoT denilir. IoT sistemlerin kullanım amaçları, kullanıldığı alanlara göre değişiklik göstermektedir. Örneğin endüstriyel sistemlerdeki uygulama amaçlarından biri cihazlara müdahale ve takibin en düşük seviyeye indirgenerek yüksek verimli, hızlı ve kendini idare edebilen sistemlerin oluşturulmasıdır. Bu seviyede kullanışlı ve yüksek verimli sistemler ev kullanıcılarının yanı sıra, gün geçtikçe işletmelerin vazgeçilmez teknolojileri olmaktadır.

2.1.1. Nesnelerin internetinin tarihçesi

Cambridge Üniversitesi'ndeki bir akademisyen grubunun kahve makinesinin çalışma durumunu izlemek için 1991'de kurdukları kamera sistemi nesnelerin internetinin başlagıcı olarak varsayılır. İlerleyen dönemde 1999'da MIT Auto-ID Laboratuvarı tarafından IoT kavramı ortaya atılmış, 2005 yılında Uluslararası Telekomünikasyon Birliği (International Telecommunication Union - ITU)'nun konuya dair ilk raporunu yayımlaması ve 2009 yılında IBM'in CEO'su Samuel J. Palmisano tarafından Smart Planet kavramının önerilmesi ile ilgi odağı haline gelmiştir [1]. Bu süreçlerin ardından IoT teknolojisi her geçen gün gelişmektedir. Bilgisayar ve internet teknolojilerinin ardından üçüncü dalga dünya endüstrisi olarak kabul edilmektedir. Nesnelerin interneti endüstriyel işletmelerin yanı sıra birçok alanda farklı sektörde kullanılmaktadır. Bunlardan en önemlileri tarım endüstrisi, enerji endüstrisi, ev otomasyon sistemleri ve sağlık sistemleri şeklindedir. Her sektörde kullanılan sensör tipleri, eyleyiciler ve mimari tasarım değişiklik gösterse de temel ihtiyaçlar ve çözümler benzerlik göstermektedir.

2.1.2. Nesnelerin internetinin bileşenleri

Nesnelerin interneti bulunduğu ortamdan, cihazlardan ve diğer birçok değişkenden bilgi toplayan, topladığı bilgileri işleyebilen ve ağ üzerinden aktarabilen nesnelerden oluşur. Bu bileşenler sensörler, eyleyiciler ve denetleyiciler olmak üzere üç ana kategoride incelenir.

Sensörler gerçek dünyadaki fiziksel ölçümlerin nicemlenmesini sağlayan cihazlardır. Sıcaklık, basınç, ışık, nem, hareket veya diğer fiziksel değişkenlerin ölçülmesinde kullanılırlar. Sensörler güç kaynağı gereksiniminin durumlarına göre aktif ve pasif olmak üzere ikiye ayrılırlar. Çalışması için bir güç kaynağına gerek duymayan sensörler pasif, güç kaynağı olmadan çalışamayan sensörler aktif olarak sınıflandırılırlar. IoT dünyasında sensörler ölçümlerden veri üretebilen kısıtlı veri işleme gücüne sahip cihazlardır.

Eyleyiciler elektrik sinyallerini eyleme çevirmeyi sağlayan cihazlardır. Sensörlerin tersine veri toplamak yerine toplanmış verilerin yorumlandıktan sonra eyleme dönüşmesi gereken noktalarda devreye girerler. Bu eylemler doğrudan bir hareket, bir cihazın çalışmasının başlatılması ya da değiştirilmesi veya bir bilgilendirme ya da ikaz ışığının yakılması olabilir. Eyleyiciler elektrik, termal, hidrolik veya pnömatik türde olabilir. Eyleyiciler gelen komutları yorumlamadan işleme alırlar.

Denetleyiciler ise sensörlerden gerekli verilerin toplanması, ağ ortamında merkezi sunuculara iletilmesi veya verilerin yorumlanarak eyleme dönüştürülmesi için eyleyicilere komut gönderilmesi işlemlerini yaparlar.

IoT sistemlerinin başlangıç noktası sensörler ya da uygulamalardan çok ağ bağlantıları olarak düşünülmelidir [2].

2.2. Temel Ağ Kavramları

Uluslararası Standartlar Teşkilatı (International Organization for Standardization - ISO) tarafından geliştirilen açık sistemler ara bağlantısı (Open Systems Interconnection - OSI) modeli ağ bağlantısı yapabilen cihazların birbirleriyle kuracakları iletişim standartlarını tanımlar. 1984'de son hali ISO tarafından yayınlanan standart kısa sürede kabul görmüş, ağ modellemesi için temel olarak ele alınmıştır.

Çizelge 2.1. 7 Katmanlı OSI Mimarisi

Katman		Veri birimi	İşlev	Örnekler
Sunucu katmanları	7. Uygulama	Veri	Kullanıcı-bilgisayar iletişimi bu katmanda sağlanır, bu katmanda uygulamaların ağa erişimi sağlanır.	Uzaktan Dosya Erişimi, elektronik mesajlaşma, dosya aktarımı, ağ yönetimi
	6. Sunum		Verinin iletim için kullanılabilecek şekle getirilmesi bu katmanda sağlanır.	Sıkıştırma/açma, şifreleme/şifre çözme, kodlama dönüştürme
	5. Oturum		Uç düğümler arası oturumların açılması, devamlığı ve kapatılması bu katmanda sağlanır.	API, WinSock
Ortam katmanları	4. Taşıma	Bölüt	Verinin iletim hata kontrolü, bölütlerin sıralanması gibi işlemler bu katmanda sağlanır.	TCP, UDP
	3. Ağ	Paket	Veri paketlerinin farklı alt ağlardaki uç düğümler arasında yönlendirilmesi bu katmanda sağlanır.	AppleTalk, ICMP, IPsec, IPv4, IPv6
	2. Veri bağlantı	Çerçeve	Verinin hata kontrolü yapılarak mantıksal iletişime dönüştürülmesi bu katmanda sağlanır.	IEEE 802.2, L2TP, LLDP, MAC, PPP, ATM, MPLS
	1. Fiziksel	Bit	Fiziksel ortam üzerinden verinin aktarılma işlemi bu katmanda sağlanır.	DSL, Ethernet Fiziksel Katman, ISDN, RS-232

OSI modeli ağ sistemlerinin mimari modellemesini 7 katmanda açıklar. Her katman bir üst katman için altyapı sağlar. İki bilgisayar iletişim kurarken eş düzey katmanlar arası doğrudan iletişim oluşmaz, ancak eş katmanlar arası sanal iletişim kurulur. Katmanlı mimari sayesinde her katman için standartlara uygun geliştirilen farklı teknolojiler kullanılabilir ve bu teknolojilerin değişimi halinde iletişim bütünlüğü sağlanır. Ortam katmanları olarak gruplandırılan ilk dört katman ağ teknolojilerini doğrudan ilgilendirir. Ortam katmanlarında verinin hangi ortamda iletileceği, anahtarlamanın, yönlendirmenin nasıl yapılacağı ve ağda taşınırken ne tür kontrollerin yapılacağı ve hizmet kalitesinin nasıl artırılacağı belirlenir. Oturum, sunum ve uygulama katmanlarından oluşan sunucu katmanları ise uygulama teknolojilerini ilgilendirir. Çizelge 2.1'de OSI mimarisideki katmanların işlevleri ve örneklerinden bahsedilmektedir.

En alt katman olan fiziksel katmanda verinin hangi ortam üzerinden aktarılacağı bilgisi mevcuttur. Bu ortam elektriksel kablo, fiber optik kablo veya radyo dalgalarının iletileceği hava olabilir. Bu katmanda anahtarlama ya da yönlendirme gibi bir işlem yapılmaz. Yalnızca iletilen verinin kopyalanması sağlanır. Bunun için en iyi örnek fiziksel katmanda çalışan hub (göbek) cihazıdır. Ethernet kabloları aracılığıyla iletilen elektrik sinyallerinin birer kopyası

hub cihazlarlarının diğer tüm portlarından iletilir. Kablosuz ağlarda kullanılan tek yönlü, çok yönlü gibi özelleştirilmiş antenler de fiziksel katmanda çalışırlar.

OSI mimarisinde ikinci katman olan veri bağlantısı katmanında ethernet, atm gibi yaygın yöntemler ile iletişim sağlanır. Veri bağlantı katmanının görevi ağ katmanından iletilen paketlerin uygun çerçevelere bölünerek fiziksel katmana iletimini sağlamaktır. Veri bağlantı katmanı ortam erişim kontrolü (Media Access Control - MAC) ve mantıksal bağlantı kontrolü (Logical Link Control - LLC) olmak üzere iki alt katmandan oluşur. Ortam erişim kontrolü alt katmanında veri iletiminde hata kontrolü ve fiziksel adreslerin iletimi sağlanır. Mantıksal bağlantı kontrolü alt katmanında farklı protokollere özgü mantıksal bağlantılar oluşturulur ve akış kontrolü sağlanır. Veri bağlantısı katmanında iletilen çerçeveler belli kurallar dahilinde işleyebilirler. Örneğin veri bağlantı katmanında çalışan ağ anahtarları iletilen çerçevelerin MAC adreslerini ve hangi portlardan geldiği bilgisini bir tabloda tutar. Bu tablo sayesinde veri bağlantı katmanında gerçekleşen veri iletişimlerinin hub cihazındaki gibi her yere kopyalanması yerine yalnızca ilgilisine iletilmesi sağlanır. Bunun yanında bilgisayarlardaki ağ arayüz kartlarında çerçeve iletime başlatılmadan önce kabloda veri iletişiminin olup olmadığı kontrol edilir. Veri bağlantı katmanındaki ethernet erişim yönteminde kullanılan MAC adresleri sabit diğer bir deyişle fiziksel adreslerdir.

Üçüncü katman olan ağ katmanında farklı ağlar arasındaki iletişim sağlanır. Ağ katmanındaki paketlerin bir noktadan diğer bir noktaya en verimli şekilde iletimi sağlanır. Bu katmandaki adresler akıllı ve geçici adreslerdir. Cihazlar ya da bilgisayarlar bulundukları farklı ağlarda farklı ağ adresleri alabilirler. Ağ katmanındaki akıllı adresleme özelliği güvenlik, performans ve esneklik sağlar. Ağ katmanındaki veri iletimini yönlendirici (router) cihazlar sağlarlar. Yönlendirici cihazlar üzerindeki yapılandırmaya göre paketlerin iletimi yedekli yollardan belirli kontroller yapılarak sağlanır.

Dördüncü katman olan taşıma katmanında veri bölütler (segment) aracılığıyla taşınır. Taşıma katmanı üst katmanlardan aldığı verilerin taşımasında önceliklendirme yaparak servis kalitesini artırır. Ayrıca uçtan uca iletişim kontrolünü kuran taşıma katmanı hata kontrolü yapar. Bu katmanda yaygın olarak aktarma kontrol protokolü (Transmission Control Protocol) ve kullanıcı veri bloğu protokolü (User Datagram Protocol) kullanılır. UDP protokolü paket teslimini garanti etmese de TCP protokülüne göre çok daha hafif ve

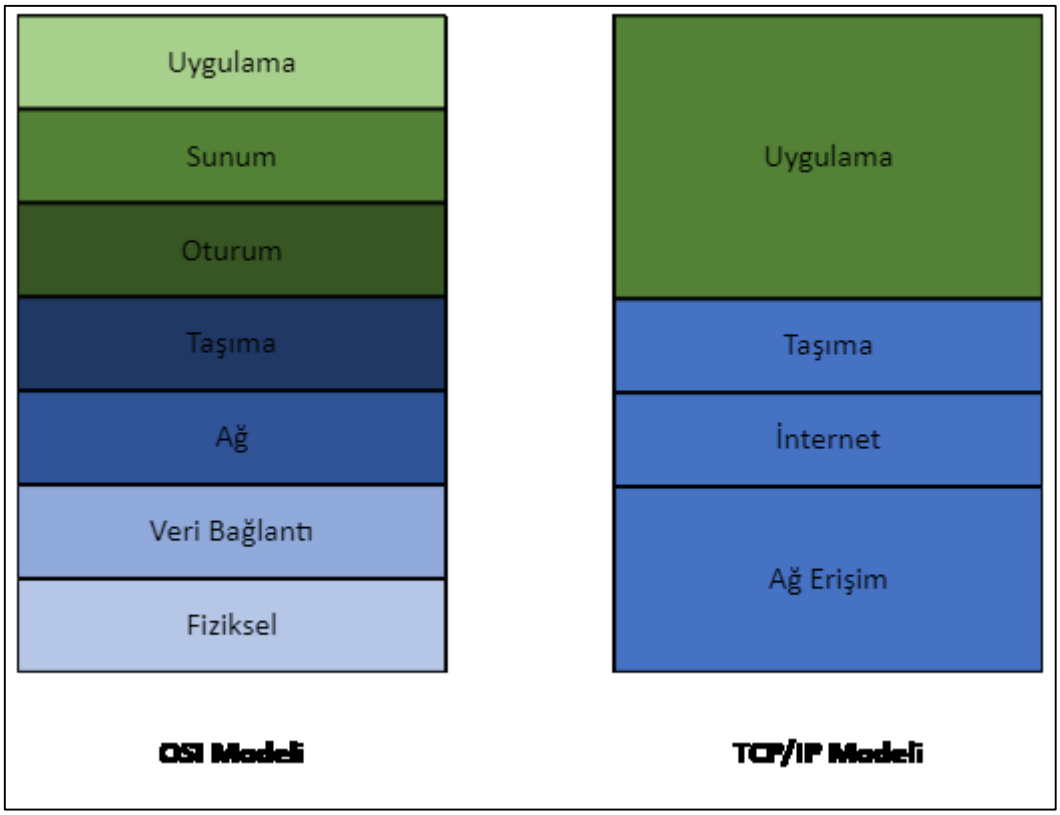
hızlıdır [3]. Dördüncü katmanda kullanılan cihaz örneği olarak geleneksel güvenlik duvarı verilir. Genel anlamda geleneksel güvenlik duvarları dördüncü katmandaki portların kontrolünü ve üçüncü katmandaki adreslerin kontrolünü yaparak erişim kontrolü sağlarlar. Ancak günümüzdeki modern güvenlik duvarları birinci katmandan yedinci katmana kadar kontroller yapabilmektedir.

Beşinci katman olan oturum katmanında uygulamalar arası bağlantıların kurulması, kontrolü ve sonlandırılması sağlanır. Bu katman sayesinde bir bilgisayar ya da cihaz birden fazla bilgisayar ya da cihaza bağlantı kurduğu zaman bu bağlantıların birbiriyle karışmaması ve her bir oturumun ayrı ayrı yönetilmesi sağlanır.

Altıncı katman olağan sunum katmanında birbirinden farklı cihazlarda kullanılmak üzere iletilen verilerin ortak formatı belirlenir. Bunun yanında bu katmanda yapılan verinin sıkıştırılması açılması ve şifrelenmesi işlemleri ile güvenlik ve performans artışı sağlanır. Örneğin uygulama katmanında kullanılan bir video konferans yazılımı sunum katmanında H264 kodlamasını kullanabilir.

En üst katman olan uygulama katmanı uygulama ile ağ arasındaki bağlantıyı kurar. Kullanıcılarla etkileşim sağlayan tek katman uygulama katmanıdır. Örneğin e-posta, veri tabanı servisleri bu katmanda çalışır.

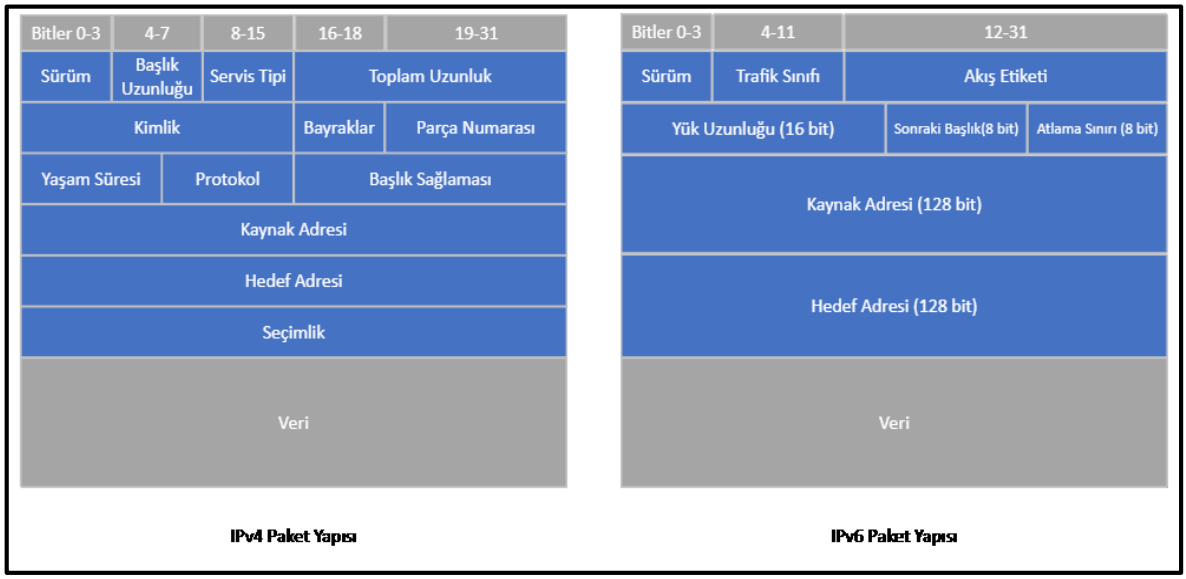
OSI modelinin yanında diğer dünyaca kabul gören ağ bakış açısıyla basitleştirilmiş TCP/IP modeli uygulama, taşıma, internet ve ağ erişimi olmak üzere dört katmandan oluşur (Şekil 2.1).



Şekil 2.1. 7 Katmanlı OSI Modeli ve 4 Katmanlı TCP/IP Modeli Karşılaştırması

2.2.1. İnternet protokolü

İnternet protokolü dünyada en yaygın olarak kullanılan yönlendirilmiş veri iletişim protokolüdür. IP ağları geçmiş dönemde bilgisayarların kendi aralarında haberleşmesi için icat edilmiş olmasına rağmen günümüzde hemen hayatımızın her alanında yer bulmaktadır. Günümüzde yaygın olarak internet protokolünün dördüncü sürümü ve altıncı sürümü yer alır. Geçtiğimiz birkaç yıla kadar IPv4 çok daha yaygın olarak kullanılmaktaydı ancak internetin nesnelerinin hayatımızın her alanına girmesi nedeniyle IP adres ihtiyacında patlama yaşandı ve böylece yeni nesil cihazlarda IP adresi aralığı kısıtlı olan IPv4 yerine çok daha geniş IP adres aralığına sahip olan IPv6 kullanım oranları artmaya başladı (Şekil 2.2). IPv6'nın geniş IP adres aralığı sağlamasının yanında artırılmış güvenlik seviyesi, ağ adres çevirisine ihtiyaç duymaması ve yüksek servis kalitesi sağlaması gibi faydaları bulunmaktadır. IP haberleşme OSI modelinin üçüncü katmanında yer alır. Alt ve üst katmanlardaki yaygın kullanılan hemen tüm teknolojilerle uyumlu çalışır. Her ne kadar adı internet protokolü olsa da internet bağlantısı dışında yerel alan ağları, kablosuz yerel alan ağları ve internete bağlantısı olmayan ya da kısıtlı olan kurumsal ağlar gibi birçok ağ ortamında da kullanılır.



Şekil 2.2. IPv4 ve IPv6 Paket Yapısı Karşılaştırması

2.2.2. Ethernet

OSI mimarisinin ikinci katmanında bulunan ethernet teknolojisi günümüzde en yaygın kullanılan kablolu ve optik yerel alan ağ teknolojisidir. Günümüzde yerel alan ağları yanında geniş alan ağlarında da kullanımı yaygınlaşmıştır. Özellikle çoklu protokol etiket anahtarlama (Multi Protocol Label Switching – MPLS) teknolojisinin internet servis sağlayıcıların en büyük taşıyıcı sistemleri olmasıyla birlikte metro ethernet internet erişimi ve metro ethernet sanal özel ağlar büyük şirket ve kurumların geniş alan ağ altyapısını oluşturmaktadır. Ethernet teknolojisinin çakışma algılama, çift yönlü iletişim, hata kontrolü gibi önemli faydaları vardır. Ethernet teknolojisi zaman içerisinde gereksinimlere uygun geliştirilen anahtarlama teknikleri sayesinde bilgisayar ağlarında yaşanan sorunları asgari seviyeye indirir.

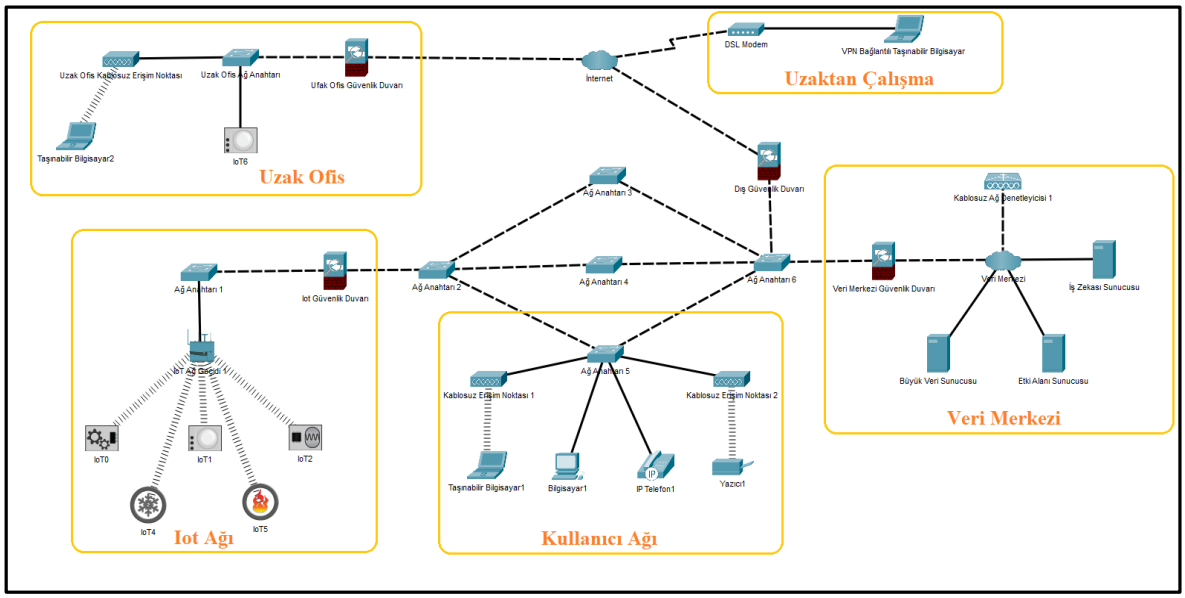
2.2.3. Wi-Fi

IEEE 802.11 standartlarıyla tanımlanmış Wi-Fi teknolojisi cihazların radyo sinyalleriyle kablosuz olarak ağa bağlanmasını sağlar. Wi-Fi teknolojisi OSI mimarisinde veri bağlantı katmanı ve fiziksel katmanda yer alır. Zaman içerisinde artan ihtiyaçlara ayak uydurmak için Wi-Fi teknolojisi farklı frekans ve bant genişliklerine sahip alt standartlar geliştirmiştir.

IoT sistemlerinde birçok farklı ağ teknolojisi kullanılır. WLAN ve IoT teknolojileri çok hızlı gelişmekte ve endüstri teknolojileri bütünleştirmenin yollarını aramaktadır [4]. Bunun yanında kablosuz ağ teknolojilerinden en yaygın olarak kullanılmakta olan Wi-Fi teknolojisinin halihazırda bulunması nedeniyle birçok IoT sistemi Wi-Fi uyumlu olarak geliştirilmektedir. Wi-Fi teknolojisi düşük güç tüketimi gerektiren IoT sistemleri için de farklı alt kırılımlara evrilmektedir. Bu tez çalışması kapsamında kurumsal ağlarda halihazırda kullanılmakta olan yaygın Wi-Fi teknolojilerine odaklanılmıştır.

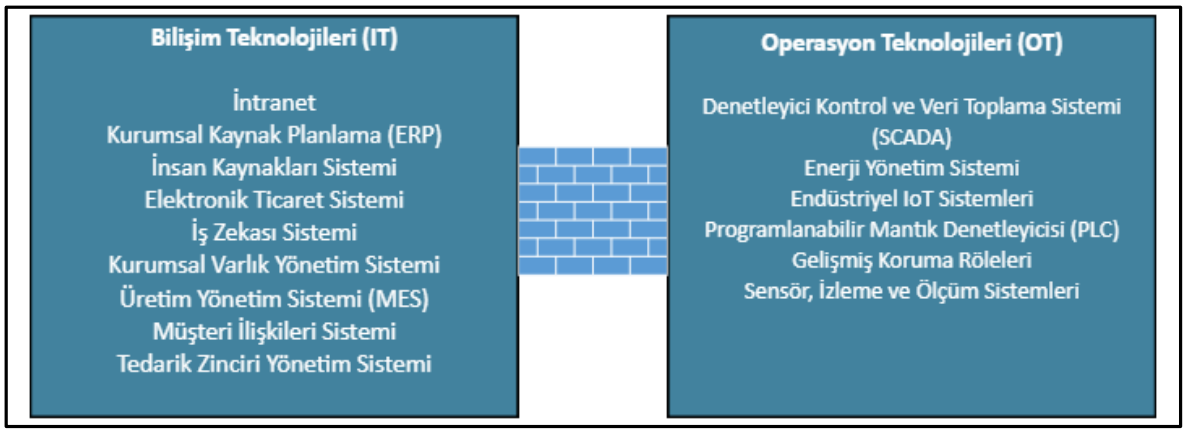
2.3. Kurumsal Ağlar

Ağlar genel bakış açısıyla geniş alan ağları (Wide Area Network – WAN) ve yerel alan ağları (Local Area Network – LAN) olarak ele alınırlar. Kurumsal ağlar yerleşke gözetmeksizin WAN, LAN, kablosuz yerel alan ağı (Wireless Local Area Network – WLAN) ve sanal özel ağ (Virtual Private Network – VPN) benzeri birçok ağ teknolojisinin birleştirilerek tek bir yerel alan ağı oluşturmasına yararlar. Üniversitelerde, kurumlarda ve işletmelerde kurumsal ağlar nesnelerin, kullanıcıların ve yazılımların verilerinin taşınmasını sağlarlar. Kurumsal ağlar üzerinden gereksinim duyulan ağ trafikleri güvenlik odağında ve yüksek performansla çalışmalıdır. Veri merkezi ile uç noktalar arası trafiklerin gereksinimlerine uygun olarak önceliklendirilmesi önem arz eder. Kurumsal ağlar artan teknolojik ihtiyaçlar karşısında gün geçtikte daha karmaşık hale gelmektedir [5]. Kurumsal ağ yöneticileri ağ tasarımı yaparken güvenlik, dayanıklılık ve başarımı sağlamak gibi birçok zorlukla mücadele etmek zorundadır [6]. Yapılan çalışmalardan ortaya çıkan istatistiklerde siber saldırıların % 65'inden fazlasının kaynağı olarak ağ tasarım ve konfigürasyon hataları işaret edilmektedir [6]. Ağ yöneticileri IoT sistemleri ile birlikte çok daha yüksek sayıdaki uç cihazı ağ üzerinde yönetmek zorundadır [3].



Şekil 2.3. Basitleştirilmiş Örnek Kurumsal Ağ

Şekil 2.3'de görüldüğü üzere kurumsal ağlar bilgisayarlar ile veri merkezleri arası iletişimi sağlar. Uzak yerleşkelerdeki IT sistemlerinin ve uzaktan çalışan kullanıcıların güvenli bir şekilde ana yerleşkeyle iletişim kurmasını sağlar. IT sistemlerine ek olarak Operasyonel Teknoloji (OT) ve IoT ağlarından veri merkezine iletişim kurarlar. Geleneksel IT sistemleri verinin veri merkezlerinde üretilmesi ve bulundurulması odaklıdır. Ancak IoT sistemlerde veriler dağıtık uç cihazlarda üretilir ve dağıtık veri merkezlerinde konumlandırır. IT sistemlerinin odağı kurumsal kaynak planlama, intranet, insan kaynakları sistemleri, iş zekası sistemleri, elektronik ticaret sistemleri ve kurumsal varlık yönetimi sistemleri, üretim yönetim sistemleri, müşteri ilişkileri yönetimi sistemleri, tedarik zinciri yönetimi sistemleri olarak gelişmiştir. OT sistemlerinin odağı merkezi denetim ve veri toplama sistemi (Supervisory Control and Data Acquisition – SCADA), enerji yönetim sistemleri, endüstriyel IoT sistemleri, programlanabilir mantık kontrolörleri, gelişmiş koruma röleleri, sensörler monitörler ve ölçümler olarak düşünülebilir. IT sistemleri şirketin IT yöneticilerinin sorumluluğundayken OT sistemleri kurumlardaki hemen tüm bölümlerin sorumluluk alanlarına girer (Şekil 2.4). Dijitalleşmenin kaçınılmaz olduğu günümüzde IoT sistemlerinin kurumsal ağlara dahil olması ile birlikte kurumların şirketlerin ve benzeri organizasyonların dijitalleşmesi yolunda kurumsal ağların önemi ortaya çıkar. Endüstri 4.0 ile birlikte kurumsal ağlar organizasyonların yalnızca bilgi teknolojileri açısından değil yönetim, üretim, araştırma ve geliştirme faaliyetleri gibi hemen her alanı açısından önem kazanır. Kurumsal ağlarda yaşanabilecek kesintiler ya da performans düşüşleri organizasyonların tüm faaliyetlerini olumsuz etkileyebilir ya da durma noktasına getirebilir.



Şekil 2.4. Bilişim Teknolojileri ve Operasyon Teknolojileri Kullanım Alanları

Geleneksel kurumsal ağlarda veri iletiminin uç noktalar ile veri merkezi arasında sağlıklı iletilmesi söz konusu iken internetin nesnelerinin de ağlara dahil olmasıyla birlikte uç noktalar arası veri iletişiminin önemi de artmıştır. Bunun yanında ağ tasarlanırken veri merkezleri ile uç cihazlar arasındaki bağlantılar ön plandadır ancak IoT sistemlerine uygun ağ tasarımı yapılırken uç cihazların birbirleri arası bağlantıların da göz önünde bulundurulması gerekir.

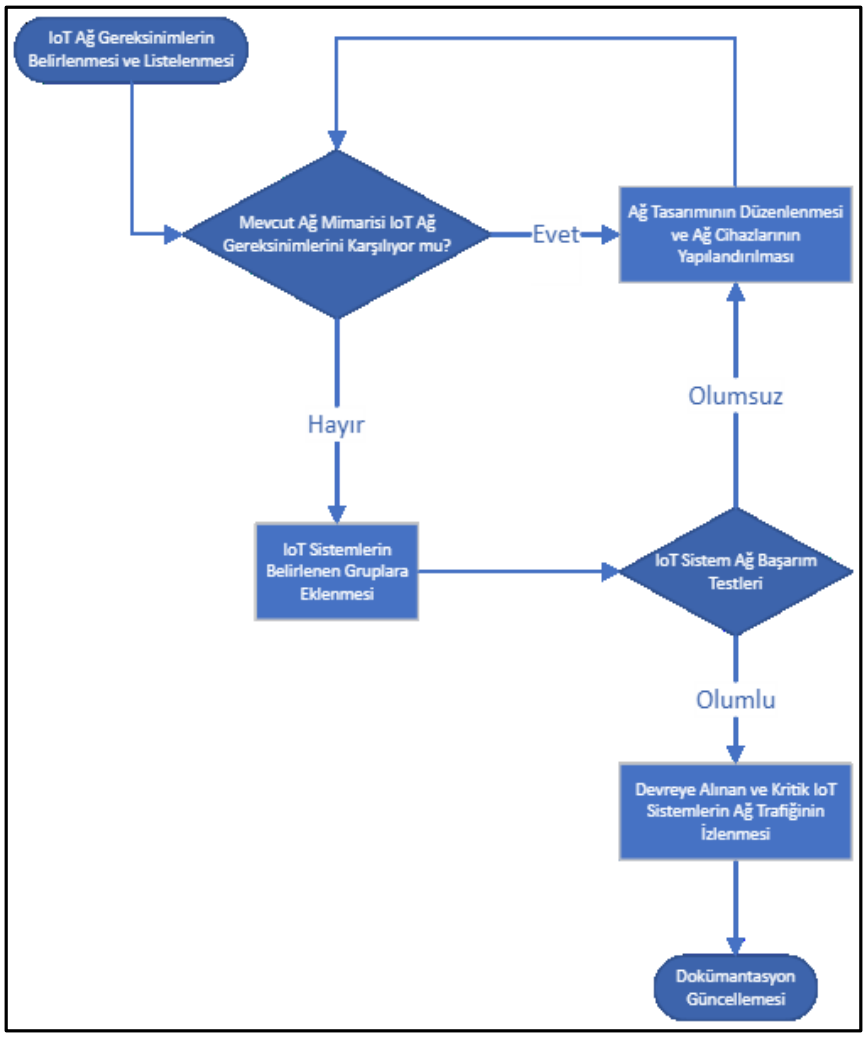
3. KURUMSAL AĞLARDA İYİLEŞTİRME ÖNERİLERİ

3.1. Kurumsal Ağlar ile Nesnelerin İnterneti Ağları Arası Uyumsuzluklar

Mevcut ağ teknolojileri sunucu kaynaklarının paylaşımı için tasarlanmış olduğu uç noktalarda üretilen veri paylaşımını temel alan IoT sistemleri tam olarak uyumlu değildir [7,8]. IoT ağlarının sunduğu birçok yeni uygulama geleneksel IP mimarisine kolay uyumlanmazlar [9]. TCP/IP protokol yığını ilk geliştirildiği dönemlerde bilgisayarların kablolu haberleşmesi için tasarlandı ve TCP/IP protokol yığını sürekli geliştirildi ancak temel mimari tasarım değişmemiştir [9]. Kurumsal ağlar, ortaya çıkma amaçları nedeniyle bilgisayarlar ve bilgisayar sistemlerinin haberleşmesi amacıyla tasarlanmıştır. İlerleyen teknolojilerle birlikte IP kamera, IP telefon vb. bilgisayar sistemlerinden ayrı olarak çalışan sistemlere de hizmet verebilmek üzere bazı geliştirmeler yapılmıştır. Örneğin ethernet üzerinden güç (Power Over Ethernet - PoE) teknolojisi ile ağ üzerinde kamera veya telefon gibi göreceli olarak düşük güç tüketimi gereken cihazların güç ihtiyacı ağ kablosu üzerinden ağ cihazları tarafından sağlanır. Ancak gelişen teknolojilerle farklı gereksinimlerle yeni cihazlar ağlara dahil olmaktadır. Eş frekanslı gerçek zamanlı çalışması gereken endüstriyel nesnelerin interneti (Industrial Internet of Things - IIoT) sistemlerinin gecikme toleransı 1 ms'nin altındadır. Geleneksel ağlarda yerel alan ağları da dahil bu performansı garanti etmek son derece güçtür. Ağ trafiğinde yaşanacak bir yoğunluk durumunda gecikme süreleri 1 ms'nin üzerine çıkabilir. Geniş alan ağlarında gecikme süreleri genellikle yerel alan ağlarından çok daha yüksektir.

3.2. Genel İyileştirme Yöntem Önerisi

Kurumsal ağ yöneticileri ağ tasarımı yaparken güvenlik, dayanıklılık ve başarımı sağlamak gibi birçok zorlukla mücadele etmek zorundadır. IoT sistem çözümlerinin şartlara ve gereksinimlere özgü tasarlanması gerekir [2]. Ağa eklenen her yeni sistem ağ tasarımı ve yapılandırmasında değişikliğe yol açabilir. IoT sistemlerin ağa dahil edilmesiyle bu sıklık artar. IoT sistemler ağa dahil edilmeden önce belirlenmiş ön çalışmalar yapılmalıdır. Öncelikle IoT sistemlerin ağ gereksinimlerine göre gruplandırılması ve ağ segmentasyonun sağlanması gerekir. Mevcut ağ topolojisi çıkarılarak izleme sistemleriyle ağın ayrıntılı bir şekilde gösterimi sağlanır. Önçalışmalar yapıldıktan sonra Şekil 3.1'deki adımlar izlenerek IoT cihazlar kurumsal ağa dahil edilir.



Şekil 3.1. IoT Odaklı Ağ Tasarım ve Yapılandırma Çalışması

Çizelge 3.1'de örneği görüldüğü üzere öncelikle IoT cihazların ağ gereksinim tablolarının oluşturulması önerilir. Böylece cihazların ne tür gereksinimleri olduğu özetlenebilir ve gruplandırma yapılabilir. İlgili gruplandırma yapıldıktan sonra mevcut ağ mimarisinin grupların ağ gereksinimlerini karşılayıp karşılamadıkları kontrol edilmelidir. Ağ gereksinimlerinin karşılanması halinde IoT cihazlar ağa dahil edilerek sistem performansı test edilir. Devreye alınan IoT sistemlerin kullanıldığı yollar mümkün ölçüde ayrı bir izleme gösterge paneline alınarak takip edilir. Ancak ağ mimarisinin IoT ihtiyaçlarını karşılamadığı durumlar ve IoT sistem başarım testlerinin ağ kaynaklı başarısız olması durumunda sorunun tespiti için ağ mimarisi üzerinde anlık ve geriye dönük performans verileri toplanarak sorunun kaynağı tespit edilir. Başarım oranının düşük olduğu ağ sorunlarında kapasite artırımı yapmadan önce ağ mimarisinin gözden geçirilmesi ve tasarımsal değişiklikler yapılması maliyet etkin bir çözümdür. Bu noktada sorunlar mimari uyumlanma ve ağ gecikmelerinin azaltılması olarak iki ana başlık altında ele alınır.

Çizelge 3.1. Örnek IoT Cihazları Ağ Gereksinim Listesi

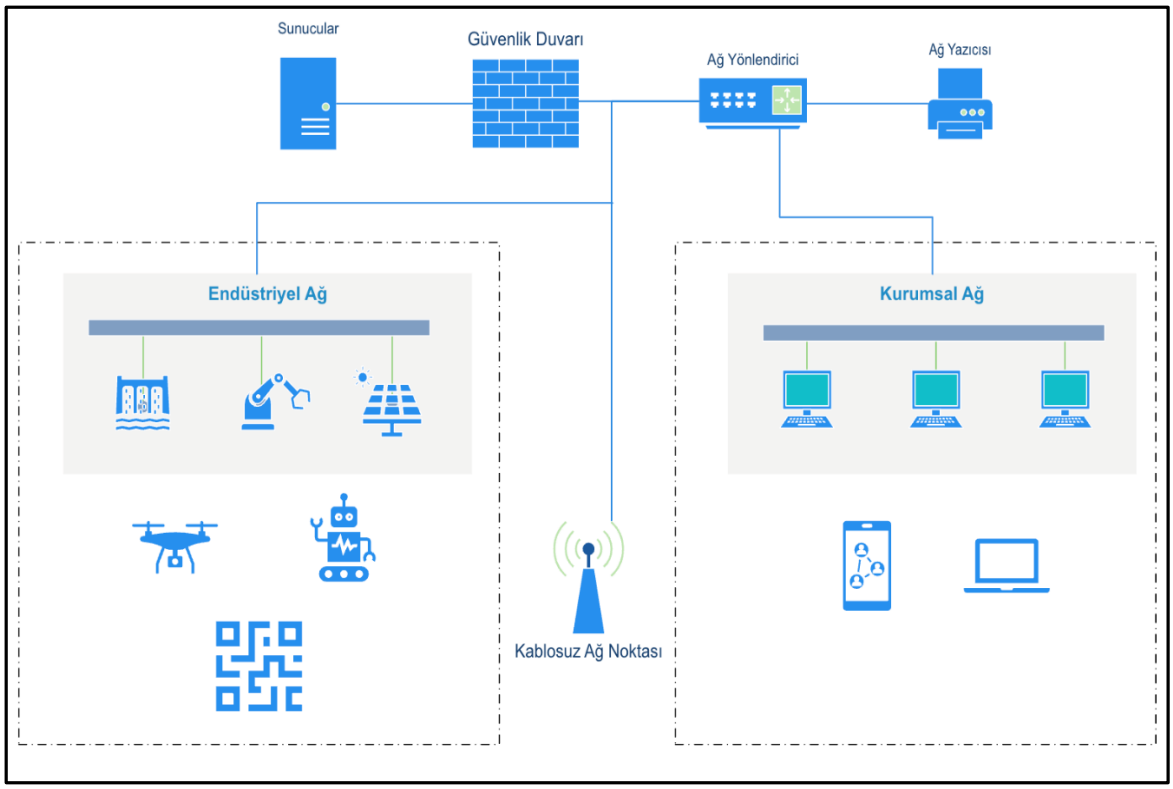
No	Cihaz Tipi	Cihaz Sayısı	Bant Genişliği	Gecikme Toleransı	Bağlantı Ortamı	Öncelik	Gecikme Değişimi	Topoloji Tipi	Hedef
1	Isı Sensörü	10	0-1 Mbit	>100 ms	802.11 b/g/n	Orta	En İyi Gayret	Yıldız	Analizör Sunucusu
2	Scada	2	1-10 Mbit	Gerçek Zamanlı, <100 ms	Fiber optik veya Bakır Ethernet	Yüksek	< %15	Yıldız	PLC Sistemleri

3.3. Yerel Alan Ağları İçin İyileştirme Önerileri

Yerel alan ağları kurumsal ağların yerleşke içi bağlantılarını sağlarlar. Geniş alan ağlarına göre genellikle yüksek bant genişliğine sahip oldukları ve düşük gecikmeli oldukları için sorunların çözümünde göz ardı edilirler. Ancak bazı durumlarda iyi yapılandırılmamış yerel alan ağları önemli sorunlara yol açarlar. Bu nedenle yerel alan ağlarının tasarımı ayrıntılı bir şekilde ele alınmalıdır ve ağ cihazlarının yapılandırılırken IoT sistemleri göz önünde bulundurulmalıdır. IT ve IoT mimarileri benzerlikler gösterse de IoT sistemlerinin gereksinimleri geleneksel IT ağlarıyla büyük farklılıklar göstermektedir [3].

3.3.1. Segmentasyon

Ağ segmentasyonu ağlarda sanal gruplar oluşturulmasını ve gruplara özgü kurallar yaratılmasını sağlar. Şekil 3.2'de endüstriyel ve kurumsal ağ segmentasyonu görülmektedir. Segmentasyon sayesinde gruplar arası güvenlik ve önceliklendirme sağlanır. Segmentasyon işlemi kurumsal ağlarda VLAN, VPN ve erişim denetim listesi (Access Control List - ACL) teknolojileri kullanılarak yapılır. Düşük gecikme gereksinimi olan cihaz grubu için oluşturulan bir VLAN, ağ cihazlarındaki yapılandırmalarla yüksek önceliklere tabi tutularak ilgili cihaz grubu için düşük gecikmeli trafik iletimi sağlanır. Bunun yanında ilgili VLAN farklı yollardan yönlendirilerek bant genişliği ve gecikme dar boğazlarından uzak tutulabilir.



Şekil 3.2 Endüstriyel ve Kurumsal Ağ Segmentasyonu

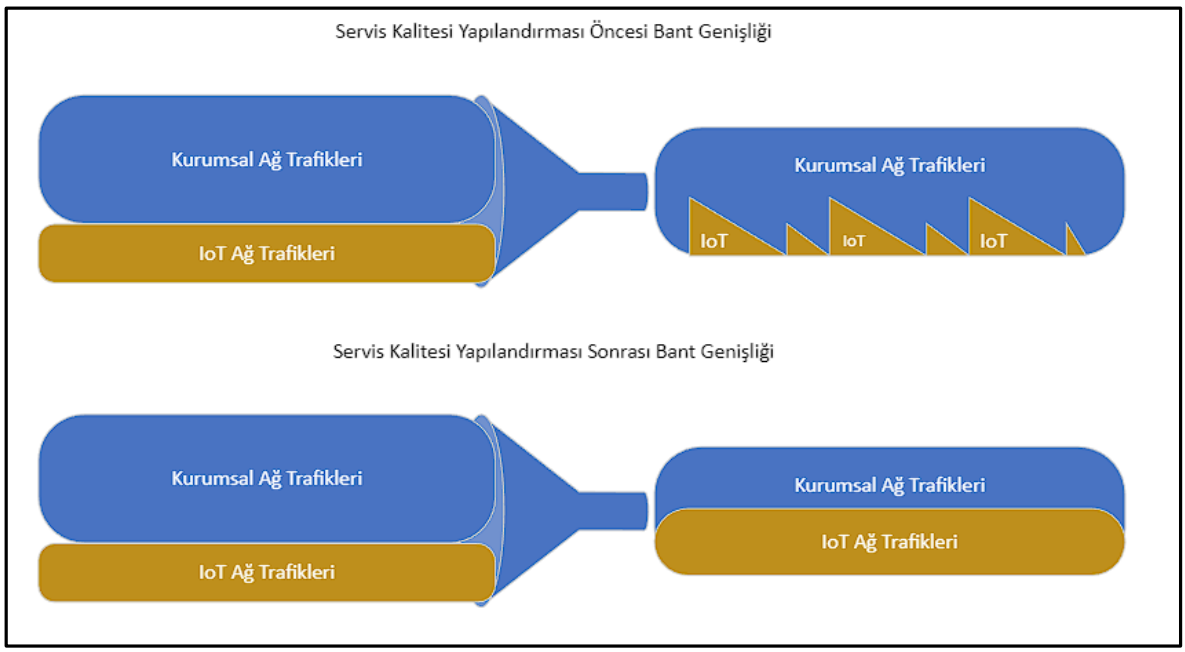
Ağ yöneticileri kendi işlerinin karmaşıklığını azaltmak için ve ağı daha kolay yönetilebilir hale getirmek için benzer işleri yapan kullanıcıları gruplandırırlar. Segmentasyon yapılırken ağ içerisinde yalnızca erişilmesi gereken noktalara erişim izni verilmesi gereklidir, gereksiz erişim yetkileri kaldırılmalıdır.

Segmentasyonun başlıca faydaları yüksek ağ performansı ve küçültülmüş saldırı alanı olsa da, ağın denetlenebilirliğinin ve gözlemlenebilirliğinin sağlanmasının başlangıcı kabul edilir. Ancak aşırı segmentasyon yapılması ağın yönetimini zorlaştıracağı ve tasarımını karmaşıklaştıracağı için gereksinim ve güvenlik seviyesi bazlı gruplanan cihazlar için en uygun segmentasyon aralığı belirlenmelidir.

3.3.2. QoS

Geçmiş dönemlerde ses ve video paketlerinin IP ağları üzerinde önceliklendirilmesi amacıyla ortaya çıkan hizmet kalitesi (Quality of Service - QoS) IoT sistemlerin desteklenmesi anlamında büyük önem arz eder. Mevcut TCP/IP mimarisi, uygulama

tanımlayıcılarının ağ paketlerinin içine gömülmesine uygun olmadığından farklı tipteki IoT uygulamaları için özelleştirilmiş iletim stratejisi oluşturulmasına izin vermez [9].



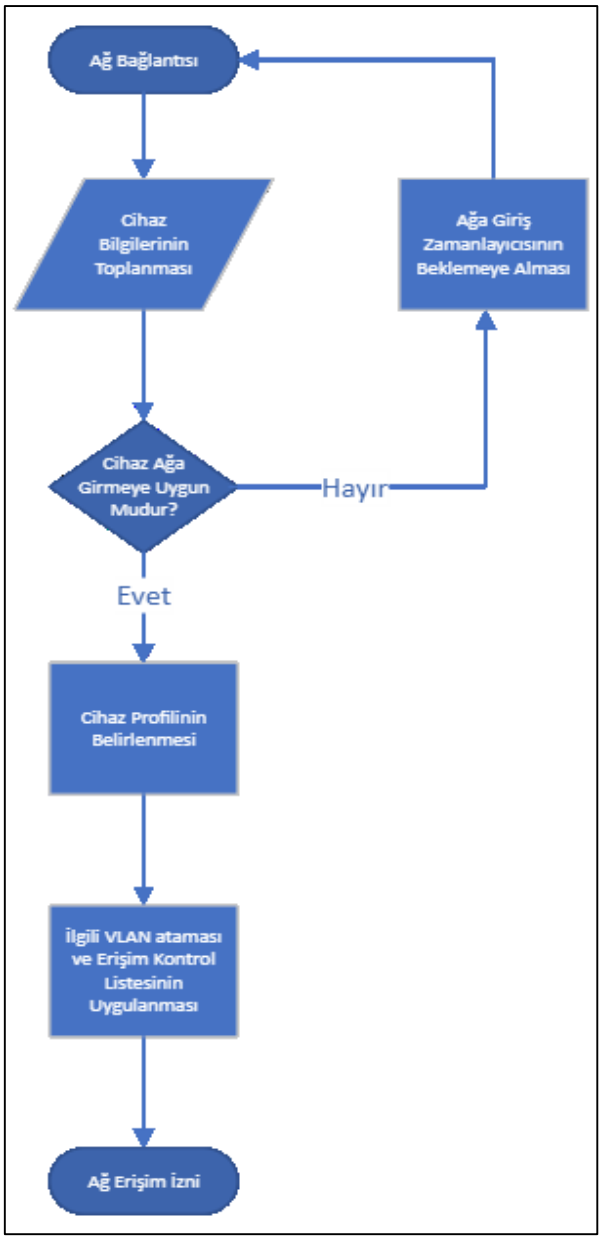
Şekil 3.3 Servis Kalitesi Bant Genişliği Yönetimi

Ağda gecikmeye duyarlı uygulamalar yüksek bant genişlikleri olduğunda genellikle sorun yaşatmazlar. Ancak dönemlik olarak artan trafikler bant genişliklerini doldurmaya başladıkları anlarda ağ cihazları fazla gelen paketleri bırakırlar. Paket kayıpları, gecikme ve gecikmedeki değişme yanında IoT deneyim kalitesini en çok etkileyen faktördür [10]. Böyle durumlarda önceden belirlenmiş olan trafiklerin feda edilmesi ve öncelikli paketlerin iletimi için QoS kullanılması gerekir (Şekil 3.3).

3.3.3. NAC

Ağ erişim kontrol (Network Access Control – NAC) sistemleri uç nokta sistemlerin ağa dahil olmaları noktasında ağ güvenliğini sağlarlar. Ağa bağlanan uç nokta cihazlarının ağ giriş öncesi doğrulanması, yetkilendirilmesi kontrollerinin sağlanması ve ağa bağlandıktan sonra gruplanması bir diğer deyişle segmentasyonun sağlanmasını sağlarlar. Segmente edilen cihazların birbirleri arasındaki erişim kontrol listelerinin uygulanarak güvenlik ve

performans artırımını sağlarlar. Ağ giriş kontrol sistemleri profilleme yetenekleri sayesinde cihaz tiplerini ayırt ederler.



Şekil 3.4. IoT Odaklı Ağ Tasarım ve Yapılandırma Çalışması

Kurumsal ağlara bağlanan IoT cihazların sayısının gün geçtikçe artığı düşünülünce NAC sistemlerinin profilleme özelliklerinin daha da önem kazandığı görülür. Ön yapılandırma ile profilleme sonucunda cihazlar farklı VLAN'lara dinamik olarak atanır (Şekil 3.4). Böylece ağ yöneticisinin müdahale etmesine gerek kalmadan otomasyon ile güvenlik sağlanır. Geleneksel NAC sistemleri bilgisayarlar için tanımlanmış olup 802.1x gibi doğrulama yöntemlerini kullanmak için kullanıcı adı ve şifre bilgilerine ihtiyaç duyarlar. IoT

cihazlarından birçoğu mevcut ürünlerin sonradan ağ yetenekleri kazandırılması ile ağlara dahil oldukları için detaylı güvenlik sağlamayazlar. Bu noktada geleneksel NAC sistemleri IoT cihazlarını doğrulamak ve yetkilendirme için MAC (Media Access Control) adreslerini kullanır. Gelişmiş NAC sistemleri profilleme için ağ üzerinden bir çok veri toplarlar. Örnek olarak uzaktan kimlik doğrulama içeri arama kullanıcı hizmeti (Remote Authentication Dial-in User Service – RADIUS), basit ağ yönetim protokolü (Simple Network Management Protocol – SNMP) tuzağı, SNMP sorgusu, dinamik ana bilgisayar yapılandırma protokolü (Dynamic Host Configuration Protocol – DHCP), DHCP SPAN, alan isimlendirme sistemi (Domain Name System – DNS), hiper metin transfer protokolü (Hyper Text Transfer Protokol – HTTP), netflow, ağ tarama (Network Mapper - NMAP), aktif dizin (AD) verilir. Profilleme yeteneği yalnızca cihaz tiplerini ayırt edici şekilde değil kullanılan protokolü ayırt edecek şekilde de yapılandırılabilir.

Örneğin cihaz tiplerine göre Ethernet/IP Düğümü, insan makine arayüzü (Human Machine Interface - HMI), giriş çıkış (Input Output – IO), programlanabilir mantıksal denetleyici (Programmable Logic Controller – PLC), Supervisor, anahtar şekilde profiller oluşturulabilirken, protokol tipine göre Bacnet, CIP, Modbus, Profinet şeklinde profiller tanımlanabilir. Bu noktada gerek cihazların tiplerine gerekse protokol tiplerine göre segmentasyon sağlanır. Gelişmiş NAC sistemlerinde Iot cihazların tanımlanma ve profilleme işlemi yapılırken pasif olarak cihazların trafik analizi yapılır, aktif olarak ağ taraması yapılır. Pasif olarak yapılan trafik analizinde cihazların gönderdikleri paketlerden cihazları tanımlayabilmek için parmak izi taraması yapılır. Bulunan parmak izleri ön tanımlı cihaz parmak izi veri tabanı içerisinden sorgulanır. Pasif tanımlama yöntemi trafik iletmeyen veya trafik içerisinde parmakizi barındırmayan cihazlar nedeniyle kısıtlıdır. Bu nedenle pasif tanımlama yöntemi ile tanımlayamayan cihazlar aktif tanımlama yöntemiyle tanımlanırlar. Ağ segmentelerine güvenlik ve performans artırımı için erişim kontrol kuralları eklenir ve segment trafiklerinin yalnızca ihityaç duyulan noktalara erişimi sağlanır.

3.3.4. Kapsayan ağaç protokolü

IoT sistemlerde veri iletiminin vazgeçilmezleri güvenilir ve zamanında olmasıdır [3]. IIoT sistemlerde gerçek zamanlı iletişim gereken üretim otomasyon sistemlerinin gecikme gereksinimleri 100 milisaniyeden az, eş frekanslı gerçek zamanlı eylem kontrolü sağlayan sistemlerin gecikme gereksinimler 1 milisaniyeden az olmalıdır. Ancak geleneksel

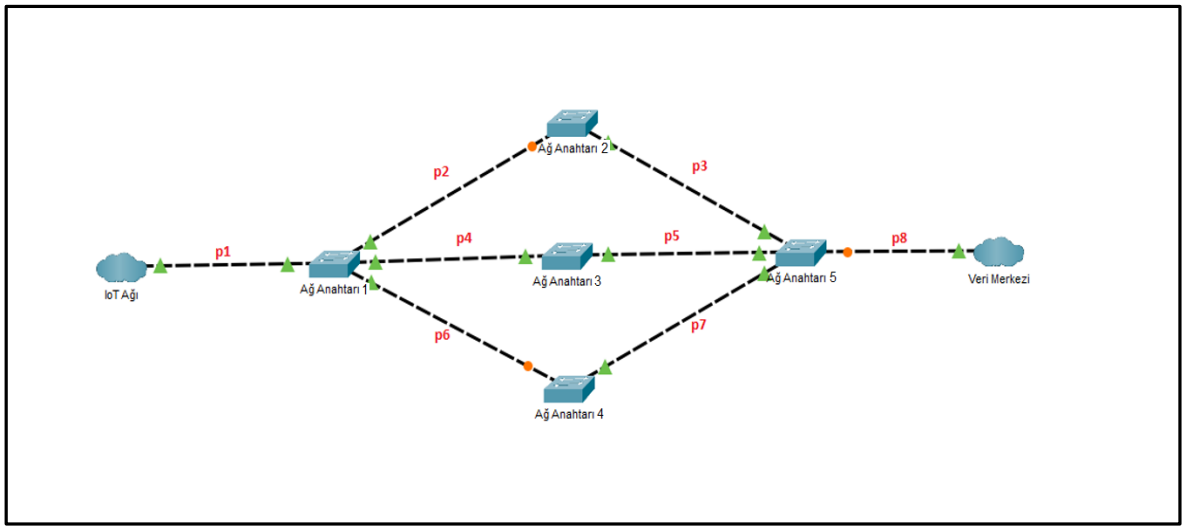
bilgisayar ağlarında bu kadar düşük gecikme değerleri sürekli olarak garanti edilemez. Bu ağlarda yalnızca IoT trafiklerin taşınmadığı diğer tüm kurumsal trafiklerin de taşındığı düşünüldüğünde kritik sistemlerin gruplandırılıp kullanılmayan bir yoldan taşınmasında gerekebilir.

Ağ gecikmeleri bağlantı kapasitelerinin doyuma ulaşması durumunda ağ paketlerinin geçici bellekte bekletilmesi veya anahtar, yönlendirici cihazların anahtarlama, yönlendirme işlemlerinden kaynaklı olabilir. Mevcut ağ cihazlarının daha yüksek kapasiteli ağ cihazlarıyla değiştirilmesi ile bağlantı hızlarının artırılması gecikmeleri düşürür. Ancak iyi yapılandırılmamış ağ cihazlarında hat kapasitesinin artışı sorunların ancak geçici olarak çözülmesini sağlar. Hat kapasitesinin doyuma ulaştığında hattın veya cihaz hızlarının artırımı yerine cihazların gereksinimlere uygun yapılandırılması ve ağ tasarımının gözden geçirilmesi sorunlara maliyet odaklı çözümler getirecektir. Yerel alan ağlarındaki MSTP, PVST+ vb. gelişmiş kapsayan ağaç protokolleri ile trafiğin farklı hat yollarından dağıtık bir şekilde iletilmesi sağlanır.

Şekil 3.5'in IoT ağı kısmındaki IoT cihazlar ile veri merkezi kısmındaki sunucular arasında sürekli olarak bir ağ trafiği oluşur. Örnek bir senaryoda IoT ağının yerel alan ağına bağlantı kurduğu nokta itibariyle her bir grubu için ayrı VLAN'lar oluşturarak segmente edilmesi gerekir. Gereksinimlerine göre farklı VLAN'larla ayrılmış olan IoT cihazlarının trafiklerinin güzergah üzerindeki kullanılmayan ya da daha düşük yoğunlukla kullanılan yollardan iletiminin sağlanması için IEEE 801.2s MSTP teknolojisi kullanılır. Böylece diğer trafiklerin yaratacağı yoğunluklardan IoT cihaz trafiklerinin etkisinin azaltılması sağlanır.

Kapsayan ağaç protokolü (Spanning Tree Algorithm - STP) yerel ağlarda bir noktadan diğer noktaya birden fazla ulaşım güzergahı varsa özellikle yayın paketlerinden kaynaklanan sonsuz döngüye girme durumunu engelleyen bir trafik yönetimi oluşturur. Genellikle sonsuz döngülerin önüne geçebilmek adına güzergaha ulaşım sağlayan yollardan STP mekanizmasına göre en verimli olanı hesaplayarak diğer yolları inaktif hale getirir ve aktif olan yolun çalışmaması durumuna karşı yedek olarak tutar. Şekil 3.5'de IoT ağı ile veri merkezi arasında p1-p2-p3-p8, p1-p4-p5-p8 ve p1-p6-p7-p8 güzergahları bulunur. STP'nin yaptığı hesaplamalar sonucunda bu yollardan ancak bir tanesi aktif diğer ikisi inaktif olarak konumlanacaktır. Örneğin bu yolların herbirinin 100 Mbit hızda olduğunu düşünürsek toplam kapasite 300 Mbit iken STP işlemleri sonrası kullanılabilir kapasite 100 Mbit olarak

sınırlanacaktır. STP ve RSTP (Hızlı Kapsayan Ağaç Protokolü) yük dengeleme yapamamakta olup düşük bant genişliği kullanılması ve çoklu yol eksikliğine sebep olmaktadırlar [11]. STP yerine gelişmiş bir versiyonu olan MSTP kullanılırsa gecikme duyarlı IoT cihazlarının olduğu VLAN'lar, aktif olmayan yollardan iletilir. Böylece diğer trafiklerden etkilenmesi asgari düzeye indirilir. Diğer bir yöntem ise belirli VLAN'lar için RSTP kullanılarak inaktif güzergahların ön yapılandırma ile aktif hale getirilmesidir. Otomatik yük dengeleme yapan gelişmiş döngü engelleme yöntemlerinde inaktif güzergahların kullanımı herhangi bir yapılandırmaya ihtiyaç duyulmadan sağlanır.

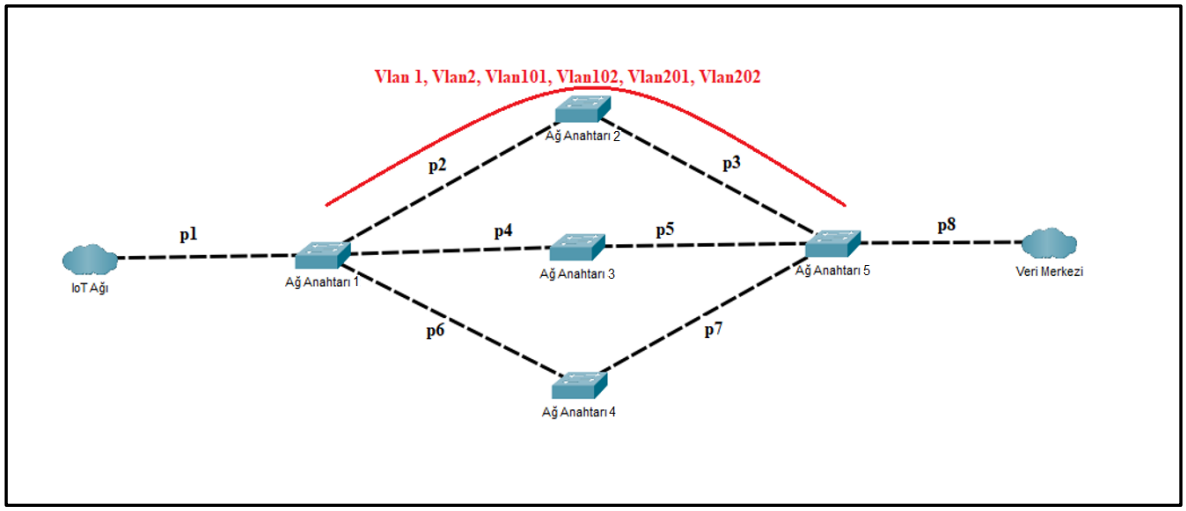


Şekil 3.5. Örnek Yerel Alan Ağ Bağlantıları

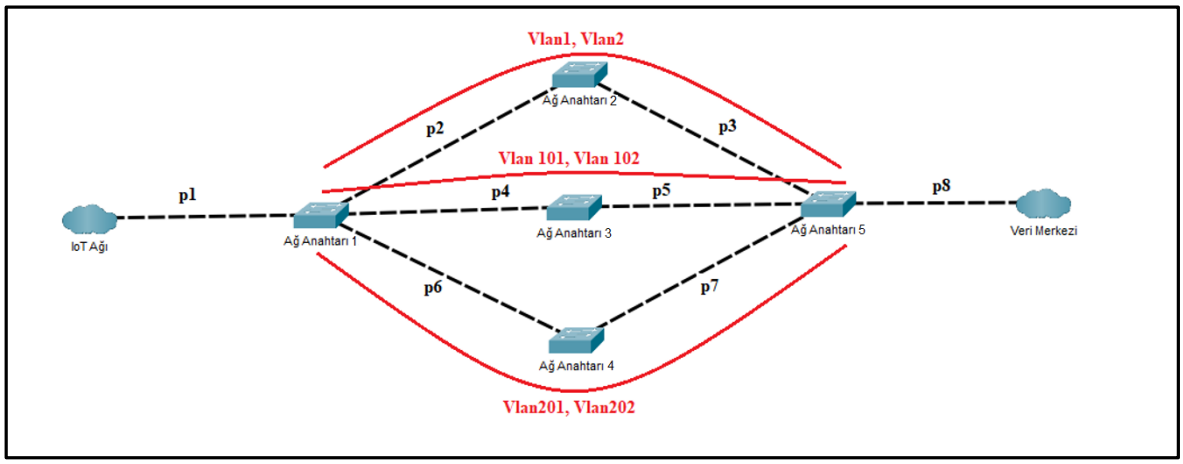
Bazı gelişmiş kapsayan ağaç protokolleri otomatik yük dengeleme yaparlar ancak VLAN'ları güzergahlara kendi algoritmalarındaki şekilde atarlar. Otomatik atama yönteminde gecikme duyarlı VLANlar algoritmaya göre atanır ve yol paylaşımı yapacağı diğer VLAN'ların ağ trafiklerinin gecikme duyarlı trafiklerin önüne geçerek IoT iletişimi sekteye uğratma riski yüksektir. Diğer bir bakış açısıyla güzergahların gecikme durum kontrolleri de yapılmaz. Örnek olarak Şekil 3.5'te 3 güzergahdan gecikmep2 + gecikmep3 , gecikmep4 + gecikmep5 ve gecikmep6 + gecikmep7 arasındaki gerçek gecikme testleri yapılarak bir karşılaştırma yapılmaz.

3.3.5. Tek yol kullanımı ve farklı çoklu yol kullanım karşılaştırması

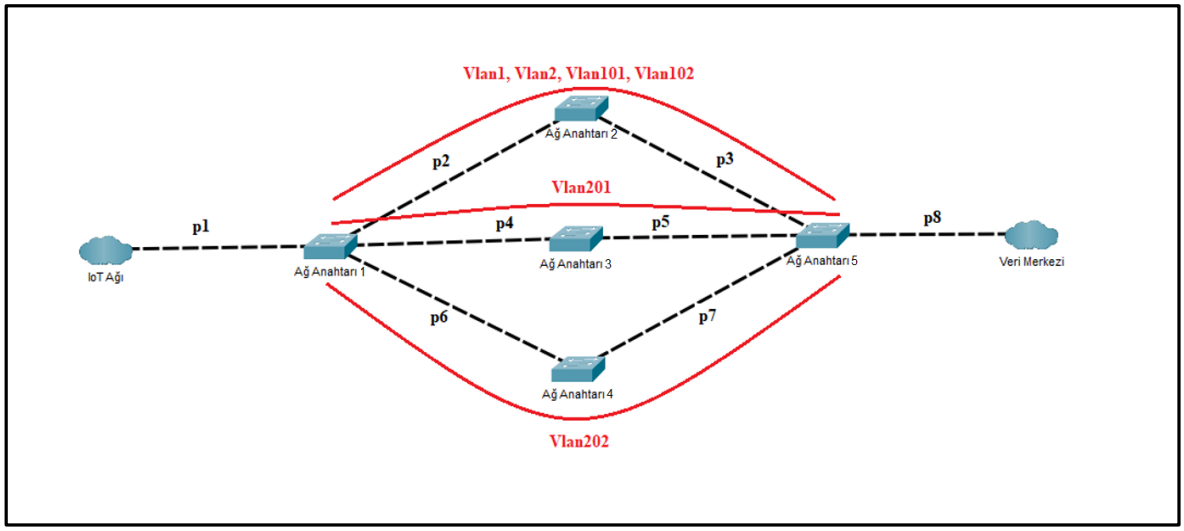
MSTP, RSTP ve PVST+ standartları kullanılarak yapılandırma ile VLAN bazlı yol kullanımı ve yük dengelemesi sağlanır. Şekil 3.6' da STP standardı tüm VLAN'ların tek yol üzerinden iletimini sağlar ve yük dengeleme yapmaz. Şekil 3.7'de otomatik yük dengeleme yapan PVST+ gibi gelişmiş bir kapsayan ağaç protokolü ile VLANlar farklı yollara dağıtılır. Şekil 3.8'de RTSP veya MSTP standardı kullanılır ve ağ yöneticisinin yapılandırması ile belirli VLANlar istenilen yollar üzerinden veri iletimi yaparlar. Veri iletiminde bant genişliği ve gecikmelerin kritik olduğu iki farklı yerel sanal alan ağını Vlan201 ve Vlan202 olarak düşünelim. Şekil 3.8'de ağ yöneticisinin yapılandırması ile bu VLANlar için birer boş güzergah atanmış olup ağ anahtarı 1 ile ağ anahtarı 5 arasındaki yol boyunca diğer ağ trafiklerinden etkilenmeksizin veri iletimi sağlanmış olur. Diğer trafikler bu VLANlar için ağ anahtarı 1 ile ağ anahtarı 5 arasındaki trafik iletimi için bant genişliğini ve gecikmeyi konusunda olumsuz bir durum oluşturmaz.



Şekil 3.6. Yük Dengelenmemiş Tek Yol Kullanımı



Şekil 3.7. Otomatik Atanmış Yük Dengelenmiş Yol Kullanımı



Şekil 3.8. Yapılandırılmış Çoklu Yol Kullanımı

Şekil 3.6'da tüm sanal yerel alan ağ trafiklerinin tek hat üzerinden akmasıyla toplam bant genişliklerinin hat bant genişliği kapasitesini aşması durumunda gecikmeler veya paket kayıpları yaşanır. VLAN'ların toplam bant genişliklerinin p2 veya p3 hatlarının bant genişliğini aşması durumunda iletimi kritik olan Vlan201 veya Vlan202 paketlerinin hedeflerine eksiksiz ve zamanında ulaşmasında riske yol açar.

Şekil 3.7'de ise Vlan201 ve Vlan202 trafiklerinin otomatik olarak aynı hat üzerine atandığını varsayarsak bu iki trafiğin toplam bant genişliğinin p6 veya p7 hatlarının bant genişliğini aşmaları durumunda paketlerde gecikmeler ve kayıplar yaşanır.

Şekil 3.8'de ağ yöneticisinin kritik olan Vlan201 ve Vlan 202 trafiklerine birer hat sağladığını varsayarsak bu iki sanal yerel alan ağı trafiğinin diğer trafiklerden etkilenmeksizin yalnızca sırasıyla p4 veya p5 ve p6 veya p7 bant genişliklerinin kapasitesine bağlı olarak iletimi sağlanır.

Ağ yöneticisi iletimi kritik olan sanal yerel alan ağlarını belirledikten sonra imkanlar dahilinde yedek ve boşta olan yolların kritik VLAN trafiklerinin boş yollardan iletimi ile gecikme ve kayıp risklerini düşürür.

3.4. Wi-Fi Kablosuz Ağlar için İyileştirme Önerileri

Geleneksel kurumsal ağlarda kablosuz yerel alan ağları için çoğunlukla Wi-Fi teknolojileri kullanılır. Wi-Fi dünyada en yaygın kullanılan kablosuz ağ teknolojisidir. Wi-Fi teknolojileri kablolu teknolojilerine oranla farklı zorlukları beraberinde getirmektedir. İlk olarak kablosuz ağların çevresel değişkenlerden kolay etkilenen radyo dalgaları olmaları nedeniyle depo, stadyum gibi değişken ortamlarda kapsama sorunları baş gösterir. Örneğin lojistik depolarında yüksek raflar ve raflar içerisinde sürekli değişiklik gösteren malzemeler bulunur. Bazı malzemeler radyo sinyallerini emerken, bazıları ise radyo sinyallerini yansıtırlar. Rafların boş olduğu dönemlerde radyo sinyalleri rafların pozisyonları ve malzeme tipine göre iletilir ya da yansıtılır. Lojistik depolarında lojistik operatörlerin kullandığı Wi-Fi bağlantılı araçlar veya el terminalleri çoğunlukla hareket eder. Hareket esnasında Wi-Fi sinyallerinin raflarda bulunan malzemeler nedeniyle zayıfladığı noktalarda cihazlar bağlantı sorunları yaşarlar. Aynı bölgede raflarda farklı malzemeler olduğunda ya da raflar boş olduğunda sinyal sorunu yaşanmaz. Böyle durumlarda sorunları tespit etmek zorlaşır, çünkü ortamda sürekli olarak kontrol edilemeyen bir değişken bulunur. Benzer bir durum futbol stadyumları için de geçerlidir. Futbol stadyumlarında çok yüksek sayıda Wi-Fi bağlantısı kuran cep telefonu ve IoT cihazları mevcuttur. Futbol izleyicileri veya stadyum görevlerilerinin kullandığı Wi-Fi tabanlı cihazlar hareketleri esnasında bölgesel olarak yoğunluklara neden olabilir. Çok yüksek yoğunluklu kullanımların olduğu noktalarda performans sorunları yaşanabilir. Bu sorunların önüne geçilebilmesi için ortam değişkenleri başlangıçta plana dahil edilmeli ve değişkenlerden en az etkilenecek şekilde kablosuz ağ tasarımı yapılmalıdır. Yapılan tasarım simülasyon ortamlarında doğrulanmalı ve sahaya uygulanması sağlandıktan sonra Wi-Fi ısı haritası çıkarılmalıdır. Kurumların önemli varlıklarının konumlarını takip edebilmeleri için belirlenmiş alanlarındaki Wi-Fi ağlarının

tam kapsama sağlaması gerekir [4]. Kapsama sorunlarının ardından kablosuz ağlarda gecikme değerleri kablolu ağlara oranla yüksek durumdadır. Gerçek zamanlı çalışması gereken IoT sistemler için ağ gecikme sürelerinin artması olumsuz sonuçlar yaratır. Bu noktada kablosuz ağa bağlanacak IoT cihazların gereksinimleri analiz edilmeli ve Wi-Fi ısı haritası üzerinde özellikle sinyal gücünün düşük olduğu noktalarla, dolaşımın sağlandığı noktalar üzerinden gereksinimlere uygun Wi-Fi değerlerinin sağlanabildiği test edilmelidir. Çizelge 3.2'de farklı IoT trafiklerinin bant genişliği tüketimi ve Çizelge 3.3'de 802.11 kablosuz ağ özellikleri verilmiştir.

Çizelge 3.2. Farklı IoT Trafiklerinin Bant Genişliği Tüketimi

Sınıf	Uygulama Bant Genişliği	Örnet IoT Cihazları
1	10 Kbps	Akıllı Lamba, HVAC, Bulaşık Makinesi, Fırın, Garaj Kapısı
2	50 Kbps	Duman Dedektörü, Akıllı Buz Dolabı
3	200 Kbps	Müzik Akışı
4	2,5 Mbps	Akıllı Telefon, Dizüstü Bilgisayar, Video Konferans Cihazı
5	5 Mbps	Video Akışı, Kamera İzleme Sistemi

Çizelge 3.3. 802.11 Kablosuz Ağ Özellikleri

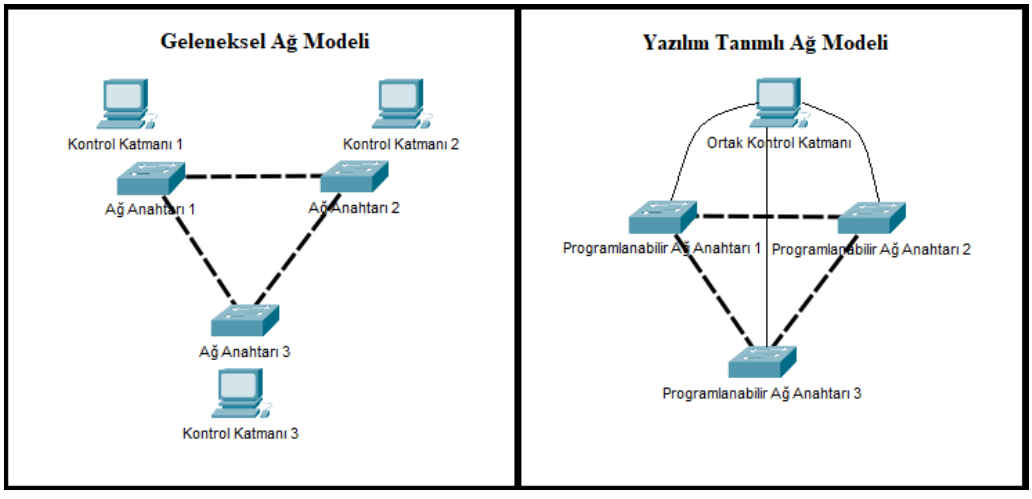
Standart	Frekans	En Yüksek Bant Genişliği	Kanal Genişliği
802.11b	2.4 GHz	Up to 11 Mbps	20 MHz
802.11a	5 GHz	Up to 54 Mbps	20 MHz
802.11g	2.4 GHz	Up to 54 Mbps	20 MHz
802.11n	2.4 veya 5 GHz	Up to 450 Mbps	20 veya 40 MHz
802.11ac	5 GHz	Up to 1300 Mbps	20 veya 40 veya 80 MHz
802.11ax	2.4 GHz	Up to 10 Gbps	160 MHz

Wi-Fi ağları çok farklı frekanslarda yayın yapan diğer kablosuz ağlardan olumsuz etkilenmemesi adına doğru frekans ve kanal genişliği ile seçilmelidir. Yapılan çalışmalardan bazıları Wi-Fi ağları ile diğer IoT kablosuz ağlarının doğru yapılandırma ile birbirlerine etkilerinin göz ardı edilebilir seviyeye indiğini gösterir [12].

3.5. Yazılım Tanımlı Ağlar

Şekil 3.9'da geleneksel ağ ve yazılım tanımlı ağ modeli karşılaştırması verilmiştir. Yazılım tanımlı ağlar ağ cihazlarının gelişmiş yazılım teknolojileriyle merkezi bir sistem üzerinden

tek bir ağ sistemi olarak yönetilmesini sağlarlar. Geleneksel yöntemlerle yönetilen ağ cihazlarının her birinin ayrı olarak yapılandırılması ve tek ağ topolojisinin kurgulanması belli zorluklar ve hatalar doğurur. Bu zorlukların ve ağ yöneticilerinin oluşturabileceği hataların önüne geçilmesi için ağ sistemlerinin topolojiye uygun şekilde yapılandırılması gerekir. Ancak her geçen gün yeni sistemlerin eklendiği yapısı büyüyen ve karmaşıklaşan kurumsal ağlarda topolojiye uygun yapılandırmaların sağlanması zorlaşmaktadır. Yapılandırma hatalarından ve ihtiyaca uygun yapılandırmaların gecikmesinden kaynaklı olarak ağ performanslarında ciddi miktarda kayıplar yaşanır. Bu kayıpların yanında her gün yenisi eklenen siber güvenlik tehditlerinin önüne geçilmezse geç kalınır. Tüm bu zorlukların önüne geçilmesi açısından yazılım tanımlı ağların kurumsal ağlara uygulanması kaçınılmazdır. SDN teknolojileri ağ yöneticilerinin ağları bütüncül ve sistematik olarak yönetmesini sağlar [4] . Yazılım tabanlı ağların kullandığı güçlü yapay zeka analiz kapasitesi ağ sistemleri ve kullanıcı deneyimi üzerinde yüksek görünürlük sağlar [4]. SDN teknolojileri kullandığı kapsamlı veri analizleri ile IoT ağ trafiklerinin iletiminde kaynak paylaşımı, servis kalitesi ve garantisi konularında yüksek seviye otomasyon sağlar [13]. Yazılım tabanlı ağların IoT sistemlerinde yüksek performans gösterdiği çalışmalar mevcuttur [13-15].



Şekil 3.9. Geleneksel Ağ ve Yazılım Tanımlı Ağ Modeli Karşılaştırması

Yazılım tanımlı ağlar kurumsal ağların birçok farklı alanında kullanılabilmektedir. Bu tez çalışmasında yazılım tanımlı ağların en çok uygulanmakta olan yazılım tabanlı geniş alan ağı (Software-Defined Wide Area Networking – SDWAN, SD Access) ve yazılım tanımlı veri merkezi (Software-Defined Data Center – SDDC) konularına değinilmiştir.

3.5.1. SD access

Yazılım tanımlı ağların kurumsal ağların kampüs ağı olarak da adlandırılan yerel ağlarındaki kullanımına yazılım tabanlı erişim ağları denilmektedir. Gün geçtikçe sayısı artan bu cihazların bağlantılarını sağlayan yerel alan ağlarındaki cihaz sayısı sürekli artar. Karmaşıklaşan mimari ve ağ cihaz sayısı nedeniyle yönetimin zorlaşması yazılım tanımlı erişim ağlarının faydasını ortaya çıkarır. Yazılım tanımlı erişim ağları ağ cihazlarının otomasyonu ve yerel alan ağındaki trafiğin anlık ve geriye dönük olarak izlenmesini sağlar. Kapsayan ağaç protokolünden kaynaklı tek yol kullanımının önüne yazılım tabanlı erişim çözümleri kullanılarak çoklu yol kullanımı sağlayan çalışmalar yayınlanmıştır [16 - 20].

3.5.2. SD WAN

Kurumsal ağların yerleşkeler arası haberleşmesinin sağlanabilmesi için gerekli olan geniş alan ağlarında dinamik olarak performans odaklı yönetimin sağlanabilmesi için yazılım tanımlı geniş alan ağ altyapılarının oluşturulması gerekir. Yerel alan ağlarına göre internet servis sağlayıcılardan alınan geniş alan ağ hizmetlerinin değişkenliğinin kontrol edilebilirliği düşüktür. Ayrıca geniş ağ alanlarının performans artırımı için gereken sürekli maliyetleri daha yüksektir. Tüm bu sebeplerden kaynaklı olarak geniş alan ağlarının en yüksek iyileştirme ile kullanılması kaçınılmazdır. Geniş alan ağ bağlantılarının anlık olarak izlenmesi ve yaşanan değişimlerde dinamik olarak yüksek performanslı olan bağlantıların tercih edilmesi gerekir. SD-WAN çalışmaları geniş alan ağlarında IoT performansını olumsuz etkileyen uçtan uca gecikmeleri azaltmak için kullanılır [21].

3.5.3. SDDC

Kurumsal ağlarda verinin depolandığı yedeklendiği ve ulaşıldığı alanlar olan veri merkezlerinin yazılım tabanlı yönetilmesi yazılım tabanlı ağların faydalarından yararlanılması gerekir. Dinamik olarak performans yönetiminin sağlanması sunucular arasında yüksek güvenlik düzeyli ve kesintisiz bağlantıların ağ yöneticilerinin hızlı müdahalesine gerek kalmadan yapılması kritiktir. Bir çok çalışma yazılım tabanlı veri merkezi yönetiminin geleneksel veri merkezi ağlarına göre daha yüksek performans sağladığını gösterir [22-23].

4. TEST VE BULGULAR

Ağ simülasyonları ağ tasarım ve yapılandırmalarının testleri ve yapılabilirliğinin onayı için kolay ve maliyet etkin bir yöntemdir [24]. Performans ölçümü ve yapılandırma testi odağıyla yapılan akademik çalışmalarda GNS3 simülatörü sıklıkla kullanılmaktadır [25-34]. GNS3 ağ cihazlarını sanallaştırılmış sürümlerini kullanıma sunan teknolojisiyle, Packet Tracer ve Boson Netsim gibi rakiplerinden ayrılarak ağ topolojilerinde gerçeğe yakın sonuçlar verir, ancak yüksek sistem hesaplama gücüne ihtiyaç duyar [35]. Bu tez çalışmasında önerilen yapılandırmaların doğrulamasını yapmak amacıyla Grafik Ağ Simülatörü 3 (Graphical Network Simulator 3 - GNS3) ağ simülasyonu yazılımı, Oracle Virtualbox sanallaştırma yazılımı, Ostinato paket üreteç yazılımı ve Wireshark paket dinleme yazılımlarından yararlanılmıştır. GNS3 ağ tasarımı ve simülasyonu yapmayı sağlayan açık kaynak kodlu ve ücretsiz bir yazılımdır. GNS3 Cisco, Juniper, Arista, HP, Fortigate gibi birçok ağ cihazının sanallaştırılmış sürümlerini kullanır. Bu sayede ağ tasarımları ve yapılandırmaları gerçek ortama geçmeden çok kez test edilerek gereksinimlere en uygun hale getirilir. GNS3 ağ cihazlarının sanallaştırılmış sürümlerini çalıştırmasının yanında sanallaştırma ortamlarındaki birçok sunucuya bağlantı kurulmasını ve farklı testlerin yapılmasını sağlar.

GNS3 yanında çalışmada Ostinato ağ paket üreteci, Wireshark ağ izleme ve analizlerinden yararlanılmıştır. Ostinato paket üreteci GNS3 yazılımı içerisine ek paket olarak yüklenir. Ostinato istenilen hemen her tür TCP ve UDP paketini oluşturur ya da elde edilmiş olan hazır bir paketin üretimini sağlar. Üretilen paketlerin hangi aralıklarla ve ne sıklıkla üretileceği benzeri senaryolar oluşturma imkanı sağlar. Wireshark ağ izleme ve analiz yazılımı GNS3 yazılımı ile uyumlu olup GNS3 üzerinde oluşturulan bağlantılardaki trafikleri kolayca izler. İzlenimi sağlanan ve kaydedilen trafikler üzerinde paket bazlı ya da toplu olarak detaylı analiz yapılması sağlanır.

Simülasyon ortamında birçok farklı yazılımı denemenin yanında sanallaştırılmış donanımların test edilmesi sağlanmıştır. Aynı simülasyon senaryosunda birçok parametre hızlı bir şekilde değiştirilerek test sonuçları karşılaştırılmıştır. Bunun yanında ağ simülasyon ortamlarının hız ve performans açısından kısıtları bulunmaktadır. Ağ cihazı üreticileri sanallaştırdıkları ağ cihazlarının performanslarına kısıt uygulayarak ilgili ortamların yalnızca simülasyonda kullanılmalarını istemektedir. Örneğin bir ağ anahtarının sanallaştırılmış hali kullanılmak istendiğinde normalde 1 Gbps mertebelerinde olan hızlar

birkaç Mbps'a düşer. Ağ simülasyonu kapsamında nesnelerin interneti ve kurumsal ağları örneklemesi açısından kısıtlı bir küme kullanılarak ağ yönlendirme cihazları üzerinde yapılandırmalar yapılmıştır. Simülasyonun daha sağlıklı çalışması açısından uç cihaz, ağ cihazı sayıları ve bant denişlikleri karşılaştırmayı sağlayabilecek asgari seviyede tutulmuştur. Ölçeklendirme yöntemiyle görece düşük trafik yoğunluğu ve az cihaz sayısı ile yapılan simülasyonlar gerçek ortamlardaki tasarım ve yapılandırmalar konusunda kestirim sağlamışlardır. Simülasyon senaryosu elle ayarlandığı için ağ trafiklerinin başlatılma ve trafik izleme zamanları farklılık göstermektedir. Zamanlama yerine her iki trafiğin anlık olarak aktığı senaryolar baz alınarak, kurumsal ve IoT trafiklerin aynı anda bulunduğu aralıklar karşılaştırılmıştır. EntGenerator cihazlarının ürettiği trafikler kurumsal ağ trafiğinin örneğini teşkil edecek şekilde TCP trafiklerden oluşturulmuştur. Gerçek dünyada kurumsal ağlar yalnızca TCP trafiklerine indirgenemez ve yapıları çok karmaşıktır. Ancak simülasyon ortamlarında sonuçların daha doğru alınabilmesi için kurumsal ağların TCP trafiklerden oluştuğu varsayılır. IoTGenerator cihazlarının ürettiği trafikler IoT ağ trafiklerine benzer şekilde UDP ağ trafiklerinden oluşur. Bazı IoT standartları taşıma katmanında TCP desteği sağlasa da, IoT standartlarının büyük bir çoğunluğu UDP protokolünü kullanmaktadır [8]. Özel bir yapılandırma olmaması durumunda ağ trafiklerinin dördüncü katman portları önemsenmemiştir. Yalnızca QoS simülasyonunda IoT trafiğinin UDP port numarası önem teşkil etmektedir. Simülasyonlar genel olarak üç farklı durumu incelemektedir. Birinci durumda IoT ağ trafiğinin ikinci katmanda kurumsal ağlardan tamamen izole olduğu ve farklı IP aralıklarına sahip olduğu durum senaryosu mevcuttur. İkinci senaryoda IoT cihazları ile kurumsal uç cihazların aynı yerel alan ağında ve aynı IP alt ağlarında olduğu yapı mevcuttur. İkinci senaryoda IoT cihazların ayırt edilmesi için ürettikleri trafik bilgisi kullanılmıştır. Üçüncü senaryoda hem ikinci katman izalosyonu hem de aynı IP alt ağlarında bunun trafikler için testler yapılmıştır.

Birinci senaryo olan kapsayan ağaç protokolü yük dengeleme simülasyonunda VLAN bazında ikinci katmanda segmente edilmiş olan IoT trafiğinin kurumsal trafiklerle birlikte tek hat ve ayrı hatlar üzerinde akış karşılaştırılması yapılmıştır.

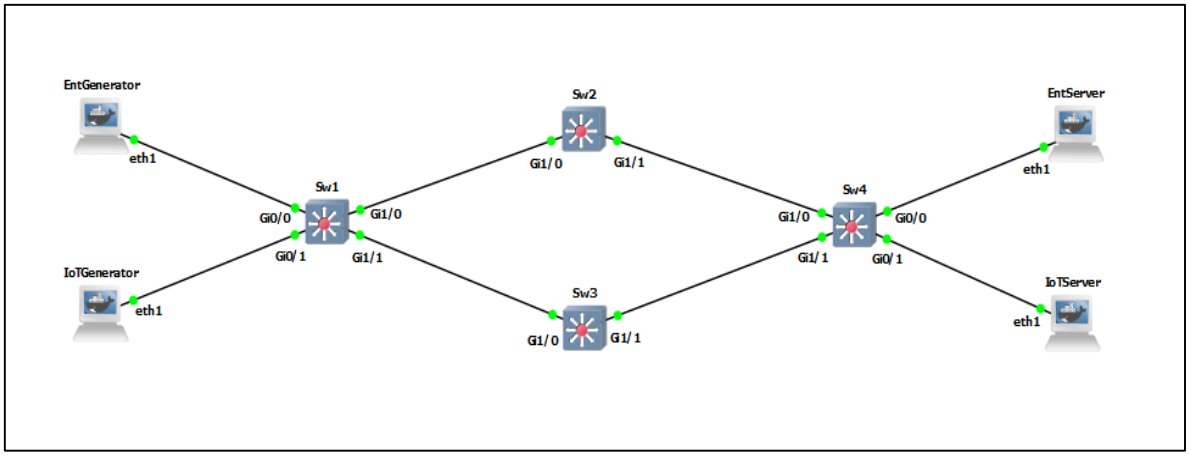
İkinci senaryo olan QoS simülasyonunda IoT paketleri yedi katmanlı OSI mimarisindeki dördüncü katmanda kullanılan hedef porta göre önceliklendirilerek bant genişliği ve gecikme değişimi gözlemlenmiştir.

Üçüncü senaryoda birinci ve ikinci senaryodaki yapılandırmalar birlikte kullanılarak sonuçları gözlemlenmiştir.

Testler ağ anahtarları üzerinde başlangıç yapılandırması olarak bulunan hızlı kapsayan ağaç protokolü ile yapılmıştır. Hızlı kapsayan ağaç yapılandırma protokülünün her Vlan için farklı işlem yapabilme özelliğinden yararlanılmıştır.

4.1. STP Simülasyonu

STP Simülasyonu için Şekil 4.1'deki ağ topolojisi kullanılmıştır. Simülasyon ortamında iki trafik üreteci, dört ağ anahtarı ve iki sunucudan oluşan topoloji kullanılmıştır.

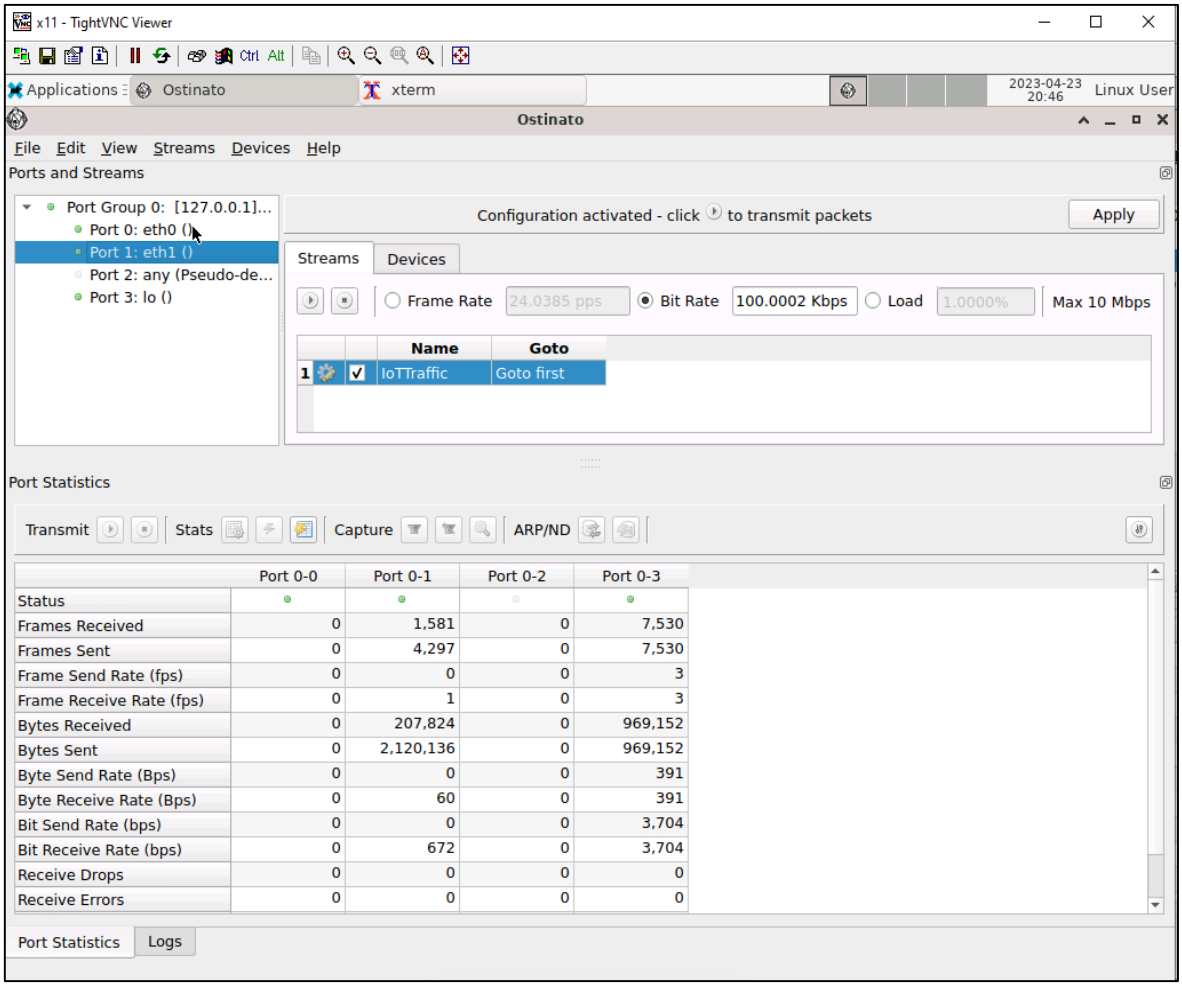


Şekil 4.1. STP Simülasyon Topolojisi

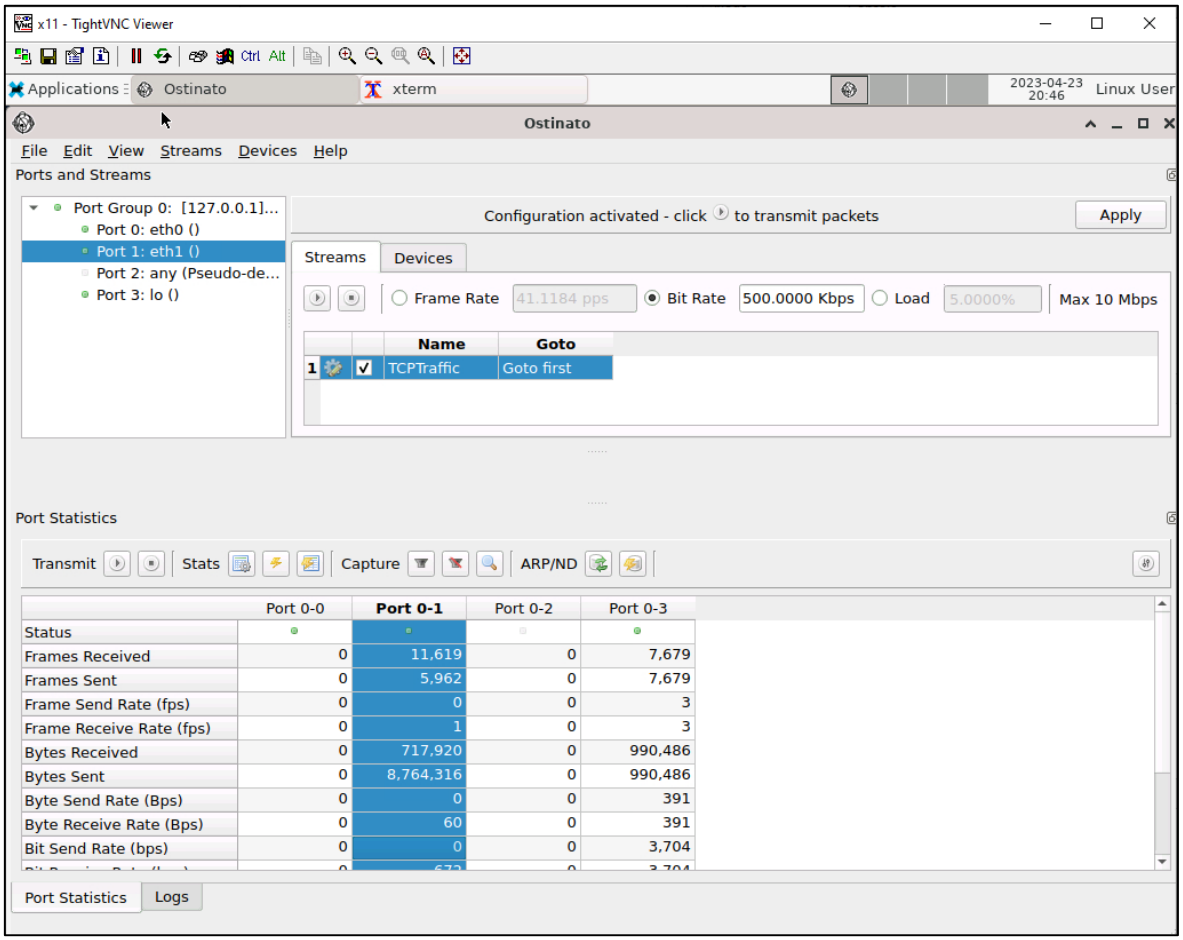
Bu testteki amaç yük paylaşımı olmadan kullanılan standart RSTP ile üretilen kurumsal trafiklerle IoT trafiklerinin aynı hat üzerinden gittiği durumu simüle etmek ve sonrasında yük paylaşımı ile ortak yol kullanımının önüne geçilmesi ve sonuçların karşılaştırılmasıdır. Günümüz dünyasına göre küçültülmüş olan 100 Kbps IoT trafiğinin ölçeğinde ağ anahtarlarının birbirleri arasındaki gidiş arayüzlerinde 500 Kbps sınırlandırması uygulanarak trafiklerin kısıtlı ağ şartlarında nasıl tepki verecekleri gözlemlenmiştir. Benzer trafikler 200 kat büyütülerek gerçek ortamlara uyarlanabilir boyutlara getirilebilir. Böylece gerçek ağ tasarımları ile ilgili ön fikir elde edilmiş olur.

4.1.1. Tek hat STP simülasyonu

Şekil 4.2.'de IoTGenerator olarak gözüken trafik üreteci 100 Kbps UDP trafik oluşturacak şekilde yapılandırılmıştır. Paketler 500 Byte boyutundadır.



Şekil 4.2. Ostinato IoT Paket Üreteci



Şekil 4.3. Ostinato Kurumsal Paket Üreteci

Benzer şekilde EntGenerator üzerinde kurumsal trafiği modellemek amacıyla 500 Kbps TCP trafik oluşturacak yapılandırma vardır. Paket boyutları 1500 Byte olarak yapılandırılmıştır (Şekil 4.3).

```
Sw4#show spanning-tree vlan 1

VLAN0001
  Spanning tree enabled protocol rstp
  Root ID     Priority    1
              Address     0c4d.d9d8.0000
              Cost        8
              Port        5 (GigabitEthernet1/0)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     0c71.f66b.0000
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi0/0               Desg BLK 4         128.1    Shr
Gi0/2               Desg BLK 4         128.3    Shr
Gi0/3               Desg BLK 4         128.4    Shr
Gi1/0               Root FWD 4         128.5    Shr
Gi1/1               Altn BLK 4         128.6    Shr
Gi1/2               Desg BLK 4         128.7    Shr
Gi1/3               Desg BLK 4         128.8    Shr

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------

Gi2/0               Desg BLK 4         128.9    Shr
Gi2/1               Desg BLK 4         128.10   Shr
Gi2/2               Desg BLK 4         128.11   Shr
Gi2/3               Desg BLK 4         128.12   Shr
Gi3/0               Desg BLK 4         128.13   Shr
Gi3/1               Desg BLK 4         128.14   Shr
Gi3/2               Desg BLK 4         128.15   Shr
Gi3/3               Desg BLK 4         128.16   Shr
```

Şekil 4.4. Sw4 Ağ Anahtarı Vlan 1 STP Durumu

```
Sw4#show spanning-tree vlan 201

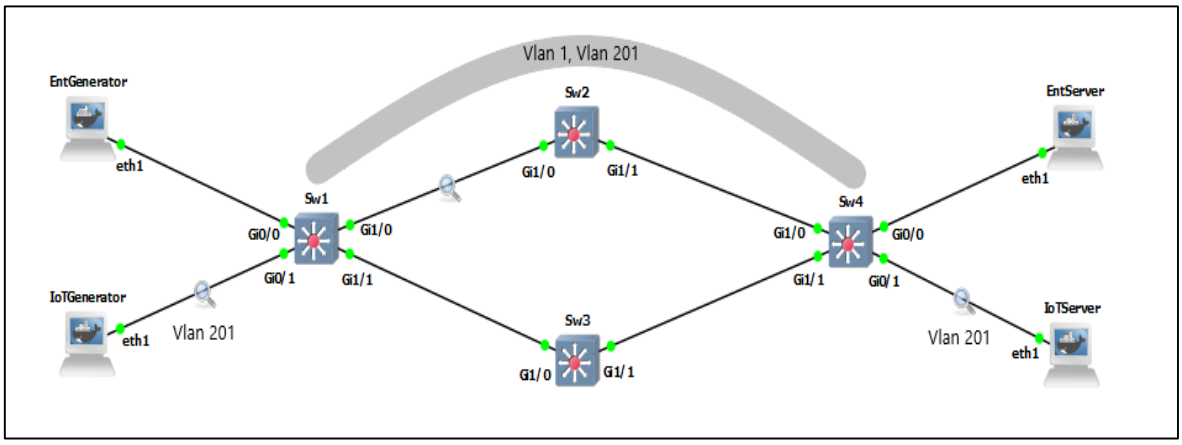
VLAN0201
  Spanning tree enabled protocol rstp
  Root ID     Priority    201
              Address     0c4d.d9d8.0000
              Cost        8
              Port        5 (GigabitEthernet1/0)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32969  (priority 32768 sys-id-ext 201)
              Address     0c71.f66b.0000
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi0/1               Desg FWD 4         128.2    Shr
Gi1/0               Root FWD 4         128.5    Shr
Gi1/1               Altn BLK 4         128.6    Shr
```

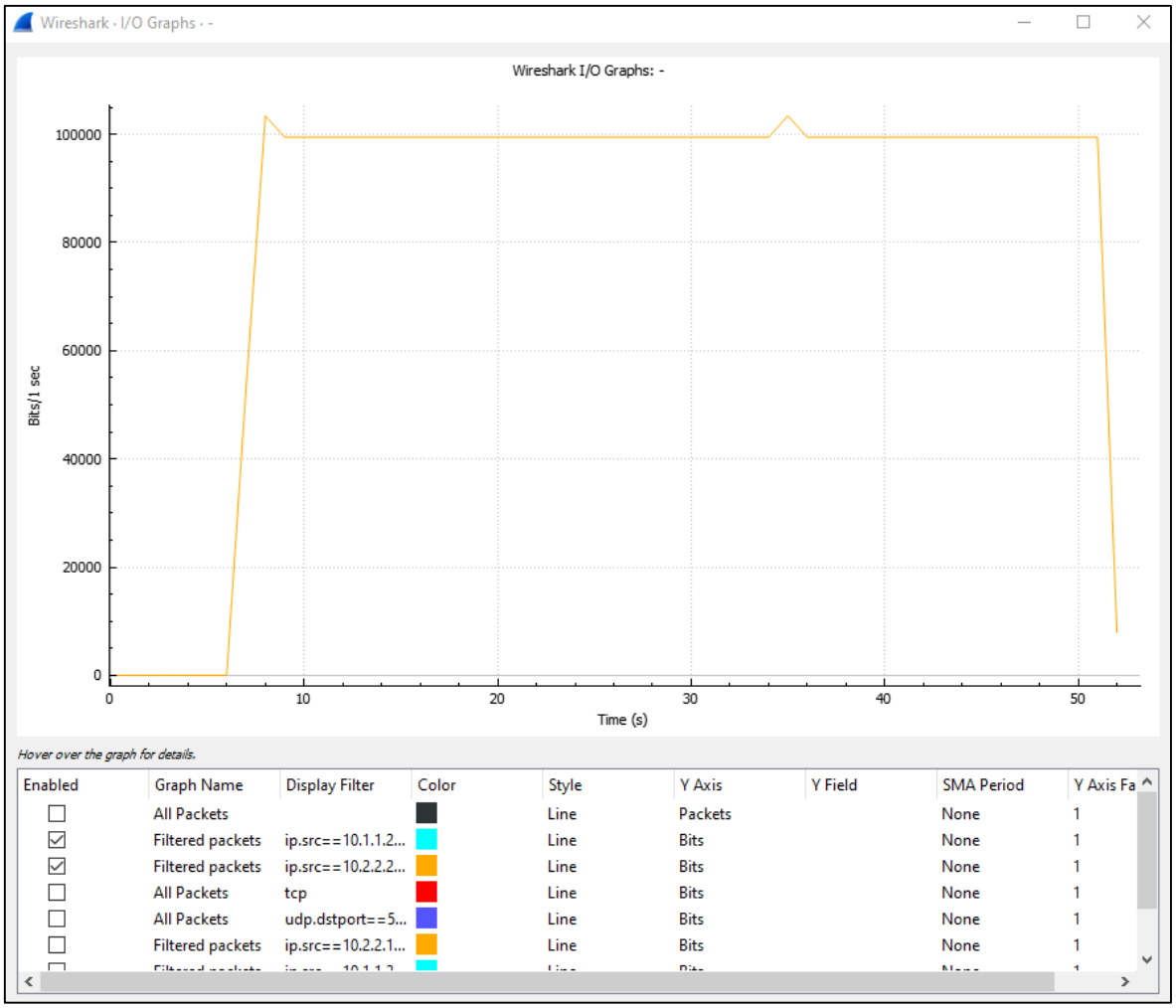
Şekil 4.5. Sw4 Ağ Anahtarı Vlan 201 STP Durumu

Şekil 4.4 ve Şekil 4.5'ten anlaşılacağı üzere Sw4 ağ anahtarının Sw1 ağ anahtarı yönünde bağlantılarını sağlayan Gi1/0 ve G1/1 arayüzlerinden Gi1/0 vlan 1 ve vlan 201 için iletimi sağlar durumda, STP durumları "FWD" yani forwarding (iletiyor) şeklindedir. G1/1 arayüzü her iki vlan için "BLK" yani blocking (durduruyor) şeklinde olup paketlerin kısır döngülere kapılmasını engellemektedir.



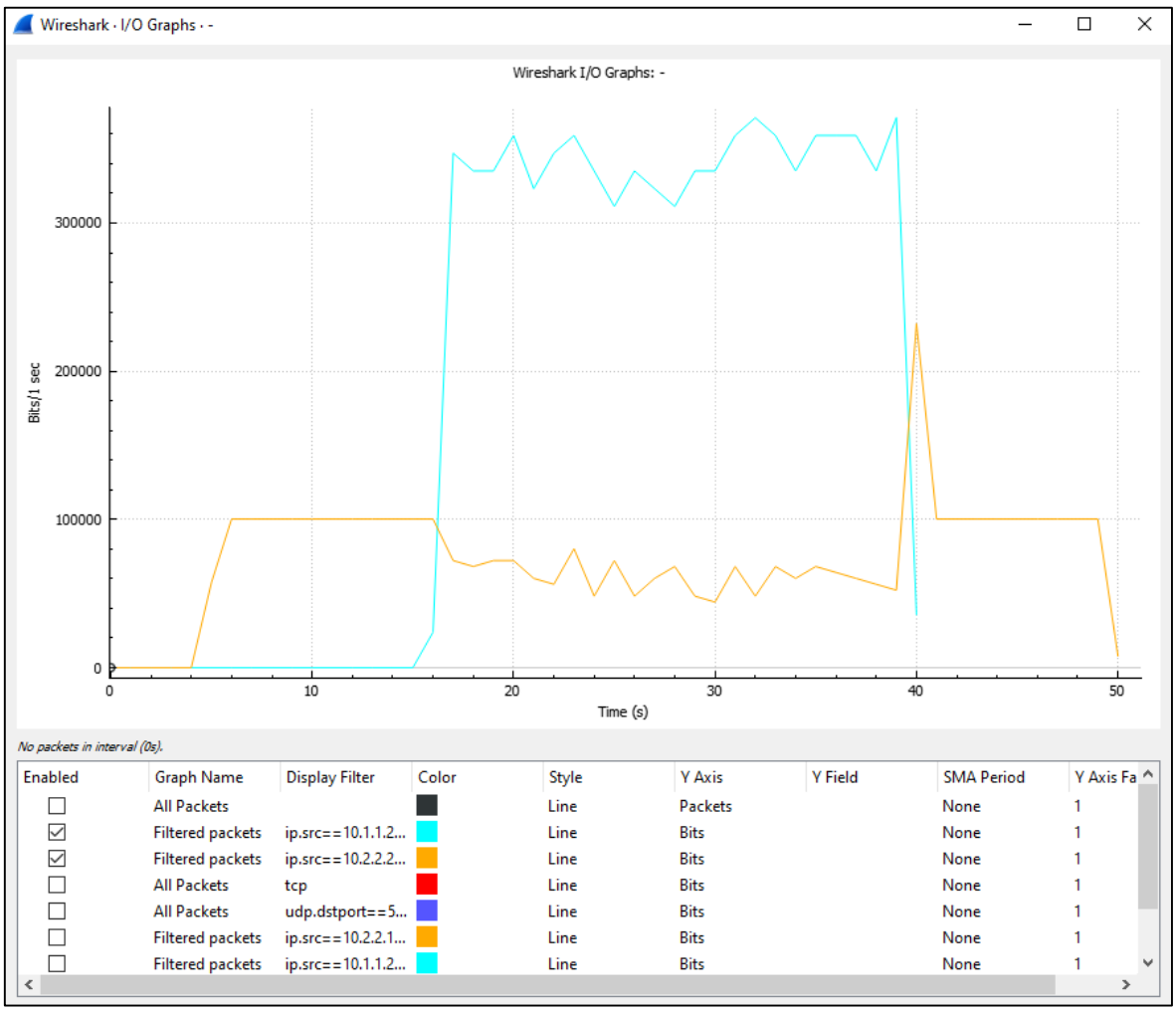
Şekil 4.6. STP Simülasyon İzleme Noktaları

Simülasyon başlamadan önce Şekil 4.6'da büyüteç simgesi ile görüleceği üzere IoTGenerator ile Sw1 ağ anahtarı üzerinden, Sw1 ağ anahtarı ile Sw2 ağ anahtarı üzerinden ve Sw4 ağ anahtarı ile IoTServer üzerinden paket akışları izlemesi başlatılmıştır. İzleme işlemi başlatıldıktan birkaç saniye sonra IoT trafik üreteci başlatılmıştır.



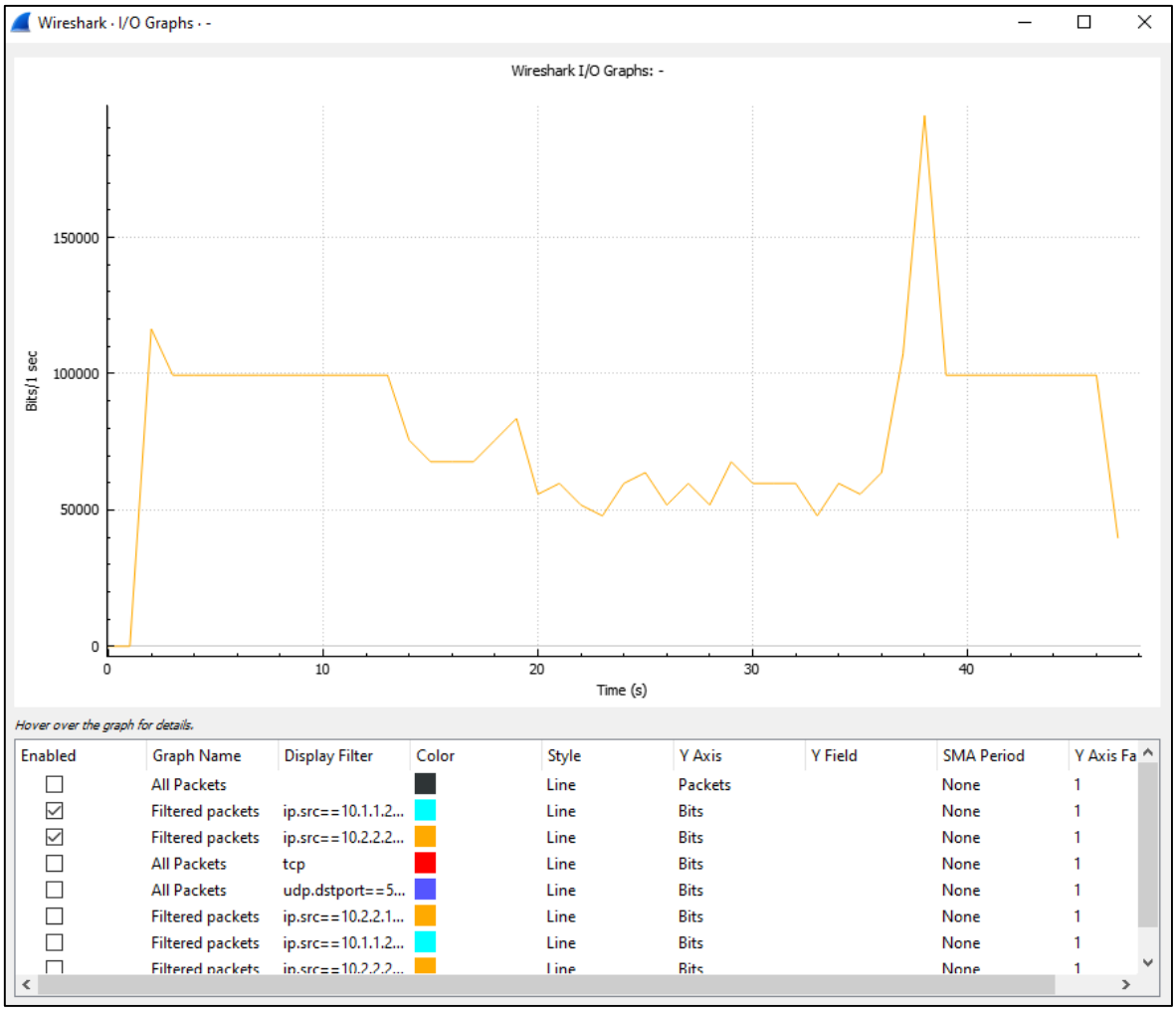
Şekil 4.7. IoTGenerator ile Sw1 Arası UDP Paket Akışı

Şekil 4.7'te görüldüğü üzere IoTGenerator ile Sw1 arasındaki trafik düzenli olarak yaklaşık 100 Kbps seviyesinde geçmektedir. Bu trafik beklenildiği üzere düzenli bir şekilde 100 Kbps civarlarında akmaktadır. Bu izleme noktası diğer noktalarla karşılaştırma yapılabilmesi için referans alınmıştır.



Şekil 4.8. Sw1 ile Sw2 Arası Kurumsal ve IoT Trafik Akışı

Simülasyon izlemelerinin başlatılmasının ardından birkaç saniye sonra IoTGenerator trafik üretmekte ve Şekil 4.8'de sarı renkle gösterilen IoT trafiği 6. ve 16. Saniyeler arasında 100 Kbps hızında akmaktadır. Şekil 4.8'de mavi renkle gösterilen kurumsal trafik 15. Saniye ile 40. Saniye aralığında EntGenerator tarafından iletilir. IoTGenerator ile EntGenerator trafiğinin birlikte geçtiği Sw1 ağ anahtarı ile Sw2 ağ anahtarı üzerinden yapılan ölçümde 500 Kbps kapasite ile sınırlandırılmış hat üzerinde 4. Saniye ile 16. Saniye içerisinde IoT trafiği yaklaşık 100 Kbps olarak düzenli bir şekilde geçmektedir. 16. Saniye sonrasında EntGeneratorün başlatmış olduğu 500 Kbps trafik Şekil 4.8'deki izleme noktasından 300 – 380 Kbps hızında geçerek IoT trafiğinin bant genişliğinde bozulmalar başlar ve paketlerin bir kısmı gecikmeye uğramıştır.



Şekil 4.9. Sw4 ile IoTServer Arası IoT Trafik Akışı

Şekil 4.8'deki izleme noktasında iki trafiğin birbirleri üzerinde olumsuz etkileri IoTServer tarafına ulaşan Şekil 4.9'da görülen IoT trafiğin IoT sunucusuna beklenenden daha gecikmeli olarak ulaşmasına neden olmuştur. Kurumsal trafiğin başlaması sonrasında bant genişliği kaybına uğradığı, geciken ve kuyrukta beklemeye alınan paketlerin bant genişliğinin rahatlamasının ardından iletilmeye çalışıldığı görülmüştür. Şekil 4.9'da 40 saniyede gözlemlenen hızlı artış ortak kullanılan tek hatta kurumsal trafiğin durdurulması anında kuyrukta bekleyen IoT trafiğinin boşalan yolda iletiminden kaynaklanmaktadır. Daha önce de bahsedildiği üzere gecikme toleransı düşük olan kritik IoT uygulamalarında bu tür gecikmeler ve paket kayıpları sistemlerin düzensiz çalışmasına veya durmasına yol açmaktadır.

4.1.2. Yük dengelenmiş STP simülasyonu

Sw4 ağ anahtarı üzerinde bloklanmış olan Gi1/1 arayüzü Sw3 ağ anahtarına bağlıdır. Bu hattın yalnızca vlan 201 sanal yerel alan ağı için kullanılabilir hale getirilmesi için Sw3 üzerinde Şekil 4.10'daki yapılandırma yapılarak Sw3 ağ anahtarının vlan 201 için önceliklendirilmesi sağlanmıştır.

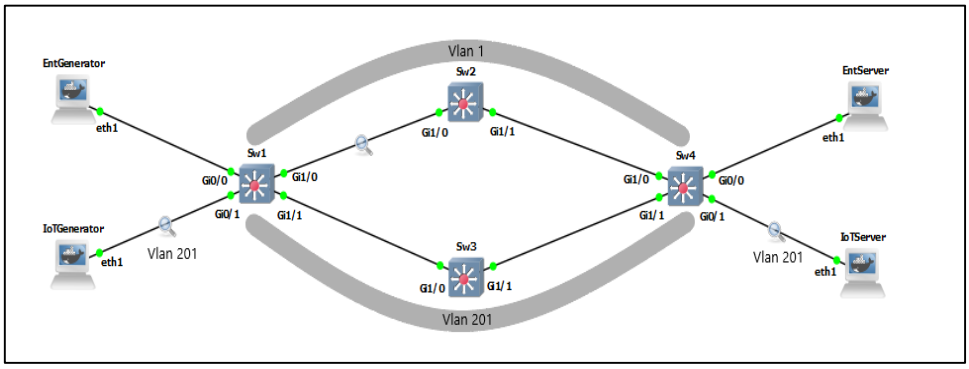
```
Sw3(config)#spanning-tree vlan 201 priority 4096
```

Şekil 4.10. Sw3 Vlan 201 STP Yük Dengeleme Yapılandırması

IoT trafiğinin kurumsal trafikle birlikte akmasının önüne geçmek adına IoT trafiğinin aktığı Vlan201 sanal yerel alan ağının iletim hattı IoTGenerator, Sw1, Sw2, Sw4, IoTServer yerine IoTGenerator, Sw1, Sw3, Sw4, IoTServer Şekil 4.10'da görülen Sw3 ağ anahtarı yapılandırması ile yük paylaşımı sağlanmıştır. İlgili yapılandırma değişikliğinin sonucunun kontrol edilmesi açısından Sw4 ağ anahtarı üzerinde hata ayıklama özelliği açılmıştır. Şekil 4.11'deki hata ayıklama çıktılarında görüleceği üzere vlan 201 için Gi1/1 arayüzü kök port olmuş ve Gi1/0 arayüzü bloklanmıştır. Böylece vlan 201 iletimi boş olan Sw1, Sw3 ve Sw4 arasındaki yoldan yapılarak yük dengeleme sağlanmıştır.

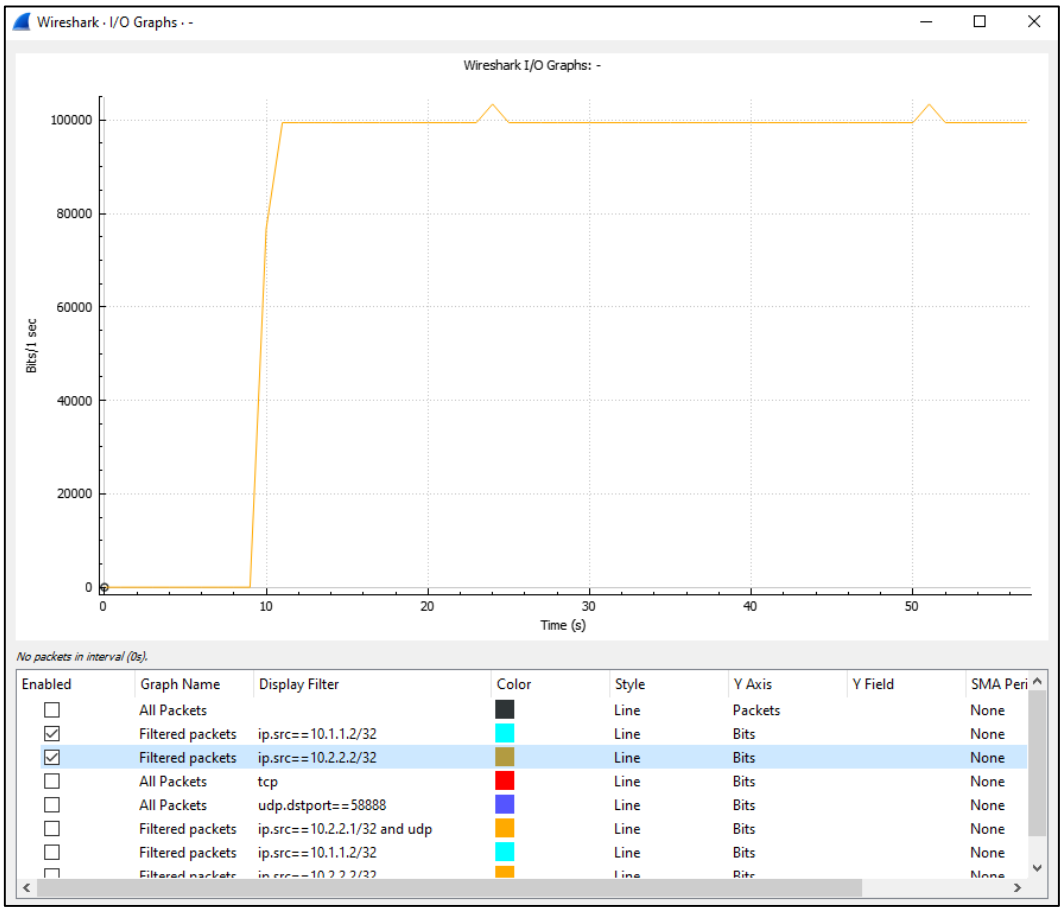
```
Sw4#
*Apr 22 03:44:34.778: RSTP(201): updt roles, received superior bpdu on Gi1/1
*Apr 22 03:44:34.778: RSTP(201): Gi1/1 is now root port
*Apr 22 03:44:34.778: RSTP(201): Gi1/0 blocked by re-root
*Apr 22 03:44:34.778: RSTP(201): syncing port Gi0/1
*Apr 22 03:44:34.778: RSTP(201): Gi1/0 is now alternate
*Apr 22 03:44:34.780: STP[201]: Generating TC trap for port GigabitEthernet1/1
*Apr 22 03:44:34.783: RSTP(201): transmitting a proposal on Gi0/1
```

Şekil 4.11. Sw4 STP Yük Dengeleme Hata Ayıklama Çıktısı



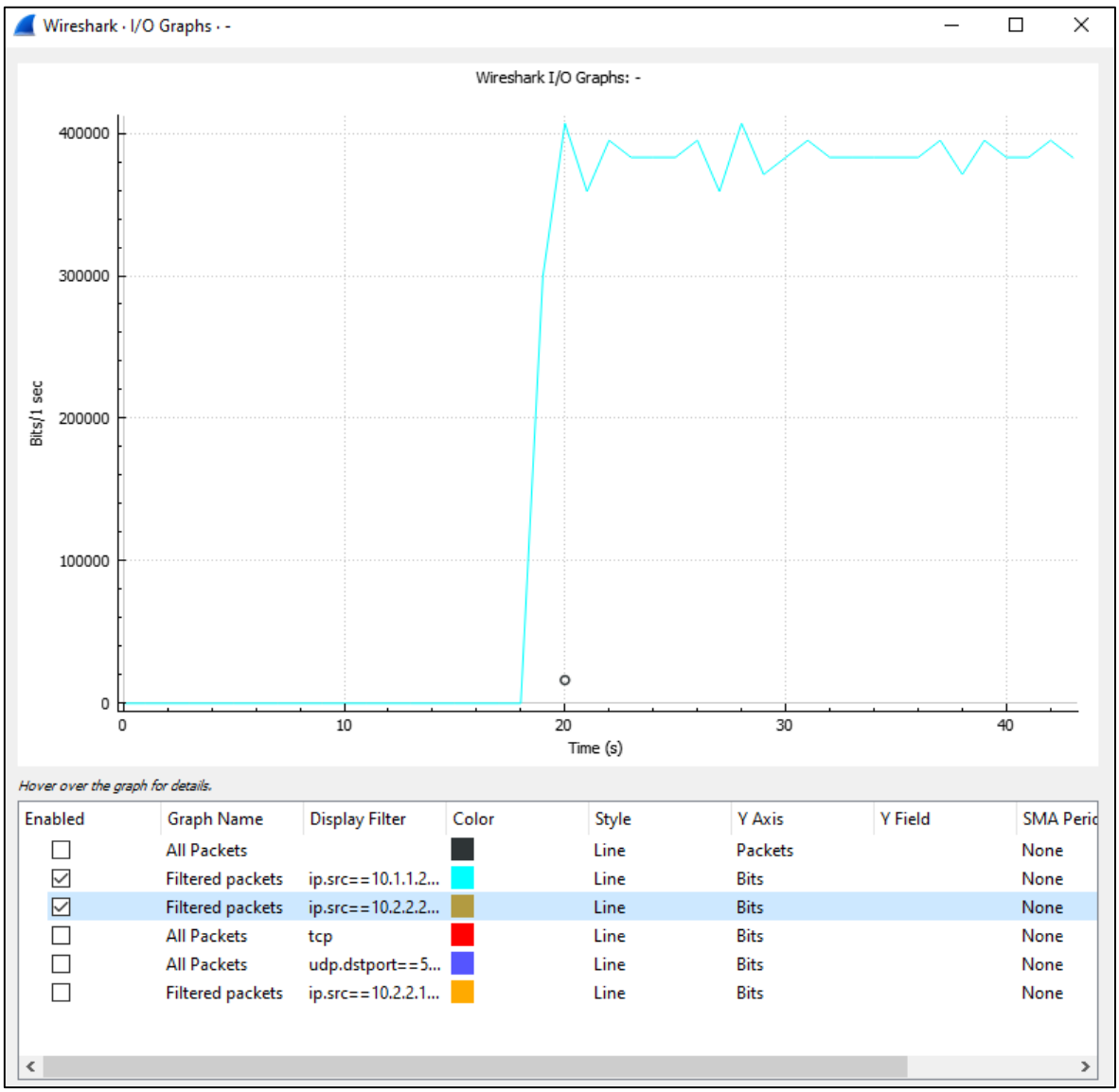
Şekil 4.12. Yük Dengelenmiş STP Simülasyon İzleme Noktaları

İlgili değişikliğin yapılmasının ardından simülasyon tekrar edilerek aynı noktalardan geçen ağ trafikleri izlemeye alınmıştır. Şekil 4.12'de görüleceği üzere Sw1 ağ anahtarı ile Sw2 ağ anahtarları arasındaki bağlantı üzerindeki izleme noktasında yalnızca vlan 1 üzerinden akan kurumsal trafiğin gözlemlenmesi beklenmektedir.



Şekil 4.13. IoTGenerator ile Sw1 Arası Ağ Trafiği

Şekil 4.13. görüldüğü üzere IoT trafiği IoTGenerator ile Sw1 ağ anahtarı arasında 100 Kbps hızında iletilmiştir. Bu trafik sonraki izleme noktaları ile karşılaştırılmıştır.

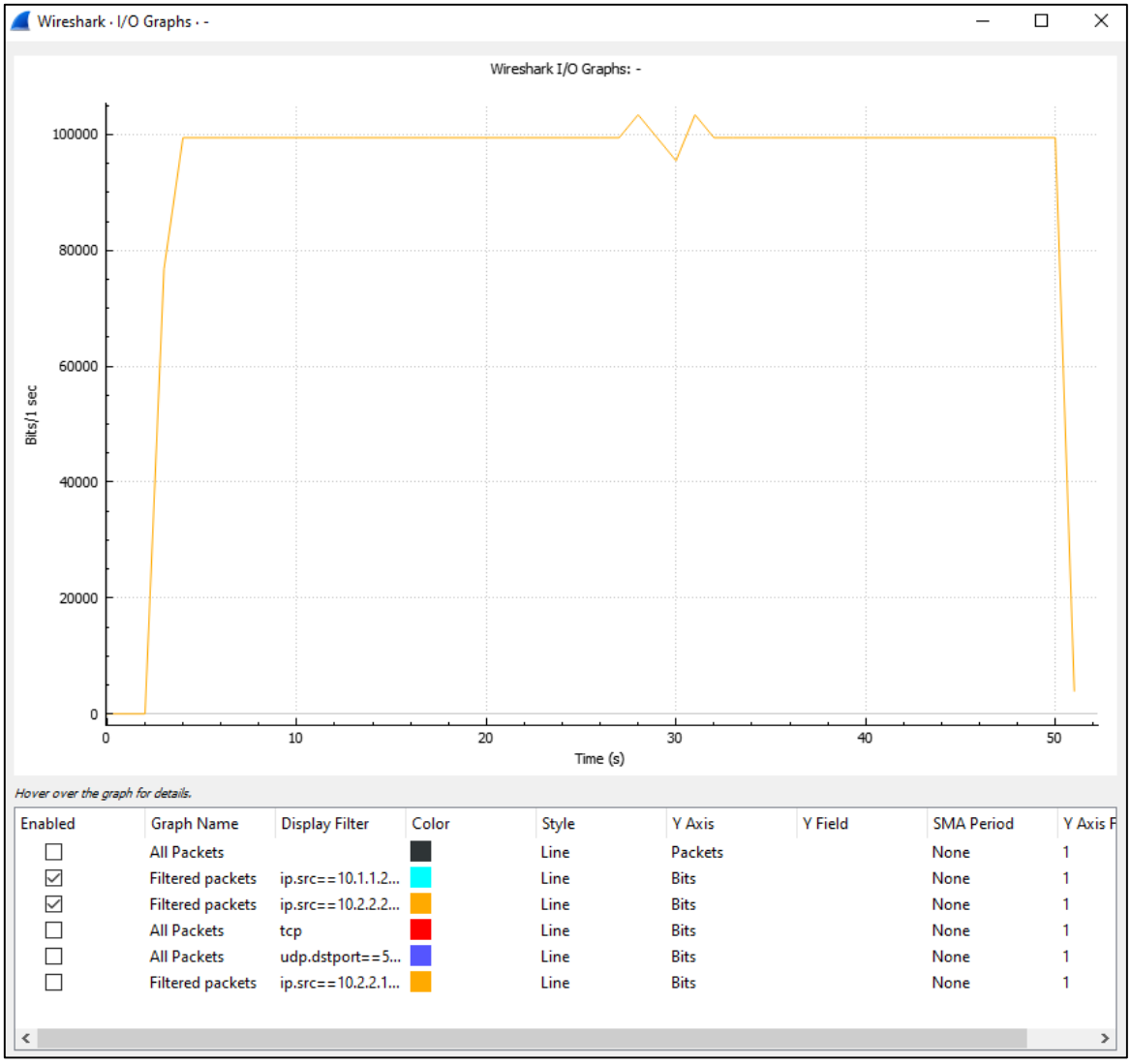


Şekil 4.14. Sw1 ile Sw2 Arası Ağ Trafiği

Daha önce beklendiği üzere Şekil 4.14'teki izleme noktasından yalnızca kurumsal ağ trafiği geçmektedir. Bu çıktı yük dengeleme işleminin sağlamasını gösteren bir unsurdur, ancak tek başına yeterli değildir. IoT trafiğin diğer yoldan hedefe ulaştığı teyit edilerek yük dengeleme işleminin sağlaması yapılmış olur. Şekil 4.14'te görülen diğer bir husus ise 500 Kbps olarak üretilen kurumsal trafiğin izleme noktasından 360 ile 400 Kbps aralığında aktığıdır. Bunun nedeni TCP trafiğin beklenen uygulanan 500 Kbps hız kısıtlamasında daha fazla etkilenmesidir. Şekil 4.15'te görülen istatistiklerde Sw1 ağ anahtarının Gi1/0 arayüzünde iletilen 10518 paketten 3521 adedi beklemeye alınmıştır ve bekleme süresini aşan paketler yok edilmiştir. Bu trafiğin gecikmesi ya da yok edilmesi çalışmamızın konusu olmadığı için söz konusu hız düşüşü göz ardı edilmiştir. Yalnızca ilgili trafiğin IoT trafiği üzerinde etkileri incelenmiştir.

```
Sw1#show traffic-shape statistics
                 Acc. Queue Packets   Bytes     Packets   Bytes     Shaping
I/F              List Depth                     Delayed   Delayed   Active
Gi0/2                 0     2         468       0         0         no
Gi0/3                 0     2         468       0         0         no
Gi1/0                 0     10518     5617664   3521      5083160   no
Gi1/1                 0     8389      1463074   11        660       no
Gi1/2                 0     2         468       0         0         no
Gi1/3                 0     2         468       0         0         no
Sw1#
```

Şekil 4.15. Sw1 Hız Kısıtlama İstatistik Çıktısı

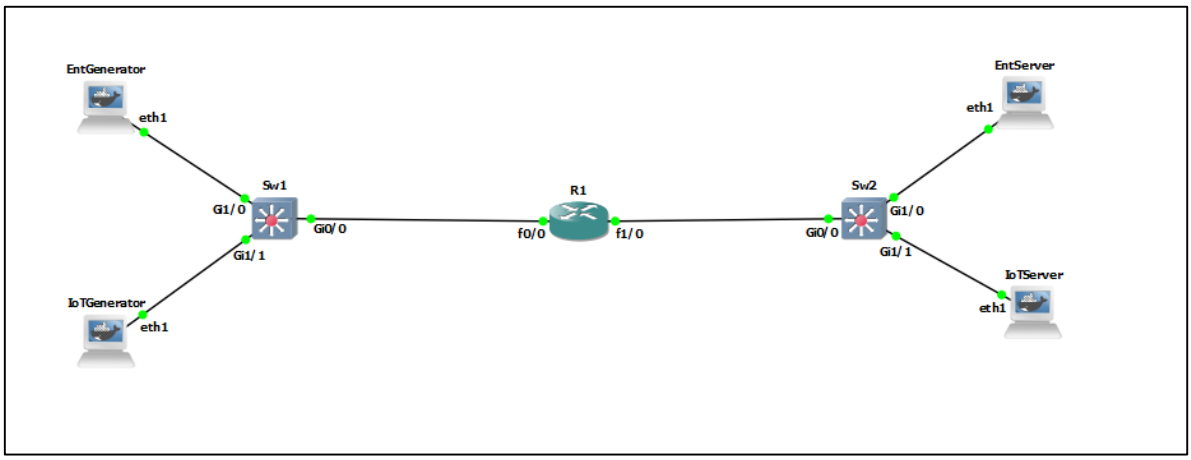


Şekil 4.16. Sw4 ile IoTServer Arası Ağ Trafiği

Yük dengeleme işlemi sonrasında Şekil 4.16'da görüleceği üzere Sw4 ağ anahtarından IoTServer cihazına akan trafik tek hat kullanım durumuna göre daha kararlı bir şekilde iletilmiştir. Kullanılan bant genişliği ile gecikme değişiminin çok daha düşük olduğu

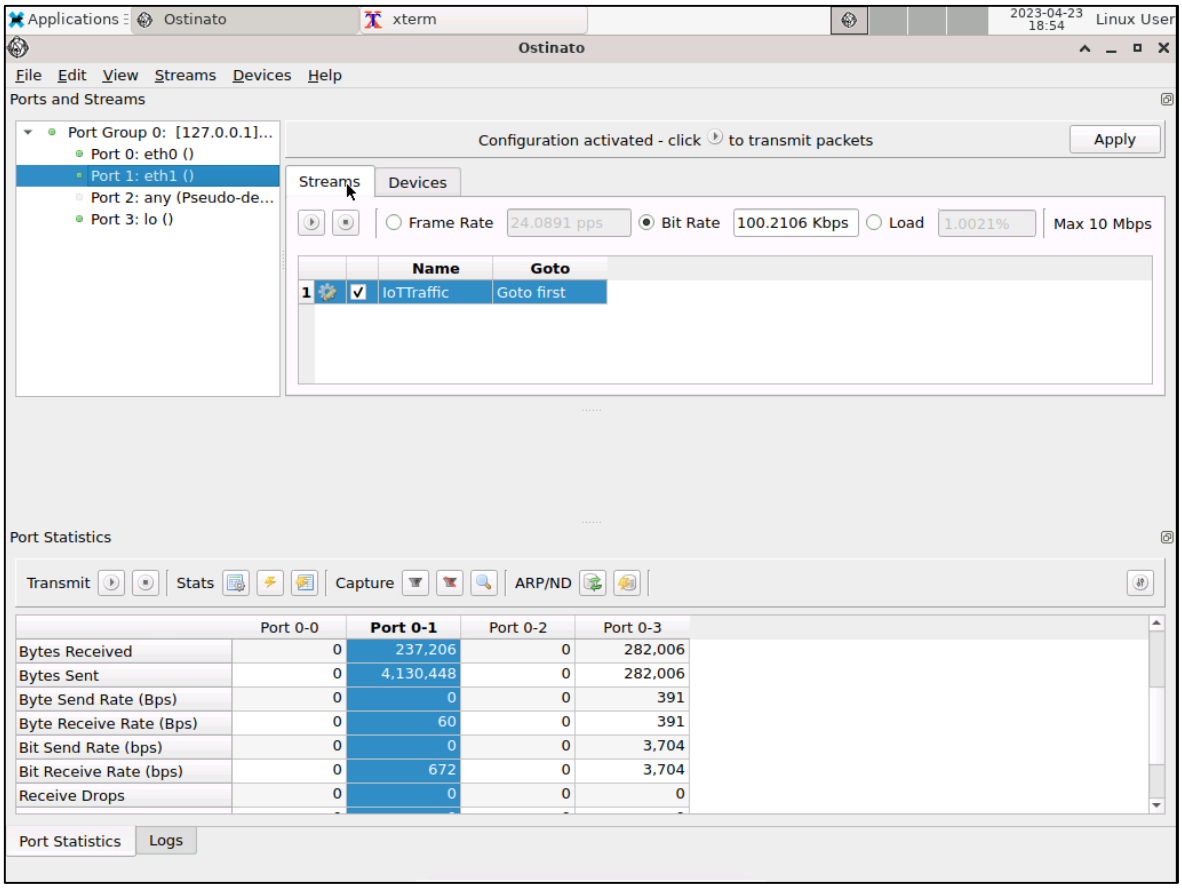
görülmektedir. Şekil 4.13'teki IoTGenerator tarafından Sw1 ağ anahtarına iletilen trafiğin izleme çıktısı ile karşılaştırıldığında çok yakın bir sonuç olduğu görülmektedir.

4.2. QoS Simülasyonu



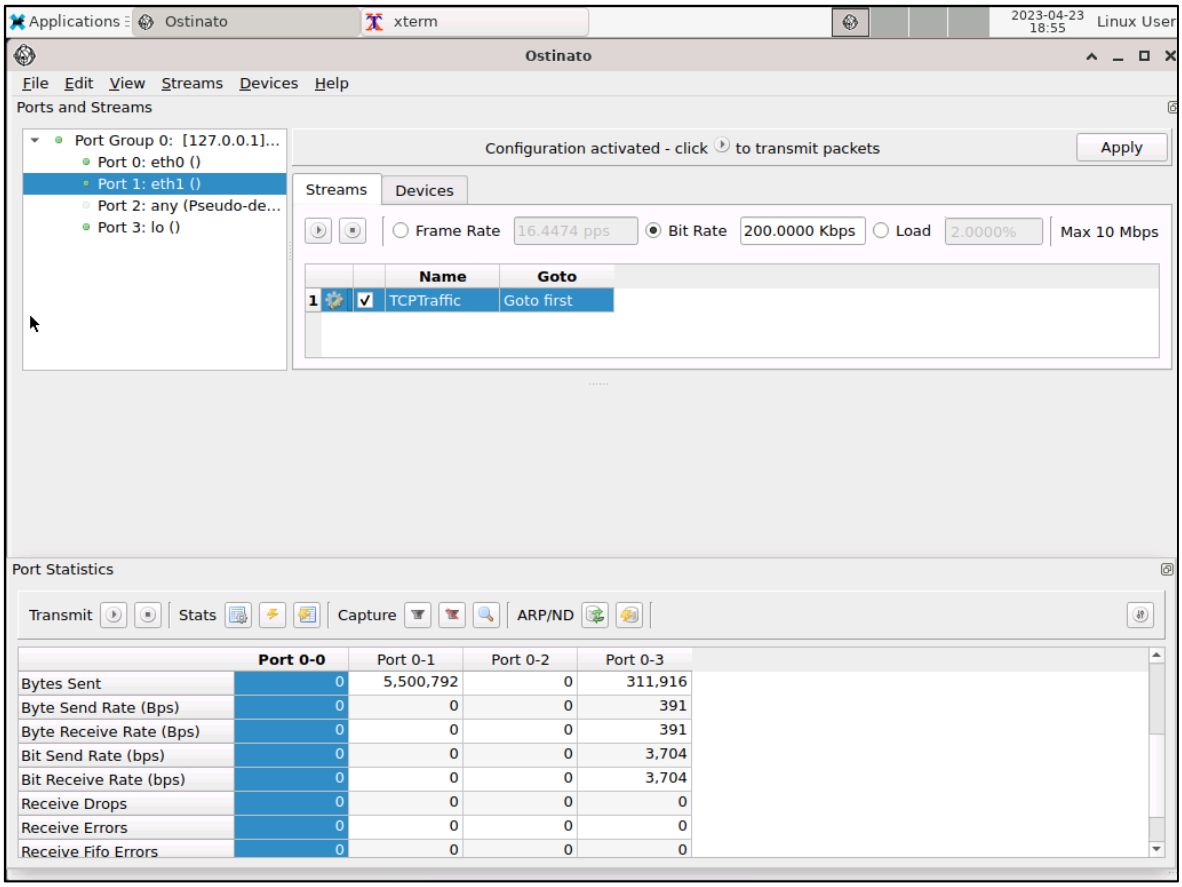
Şekil 4.17. QoS Simülasyonu Ağ Topolojisi

EntGenerator ve IoTGenerator cihazları aynı yerel alan ağı içerisinde olup, cihazlara sırasıyla 10.1.1.2 ve 10.1.1.3 IP adresleri atanmıştır. Ulaşmaya çalıştıkları EntServer ve IoTServer trafik üreteçlerinden farklı yerel alan ağındadır. EntServer ve IoTServer aynı yerel alan ağında olup, cihazlara sırasıyla 10.2.2.2 ve 10.2.2.3 IP adresleri atanmıştır. R1 ağ yönlendirme cihazının f0/0 arayüzüne 10.1.1.1, f1/0 arayüzüne 10.2.2.1 IP adresleri atanmıştır. Sw1 ve Sw2 ağ anahtarları üzerinde herhangi bir yapılandırma olmaksızın ikinci katman trafiklerini başlangıç yapılandırmaları doğrultusunda iletmeleri beklenmektedir.



Şekil 4.18. Ostinato IoT Paket Üreteci

Şekil 4.18'de görüldüğü üzere IoTGenerator cihazı UDP 58888 hedef portu üzerinden IoTGenerator cihazından IoTServer cihazı yönünde 100 Kbps hızında trafik üretmektedir. UDP paketlerin boyutu 500 Byte olarak yapılandırılmıştır.



Şekil 4.19. Ostinato Kurumsal Paket Üreteci

Şekil 4.19'da görüldüğü üzere EntGenerator cihazı EntServer cihazı yönünde 100 Kbps hızında TCP ağ trafiği üretmektedir. TCP paketlerin boyutu 1500 Byte olarak yapılandırılmıştır.

4.2.1. QoS yapılandırma öncesi trafik simülasyonu

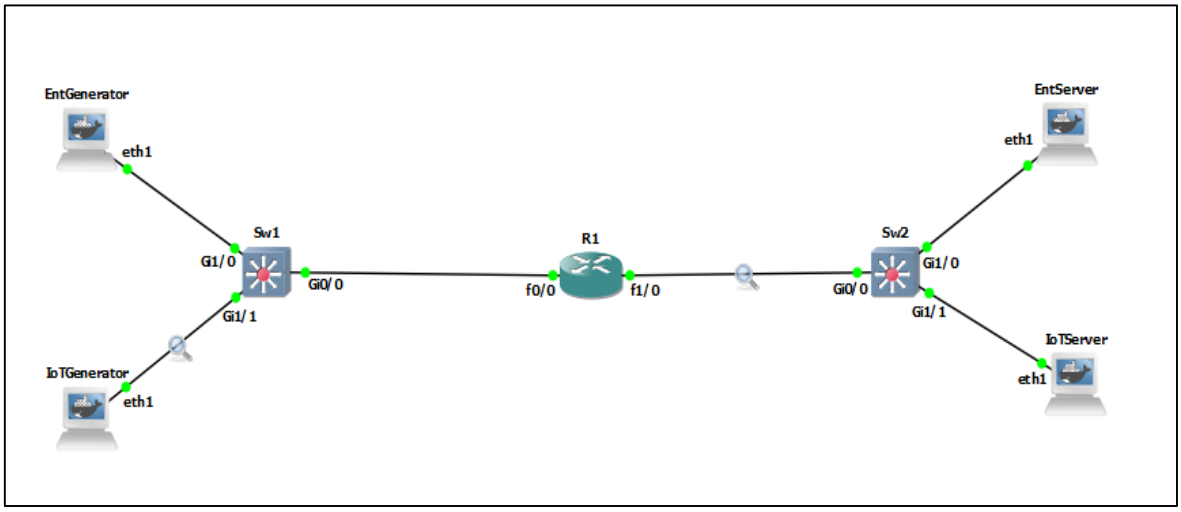
```
class-map match-all POLICE
 match any
class-map match-all IoTcs7
 match dscp cs7
class-map match-all IoT
 match protocol IoTTraffic
!
policy-map POLICE
 class IoTcs7
  police cir 100000
 class POLICE
  police 250000 conform-action transmit  exceed-action drop  violate-action drop
policy-map IoT
 class IoT
  set dscp cs7
```

Şekil 4.20. R1 Ağ Yönlendirici QoS Politikaları

Şekil 4.20'de R1 ağ yönlendiricisi üzerinde yapılandırılmış olan QoS politikaları bulunmaktadır. Senaryonun birinci kısmında Şekil 4.21'de görüleceği üzere QoS politikalarından yalnızca "POLICE" politikası uygulanarak R1 ağ anahtarının f1/0 (FastEthernet1/0) arayüzünde 250 Kbps hız kısıtlamasına gidilmiştir.

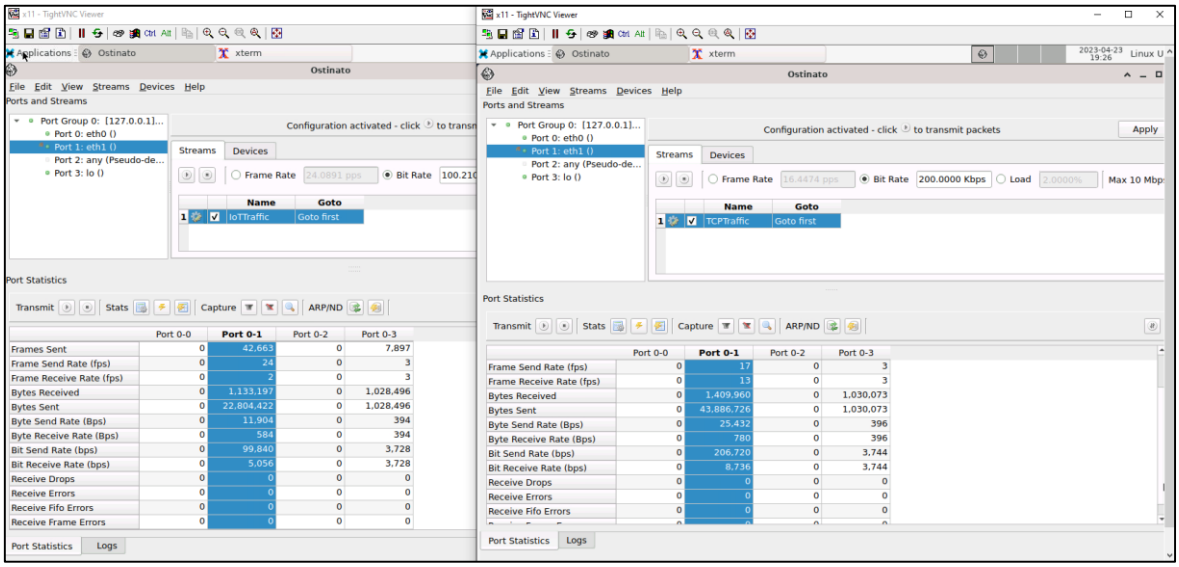
```
interface FastEthernet0/0
 ip address 10.1.1.1 255.255.255.0
 duplex full
!
interface FastEthernet1/0
 ip address 10.2.2.1 255.255.255.0
 duplex full
 service-policy output POLICE
```

Şekil 4.21. R1 Ağ Anahtarı f1/0 ve f1/1 Arayüz Yapılandırması



Şekil 4.22. QoS Simülasyonu İzleme Noktaları

Şekil 4.22'de görüldüğü üzere R1 ağ yönlendiricisi ile Sw2 ağ anahtarı arasındaki bağlantı izleme noktasındaki trafik durumu ile karşılaştırma yapılabilmesi açısından öncelikle IoTGenerator tarafından üretilen IoT trafiğinin IoTGenerator ile Sw1 ağ anahtarı arasındaki bağlantının izlenmesi sağlanmıştır. Sonrasında ağ yönlendirme cihazının önceliklendirme işleminin izlenebilirliği açısından R1 ağ yönlendiricisi ile Sw2 ağ anahtarı arasındaki bağlantı üzerinden izlenmesi sağlanmıştır.



Şekil 4.23. Ostinato Paket Üreteçlerinin Anlık İletim Hızları

Şekil 4.23'te aynı anda üretilen IoT ve kurumsal ağ trafiklerinin anlık iletim hızları sırasıyla 99840 bps ve 209720 bps olarak görülmektedir. Toplamda yaklaşık olarak 300 Kbps hızında bir trafik oluşmuştur. Hız sınırlandırma işleminin çalışırlığının kontrolü açısından Şekil 4.24'teki f1/0 arayüzünden son 5 dakika içerisinde ortalama olarak 292 Kbps hızında akan ağ trafiğinin ortalama 42 Kbps hızındaki kısmı yok edilmiştir.

```
R1#show policy-map interface fastEthernet 1/0
 FastEthernet1/0

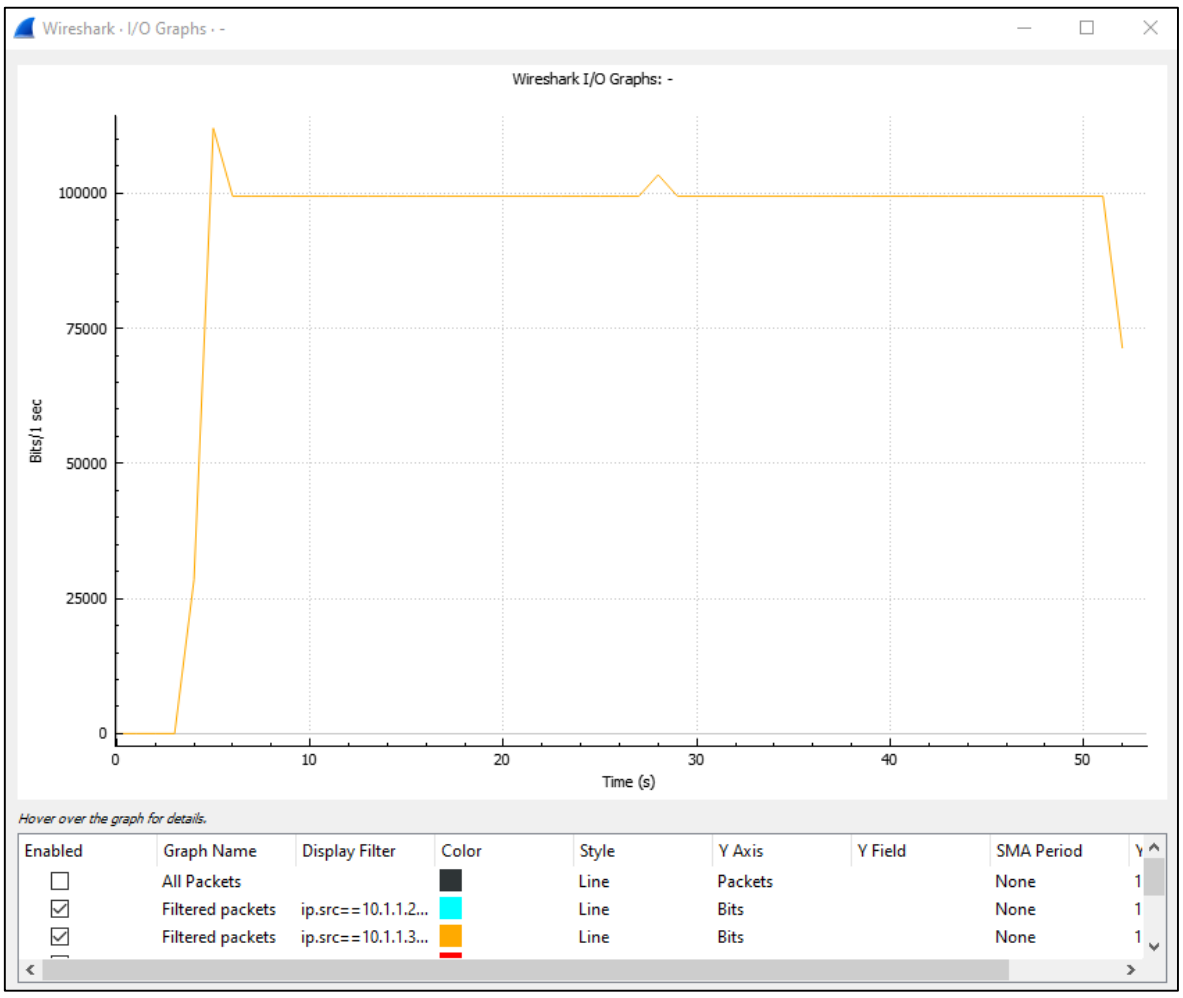
  Service-policy output: POLICE

    Class-map: IoTcs7 (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match:  dscp cs7 (56)
      police:
          cir 100000 bps, bc 3125 bytes
        conformed 0 packets, 0 bytes; actions:
          transmit
        exceeded 0 packets, 0 bytes; actions:
          drop
        conformed 0000 bps, exceeded 0000 bps

    Class-map: POLICE (match-all)
      37503 packets, 33693427 bytes
      5 minute offered rate 292000 bps, drop rate 42000 bps
      Match: any
      police:
          cir 250000 bps, bc 7812 bytes, be 7812 bytes
        conformed 33199 packets, 28793704 bytes; actions:
          transmit
        exceeded 0 packets, 0 bytes; actions:
          drop
        violated 4150 packets, 4885400 bytes; actions:
          drop
        conformed 250000 bps, exceeded 0000 bps, violated 42000 bps

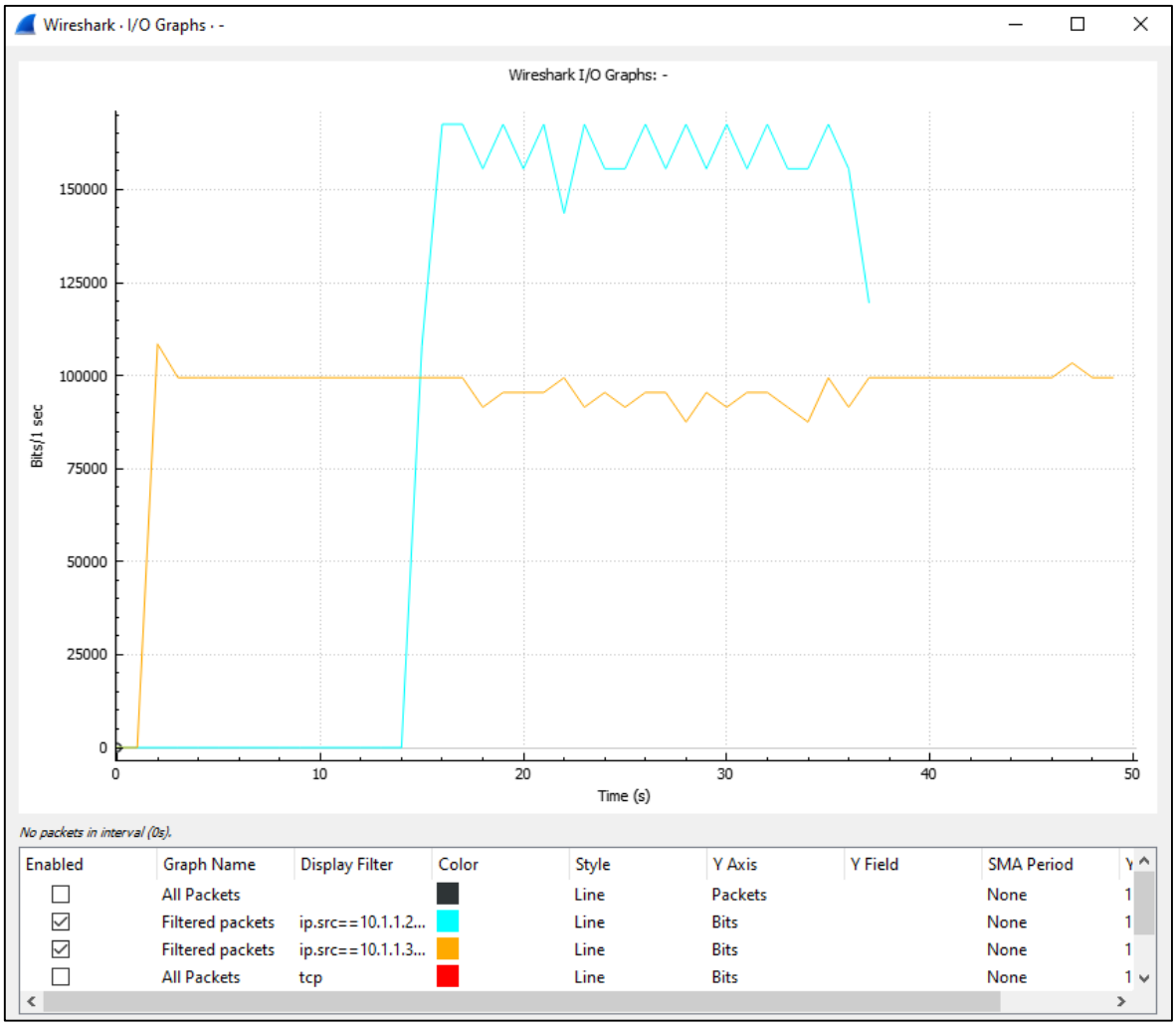
    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: any
```

Şekil 4.24. R1 Ağ Yönlendiricisi f1/0 Arayüzü QoS Politika Çıktısı



Şekil 4.25. IoTGenerator ile Sw1 Arası Ağ Trafiği

Şekil 4.25'te IoTGenerator ile Sw1 ağ anahtarı arasında izlenen trafikte 100 Kbps hızındaki sarı renkle gösterilen ağ trafiği 3. Saniyeden itibaren IoTGenerator yönünden IoTServer yönüne doğru akmaya başlamıştır.



Şekil 4.26. R1 ile Sw2 Arası Ağ Trafiği

Şekil 4.26'da görülen R1 ağ yönlendirici ile Sw2 ağ anahtarı arasında izlenen trafikte ise mavi renkle gösterilen kurumsal trafik ile sarı renkle gösterilen IoT trafiği 17. saniyeden itibaren birlikte akmaktadır. Sarı renkle gösterilen IoT trafiğinin 17. saniyeye kadar kararlı bir şekilde 100 Kbps hızında iletildiği görülürken, 17. saniye sonrasında kurumsal trafiğin aynı hat üzerinden akmaya başlaması ile kararsız hale geldiği, hızının 100 Kbps altına düştüğü ve gecikmelerin arttığı gözlemlenmiştir.

4.2.2. QoS yapılandırma sonrası trafik simülasyonu

Şekil 4.27'de görüleceği üzere UDP hedef 58888 portuyla üretilen IoT trafiğinin önceliklendirilmesi için R1 ağ yönlendirme cihazı üzerinde ağ tabanlı uygulama tanıma (Network Based Application Recognization - NBAR) yöntemi uygunarak trafik ayrımı sağlanmıştır.

```
!
ip nbar custom IoTTraffic udp 58888
!
```

Şekil 4.27. Ağ Tabanlı Uygulama Tanıma Yapılandırması

```
class-map match-all POLICE
 match any
class-map match-all IoTcs7
 match dscp cs7
class-map match-all IoT
 match protocol IoTTraffic
!
policy-map POLICE
 class IoTcs7
  police cir 100000
 class POLICE
  police 150000 conform-action transmit  exceed-action drop  violate-action drop
policy-map IoT
 class IoT
  set dscp cs7
```

Şekil 4.28. R1 QoS Politika Yapılandırması

Şekil 4.28'de görüleceği üzere R1 ağ yönlendirme cihazı üzerindeki toplam 250 Kbps hız sınırlandırılması sağlanabilmesi için IoT trafiği için 100 Kbps ve kurumsal trafikler için 150 Kbps bant genişliği sınırlandırması yapılmıştır.

```
interface FastEthernet0/0
 ip address 10.1.1.1 255.255.255.0
 duplex full
 service-policy input IoT
!
interface FastEthernet1/0
 ip address 10.2.2.1 255.255.255.0
 duplex full
 service-policy output POLICE
```

Şekil 4.29. R1 Ağ Yönlendiricisi f0/0 ve f1/0 QoS Arayüz Yapılandırması

Şekil 4.29'da görüleceği üzere R1 ağ yönlendiricinin arayüzlerine yapılandırmalar uygunlanarak senaryo son haline getirilmiştir. Öncelikle IoT trafiği başlatılmış ve bir süre sonra kurumsal trafik başlatılarak IoT trafiği üzerindeki etkileri gözlemlenmiştir.

```
R1#show policy-map interface fastEthernet 1/0
 FastEthernet1/0

  Service-policy output: POLICE

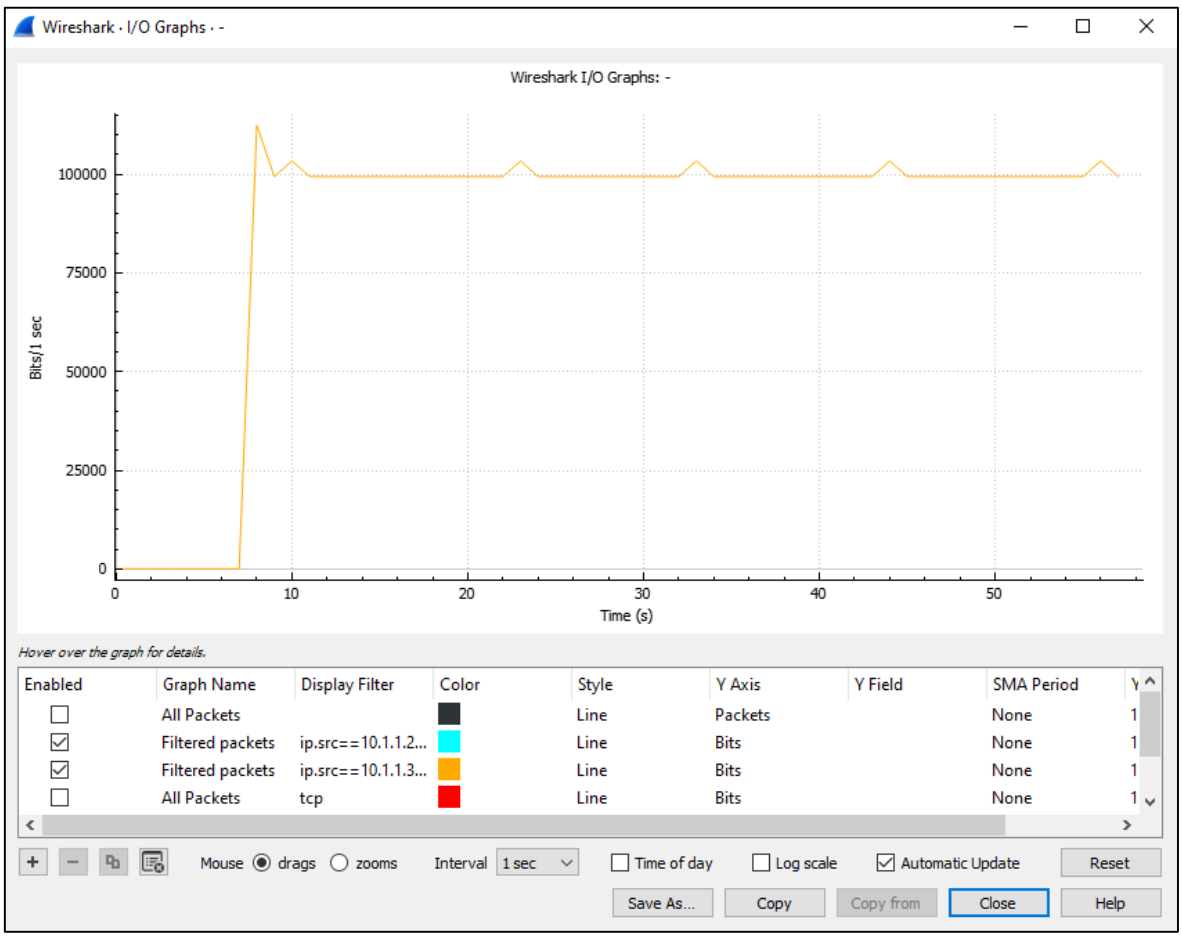
    Class-map: IoTcs7 (match-all)
      20720 packets, 10277120 bytes
      5 minute offered rate 95000 bps, drop rate 0000 bps
      Match:  dscp cs7 (56)
      police:
          cir 100000 bps, bc 3125 bytes
        conformed 20720 packets, 10277120 bytes; actions:
          transmit
        exceeded 0 packets, 0 bytes; actions:
          drop
        conformed 95000 bps, exceeded 0000 bps

    Class-map: POLICE (match-all)
      13417 packets, 19776618 bytes
      5 minute offered rate 196000 bps, drop rate 46000 bps
      Match: any
      police:
          cir 150000 bps, bc 4687 bytes, be 4687 bytes
        conformed 10069 packets, 15063224 bytes; actions:
          transmit
        exceeded 9 packets, 13464 bytes; actions:
          drop
        violated 3128 packets, 4679488 bytes; actions:
          drop
        conformed 149000 bps, exceeded 0000 bps, violated 46000 bps

    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: any
```

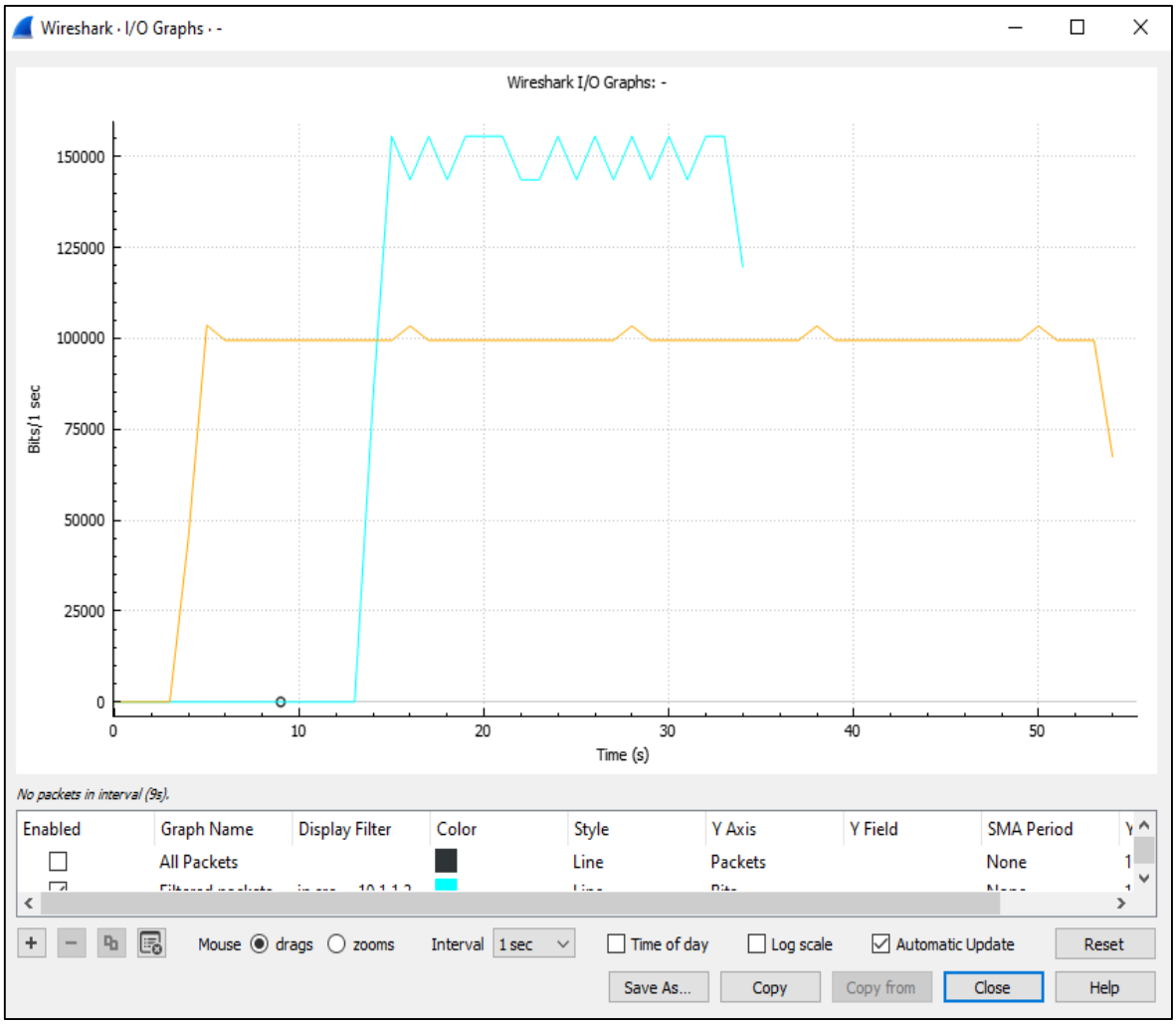
Şekil 4.30. R1 QoS f1/0 Arayüz İstatistiği

Böylece her iki ağ trafiğinin de servis kalitesi politikalarına uygun şekilde yapılandırıldığının kontrolü sağlanmıştır. Şekil 4.30'da görüldüğü üzere "IoTcs7" ve "POLICE" sınıf haritalarından ilgili trafikler akmaktadır. Son 5 dakikalık ortalamalarda "IoTcs7" sınıf haritasına tabi olan 95 Kbps trafik yani IoT trafiği, "POLICE" sınıf haritasına tabi olan 196 Kbps hızında kurumsal trafik görülür. Hız kısıtlamasına tabi olan her iki trafikten kurumsal trafiğin 150 Kbps hız sınırını aşması nedeniyle 46 Kbps hızındaki kısmı yok edilmiştir.



Şekil 4.31. IoTGenerator ile Sw1 Arası İzlenen Trafik

Şekil 4.31'de IoTGenerator cihazı ile Sw1 ağ yönlendiricisi arasındaki bağlantı izlendiğinde yaklaşık olarak 100 Kbps sarı renkle gösterilen IoT trafiğinin iletildiği gözlemlenmiştir.

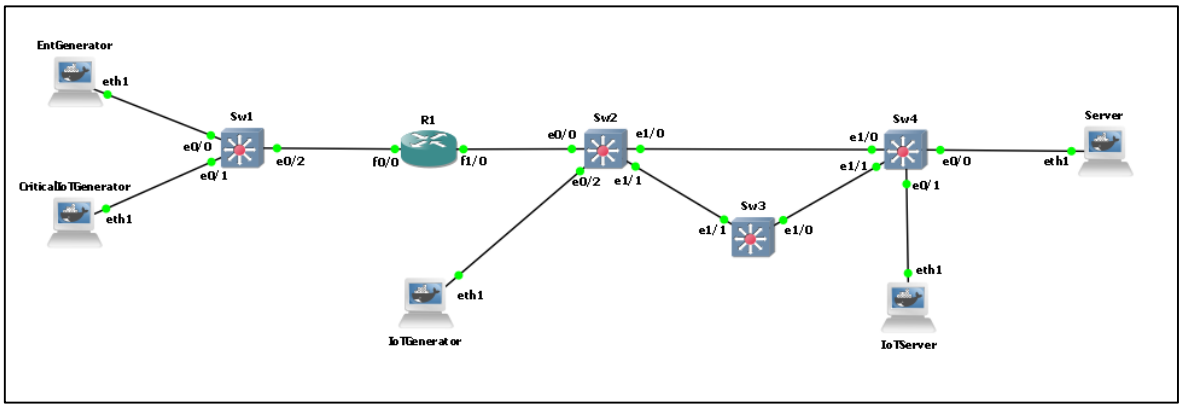


Şekil 4.32. Sw1 ile Sw2 Arası Ağ Trafiği

Şekil 4.32'de R1 ağ yönlendiricisi ile Sw2 ağ anahtarı arasındaki trafik izlendiğinde mavi renkle gösterilen kurumsal trafik ve sarı renkle gösterilen IoT trafiği gözlemlenmektedir. Kurumsal trafiğin 13. saniyeden itibaren başlaması sonrasındaki aralıkta IoT trafiğinin hızında bir değişiklik gözükmez. IoT paketlerinin iletimi QoS yapılandırması sonrasında daha karalı hale getirilir ve gecikme değişimleri kayda değer şekilde azalır.

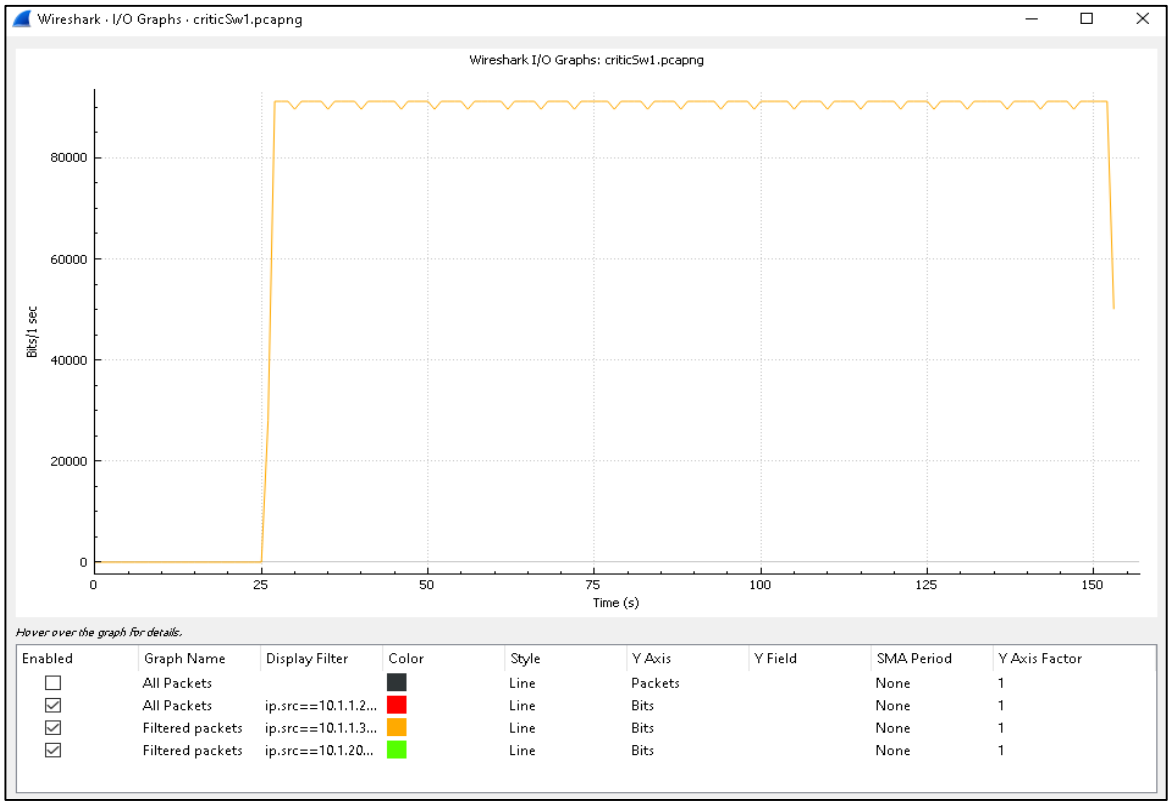
Yapılan simülasyon çalışmalarının çıktısı olarak IoT trafiklerinin ayırt edilmesi ve kurumsal ağlar üzerinde bu trafiklerin gereksinime uygun şekilde önceliklendirilmesi ile IoT trafik iletiminin olumlu yönde etkilendiği gözlemlenmiştir.

4.3. STP-QoS Birleşik Kullanım Simülasyonu

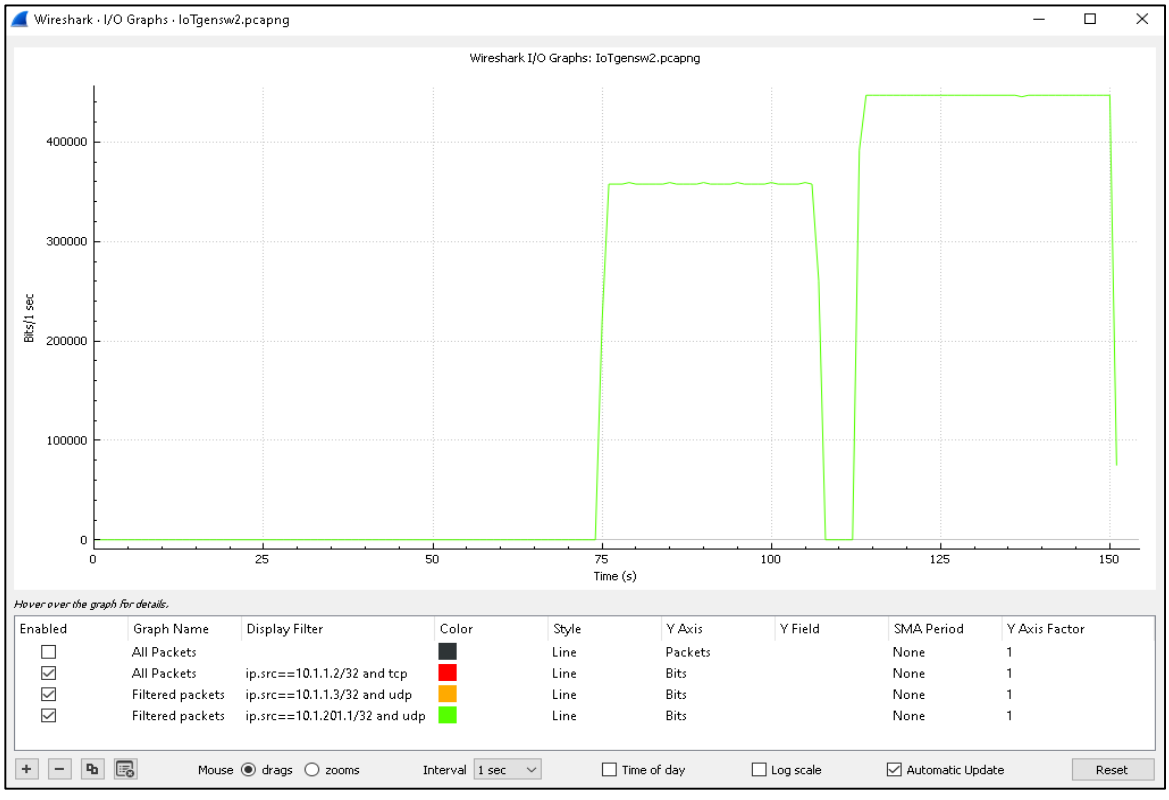


Şekil 4.33. STP-QoS Bütünsel Kullanım Simülasyon Ağ Topolojisi

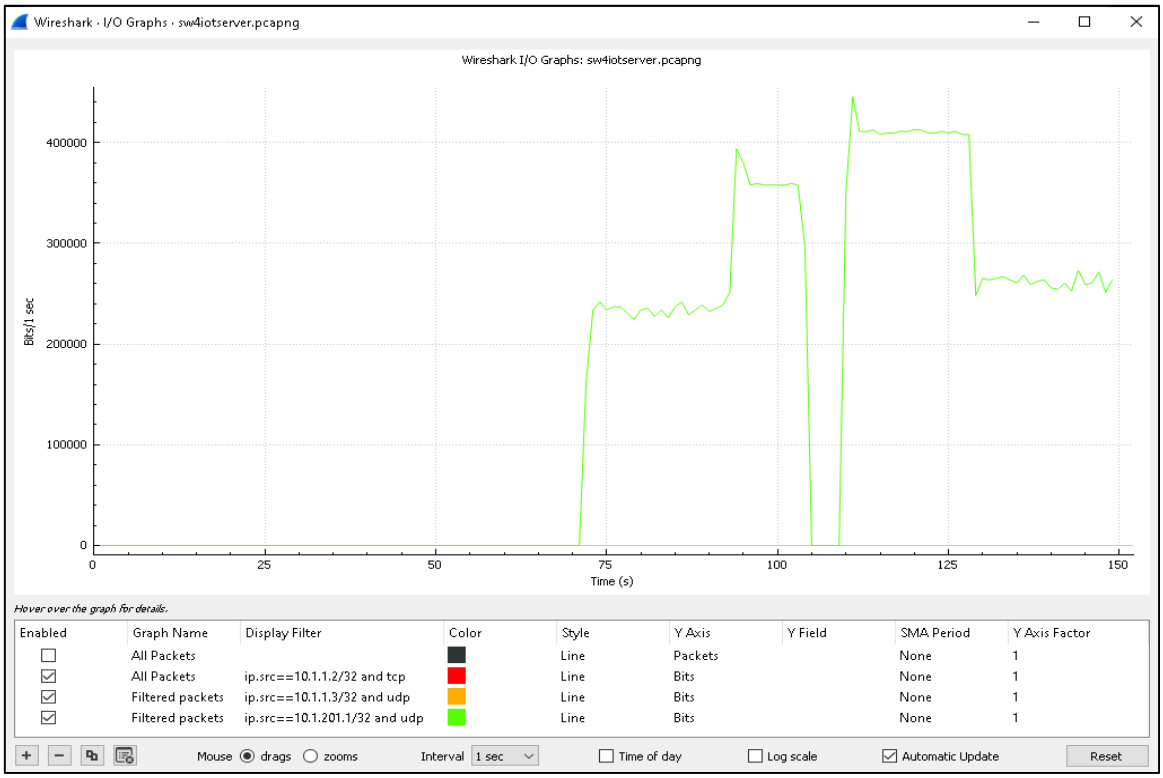
STP ve QoS senaryolarının birlikte kullanılması ile daha gerçeğe yakın bir test ortamı oluşturulmuştur. Şekil 4.33.'teki topoloji ile üç farklı trafik üretecinden ağ trafikleri oluşturulmaktadır. Oluşturulan trafikler farklı zamanlarda eş zamanlı ve tek başına izlenmiştir. EntGenerator cihazından kurumsal trafik örneği olarak 350-450 Kbit aralığında TCP, CriticalIoTGenerator cihazından hassas IoT trafik örneği olarak yaklaşık 100 Kbit UDP ve IoTGenerator cihazından IoT trafik örneği olarak 350-450 Kbit aralığında UDP trafikleri üretilmiştir. EntGenerator ve CriticalIoTGenerator cihazlarının ürettiği trafik Server cihazına iletilmektedir. IoTGenerator cihazının ürettiği trafik IoTServer cihazına iletilmektedir.



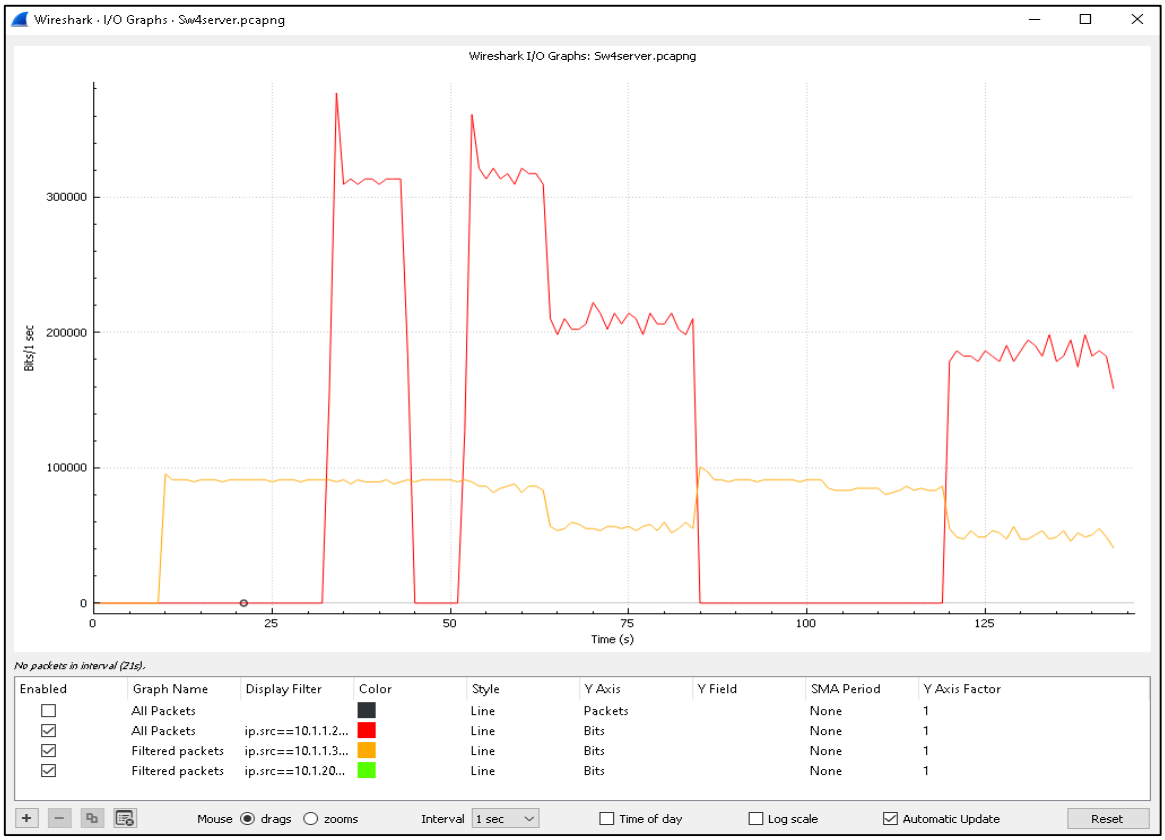
Şekil 4.34. CriticalIoTGenerator ile Sw1 Arası Ağ Trafiği



Şekil 4.35. IoTGenerator ile Sw2 Arası Ağ Trafiği

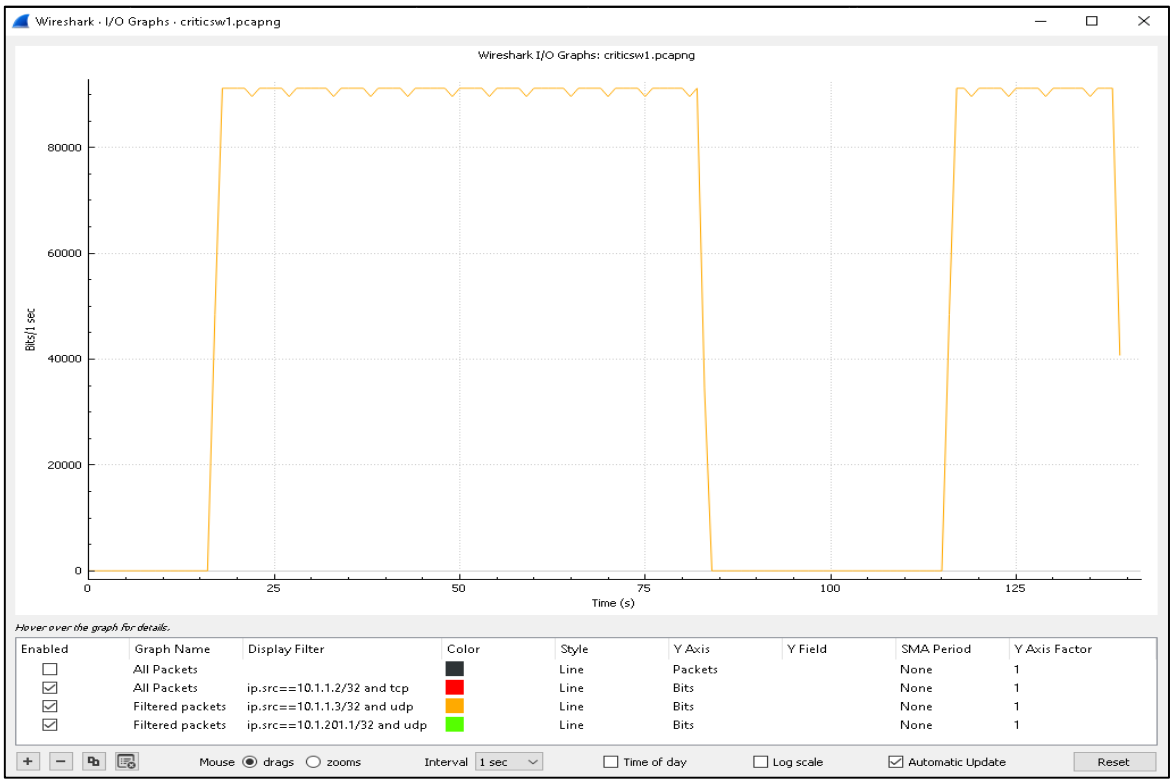


Şekil 4.36. CriticalIoTGenerator ile Sw1 Arası Ağ Trafiği

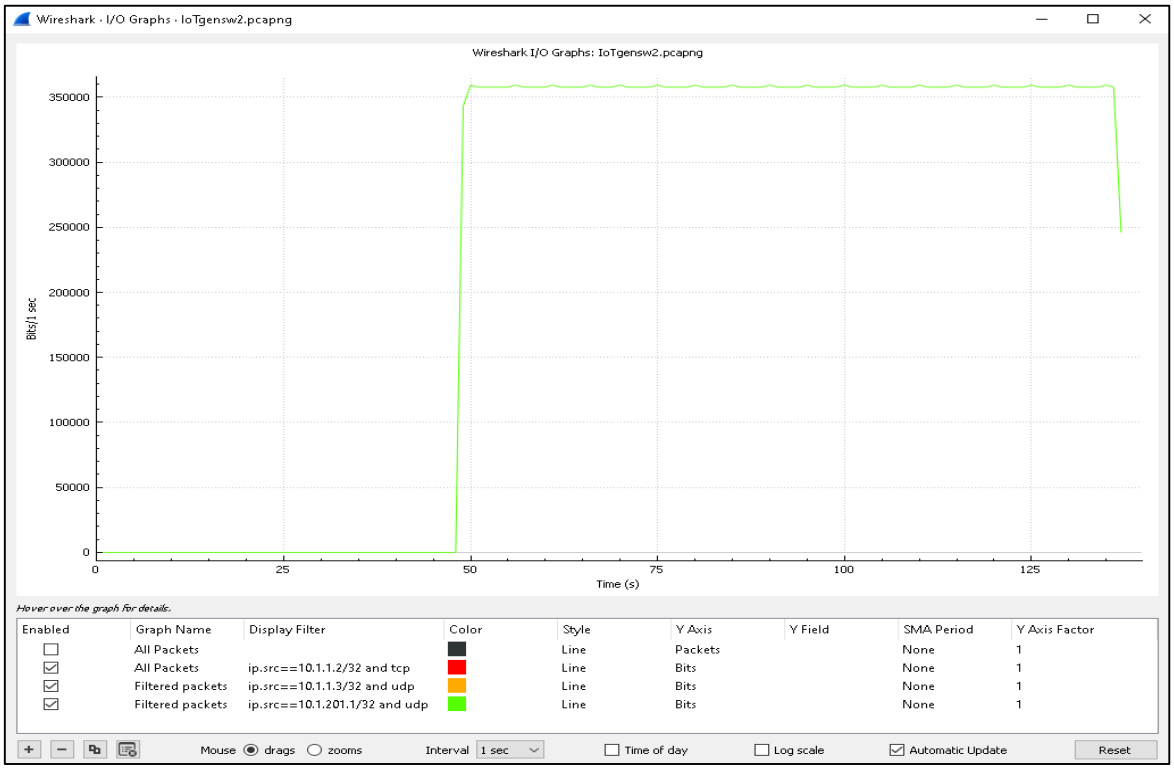


Şekil 4.37. Sw4 ile Server Arası Ağ Trafiği

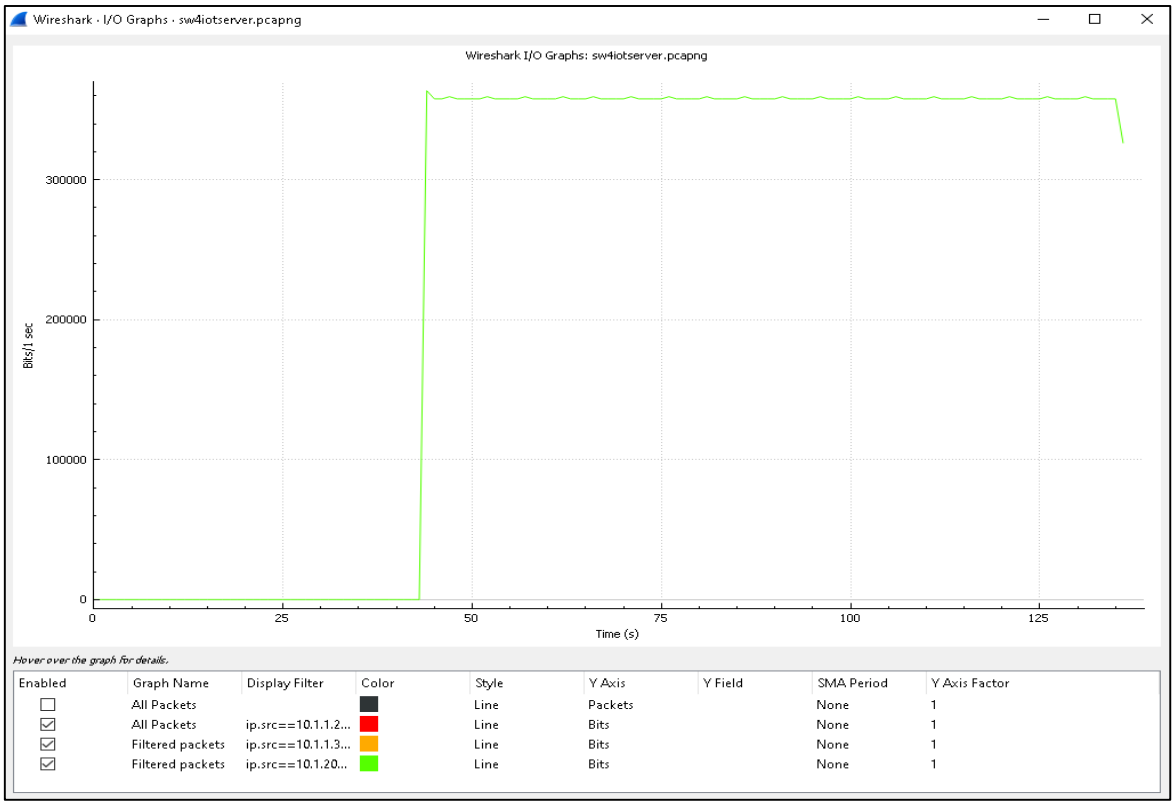
Şekil 4.34. ve 4.35'te üretilen trafiklerin etkileşim olmamış hali gözükmektedir. Şekil 4.36. ve 4.37'de üç trafik içinde ortak yol kullanımından kaynaklı olarak, trafik iletimin bozulduğu ve paketlerin önemli bir kısmının hedefe ulaşmadığı gözlemlenmiştir. Senaryonun amacı uygun şekilde R1 cihazı üzerinde QoS yapılandırması ile hassas IoT trafiği, kurumsal trafiğe göre önceliklendirilmiştir. STP senaryosundaki çoklu yol kullanımı Sw2, Sw3 ve Sw4 cihazları arasında uygulanarak IoT trafiği ile kurumsal ve hassas IoT trafiklerinin yolları ayrıştırılmıştır. Bu iki yapılandırma ile hassas IoT ve IoT trafiklerinin kurumsal trafikten etkilerine asgari seviyede maruz kalması hedeflenmektedir.



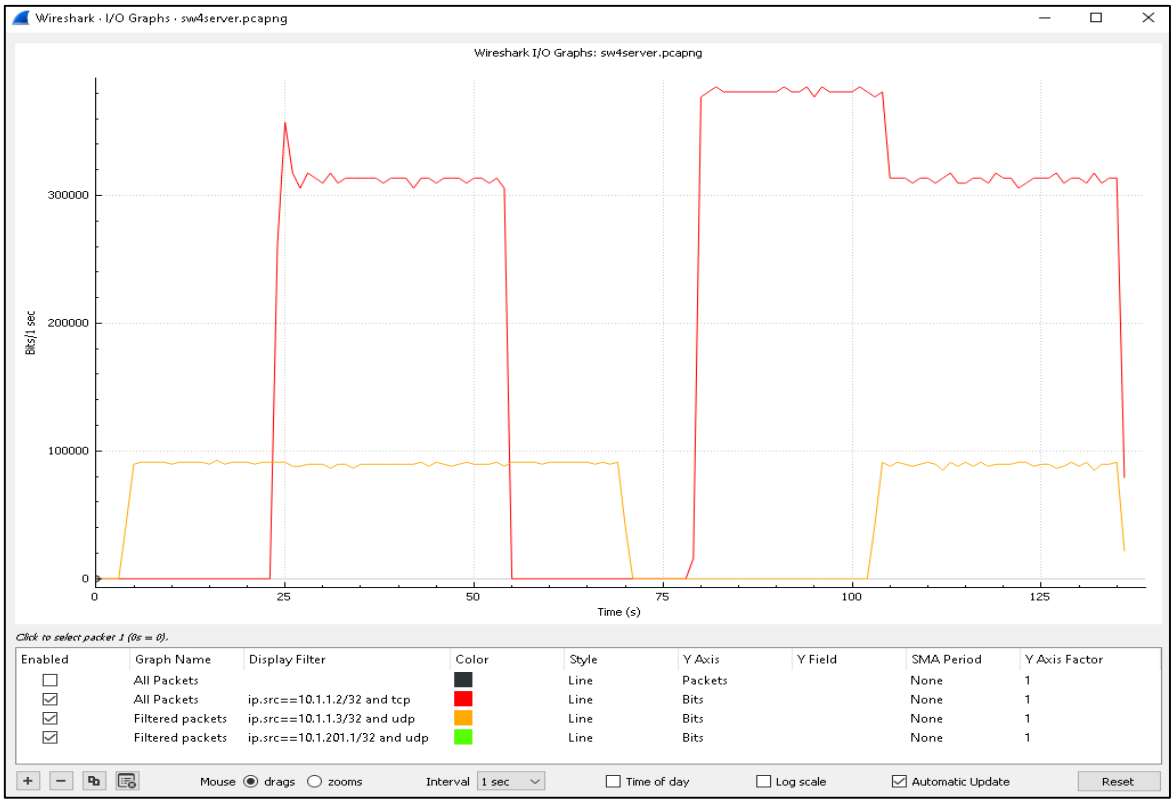
Şekil 4.38. CriticalIoTGenerator ile Sw1 Arası Ağ Trafiği



Şekil 4.39. IoTGenerator ile Sw2 Arası Ağ Trafiği



Şekil 4.40. CriticalIoTGenerator ile Sw1 Arası Ağ Trafiği



Şekil 4.41. Sw4 ile Server Arası Ağ Trafiği

STP ve QoS yapılandırmaları sonucunda Şekil 4.38. ve 4.39'da diğer trafiklerden etkilenmemiş hali gözlemlenen hassas IoT ve IoT trafikleri Şekil 4.40. ve 4.41'de görüleceği üzere gözlemlenebilir bir paket kaybı ya da gecikme olmadan hedeflerine iletilmektedir.

5. SONUÇ VE ÖNERİLER

Günümüzde kurumsal ağların yalnızca bilgisayarlar için kullanımı söz konusu değildir. Yeni gelişen teknolojilere karşı ağda sürekli cihaz değişimi yapmak maliyet anlamında etkin olmamaktadır. Ağda yapılacak yapılandırma ve tasarım değişiklikleriyle yeni gelişen teknolojilerin ağa dahil edilmesi sağlanmalıdır. IoT sistemlerin gelişmekte ve her geçen gün yenilerinin ortaya çıktığı düşünüldüğünde yeni sistemlerin gereksinimlerine hakim olunmalı ve gereksinimlere uygun olarak ağ üzerinde segmentasyon sağlanmalıdır. Her segmentasyon için ağ gereksinimleri ayrı ayrı yönetilmelidir. Gecikme duyarlı sistemler için ağda yedek olarak tutulan boş yolların kullanılması sağlanmalıdır. Kritik sistemlerin ağ performansları izleme sistemleri ile sürekli olarak izlenmeli ve kaydedilmelidir. Performans kısıtı yaşanan noktalarda geriye dönük incelemeler yapılarak darboğaz belirlenir ve iyileştirmeler yapılır. Manuel olarak oluşturulan tüm bu çözümlere ek olarak ağların dinamik ve ön yapılandırılmış olarak ihtiyaçlara uygun yönetiminin sağlanması için yazılım tanımlı olarak yönetilmesi gereklidir. Kısıtlı bilgi teknolojileri bütçelerini göz önünde bulundurularak ileriye dönük yapılan her değişiklikte yazılım tanımlı altyapıların düşünülmesi ve ağlara eklenecek her ağ cihazının yazılım tanımlı olarak seçilmesi gerekir.

Bu tez çalışmasında nesnelerin interneti, temel ağ kavramları ve kurumsal ağlar hakkında genel bilgilere yer verilerek kurumsal ağlar ile nesnelerin interneti arasındaki uyumsuzluklar üzerinde durulmuş, uyumlanma için yöntem önerisi sunulmuş ve iyileştirme yapılacak ağ teknolojileri irdelenmiştir. Çalışmada önerilen ağ teknolojilerinden kurumsal ağlarda en yaygın olarak kullanılan kapsayan ağaç protokolü ve servis kalitesi teknolojileri açık kaynak kodlu simülasyon ortamında IoT paketlerinin daha verimli çalışması için yapılandırılarak test sonuçları irdelenmiştir. Sonuçlarda açıkca görüleceği üzere IoT sistemlerinin kurumsal ağlar üzerinde etkin bir şekilde kullanımı için ağ sistemlerinde önerilen yapılandırmaların uygulanması hızlı ve verimli iyileştirmeler sağlar. Bunların yanında maliyet etkin olarak kısa vadede ağ sisteminin güncellenmesi mümkün olmayan kurumlarda mevcut ağ yapılandırmaları ile IoT trafiklerin daha güvenilir olarak hedeflerine ulaşmaları sağlanır. Yapılan simülasyonlarda görüleceği üzere mevcut ağ sistemleri üzerindeki yapılandırma olanakları gözden geçirilerek ağlarda kısa vadeli çözümler oluşturulur.

KAYNAKLAR

1. Liu, Y. ve Zhou, G. (2012). *Key Technologies and Applications of Internet of Things.* 2012 Fifth International Conference on Intelligent Computation Technology and Automation, Zhangjiajie,197–200.

2. Lea, P. (2020). *IoT and Edge Computing for Architects. Implementing edge and IoT systems from sensors to clouds with communication systems, analytics, and security*. (Second Edition). Birmingham: Packt Publishing Ltd. 32-44.

3. Hanes, D., Salguerio, G., Grossetete, P., Barton, R. ve Henry, J. (2017). *IoT Fundamentals. Networking Technologies, Protocols, and Use Cases for the Internet of Things*. (First Edition). Indianapolis: Cisco Press. 28-58.

4. Wu, R., Yang, X., Zhou, X. ve Wang, Y. (2021). *Enterprise Wireless Local Area Network Architectures and Technologies.* (First Edition). Florida: CRC Press, 9-10, 251, 404-405.

5. Kırışoğlu, S. (2018). *Kurumsal Ağların Sistematik Tasarımı İçin Yeni Bir Dinamik Vlan Yaklaşımı*. Yüksek Lisans Tezi, Düzce Üniversitesi Fen Bilimleri Enstitüsü, Düzce, 2.

6. Sung, Y.-W. E., Sun, X., Rao, S. G., Xie, G. G. ve Maltz, D. A. (2010). Towards Systematic Design of Enterprise Networks. *IEEE/Acm Transactions On Networking*, 19(3), 695.

7. Zhang, Y., Cui, M., Abadeer, M. ve Gorlatch, S. (2023, 11-14 Ocak). *A QoS-Aware Routing Mechanism for SDN-Based Integrated Networks.* 2023 International Conference on Information Networking, Bangkok, 287–292.

8. İnternet: Shang, W., Yu, Y. ve Droms, R. (February, 2016). Challenges in IoT Networking via TCP/IP Architecture. *UCLA Resmi Web Sitesi.* URL: https://irl.cs.ucla.edu/data/files/techreports/ndn0038-1.pdf Son Erişim Tarihi: 10.01.2023.

9. Khamosh, A., Anwer, M. A., Nasrat, N., Hamdard, J., Gawhari, G. S. ve Ahmadi, A. R. (2020, 21-22 Ekim). *Impact of Network QoS factors on QoE of IoT Services*. The 5th International Conference on Information Technology, Chonburi, 61–65.

10. Hui, W. ve Zhongsheng, W. (2012, 23-25 Ağustos). *Research on Load Balancing Algorithm Based on MSTP in Dynamic Network.* 2012 International Conference on Industrial Control and Electronics Engineering, Xi'an, 330–334.

11. Rincon, F., Tanaka, Y. ve Watteyne, T. (2018, 21-23 Ekim). *On the Impact of WiFi on 2.4 GHz Industrial IoT Networks.* 2018 IEEE International Conference on Industrial Internet, Bellevue, 33–39.

12. İnternet: Jacquenet, C. ve Boucadair, M. (November, 2015). A Software-Defined Networking Approach to IoT. *ZTE Resmi Web sitesi*. URL: https://res-www.zte.com.cn/mediares/magazine/publication/com_en/article/201601/448976/P020160311298781218045.pdf. Son Erişim Tarihi: 10.01.2023.

13. Rahman, A., Islam, M. J., Montieri, A., Nasir, M. K., Reza, M. M., Band, S. S., Pescape, A., Hasan, M., Sookhak, M. ve Mosavi, A. (2021). SmartBlock-SDN: An Optimized Blockchain-SDN Framework for Resource Management in IoT. *IEEE Access,* 9, 28361–28376.

14. Shi, Y., Zhang, Y. ve Chen, J. (2020). Cross-layer QoS enabled SDN-like publish/subscribe communication infrastructure for IoT. *China Communications*, 17(3), 149–167.

15. Sinh, D., Le, L.-V., Lin, B.-S. P. ve Tung, L.-P. (2018, 30 Nisan-1 Mayıs). *SDN/NFV — A new approach of deploying network infrastructure for IoT.* 2018 27th Wireless and Optical Communication Conference, Hualien, 1–5.

16. Dantas Silva, F. S., Neto, E., Santos, C., Almeida, T., Silva, I. ve Neto, A. V. (2020, 10-12 Kasım). *Evolving Fast Innovation in Next-Generation Networking Through Flexible and Customized Softwarization and Slicing Capabilities.* 2020 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN). Leganes, 188–193.

17. Alvarez-Horcajo, J., Ibanez, G., Constantin, B. N., Martinez-Yelmo, I. ve Arco, J. M. (2019, 14-17 Ekim). *Scaling and Interoperability of All-Path with Bridged and SDN Domains using VXLANs.*2019 IEEE Conference on Local Computer Networks (LCN), Osnabrueck, 97-100.

18. Chen, C., Chen, Y., Tsai, S. ve Yang M. (2017, 27-29 Eylül). *Forwarding Path Discovery with Software Defined Networking.* 2017 19th Asia-Pacific Network Operations and Management Symposium (APNOMS), Seoul, 299-302.

19. Khaliq, A., Adil, S. H. ve Jamshid, J. (2018, 3-4 Mart). *Enhancing throughput and load balancing in software-defined networks.* 2018 International Conference on Computing, Mathematics and Engineering Technologies (iCoMET). Sukkur, 1–6.

20. Ramdhani, M. F., Hertiana, S. N. ve Dirgantara, B. (2016). *Multipath routing with load balancing and admission control in Software-Defined Networking (SDN).* 2016 4th International Conference on Information and Communication Technology (ICoICT), Bandung, 1–6.

21. Rachuri, S. P., Ansari, A. A., Tandur, D., Kherani, A. A. ve Chouksey, S., (2019, 12-14 Aralık). *Network-Coded SD-WAN in Multi-Access Systems for Delay Control.* Proceedings of the Fourth International Conference on Contemporary Computing and Informatics (IC3I), Singapore, 32-37.

22. Fang, S., Yu, Y., Foh, C. H. ve Aung, K. M. M. (2013). A loss-free multipathing solution for data center network using software-defined networking approach. *IEEE Transactions on Magnetics*, 49(6), 2723–2730.

23. Vora, J., Kaneriya, S., Tanwar, S. ve Tyagi, S. (2018, 23-24 Şubat). *Performance Evaluation of SDN based Virtualization for Data Center Networks.* 2018 3rd International Conference On Internet of Things: Smart Innovation and Usages (IoT-SIU), Bhimtal, 1–5.

24. Sangeetha, S. ve Vairam, T. (2020). Implementing SDN in GNS3 with Cloud. *International Journal Of Innovative Research In Technology*, 6(9), 99–102.

25. Han, M. P., Htet, S. Y. ve Wuttisttikulkij, L. (2022, 05-08 Temmuz). *Hybrid GNS3 and Mininet-WiFi Emulator for SDN Backbone Network Supporting Wireless IoT Traffic.* 2022 37th International Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC), Phuket, 768–771.

26. Barry, M. A., Tamgno, J. K., Lishou, C. ve Cisse, M. B. (2018, 11-14 Şubat). *QoS impact on multimedia traffic load (IPTV, RoIP, VoIP) in best effort mode.* 2018 20th International Conference on Advanced Communication Technology (ICACT), Chuncheon, 694–700.

27. Castillo-Velazquez, J.-I., Ramos-Estela, J. ve Marchand-Nino, W.-R. (2021, 12-15 Ekim). *Comparison for the Hardware Defined Networks vs the Software Defined Networks Environments for IPv6 When Applied to the Backbone of the Advanced Network REUNA.* 2021 IEEE Fifth Ecuador Technical Chapters Meeting (ETCM), Cuenca, 1–6.

28. Dumitrache, C., Predusca, G., Gavriloaia, G., Angelescu, N., Circiumarescu, D. ve Puchianu, D. C. (2022, 30 Haziran-1 Temmuz). *Comparative analysis of routing protocols using GNS3, Wireshark and IPerf3.* 2022 14th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Ploiesti, 1–6.

29. Ramadhan, E. ve Firdausi, A, Budiyanto, S. (2017, 21-23 Kasım). *Design and Analysis QoS VoIP using Routing Border Gateway Protocol (BGP).* 2017 International Conference on Broadband Communication, Wireless Sensors and Powering, Jakarta, 1-4.

30. Imran, M., Khan, M. A. ve Abdul Qadeer, M. (2018, 15-16 Şubat). *Design and Simulation of Traffic Engineering using MPLS in GNS3 Environment.* 2018 Second International Conference on Computing Methodologies and Communication (ICCMC), Erode, 1026–1030.

31. Sookun, Y. ve Bassoo, V. (2016, 3-6 Ağustos). *Performance analysis of IPv4/IPv6 transition techniques.* 2016 IEEE International Conference on Emerging Technologies and Innovative Business Practices for the Transformation of Societies (EmergiTech), Balaclava, 188–193.

32. Tego, E., Attanasio, V. ve Matera, F. (2022, 3-5 Ekim). *GNS-3 Emulation Platform to Study Wide Area Network Performance in Contexts Close to Reality.* In 2022 AEIT International Annual Conference (AEIT), Roma, 1–6.

33. Castillo-Velazquez, J. -I. ve Delgado-Villegas, A. (2020, 30 Ağustos-2 Eylül). *GNS3 Limitations when Emulating Connectivity and Management for Backbone Networks: A Case Study of CANARIE.* 2020 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE), Londra, Kanada, 2974–2979.

34. Velieva, T. R., Korolkova, A. V. ve Kulyabov, D. S. (2014, 6-8 Ekim). *Designing installations for verification of the model of active queue management discipline RED in the GNS3*. 2014 6th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), St. Petersburg, 570–577.

35. Mohtasin, R., Prasad, P. W. C., Alsadoon, A., Zajko, G., Elchouemi, A. ve Singh, A. K. (2016, 23-25 Mart). *Development of a virtualized networking lab using GNS3 and VMware workstation.* In 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, 603–609.



Gazili olmak ayrıcalıktır