AĞ YÖNETİM SİSTEMLERİNİN İNCELENMESİ VE ÖRNEK BİR KURUMSAL GENİŞ ALAN AĞI UYGULAMASI

YÜKSEK LİSANS TEZİ

Abdullah YILDIRIM

Danışman

Dr. Öğr. Üyesi Said Mahmut ÇINAR

İNTERNET VE BİLİŞİM TEKNOLOJİLERİ

YÖNETİMİ ANABİLİM DALI

Haziran 2019

AFYON KOCATEPE ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ

AĞ YÖNETİM SİSTEMLERİNİN İNCELENMESİ VE ÖRNEK BİR KURUMSAL GENİŞ ALAN AĞI UYGULAMASI

Abdullah YILDIRIM

Danışman
Dr. Öğr. Üyesi Said Mahmut ÇINAR

İNTERNET VE BİLİŞİM TEKNOLOJİLERİ YÖNETİMİ
ANABİLİM DALI

Haziran 2019

TEZ ONAY SAYFASI

Abdullah YILDIRIM tarafından hazırlanan "Ağ Yönetim Sistemlerinin İncelenmesi Ve Örnek Bir Kurumsal Geniş Alan Ağı Uygulaması" adlı tez çalışması lisansüstü eğitim ve öğretim yönetmeliğinin ilgili maddeleri uyarınca 21/06/2019 tarihinde aşağıdaki jüri tarafından **oy birliği** / ~~**oy çokluğu**~~ ile Afyon Kocatepe Üniversitesi Fen Bilimleri Enstitüsü **İnternet ve Bilişim Teknolojileri Yönetimi Anabilim Dalı'nda YÜKSEK LİSANS TEZİ** olarak kabul edilmiştir.

Danışman : Dr. Öğr. Üyesi Said Mahmut ÇINAR

İmza

Başkan : Doç. Dr. Ahmet ZENGİN
Sakarya Ü., Bilgisayar ve Bilişim Bilimleri F. .....

Üye : Dr. Öğr. Üyesi Said Mahmut ÇINAR
Afyon Kocatepe Ü., Mühendislik F. .....

Üye : Dr. Öğr. Üyesi Emre AKARSLAN
Afyon Kocatepe Ü., Mühendislik F. .....

Afyon Kocatepe Üniversitesi
Fen Bilimleri Enstitüsü Yönetim Kurulu'nun
...../...../..... tarih ve
..... sayılı kararıyla onaylanmıştır.

.....
Prof. Dr. İbrahim EROL
Enstitü Müdürü

BİLİMSEL ETİK BİLDİRİM SAYFASI
Afyon Kocatepe Üniversitesi

Fen Bilimleri Enstitüsü, tez yazım kurallarına uygun olarak hazırladığım bu tez çalışmasında;

- Tez içindeki bütün bilgi ve belgeleri akademik kurallar çerçevesinde elde ettiğimi,
- Görsel, işitsel ve yazılı tüm bilgi ve sonuçları bilimsel ahlak kurallarına uygun olarak sunduğumu,
- Başkalarının eserlerinden yararlanılması durumunda ilgili eserlere bilimsel normlara uygun olarak atıfta bulunduğumu,
- Atıfta bulunduğum eserlerin tümünü kaynak olarak gösterdiğimi,
- Kullanılan verilerde herhangi bir tahrifat yapmadığımı,
- Ve bu tezin herhangi bir bölümünü bu üniversite veya başka bir üniversitede başka bir tez çalışması olarak sunmadığımı

beyan ederim.

21/06/2019

Abdullah YILDIRIM

ÖZET
Yüksek Lisans Tezi

AĞ YÖNETİM SİSTEMLERİNİN İNCELENMESİ VE
ÖRNEK BİR KURUMSAL GENİŞ ALAN AĞI UYGULAMASI

Abdullah YILDIRIM
Afyon Kocatepe Üniversitesi
Fen Bilimleri Enstitüsü
İnternet ve Bilişim Teknolojileri Yönetimi Anabilim Dalı
Danışman: Dr. Öğr. Üyesi Said Mahmut ÇINAR

Bilgi güvenliği gibi, ağ yönetimi de bilgisayar ve ağ kullanıcılarının görmezden geldiği önemli bir konudur. Kurumsal uygulamalarda geniş ve birbirinden uzak coğrafi bölgeler ile çok sayıda yönetim alanına yayılabilen, güvenli ve yüksek performansa sahip ağ bağlantılı bilgisayar altyapılarına ihtiyaç duyulmaktadır. Ancak bu tür altyapılarda kullanılan donanımlarda fiziksel ya da yazılım kaynaklı arızalar meydana gelebilmekte ve ağ performansı yetersiz kalabilmektedir. Bu çalışmada ağ yönetim sistemi alt yapısında yer alan mimari araştırılarak, tasarlanacak ağ yönetim sistemine örnek olması için günümüzde en çok kullanılan ağ yönetim sistemlerinin özellikleri incelenmiştir. İncelemelerden edinilen kazanımlar doğrultusunda yönetimi kolaylaştırmak için kurumsal geniş alan ağının nasıl kurulacağı ve ideal bir ağ yönetim sisteminin tercih edilmesi için gerekli olan özellikler hakkında detaylı bilgiler verilmiştir. Tasarım aşamasında, ağ yönetim sisteminin kurulumunda yapılması gerekli işlemler adım adım anlatılarak, yapılan işlemlerin sonucunda kurumsal şirketlerin hata yönetimi, performans yönetimi, hesap yönetimi, yapılandırma yönetimi ve güvenlik yönetimi alanlarında elde edeceği faydalar ortaya çıkarılmıştır.

2019, xii + 101 sayfa

Anahtar Kelimeler: Ağ Yönetim Sistemleri, Kurumsal Geniş Alan Ağı, Basit Ağ Yönetim Protokolü

ABSTRACT
M.Sc. Thesis

ANALYSING NETWORK MANAGEMENT SYSTEMS AND
EXAMPLE OF AN ENTERPRISE WIDE AREA NETWORK APPLICATION

Abdullah YILDIRIM

Afyon Kocatepe University

Graduate School of Natural and Applied Sciences

Department of Internet and Information Technologies Management

Supervisor: Asst. Prof. Said Mahmut ÇINAR

Network Management is an important topic, which is ignored by network users like information security. Enterprise business applications need wide and geographically remote locations that can spread over multiple management areas and network connected computer infrastructures with secure and high performance. However, physical or software related failures might occur in hardware that is used in this kind of infrastructure. Therefore network performance would be insufficient. In this study, the architecture in network management system has been investigated. The properties of today's most widely used network management systems has been analysed in order to be an example for the system to be designed. In accordance with the achievements from the analysis, detail information has been given in order to to simplify the management how to establish an enterprise network and prefer an ideal network management system. During the design stage, the operations that should be performed in establishing network management system, has been clarified systematically. The benefits that can be obtained by enterprise companies in terms of fault management, performance management, account management, configuration management and security management have been discovered.

2019, xii + 101 pages

Keywords: Network Management Systems, Enterprise Wide Area Network, Simple Network Management Protocol

TEŞEKKÜR

Bu araştırmanın konusu, deneysel çalışmaların yönlendirilmesi, sonuçların değerlendirilmesi ve yazımı aşamasında yapmış olduğu katkılarından dolayı tez danışmanım Sayın Dr. Öğr. Üyesi Said Mahmut ÇINAR'a, araştırma ve yazım süresince görüş ve önerilerinden yararlandığım Emin Orçun MENGENLİ'ye, her konuda öneri ve eleştirileriyle yardımlarını gördüğüm hocalarıma ve arkadaşlarıma teşekkür ederim.

Hayatıma girdiği ilk günden itibaren her daim yanımda olan, araştırma süresince sabırla bana katlanıp yardımlarını esirgemeyen kıymetli eşim Betül YILDIRIM'a, tez sürecinde ailemize yeni katılan oğlum Mustafa Zihni'ye ve sadece bu araştırma sürecinde değil hayatımın her alanında maddi, manevi desteklerini ve dualarını benden eksik etmeyen sevgili babam Zihni YILDIRIM, annem Nurten YILDIRIM ve abim Muhammed YILDIRIM'a sonsuz teşekkür ederim.

Abdullah YILDIRIM

AFYONKARAHİSAR, 2019

İÇİNDEKİLER DİZİNİ

Sayfa

KISALTMALAR DİZİNİ

Kısaltmalar	
ARP	Address Resolution Protocol
ARPANET	Advanced Research Projects Agency Network
BT	Bilişim Teknolojileri
CDP	Cisco Discovery Protocol
CLI	Command Line Interface
CMIP	Common Management Information Protocol
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DOS/DDOS	Denial of Service/ Distributed Denial of Service
HTTP	Hyper-Text Transfer Protocol
IDS	Intrusion Detection System
IETF	The Internet Engineering Task Force
IP	Internet Protocol
ISO	International Organization for Standardization
ISP	Internet Service Provider
ITU	International Telecommunications Union
LAN	Local Area Network
LLDP	Link Layer Discovery Protocol
MAC	Media Access Control
MIB	Management Information Base
NMS	Network Management System
OSI	Open Systems Interconnetion
PDU	Protocol Data Unit
RFC	Request for Comments
RMON	Remote Monitoring
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SYN	Synchronize
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/ Internet Protocol
TELNET	Telecommunication Network
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAN	Wide Area Network

ŞEKİLLER DİZİNİ

Sayfa

ÇİZELGELER DİZİNİ

Sayfa

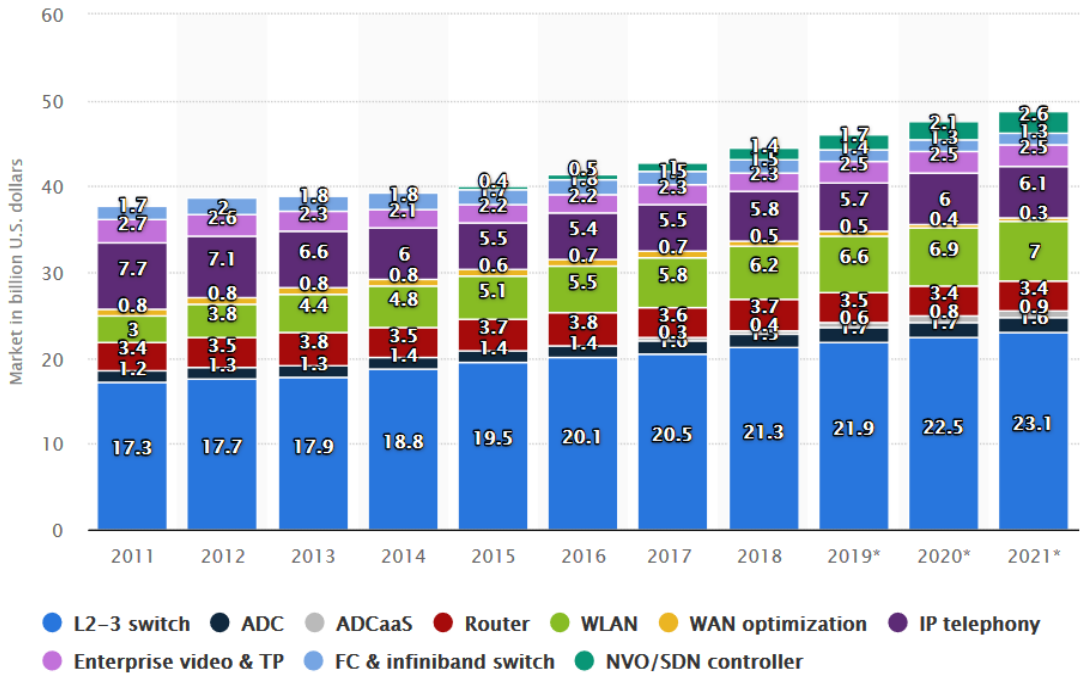
RESİMLER DİZİNİ

Sayfa

1. GİRİŞ

Bilgi ve iletişim, her kurumsal şirketin başarısı için en önemli stratejik konulardan ikisidir. Bu iki konunun stratejik önem arz etmesinin en büyük nedeni, iş kaynaklarını tüm çalışanlarla paylaşabilmek ve müşterilere en iyi hizmeti ulaştırabilmektir. Bilgiye erişimi sağlayacak en önemli kaynak ise iletişim araçlarıdır.

Günümüzde bilgeye ulaşmamıza yardımcı olacak en önemli iletişim kaynağı bilgisayar ağlarıdır. İnsanlar farklı binalarda, bölümlerde ve organizasyon yapılarında bulunabilir. Ancak kurumsal ağ hepsini bir araya getirebilir, iletişim kurmalarına ve kaynakları paylaşmalarına yardımcı olabilir. Bu nedenle şirketler, farklı coğrafi alanlarda faaliyet göstermesi ve uzak yerleşkeler arasında veri iletimi ihtiyacı doğmasından dolayı ağ iletişim altyapılarının kurulmasına yönelik yatırımlar gerçekleştirmektedir. Statista araştırma şirketinin yayınlamış olduğu istatistik raporuna göre 2021 yılına kadar dünya genelinde kurumsal ağ altyapısı pazarının 50 milyar dolar olması öngörülmektedir (Şekil 1.1). Günümüzde ise bu rakam yaklaşık 44 milyar dolar seviyesindedir.



Şekil 1.1 Dünya genelinde, kurumsal ağ altyapı pazarı grafiği (İnt. Kyn. 1).

Özellikle de mobil iş gücü, nesnelerin interneti ve bulut uygulamalarının çoğalmasıyla birlikte ağlar her zamankinden daha kritik hale gelmektedir. Bundan dolayı şirketler mevcut ağ altyapılarını iyileştirme ve geliştirme çabasının içine girmektedir. Interop ITX araştırma şirketinin "2018 Altyapı Durumu" raporuna göre ise, şirketlerin ağ altyapılarını iyileştirme ve büyütme talepleri artmaktadır (İnt. Kyn. 2). Farklı sektör ve büyüklükteki şirketlerde görev alan 150 bilişim teknolojisi uzmanı ile gerçekleştirilen ankette, kuruluşların şubeleri ile arasında bulunan hatlarının bant genişliğini artırmaya, ağlarını yazılımla modernize etmenin yollarını araştırmaya ve kablosuz ağ sistemlerini genişletmeye odaklandığı tespit edilmiştir.

Bu kadar çok donanım ve yazılımın bir araya gelmesiyle oluşan sistemlerin gelişimiyle birlikte bazı yönetimsel sorunlar da ortaya çıkmıştır. Örneğin hizmet kesintileri ciddi maddi kayıplara neden olmaktadır. IHS Markit'in yaptığı araştırmaya göre, hizmet kesintileri ve yavaşlamaların işletmelere yılda 700 milyar dolar mal olduğu tahmin edilmektedir (İnt. Kyn. 3). Sebep ne olursa olsun, ağın kapalı kalma süresi şirketler için büyük maddi kayıplara yol açmaktadır. Hizmet kesintisi sorunun dışında donanımsal sorunlar, performans problemleri, zaman yetersizliği ve siber tehditler gibi birçok yönetimsel sorunlar ile karşılaşılmaktadır.

Kurumsal ağlarda yaşanacak sorunlara karşı zamanında ve etkili önlemler alınmadığı takdirde, bu durum zaman, maliyet ve kaynak açısından ağ altyapısına ciddi zararlar verebilmektedir. Tüm bu engellerin üstesinden gelinebilmesi için ağda yer alan cihazların tümünün kesintisiz takibi yapılması ve sorunlara anlık müdahale edilmesi gereklidir. Bu yüzden ağ yönetiminin insan kontrolü ile yapılması zaman ve maliyet açısından uygun değildir. Zararların önüne geçilmesi ve ağ yöneticilerinin yapması gereken görevlerini etkin yürütebilmesi amacıyla bir ağ yönetim sistemine ihtiyaç duyulmaktadır.

Ağın etkili yönetilebilmesi için yapılması gereken ilk iş, kurulum öncesi ve kurulum aşamasında gerekli adımlara, yöntemlere dikkat edilmesidir. Kullanılacak olan ağ yönetim sistemleri ve teknolojileri iyi analiz edilip, sağlanacak olan faydanın tespiti doğru yapılmalıdır. Yapılacak olan adımların sistematik şekilde planlanması ve ağı yönetecek uzmanların karşılaşacakları işlerin niteliklerini doğru bilmesi, ağların yönetimi konusunda her zaman fayda sağlamaktadır.

Bu çalışma; giderek daha fazla önem arz eden ağ yönetim konusunu tanıtması, altyapısında yer alan parçaları göstermesi, ticari pazarda bulunan ağ yönetim sistemlerini incelemesi ve örnek bir ağ yönetim sisteminin nasıl kurulacağını anlatması bakımından, ağ yönetimi konusunda bilgi edinmek isteyenlerin başvurabileceği kaynak niteliğinde olacaktır.

Tez çalışması giriş bölümü ile birlikte beş ana bölümden oluşmaktadır. Litetatür bölümünde, ağ kavramının nasıl meydana geldiği ve gelişim aşamalarına değinildikten sonra, ağ yönetiminin neden gerekli olduğu sorusuna yanıt aranmıştır. Konunun önemi, hayatımızdaki etkileri ifade edilerek, bu alanda yapılan tez çalışmaları ve makalelerden örnekler sunulmuştur. Materyal ve metot bölümünde, ağ sistemleri ve özellikle bilgisayar ağlarının neyi ifade ettiği tanımlanarak, tezin bulgular bölümünde sıkça kullanılan temel ağ terimleri açıklanmıştır. Bilgisayar ağlarında ağ yönetimi kavramı ayrıntılı şekilde anlatılıp, ağ yönetim sistemlerinin altyapısını oluşturan model, mimari ve protokoller hakkında detaylı bir bilgi sunulmuştur. Ayrıca kurumsal geniş alan ağların yönetiminde birçok ihtiyacı karşılayan, geliştiriciler tarafından ücretli veya ücretsiz sunulan bazı ağ yönetim sistemleri incelerek; yazılımların yetenekleri, artı yönleri, eksik yönleri hakkında yararlı bilgiler verilmiştir. Bulgular bölümünde, kurumsal geniş alan ağının etkili ve doğru yönetimi için gerekli ilk adım olan ağın kurulumu öncesi ve kurulumu sırasında yapılması gerekli işler anlatılmıştır. İkinci adımda materyal ve metot bölümünde edinilen bilgiler doğrultusunda bir ağ yönetim sistemi tercih edilirken bakılması gereken özellikler belirtilip, ağ yönetim sisteminin kurulumu aşamasında yapılması gerekli adımların üzerinde durulmuştur. Son olarak gerçekleştirilen kurulum işlerinin sonucunda elde edilen faydalar açıklanmıştır. Tartışma ve sonuç bölümünde, ağ yönetiminin şirketlere neler kattığı ve çıkarılan sonuçlar değerlendirilerek, ağ yönetiminin günümüzdeki eksiklikleri ve gelecekte nasıl olacağı yorumlanmıştır.

2. LİTERATÜR BİLGİLERİ

2.1 Bilgisayar Ağları ve Tarihçesi

Ağ kelime anlamı olarak benzer tipteki varlıklar arasındaki bağlantı anlamına gelir. Burada varlık insan, makine vb. her şey olabilir. İnsanlar da makinalar da ağlar aracılığıyla tanımlanmış alan içerisinde birbirleriyle paylaşımda bulunabilir. Örneğin sosyal bir ağ da insanlar fikirlerini, duygularını paylaşmak için iletişim kurabilir. Bilgisayar ağlarında da benzer durum söz konusudur (Dixit and Singh 2012).

Bilgisayar Ağı, birden çok bilgisayarın çeşitli iletişim ortamları vasıtasıyla, kaynakları paylaşmak üzere, birbirleri ile iletişim kurduğu sistemdir. Bilgisayar ağlarının kullanılmasına ihtiyaç duyulmasının en büyük nedeni coğrafi konumdan bağımsız olarak tüm fiziksel ve mantıksal kaynakları (yazıcı, program, veri vb.) ağdaki herkes için kullanabilir hale getirmektir.

Geçmişten günümüze bilgisayar ağlarının değişimine ve gelişimine bakacak olursak. En eski bilgisayar ağlarından biri olan ARPANET (Advanced Research Projects Agency Network)'in fikri 1961'de Leonard Kleinrock tarafından "Büyük İletişim Ağlarında Bilgi Akışı" başlıklı makalesinde önerildi (İnt. Kyn. 4). ARPANET'in gelişimi 1966'da başladı ve ilk iki düğüm, UCLA ve SRI (Standford Araştırma Enstitüsü) bağlandı (İnt. Kyn. 5). 1969'da resmi olarak ARPANET hayata geçirildi. Ray Tomlinson ilk e-postayı 1971 yılında gönderdi. ARPANET, 1983 yılında ikiye ayrılarak TCP/IP yani internet kavramının hayatımıza geçişi tamamladı. Günümüze kadar ki evrede kablolu ve kablosuz ağ teknolojileri gelişimlerini halen devam ettirmektedir. Bu gelişmelerin sonucunda bilgisayar sistemleri sağlık, ekonomi, ticaret, eğitim gibi hayatımızın tüm alanında kullanılmaktadır.

2.2 Ağ Yönetimi

Ağ sistemlerinin gelişiminin başladığı ve araştırma çalışması olduğu dönemde, bilgisayar ağlarının günde yüz milyonlarca insan tarafından kullanılan kritik bir altyapı olacağı düşünülmediğinden, ağ yönetimi kavramı hakkında bir çalışma yapılmamıştır. Eğer biri ağ problemiyle karşılaştıysa, problemin kaynağını bulmak için birkaç ping uygulayabilir,

sistem ayarlarını değiştirebilir, donanımı yeniden başlatabilir veya cihaza yakın bir meslektaşı arayarak sorunu çözebilirdi (Verma 2009).

1980 yılında ARPANET, sistem kaynaklarını tüketen ve sistemin içinde zaman aşımına uğrayan yüksek öncelikli işlemler nedeniyle birkaç saat hizmet veremedi (Rosen and Rose 1981). Bu olay 1981 yılında Eric Rosen tarafından ağ kontrol protokollerinin güvenlik açıkları konu başlığı altında incelendi ve RFC (Request for Comments) 789 olarak yayınlanmıştır. İlk kez ağın yönetilmemesinin bir sorun olduğu ve hata üreten donanım ve yazılımın anlık kontrol edilmesi gerektiği bu olay incelemesinde ifade edilmiştir.

TCP/IP (Transmission Control Protocol/Internet Protocol)'ye geçiş sonrası halka açık internet ve özel intranetler küçük ağlardan büyük bir küresel altyapıya dönüştüğü için, bu ağlardaki çok sayıda donanım ve yazılım bileşenini daha sistematik olarak yönetme ihtiyacı ortaya çıkmıştır. Bu ihtiyacı gidermek için bir grup akademisyen tarafından basit ağ yönetim protokolü (Simple Network Management Protocol-SNMP) tasarlanmıştır. SNMP yeni sürümleriyle birlikte halen ağ yönetiminde kullandığımız bir protokoldür. Kullanımı en çok tavsiye edilen sürümü SNMP sürüm 3 (SNMPv3)'dür. Bu sürüm ile gelen paket şifreleme ve güvenlik politikaları ağ yönetiminin güvenliğini artırmıştır. SNMPv3'ü geliştiren grup ilk olarak güvenlik ve yönetime odaklanmıştır. Kimlik doğrulama, gizlilik, yetkilendirme ve uzaktan yapılandırma özellikleri protokole kazandırılmıştır. Bu yeni protokolü geliştiren grup aslında tekerleği yeniden icat etmemişlerdir. SNMPv3, ek güvenlik ve yönetim özelliklerine sahip SNMPv2 olarak düşünülebilir (Case *et al.* 2002).

Ağ yönetim yazılımlarının gelişimi, ağın gelişimi ile yavaş yavaş olgunlaşmıştır. Bu yazılımların ilk sürümleri yalnızca aynı satıcı tarafından üretilen donanımlarla çalışmıştır. Ancak bilgisayar ağları, birden çok üreticinin donanımına dayanan mimarilere geçtikçe bu sınırlamalar büyük ölçüde ortadan kalkmıştır. Diğer önemli bir olay ise kablosuz ağ iletişiminin daha yaygın hale gelmesinden kaynaklı, hem kablolu hem kablosuz ağ cihazlarının tek bir yönetim konsolu üzerinden yönetilmesi ihtiyacının ortaya çıkmasıdır. Bu ihtiyacın giderilmesi için yapılan geliştirme çalışmaları sonucunda, günümüzde

birçok üreticinin yazılım mimarisinin temelini oluşturan birleşik ağ yönetim sistemi modeli kullanılmaya başlanmıştır. Margaret Rouse makalesinde birleştirilmiş bir ağı; iki ayrı ağ olmak yerine, mümkün olduğunda ağ öğelerini ve hizmetlerini paylaşan, kablolu ve kablosuz bileşenleri birleştiren ağ yapıları olarak tanımlamaktadır. Devamın da ise birleşik bir ağ yönetim sisteminin; planlama, sağlama, yapılandırma, izleme, hataları işleme, log kaydetme ve raporlama gibi fonksiyonları tek bir konsoldan yönetilebilmesi gerektiğini ifade etmektedir (İnt. Kyn. 6). Oluşan ticari pazar nedeniyle yüzlerce ağ yönetim yazılımı üreticiler tarafından piyasaya sunulmaya başlamıştır. Honglei vd. (2017)'ye göre mevcut piyasada bireysel veya kurumsal ihtiyaçları karşılayabilecek birçok ağ yönetim yazılımının bulunmasından dolayı, kullanım amacına en uygun yazılımın nasıl seçileceği sorusunun cevabı aranmalıdır. Yazılımın katabileceği kolaylıklar, kurumsal yapıya olan uygunluğu ve maliyeti konuları genellikle uzun araştırmalar ve denemeler sonucunda edinilebilecek bir bilgidir.

Kullanılan ağ yönetim sistemleri genellikle ağ katmanında (Open Systems Interconnetion-OSI) çalışan cihazların SNMP ile yönetildiği ve kontrol edildiği modele odaklanmaktadır. Ancak artan ağ kullanıcısı ile birlikte ağın topolojik yapısının karmaşıklığı devamlı büyümekte ve ağın bant genişliğini artıran kullanıcı uygulamaları çoğalmaktadır. Xiaoyu vd. (2012)' ye göre günümüzde ağ yönetimi teknolojisinin odağı, ağ yönetim sistemlerinde işleyişin ağ katmanından uygulama katmanına aktarılmaya başlanmasıyla, kullanıcıların kullandığı uygulamalar olmuştur. Yang ve Wang (2013)'ye göre ise ağın yalnızca yerel yönetim konsolundan yönetilemeyeceği, farklı izin seviyesine sahip yöneticilerin dünyanın herhangi bir yerindeki verileri görüntüleyebilmeli ve yönetebilmelidir. Ağ yönetiminin gelişimi sadece bu kadarla kısıtlı değildir. Farklı birçok ihtiyaca yönelik özellikler bünyesine katarak gelişmeye devam etmektedir.

İş ihtiyaçları arttıkça ağ karmaşıklığı da artmaktadır. Ağ yöneticileri, şirketlerin iş gereksinimlerini karşılamak, ağın her zaman açık ve çalışır durumda olmasını sağlamak için sürekli baskı altındadır (Rao and Mohapatra 2010). Baskı ne kadar çok olsa da işlerin etkin bir şekilde yürümesi için ağı yönetmelidir. Kurumsal ağlarda, ağ yöneticisinin görevini kolaylaştırmak için edinilen ağ yönetim araçları olmasına rağmen, bu ürünlerin kullanıcı dostu olması ve bu araçları verimli kullanabilmek için gerekli bilgilerde eksiklik

olmamalıdır. Rao ve Mohapatra (2010)'nın bu problemden yola çıkarak yapmış olduğu vaka çalışması Hindistan'ın büyük bir şirketinde uygulanmıştır. Ağda bulunan donanım, yazılım, ağ mimarisi, ağ araçları, ağ uygulamaları, izlenecek cihazlar, oluşturulacak rapor türleri ve kullanılacak yönetim araçları dâhil olmak üzere ağ yönetimi işi için gerekli tüm paydaşlar tanımlanarak, toplanan bilgiler doğrultusunda bir strateji belirlenmiş ve sonucunda birçok fayda elde edilmiştir.

Technavio teknoloji araştırma şirketi "Küresel Ağ Yönetim Sistemi (NMS) Piyasası 2018-2022" başlıklı raporuna göre ağ yönetim sistemi pazarının önümüzdeki 4 yıl içerisinde % 4 lük bir hızla büyüyerek 9 milyar ABD Doları seviyesine geleceği bekleniyor (İnt. Kyn. 7). Bu rapordan anlaşılacağı gibi şirketler ağ altyapılarının yönetimi için ciddi maddi yatırımlar yapmaktadır. Ancak ağ altyapısı oluşturmanın çeşitli zorlukları vardır. Bunlar uygun maliyetli altyapı kurmak, bant genişliğini optimize etmek, ağ yüklerini dengelemek, trafiği güvence altına almak vb. tüm bu görevler çok dikkatli bir planlama ve uzmanlık gerektirir. Yine de ağ oluşturmak çoğu zaman bir ağ yöneticisi olmanın en kolay parçasıdır. Asıl zorluk, ağın her zaman sorunsuz ve güvenli bir şekilde çalışmasını sağlamak için yönetilmesidir. Yüzlerce fiziksel cihazın dağıtık şekilde ve binlerce insana hizmet veren bulut sistemlerinin içinde bulunduğumuz bu çağda, etkili bir ağ yönetimi hiç olmadığı kadar zorlaşmıştır. TechTarget tarafından 2017 yılında "Bilişim Altyapısı Öncelikleri" başlığı altında yapılan ankette bilişim yöneticilerine yöneltilen "Şirketinizin BT (Bilişim Teknolojileri) ağının 2017 yılında önceliği nedir" sorusuna cevap olarak ağ yönetimi ve izleme yanıtının üst sıralarda yer alması ağ yönetiminin önemini açıkça ifade etmektedir (İnt. Kyn. 8).

İyi bir ağ yönetimi, ağ sistemlerinde her şeyin yolunda gitmesini sağlamak ve ağ altyapısından daha fazla verim elde etmek için artık her zamankinden daha çok önem kazanmıştır. Ağdaki kaynakların ve özellikle trafiğin ayarlanabilmesi, gerektiğinde ağ ölçeğinin genişletilmesi, ağ kullanımının en iyi duruma getirilmesi ve ağ altyapısının verimli kullanılabilmesi gereklidir. Kara vd. (2018)'nın ağ performansını artırmak, güvenlik yönetimini kolaylaştırmak ve IP yönetimini sağlamak için hazırlamış olduğu çalışması sonucunda geliştirilen yazılım sayesinde, yerel alan ağlarında oluşan veri trafiğini en iyi seviyeye getirilmesi amaçlanmıştır. Çalışma kapsamında yapılan gerçek

ortam uygulamaları ve testlerden elde edilen verilerden, ağda oluşan trafik yükünün dengelenmesini sağlamak için yeni bir yaklaşım sunulmaktadır.

Ağ yönetim sistemlerinde en önemli görevi üstlenen parça ağ yönetim protokolüdür. Ağ yönetim protokolleri içerisinden ise en çok kullanılanı SNMP protokolüdür. SNMP ağ topolojisinin çıkarılması, ağ cihazlarının yönetimi, veri trafiği kontrolü gibi birçok görevi yerine getirmektedir. Balta (2012)'nın kurumsal bir ağın topolojisinin SNMP ile keşfini konu edinen tez çalışması, tüm detaylarıyla SNMP protokolünü anlatmakta ve ağ cihazlarında protokolün yapılandırmasını göstermektedir. Kırışoğlu'nun (2018) tez çalışmasında ise kurumsal ağların yönetiminde sıkça kullanılan sanal yerel alan ağları nda (Virtual Local Area Network-VLAN), ağ trafiğinin dengelenmesi ve ağdan en iyi verimin sağlanması için SNMP protokolü kullanılarak geliştirilen bir algoritma vasıtasıyla çözüm üretilmiştir. Tüm bu çalışmalarda görüldüğü gibi ağ yönetim protokolleri amaca göre programlana bilmekte ve ağların yönetiminde etkili kullanılabilmektedir.

Kurumsal ağlarda ücretli geliştirilen ağ yönetim sistemleri kullanılabileceği gibi maliyeti azaltmak ve ağın ihtiyaçlarını karşılamak için SNMP protokolünün çeşitli yazılım dillerinde kullanılan kod kütüphaneleri kullanılarak, açık kaynaklı bir ağ yönetim sistemi geliştirilebilir. Demirbaş'ın (2017) yapmış olduğu çalışma bu konuya en güzel örneklerden birisidir. Üniversite ağının ihtiyaçları doğrultusunda kullanımı kolay, açık kaynaklı, Dokuz Eylül ağ yönetim aygıtı (DENET) adıyla anılan bir ağ yönetim sistemi geliştirmiştir. Yazılım sayesinde üniversite ağında bulunan sunucu sistemlerinin ve ağ cihazlarının kontrolü sağlanmaktadır. Altıntaş vd. (2003)'ın GuardiLan projesi de benzer amaçlar doğrultusunda hayata geçirilmek istenmiştir. İzmir Yüksek Teknoloji Enstitüsü'nün yerel alan ağının yönetimi için açık kaynak kodlu yapılan bir çalışmadır. Proje ağ topolojisinin keşfi, kullanılan bilgisayar, sunucu, ağ cihazlarının IP/MAC adres yönetimi ve son olarak internet bağlantısının etkin kullanımı için bant genişliği yönetimine çözüm üreten web tabanlı bir ağ yönetim sistemidir.

Ağın yönetimi ve izlenmesi yalnızca yönlendirici, anahtar, köprü ve ana bilgisayar gibi fiziksel ağın değil, aynı zamanda bu cihazların bazılarında çalışan hizmetlerin izlenmesiyle de ilgilidir. Ağ yönetim protokolleri, dinamik ana bilgisayar kontrol protokolü (Dynamic Host Configuration Protocol-DHCP), basit mesaj aktarım protokolü

(Simple Mail Transfer Protocol-SMTP), üst metin transfer protokolü (Hyper-Text Transfer Protocol-HTTP) gibi uygulamalara hizmet sağlayan servislerin kontrolünü sağlamak için de kullanılabilir. Kijazi ve Michael (2014)'ın hazırlamış olduğu makale uygulamaların SNMP protokolü ile izlenmesi için gerekli ağ yönetim sistemlerinin nasıl geliştirileceği konusunda detaylı bilgiler verilmektedir. Java tabanlı bir yazılım ve SNMP ile Microsoft Windows işletim sisteminde çalışan ağ tabanlı uygulamaların yönetimi ve bir sorun yaşandığında alınacak eylemlerin nasıl yapılacağı gösterilmektedir.

Ağ yönetim sistemleri, şirketlerin bilişim altyapısındaki güvenlik yönetimi, sunucu sistemleri yönetimi, son kullanıcı yönetimi gibi birçok alana dâhil olmuş durumdadır. Bugün şirketlerin en çok üstünde durduğu güvenlik yönetimi konusu ele alınacak olursa, David Geer'ın yapmış olduğu değerlendirmeye göre koordineli iletişim ağ yönetimi ve güvenliği için anahtar rol oynamaktadır. Kurulum aşamasında uyumlu ağ sistemleri ve güvenlik politikaları oluşturulması, ağda yaşanacak sorunların ve güvenlik kontrollerindeki başarısızlıkları önemli ölçüde azaltacağını düşünmektedir. Ağı oluşturan uzmanların, görevlerinde güvenlik alanını içerecek şekilde gelişim göstermesi, güvenlik uzmanları ile daha uyumlu ve ağdaki güvenlik olaylarına daha fazla hâkim olacakları tespitinde bulunmaktadır (İnt. Kyn. 9). Alkasassbeh vd.(2016)'e göre tüm siber saldırı türleri arasında hizmet dışı bırakma (Denial of Service/ Distributed Denial of Service-DOS/DDOS) saldırıları en önemli ve tehlikeli olanıdır (Al-Naymat *et al.* 2018). İnternet için ana tehditlerden bir tanesi olan bu saldırıyı engellemek için izinsiz girişlerin hızlıca saptanması gerekmektedir. Bunun yapılabilmesi için kullanılabilecek en uygun teknik anormal etkinliği normal bir ağ davranış profili ile karşılaştırılması sonucu tanımlama yapılarak ağ güvenliğini korumaktır. Al-Naymat vd. (2018)'in yapmış olduğu çalışmada, izinsiz girişlerin engellenmesine yönelik görevi yapan saldırı tespit sistemlerinin (Intrusion Detection System-IDS) ağ cihazlarından toplanan ham verilerin analizi ile vakit kaybetmesi yerine, cihazlardan toplanan işlenmiş verilerinin bulunduğu SNMP veritabanı kullanarak ağ saldırılarının tespiti ve saldırı türlerinin sınıflandırılması için etkili bir mekanizma tasarlamıştır. Bu sayede önemli bir işlem yükünü ve geç tespit süresi ortadan kaldırılmıştır.

Finans, yer bilimleri, telekomünikasyon, ulaşım ve enerji gibi birçok alanda bilgisayar ağlarının kullanılmaya başlanması, ağ yönetimi teknolojisinin sadece kurumsal şirketlerin

yönetiminin yanı sıra farklı amaç ve problemlerin çözümüne hizmet etmesi için kullanılmasına neden olmuştur. Tün vd. (2015)'ün geliştirdiği projede deprem anında yer sarsıntı haritaları ve olası hasar dağılım haritaları ağ yönetim sistemleri ve coğrafi bilgi sistemleri bir arada kullanılarak alınan veriler ile elde edilmiştir. Yapılan çalışmada öncelikle AnaNet adı verilen, 26 adet istasyondan oluşan ağ altyapısı kurulup, bu istasyonlardan gelen depreme ait iveme, hız ve yer değiştirme verileri geliştirilen AnaNet Sismik ağı yazılımı sayesinde hesaplanarak, sms veya eposta yoluyla yöneticilerle paylaşılmaktadır. Tüm bu mekanizma kurumsal bir şirketin ağında yaşanan problemlerin alarm yoluyla ağ yöneticilerine bildirilmesi ile benzer yapıya sahiptir. Ağı uzaktan izleme ve müdahale konusunda verilebilecek önemli bir örnek ise finans sektöründe kullanılan bankamatik (ATM) cihazlarının yönetiminin ağ yönetim protokolleri aracılığıyla yapılmasıdır. Iqbal (2009)'in yapmış olduğu tez çalışması geniş bir coğrafi alana yayılan bankamatik hizmetinin maliyetlerini düşürmek için yapılabilecek çözümleri içermektedir. Yapılan gerçek ortam testleri çıktılarına göre SNMP aracılığıyla uzaktan izlenen bankamatikler sayesinde yerinde müdahale maliyetinde azalma, kesintisiz bankacılık hizmeti sağlanması, çalışma süresinin artırtması ve aksama süresinin ise azaltılarak müşterilerine kaliteli hizmet sağlandığı sonuçlarına ulaşılmıştır. Ağ yönetiminin büyük coğrafi alana yayılmış kritik öneme sahip işlerde kullanılması ve farklı sektörlerdeki problemlere çözüm üretmesi gösteriyor ki, çoğu zaman farkında olunmasa da kullandığımız veya yaşamımızı etkileyen birçok konuda işimizi kolaylaştırmaktadır.

Ağ yönetim sistemlerinin bu kadar çok alanda kullanılması ile birlikte ağın içerden veya internet gibi herkese açık geniş alan ağlarından gelebilecek tehditlere maruz kalması kaçınılmaz olmaktadır. SNMP üzerinde gerekli güvenlik tedbirleri ve doğru yapılandırma yapılmaması durumunda ağ servislerinin kullanılamaz hale getirecek hizmet dışı bırakma (DOS/DDOS), IP aldatması (IP Spoofing) gibi siber saldırılara açık hedef haline gelinebilir. Bu konuyla alakalı ağ yönetim uygulamaları ve kullanıcıları etkileyebilecek diğer ilgili teknik konularda çalışmalar yapan geniş bant internet teknik danışma grubu (BITAG) organizasyonu SNMP açıklarından kaynaklı DDOS saldırılarını önlemeye yönelik çalışma raporu yayınlamıştır. Raporda organizasyona üye olan Comcast internet servis sağlayıcı (Internet Service Provider-ISP) şirketinin SNMP açıklarından

kaynaklanan DDOS saldırılarına maruz kalmasından yola çıkarak, ağ yönetim protokollerinin doğru kullanılmaması durumunda güvenlik açığına yol açtığı ve internet servis sağlayıcıları ile cihaz üreticilerinin bir takım önlemler alması gerektiği sonucuna varılmıştır. Konu ile ilgili kaygılar ve olabilecek etkiler sırasıyla ifade edilerek, organizasyonun teknik çalışma grubu tarafından SNMP güvenliği için servis sağlayıcıları, son kullanıcılar ve ağ yöneticileri tarafında yapılmasının gerekli olan tedbir, ayar ve uygulamaların tümü gösterilmiştir (BITAG 2012).

Bu tez kapsamında, araştırmaya konu olan kaynakların incelenmesi ve akabinde yürütülen testler sonucunda, kurumsal ağların etkin ve verimli bir şekilde yönetilmesi için yapılması gereken çalışmalara katkı sağlanması hedeflenmiştir. Ayrıca günümüzde kurumsal ağlarda dikkate alınmayan ama ağ genelinde önemli yönetimsel unsurların, ağ yöneticileri tarafından anlaşılmasını sağlayıp, eksiklerin giderilmesine de yardımcı olması beklenmektedir.

3. MATERYAL ve METOT

3.1 Ağ Kavramına Giriş

Genel olarak, ağ terimi birbirine bağlı herhangi bir grubu veya sistemi ifade etmektedir. Daha özel olarak ağ, iki sistem arasında bilgi paylaşımını sağlayan bir yöntemdir. Bilgi teknolojisinde ise bir ağ iletişim yolları ile birbirine bağlı bir dizi nokta veya düğümdür. Ağlar diğer ağlarla bağlantı kurabilir ve alt ağlar içerebilir. Mevcut bilgi alanında ağlar, telekomünikasyon ağları ve bilgisayar ağları olarak tanımlanmaktadır.

Telekomünikasyon ağı, verilerin bir bölümden diğerine çoklu bağlantılar ve çeşitli düğümler üzerinden geçerek ulaştığı ağlardır. Telekomünikasyon ağı arasındaki bilgi alışverişi işlemi elektronik vericiler tarafından elektromanyetik dalgaların gönderilmesiyle sağlanmaktadır. Günümüzde dünyanın birçok yerinde televizyon, radyo, telefon gibi iletişim cihazlarına erişim telekomünikasyon ağı aracılığıyla sağlanmaktadır. İnternet üzerinden bilgisayarların iletişim kurması telekomünikasyon ağına verilebilecek en önemli örnektir.

Bilgisayar ağı, birbirine bağlı bilgisayar sistemleri veya cihazlar topluluğudur. Ayrıca bilgisayarların birbirleriyle iletişim kurmasına, kaynakları ve bilgileri paylaşmasına olanak tanımasıdır. Bilgisayar ağlarında genellikle biri bilgisayar olmak üzere ağa bağlanabilen en az iki cihaz bulunmaktadır. Cihazlar birkaç metre (Ethernet veya wifi aracılığıyla) veya neredeyse sınırsız mesafelerle (internet üzerinden) ayrılabilirler. Evdeki kişisel bilgisayar üzerinden internet bağlantısı kurulması veya bir sensör üzerinden sıcaklık, ses, hareket gibi bilgilerin elde edilmesi bilgisayar ağlarına verilebilecek en temel örneklerdir.

3.2 Ağ Türleri

Bilgisayar ağları, ağdaki bilgisayarlar arasındaki mesafeye göre sınıflandırılmaktadır. Bilgisayarların bir bölümde mi, bir şehirde mi, yoksa bir ülke veya kıta gibi geniş bir coğrafi bölgede olup olmadığına göre üç farklı ağ türü tanımlanmıştır.

3.2.1 Yerel Alan Ağı (Local Area Network-LAN)

Yerel alan ağları ev, ofis veya bina gibi küçük bir coğrafi alanı kapsayan ağ türüdür. Bu ağ türü üç coğrafi sınırlamanın en düşük maliyetine ve en az genel kapasiteye sahip olanıdır. Genellikle yazıcı, dosya gibi kaynakların paylaşmak için kurulan ağlardır. Ayrıca yerel alan ağları daha büyük ağlar oluşturmanın yapı taşlarını oluşturmaktadır.

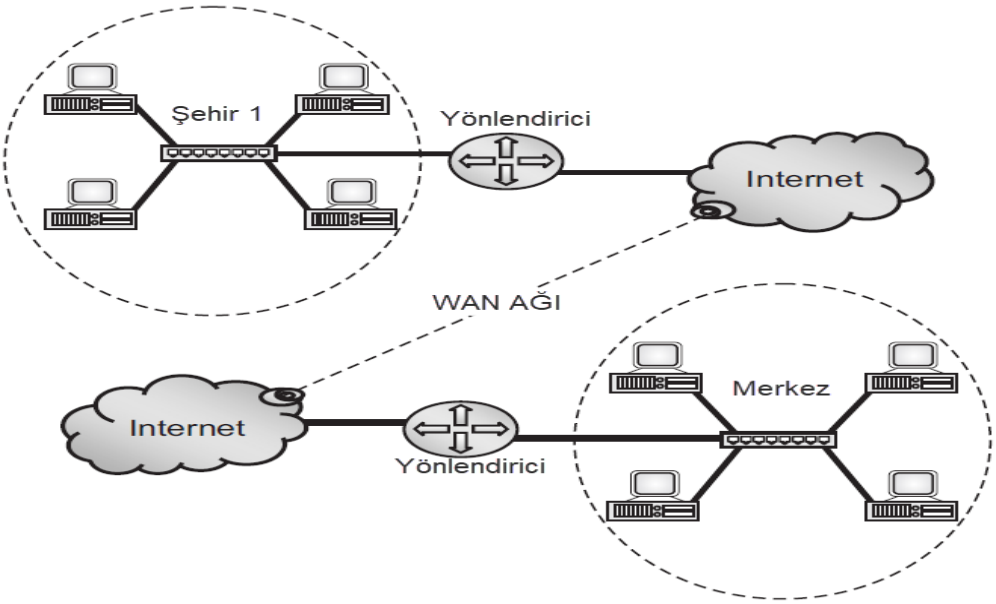
3.2.2 Şehir Alan Ağı (Metropolitan Area Network-MAN)

Bilgisayarlar birbirinden ayrıldıkça, LAN kurulumu daha zor hale gelmekte ve ek iletişim cihazları(yönlendirici, köprü, ağ geçidi) kullanılması gerekmektedir. Şehir alan ağı iki veya daha fazla yerel alan ağını birbirine bağlayan ancak yakın şehir sınırlarının ötesine geçmeyen ağ türüdür. Bu ağlar kullanımını kaybetmeye başlasa da, yerel sınırlarını aşan ve ek kaynak gerektiren ağ kavramı hala geçerlidir.

3.2.3 Geniş Alan Ağı (Wide Area Network-WAN)

Kullanılan ağ şehir alanlarının sınırlarının ötesine genişlemesi gerektiğinde şehir alan ağlarının kullanılabilirliği azalmaktadır. Bu nedenle ağ, Şekil 3.1'de gösterildiği gibi daha geniş bir alana yayıldığında geniş alan ağı olarak sınıflandırılmaktadır. Geniş alan ağlarının iletişim kurması gerektiği çok uzak mesafeler olmasından dolayı, bağlantıları için telekomünikasyon ağları (Servis sağlayıcı) kullanılmaktadır.

LAN bilgisayarları, çevre birimleri ve diğer aygıtları tek bir binada veya başka bir küçük coğrafi alanda bağlarken, WAN daha büyük coğrafi mesafeler arasında veri iletimini gerçekleştirmektedir. LAN teknolojileri, şirketlerdeki küçük coğrafi alanlarda veri iletimi için hem hız hem de maliyet verimliliği sağlamaktadır. Bununla birlikte şirketlerin bölge veya şubelerindeki kişilerin merkezi sistem ile iletişim kurabilmeleri ve kaynaklarını paylaşabilmeleri gerekmektedir. Bugün en büyük geniş alan ağına internet örnek verilmektedir. Geniş alan ağları sayesinde bankacılık, teknoloji, iletişim, endüstri gibi farklı ticari faaliyetler yaygın olarak kullanılabilmektedir.



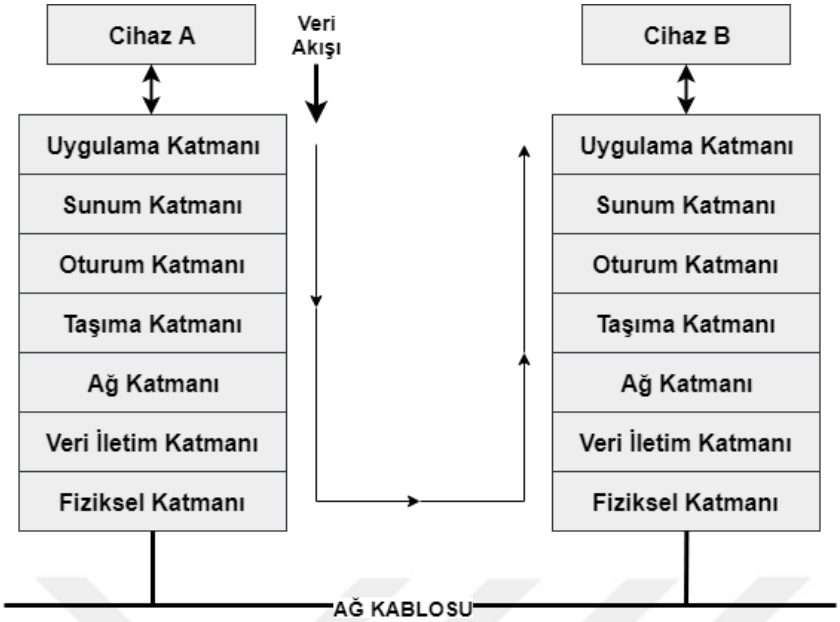
Şekil 3.1 Geniş alan ağı topolojisi.

3.3 Ağ Modelleri

Ağ teknolojisinin çalışma yapısını tanımlayan OSI referans ve TCP/IP olmak üzere iki önemli ağ modeli bulunmaktadır.

3.3.1 OSI (Open Systems Interconnetion) Referans Modeli

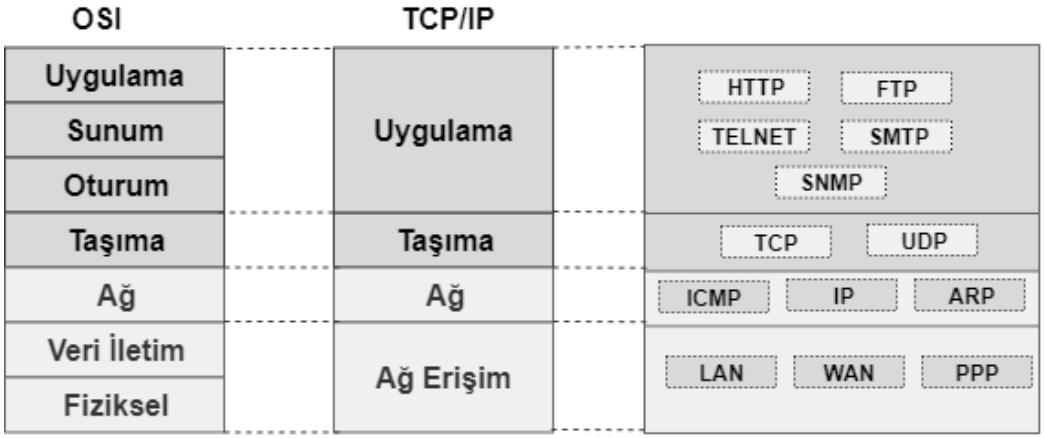
OSI, Uluslararası Standartlar Örgütü (International Organization for Standardization-ISO) tarafından 1978 yılında iki cihaz arasındaki haberleşmeyi tanımlamak için geliştirilmiş referans modelidir. Bilgisayar ağlarının kullanılmaya başlandığı ilk zamanlarda yalnız aynı üreticiye ait olan iki cihaz birbiriyle haberleşmekteydi. OSI referans modeli farklı üreticilere ait ağ cihazları birbiriyle haberleşmesini sağlamıştır. Şekil 3.2'de görüldüğü gibi OSI referans modeli yukarıdan aşağıya doğru yedi katmandan oluşmaktadır. Katmanlar kendinden sonraki bir üst katmana servis sağlama görevini yerine getirmektedir. Bununla birlikte her katman kendisine ait işleve ve bir dizi protokole sahiptir.



Şekil 3.2 İki cihaz arasındaki iletişimin OSI Referans modelindeki mantıksal şeması.

3.3.2 TCP/IP (Transmission Control Protocol/Internet Protocol) Modeli

TCP/IP modeli, sağlam bir ağ iletişim sistemi için 1982 yılında ABD Savunma Bakanlığı standartlarının gereksinimlerini karşılamak üzere tasarlanmış dört katmanlı bir referans modelidir. İletişim kuran tüm ağlar, TCP/IP modeline dayanmaktadır. TCP/IP, Şekil 3.3'de görüldüğü gibi OSI referans modelinde bulunan veri iletim katmanı fiziksel katmanıyla, sunum ve oturum katmanının uygulama katmanıyla birleşmesiyle oluşan dört katmanlı bir yapıya sahiptir.



Şekil 3.3 TCP/IP Modeli katmanlarının OSI referans modelindeki karşılığı.

3.4 Ağ Altyapısı Bileşenleri

Ağ yalnız bilgisayarlar ve kablolardan oluşan bir yapıdır demek yanlış olacaktır. Elektrik sinyallerini ve dijital bağlantıları yöneten, ağın işleyişi için belirli görevleri yerine getiren özel cihazlar da bulunmaktadır. Bilgisayarları, yazıcıları, faks makinelerini ve diğer elektronik aygıtları bir ağa bağlamak için kullanılan donanımlara ağ cihazları denir. Bu cihazlar aynı veya farklı ağlar üzerinden verileri hızlı, güvenli ve doğru bir şekilde aktarmaktadır. Ağ cihazları ağlar arası veya ağ içi olabilmektedir. Bazı cihazlar Ethernet kartı veya RJ45 konektörü gibi cihaza kurulurken, bazıları yönlendirici, anahtar gibi ağın bir parçası olmaktadır.

3.5 Bilgisayar Ağlarında Ağ Yönetimi

Günümüzde ağlar ve dağıtık sistemler kurumsal işletmelerin hepsinde kritik ve büyüyen bir öneme sahiptir. İşletmeler çeşitli ihtiyaçlar nedeniyle daha fazla uygulama ve kullanıcıyı destekleyen büyük ve karmaşık ağlara yönelmektedir. Bunun sonucunda bir ağ; bağlantılar, anahtarlar, yönlendiriciler, ana bilgisayarlar ve diğer aygıtlar içeren çok sayıda karmaşık, etkileşimli donanım ve yazılım parçasından oluşmaktadır. Farklı bileşenlerin bir araya gelmesiyle oluşan ağların zaman zaman arızalanacağı, ağ öğelerinin yanlış yapılandırılacağı, ağ kaynaklarının fazla kullanılacağı göz ardı edilmemelidir. Bu durumda ağın arıza sonucu verimli bir şekilde işlev görmemesinin maliyeti şirketler için son derece yüksek olacaktır. Görevi ağı çalışır ve sürdürülebilir durumda tutmak olan ağ yöneticileri bu tür sorunları tespit edebilmeli ve mümkün olan en kısa zamanda giderebilmelidir. Ancak büyük bir ağ, sadece insan gücüyle tek başına bir araya getirilemez ve yönetilmez. Bu nedenle ağ yöneticisi, geniş alana yayılmış binlerce ağ bileşeninin takibini yapabilmesi için merkezi bir noktadan ağın izlenmesine, yönetilmesine ve kontrolüne yardımcı olacak araçlara ihtiyaç duyulmaktadır.

Hegering vd.'ne (1999) göre ağ yönetimi, bir sistemin kurumsal hedeflere uygun olarak etkin ve verimli şekilde çalışmasını sağlayan işlemler bütünüdür. Bunu başarmak için ağ kaynaklarının denetlenmesi, ağ hizmetlerinin koordine edilmesi, ağ durumlarının izlenmesi ve ağ durumunun raporlanması gerekmektedir.

Tanımdan da anlaşılacağı gibi ağ yönetiminin amaçları aşağıdaki başlıklarda özetlenebilir.

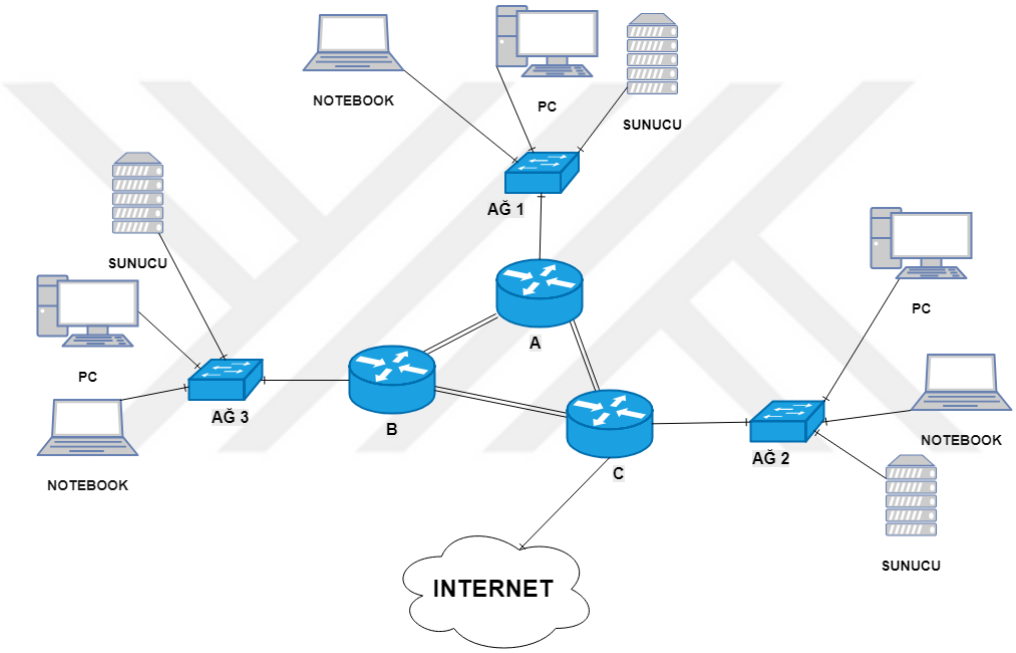
- **Sistem kaynaklarını ve hizmetlerini yönetmek:** Sistem durumlarını, aygıt yapılandırmalarını ve ağ hizmetlerini denetleme, izleme, güncelleştirme ve raporlamayı içerir.
- **Karmaşık sistem yönetimini basitleştirmek:** Sistem yönetimi bilgisini insani olarak yönetilebilir bir biçime ayıran yönetim sistemlerinin görevidir. Tersine, yönetim sistemleri de üst düzey yönetim hedeflerini yorumlama yeteneğine sahip olmalıdır.
- **Güvenilir hizmetler sağlamak:** Yüksek kaliteli hizmet ağları sağlayarak sistem kesintilerini en az seviyeye indirmek anlamına gelir. Ağ yönetim sistemleri ağdaki hataları tespit etmeli, düzeltmeli ve sistemlerin doğru çalışmasına yardımcı olmalıdır.
- **Maliyet bilincinin korunması:** Sistem kaynaklarını ve ağ kullanıcılarını takip ederek tüm ağ kaynağı ve servis kullanımları izlenmeli ve raporlanmalıdır.

Bir başka kabul edilebilir tanım olarak ağ yönetimi; ağa bağlı sistemlerin çalışması, yönetimi, bakımına ilişkin; faaliyetler, yöntemler, işlemler ve araçlar bütünü şeklinde ifade edilebilir (Clemm 2006).

- Faaliyet; ağın düzgün ve sorunsuz çalışmasını sağlar. Kullanıcılar etkilenmeden önce, sorunların en kısa sürede tespit edilebilmesi için ağın izlenmesini içerir.
- Yönetim; ağdaki kaynakları takip etme ve bunların nasıl atanacağını ele alır. Ağı kontrol altında tutabilmek için gerekli olan tüm yönetim faaliyetlerini içerir.
- Bakım; onarımların ve yükseltmelerin gerçekleştirilmesi ile ilgilidir. Örneğin, donanımın değiştirilmesinin gerektiği durumda, bir yönlendiriciye işletim sistemi güncellemesi imajı kurulmasına ihtiyaç duyduğunda veya ağa yeni anahtar cihazı eklendiğinde yapılması gereken faaliyetlerdir. Bakım ayrıca, yönetilen ağın cihaz yapılandırma parametrelerini ayarlama, daha iyi çalışmasını sağlamak için düzeltici ve önleyici tedbirleri içerir.
- Sağlama; belirli bir hizmeti desteklemek için ağdaki kaynakları yapılandırmakla ilgilidir. Örneğin, yeni müşterinin internet hizmeti alabilmesi için geniş alan ağındaki cihazlarda gerekli yapılandırma ayarlarının yapılmasını içerir.

Kısacası ağ yönetimi; faaliyetlerin ve kaynakların planlanması, organize edilmesi, izlenmesi ve kontrol edilmesi ile ağ hizmetinin kullanılabilir ve doğru kalmasıdır.

Şekil 3.4'de bu durum basit bir senaryo ile anlatılmaktadır. Şekilde üç yönlendiriciden, ana bilgisayarlardan ve sunuculardan oluşan bir ağ topolojisi gösterilmektedir. Bu örnekte topoloji üzerinden ağ yöneticisinin ağ yönetim araçlarına sahip olmasının getireceği birçok fayda bulunmaktadır. Bunlar:



Şekil 3.4 Ağ yönetiminin kullanımını gösteren basit bir senaryo.

Bir anahtar veya yönlendiricide port arayüz arızasını tespit etme: Uygun ağ yönetim araçları, bir ağ öğesinin (Yönlendirici A), port arayüzlerinden birinde bağlantının kopmuş olduğunu ağ yöneticisine bildirebilir. Ağ trafiğini aktif olarak izleyen ve analiz eden bir ağ yöneticisi, problemleri algılayarak kullanıcıların sorundan etkilenmesini engelleyebilir ve cihaz port arayüz durum bilgilerini anlık olarak raporlayabilir.

Ana bilgisayarı izleme: Ağ yöneticisi tüm istemci bilgisayarlarının çalışıp çalışmadığını düzenli olarak kontrol edebilir. Yaşanan bağlantı kesintilerini şirkette çalışan bir personel tarafından rapor edilmeden hızlı şekilde görüntüleyebilir.

Ağın bant genişliğinin dağıtımına yardımcı olmak: Bağlantı kullanımını izleyerek, ağ yöneticisi yerel ağ veya internete giden bağlantıya (Yönlendirici C den giden dış ağ) aşırı yüklenildiğini ve daha yüksek bant genişliği bağlantısının sağlanmasının gerekli olduğunu belirleyebilir. Ağ yöneticisi, sunuculara ana bilgisayarlardan gelen isteklerin oluşturduğu trafiği etkin bir şekilde kontrol ederek bant genişliği kullanımının ağda ciddi soruna yol açmadan önce bağlantıdaki tıkanıklık seviyeleri belirli bir eşik değerini aştığında otomatik olarak bilgilendirilmek isteyebilir. Tüm bu gelen bilgiler doğrultusunda ağdaki gereksiz trafik kaynakları tespit edilerek, engellenebilir.

Yönlendirme tablolarındaki değişiklikleri tespit etme: Hat yedekliğinin bulunduğu geniş alan ağlarında yönlendiricilerin yönlendirme yapılandırılması sırasında dinamik yönlendirme (örneğin Ağ 2 de bulunan PC Ağ 3 deki sunucuya ulaşmak için yönlendirici B üzerinde bulunan hattı veya yönlendirici C üzerindeki hattı kullanabilir) yanlış yapılmış ise Route flapping (yönlendirme tablolarındaki sık değişiklikler) meydana gelir. Bu şekilde ağ yöneticisi tarafından yanlış yapılandırılmış bir yönlendirici tespit edilerek ağ çökmeden önce hata düzeltilebilir.

Ağa izinsiz girişlerin tespiti: Ağ yöneticisi, trafiğin şüpheli bir kaynaktan (TCP 1700) geldiğini veya belirli trafik türlerinin (belirli bir sunucuya yönlendirilen çok sayıda SYN paketi) varlığını tespit etmek isteyebilir. Bu şekilde sistemlere yapılan olası siber saldırılara karşın önlem alınması sağlanabilir.

Ağ yönetim sistemleri dört temel aşamayı mutlaka gerçekleştirmelidir. Bunlar:

- Kural Oluşturma: Ağ için normal çalışma koşullarını ve beklentileri tanımlar.
- İzleme: Oluşturulan kurallara uyulup uymadığını görmek için ağın durumu raporlanır.
- Analiz: Ağın düzenli çalışıp çalışmadığı belirlenir. Ağ düzgün çalışmıyorsa, sorunun nedeni belirlenir ve sorunun giderilmesi için yapılması gerekenler bulunur.
- Kontrol: Bu aşamada, ağın davranışını düzeltmek için analiz aşamasındaki eylem planları uygulanır.

3.6 Ağ Yönetim Modeli

Uluslararası Standardizasyon Örgütü (ISO), ağ yönetiminin yapısal bir çerçeveye yerleştirilmesi ve tutarlılık sağlaması amacıyla uluslararası bir ağ yönetim modeli oluşturmuştur. Model FCAPS olarak isimlendirilmiştir. FCAPS, ağ yönetimi için gereksinimlerimizi organize etmemizi sağlayacak beş temel alanı belirler. Bunlar Hata Yönetimi, Yapılandırma Yönetimi, Hesap Yönetimi, Performans Yönetimi, Güvenlik Yönetimidir.

3.6.1 Hata Yönetimi (Fault Management)

Karmaşık bir ağın düzgün çalışmasını sağlamak için, sistemlerin bir bütün olarak ve her temel bileşenin uygun çalışma düzenine sahip olmasına dikkat edilmelidir. Ağ cihazları çeşitli elektriksel veya çevresel faktörlerden dolayı bozulabilir, yanlış yapılandırmalardan dolayı servislerde ve hatlarda kesintiler yaşanabilir. Hata meydana gelmeden önce önlem alınmamasından dolayı yaşanabilecek hizmet kesintileri nedeniyle maddi kayıplar yaşanabilir. Bu nedenle hata oluştuğunda, mümkün olduğu kadar hızlı bir şekilde;

- Arızanın tam olarak nereden olduğu belirlenmeli,
- Ağ, arızalı bileşen veya bileşenler olmadan çalışmanın etkisini en aza indirecek şekilde yeniden yapılandırılmalı,
- Ağın geri kalanını arızadan izole edilerek sistemlerin devamlılığı sağlanmalı,
- Ağı ilk durumuna geri yüklemek için hatalı bileşenler onarılmalıdır.

Hatalar beklenmedik kesinti, performans düşüşü ve veri kaybı ile sonuçlanabilir. Bu nedenle arıza durumlarının mümkün olduğunca çabuk çözülmesi gerekir. Hata yönetimi yapmanın amaçları; ağın kullanılabilirliğini artırmak, ağ kesintilerini azaltmak ve ağ arızasını hızlı bir şekilde çözüp ağı eski haline geri getirmektir. Bugün ağ yönetimi mimarisinin önemli bir parçası olan hata yönetimi, bir ağdaki arızayı tespit etme, izole etme, nedenini belirleme ve arızaları düzeltme gibi işlevleri kapsar (ANSI 1994).

Hata Tespiti: Hata tespiti, bir arızanın temel nedenini belirler. İlk hata bilgisine ek olarak, arızayı ilişkilendirmek ve sınırlamak için diğer varlıklardaki hata bilgileri kullanılabilir.

Hata İzolasyonu: Alarmların bir açıklamasını bulmak için gözlenen bir dizi arıza göstergesi analiz edilir. Bu aşamada, hata yayılımı ve kök nedeninin saptanması durumunda tespit edilen arızaya neden olan sorunun belirlenir. Hata izolasyonu süreci büyük önem taşımaktadır, çünkü hata yönetim sürecinin hızı ve doğruluğu büyük ölçüde ona bağlıdır.

Hata Düzeltme: Arızanın giderilmesinden ve arızalı cihaz veya tesislerin yerine yedek kaynak kullanan prosedürlerin kontrolünden sorumludur.

Yukarıda belirtildiği gibi, hata yönetimi iki teşhis adımından (hata tespiti ve hata izolasyonu) ve bir planlama adımından (hata düzeltme) oluşur. Hata yönetiminin temel görevi şunlardır:

- Potansiyel hataları önlemek ve tahmin etmek için ağ cihazlarının üzerinden geçen trafik durumları ve kullanımlarının gerçek zamanlı olarak izlenmesi.
- Ağ yöneticisini uyarmak için ağ hatalarına neden olabilecek eşikleri ve alarmların ayarlanması.
- Ağ cihazlarında ve bağlantılarda performans düşüşünü bildiren alarmların ayarlanması.
- Yeniden başlatmak, kapatmak için ağ cihazlarının uzaktan kontrol edilmesi.

3.6.2 Yapılandırma Yönetimi (Configuration Management)

Yapılandırma yönetimi, bir ağın başlangıçta yapılandırılması ve ardından değişen ağ gereksinimlerine uygun olarak ayarlanması işlemidir. Bu işlev ağ yönetiminin en önemli kısmıdır, çünkü yanlış yapılandırma ağın düzensiz veya hiç çalışmamasına neden olabilir.

Yapılandırma yönetimi süreci, ağ bileşenlerinin ve bağlantılarının tanımlanmasını, her bir cihazın yapılandırma bilgilerinin toplanmasını ve ağ bileşenleri arasındaki ilişkinin

tanımlanmasını içerir. Bu görevleri yerine getirmek için, ağ yöneticisinin ağ hakkında topoloji ve cihaz yapılandırma bilgileri ile ağ bileşeninin kontrolüne ihtiyacı vardır. Cihazlar hakkındaki bilgilerin merkezi olarak depolanması için gerekli araçları sağlar ve bu nedenle arıza, güvenlik, performans ve hesap yönetimi için temel oluşturur. Yapılandırma yönetiminin temel görevleri şunlardır:

- Kontrollerin oluşturulmasını kolaylaştırmak.
- Belirli donanım ve yazılım için temel standartları izleme ve uygulama.
- Yapılandırma yedeklerini saklama ve tüm ağ bileşenlerinin dökümünün tutulması.
- Kullanıcı bilgileri ile yapılandırma değişikliklerinin loglarının kaydedilmesi.

3.6.3 Hesap Yönetimi (Account Management)

Hesap yönetimi, ağı ve sistem kaynaklarını kimin kullandığını, ne ölçüde kullandığını belirleme ve bu kullanıcılara kullanımlarına göre bant genişliği veya kota tahsis etme işlemidir. Bu tür bilgiler, bir ağ yöneticisinin, kullanıcılara doğru kaynakları tahsis etmesinin yanı sıra, ağ büyümesi için plan yapmasına yardımcı olur. Bu planlama ağ sorunlarını azaltır. Çünkü ağ kaynakları, kaynak kapasitelerine göre paylaştırılabilir ve tüm kullanıcılar arasında ağ erişiminin adilliğini en üst düzeye çıkarır. Bunun yanı sıra, erişim ayrıcalıkları ile kullanım kotaları oluşturulabilir ve kaynak bilgileri kontrol edilebilir. Bu aynı zamanda iç operasyonların maliyetinin piyasa ile ilgili fiyatlarla karşılaştırılması ve çok pahalı olması durumunda hizmetin alternatif kaynaklardan alınması için bir temel sağlayacaktır. Hesap yönetiminin temel görevleri şunlardır:

- Servis / kaynak kullanımını takip etme.
- Hizmet bedeli saptama.
- Kullanım kotalarını belirleme.
- Dolandırıcılık raporları hazırlama.
- Birden fazla kullanıcı ve cihazdan gelen kaynak kullanımlarını birleştirme.

3.6.4 Performans Yönetimi (Performance Management)

Performans yönetimi, bir ağın ve kaynaklarının kullanım, verimlilik, hata miktarları ve yanıt süreleri bakımından performansını ölçmeyi içerir. Performans yönetimi bilgisiyle, bir ağ yöneticisi ağdaki olası aşırı trafik yoğunluğu ve erişim kesintilerini azaltabilir veya önleyebilir.

Performans metrikleri makro ve mikro olmak üzere iki düzeyde çalışır. Makro seviye verim, tepki süresi, kullanılabilirlik ve güvenilirliği hedefler. Mikro seviye bant genişliği, kullanım, hata oranı, en yüksek yük, ortalama yük ile ilgili değerleri içerir. Performans yönetiminin amacı, mevcut bant genişliğini aşan kullanımları tespit ederek bundan kaynaklı arızaları giderip ağ kaynaklarının etkin kullanımını sağlamaktır.

Ağ Performansı yönetimi iki bileşenden meydana gelmektedir. Birincisi, ağ donanımının davranışını ve ağdaki ögelerin etkinliğini değerlendiren işlevdir. İkinci de istatistiksel bilgilerin toplanarak, geçmiş logların korunmasını ve incelenmesini, sistem performansının belirlenmesi ile sistem çalışma modlarını değiştirmeyi içeren işlevdir. Performans yönetiminin temel görevleri şunlardır:

- Kullanım ve hata oranlarının belirlenmesi.
- Performans verilerinin toplanması.
- Performans veri analizinin yapılması.
- Sorun bildirilmesi.
- Kapasite planlamasının yapılması.
- Performans raporunun oluşturulması.

3.6.5 Güvenlik Yönetimi (Security Management)

Güvenlik yönetimi, ağ kaynaklarına erişimi yerel yönergelere göre kontrol etmek için bir uygulanması gereken bir işlemdir. Güvenlik yönetimi sayesinde ağ sabote edilemez ve uygun yetkiye sahip olmayan kullanıcılar tarafından hassas bilgilere erişilemez.

Güvenlik yönetimi, ağları ve sistemleri kişilerin yetkisiz erişimlerinden koruma, güvenlik hizmetlerini ve mekanizmalarını oluşturma, güvenlikle ilgili olayları bildirme, kriptografik anahtarlama malzemesinin dağılımını kontrol etme, kullanıcı erişim haklarının yetkilendirilmesi gibi çeşitli güvenlik politikalarını içerir.

Güvenlik yönetimi iki eylem grubu ile ilgilidir. Birincisi, yetkisiz kullanıcılar tarafından hassas bilgilere veya kaynaklara erişimin engellenmesi, İkincisi yetkili kullanıcıların erişimini kısıtlamaya neden olacak kötü niyetli eylemlerin önlenmesidir (DDOS veya DOS atak). Ağın güvenlik ihlallerini önleyen kaynaklar aşağıdaki gibidir.

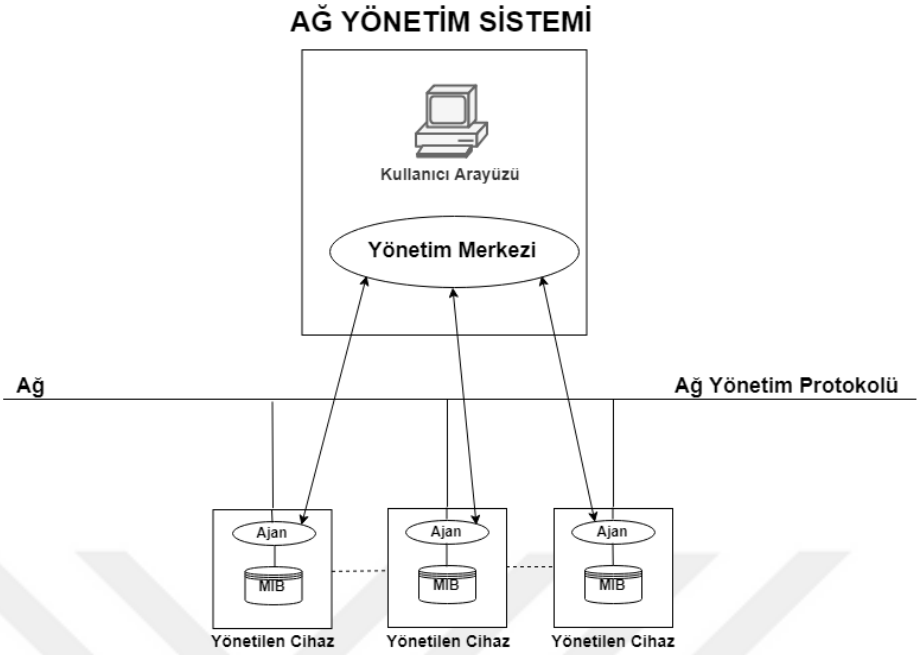
- Güvenlik Duvarı (Bir TCP/UDP bağlantı noktası adresi kullanarak paket filtreleme)
- Şifreleme (Paketlerin SSL ile şifrelenmesi)
- Kimlik Doğrulama (Veri bütünlüğü ve veri kaynağı kontrolü)
- Yetkilendirme (Okuma, okuma-yazma, erişimin reddi)

Güvenlik Yönetiminin temel görevleri şunlardır:

- Dış kaynak Erişim kontrolü.
- Erişim kayıtlarının tutulması.
- Veri gizliliğinin sağlanması.
- Kullanıcı erişim haklarının kontrolü.
- Güvenlik ihlallerine ve girişimleri karşı önlem alınması.
- Güvenlik alarmı ve olay raporlarının oluşturulması.

3.7 Ağ Yönetim Mimarisi

Kurumsal bir yapının geniş alan ağında, ağ cihazları dağıtık bir şekilde ve merkezden uzak bölgelerde bulunur. Dolayısıyla söz konusu cihazlardan veri toplanabilmesi için cihazlar uygun ve gerekli şekilde yapılandırılmalıdır. Bu yapılandırma işlemini de ağ yönetim mimarisine uygun hazırlanması gerekmektedir. Şekil 3.5'de gösterildiği gibi ağ yönetim mimarisinin üç ana bileşeni vardır. Bunlar; yönetim merkezi, yönetilen cihaz ve ağ yönetimi protokolüdür.



Şekil 3.5 Temel ağ yönetim mimarisi.

Yönetim merkezi; ağ yöneticisi ve araçlardan oluşur. Yönetici, ağ yöneticisinin ağ yönetimi işlevlerini gerçekleştirdiği konsoldur. Yönetici, sunucuya kurulu bir yönetim yazılımı veya donanımı olabilir.

Yönetilen cihaz; yönetim merkezi tarafından yazılım dâhil olmak üzere kontrol edilen ağ cihazlarıdır. Anahtar ve yönlendirici buna örnek olarak verilebilir.

Ağ yönetimi protokolü; yönetim merkezi ile yönetilen cihazlar arasında uygulanan bir politikadır. Bu protokol ile yönetim merkezinin yönetilen cihazların durumunun belirlenmesi sağlanır. Yönetici, gerekli olan tüm bilgileri her uç noktaya kurulmuş olan ajanlar aracılığı ile toplar. Ajanlar, yönetilmekte olan cihaza bir arayüz ortamı oluştururlar. Ajan, yönetilen cihazlardan aldıkları donanım bilgileri, yapılandırma ayarları, performans verileri gibi nesneleri yönetim veri tabanına (MIB)'e aktarır. Ağ yönetimi protokolleri (SNMP, CMIP vb.) ise, yöneticilerin ve ajanların bu nesnelere erişip iletişim kurmasına izin verir.

Tipik bir ağ yönetim sistemi aşağıdaki parçalardan oluşur:

Ağ elemanları: Uluslararası Telekomünikasyon Birliği (International Telecommunications Union- ITU-T) tarafından belirlenen standartlara göre ağ ile iletişimde olan ve izlenmesi veya kontrol edilmesi amacıyla kullanılan cihazlar ağ elemanları olarak adlandırılır (ITU-T 2000). Ağ elemanları, ağlara bağlı bilgisayarlar, yönlendiriciler ve sunucuları gibi donanım aygıtlarıdır.

Yönetici: Bir yönetici komutlar üretir ve ajanlardan gelen bildirimleri alır. Bir sistemde genellikle bir ya da iki yönetici bulunur.

Ağ Yönetim İstasyonları (NMSs): Ağ yönetim istasyonları, ağ elemanlarını izleyen ve kontrol eden uygulamaları yönetir. Fiziksel olarak ağ yönetim istasyonları yüksek hızlı işlemci, bellek ve geniş disk alanlarına sahip bilgisayarlardır. Yönetilen her ağ da en az bir ağ yönetim istasyonu bulunmaktadır.

Yönetim protokolü: Yönetim protokolü, ajanlar ve ağ yönetim istasyonları (NMSs) arasında yönetim bilgilerinin aktarımında kullanılır. Bu konu ağ yönetim protokolleri başlığı altında ayrıca incelenecektir.

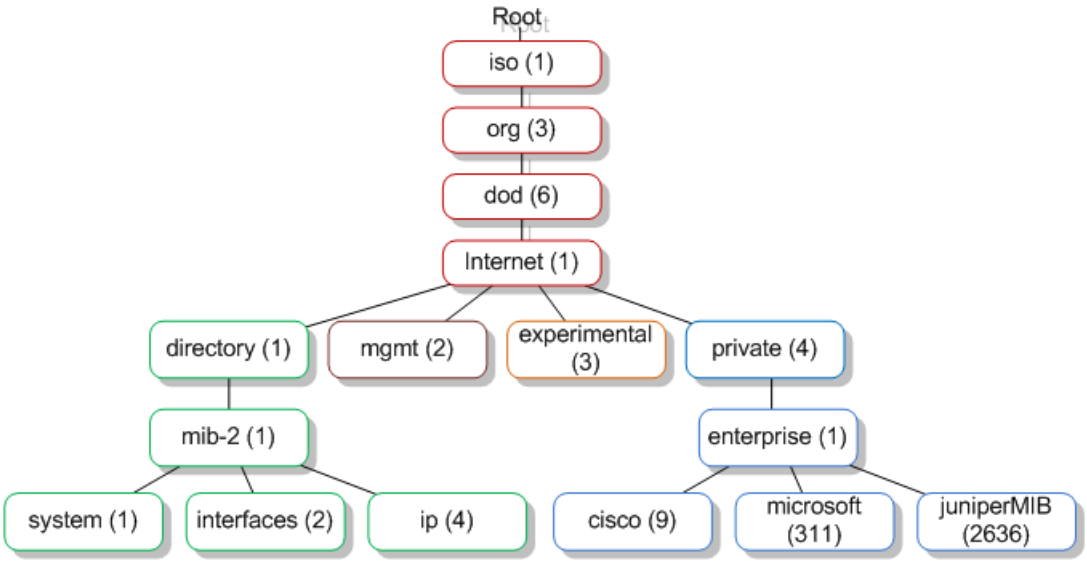
Ajanlar: Ajanlar, bir ağ elemanı tarafından alınan hata paketlerinin sayısı, performans bilgileri gibi yönetim bilgilerini toplar ve saklar. Ajanlar üzerindeki ağ bilgilerini yöneticinin anlayabileceği, ağ protokolü ile uyumlu bir biçime dönüştürerek yöneticinin komutlarına cevap verir ve yöneticiye gerekli bildirimleri gönderir. Bir sistemde çalışan birçok ajan kullanılabilir.

Yönetilen nesne: Sinyal terminalleri, yönlendirmeler, olay kayıtları, alarm raporları ve kullanıcı verileri gibi tüm fiziksel ve mantıksal kaynaklar yönetilen nesneler olarak kabul edilir (ITU-T 2000). Örneğin; Anahtar cihazının üzerinde takılı olan bilgisayarların bilgisini tuttuğu tablo yönetilen bir nesnedir.

Yönetim bilgisinin yapısı (SMI): Yönetim bilgisinin yapısı, nesnelerin isimlendirilmesine ilişkin kuralları tanımlamak ve yönetilen bir ağ merkezindeki nesneleri kodlamak için kullanılır. SMI ile tanımlanan ve yönetilen nesneler, yine SMI'da

tanımlanan hiyerarşik yapıya uymalıdırlar (RFC 1213). Bir başka ifade ile SMI, yönetilen bir ağ merkezindeki belirli bir veri tipinin tanımlandığı dildir. Bu tanımlamaya göre yönetim bilgi tabanı (MIB) içerisindeki her nesne SMI'daki kurallara göre tanımlanmıştır.

Yönetim bilgi tabanı (Management Information Base-MIB): Ağdaki cihazları yönetmek için kullanılan bir veri tabanı türüdür. Bir ağdaki cihazları yönetmek için kullanılan veri tabanındaki nesneler topluluğunu içerir. MIB'deki nesneler, yönetim bilgi yapısının (SMI) ASN.1 alt kümesi kullanılarak tanımlanmıştır. Şekil 3.6'daki örnek MIB ağacında yönetilecek cihazın üreticisi için ayrılmış dalı göstermektedir. Burada üretici (Cisco, Microsoft vb.) firmaların sahip oldukları dalın altında geliştirdikleri donanım ve yazılımın yönetim parametreleri bulunmaktadır. Yönetici bu düğümlere erişerek yöneteceği nesnenin bilgilerini elde edebilir.



Şekil 3.6 MIB ağacı ve erişilecek nesnelerin dalları (İnt. Kyn. 10).

3.8 Ağ Yönetim Protokolleri

Protokoller, ağ yönetim sistemi ile yönetilen cihazlar arasındaki iletişimi sağlayan kurallardır. Yönetim sistemi, cihazların durumunu sorgulayarak ajanlar aracılığıyla işlem yapmasına olanak sağlar. Ajanlar ağ da yaşanan alarmları ve hataları (bileşen arızaları, performans eşiklerinin aşılması) yöneticiye bildirmek için ağ yönetim protokolünü

kullanır. Ağ yönetim protokolleri ağı yönetmek için kullanılmaz. Ağ yöneticisinin ağı yönetmek için kullanacağı özellikleri sağlar.

Bu protokolleri standart haline getiren farklı kuruluşlar vardır. Standart haline getirilmesi sayesinde üreticiler geliştirdikleri ürünleri piyasaya bu standartlara uygun şekilde çıkarmaktadır. Çizelge 3.1'de standart kuruluşları tarafından verilen ağ yönetim protokolleri listesi verilmektedir.

Çizelge 3.1 Ağ yönetim protokolleri.

Kısaltma	Kuruluş	Protocol
IETF	The Internet Engineering Task Force	SNMP, MIBs, SMI, Netconf
ISO	International Organization for Standardization	CMIS, CMIP
ITU	International Telecommunication Union	TMN
W3C	World Wide Web Consortium	XML technologies
DMTF	Distributed Management Task Force	WBEM, CIM
OASIS	Organization for the Advancement of Structured Information Standards	WSDM
TMF	Tele Management Forum	eTOM, ITIL
OMG	Object Management Group	UML, Corba

Ağ yönetim protokolleri içerisinde ilk geliştirilen basit ağ yönetim protokolüdür (SNMP). Bilgisayar ağları ilk gelişmeye başladığı zamanlarda bu ağların yönetim ihtiyacının olduğu görülmüştür. Fakat henüz ağ sistemleri olgunlaşmadığı ve tanımlı standartlar bulunmadığı için yönetim protokolü yerine üreticiler tarafından kolay uygulanabilecek basit bir protokol geliştirilmiştir. Bu basit protokol uzun yıllar birçok üretici tarafından uygulanmış ve desteklenmiştir. Daha sonra uzaktan ağ izleme (RMON) ve ortak yönetim bilgi protokolü (CMIP) gibi ağ yönetimi açısından daha kabiliyetli protokoller geliştirilmiştir. Fakat bu protokoller karmaşık oldukları, daha fazla sistem kaynağı tükettikleri ve sonradan uygulamaya girmiş olmaları gibi nedenlerden dolayı beklenen ilgiyi görememişlerdir (Binici 2006).

3.8.1 Basit Ağ Yönetim Protokolü (Simple Network Management Protocol-SNMP)

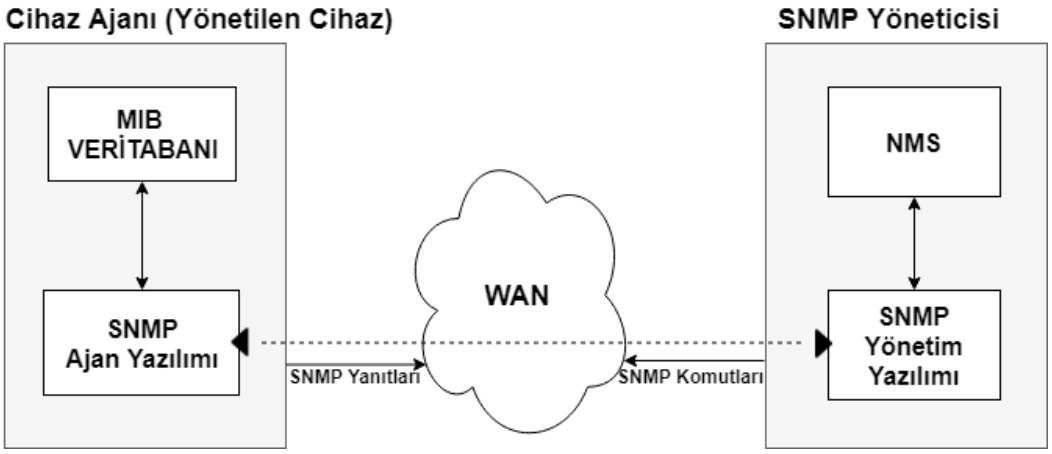
SNMP, 1988 yılında IP tabanlı cihazları yönetmek için bir standardın artan ihtiyacını karşılamak üzere geliştirilmiştir. SNMP, bir ağı üreticiden bağımsız bir şekilde izlemek ve kontrol etmek için standart sunar. Uygulama katmanında çalışan TCP/IP paketinin bir parçası olan bu protokol, bir ağa bağlı ana bilgisayarlar ve cihazlar tarafından tutulan ağ bilgilerinin alınmasına ve değiştirilmesine izin verir.

SNMP protokolü donanımlardan bilgi toplayabildiği gibi gerekli izin ve tanımların yapılmasıyla sunucu sistemleri, veri tabanları ve işletim sistemlerinden de bilgi toplayabilir. Ağ yöneticisi, uzak ana bilgisayarlardan gelen ağ sorunlarını tespit etmek, bu sorunları düzeltmek ve yönetimi merkezileştirmek için SNMP'yi kullanabilir.

3.8.1.1 SNMP Mimarisi

SNMP; yönetici, ajanlar, yönetim bilgisi veri tabanı (MIB), yönetilen nesneler ve ağ protokolünden oluşan yönetici/ajan modeline dayanmaktadır. SNMP, yöneticilerin ve ajanların nesnelere (donanım bilgisi, yapılandırma parametreleri, performans verileri vb.) erişmek amacıyla iletişim kurmasını sağlar.

Ağ aygıtları yönetilmeyen ve yönetilen olmak üzere iki sınıfa ayrılır. Yönetilmeyen aygıtlar, ağ yönetim protokolü veya uygulaması tarafından analiz edilme yeteneğine sahip değildir. Yönetilen aygıtlar için bir ağ yöneticisine veya bilgi teknolojisi uzmanına izin verilir. Yönlendirici, ağ geçidi veya sunucu gibi yönetilen her ağ cihazının ajan olarak adlandırılan bir toplayıcısı vardır. Ajan, cihaz hakkında bilgi toplar ve bu bilgileri yönetim bilgi tabanı (MIB) olarak adlandırılan veri tabanında saklar. Yönetici, yönetilebilir ağ cihazlarında bulunan ajanlara istekleri gönderen, üzerinde ağ yönetim yazılımı bulunan bir sunucudur (Şekil 3.7).



Şekil 3.7 SNMP çalışma mimarisi.

SNMP, yönetici ile ajan arasındaki haberleşme için UDP'yi kullanır. UDP, istekleri ve veri gönderimlerinin takibini yapmadığından dolayı güvenilir olmasa da daha hızlı veri akışı sağlar. SNMP veri paketlerinde gönderilip alındığına dair hiçbir onay bulunmadığından, ajanlardan gönderilen paketler kaybolabilir ve bu kayıptan yöneticinin haberi olmaz.

3.8.1.2 SNMP Sürümleri (SNMP Versions)

(The Internet Engineering Task Force-IETF) SNMP de dâhil olmak üzere İnternet trafiğini düzenleyen standart protokollerinin tanımlanmasından sorumludur. IETF tarafından tanımlanmış üç SNMP sürümü vardır. Bunlar SNMPv1, SNMPv2 ve SNMPv3'dür. SNMPv1 ve SNMPv2 ortak özelliklere sahiptir. SNMPv2 ek protokol işlemleri gibi daha gelişmiş özelliklere sahiptir. İki sürümün yanı sıra günümüzde en çok kullanılan SNMPv3'de önceki sürümlerden farklı olarak güvenlik ve uzaktan yapılandırma özellikler bulunmaktadır.

3.8.2 Uzaktan Ağ İzleme (Remote Network Monitoring-RMON)

RMON, 1992 yılında IETF tarafından izleme ve protokol analizi için geliştirilen standart bir izleme protokolüdür. RMON ağ yönetimi için kapsamlı arıza teşhisi, planlama ve performans düzenlemesi sağlar. Cihazları uzaktan keşfederek veri toplamak ve bu verileri işlemek için tasarlanmıştır. Toplanan ham veriler, analiz araçları aracılığıyla yararlı bilgilere dönüştürülerek ağ yöneticilerinin ağlarını yönetmelerine ve ağ performansını

optimize etmelerine yardımcı olur.

Protokol iki ana unsurdan oluşur. Ağ Yönetim İstasyonu (Network Management Station-NMSs) ve RMON Probları. Bir RMON probu, belirli bir cihazdan ziyade, içinden geçen trafiğe göre ağın sağlığı hakkında bilgi toplar. Olağan dışı bir durumla karşılaştığında durumu ağ yönetim istasyonuna iletir. RMON desteğine sahip cihazlarda yönetim ve gözleme koşulları bir defa yerleştirildiğinde, ağ yönetim istasyonunun o cihazı sürekli yoklamasına (SNMP üzerinden) gerek kalmaz. Böylece ağ üzerinde fazladan trafik oluşmaz. RMON genellikle bir protokol olarak adlandırılır. Aslında ağ trafiğinde yaşanabilecek olası sorunların önlemlerini önceden alınması ve etkili yönetimi için destek sağlayan bir yönetim bilgi tabanı (MIB)'dır. SNMP'nin bir parçası olmuş ve onun için gelişmiş ağ yönetim yeteneklerine izin veren, nesneleri tanımlayan bir MIB modülüdür.

Ağ üzerinde SNMP mesajları yönetici ile ajanlar arasında iletilmektedir. SNMP'de LAN üzerinden giden her paketin arasına giren, açan ve analiz eden bir araç bulunmaktadır. Bu, işlemi yavaşlatan ve hedeflerine sürekli paket göndermeye devam eden bir cihazda uygulanacak bir çözüm değildir. Böyle bir durumda cihazdan gelen paketler yerine, ağın tamamı izlenerek keşfedilmesi gerekmektedir. Bu işlevi yerine getiren araca ağ izleme veya prob denir. Ağdaki iletim ortamına bağlı fiziksel bir nesne ve bu verileri analiz eden işlemci olmak üzere probun iki bileşeni bulunmaktadır. Her iki bileşen de coğrafi olarak aynı düzlemde ise prob, yerel olarak adlandırılır. Bileşenler fiziksel olarak ayrıysa, izlenen bilgiler yerel olarak toplanır, analiz için bir uzak ağ yönetim istasyonuna iletilir. Buna da uzak ağ izleme adı verilir.

RMON Protokolünün ağ yönetiminde sağladığı avantajlar şunlardır:

- Verileri lokal olarak izleyip, analiz ederek iletir. Bu sayede ağda daha az yük meydana gelir.
- NMS tarafından doğrudan görünürlük gerektirmez.
- Daha sık izlemeye izin vererek daha hızlı arıza teşhisi yapar.
- Yöneticiler için üretkenliği arttırır.
- Belirli bir süre boyunca performans parametrelerinin sürekli izlenmesine izin

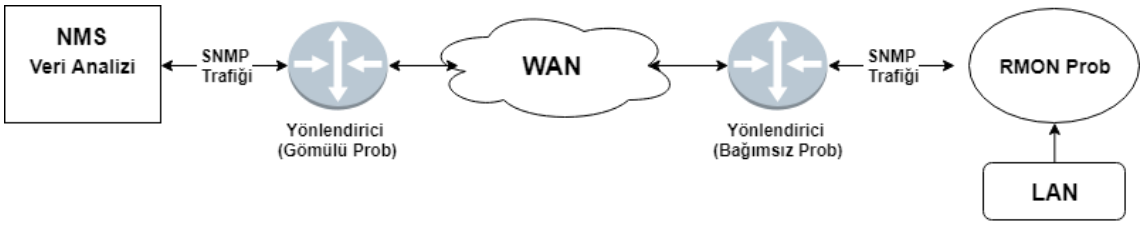
vererek, MIB yalnızca birikmiş anlamlı sonuçların saklanmasını sağlar.

- RMON, MIB verilerini toplayabilir ve tüm verileri ağ trafiğini azaltmaya yardımcı olacak şekilde ağ yönetim istasyonuna göndermeden kendisi yerel olarak analiz edebilir.

3.8.2.1 RMON Mimarisi

RMON, istemci/sunucu mimarisine dayanır. İstemci, kullanıcıya RMON bilgisi sunan ağ yönetim istasyonunda çalışan bir uygulamadır. Sunucu, bilgi toplamak için RMON prob olarak adlandırılan bir yazılım programı kullanan izleme cihazıdır. RMON probları, sunucudaki izleme sisteminin kilit unsurlarıdır. Aynı anda birden fazla istemci aynı probu kullanabilir.

Bağımsız ve gömülü prob olarak adlandırılan iki türü bulunmaktadır. Bağımsız problar taşınabilir ve bir donanım cihazında kendi içinde bulunurlar. Gömülü probları anahtarlar, yönlendiriciler ve ağ arabirim kartları gibi ağ cihazlarına yerleştirilebilir. Uzaktan erişim yöntemi ile LAN arabirimlerindeki etkinlikleri izleyebilir. RMON protokolü mimarisi, Şekil 3.8'de gösterilmektedir.



Şekil 3.8 RMON çalışma mimarisi.

3.8.2.2 RMON Sürümleri (RMON versions)

RMON'un 2 standart sürümü vardır: RMONv1 ve RMONv2'dir.

RMONv1: RMON'un çalışması için, yönlendirici ve anahtarlar gibi ağ cihazlarının destekleyecek şekilde tasarlanması gerekir. SNMP, ağ verilerini tek bir yönetim bilgi tabanı (MIB) türünden toplar. RMONv1 ise ağ kullanımı hakkında daha zengin bir veri kümesi sağlayan dokuz tane MIB tanımlar ve maksimum 10 tane MIB grubu

tanımlamaya izin verir. Ethernet ve token ring ağlarının Fiziksel ve Veri Bağlantısı katmanları (OSI Referans) izlenmesine olanak sağlar.

RMONv2: RMONv2'nin geliştirilmesinin en büyük nedeni, IP trafiği ve uygulama düzeyi trafiğini kontrol etmektir. RMONv1'den tek farkı tüm ağ katmanlarındaki (OSI Referans) paketleri izleyebilmesidir.

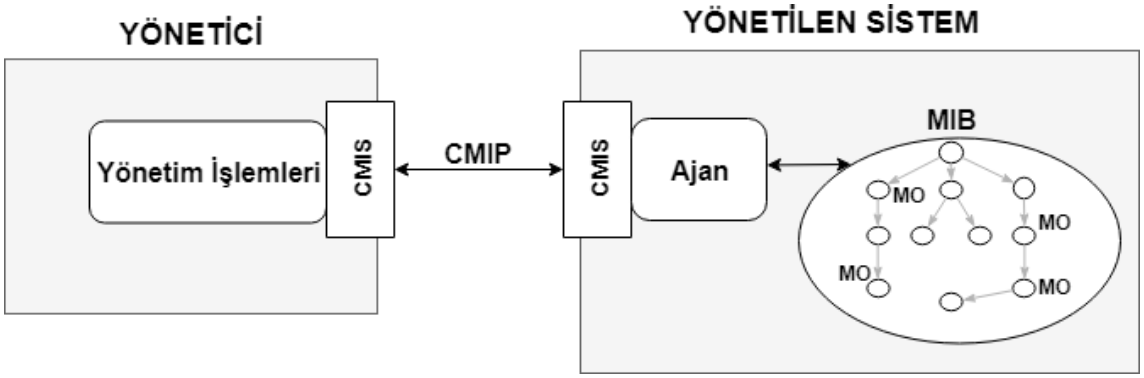
3.8.3 Ortak Yönetim Bilgi Protokolü (Common Management Information Protocol-CMIP)

CMIP, ISO tarafından geliştirilmiş, OSI tabanlı bir ağ yönetimi protokolüdür. CMIP protokolü SNMP'de bulunan yönetimsel eksiklikleri gidermek, daha ayrıntılı bir ağ yönetimi yapmak ve SNMP'nin yerini alması için hükümet ve şirketler tarafından finanse edilip geliştirilmiştir. (Ding 2010)

SNMP'ye göre yetenekleri daha gelişmiş bir protokoldür. Ancak bununla birlikte daha karmaşık bir yapıya sahiptir. Sistem kaynaklarını (işlemci, bellek, disk kapasitesi vs.) daha fazla tüketmesi ve yapılandırma ayarlarının uzman kişiler tarafından yapılabilmesi gibi nedenlerden dolayı kurumsal ağların yönetiminde fazla tercih edilmemektedir. Bunun yanı sıra CMIP telekomünikasyon alanında yaygın olarak kullanılmaktadır ve telekomünikasyon cihazları varsayılan olarak CMIP protokolünü desteklemektedir.

3.8.3.1 CMIP Mimarisi

CMIP protokolü mimarisi SNMP'ye göre biraz daha karmaşıktır. Şekil 3.9'da yönetilen bilgiye erişmek için CMIP kullanan ağ yönetim sistemi mimarisi gösterilmektedir. Yapının en önemli parçası ortak yönetim bilgi servisi (CMIS)'dir. CMIS, ağ yönetimi sistemi ve yönetim araçları arasında iletişime izin veren bir hizmettir. CMIP tarafından uygulanan servis arayüzünü tanımlar. CMIP aracı veri tabanı olarak bir yönetim bilgi ağacı (MIT) tutar. Bu veri tabanında bulunan yönetilen nesneleri (MO) kullanarak platformları ve aygıtları (LAN, Port vb.) modeller. Ajan aracılığıyla bu yönetilen nesneleri (MO) değiştirir, oluşturur, alır veya siler.



Şekil 3.9 CMIP çalışma mimarisi.

3.9 Ticari Pazarda Yer alan Ağ Yönetim Sistemi Ürünleri

Ağ ve sunucu sistemlerinin gelişmesi, farklı ağ türlerinin ortaya çıkması ve bu ağ ortamlarının bir birleri ile birleşmesi, çeşitli yönetim zorluklarını da beraberinde getirmiştir. Ağ yöneticileri, insan çabalarını desteklemek, ağ elemanlarının durumu ve davranışları hakkında bilgi toplamak için bu işlemleri otomatik olarak yapabilecek araçlara ihtiyaç duymuştur. Ticari pazarda birçok üretici ağ planlaması, güvenlik kontrolü, döküm yönetimi ve trafik izleme gibi çeşitli yönetim faaliyetlerini destekleyen ağ yönetim sistemi çözümü geliştirmektedir.

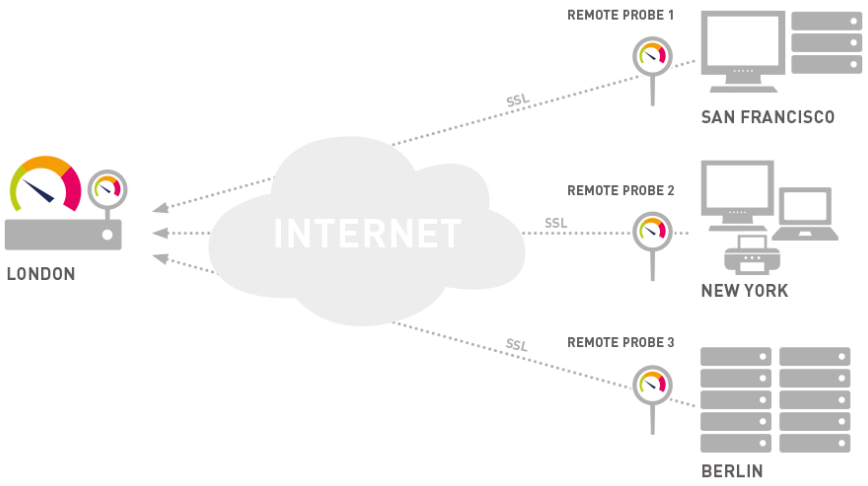
Bu ürünlerin büyük bir bölümü ticari amaç izlediği için kullanımları da belirli bir ücret karşılığı olmaktadır. Bunun aksine kullanımı ücretsiz olan ürünler de mevcuttur. Kurumsal bir geniş ağı yönetebilmek için bu çözümleri üretebilecek bir yazılım altyapısı yoksa ağ yönetim sistemi satın almak veya ücretsiz ürünleri temin etmek gerekmektedir. Ağ yönetim sistemi seçiminde en önemli faktör, kullanılması düşünülen ürünün ihtiyaçları karşılayabilecek yeteneğe sahip olmasıdır. Örneğin, söz konusu ihtiyaç; ağı sadece izlemek ve ağdaki cihazların işlemci, bellek ve depolama kapasitesi gibi bilgileri toplamak ise bu konularda öne çıkan bir ürünü tercih etmek maddi açıdan daha isabetli olacaktır.

Birçok çözümü içinde barındıran ve farklı alanlarda ihtiyaçları karşılayabilecek ağ yönetim sistemlerinden bazıları aşağıda incelenerek, karşılaştırmaları yapılmıştır.

3.9.1 Paessler PRTG Ağ İzleme Yazılımı

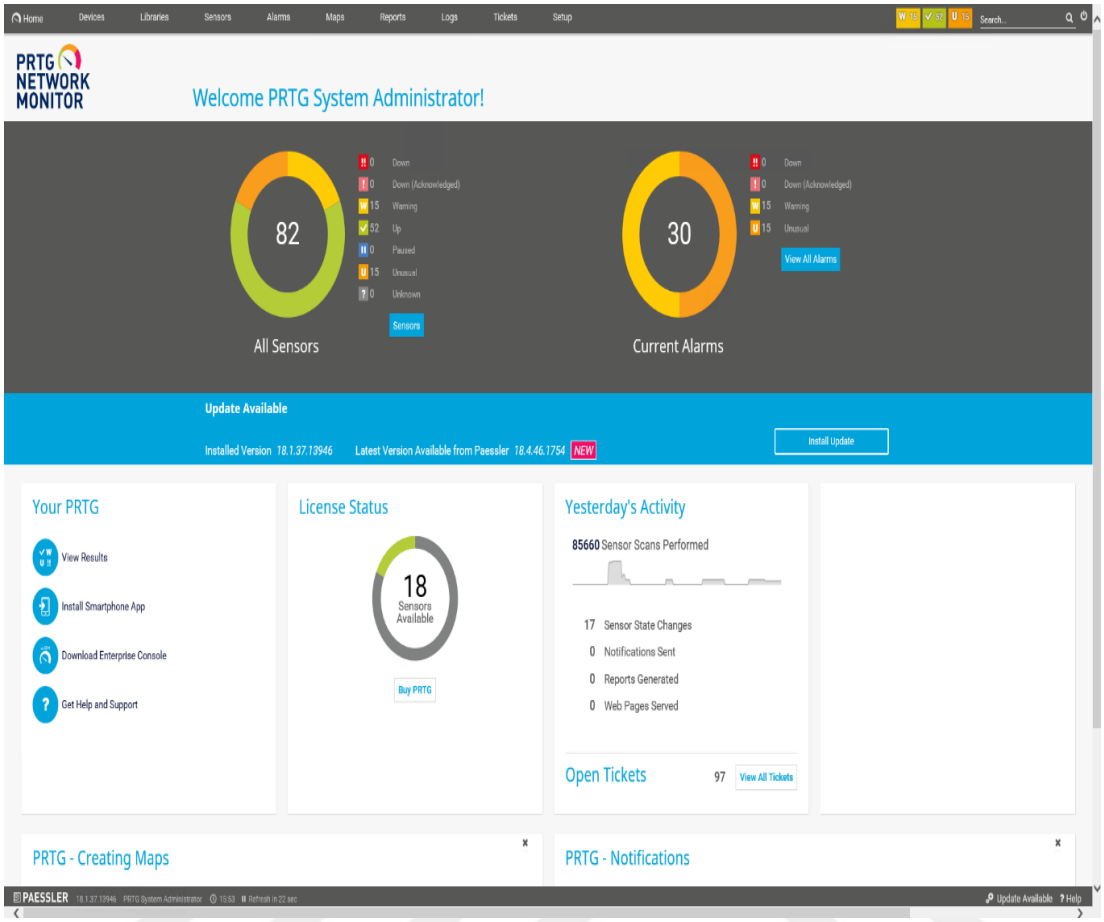
PRTG ürünü Paessler firmasının ağ yönetim sistemidir. Ağ izleme konusunda oldukça başarılı olan ve şirketler tarafından çok tercih edilen bir yazılımdır. Tüm bilgi teknolojileri altyapısının düzgün ve kararlı çalışmasını sağlayarak ağın performansını analiz edebilmesine yardımcı olmaktadır. Altyapı olarak RMON protokolünde bulunan Prob yapısını kullanmaktadır. Çok sayıda izlenecek sistem veya şekil 3.10'daki gibi farklı lokasyonlarda dağınık bir yapı varsa Prob kurulumu yapılabilmektedir. Probun görevi, üzerinde tanımlanan sistemlerden (Sunucu, anahtar, yönlendirici vb.) sensörlere (cpu değeri, bellek kapasitesi, bant genişliği vb.) göre verileri toplayıp uygun şekilde derledikten sonra yönetim yazılımına göndermektir. Bu sayede izleme yükünü dağıtılarak, sistemin kaynakları verimli bir şekilde kullanılmaktadır.

PRTG bir ağ yönetim sisteminden ziyade ağ izleme çözümü sunmaktadır. Ağ da yaşanan hatalara ve olası yapılandırma sorunlarına karşı bir aksiyon almaması ürünün en önemli eksiğidir. Örneğin aynı marka-model anahtar cihazlarının toplu olarak yapılandırılması mümkün değildir.



Şekil 3.10 Uzak konumları izleme ve prob yapısı (İnt. Kyn. 11).

PRTG her hangi bir fiziksel ya da sanal sunucuya kurularak, web tabanlı bir arayüze sahip uygulama olarak kullanılabilmektedir. Kurulum yapıldıktan sonra Resim 3.1'de görüldüğü gibi şirketin geniş alan ağındaki tüm ağ cihazların ve sunucuların aktiviteleri, oluşturdukları alarmlar ve risklerin özeti tek ekrandan görüntülenebilmektedir.

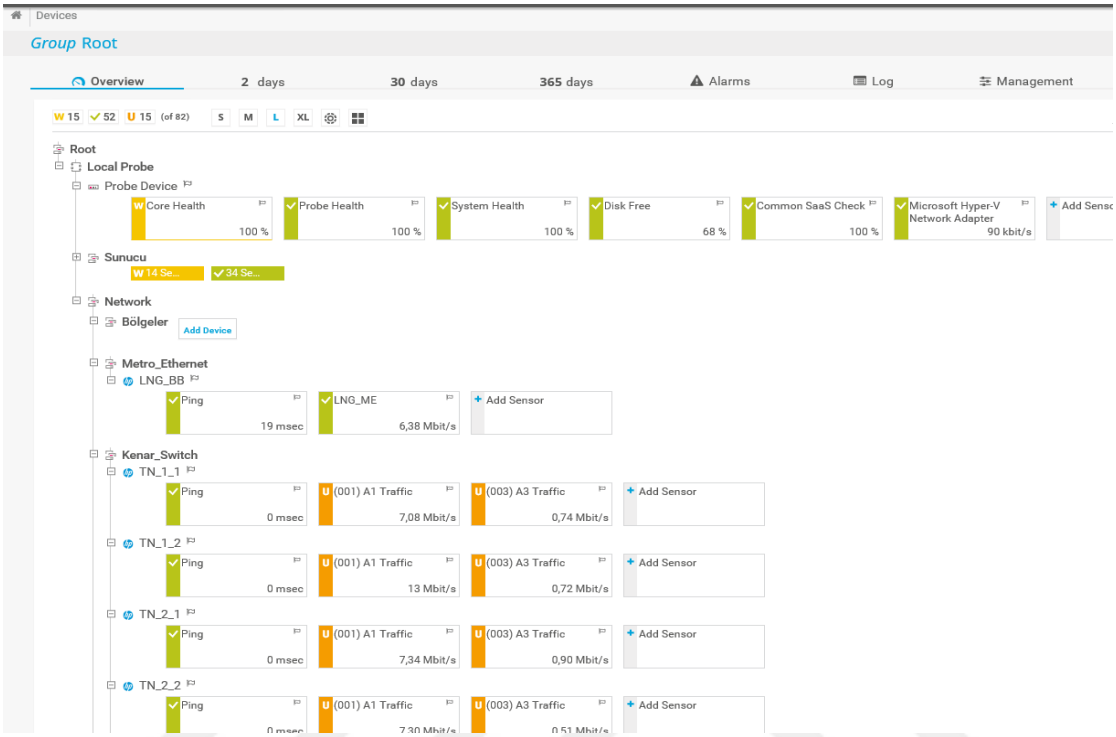


Resim 3.1 Kontrol paneli ekranı.

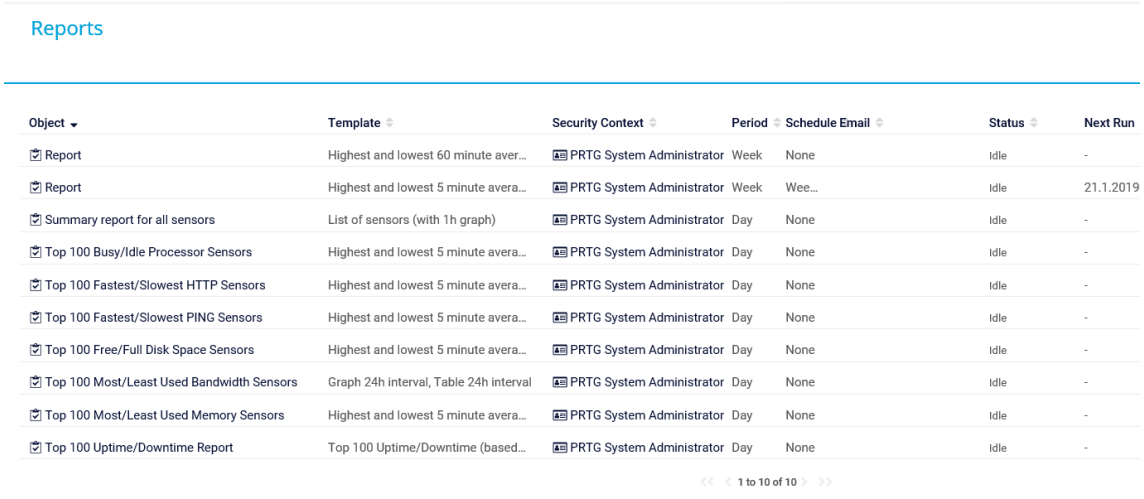
Cihazlar, tek tek veya toplu şekilde NMS'e tanıtılıp, takibi yapılmak istenen sensörler eklenebilmektedir (Resim 3.2). Cihazları tanıtırken önde gelen üretici firmaları (Cisco, Vmware, Microsoft, Hp, Oracle vb.) için hazır eklentiler kullanılabileceği gibi, standart dışı cihazlar için özel yapılandırma seçeneklerinin tanınması ağ yöneticilerinin işini oldukça kolaylaştırmaktadır.

Büyük ve dağıtık bir BT altyapısını yöneten ağ yöneticileri için en önemli husus istenilen ölçeklerde, ön görülen zaman aralıklarında ve istenilen biçimde sistemlerin raporlanabilmesidir. PRTG de raporlar, takibi yapılan ağ cihazlarının ve sunucuların sensörlerini temel alarak (işlemci değeri, bant genişliği değeri vb.), çeşitli gruplama kombinasyonlarından seçim yaparak (ilk 100, en çok hata veren 10 cihaz vb.), sunulan veri formatında (pdf, cvs, xml) ve belirtilen zaman aralıklarında alınabilmektedir. Alınan raporlar yöneticiye e-mail, syslog, sms veya yazılan script aracılığıyla günlük, haftalık

veya istenilen süre aralıklarında gönderilebilmektedir. Bu raporlar sayesinde ağ yöneticisi, geçmişe dönük tüm olaylara ulaşabilmektedir (Resim 3.3).



Resim 3.2 Yönetilen cihazlar ve bilgisi çekilen sensörler.

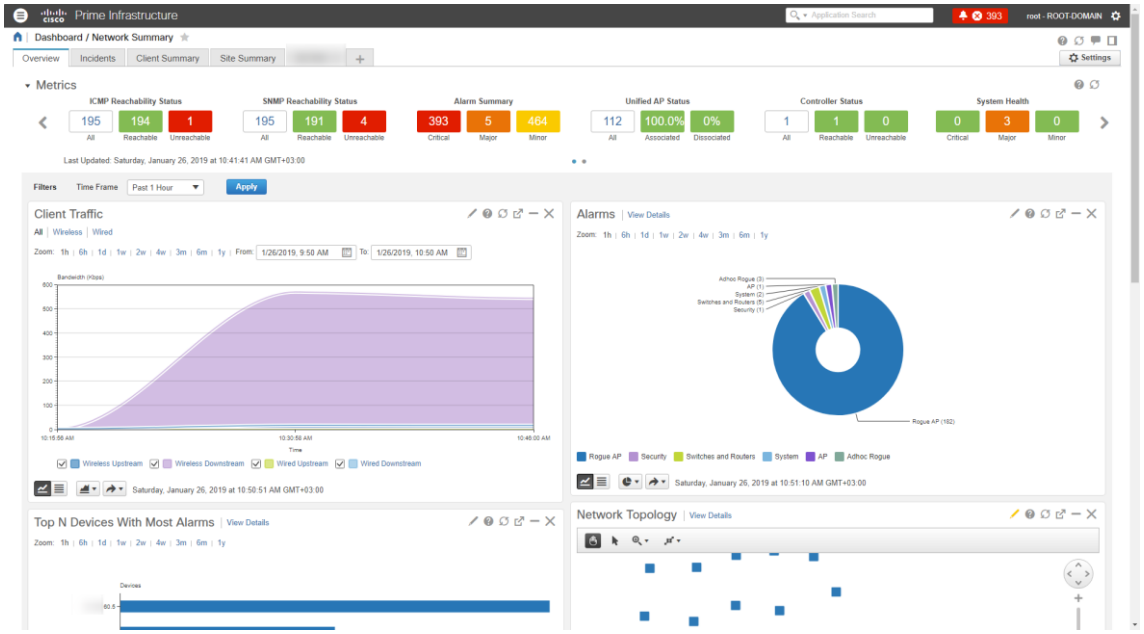


Resim 3.3 Şablonu oluşturulmuş raporların listesi.

3.9.2 Cisco Prime Ağ Bileşenleri Yönetim Yazılımı

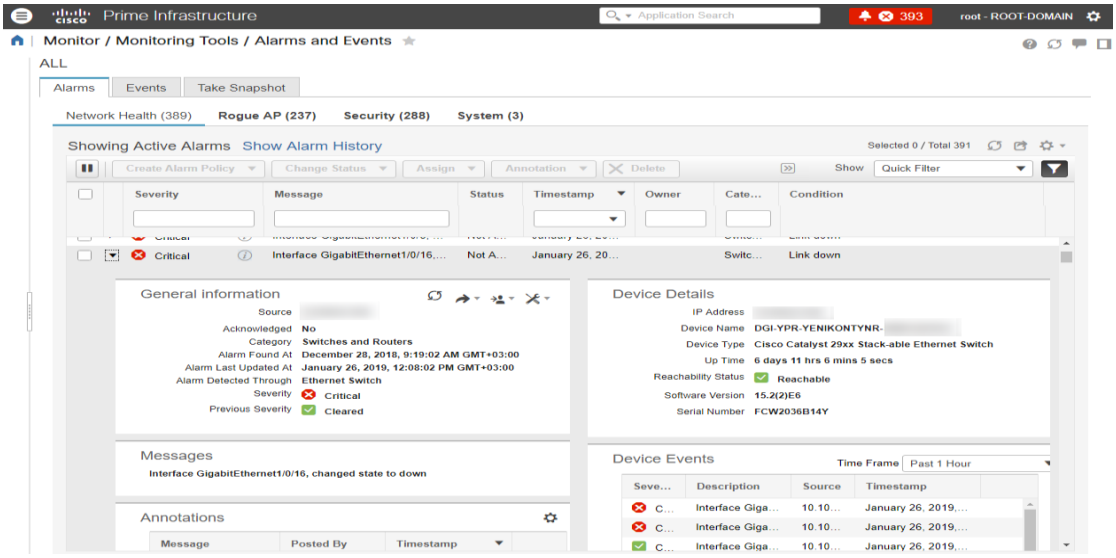
Prime, ağ cihazları ve standartlarının en büyük geliştiricilerinden olan Cisco firmasının üretmiş olduğu ağ yönetim sistemidir. Ağ altyapısı üzerinde bulunan kablolu ve kablosuz cihazların durumu hakkında istatistiksel ve grafiksel detay veren, toplu yapılandırma işlemlerini yapmayı sağlayan ve ağ cihazlarından son kullanıcıya kadar geniş bilgiler sunan bir ağ yönetim çözümüdür. Ürünün ana hedef kitlesi cisco ürün ailesinde bulunan anahtar, yönlendirici, kablosuz denetleyici gibi ağ cihazlarının yönetimini sağlamaktır. Bu yönetimi yaparken diğer üreticilerin ağ yönetim sistemlerinden farklı olarak Cisco'nun kendi cihazlarında kullandığı protokolleri kullanmasıdır. Cisco Prime ağ altyapısında bulunan cihaz miktarına göre lisanslama yapılarak dağıtımı ücretli bir ağ yönetim sistemidir. Donanım olarak satın alınıp herhangi bir kurulum yapmadan ya da bir sunucu üzerine yazılım kurularak, web tabanlı arayüz üzerinden kullanılabilmektedir.

NMS cihazlardan gelen alarmların özeti, en çok işlemci kullanımı, son kullanıcı trafiği gibi kritik öneme sahip verilerin saatlik değişkenlerinin incelenmesine olanak tanımakla birlikte ağ yöneticisinin amacına ve önceliğine göre bu verilerin hangilerinin gösterileceği seçilebilmektedir (Resim 3.4).



Resim 3.4 Ağda yaşanan olayları izlenildiği kontrol ekranı.

Ağdaki kablolu ve kablosuz cihazların durumlarına, aktif son kullanıcı bilgilerine, oluşan hatalar ile olay kayıtlarına ulaşım sağlanabilmektedir. Cihazlar da veya ağ da yaşanan alarmın neden kaynaklandığını, olayın gerçekleştiği zamanı ve geçmiş yaşanan olaylar detaylı bir şekilde görüntülenebilmektedir (Resim 3.5). Ayrıca anlık gelen veriler üzerinden takibi yapılmakta olan cihazın, kaynak kullanım verilerine, takılı olduğu arayüz bilgilerine, üzerine tanımlanmış ayarlara ve kendisine erişim sağlayan kullanıcı bilgilerine grafiksel olarak bakılabilmektedir.

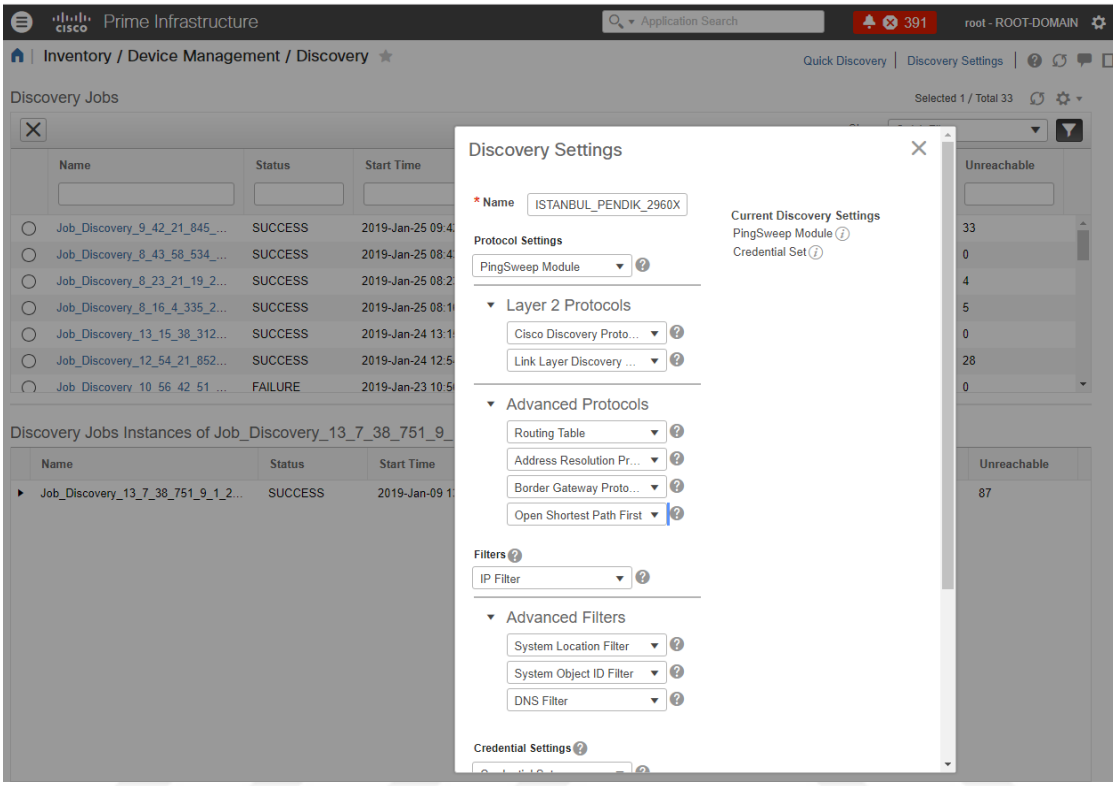


Resim 3.5 Alarm detayları inceleme ekranı.

NMS önceliklere göre alarm kuralları oluşturulabilmektedir. Önemsiz olduğu düşünülen olaylar engellenebileceği gibi cihazlarda, port arayüzlerinde veya hatlarda yaşanabilecek olası hatalara yönelik kurallar yazılarak, problem meydana geldiği anda yapılması gerekli eylemler otomatik sisteme yaptırılabilmektedir. Ağda yaşanacak en ufak gecikme maddi zararlara neden olacağından bu özellik ağ yöneticilerine zaman ve hız kazandırmaktadır.

Ağdaki cihazları NMS'e tanıtmanın birden fazla yolu bulunmaktadır. Diğer ağ yönetim yazılımlarının hepsinde olduğu gibi SNMP, TELNET(Telecommunication Network), SSH (Secure Shell), ICMP gibi ağı keşfetmemize yarayan protokoller aracılığıyla cihazlar eklenebilmektedir. Ancak Cisco Prime'ı diğer ağ yönetim sistemlerinden ayıran özelliği Resim 3.6'da görüldüğü gibi OSI katman 2 (lldp, cdp) ve OSI katman 3 (eigrp,

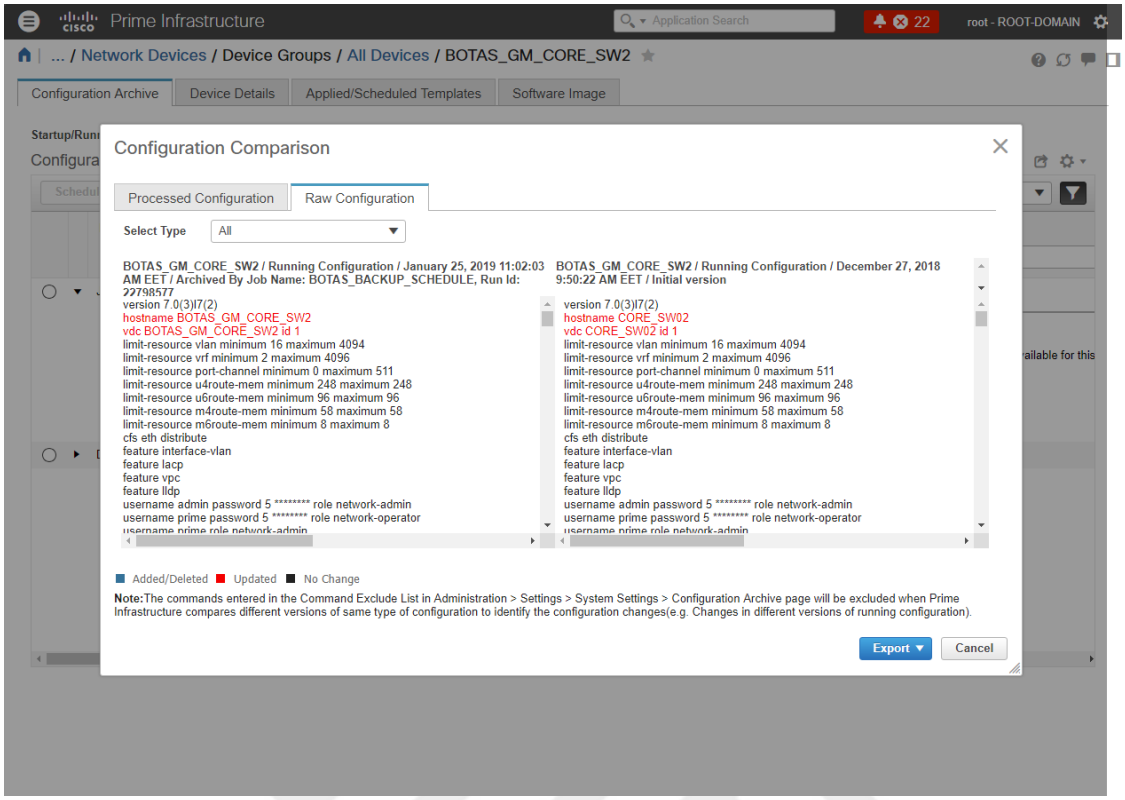
ospf, arp) seviyesindeki protokoller aracılığıyla daha detaylı bir keşif ve cihaz yönetimi yapılabilmesidir.



Resim 3.6 Cihaz ekleme ve keşfetme yöntemlerinin seçimi.

Cisco Prime'ın bir diğer önemli özelliği cihazlara toplu yapılandırma yükleme, yapılandırma yedeği alma ve yapılandırmalar arası kontrol sağlaması yapabilmesidir (Resim 3.7). Bu sayede iki ayar arasında yapılan değişiklikler kontrol edilebilmekte ve cihazların düzenli yapılandırma yedeği alınmaktadır. Cihazlarda olası yapılandırma silinmelerinde veya yanlış yapılandırma çalışmalarından sonra hızlı bir şekilde eski yapılandırma ayarları alınan yedekten getirilebilmektedir.

NMS'in takibi ve ağda yaşanan olayların geçmişe dönük incelenmesi için istenen cihaz, port arayüzü veya hattın bilgileri girilerek rapor alınabilmektedir. Ayrıca ihtiyaçlara uygun rapor şablonları oluşturularak, raporların belli tarih aralıklarında tekrar tekrar alınmasına olanak sağlamaktadır.



Resim 3.7 Farklı günlerde yüklenmiş olan yapılandırmalar da yapılan değişikliklerin görüntüsü.

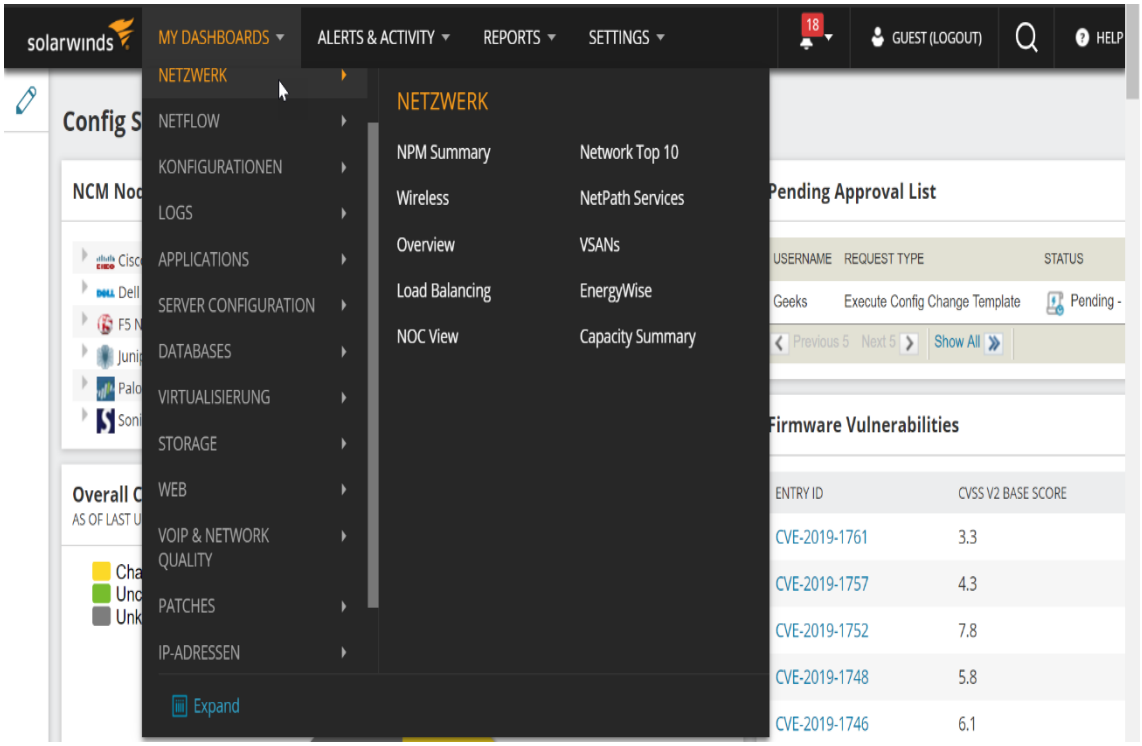
Prime, Cisco'nun kendi geliştirmiş olduğu anahtar, yönlendirici, kablosuz denetleyici ve kablosuz erişim noktaları gibi donanımların yönetiminde oldukça başarılı olan ve birçok işi kendisi yaparak hataların çözümünde ağ yöneticilerine zaman kazandıran başarılı bir ağ yönetim sistemidir. Ancak diğer üreticilere ait cihazların ve sunucu sistemlerinin yönetiminde bu başarısını sürdürememesi, özellikle Cisco dışı cihazlarda izlenecek olan işlemci, ısı, bellek gibi sensörlerin kısıtlı olması yazılımın en önemli eksikliğidir.

3.9.3 Solarwinds Ağ Yönetim Sistemi

Solarwinds ağ, sistem, güvenlik, veritabanı, son kullanıcı ve bulut altyapılarının yönetimi için geliştirilmiş otuza yakın çözümü içerisinde barındıran ağ yönetim sistemidir. Modüler yapısı sayesinde BT yöneticilerine çok yönlü bir yönetim imkânı sunması, sistemlerin yönetiminde ciddi ölçüde kolaylık sağlamaktadır.

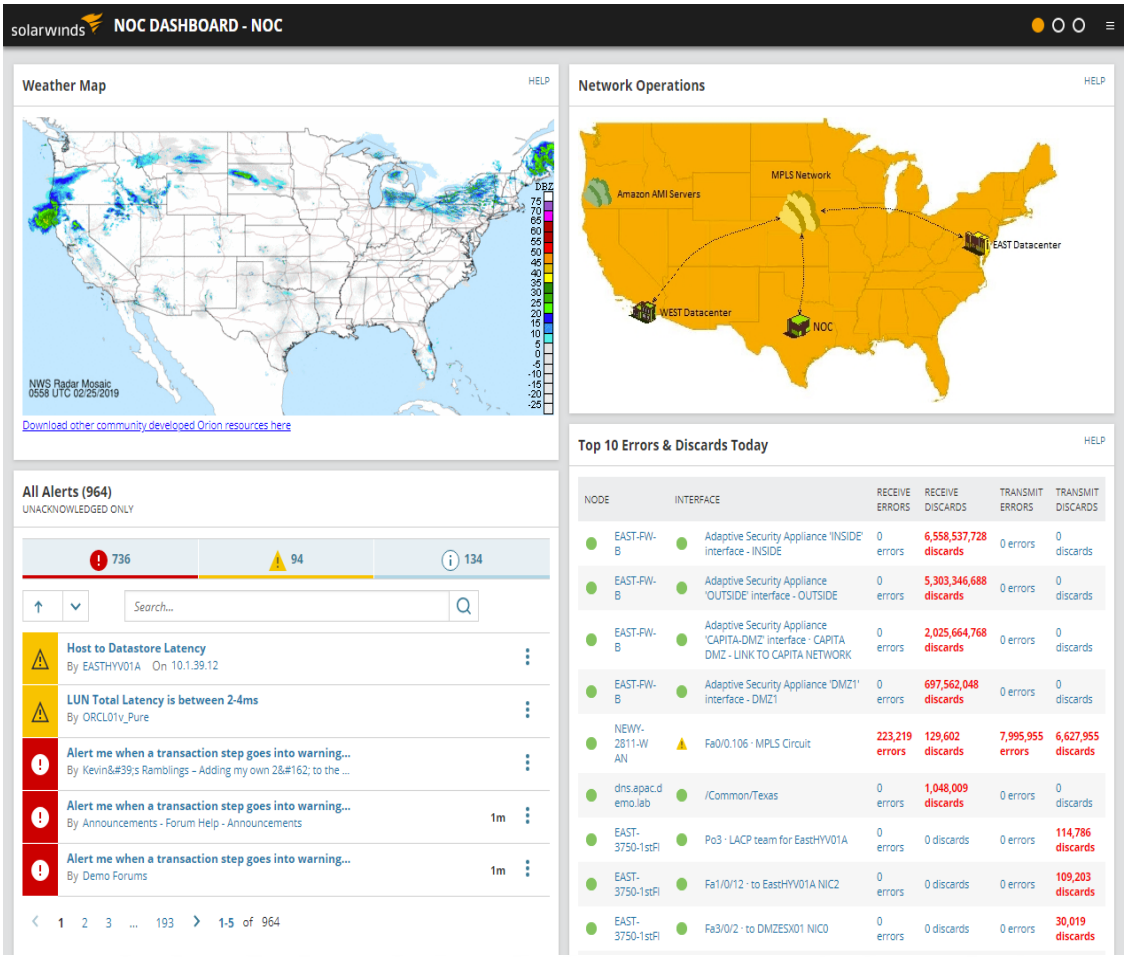
Kullanılacak olan tüm modüllere web ortamında tek bir arayüz içerisinden erişilebilmektedir. Her bir modül için ayrı arayüz hazırlanması yerine ürünün tek bir

ekran üzerinden kullanılabilmesi yöneticilere basitlik sağlamaktadır. Bu basit yapı, tüm yönetim modüllerini gruplayarak, Solarwinds Orion platformu üzerinde birleştirilmesiyle hazırlanmıştır (Resim 3.8). Sisteme farklı yetkilere sahip kullanıcılar tanımlanarak, farklı modüllerde yönetim imkânına sahip gruplar oluşturulabilmektedir. Bu özellik daha sonra alarm yönlendirmede ve iş paylaşımında kolaylık sağlamaktadır.



Resim 3.8 Solarwinds Orion platformu içerisinde bulunan yönetim modülleri.

NMS'de kontrol paneli zengin ve özel içerikler barındırmaktadır. Her bir modül için özel kontrol paneli sayfası oluşturulabilmektedir. Ağ cihazları, sunucular, kullanıcılar için ayrı kontrol sayfaları hazırlanıp, ağ işlem merkezi (Network Operation Center-NOC) görünümüyle istenen kontrol sayfaları, belirlenen aralıklarda ekranda otomatik olarak döndürülebilmektedir (Resim 3.9). Kriz yönetim odalarında bu şekilde otomatik değişen ekranların olması sistemin takibini kolaylaştırmaktadır.

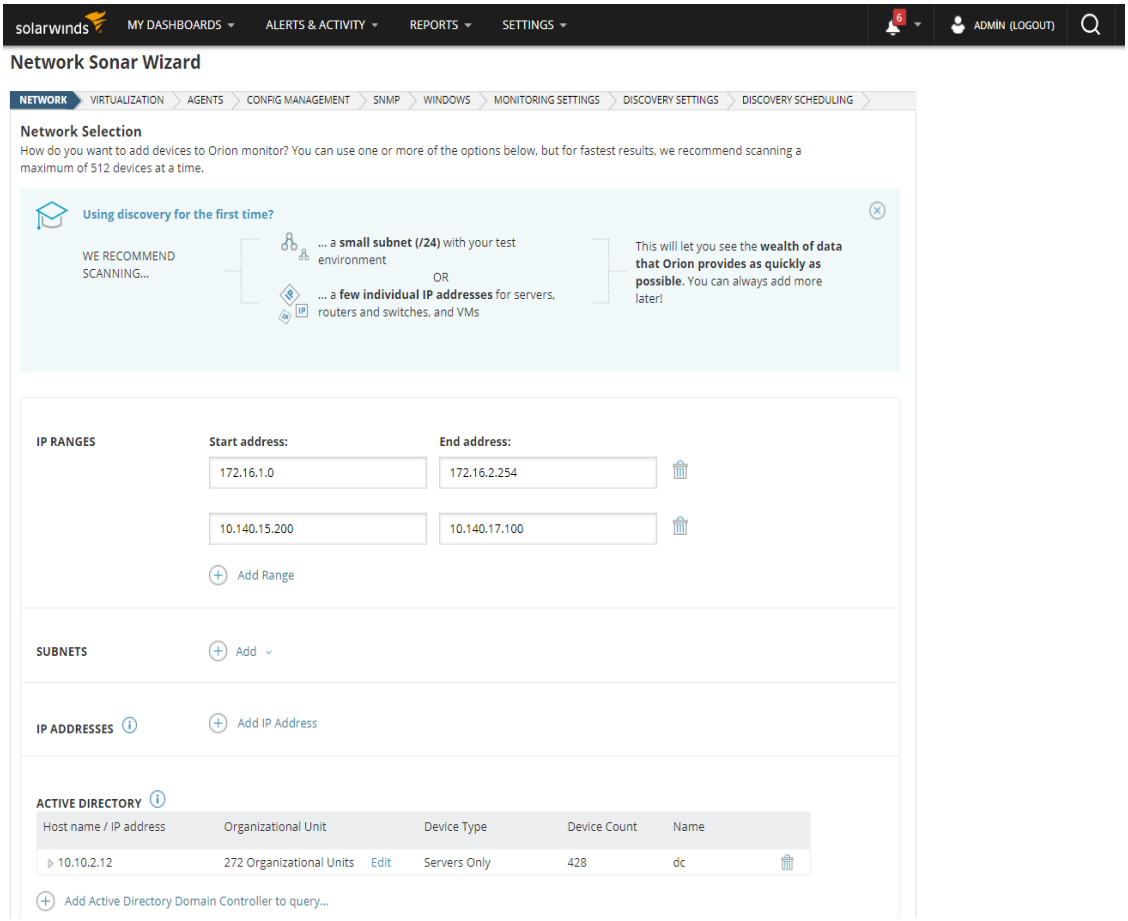


Resim 3.9 NOC modu kontrol panelinin görüntüsü.

Sisteme yeni bir cihaz ekleme veya toplu şekilde keşif yaptırmak mümkündür. Sonar adı verilen araç sayesinde markadan bağımsız, tüm ağ ve sitem dökümü tanıtılabilmektedir. Resim 3.10'da görüldüğü gibi sisteme, tüm cihazlar tek tek yapılandırmaya gerek duyulmadan, aynı özelliklere sahip cihazlar IP aralığı, kimlik bilgisi (SNMP, SSH, LDAP) ve isteğe bağlı ajan belirtilerek eklenebilir. Girilen bu bilgiler veritabanında tutularak istenilen aralıklarda sürekli döküm taraması yapılabilmektedir.

Sonar aracı, döküm taraması sırasında cihazın ağ cihazı mı yoksa bir sunucu mu olduğunun tespitini kendisi yaptıktan sonra, ağ cihazı ise; güvenlik duvarı, yük dengeleme cihazı, saldırı tespit sistemi (IDS) gibi güvenlik cihazları ile anahtar, yönlendirici, kablosuz erişim noktası gibi ağ altyapı cihazlarını otomatik olarak algılayabilmektedir. Bu cihaz bir sunucu ise; hangi işletim sistemine (windows, linux) sahip olduğu, üzerinde yüklü olan servisin (IIS, Exchange, Sql, Backup) ne işe yaradığı bilgisini yine otomatik olarak algılayabilmektedir. Bu özellik yöneticilerin iş yükünün

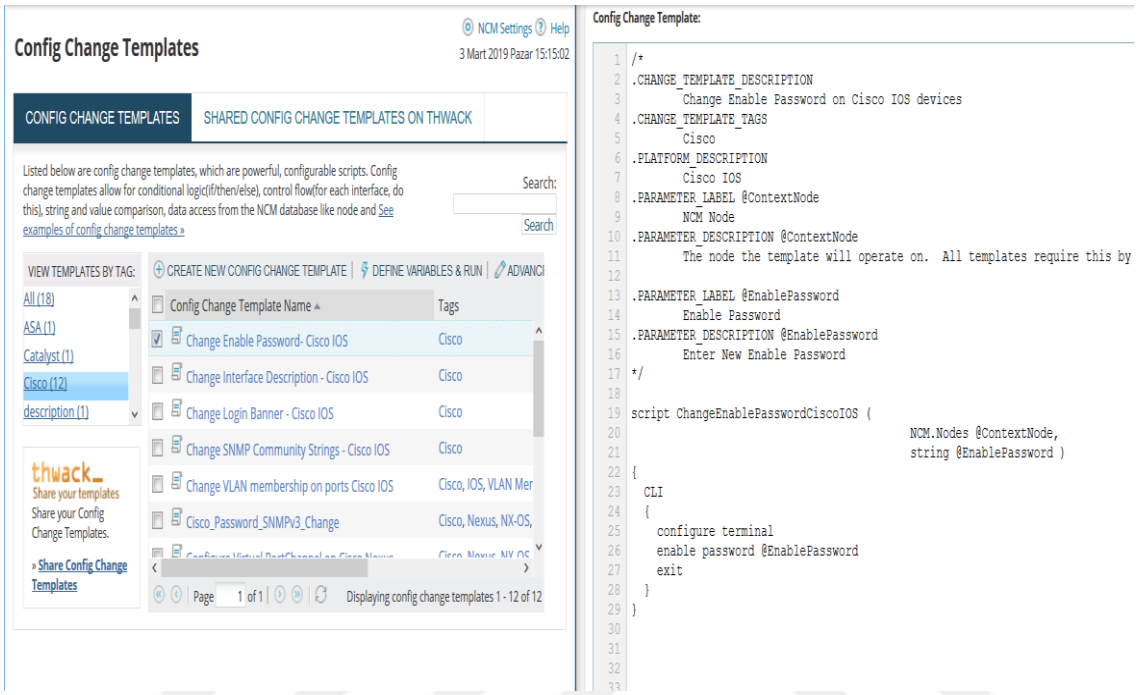
azalmasını sağlayarak ağ yönetim sisteminin daha efektif şekilde kullanımına yardımcı olmaktadır.



Resim 3.10 Sonar cihaz ekleme ekranı.

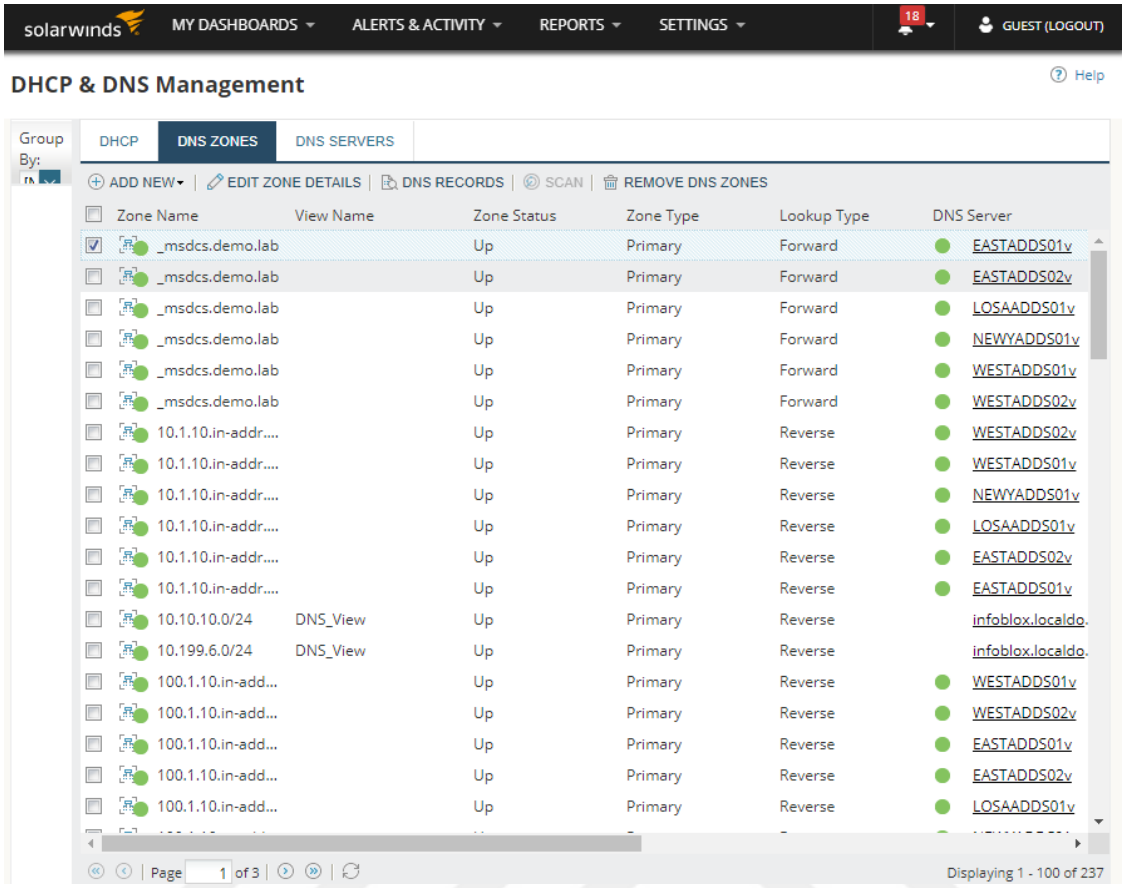
Cihazların yapılandırma ayarlarının yedekleri istenen aralık ve saatte alınıp, aksi bir durum olması halinde geri yüklenebilmektedir. Solarwinds'in geliştirmiş olduğu önemli bir özellik ise yapılandırma ayarı şablonlarıdır. Ağ yöneticilerin cihaz yapılandırma ayarı yaparken zorlandıkları yerlerde yardım alabilecekleri bir özelliktir. Resim 3.11'de görüldüğü gibi NMS tarafından sunulan varsayılan şablonlar kullanılabileceği gibi yöneticiler kendi ihtiyaçlarına göre özel yapılandırma şablonları da hazırlayabilmektedir. Ayrıca Thwack adı verilen topluluk veri tabanından farklı üreticilerin ürünlerine ait yüzlerce yapılandırma ayarlarına erişilip, yerel NMS'e yüklenebilmektedir. Yapılandırma ayarları aynı olan ağ cihazlarına temel bir yapılandırma şablonu hazırlanarak, tüm cihazlarda gerçek zamanlı ayar kontrolü de yaptırılabilmektedir. Yöneticilerden habersiz yapılan yapılandırma ayarlarının önüne geçen bu özellik

sayesinde, cihazların mevcut ayarları otomatik yüklenebilmektedir. NMS tüm bu özellikleri sayesinde hatalı işlemlerin önüne geçerek, başarılı bir yapılandırma yönetimi sağlamaktadır.



Resim 3.11 Yapılandırma ayarı şablonları uygulama ekranı.

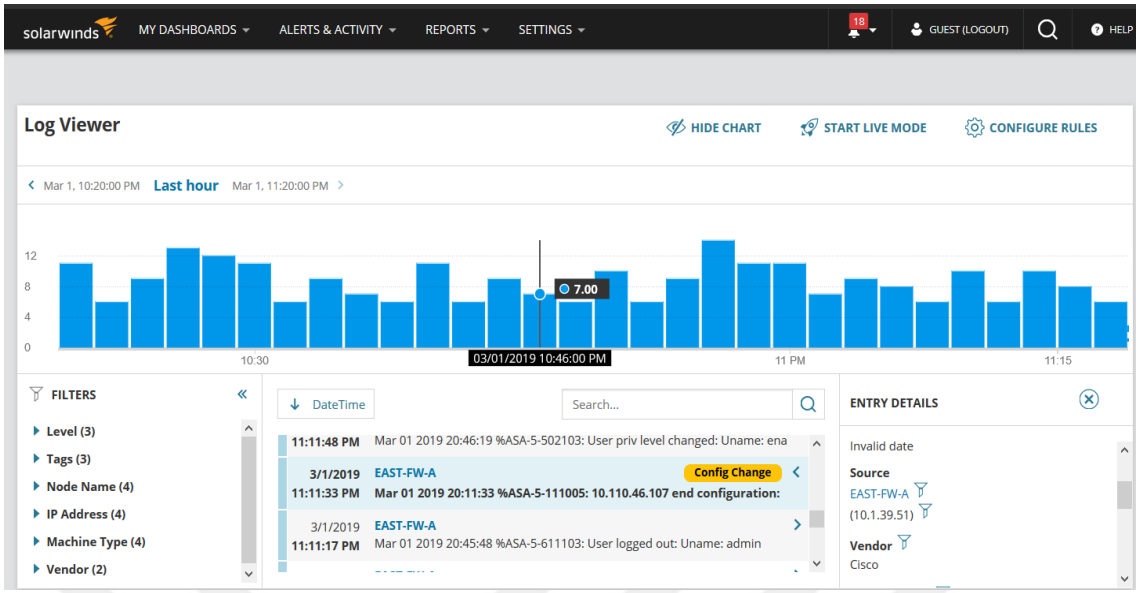
Solarwinds ağ cihazları ve sunucu yönetimi dışında, son kullanıcı ve IP adresi yönetimi çözümleri de sunmaktadır. Bu modülün içerisinde; alt ağ, DHCP ve DNS (Domain Name System) sunucusu yönetimi yapılabilmektedir. Ağdaki IP yoğunluğunun, DNS trafiğinin ve DHCP alanlarının kapasitesinin takibi yapılabilmektedir. DNS sunucularında bulunan bölgelerin (Zones) anlık takibi gerçekleştirilmektedir. Bölgenin hangi DNS sunucunda tanımlı olduğu, en son yapılan sorgu bilgisi, bölgelerin çalışabilirlik durumu ve güncelleme seçenekleri gibi özellikler kontrol edilebilmektedir (Resim 3.12). DHCP sunucularından alınan bilgilerle son kullanıcıların almış oldukları IP adresi ve kullandıkları anahtar cihazı bilgilerine hızlı bir şekilde ulaşılabilmektedir.



Resim 3.12 DHCP, DNS sunucusu yönetimi ekranı.

Diğer bir modül ise yönlendiriciler üzerinden geçen trafiğin bant genişliğinin kontrolünü sağlayan Netflow arayüzüdür. Bu özellik sayesinde yönlendiriciden geçen kaynak ve hedef bilgilerini yönetici görüntüleyebilmektedir. Hattı kullanan uygulama (internet, mail, ftp vb.), bant genişliğini tüketen kaynak cihaz ve saatlik hat trafiği bilgisi gibi detaylar görüntülenebilmektedir.

Ağ cihazları ve sunuculardan gelen syslog mesajlarına ve ağ yönetim protokolünün (SNMP) erişim sağladığı yönetim bilgi tabanındaki (MIB) nesnenin detayına ulaşılabilmektedir. Bu özellik sayesinde ağ cihazlarının komut satırı arayüzü (Command Line Interface-CLI)'nde yazılan komutlardan, mevcut yapılandırma ayarı üzerinde sonradan yapılan değişikliklerden ve kontrol edilen nesnenin yönetim bilgi tabanında bulunan değerine kadar birçok bilgi kaydedilip istenildiğinde ulaşılabilmektedir (Resim 3.13).



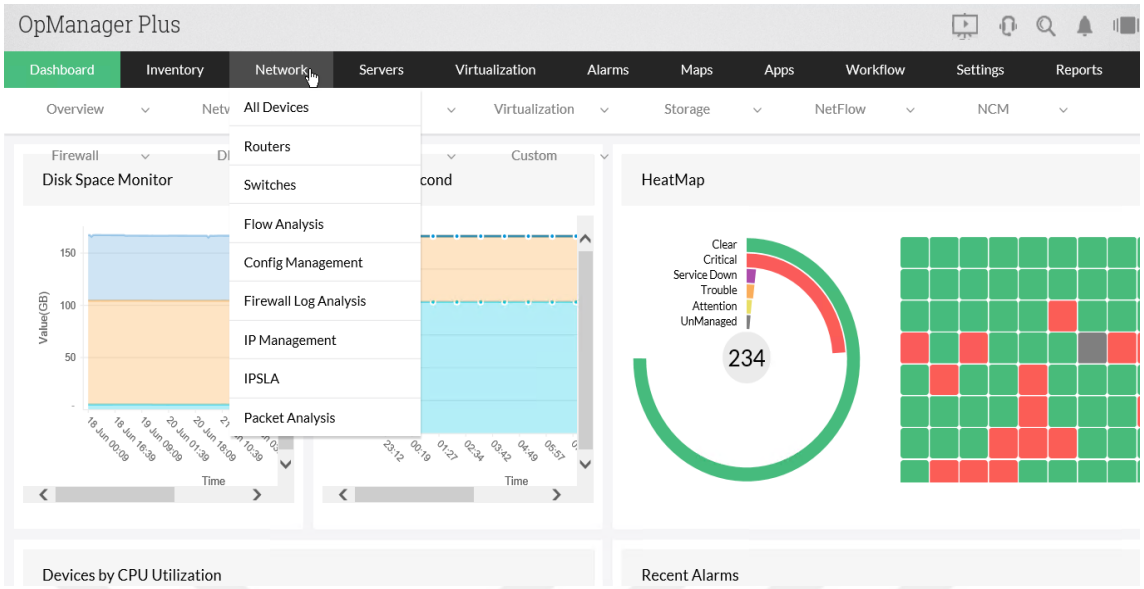
Resim 3.13 Cihazlardan gelen log kayıt geçmişi takip ekranı.

Solarwinds birçok yönetimsel özelliği içermesi ve bunu tek bir ara yüz üzerinden sunması diğer anlatılan NMS ürünlerine göre kendisini öne çıkarmaktadır. Ancak bu kadar çok yönetimsel aracı içerisinde barındırması nedeniyle maliyet ve kullanım açısından daha fazla yük getiren bir üründür.

3.9.4 Manageengine Opmanager Ağ Yönetim Sistemi

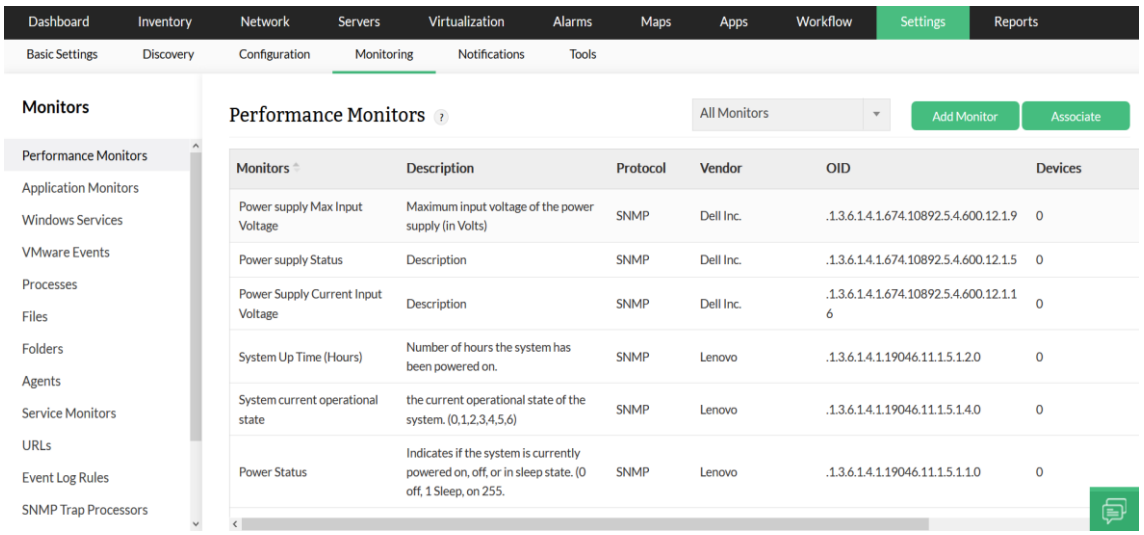
Manageengine firması da Solarwinds gibi BT altyapısını yönetmek için çok yönlü çözümler geliştiren bir üreticidir. Yardım masası ve envanter, active directory araçları, masaüstü ve mobil cihaz ,log analizi ve güvenlik, ağ,sunucu ve uygulama yönetimi olmak üzere birçok yönetimsel faaliyetlere çözümler üretmektedir.

Manageengine Opmanager ürünü geniş alan ağındaki ağ, sunucu ve uygulama performansı izleme ve yönetimi için geliştirilen ağ yönetim sistemidir. Resim 3.14'de görüldüğü gibi NMS modüler yapıya sahip bir arayüze sahip olup, yönetimsel araçların hepsine tek menüden ulaşılabilmektedir. Menüler arasındaki bağlantı ve arayüz incelenen diğer NMS ürünlerine göre daha kullanışlı bir tasarıma sahiptir. Kontrol ekranı düzenlenmesi, kullanıcı yetkilendirme, otomatik döküm taraması, alarm yönetimi ve yapılandırma yönetimi yapmaya imkan veren araçlar bulunmaktadır.



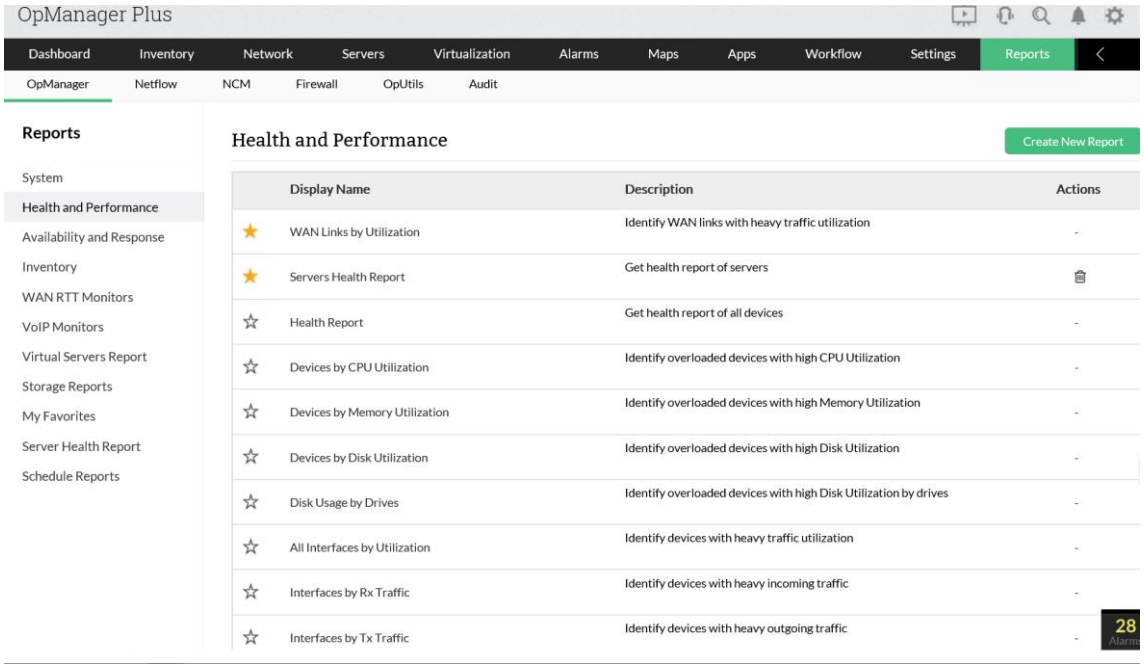
Resim 3.14 Manageengine Opmanager araç menüleri (üstte) ve kontrol ekranı.

Bu araçların dışında özellikle sunucu ve uygulama yönetimi için geliştirilmiş sanallaştırma, depolama, veritabanı, güvenlik duvarı ve iletişim hatları trafiği yönetimi araçlarını da kullanıma sunarak etkili bir BT altyapısı yönetimi yapılmasına imkân sağlamıştır. SNMP, WMI, CLI ve UCS gibi birçok protokol ile piyasada bulunan Cisco, Huawei, Citrix ve Alcatel gibi üreticilere özel nesneler kullanılarak ağ izleme (monitor) yapılabilmektedir (Resim 3.15). Ağı izleme özelliği piyasada kullanılan NMS ürünlerine göre daha geniş ürün desteği sağlamasıyla Manegeengine'i bu alanda öne çıkarmıştır.



Resim 3.15 Ağ izleme özelliği yönetim ekranı.

NMS bu kadar iyi bir ağ izleme yapabilirken, elde edilen performans verilerinin toplu görünebileceği rapor şablonu oluşturulmaması, bir eksikliğe neden olmaktadır. Resim 3.16'da görülen ekran görüntüsündeki gibi, sistem tarafından hazır sunulmuş şablonlar üzerinden performans, sistem, döküm raporları almak mümkündür. Son olarak yönetilen cihazların bulunduğu konum girilmesi halinde, Google haritalar gibi gerçek haritalarla topoloji çizimi otomatik yapabilmektedir.



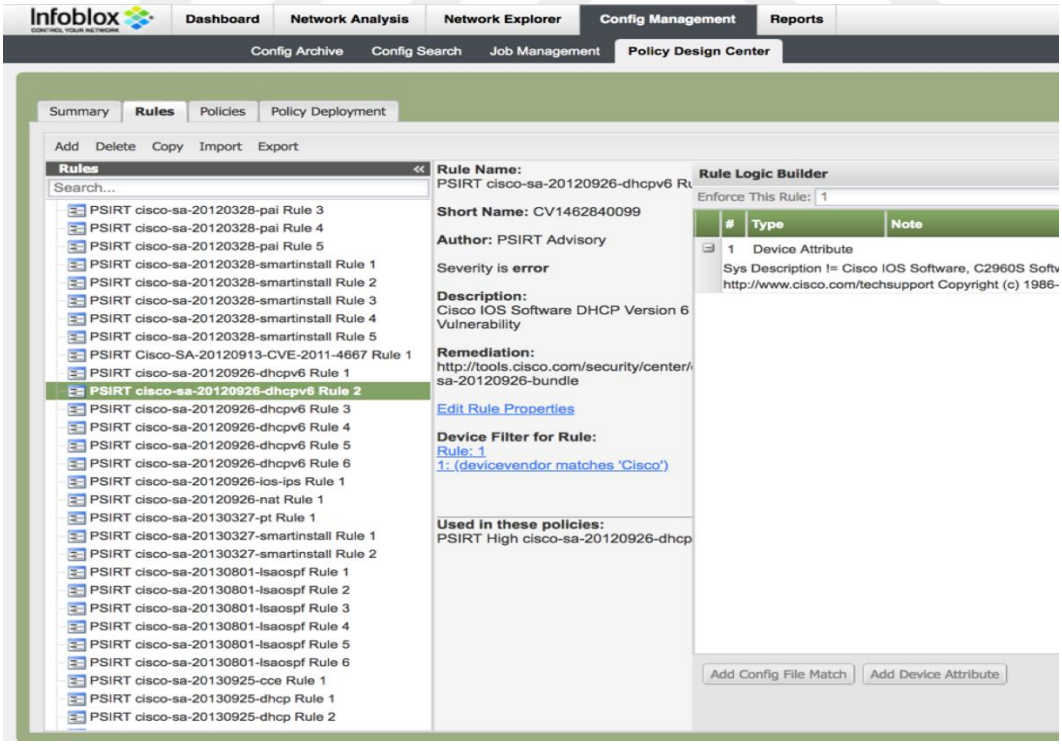
Resim 3.16 Hazır şablonlar üzerinden rapor alma ekranı.

Manageengine de alım maliyeti şirketlere fazla yük getirecek bir üründür. Ağ izleme özelliğinin oldukça başarılı olması ve içerisinde bulunan araçların, ağ uzmanlarının işini kolaylaştırabilecek özeliklere sahip olması avantajlarının yanı sıra alarm mekanizmasının ve yapılandırma yönetiminin biraz yetersiz kaldığı görülmektedir. Sunulan araçlar içinden bir seçim yapılarak satın alınması maliyeti düşürebileceği düşünülecek olursa, ağ yönetimi için tercih edilebilecek başarılı bir ürün olarak karşımıza çıkmaktadır.

3.9.5 Infoblox NetMRI Ağ Otomasyon Yazılımı

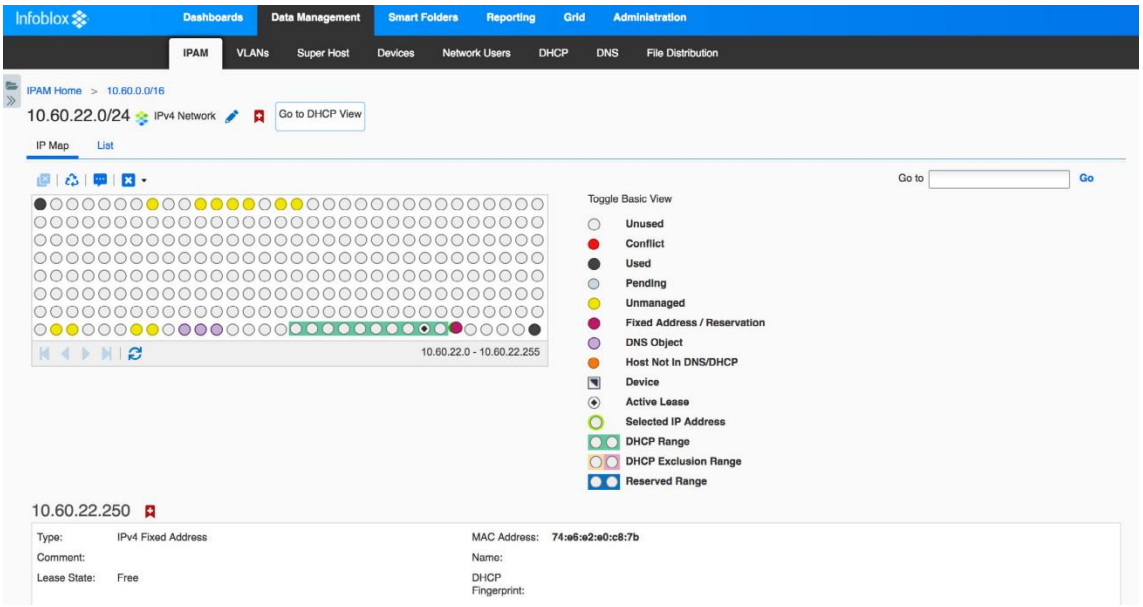
Infoblox NetMRI ağın ve yönetilecek cihazların keşfi, ağ durumu analizi, yapılandırma yönetimi, ağda toplu işlem yapılması ve uygunluk denetimi gibi gelişmiş ağ yönetim kabiliyetlerine sahip bir ağ yönetim sistemidir. Yönetilecek cihazları toplu ekleyerek, ağın katman 2 ve katman 3 (OSI Referans) topoloji çizimini otomatik yapabilmektedir. Ayrıca eklenen cihazlar yazılım tarafından türüne (yönlendirici, anahtar, güvenlik duvarı vb.) göre gruplara ayrılmaktadır. NMS'in ağın keşfini yaparken geçen uzun süreler (1-2 gün) diğer ürünlere göre biraz daha fazla vakit kaybettirmektedir.

NetMRI ağda yapılan yapılandırma değişikliklerinin kontrolünü yapmak için tarihsel yapılandırma ayarı yedeği tutmaktadır. Olası bir güvenlik ihlali veya yetkisiz ayar değişikliği tespiti olması halinde Resim 3.17'de görülen ekrandaki gibi kurallar yazılarak ağın eski haline getirilmesi otomatikleştirilebilmektedir. Bu sayede cihazlarda yapılan en ufak değişikliği yöneticilere bildirerek ağda oluşabilecek sorunların önüne geçilmesi sağlanmaktadır.



Resim 3.17 Kuralların test edildiği ve uygulandığı ekran.

Infoblox NetMRI, ağdaki anahtar cihazların ve bu cihazlar üzerindeki portların yönetimini başarıyla yapabilmektedir (Resim 3.18). Uzun süreli kullanılmayan port bilgilerini ve Active diretory entegrasyonu yapılması halinde kullanıcıların bilgisayarlarının takılı olduğu port bilgisi gibi yönetimsel işlemler yapılabilmektedir. Bu özellik gereksiz yapılan anahtar cihazı alımlarının önüne geçerek, anahtarlara takılan yabancı cihazların kontrolünün yapılmasını kolaylaştırmaktadır.



Resim 3.18 Anahtar cihazı ve kullanıcı port yönetimi.

NetMRI ağda yapılacak ayar değişikliklerinin dağıtma süresini kısaltan, güncel güvenlik politikalarının uygulanmasını sağlayan, gerçek zamanlı olarak tam görünürlük sağlayan, değişiklik ve yapılandırma yönetimini kontrol eden bir otomasyona sahiptir. Alarm yönetim mekanizmasının ağdaki değişilikleri kontrole bağımlı kalması ve oluşabilecek hataların kural tabanlı kontrolünün sağlanamaması ürünün bir eksikliğidir. Ayrıca modüler bir yapıya sahip olmamasına rağmen yüksek maliyetlere ulaşan fiyatları tercih aşamasında dikkat edilmesi gereken başlıklardır.

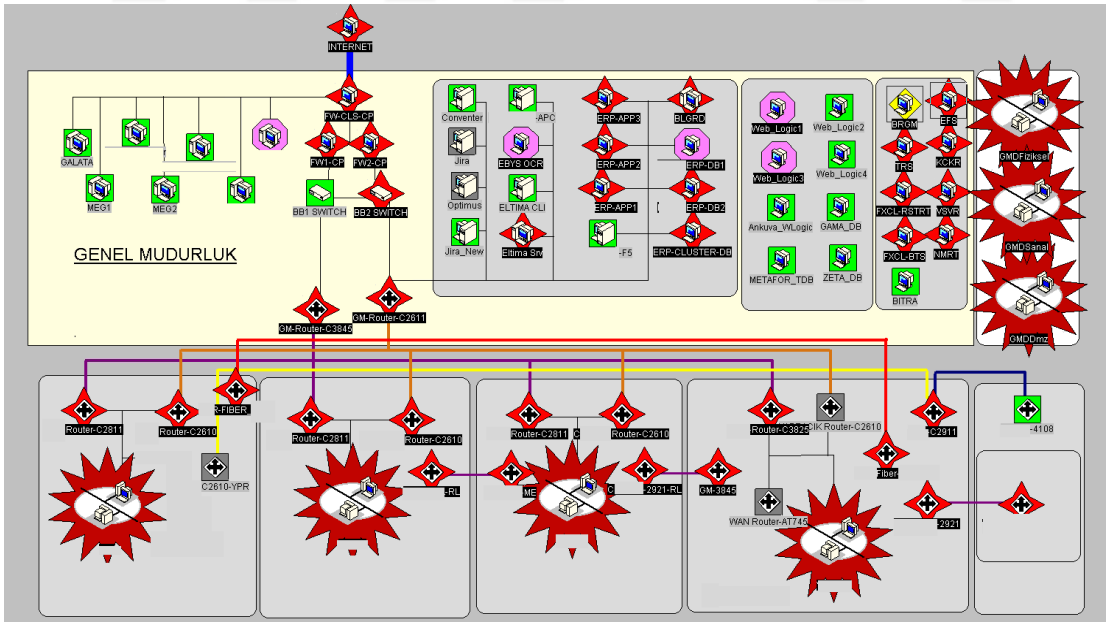
3.9.6 Açık Kaynak Kodlu ve Ücretsiz Ürünler

Ağ yönetim sistemini Paessler Prtg, Cisco Prime, Solarwinds gibi ücretli lisanslanan ürünler kullanılabileceği gibi, ücretsiz kullanımına izin verilen veya açık kaynak kodlu

dağıtımı yapılan yazılımlar da tercih edilebilir. Genellikle farklı çözümler için geliştirilen yazılımlar olmasından dolayı, ücretli ürünlerde olduğu gibi tek bir ekrandan bütün araçlara ulaşılabilecek bir ara yüz yoktur. Bu durum ağın yönetilmesinde ekstra bir zorluk getirmektedir. Etkili bir yapı kurulabilmesi için, en doğru yazılımların tercih edilmesi gereklidir. OpenNMS, LibreNMS gibi ürünlerle tek arayüzden ağ izleme, hata yönetimi yapılabileceği gibi; Cacti, Whatsup Gold gibi ürünlerle bant genişliği yönetimi, topoloji takibi gibi temel kontrollere yönelik çözümler kullanılabilir. Yüzlerce açık kaynak kodlu veya ücretsiz kullanılabilecek NMS ürünü bulunmaktadır. Dağıtımı ücretsiz olan dört farklı ağ yönetim sistemi bu başlık altında incelenmiştir.

3.9.6.1 Whatsup Gold Ağ İzleme Aracı

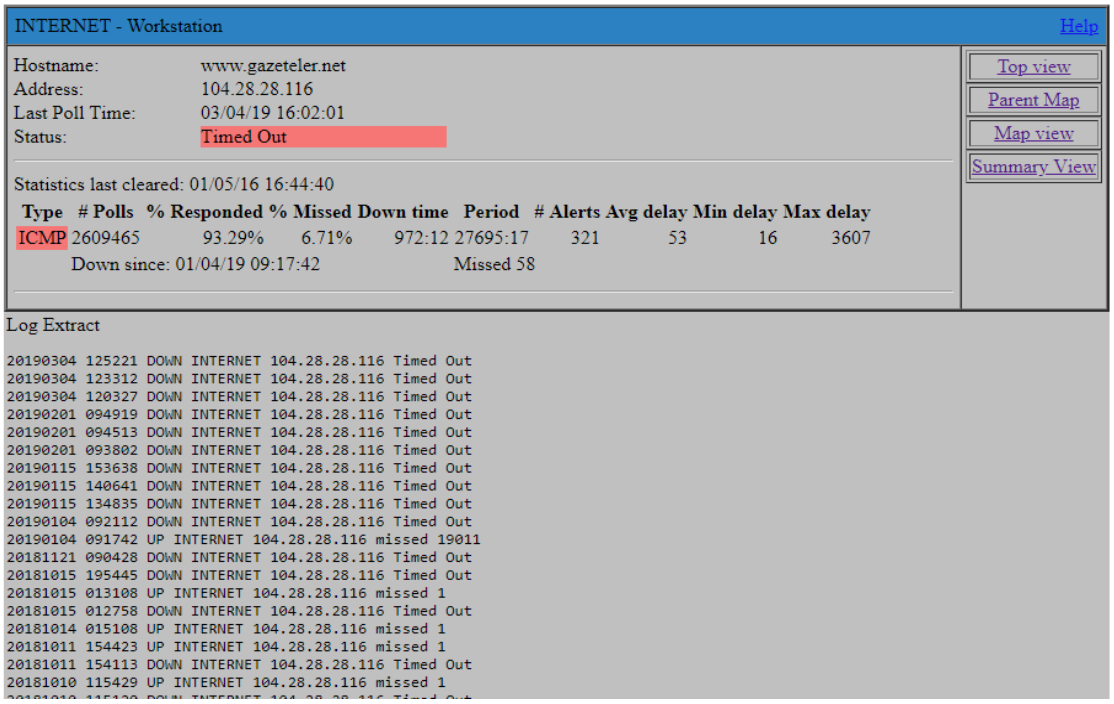
Ağ cihazlarını ve sunucuları izlemek için geliştirilen, eski sürümleri ücretsiz ve lisanslama gerektirmeden sınırsız kullanılabilen ağ izleme yazılımıdır. Web tabanlı bir arayüze sahip olan yazılım ile çeşitli topolojik haritalar oluşturulup, alarm takibi yapılabilmektedir (Resim 3.19).



Resim 3.19 Ağdaki cihazların topoloji haritası ve alarm takip ekranı.

Cihazlar ve portlar nesne olarak topolojiye eklenerek takibi yapılmaktadır. Resim 3.20'de görüldüğü gibi alarm bölümünde sadece cihazın durumu bağlantı (up/down) hakkında

bilgiler yer almaktadır. Takibi gerçekleştirilen cihaz ile bağlantının kesilmesi durumunda yöneticilere e-mail yoluyla alarm bildirimi yapılmaktadır. İşlemci, ısı, bellek kullanımı bilgileri veya diğer ulaşılabilen sensörlerle ilgili bir alarm mekanizması bulunmamaktadır. Whatsup Gold ağ ve sunucu sistemlerinin bağlantı durumunun izlenmesine yönelik geliştirilmesi ve basit bir ağ yönetimi çözümü sunması nedeniyle, yazılımın eksiklikleri tamamlayıcı özelliklere sahip ürünler ile birlikte kullanılması gereklidir.

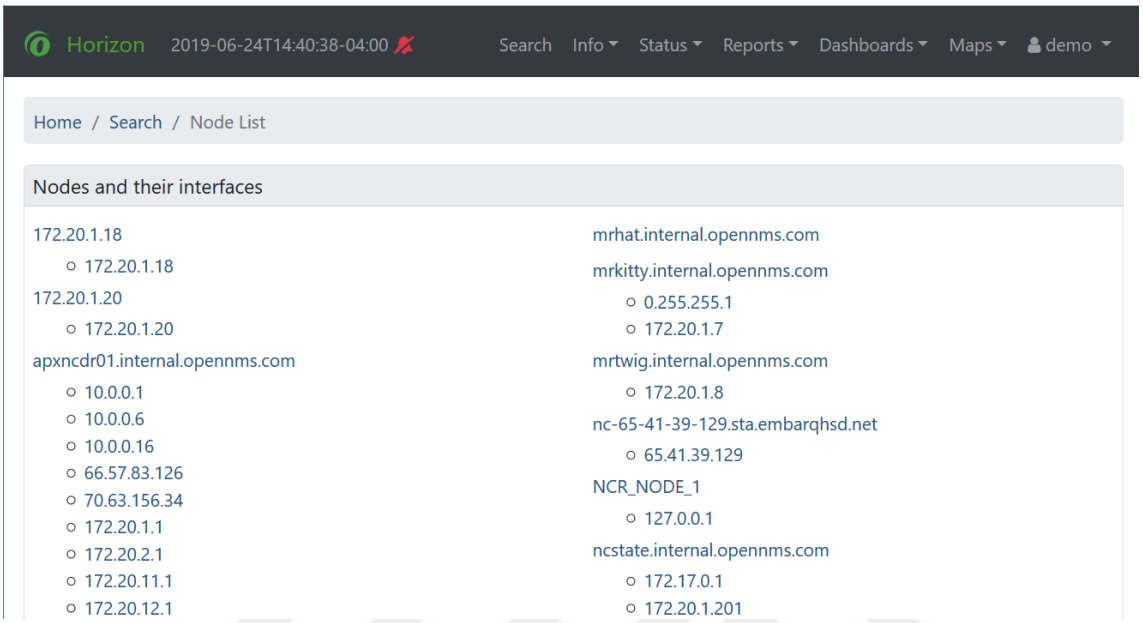


Resim 3.20 Alarm detay ekranı.

3.9.6.2 OpenNMS Açık Kaynak Kodlu Ağ Yönetim Sistemi

Temel düzeyde ağ yönetimi yapmaya imkân veren, OpenNMS grubu tarafından geliştirilen ana bir yazılım üzerinden açık kaynak kodlu ve ücretsiz dağıtımı yapılan ağ yönetim sistemidir. Bu üründe raporlama, performans verilerini toplama ve olay bildirimi olmak üzere üç temel özellik sunulmaktadır. Diğer ücretsiz yazılımlardan farklı olarak teknik destek alınabilen bir topluluğun bulunması sayesinde yazılımsal yaşanabilecek problemler çözüme kavuşturulabilmektedir. Ancak bu hizmetten yararlanabilmek için belli bir miktar ücret ödenmesi gerekmektedir. Resim 3.21'deki yönetilen cihazların

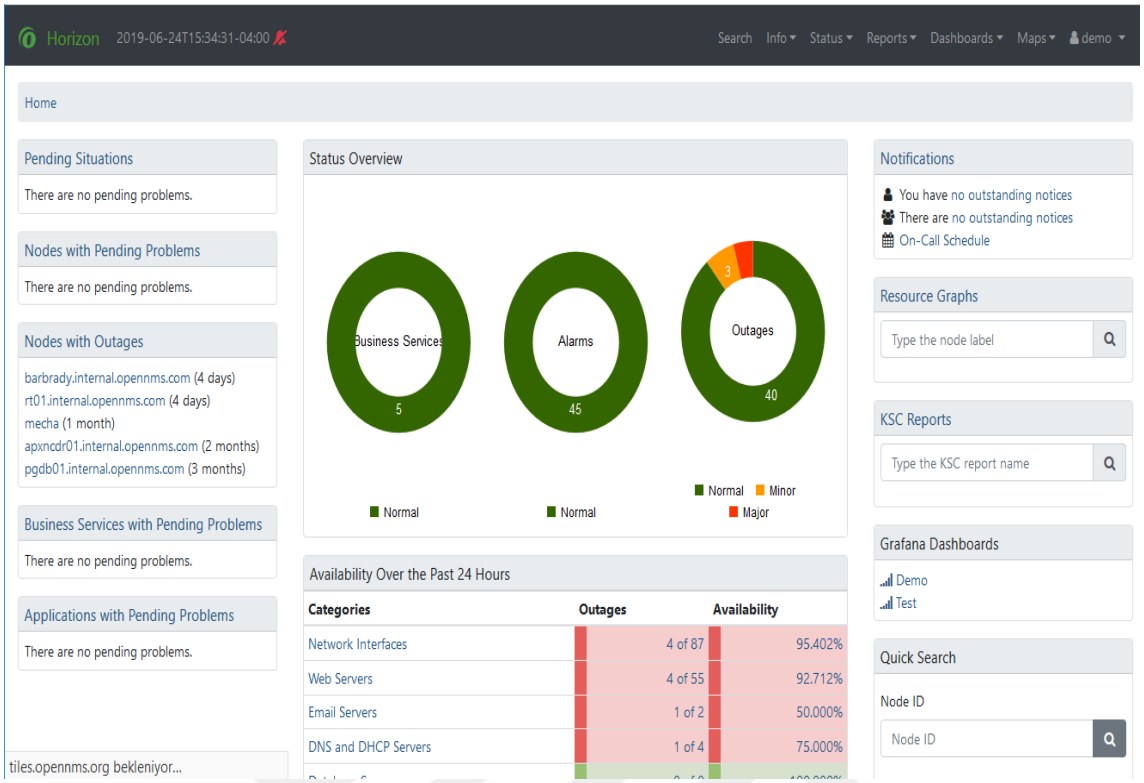
listesinin olduğu ekrandaki gibi tek menüden tüm araçlara ulaşılan bir arayüz olmasına rağmen, tasarımı önem verilmemiş butonlar ve pencereye doğru konumlandırılmamış yazılar nedeniyle NMS'in kullanımı zorlaşmaktadır.



Resim 3.21 OpenNMS araç menüleri(üstte) ve yönetilen cihazların dökümü(ortada).

Kullanıcı gruplarının oluşturarak bu gruplardaki üyelerin yetkileri belirlenebilmekte ve gerektiğinde alarm bildirimi yapılırken gruplar kullanılabilmektedir. Otomatik döküm taraması, yönetilen cihazlarla ilgili basit raporlamalar, hata seviyelerine göre alarm yönetimi ve cihaz performansı takibi işlemlerini yapılabileceği gibi tüm bu verileri Resim 3.22'deki kontrol ekranından anlık görüntülenmesi sağlanmaktadır.

Yapılandırma yönetimi, kural tabanlı alarm yönetimi gibi üst seviye NMS ürünlerinde bulunan özellikleri içermese de yazılımın kaynak kodlarına resmi web sitesinden tamamen ücretsiz erişilebilmesi ve kullanılabilecek kod kütüphanelerin OpenNMS topluluğu tarafından doküman haline getirilerek, ihtiyaçlara ve amaca uygun geliştirilebilmesine imkân sağlanmıştır.

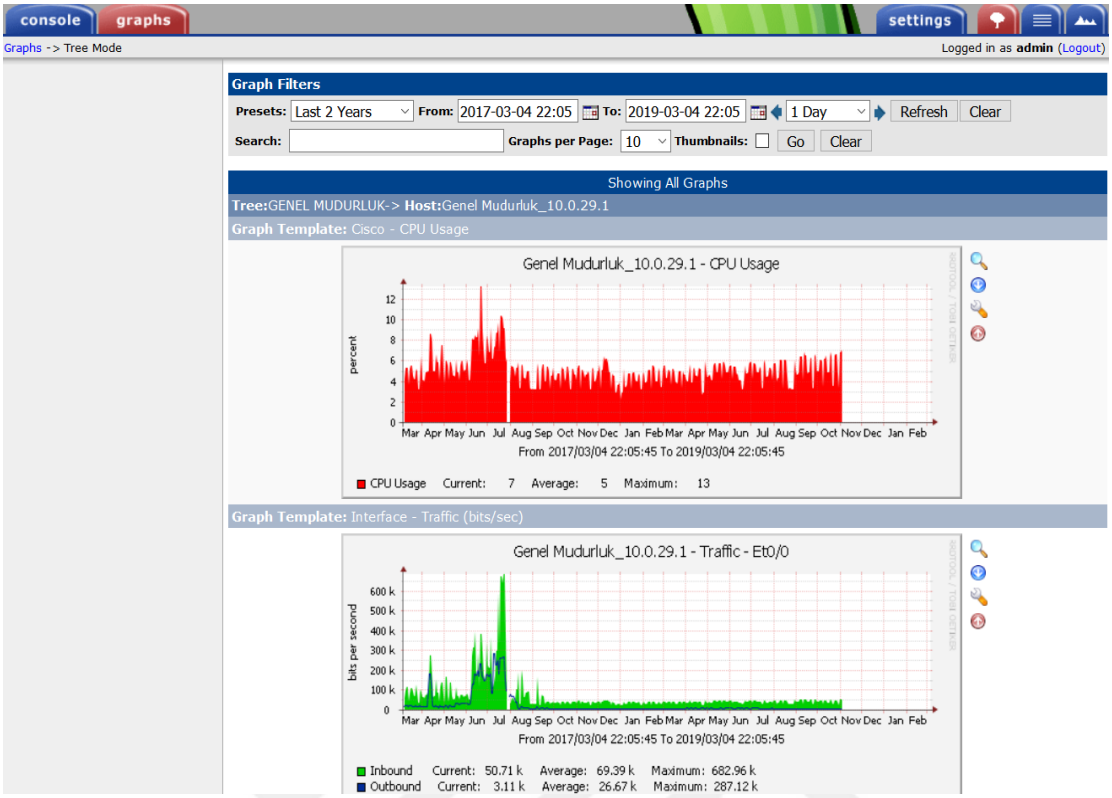


Resim 3.22 Kontrol ekranı ekran görüntüsü.

3.9.6.3 Cacti Kaynak İzleme ve Grafik Yazılımı

Aktif ağ cihazlarının işlemci, bellek, disk ve trafik bant genişliği bilgilerini grafiksel olarak gösteren ağ yönetim yazılımıdır. Ücretsiz ve açık kaynak kodlu dağıtıma sahip olan ürüne, php programlama dili kullanılarak ihtiyaçlara yönelik eklentiler yazılabilmektedir. Ayrıca yazılım içerisinde eklenti yönetimi bölümü içerisinde farklı geliştiricilerin hazırlamış olduğu araçlar kullanılabilmektedir.

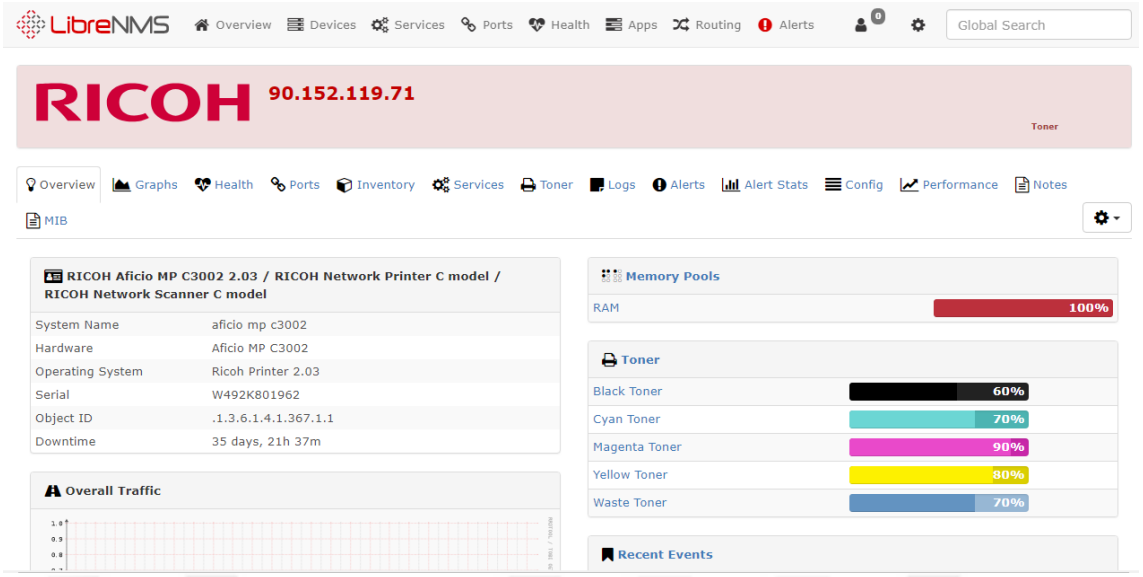
Ağ cihazlarının işlemci, bellek ve disk kullanımlarını, ağdaki genel yük ortalamasını, port arayüzündeki bant genişliği tüketimini ve dosya sistemindeki aktivitelerin takibinin yapılabileceği farklı grafikler oluşturulabilmektedir. Daha sonra eklenen grafiklerdeki aktiviteler görüntülenebilmekte ve rapor olarak alınabilmektedir (Resim 3.23).



Resim 3.23 Grafik görüntüleme ekranı.

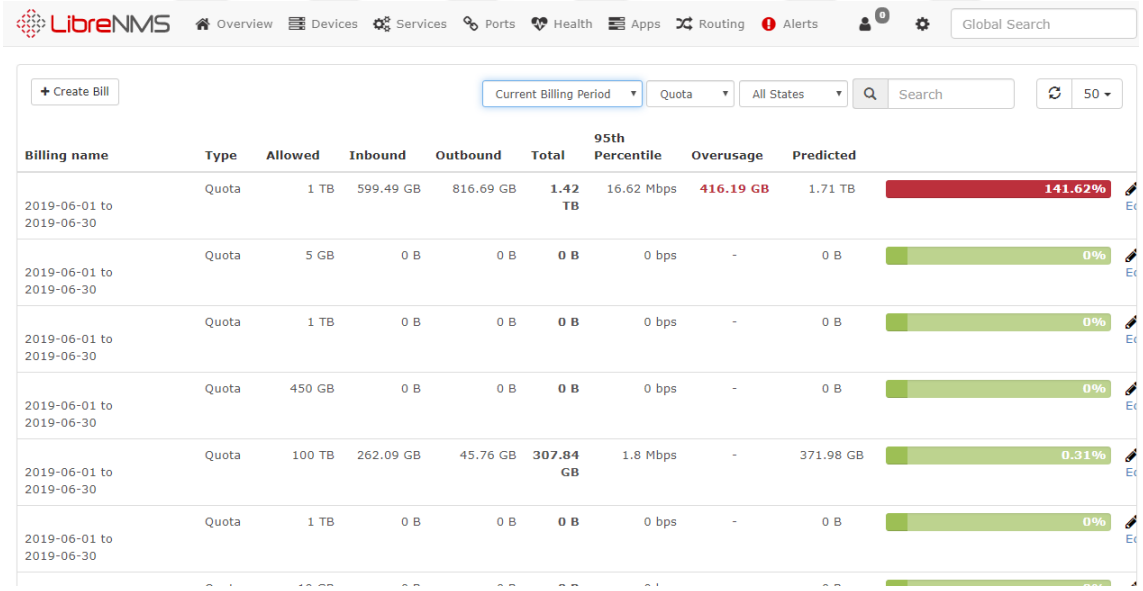
3.9.6.4 LibreNMS Ağ Yönetim Sistemi

İncelenen ücretsiz yazılımlar içerisinden en kararlı ve bir ağ uzmanının işine yarayacak özelliklerin tek arayüz üzerinden sunan ağ yönetim sistemidir. Github üzerinden kaynak kodlarına ulaşılıp, PHP/Mysql dilleriyle yazılım amaca uygum geliştirilebilmektedir. Yönetilen cihazların işlemci, depolama, ısı gibi durum bilgilerine takip edilebildiği gibi Resim 3.24'deki cihaz ekranında görülen ofislerde sıkca kullanılan yazıcıların toner bilgilerini görüntülemek de mümkündür. Özelikle Solarwinds ürünü incelenirken üstünde durulan cihazlardan gelen log kayıtlarının yönetimi, LibreNMS'de başarılı bir şekilde yapılmaktadır. Cihazların verdiği hata mesajlarının toplandığı ve bu mesajların alarm haline getirebildiği bir menü bulunmaktadır. Cihazlarda yaşanan tüm olayların alarmlar ile yöneticilere bildirilmesi de sağlanmıştır. Kullanıcı gruplarına göre yetkilendirme ile eposta, Syslog, Jira ve hatta Philps hue ile alarm bildirimi yapılabilmektedir. 400'e yakın üretici desteğine sahip olan yazılım bu üreticilere uygun tanımları ve sensörlerin kullanımına imkân vermektedir.



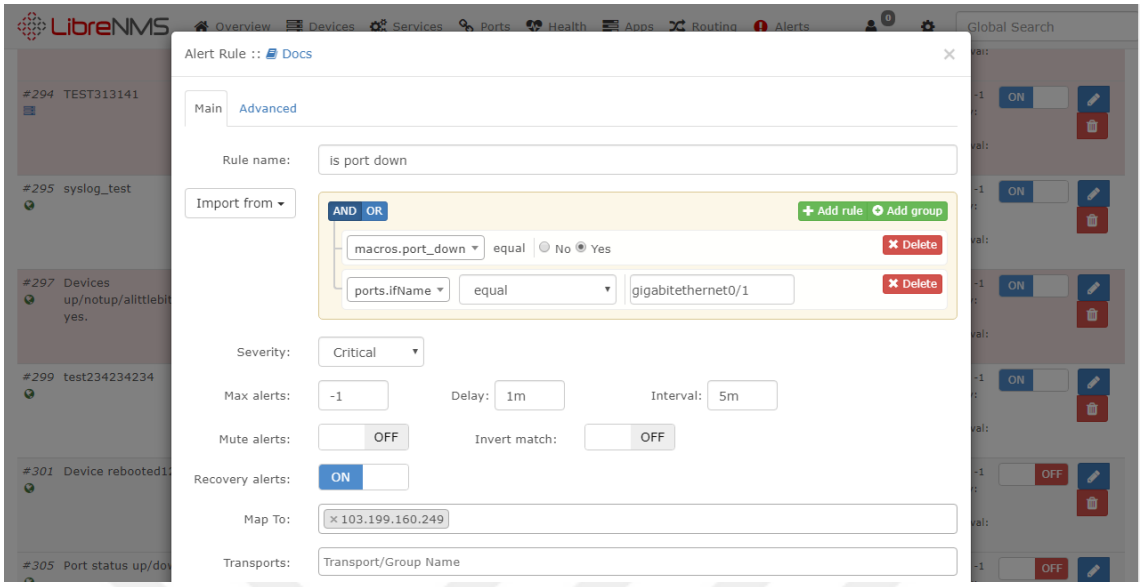
Resim 3.24 Yazıcı cihazı görüntüleme ekranı.

İletişim hatlarının trafik kontrolü yapmak mümkündür (Resim 3.25). Anlık ve geçmiş trafik kontrolü yapılabileceği gibi, hattı en çok kullanan kaynak IP bilgisine de ulaşılabilmektedir.



Resim 3.25 İletişim hattı trafiği bilgileri kontrol ekranı.

Oluşabilecek olası hatalar için alarm kuralları yazılabilmektedir (Resim 3.26). 100'e yakın hazır şablon kullanılarak kontrol edilmesi istenen nesnelere kurallar yazılmaktadır. Bu şablonların dışında PHP diliyle ağın ihtiyaçlarına uygun kural şablonu oluşturmak mümkündür.



Resim 3.26 Alarm kuralı yazım bölümü.

LibreNMS çoğu ücretli ağ yönetim sisteminin yaptığı işleri yapabilmesi ve bu işleri yaparken kullanılan araçları basit bir arayüz ile sunan açık kaynak kodlu üründür. Detaylı ağ performansı izleme, sistem raporları alma ve yapılandırma yönetimi konularında geliştirilmiş araçlarının olamaması NMS'in eksiklikleri arasındadır.

3.9.7 İncelenen Ürünlerin Karşılaştırılması

Çeşitli özeliklere sahip ve benzer sorunlara çözüm üretmek için geliştirilen 9 adet ağ yönetim sistemi incelenmiştir. Ürünlerin özelliklerini daha iyi ortaya çıkarmak ve seçim aşamasında tercihi kolaylaştırmak için incelenen tüm ürünlerin 15 farklı kriter üzerinden karşılaştırılığı bir tablo hazırlanmıştır (Çizelge 3.2). Kurumsal bir ağın yönetimi için kullanılacak ağ yönetim sisteminde olması gereken araçlar yeterli düzeyde olacağı gibi ürünün maliyetinin de uygun seviyelerde olması gerekmektedir. Alınacak NMS'deki özelliklerin çıkarılması veya eklenmesiyle ve yönetilecek cihaz sayısındaki miktara göre fiyatlarda değişiklikler olabilmektedir. Tabloda verilen maliyet bilgileri ortalama değerleri ifade etmektedir.

Çizelge 3.2 İncelenen ağ yönetim sistemlerinin karşılaştırılması.

NMS	Tek Arayüz Yetkilendirme	Ağ Keşfetme	Hata Ayırt etme	Alarm Mekanizması	Yapılandırma Yedekleme/Yükleme	Yapılandırma Ayarı Kontrolü	Toplu İşlem	Veri trafiği Takibi	Ağ İzleme	Log Analizi	Raporlama	Modüler yapı	Tenik Destek	Maliyet
Paessler PRTG	V	Y	V	Y	V	Y	Y	Y	V	V	V	Y	V	13000
Cisco Prime	V	V	V	V	V	V	V	V	V	V	V	Y	V	9200
Solarwinds	V	V	V	V	V	V	V	V	V	V	V	V	V	21000
Manageengine Opmanager	V	V	V	V	V	V	V	V	V	V	V	V	V	36000
Infoblox NetMRI	V	V	V	V	V	V	V	V	Y	V	V	V	V	35000
Whatsup Gold	Y	Y	Y	Y	V	Y	Y	Y	Y	Y	V	Y	Y	-
OpenNMS	V	V	V	Y	V	Y	Y	Y	Y	V	Y	V	Y	-
Cacti	Y	Y	Y	Y	Y	Y	Y	Y	V	V	Y	V	Y	-
LibreNMS	V	V	Y	V	V	Y	Y	V	V	V	Y	Y	Y	-

V; Var. Y; Yok. Maliyet sütunundaki tüm birim fiyatları amerikan doları cinsindendir.

4. BULGULAR

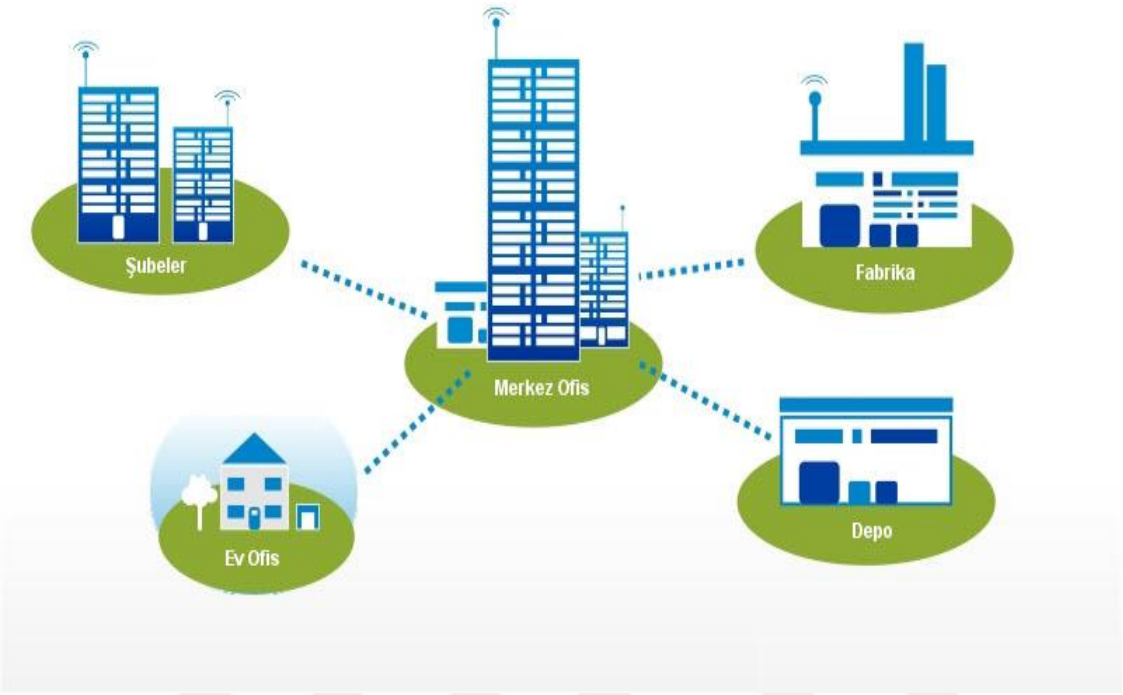
Büyük ölçekli coğrafi alanlarda faaliyet gösteren kurumsal şirketlerin bilgiyi, çalışanlarına ve müşterilerine hızlı, sürekli ve güvenli bir şekilde ulaştırması büyük önem arz etmektedir. Günümüzde bunu sağlayan en önemli aracın bilgisayar ağları olduğu bir gerçektir. Yerel alan ağlarının, geniş alan ağlarını oluşturmasıyla meydana gelen bu yapı, şirketlerin bilgiye erişim ihtiyaçlarını karşılamaktadır. Farklı amaçlara hizmet eden sistemlerin birleşimiyle kurulan bu yapının, kurulum aşamasının yanlış yapılması veya sonrasında yaşanabilecek yönetimsel sıkıntılar, şirketler için maddi sorunlara neden olabilmektedir. Yaşanabilecek sorunların üstesinden gelinebilmesi için ağım kurulumu öncesi ve kurulum aşamasında yapılması gerekli işlemlerin eksiksiz yapılması gerekmektedir.

Kurumsal geniş alan ağı altyapısı kurulduktan sonra sorunsuz ve kendi kendine çalışmasının beklenmesi en büyük hatadır. Ağın etkili yönetilebilmesi için, yaşanacak sorunlara müdahale edebilecek, alanında uzman ağ yöneticilerine ve en önemlisi yönetim ekibine yardımcı bir ağ yönetim sistemine ihtiyaç duyulacaktır. Ağ yönetim sistemi seçilirken ağın ihtiyaçları göz önüne alınarak; yazılımın yapabileceği yetenekler ve sunduğu çözümler değerlendirilmelidir. Tüm bu anlatılan bilgiler doğrultusunda 3000 çalışan personeli, birbirinden uzak 6 farklı yerleşkede hizmet veren ve toplam 410 adet aktif kullanılan ağ cihazı(yönlendirici, anahtar, kablosuz erişim noktası vb.) bulunan örnek bir şirket üzerinden kurumsal geniş alan ağının nasıl kurulması gerektiği, etkin bir yönetim için gerekli ağ yönetim sisteminin kurulum aşamaları ve gerçekleştirilen işlerden elde edilen sonuçlar aşağıda iki ayrı başlık altında açıklanacaktır.

4.1 Tasarımı ve Yönetimi Gerçekleştirilen Kurumsal Geniş Alan Ağı

Kurumsal bir geniş alan ağını doğru ve etkin yönetilebilmesi için öncelikle işe ağın kurulumundan başlanılması gerekilmektedir. Şekil 4.1'de görüldüğü gibi şirketler, kaynaklarını merkezi ofiste bulunan veri merkezinden uç noktalara dağıtımı gerçekleşecek şekilde tasarlanan geniş alan ağı mimarisini kullanmaktadır. Örnek geniş alan ağımız da bu mimari etrafında şekillendirilecek olup, tüm altyapının kurulumu,

planlaması ve yönetimi bu merkez ofis üzerinden yapılıp, uç noktaların merkeze erişimi iletişim hatları üzerinden sağlanacaktır.



Şekil 4.1 Merkezden yönetimi sağlanan kurumsal geniş alan ağı (İnt. Kyn. 12).

Kurulum aşamasında yapılacak olan işlemlerin daha doğru planlanması için Çizelge 4.1'de örnek şirketimizin yerleşkeleri ve bu yerleşkelerde çalışan personel ile kullanılan cihaz sayıları çıkarılmıştır.

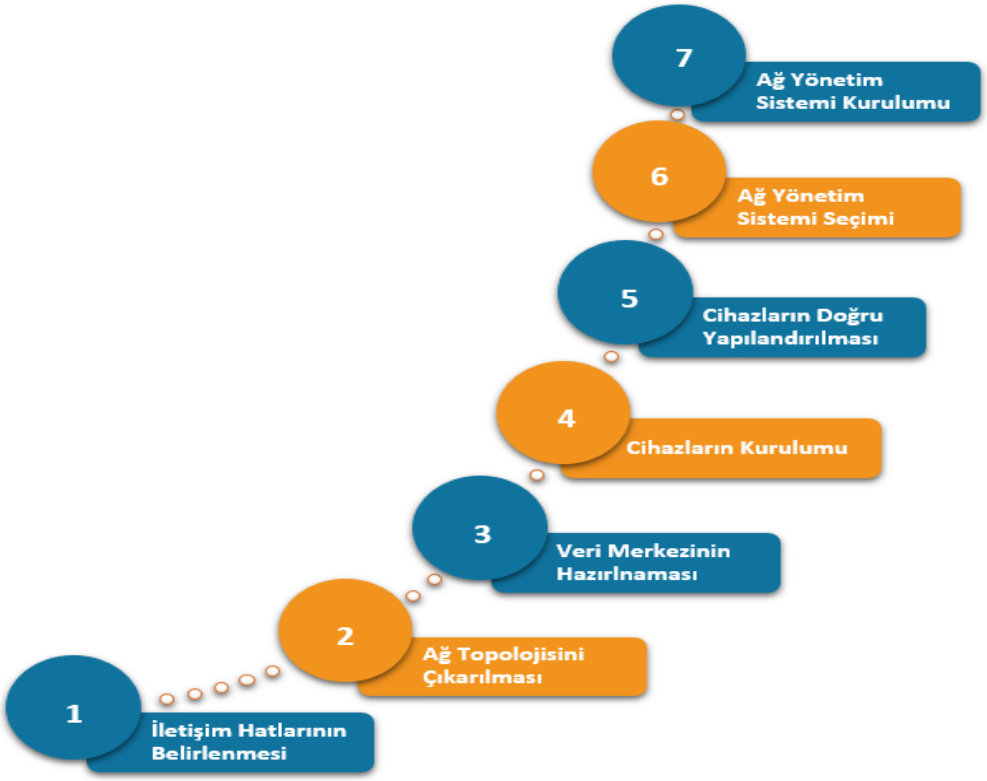
Çizelge 4.1 Şirket bilgilerini gösteren tablo.

Yerleşke	Çalışan Personel Sayısı	Kullanılan Ağ Cihazı
Merkez Ofis	1000	2 adet Yönlendirici 2 adet Omurga Anahtar 60 adet Anahtar(24 portlu) 2 adet Kablosuz denetleyici 100 adet Kablosuz erişim noktası 14 adet Güvenlik cihazı

Çizelge 4.1 (Devam) Şirket bilgilerini gösteren tablo.

İstanbul Şube	100	2 adet Yönlendirici 2 adet Omurga Anahtar 6 adet Anahtar(24 Portlu) 20 adet Kablosuz erişim noktası
Antalya Şube	50	2 adet Yönlendirici 2 adet Omurga Anahtar 4 adet Anahtar(24 Portlu) 10 adet Kablosuz erişim noktası
Müşteri Haberleşme	350	2 adet Yönlendirici 2 adet Omurga Anahtar 18 adet Anahtar(24 Portlu) 30 adet Kablosuz erişim noktası
Müşteri Depo	300	2 adet Yönlendirici 2 adet Omurga Anahtar 4 adet Anahtar(24 Portlu) 30 adet Kablosuz erişim noktası
Afyon Fabrika	500	2 adet Yönlendirici 2 adet Omurga Anahtar 6 adet Anahtar(24 Portlu) 50 adet Kablosuz erişim noktası
Bursa Fabrika	700	2 adet Yönlendirici 2 adet Omurga Anahtar 8 adet Anahtar(24 Portlu) 30 adet Kablosuz erişim noktası

Kurumsal bir geniş alan ağının kurulum aşamasında merkezde bulunan veri merkezinde ve uç noktalardaki yerel alan ağlarında yapılması gereken birtakım işlemler vardır. Bu işlemler atlanmadan ve doğru planlanarak yapılması durumunda, kurulumu gerçekleşen ağın yönetimi daha kolay hale gelecektir. Şekil 4.2'deki şemada sırasıyla yapılması gerekli kurulum adımları gösterilmektedir. Görülen bu adımlar tüm detaylarıyla aşağıda açıklanacaktır.

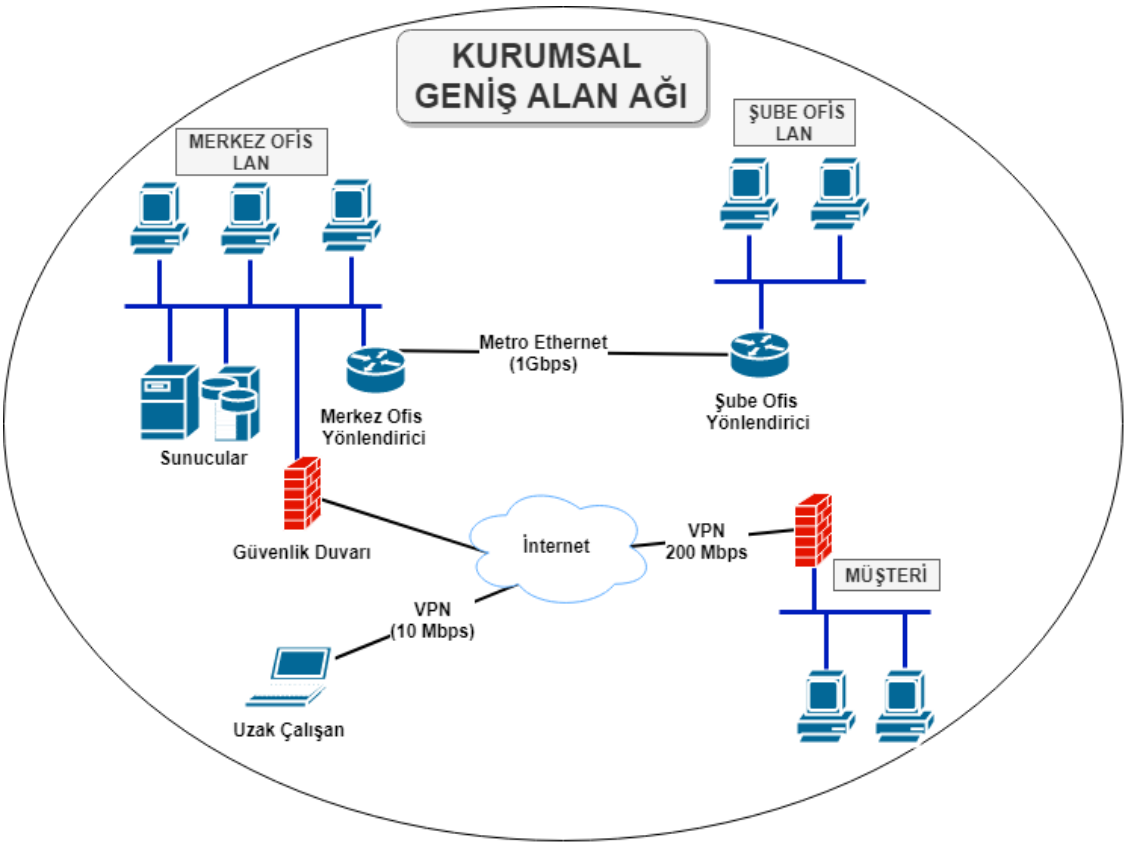


Şekil 4.2 Kurumsal geniş alan ağı kurulum ve yönetim adımları.

4.1.1 İletişim Hatlarının Belirlenmesi

Şirketler için WAN'ın nasıl bir araya geldiği veya yerel ağların birbirinden ne kadar uzakta olduğu bilgisinin önemi yoktur. Her zaman farklı konumlardaki yerel ağların merkez ve birbirleriyle iletişim kurması amaçlanmaktadır. Bu amacı gerçekleştirilebilmesi için günümüzde iki seçenek vardır. Birincisi ve daha az maliyetli olanı sanal özel ağ (Virtual Private Network-VPN) bağlantısı, diğeri ise kiralık hatlardır (Metro Ethernet). Metro ethernetler; noktadan noktaya ethernet bağlantıları kurmaya yarayan, dış dünyaya tamamen kapalı, VPN bağlantısına göre daha güvenli ve yüksek hızlarda (1Gbps, 10 Gbps vb.) veri aktarımına olanak tanıyan fiber hatlardır. Şekil 4.3'deki basit geniş alan ağı topolojisinde görüleceği gibi, veri aktarımı daha az olan uç noktalarda, internet üzerinden VPN hizmeti alınarak bağlantı gerçekleştirilebilir. VPN'ler makul düzeyde güvenlik sağlasa da, internet bağlantısı üzerinden alınan bir hizmet, özel hat bağlantısının verebileceği yüksek bant genişliği seviyelerini sağlayamaz. Metro ethernet hatları ise maliyet açısından şirketlere ek yük getireceğinden, kullanım yerlerine

göre dezavantaj sağlayabilir. Kurumsal geniş alan ağlarında hat seçiminde uç noktadaki ofislerde bulunan kullanıcıların yapacağı trafik tüketimi ve oluşacak maliyet göz önüne alınarak bir tercih yapılması gereklidir. Ayrıca kullanılan kiralık hatların fiziksel yedekliğinin sağlanması, olası bir sorun anında hizmet kesinti yaşanmaması için gerekli bir işlemdir.



Şekil 4.3 Geniş alan ağında kiralık ve VPN hatlarını gösteren örnek topoloji.

Kurulumunu yapacağımız geniş alan ağı 1 merkez ve 5 uç nokta olmak üzere toplam 6 farklı konumda hizmet veren bir yapıya sahiptir. Uç noktalardaki yerleşkelerdeki merkezde internet çıkışına ve kurumsal uygulamalara erişecek personel sayısına göre hat seçimi ve hız tercihi yapılacaktır. 350 çalışanının hepsinin bilgisayar kullandığı Müşteri haberleşme yerleşkesi ile 700 çalışanı olması rağmen 100 kişinin bilgisayar kullandığı Bursa fabrika yerleşkesine belirlenecek olan hattın hızı ve türü farklılık göstermiştir.

4.1.2 Ağ Topolojinin hazırlanması

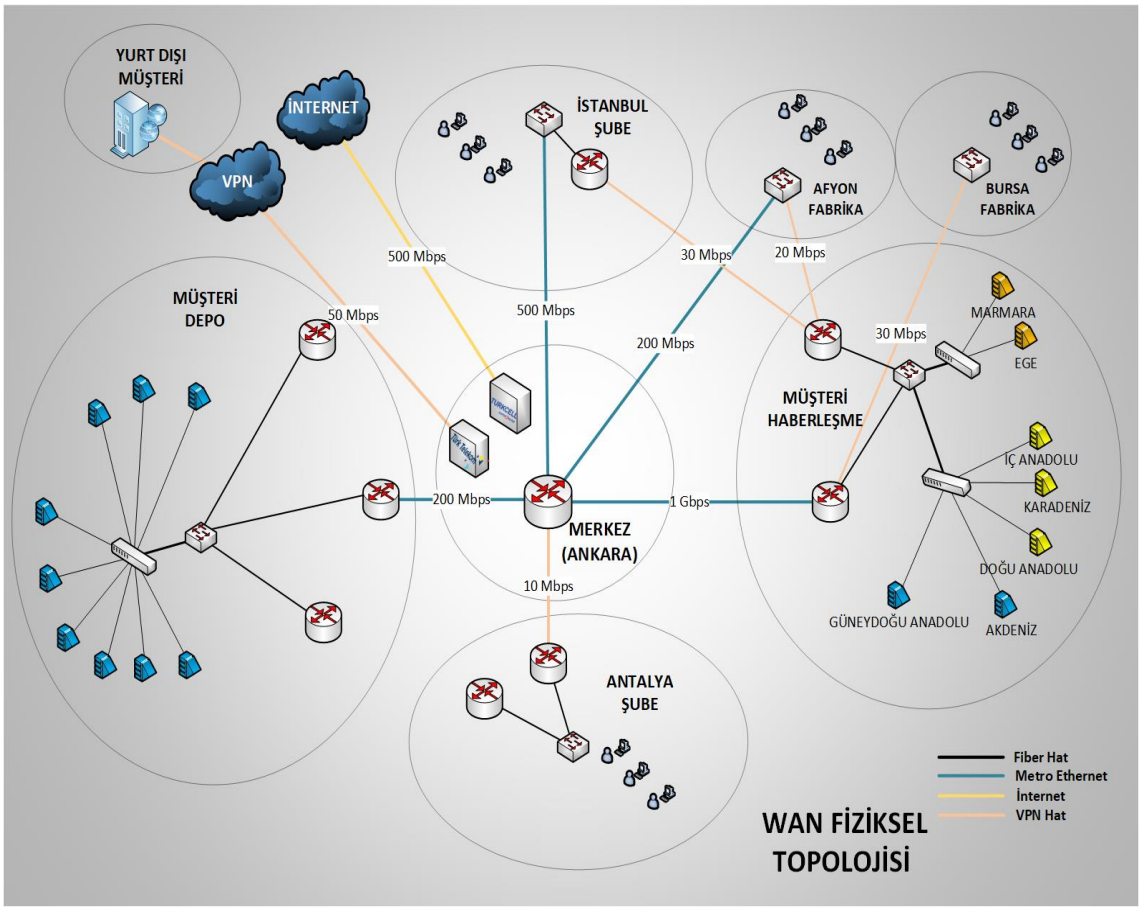
Topolojiler ağın bilinirliği ve hataların giderilmesi açısından en temel araçtır. Bilinmeyen bir ağın yönetimi yapılamaz, yönetilemeyen bir ağ da hiçbir zaman güvenli değildir. Ağ topolojisi, ilk bakışta cihazlar ve ağ hakkında bilgi edinilmesini sağlayan, bir sorunla karşı karşıya gelindiğinde çözme süresini azaltan, cihazların bağlantı düğümlerini görmemize yarayan çizimlerdir. Kısacası, veri merkezlerinin içerisindeki cihazların birbirleriyle olan bağlantının ve merkez ofis ile uç noktalar arasındaki hatların haritası niteliğindedir. Topoloji çizimleri ağ kurulurken bir kere çizilip bırakılması yerine, ağda yapılan her değişiklik sonunda mutlaka güncellenmesi gerekmektedir.

Topolojinin çizim öncesi, çizim aşamasında ve çizimden sonra bazı hususlara dikkat edilmesi gerekmektedir. Bunlar:

- Topoloji çizilmeden önce ağ cihazların, sunucu sistemlerinin marka-model içerecek şekilde dökümünün çıkarılması, kullanılacak olan IP bloklarının hazırlanması ve ağ bölümlerinin oluşturulması gerekmektedir.
- Topolojinin fiziksel ve mantıksal ayrımı yapılıp, her bir ağ bölümü (uç noktalar) ayrı ayrı çizilmelidir.
- Ağ da yapılan her bir değişiklik topolojide güncellenmeli ve tüm ağ, sistem, yazılım yöneticileri bilgilendirilmelidir.
- Çizilen ve güncellenen her topoloji, bir sürüm ismi ya da kodu saklanmalı ve yapılan değişikliklerin ardından güncelleme tarihleri eklenmelidir.
- Topoloji üzerinde, cihazların simgeleri için standart haline gelmiş nesneler tercih edilmeli, farklı bağlantılar için değişik renkler kullanılmalı ve bu kullanılan görsellerin topoloji altında neyi ifade ettiği belirtilmelidir.

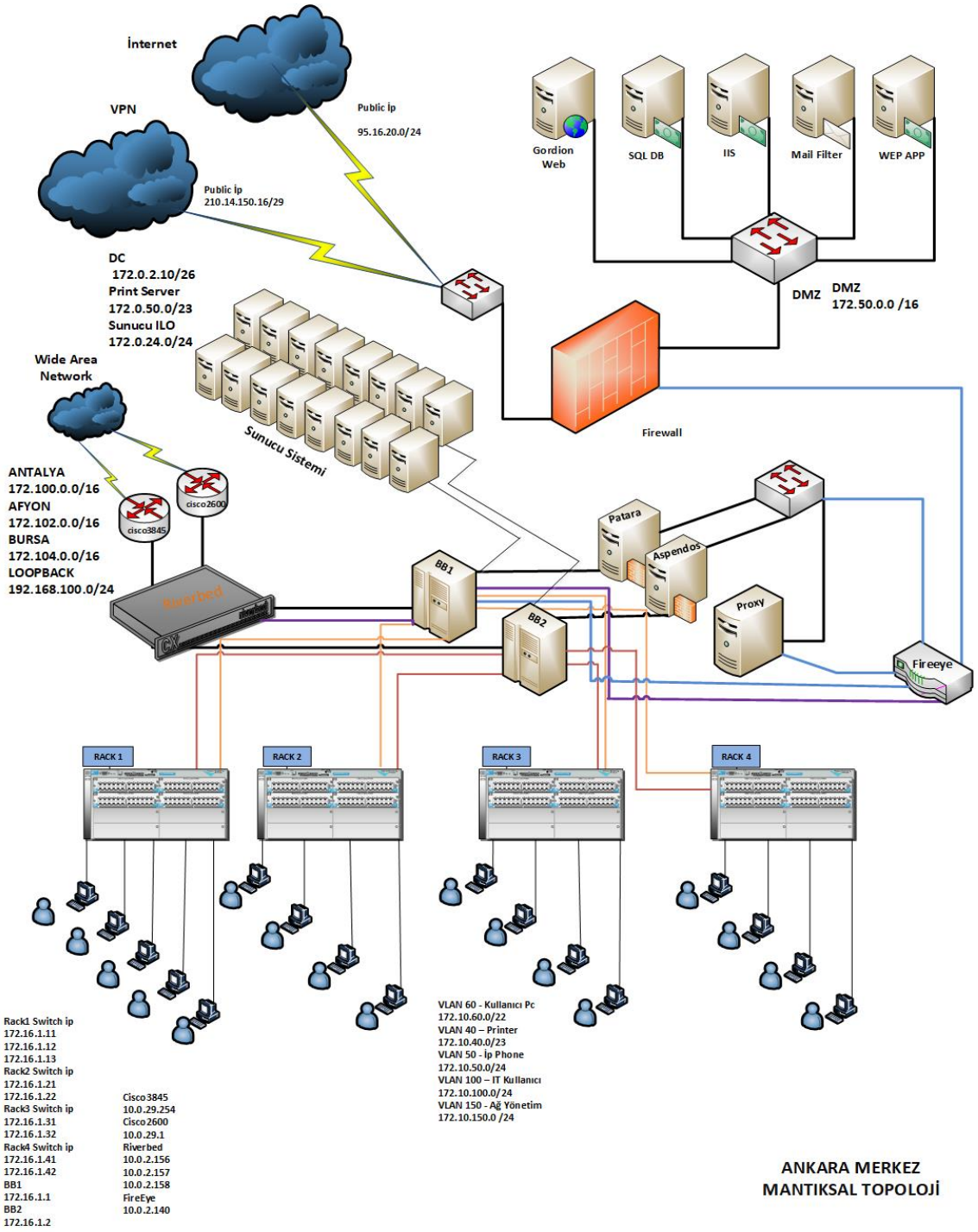
Fiziksel topolojiyi oluşturan önemli etkenler ağ cihazlarının konumlandırılacağı konumların ve ağ trafiğinin gideceği hatların belirlenmesidir. Bu iki faktörün belirlenmesinin ardından Şekil 4.4’de uç noktalardaki yerleşkelerin, merkez ofis ve birbirleriyle bağlantısını gösteren fiziksel topolojisi gösterilmiştir. Fiziksel topoloji haritası, haberleşmenin nasıl gerçekleşeceğini bize öğretmek yerine merkez ile uç nokta hat bağlantılarının ve cihazların bağlantılarının hangi fiziksel arayüzler üzerinden

gerçekleştiğini göstermektedir. Fiziksel topoloji çizilirken ağı bölümlere ayırarak çizilmesi daha sonra bakıldığında topolojinin anlaşılabilir olması açısından daha doğru olacaktır. Örneğin son kullanıcıların bağlantılarının görüldüğü fiziksel topoloji ve sunucu sistemlerinin bağlantılarını gösteren fiziksel topolojinin ayrı olması yönetim açısından kolaylık sağlayacaktır.



Şekil 4.4 İletişim hattı bağlantılarının görüldüğü fiziksel topoloji çizimi.

Mantıksal topoloji ağda yer alan, ağ bölümlerinin ve cihazlarının çalışma trafiğini bize göstermektedir. Topolojinin mantıksal çizilmesi gruplar arasındaki veri akışının kablolu bağlantıdan bağımsız olarak gösterilmesidir. Fiziksel topolojideki gibi ağı bölümlere ayırarak çizilmesi yönetim açısından kolaylık sağlayacaktır. Şekil 4.5'deki mantıksal topoloji çiziminde görüldüğü gibi merkez ofis de bulunan ağ cihazları; bölüm, IP ve fiziksel konum şeklinde gruplanarak gösterilmiştir.



Şekil 4.5 Merkez ofis yerleşkesinin mantıksal topoloji çizimi.

4.1.3 Cihazların Kurulumu

Cihazların kurulumu yapılmadan önce merkezde bulunacak olan ağ ve sunucu sistemlerinin konulacağı veri merkezinin fiziksel ortamının hazırlanması gerekmektedir. Veri merkezi hazırlanmasında dikkat edilmesi gereken maddeler şunlardır:

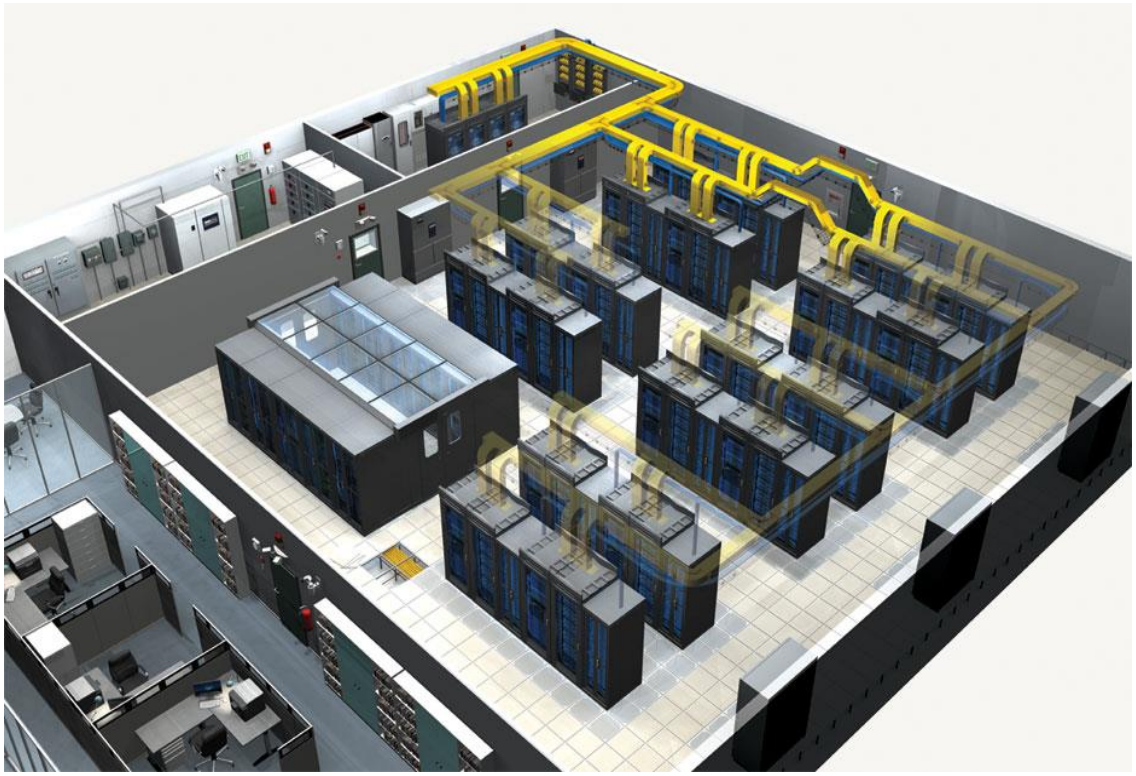
- Fiziksel alan, teknik personelin rahat çalışabilmesi için büyük tasarlanmalıdır. Zemin, tavan ve duvarlar ısı yalıtımlı olmalıdır. Ayrıca güç ve veri kablolarının rahat organize edilebilmesi için asma tavan ve zemine yükseltilmiş döşeme yapılmalıdır.
- Yedekli yapıya sahip iklimlendirme sistemleri yerleştirilmeli ve iklimlendirmenin ortamın sıcaklığına göre alarm mekanizması mutlaka olmalıdır.
- Su kaçaklarına karşın nem sensörleri ve dışarıya verilecek ses kirliliğini önleyici yalıtılmış duvarlar yapılmalıdır.
- Enerji kesintilerine karşı yedekli yapıya sahip kesintisiz güç kaynağı (UPS) bulundurulmalıdır.
- Olası yangın durumlarına karşı yangın söndürme sistemleri yerleştirilmelidir.
- Ağ ve sunucu kabinleri boyutları standartlara uygun olmalı ve akıllı PDU (Protocol Data Unit) sistemleriyle temin edilip, cihazların tükettiği elektrik, kabin ısısı ve olası bir arızanın kaynağının bilgisine hızlı şekilde ulaşılmalıdır.
- Veri merkezine girişlerin kamera ile takip edilmesi, kart, parmak izi vb. gibi yöntemlerle kontrolünün sağlanması gerekmektedir.

Fiziksel ortamı ve parçaları standartlara uygun tasarlanmış örnek bir veri merkezinin çizimi Resim 4.1'de gösterilmiştir.

Kurumsal şirketin veri merkezi, yukarıda verilen bilgiler doğrultusunda iletişim hatlarının toplandığı merkez ofis binası içerisinde bulunan bir odaya kurulumu gerçekleştirilmiştir. Cihazlar kurulum aşamasında seçilecek olan topolojiye uygun şekilde konumlandırılmıştır. Merkez ofis ve uç noktalar dâhil tüm yerleşkelerin yerel alan ağlarında yıldız topoloji tercih edilip, omurga anahtarlar üzerinden kablo dağıtımı yapılmıştır. Şekil 4.6'da merkez ofis örneğinde görüldüğü gibi omurga anahtarlar etrafında takılacak olan diğer ağ cihazları ve güvenlik duvarı mesh topoloji yapısına uygun olacak şekilde tam yedekli bir yapıda kurulmuştur. Bu sayede aktif cihazlardan birisinde yaşanabilecek olası kesintide ağ, yedek hattan hizmet vermeye devam edecektir.

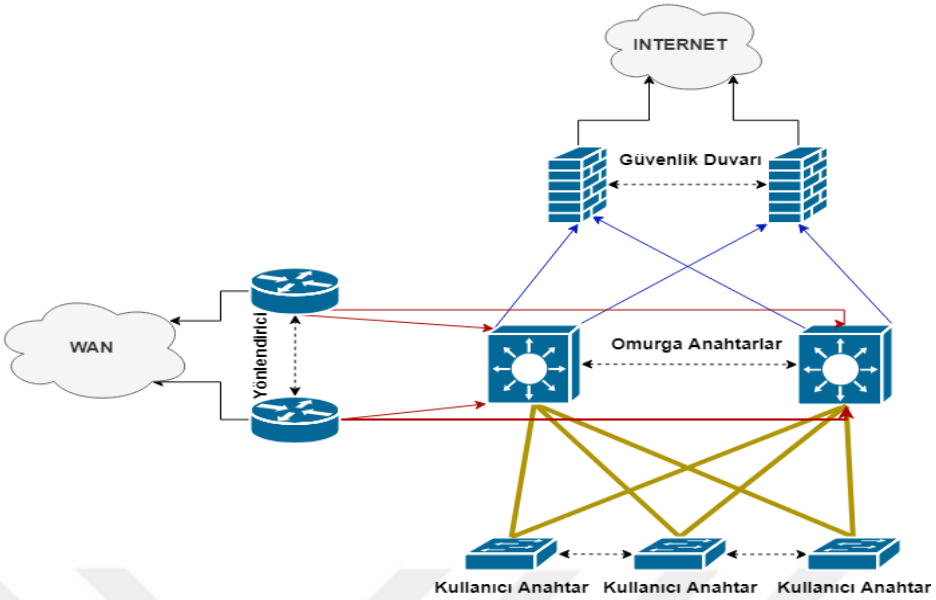
Kurulumu yapılacak olan geniş alan ağında kullanılacak olan ağ cihazları şirketin ürün alım politikası nedeniyle farklı üreticilere ait ürünlerden oluşmaktadır. Ayrıca fayda

maliyet analizi göz önüne alındığında, cihazların kurulacağı yerleşkelerdeki personel sayısı düşünülerek farklı donanım özelliklerine sahip ürünler alınmıştır. Yönlendiriciler; Cisco markasının ürün ailesinden tercih edilmiştir. Omurga anahtarlar ve kullanıcı anahtarları; merkez ofis ve İstanbul şube de Cisco marka, diğer yerleşkelerde HP marka ürünler tercih edilmiştir. Kablosuz erişim noktaları ve kablosuz denetleyiciler ise tüm yerleşkelerde Aruba markasına ait dış ve iç mekân ürünlerinden tercih edilmiştir.



Resim 4.1 Örnek veri merkezi tasarımı (İnt. Kyn. 13).

Ağdaki cihazların kurulumu aşamasında dikkat edilmesi gereken diğer bir konu da ağın parçalara bölünmesidir. Bölme işlemi VLAN teknolojisi ile yapılabilmektedir. VLAN ağda yer alan cihazların ve kullanıcıların mantıksal olarak sınıflandırılmasıdır. Resim 4.2'deki liste kurulumu yapılan geniş alan ağının VLAN sınıflarını göstermektedir. VLAN sınıfları üstlendiği hizmetler ile adlandırılarak, listeye daha sonra bakıldığında VLAN'ların daha kolay anlaşılabilir olması sağlanmıştır. Ağın parçalara bölme işlemi, ağdaki sorunları daha hızlı çözmeye ve çeşitli yönetimsel politikaların daha kolay uygulanmasına yardımcı olacaktır.



Şekil 4.6 Merkez ofisde kurulumu yapılan tam yedekli yapı.

KURUMSAL GENİŞ ALAN AĞI VLAN TABLOSU

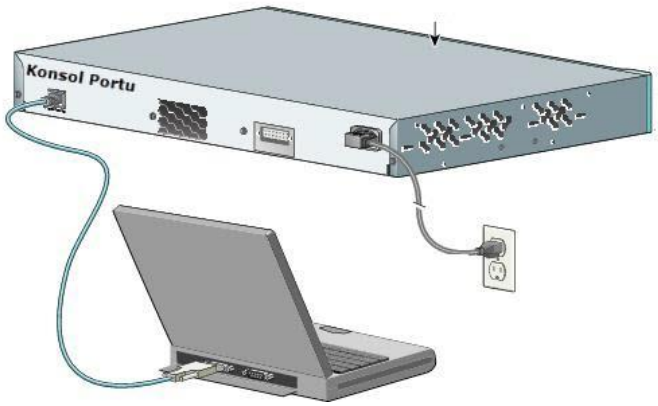
AĞ ADRESİ	AĞ GEÇİDİ	VLAN ID	VLAN ADI	VLAN İŞLEVİ
172.100.60.0/22	172.100.60.1	60	Merkez Kullanıcı	Kullanıcı VLAN
172.100.64.0/22	172.100.64.1	64	İstanbul Şube Kullanıcı	Kullanıcı VLAN
172.100.80.0/22	172.100.80.1	80	Antalya Şube Kullanıcı	Kullanıcı VLAN
172.100.84.0/22	172.100.84.1	84	Afyon Fabrika Kullanıcı	Kullanıcı VLAN
172.10.110.0/24	172.10.110.1	110	Yangın Sistemleri	Yangın Sistemleri
172.10.210.0/24	172.10.210.1	210	Misafir Kullancı	Misafir
172.10.220.0/24	172.10.220.1	220	Kablosuz Erişim Noktası	Wireless
172.10.140.0/24	172.10.140.1	140	Ağ Yönetimi	NMS-Network Mngmt-F5..
172.10.24.0/24	172.10.24.1	24	ILO	ILO Ağı
172.10.25.0/24	172.10.25.1	25	HYPERV-MGMT	Hyper-V Management / Backup
172.10.20.0/24	172.10.20.1	20	DOMAIN	Domain Servisleri
172.10.30.0/24	172.10.30.1	30	Exchange	Exchange Sunucular
172.10.90.0/24	172.10.90.1	90	VERITABANI	SQL Veritabanı
172.10.70.0/24	172.10.70.1	70	ALTYAPI-UYGULAMA	Yönetimsel Servisler
172.10.50.0/24	172.10.50.1	50	YAZICI	Yazıcı Servisleri
172.10.4.0/24	172.10.4.1	4	DOSYA VE DİĞER	Dosya ve Diğer Sunucu Servisleri
172.10.40.0/24	172.10.40.1	40	TEST-SISTEM	Sistem Test Ağı
172.10.8.0/24	172.10.8.1	8	VPN SUNUCU	Internal VPN Sunuclar
172.10.13.0/24	172.10.13.1	13	VOİCE-SERVER	Voice

Resim 4.2 Kurumsal geniş alan ağının VLAN bölümlerini gösteren tablo.

4.1.4 Cihazların Doğru Yapılandırılması

Kurulumları gerçekleştirilen ağ cihazlarının yönetimi için gerekli olan en önemli unsur ağ yönetim protokollerinin aktifleştirilmesidir. Ağ yönetim protokolü, NMS ile cihaz arasındaki iletişimi sağlayan köprüdür. Bu nedenle tüm cihazlarda aktif hale getirilmesi gereklidir. Aynı şekilde ağ hizmetini etkileyecek veya cihazların çalışmasını durduracak saldırılara karşı güvenlik önlemlerinin alınması da gereklidir.

Ağ yönetim sistemlerinin döküm oluşturma ve cihaz yönetimi için kullandığı ağ yönetim protokolleri SNMP ve RMON'dur. Ağ cihazlarında bu protokollerin tanımlaması ve aktifleştirilmesi gereklidir. Yönlendirici ve anahtar gibi aktif ağ cihazlarında bu işlem CLI ekranından yapılmaktadır. CLI ekranına, ağ cihazının uzaktan erişim arayüzünden (SSH/TELNET) veya Resim 4.3'deki gibi konsol portu üzerinden erişilebilmektedir.



Resim 4.3 Anahtar cihazına konsol portundan erişim.

Yönetilecek olan yönlendirici, omurga anahtar, kullanıcı anahtar, kablosuz denetleyici ve güvenlik cihazlarının ilk kurulumlarında aşağıdaki talimatlara uygun bir şekilde yapılandırma ayarları yapılmıştır. Kablosuz erişim noktalarında ise bu işleme gerek yoktur. Tüm kablosuz cihazlar, kablosuz denetleyici (Wireless Controller) sayesinde toplu programlanabileceğinden sadece denetleyici üzerinde bu ayarların yapılması yeterlidir. Kablosuz denetleyici cihazının bulunmaması durumunda ise tüm kablosuz erişim noktalarına yapılandırma ayarları tek tek yapılması şarttır.

Resim 4.4'de yönlendirici cihazında SNMPv2 ve SNMPv3 yönetim komutları görülmektedir. Üreticiye göre komut satırı sözdizimi farklılık gösterebilir. Ancak çalışma prensibi her zaman aynıdır.

```
yonlendirici#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
yonlendirici(config)#snmp-server community SNMPv2 rw
yonlendirici(config)#snmp-server enable traps
yonlendirici(config)#snmp-server host 172.16.100.2 version 2c SNMPv2
yonlendirici(config)#
yonlendirici(config)#snmp-server group yonetimgroup v3 priv
yonlendirici(config)#snmp-server user SNMPv3 yonetimgroup v3 auth sha Ankara2016** priv AES 128 Ankara2016**
yonlendirici(config)#snmp-server enable traps
yonlendirici(config)#snmp-server host 172.16.200.2 version 3 priv SNMPv3
yonlendirici(config)#
```

Resim 4.4 Yönlendirici cihazında SNMP versiyon 2 ve versiyon 3 yapılandırma komutları.

Sırasıyla komutlar şunlardır:

- SNMP versiyon2 de *"snmp-server community SNMPv2 rw"* komutu girilerek NMS'de kullanılacak olan SNMPv2 oluşturulur.
- SNMP versiyon3 de *"snmp-server group yonetimgroup v3 priv"* ve ardından *"snmp-server user SNMPv3 yonetimgroup v3 auth sha Ankara2016** priv AES 128 Ankara2016**"* komutları girilerek cihazda aktifleştirilir. Komutlardan da görüleceği gibi SNMPv3 de kimlik doğrulama ve şifreleme algoritması çalışmaktadır. Bu da onu SNMPv2 den daha güvenli hale getirmektedir. NMS'e veri paketlerinin şifreli gönderilmesi için SNMPv3 kullanılması her zaman önerilir.
- Hemen sonra her versiyon da *"snmp-server enable traps"* komutunun sonuna öğrenilmesi istenen durumlar (arayüz durum bilgisi, yapılandırma ayarı değiştirme, cihazda oluşan alarmlar vb.) girilerek, bu durumların bir kısmı veya tamamı aktifleştirilebilmektedir. Bunun nedeni güvenlik amaçlı, cihazdan sadece kontrolünü gerçekleştirmesini istediğimiz özelliklerin bilgisini ağ yönetim sistemine ulaştırmasını sağlamaktır.
- Son olarak güvenlik açısından önem arz eden *"snmp-server host 172.16.200.2 version 3 priv SNMPv3"* komutu girilmelidir. Bu sayede verilerin sadece ağ yönetim sistemine iletilmesi sağlanmış olacaktır.

Bir diğer ağ yönetim protokolü olan RMON ile ağ cihazlarının veya üzerlerinde bulunan port arayüzlerinden, kaynaklar izlenebilmekte ve alarm oluşması durumunda çeşitli aksiyon tetikleme mekanizmaları kullanılabilmektedir. Ayrıca RMON, SNMP ile entegre çalışabilmektedir. SNMP'de olduğu gibi cihaz CLI ekranından tanımlama yapılması gerekilmektedir. Resim 4.5'de RMON protokolüyle port arayüzleri izlenen yönlendiricinin yapılandırma komutları gösterilmektedir.

```
yonlendirici#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
yonlendirici(config)#rmon alarm 1 ifInUcastPkts.1 20 delta rising-threshold 300 1 falling-threshold 20 owner SIRKET
yonlendirici(config)#rmon event 1 log trap SNMPv2 description TRAFIK_ALARM owner SIRKET
yonlendirici(config)#
```

Resim 4.5 Yönlendirici cihazında RMON yapılandırma komutları.

Sırasıyla komutları şunlardır:

- RMON protokolünü aktif hale getirmeden önce, izlenilmesi istenen nesneye ait alarm oluşturulmalıdır. Bunun için alarm üretilmesi istenen cihaz da *"rmon alarm 1 ifInUcastPkts.1 20 delta rising-threshold 300 1 falling-threshold 20 owner SIRKET"* komutu yazılmalıdır. Bu komut sayesinde arayüz portuna 20 saniye içerisinde 300 paketin üstünde bir trafik oluşması halinde alarm vermesi sağlanmıştır.
- İkinci yapılacak işlem alarm oluşunca tetiklenecek olayın belirlenmesidir. *"rmon event 1 log trap SNMPv2 description TRAFIK_ALARM owner SIRKET"* komutuyla oluşan alarmın SNMP protokolüne bildirilmesi sağlanmaktadır.

Bu örnek dışında RMON ile farklı nesnelerin takibi ve aksiyon aldırılabilir. Üreticilerin kendi ağ cihazları için yayınlamış olduğu RMON yapılandırma kılavuzu (Configuration Guide)'ndan yapılacak işlemlere ulaşılabilir.

4.1.5 Ağ Yönetim Sistemi Yazılımı Seçimi

Ağ yönetim Sistemleri (NMS) kurumsal geniş alan ağlarının yönetimini sağlayan, ağ yöneticilerinin iş yükünü önemli ölçüde azaltan ve ağda yaşanabilecek olası sorunlara

önceden müdahale etme şansını sağlayan yazılım tabanlı araçlardır. Bu tanımdan anlaşılacağı gibi bir ağı sadece insan çabasıyla yönetmek mümkün değildir. Bundan dolayı kurumsal ağlarda mutlaka ağ yönetim sistemi kullanılmalıdır.

Ağ yönetim sistemi seçilirken ürünün hangi ölçüde, ne gibi çözümler sunduğu ve ne kadar maliyetle edinilebileceği şirketler için önem arz etmektedir. Sadece protokol tabanlı ağ etkinliklerini izleyen basit bir ürün tercih edilebileceği gibi cihazları otomatik yoklayan, dağıtılmış bir veri tabanına sahip, gerçek zamanlı grafik görünümleri üreten ve üst düzey iş istasyonlarına sahip bir ürün de tercihler arasında yer alabilir. Bunun yanı sıra ağ yönetim sistemlerinin seçiminde ücretsiz ve açık kaynak araçlar ya da ücretli ürünler tercih edilebilir. Burada dikkat edilmesi gereken fiyat ve kullanıcı tercihinin yanı sıra, tercih edilecek ağ yönetim sisteminin işlevselliği olmalıdır. Tercih edilen ağ yönetim sistemi sayesinde cihazların kullanmış olduğu kaynakların (işlemci, disk, bellek vb.) analizi yapılarak, kaynaklarının büyük bölümünü kullanmayan cihazlar tespit edilebilir. Elde edilen bilgiler sonucu, yılsonu yatırım planlamalarında gereksiz satın almalar önlenmiş olur. Cihazlarda fiziksel arızalara sebep olan yüksek ısı, güç kaynağı arızası gibi durumlara kesinti olmadan müdahale edilebilmektedir. Bu sayede verilen hizmetinin devamlılığı sağlanmış olur. Bahsi geçen bu iki durum ağ yönetim sisteminin işlevselliğini en iyi şekilde ifade etmektedir.

Bu doğrultuda doğru NMS'i seçmek, en az kaynak yatırımıyla üst düzey bir yönetim yapılmasıyla mümkün olmaktadır. Ayrıca Ağ yönetim yazılımları değerlendirilirken, aşağıdaki beş etkeni göz önünde bulundurmak önemlidir.

Kapsam: Düşünülecek ilk konu NMS'in neleri kapsadığıdır. Bunun belirlenebilmesi için aşağıdaki soruların yanıtının ağ uzmanları tarafından verilmesi gereklidir.

- Yazılım kurumsal geniş alan ağının yalnız bir bölümünde mi kullanılacak yoksa birden fazla yerde kullanılacak mı?
- NMS ile ağ cihazları dışında sunucu, servis, sanal ortamlar gibi farklı sistemler de yönetilecek mi?
- Yazılım ağda kullanılan cihazların ve bu cihazların üreticilerinin kullandığı protokollerin yönetimini destekliyor mu?

Bu soruların cevapları ile verilen kararlar, NMS'in seçimini ve değerlendirilmesini nerdeyse tüm yönleriyle etkileyecektir.

Ölçeklenebilirlik: Yıllar geçtikçe ağın sürekli genişleyeceği ve iş gereksinimlerinin artacağı düşünülerek, bununla paralel NMS'in gelişen ihtiyaçlara cevap verebilmesi gereklidir. Özellikle yazılımın kaç cihaza kadar yönetim sağlayacağı, nasıl bir teknolojiye sahip olduğu (ajanlı veya ajansız) ve yazılımın kurulu olduğu donanımın kullanabileceği kaynak (İşlemci, bellek, depolama alanı) sınırları incelenmelidir. Yapılan yatırımın uzun vade de işe yaraması için bu konu önemlidir.

Dağıtım: Tercih edilecek ürünün yerinde mi yoksa bulut ortamı üzerinden mi edinileceğine karar vermek gereklidir. Bu durum doğrudan maliyeti etkilediğinden seçim aşamasında iki seçeneğin avantajlarına ve dezavantajlarına bakmak gereklidir. NMS'i şirketin veri merkezinde bir sunucuya kurarak kullanmanın en önemli avantajı veri güvenliğidir. Şirket bilgilerinin dışarıda bir ortamda tutulmaması olası veri hırsızlıklarının önüne geçecektir. Diğer bir konu ise internet servis sağlayıcı (ISP) kaynaklı kesintilere mahal vermeden canlı ortam izleme yapılabilmektedir. NMS'i bulut tabanlı edinmenin en büyük avantajı ise maliyetlerinin yerinde kuruluma göre düşük olmasıdır. Şirket dışından, VPN hizmeti almadan tüm ağın yönetiminin yapılabilmesi de bulut tabanlı kurulumun tercih sebeplerinden birisidir.

Destek: Tercih edilecek olan ürünün üreticisi tarafından teknik desteğinin olması önemlidir. Yaşanabilecek yazılımsal hataların düzeltilmesi, güncellemeler ile yenilikler yapılması ve ihtiyaç halinde yeni araçların yazılıma dahil edilebilmesi gibi konularda gelişime ve yardıma açık bir NMS tercih edilmesi dikkat edilmesi gerekli bir husustur.

Özellikler ve Araçlar: Öncelikle ağın ve ağdaki cihazların özellikleri göz önünde bulundurularak bir araç listesi oluşturulmalıdır. Örneğin ağda bulunan yönlendirici cihazları, fiziksel portun üzerinden geçen trafik bilgilerini toplayan protokollere (Netflow) sahip olabilir. Bu durumda ağ yöneticisi hatlarının bant genişliğini tüketen uygulamaların listesini öğrenip, raporlayabilecek bir araca ihtiyaç duyulabilir. Ağ yönetim sistemlerini incelediğimiz bölümde karşılaştırılan 15 kriterden yola çıkarak

hazırlanan; bir NMS'de mutlaka olması gereken temel özellikler ve ideal bir ağ yönetim sisteminde olması gereken özelliklere göre ağ yönetim sistemi belirlenmelidir.

Ağ yönetim sisteminde olması gereken temel özellikler şunlardır:

- Görülmesi gereken her şey kolayca ulaşılabilir olmalı ve farklı yöneticiler için özelleştirilebilen kontrol ekranına sahip olmalıdır.
- Kontrolü sağlanacak ağ cihazlarının sisteme eklenmesine ve protokollerin tanımlanmasına olanak sağlanmalıdır.
- Ağ yönetim sistemi, hataları ve güvenlikle ilgili olayları bildirmek için, normal ağ işlemlerini tanıyabilmesi gereklidir.
- Ağ yönetim sistemi bir olayı rapor ediyorsa, bu bilgiler üzerinden aksiyon alabilecek araçlara da sahip olmalıdır.

İdeal bir ağ yönetim sisteminde olması gereken bazı özellikler şunlardır:

- Ağdaki cihazlar otomatik olarak keşfedilebilmelidir. Bunu yapabilmek için ürünlerde IP adres aralığı belirlenerek çeşitli dosya formatlarında (xml, xls, cvs vb.) döküm girişi yapılarak tanımlama yapılabilmelidir.
- Yapılandırmaları içe aktarma ve analiz etmeye olanak sağlamalıdır. Ağı yapılandırmak ve optimize etmek çok uzun süreler alabilir. Dolayısıyla yanlış bir yapılandırma neticesinde çalışmaların tümü kaybedilebilir. Bu özellik mevcut yapılandırmaları, cihaz politikalarını sorunsuz bir şekilde ağa bütünleştirmeyi ve yapılandırmaları gerektiğinde orijinal ayarlarına döndürülmesini sağlar.
- Etkili bir ağ yönetim sistemi ağ yöneticisine zaman kazandırmalıdır. Birden fazla cihaza uygulanacak yapılandırma ayarına kural yazılarak, zaman ve kaynaklar diğer işlere ayrılabilir. Kurallar bir kez hazırlandıktan sonra, güncellenebilmelidir. Güncelleme zamanlarının düşük ağ trafiği dönemlerinde olması, verilen hizmetin kesintiye uğramaması için önemlidir. Bu yüzden ağ yönetim sisteminde kural yazma aracı ve zamanlama özelliği olmalıdır.
- Kurallara dayalı denetim mekanizması olmalıdır. Bu özellik, düzenli olarak yapılan tüm yapılandırmaların ağ için belirlenmiş standartları karşıladığını doğrular. Aynı zamanda ağdaki hataları ve tutarsızlıkları tespit eder. Bunun örneği

sistem içinde bir alarm oluşması sonucunda e-posta veya cep telefonlarına uyarı gönderme yeteneğidir.

- Gerçek zamanlı veri toplama ve raporlama özelliği olmalıdır. Sağlıklı bir ağın korunmasında sürekli veri toplama ve bunları ağ yöneticisine raporlama yeteneğinin bulunması çok önemlidir. Performansla ilgili sorunları tespit etmek için, ağı gerçek zamanlı izleyip bu verilerin diğer ağ olaylarıyla ilişkilendirilmesi gerekmektedir. Elde edilen bu raporlar, ağ sorunlarının iş süreçleri üzerindeki etkilerini değerlendirmek için, sorumlu ağ yöneticilerine iletilmelidir.

Farklı üreticilere ait incelenen ücretli-ücretsiz NMS çözümleri ve yukarıda ağ yönetim sistemini seçmemizde yol gösteren beş etken göz önüne alınarak, örnek kurumsal geniş alan ağımızı yönetmek için iki farklı ağ yönetim sistemi seçilmiştir. Bu ürünler Cisco Prime ve Solarwinds'dir. Tercihin bu iki ürün üzerinde yapılmasına maliyet, yazılımların özeliklerinin geniş alan ağının yönetimini karşılayacak olması, ağdaki büyümeye uygun güncellenebilmeleri, NMS'de olası bir problemde destek alınabilecek karşı muhatabın bulunması ve solarwinds özelinde bulut tabanlı edinilebilmeye imkân sağlaması gibi etkenler neden olmuştur.

Kurulumunu gerçekleştirdiğimiz geniş alan ağında yönlendirici cihazların tümünün, merkez ofis ve İstanbul şubedeki anahtar cihazlarının Cisco marka olması ve bu cihazlardaki Cisco'ya özel protokollerin (EIGRP, HSRP, CDP vb.) diğer NMS ürünleri tarafından desteklenmemesi nedeniyle 100 cihaz lisanslı, yerinde kurulum yapılacak şekilde Cisco Prime ağ bileşenleri yönetim yazılımı satın alınmıştır.

Cisco Prime'ın kendi ürünleri dışındaki ağ cihazları, sunucu sistemleri ve güvenlik cihazlarının yönetimini etkili bir şekilde yapamaması nedeniyle diğer yerleşkelerde kullanılan HP marka anahtar cihazlarının, Aruba marka kablosuz cihazlarının ve projeye sonradan dâhil edilmesi ihtimaline karşın sunucu yönetimi, son kullanıcı yönetimi, ağ bant genişliği yönetimi gibi farklı yönetimsel modülleri ayrı ayrı satın alma imkanı sağlayan Solarwinds ağ yönetim sistemi 500 cihaz lisanslı, ağ ile ağ yapılandırma modülleri içerecek şekilde satın alınmıştır. Solarwinds farklı olarak bulut tabanlı kullanılması ön görülmüştür. Maliyet açısından yerinde kuruluma göre daha uygun

olması ve yönlendirici cihazları ile merkez ofisdeki veri merkezinde bulunan omurga anahtarları gibi kritik öneme sahip cihazların Solarwinds ile yönetilmeyecek olması bulut tabanlı kurulumun tercih edilmesini sağlamıştır. İncelenen diğer benzer özelliklere sahip ücretli ürünlerin tercih edilmemesinin nedeni ise bulut tabanlı kuruluma imkân verilmemesi ve maliyetlerin şirket bütçesini aşan yüksek rakamlara çıkmasıdır. Ayrıca ücretsiz ürünlerin tercih edilmemesinin en büyük nedeni ağın yönetimi için gerekli ihtiyaçları karşılayacak tüm araçların bulunmaması ve teknik destek verebilecek bir üreticinin bulunmamasıdır.

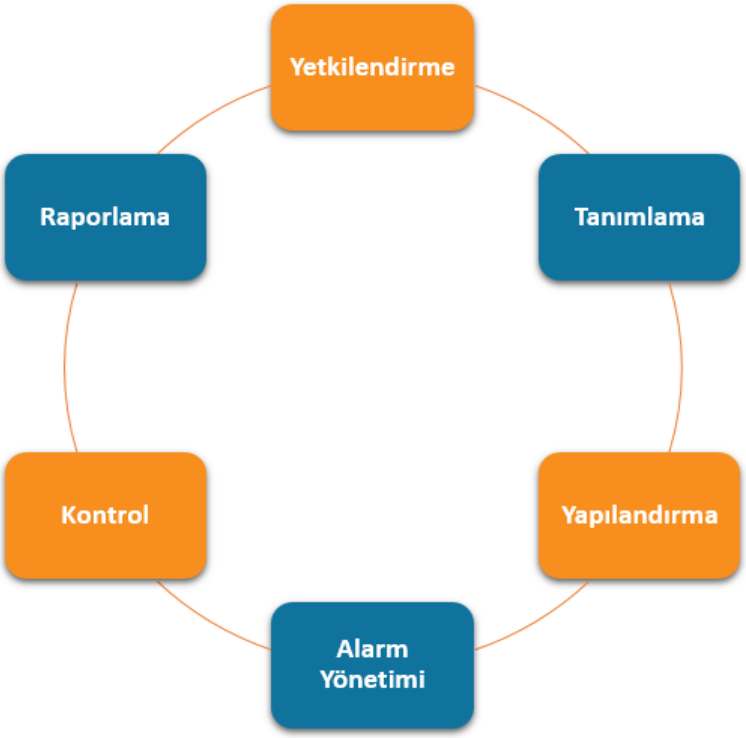
4.1.6 Ağ Yönetim Sistemi Kurulumu

Ağ yönetim sistemi üreticileri üç farklı şekilde kurulum hizmeti sunmaktadır. Birincisi donanım olarak içerisinde tüm yazılımlar yüklü şekilde verilen donanım (appliance) kutularına (Resim 4.6), ikincisi sanallaştırma teknolojisi(Hyper-v, Vmware) aracılığıyla şirketin sunucularına, son olarak bulut teknolojisi aracılığıyla üretici firmanın sunucularına kurulum yapılarak NMS kullanılabilmektedir.

Tercih edilen ağ yönetim sistemlerinden Cisco Prime, üretici tarafından hazırlanan donanıma kurulumu yapılarak; tercih edilen diğer bir ağ yönetim sistemi olan Solarwinds ise bulut tabanlı olarak herhangi bir ilk kurulum yapılmadan üretici sunucularına internetten bağlanılarak kullanıma hazır hale getirilmiştir. NMS'e erişim sağlandıktan sonra gerekli yönetimsel işlemleri yapmadan önce, alarm yönetiminde yöneticileri bilgilendirmek için gerekli mail protokolünün (SMTP) tanımlaması, cihazların keşfinde kullanılacak kimlik bilgilerinin(SNMP, Windows) eklenmesi ve kişisel özelleştirmeler (menüler, renk vb.) gibi yazılımın ana ayarları her iki üründe de hazır hale getirilmiştir.

Resim 4.6 Ağ yönetim sistemi cihaz kutusu (İnt. Kyn. 14).

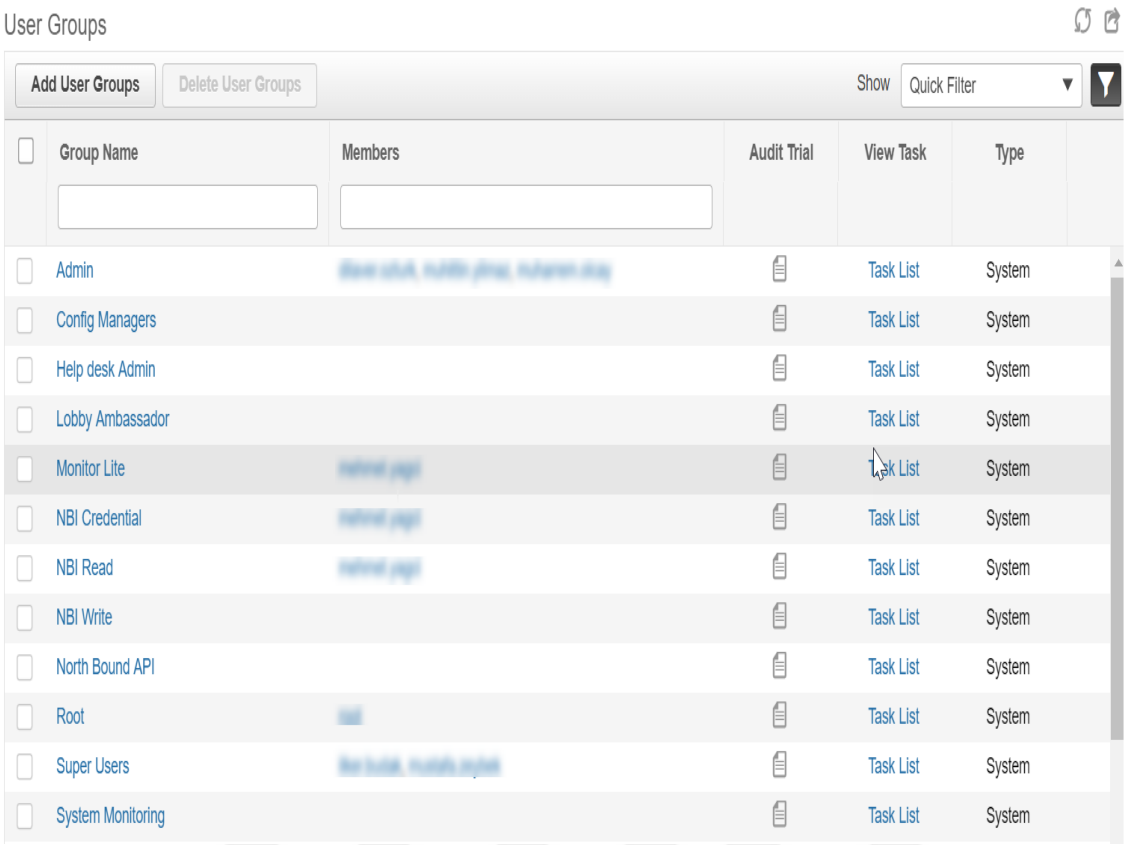
Ağ yönetim sistemini temel ayarları yapıldıktan sonra hesap, hata, yapılandırma, performans ve güvenlik yönetimleri için yapılması gerekli işlemler bulunmaktadır (Şekil 4.7). Bu işlemeler eksiksiz yapılması halinde, ağ yöneticilerin iş yükü büyük ölçüde azalacak, ağda yaşanacak sorunlar hızlı çözümlenecek, kurumsal sistemlerin güvenliği sağlanacak ve kaynakların performansı verimli kullanılacaktır. Aşağıda listelenen tüm işlemler hem Cisco Prime için hem de Solarwinds için yapılmıştır.



Şekil 4.7 Ağ yönetim sistemi kurulum aşamaları.

4.1.6.1 Yetkilendirme

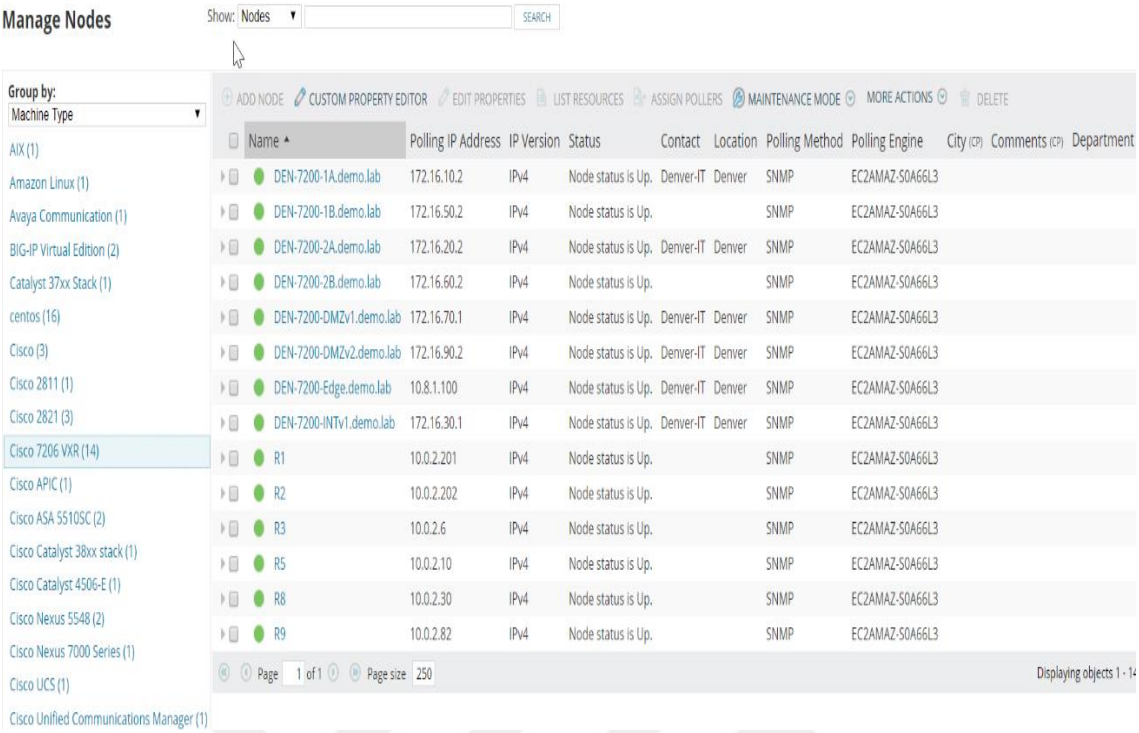
Ağı yöneten her bir kullanıcı için farklı giriş hesabı açılıp, sistemde sorumlu olduğu alanlara yetkilendirilmiştir. Bunu yaparken Resim 4.7'de görüldüğü gibi ana yönetici, yapılandırma yöneticisi, sunucu yöneticisi, izleme gibi kullanıcı grupları oluşturulup, NMS'e erişecek kullanıcıların yazılım içerisinde yapabilecekleri işlemler kısıtlanmıştır. İş paylaşımının doğru yapılması, oluşacak alarmların yetkili yöneticiye yönlendirilmesi ve NMS ayarlarında yanlış değişikliklerin önüne geçilmesi açısından gerekli bir işlemdir.



Resim 4.7 Kullanıcı yetkilerinin belirlendiği grup listesi (Cisco Prime).

4.1.6.2 Tanımlama

IP tanıtılması, VLAN yapılandırmaları ve protokolleri hazır hale getirilen aktif cihazlar (yönlendiriciler, anahtarlar vb.) otomatik keşif özelliğiyle kısa bir sürede NMS'e öğretilmiştir. Döküm taraması yapılan cihazların yönetimin de kolaylık sağlaması amacıyla üretici, cihaz türü, bulunduğu konum, durum bilgisi (açık/kapalı) gibi belirleyici gruplara ayrılmıştır (Resim 4.8). Bu örnek ağın yönetiminde kullandığımız her iki NMS bu özelliği desteklemektedir. Ancak kullanılan NMS otomatik olarak bu işlem yapmıyorsa, mutlaka yönetici tarafından gruplandırılmalıdır. Bu işlem sayesinde cihazlara toplu yapılandırma ayarı gönderilirken ve kontrol ekranı hazırlanırken yapılacak işi hızlandıracaktır.

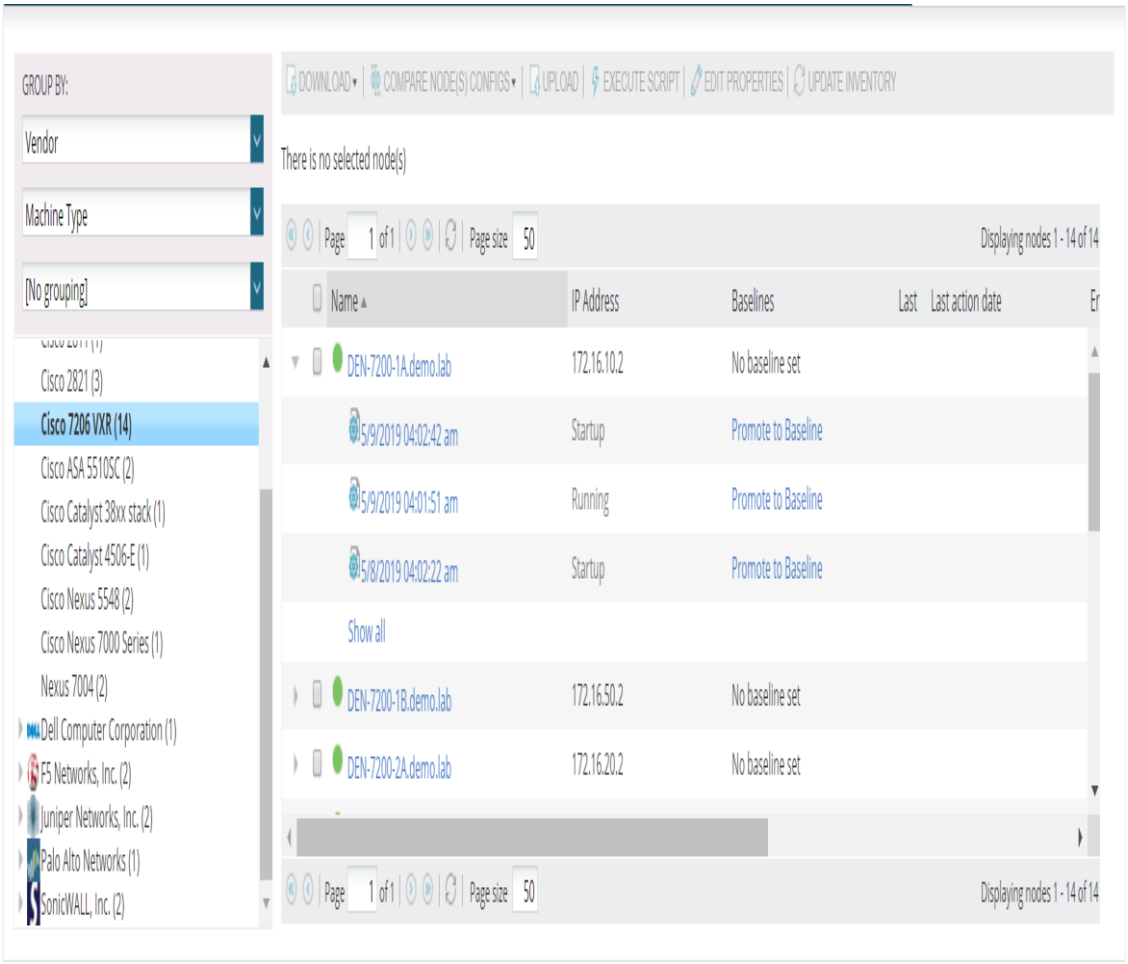


Resim 4.8 Yönetilen cihazların gruplandığı liste (Solarwinds).

4.1.6.3 Yapılandırma

Ağ cihazlarının yapılandırma ayarları organize edilmiştir. Cihazların belli aralıklarla ve ayarlarda yapılan değişikliklerden sonra otomatik yedeklerinin alınması sağlanmıştır. Alınan yedekler Resim 4.9'daki gibi kayıt altında tutulup, her iki NMS'inde yedekten geri dönme (recovery) özelliği sayesinde ihtiyaç halinde yapılandırma ayarlarının tekrardan yüklenmesi hazır hale getirilmiştir.

Güvenlik yönetimi için gerekli yapılandırma ayarları tüm cihazlara uygulanmalıdır. Tek tek tüm cihazlara bu yapılandırmaları yapmak yerine toplu yapılandırma yükleme özelliği kullanılarak cihazların tümüne şifre verilmesi, telnet bağlantısının kapatılması, cihazlara yetkisiz erişim veya ağda yaşanabilecek sızmalara karşı MAC ve IP adresi tabanlı saldırıları önleyici ayarların yüklenmesi kısa sürede tamamlanmıştır. Çizelge 4.1'de olası saldırılara karşı cihazlarda alınması gereken önleyici yapılandırma ayarları listelenmiştir.



Resim 4.9 Ağ cihazlarının yapılandırma yedeklerinin tutulduğu ekran (Solarwinds).

Çizelge 4.2 MAC ve IP adresi tabanlı saldırılara karşı alınacak önlemler.

Saldırı	Açıklama	Önleyici Ayar
LLDP, CDP Manipülasyon	Bu protokollere ait paketler, anahtar ve yönlendirici cihazların tüm portlarında etkindir. Araya girecek zararlı bir cihaz ağ ile ilgili tüm bilgilere ulaşır.	Yönetim dışı tüm portlarda CDP ve LLDP devre dışı bırakmak.
VTY Hattı Saldırısı	Cihazlara kullanıcı adı, parola verilmemesi ve Telnet bağlantısı ile uzak bağlantıya izin verilmesi yetkisiz erişimlere neden olur.	Parola verilmesi ve SSH protokolünü aktifleştirmek.

Çizelge 4.2 (Devam) MAC ve IP adresi tabanlı saldırılara karşı alınacak önlemler.

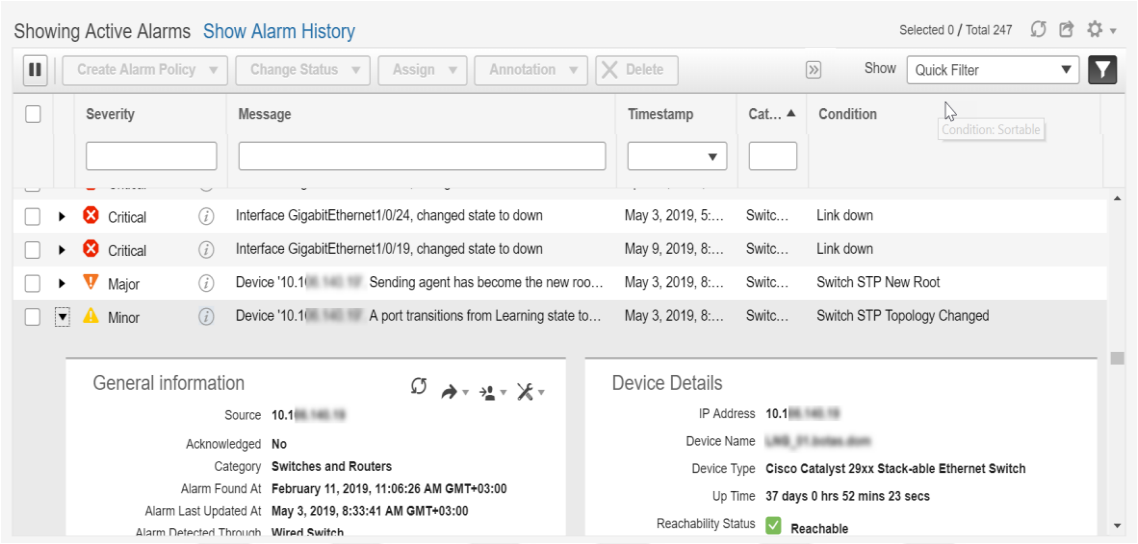
Mac Taşması	Yetkisiz bir kullanıcının anahtar cihazındaki MAC adresi tablosunun üst satırını doldurarak, anahtarı hub mantığıyla çalıştırarak ağ trafiğini inceleyebilmesine imkan sağlar.	Port Security yapılandırması uygulamak.
DHCP Aldatma	Saldırı yapan bilgisayar ağda kendini varsayılan ağ geçidi olarak tanıtması sonucu DHCP isteklerini öğrenir.	DHCP Snooping yapılandırması uygulamak.
ARP Aldatma	Saldırı yapan bilgisayarın tüm isteklere hedef MAC adresi olması sonucu ağdaki tüm paketleri	Dinamik ARP kontrolü (DAI) etkinleştirmek.
STP Saldırısı	Saldıran cihaz STP topolojisini bozmak için kendisini ana köprü yaparak ağdaki paketleri öğrenir.	Root Guard yapılandırması uygulamak.

4.1.6.4 Alarm Yönetimi

Problemlere hızlı müdahale edilmesi, çoğu zaman problemin krize dönüşmeden engellenmesini sağlar. Bu da yaşanabilecek problemlerin önceden tahmin edilerek, çözümüne yönelik planlama yapılmasıyla başarılabilir.

İşe ağda yaşanabilecek hataların, NMS'e tanımları yapılarak başlanmıştır. Cihazlardan herhangi birisine yetkisiz giriş denemesi sonucu oluşan alarm ile geniş alan ağı hat trafiğinde yaşanan kesinti sonucu oluşan alarmın önem derecesi farklı olmalıdır (Resim 4.10). Bunun için alarmlar önem derecesine göre gruplara (kritik, önemli, uyarı) ayrılarak hata yönetimi kolaylaştırılmıştır. İkinci olarak alarm eşik değerleri girilmiştir. Özelliklede cihaz kaynak kullanım durumlarında(işlemci, bellek, ısı) eşik değerleri oluşturularak, donanımların zarar görmeden müdahale edilmesi sağlanmıştır. Son olarak alarm oluşması

anında, NMS'in yapması gerekli olayların (sorumlu birim yöneticilerine bildirimin sağlanması, ağ cihazı üzerinde yapılandırma değişikliğinin yapılması, port arayüz durumunun değiştirilmesi vb.) kuralları oluşturulmuştur. Bu kurallar bir yöneticinin yapması gerekli işlemleri NMS'e yaptırarak anında müdahale edileceğinden, hizmet kesintisine uğramadan hatalar giderilecektir.



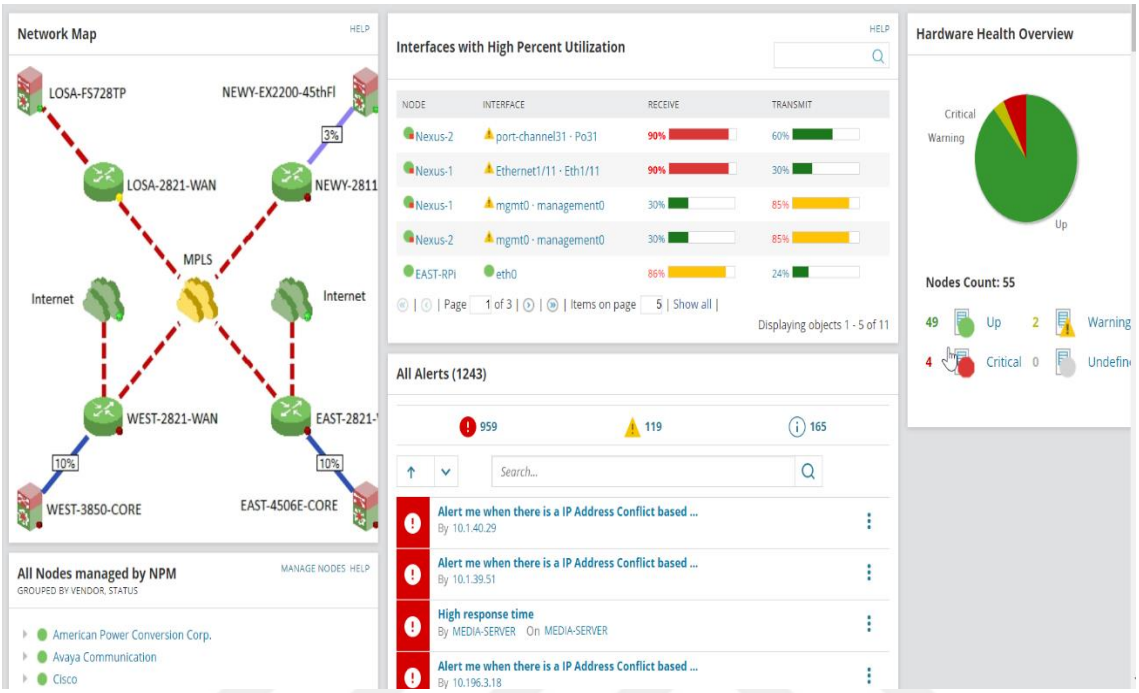
Resim 4.10 Hataların kritiklik seviyesine göre bildirildiği alarm mekanizması (Cisco Prime).

4.1.6.5 Kontrol

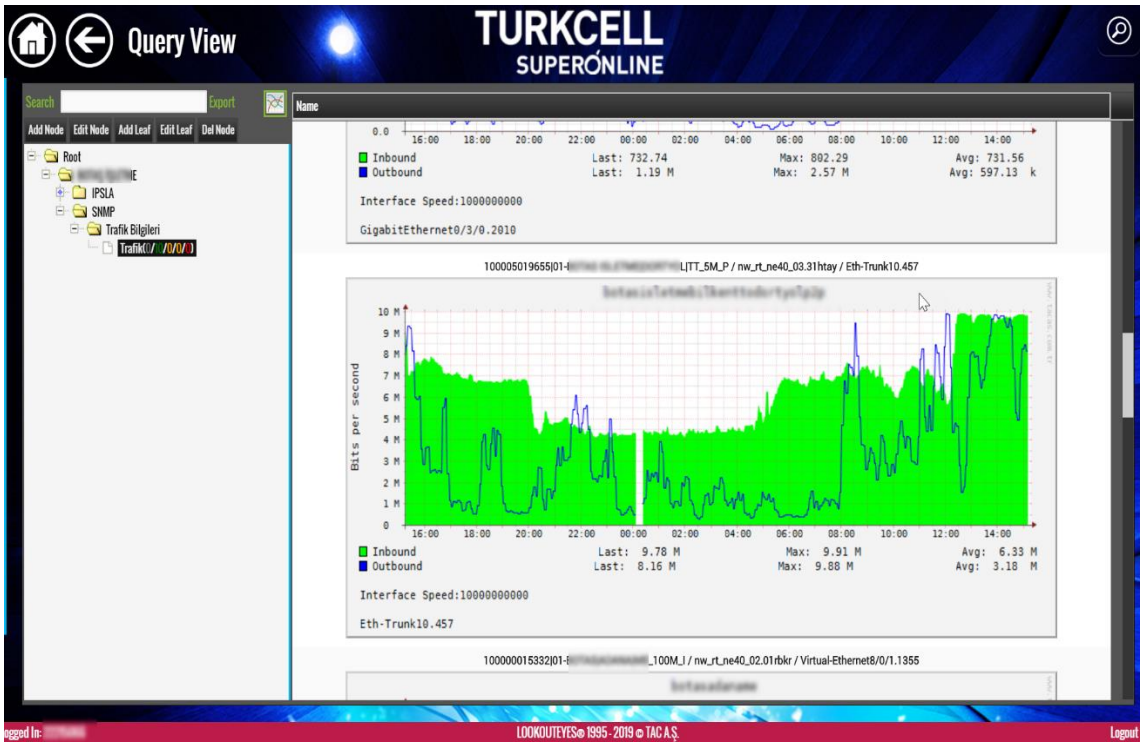
Cihazların durumu, alarm bildirimleri ve ağda yaşanan tüm olayların takibi için kontrol ekranı hazırlanmıştır. Resim 4.11'de hazırlanan kontrol ekranında görüldüğü gibi görüntülenmesi önem arz eden nesnelerin alarm bildirimleri, bilgi grafikleri ve görselleri hazır hale getirilmiştir. Yönetici için görülmesi gereksiz olan bilgiler ekran üzerinden kaldırılmıştır. Her iki NMS için hazırlanan kontrol ekranının sürekli açık olacağı bir monitör yöneticinin görebileceği bir yere konumlandırılarak tüm olayların görüntülenmesi sağlanmıştır.

Merkez ile uç noktalardaki yerleşkeler arasında bulunan iletişim hatlarının bant genişliği kontrolü de sağlanmalıdır. Ancak kullanılan hatların kiralık (metro ethernet) olması durumunda, cihazların hizmet sağlayıcı şirkete ait olacağından, NMS ile kontrolün

yapılması mümkün değildir. Bu işlem Resim 4.12'deki gibi kiralanan hattın hizmet sağlayıcısının izleme araçlarıyla yapılmıştır.



Resim 4.11 Ağın durumu, oluşan alarmlar gibi bilgilerin bulunduğu kontrol ekranı (Solarwinds).



Resim 4.12 Kiralık hatların bant genişliği kullanımını gösteren kontrol ekranı.

4.1.6.6 Raporlama

Ağ ve sistemlerle ilgili günlük, haftalık, aylık raporlar ve sistem log kayıtları dosya sunucularına yedeklenerek, yetkili yöneticilere mail yoluyla gönderilmesi sağlanmıştır. Bu raporlar sayesinde yöneticilerin geçmişte oluşan hataların, olayların bilgisine ve yapılan işlemler hakkında bilgi alması sağlanmıştır. Raporlama yapılırken özellikle cihazların, hatların ve uygulamaların kaynak kullanımına yönelik şablonlar hazırlanmıştır (Resim 4.13). Bu şablonlardan elde edilecek veriler ağın performansının takibi ve alınacak tedbirlerin yol haritasının belirlenmesi için önemlidir.

Device Health

Cisco Prime
Infrastructure

Generated: 2019-Jun-20, 16:04:24 EET

Report By: Devices By Groups
Groups: Location/All Locations
Reporting Period: Last 7 Days
Show: Up to 10 records

Top Device CPU Utilization

Device IP Address	Device Name	Cpu Instance	Min CPU (%)	Max CPU (%)	Avg CPU (%)
[redacted]61.195	[redacted]	1	38	90	43
[redacted]61.182	[redacted]	1	37	87	42
[redacted]61.186	[redacted]	1	38	55	40
[redacted]61.181	[redacted]	1	38	66	40
[redacted]61.197	[redacted]	1	38	66	40
[redacted]61.201	[redacted]	1	37	53	40
[redacted]140.13	[redacted]	1	38	44	40
[redacted]61.183	[redacted]	1	38	52	39

Resim 4.13 Son bir haftada en çok işlemci tüketen cihazların rapor şablonu (Cisco Prime).

4.2 Gerçekleştirilen Kurumsal Ağ Yönetim Sisteminde Elde Edilen Sonuçlar

Kurumsal ağın anlatılan talimatlar doğrultusunda kurulup, ağ yönetim sistemiyle bütünleştirilmesiyle zaman, iş gücü, maliyet, güvenlik, kaynak kullanımı gibi ağın işleyişini sağlayan birçok etkende fayda sağlanmıştır. Çizelge 4.3'de özet bir tabloda yapılan işlemler ve sağlanan faydalar gösterilmiş olup, kurumsal geniş alan ağının tasarım ve yönetim bölümlerinde elde edilen sonuçlar, ağ ihtiyaçlarını organize etmemizi yarayan hata, yapılandırma, hesap, performans ve güvenlik yönetimleri göz önüne alınarak detaylıca değerlendirilecektir.

Çizelge 4.3 NMS kurulumunda yapılan işlemlerden elde edilen sonuçlar.

Yapılan İşlemler	Sonuçlar
Veri merkezi düzenlemeleri	Yönetilecek cihazların kurulumu yapılacağı ortam standartlara uygun bir şekilde hazırlanarak, çevresel ve fiziksel unsurlardan kaynaklı veri kayıpları, donanım arızaları önlenmiştir.
Yedekli kurulum	Donanımların ve hatların tam yedekli yapıda kurulumlarının gerçekleştirilmesi ağda yaşanabilecek olası hatalarda hizmetlerin sürekliliğini sağlamıştır. Bu durum yöneticilere hem problemlerin çözümünde zaman kazandırmış hem de maddi kayıpların önüne geçmiştir.
Cihazlara doğru yapılandırma ayarı yapma	Ağ cihazlarının yönetimi için yapılması gerekli yapılandırma ayarları; NMS'in donanımlar ile iletişim kurmasını sağlamak ve ağ yönetim protokollerinden kaynaklı olabilecek siber tehditleri önlemek için yapılmıştır.
Ağ topolojileri oluşturma	Hazırlanan fiziksel ve mantıksal topolojiler ağın bilinirliğini sağlamıştır. Ağa eklenecek yeni bir donanım veya yeni bir LAN yapılanmasının kurulumunda, yöneticilere yol gösterici bir rehber olmasıyla, zamandan ve iş gücünden ciddi bir kazanım elde edilmiştir.
Toplu döküm tarama	NMS kurulurken ilk yapılan işlem, ağın ve cihazların yazılıma tanıtılması olmuştur. Bu işlem toplu yapılmasıyla saatler sürecek bir işlem, çok kısa sürede gerçekleştirilmiştir.
Yönetilecek cihazları gruplama	Cihazlar; anahtar, yönlendirici, kablosuz erişim cihazı; ağ sistemleri, güvenlik sistemleri, sunucu sistemleri gibi çeşitli kategorilerde gruplandırılarak yapılandırma, alarm, raporlama aşamalarında yöneticilerin işi kolaylaştırılmıştır.

Çizelge 4.3 (Devam) NMS kurulumunda yapılan işlemlerden elde edilen sonuçlar.

Toplu yapılandırma ayarı yükleme	Aynı işlevi yerine getiren ve mevcut ayarları benzer olan cihazlara tek seferde yapılandırma ayarı yüklenmesiyle, binlerce cihaza ayrı ayrı işlem yapma yükü ortadan kaldırılmıştır.
Güvenlik yapılandırmaları hazırlama	Toplu yapılandırma ayarı yüklemenin bir parçası olan bu işlem sayesinde özellikle yönlendirici ve anahtar cihazları üzerinden yapılabilecek siber tehditler önlenmiştir.
Yapılandırma ayarı yedekleri alma	Ağ cihazları ve sistemlere olası saldırı tehditlerini engellemek için kullanılan güvenlik cihazlarının yapılandırma ayarları yedeklerinin alınması ve bu yedeklerden ihtiyaç halinde geri dönülebilmesi sağlanarak, yanlış yapılandırmaların yüklenmesi sonucu oluşacak hizmet kesintilerinin önüne geçilmiştir.
Kritiklik seviyesi ve eşik değeri belirleme	Oluşan hatalar önem derecesine göre yöneticilere yönlendirilerek gereksiz alarmların önü kesilip, önem arz eden problemler öne çıkarılmıştır. Cihazların kullandıkları kaynaklara ve kullanıcıların kullandıkları hatlara eşik değerleri girilip takibi yapılmasıyla, oluşabilecek donanım arızalarının ve hat bant genişliği doygunluğunun (saturation) önüne geçilmiştir. Tüm bu işlemler hata oluşmadan önce yöneticilerin problemi çözmelerine imkan sağlamıştır.
Alarm kuralları yazma	Oluşabilecek hatalara yönelik yapılacak aksiyonlar önceden kurallar ile belirlenerek, yönetici kontrolünden bağımsız ve hatalar krize dönüşmeden otomatik giderilmiştir.
Kullanıcı grupları oluşturma	NMS'i kullanan yöneticilerin yetkileri belirlenerek, erişebilecekleri özellikler ve görebilecekleri alanlar kısıtlanmıştır. Yapılan bu işlem alarm bildirimi, kontrol ekranı düzenlemesi ve rapor dökümlerinde yönetimi kolaylaştırmıştır.

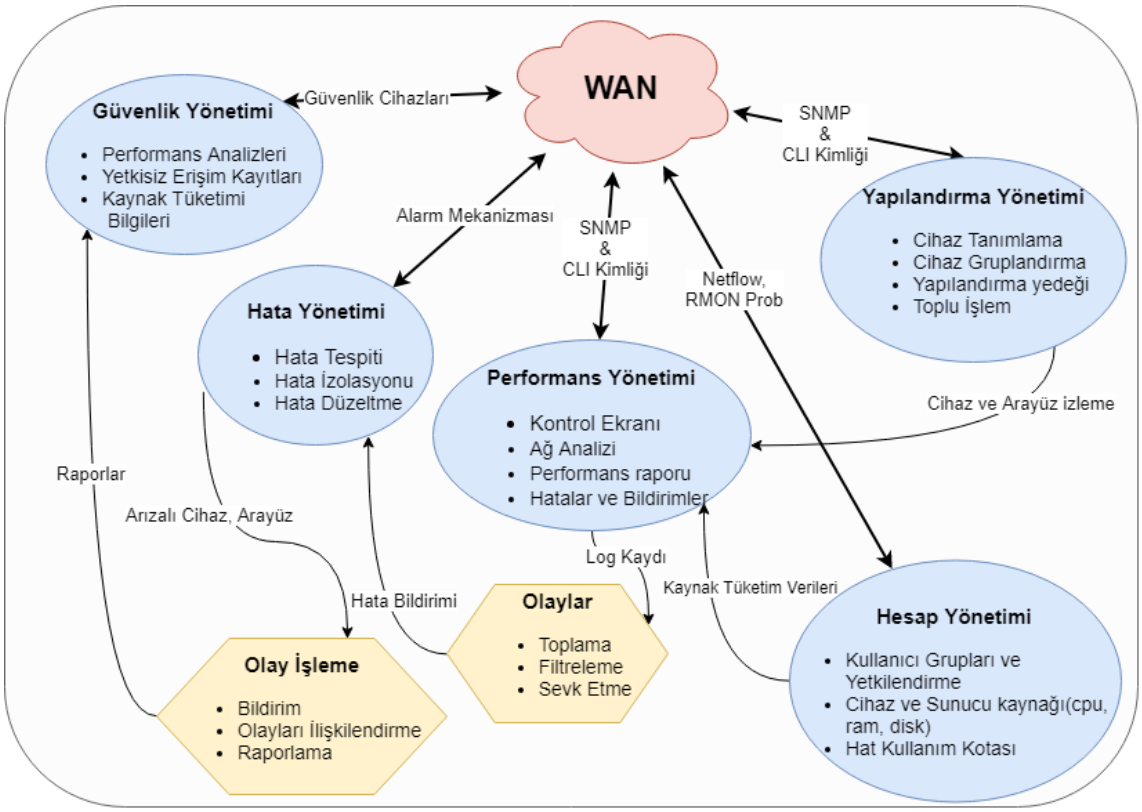
Çizelge 4.3 (Devam) NMS kurulumunda yapılan işlemlerden elde edilen sonuçlar.

Kontrol ekranı düzenleme	NMS'in görünen yüzü olan kontrol ekranı, performans verileri, kaynak tüketim değerleri, alarm bildirimleri ve çeşitli topolojik görsellerle düzenlenerek, yöneticilerin ağı ve ağda oluşan olayların anlık takibini yapabilmeleri sağlanmıştır.
Cihaz log kayıtları tutma	Ağ cihazlarında; donanım arızaları, yapılandırma ayarı değişiklikleri veya yetkisiz erişimler olması halinde işletim sistemleri tarafından oluşturulan log kayıtlarının NMS'de kayıt altına alınmasıyla, ağda oluşan hatanın hangi etkenden kaynaklandığının bulunması kolaylaşmış ve dolaylı yoldan yöneticilerin sorun giderme süreleri kısalmıştır.
Rapor şablonları hazırlama	Performans verileri, kaynak kullanım bilgileri, hata istatistikleri raporlanarak, yöneticilerin ağ ve sistemler hakkında geçmişe dönük günlük, haftalık, aylık, yıllık detaylı bilgiler almaları sağlanmıştır. Bu raporlar doğrultusunda şirketlerin yatırım maliyetlerini doğrudan etkileyecek veriler elde edilmiştir.

Öncelikle geniş alan ağının doğru kurulmasıyla olası fiziksel ve donanımsal sorunlarından kaynaklı hizmet kesintilerini azaltacak işlemler yapılmıştır. Bu işlemler sayesinde:

- Yedekli kullanılmış ağ cihazları ve iletişim hatları sayesinde, cihazlardan veya hatlardan birisinin arızalanması durumunda yedek üzerinden veri trafiğinin devam etmesi sağlanmıştır.
- Ağın fiziksel ve mantıksal topolojilerinin hazır hale getirmesiyle, donanım bağlantılarının ve çalışma trafiğinin bilinirliği güncel tutulmuştur. Olası problemlerde, ağın durumu hakkında kişiden bağımsız bir öğrenme sağlanmıştır.
- Veri merkezin de yapılan gerekli düzenlemeler sayesinde, çevresel faktörlere karşı (yangın, güç kesintisi, su kaçağı vb.) önlemler alınmıştır. Ayrıca veri merkezine konulan akıllı PDU sistemleriyle, arızanın tespiti hızlandırılmıştır.

Şekil 4.8'deki şemada görüldüğü gibi birbiriyle doğrudan ilişkisi bulunan işlemlerin gerçekleştirilmesi sonucunda NMS'in kurul aşaması tamamlanmıştır. Yapılan işlemler ve elde edilen sonuçlar şemada görülen beş temel bölüm üzerinden aşağıda anlatılmıştır.



Şekil 4.8 Ağ yönetimi kurulum aşamasında bölümlerin birbiriyle ilişkisi.

Hata Yönetimi: Hazırlanan alarm mekanizması aracılığıyla hata yönetiminin üç temel aşaması (Şekil 4.9) başarıyla gerçekleştirilmiştir.

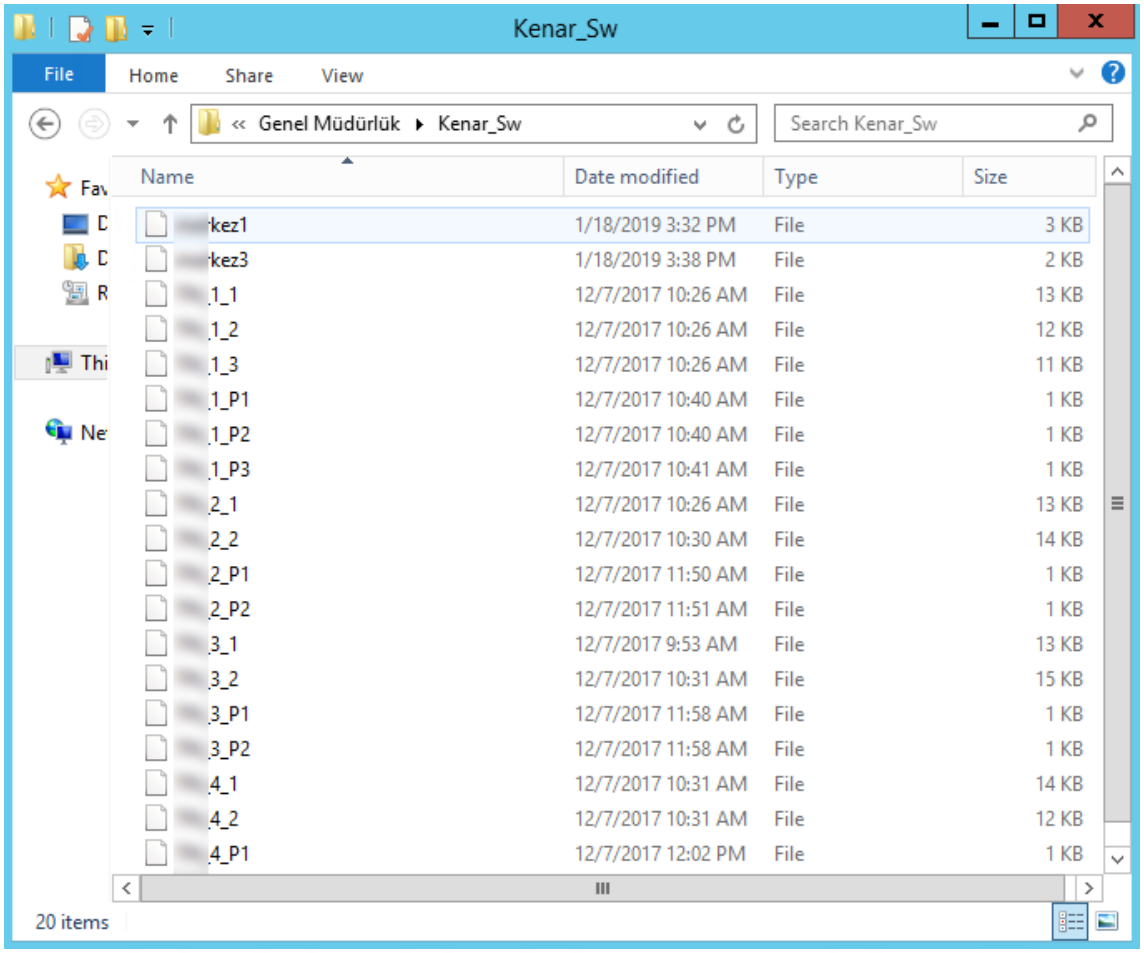
Şekil 4.9 Hata yönetimi aşamaları.

Alarm mekanizması devreye alınmasıyla;

- Girilen eşik değerleri ve kritiklik seviyesine göre alarm bildirimi sayesinde hata tespiti başarıyla yapılmış olup, oluşabilecek sorunlar önceden çözümlenmesi sağlanmıştır.
- Cihazlarda ve hatlarda yapılan yedeklik sayesinde, arızalı bölüm devre dışı bırakılıp yedek üzerinden veri trafiği sağlanarak hata izole edilmiştir.
- Planlanıp, oluşturulan alarm kuralları ve yöneticilere anlık bildirim yapılması sayesinde oluşan sorunlar krize dönüşmeden ortadan kaldırılmıştır.

Yapılandırma Yönetimi: Yapılandırma ayarı yöneticinin ağın kurulumunda en fazla zaman harcadığı ve hataya düşebildiği bölümdür. Yapılandırma adımında yapılan işlemler vasıtasıyla;

- Cihazlar kurulum aşamasında ağ yönetimi için gerekli protokol yapılandırmaları yapılarak NMS'in cihazlara güvenli erişimi sağlanmıştır.
- Yönetilecek cihazlar tanımlandıktan sonra gruplara ayrılarak, toplu yapılandırma ve kontrol ekranı düzenlemesi aşamalarında yöneticilere kolaylık sağlanmıştır.
- Ağdaki cihazların yapılandırma ayarlarının yedekleri alınıp, arşivlenmiştir (Resim 4.14). Bu sayede cihaz yapılandırmasında olası bir değişiklikte yapılacak hata sonucu, eski ayarlara geri dönmesi sağlanmıştır.
- Aynı işi yapan cihazlarda (kullanıcı anahtarları, kablosuz erişim noktaları vb.), benzer ayarların toplu yapılandırılması yapılarak, insan kaynağı ve zamandan tasarruf edilmiştir.
- Yönetilen cihazlara IP ve MAC adresi tabanlı yapılabilecek saldırıları önleyici yapılandırma ayarları sayesinde, dışarıdan gelebilecek yetkisiz erişimlere ve siber saldırılar engellenmiştir.

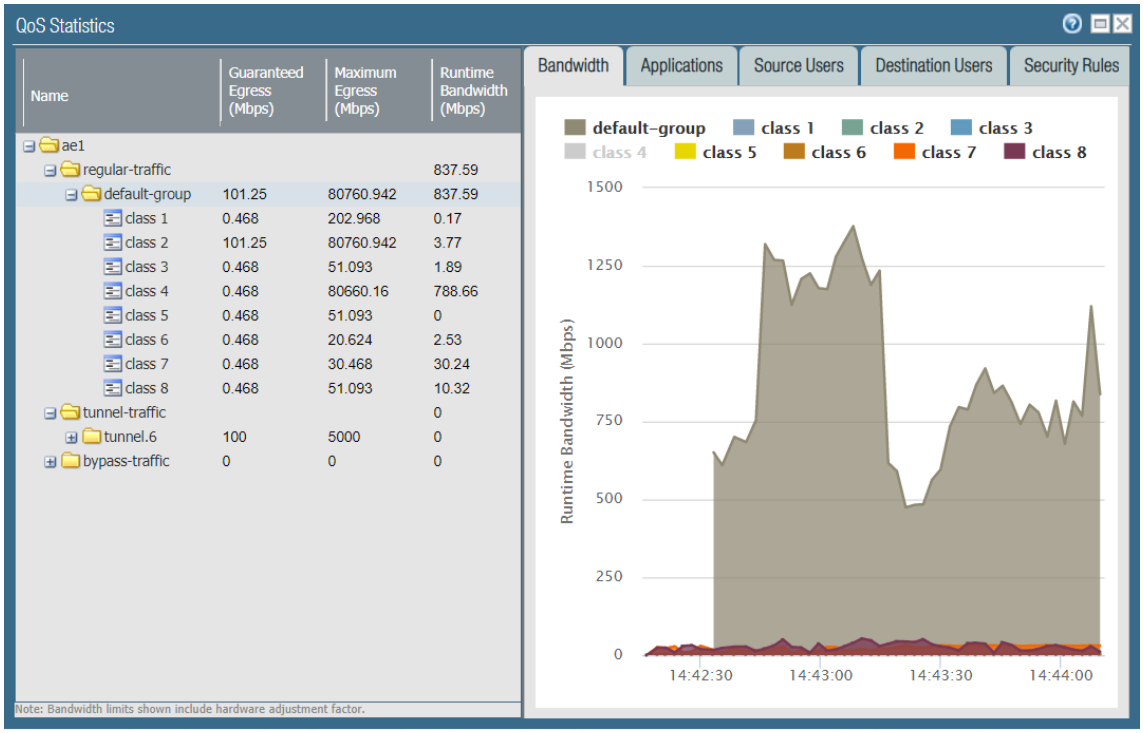


Resim 4.14 Ağ cihazlarının yapılandırma ayarları yedeklerinin dosya sunucundaki arşivi.

Hesap Yönetimi: NMS kurulumunun yetkilendirme ve raporlama adımlarında hesap yönetimine yönelik işlemler yapılmıştır. Bu işlemler sonucunda;

- Kullanıcı grupları oluşturularak, NMS'e erişim sağlayacak yöneticilerin yazılım içerisinde yapabilecekleri işlemler kısıtlanmıştır. Bu sayede yöneticilere doğru kaynak tahsisi yapılmış, yetkisiz işlem yapılması engellenmiştir. Ayrıca olası bir problemde yetkili yöneticilere bildirim sağlanmıştır.
- NMS'den alınan kaynak tüketimi raporları sayesinde adil ve tutarlı kullanım kotaları uygulanabilir. Elde edilen bu çıktılar sayesinde sunucu sistemlerinde işlemci, bellek, disk gibi kaynakların kapasiteleri verimli bir şekilde dağıtılabilir ve Resim 4.15'de görülen iletişim hattı veri bant genişlikleri, yönlendirici veya güvenlik duvarı cihazlarından sınırlandırılarak, gereksiz kullanımların önüne geçilmesi sağlatılabilmektedir.

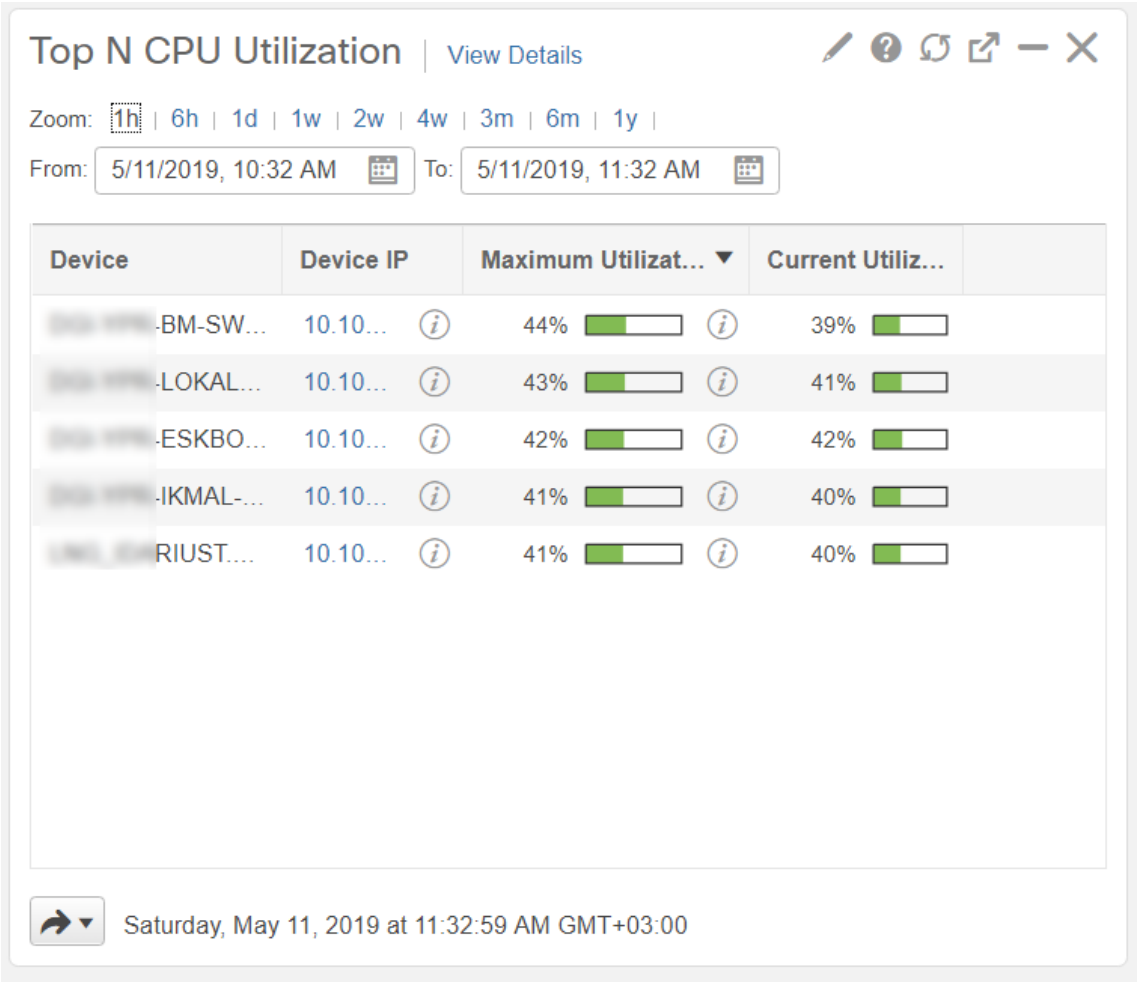
- Tüm bu yapılan kota dağıtımı, kaynak bilgilerinin kontrolü ve erişim ayrıcalıkları sayesinde gereksiz kullanımın önüne geçilerek, ağda kullanılan hatlar ve donanımlar için yapılacak olan harcamalarda azalma sağlanacaktır.



Resim 4.15 Güvenlik duvarı ile iletişim hattı bant genişliği kotası verilmesine örnek görsel.

Performans Yönetimi: Ağdaki cihazların geçmiş davranışlarını, yaptıkları etkinlikleri gösteren log kayıtlarıyla elde edilen veriler ve NMS kurulumunun kontrol adımında yapılan düzenlemeler sayesinde performans yönetimi yapılmıştır. Yapılan düzenlemeler ve alınan log kayıtları sonucunda;

- Kontrol ekranları düzenlenerek, yöneticilerin NMS bilgi tabanından kendisi için gerekli verilere ulaşması sağlanmıştır. Resim 4.16'deki tablo gibi ağ ve cihazlar hakkında görülmesi istenen veriler kontrol ekranına konularak, anlık performans analizi yapılması sağlanmıştır. Kontrol ekranına konulan bu görseller yöneticinin görebileceği, sürekli açık olan bir monitöre verilerek ağda yaşanan olayların takibi gerçekleştirilmiştir.
- Raporlama aşamasında cihazlarda oluşan arıza veya yapılan işlemleri gösteren log kayıtlarının arşivlenmesiyle, olası bir problemde sorunun kaynağının zaman harcanmadan bulunması sağlanmıştır.



Resim 4.16 En çok işlemci kullanan cihazları gösteren bilgi tablosu.

Güvenlik Yönetimi: Kurumsal geniş alan ağlarında güvenlik yönetimi işini güvenlik cihazları yapmaktadır. Güvenlik duvarı, ağ erişim kontrolü (Network Access Control – NAC), IDS, saldırı önleme sistemi (Intrusion Prevention System- IPS) gibi siber saldırıları önlemeye ve ağa erişim kurallarını belirlemeye yönelik geliştirilen cihazlar kullanılmaktadır. Ancak NMS'den alınacak performans analizleri, yetkisiz erişim kayıtları ve kaynak tüketimi raporlarından elde edilecek veriler doğrultusunda, güvenlik cihazlarında çeşitli güvenlik kuralları ve kaynak engellemeleri yapılabilir.

5. TARTIŞMA ve SONUÇ

Yapılan tez çalışması sonucunda ağ yönetimi konusunun önemi ve kurumsal ağlarda ne kadar kritik bir rol oynadığı ortaya koyulmuştur. Bununla birlikte ağ uzmanlarının büyük ölçekli sistemleri kurarken dikkat etmesi gereken hususlar ve bilgisayar ağlarının altyapısını oluşturan kaynakların kullanımı konusunda çözümlere değinilmiştir. Ağın kurulum aşamasında, planlı ve ağ yönetimine uygun bir çalışma yapılması, ağın yönetimini doğrudan etkilediği görülmüştür. Devamında ağ cihazlarında doğru yapılandırma ayarları ve gerekli güvenlik önlemlerinin alınması, donanımların bulunacağı veri merkezinin standartlara uygun inşa edilmesi, hiçbir işlem yapmadan önce ağın detaylı topolojisinin çıkarılması konularında yapılması gereken adımlar ifade edilmiştir.

Ağ yönetim sistemi denilince içerisinde barındırdığı teknoloji ve mimari detaylı anlatılarak, bu kavramla ilgili standartlar, protokoller ve modeller ağ yönetiminde görev alan uzmanlara içerik olarak sunulmuştur. Ayrıca ağ yönetimi sistemi seçilirken bakılması gereken noktalar, olması halinde fayda sağlayacak özellikler ve bir ağ yönetim sistemi kurulurken yapılacak adımlar listelenerek, yol gösterici bir kaynak olması hedeflenmiştir.

Kurumsal şirketler ağ yönetim sistemi tercih ederken genellikle belli bir yatırım maliyeti göze almaktadır. Buradaki odak noktası maliyetten ziyade, her zaman kazanımlar olmalıdır. Geniş alan ağlarının işletmeye ve gereksinimlere uygun olarak büyümesi gerekebilir. Bu ağ ortamını sürekli görme, canlı istatistiki veri alma ve geçmişe dönük analiz için binlerce ağ cihazından gelen, devamlı güncellenen ağ ölçümlerine güvenmek anlamına gelir. Ağ yönetim sisteminin; alarm mekanizması, kaynak izleme, raporlama ve analiz becerisi bu noktada belirleyici faktör olması gerekir. Şirketler, ağ ile ilgili bilgileri bildirmek ve kaydetmek için belirlemiş olduğu kurallarla bütünleşmiş bir ağ yönetim sistemi tercih etmelidir. Bu sayede ağ ve sunucu sistemlerindeki kaynaklardan fazlaca yararlanma durumu, gereksiz yapılacak olan yatırımların önüne geçecektir. Tercih aşamasında şirketlerin kendi ihtiyaçlarına cevap verecek yönetimsel özelliklerin daha iyi anlaşılabilmesi için, ticari pazarda yer alan ağ yönetim sistemleri ve dağıtımı ücretsiz

yapılan ürünler incelenmiştir. Kullanılan bu ürünlerin güçlü ve zayıf yönleri ile geliştirici firmaların ağ yönetimine kattığı farklı çözümler detaylıca anlatılmıştır.

Ağın doğru şekilde kurulması ve ağın yönetimi ne kadar basit görünse de belli bir seviyede bilgi birikim ve deneyim gerektirir. Bu tez çalışmasında verilen tüm bu bilgiler örnek bir kurumsal geniş alan ağında uygulamalı olarak gösterilmesi sonucunda çalışmanın, ağ uzmanlarına kurumsal bir ağın kurulumu ve yönetilmesi konularında yol gösterici bir kaynak niteliğinde olması sağlamıştır.

Geliştirilen ağ yönetim sistemleri ne kadar yöneticilerin işini kolaylaştırsa da en önemli eksiklikleri tam otonom yapıya sahip olmamalarıdır. Tez çalışmasında yapılan ağ yönetim sistemleri incelemesinde de görülen hata yönetimi ele alınırsa; hatalar, yöneticinin belirleyeceği alarm ve olay şartına göre veya yazılımın alabileceği aksiyon yetenekleri ile giderilebilmekte olup, kısıtlı bir yarı otonom mekanizma mevcuttur. Otonom ağ yönetim sistemi, kendini en iyi duruma getirme, kendini koruma, kendini yapılandırma ve kendini iyileştirme yeteneklerine sahip olması gerekir. Ağın çalışması için, asgari veya hiç insan müdahalesine ihtiyaç duymadan kendini yönetebilmeli ve düzenleyebilmelidir.

Otonom bir ağ yönetim sisteminin; kullanılan ağı, cihazları ve meydana gelen olayları sürekli öğrenebilmesi ve analiz edebilmesi gereklidir. Bunu günümüzde çeşitli alanlarda kullanılmaya başlanan ve insan zekâsı gerektiren işleri yapabilen bilgisayar sistemleri geliştirilmesini sağlayan yapay zekâ yöntemleriyle yapabilmek mümkündür. Bu teknolojilerle donanmış olan ağ yöneticileri, sorunların nerede yaşandığını daha iyi anlayabilir, yapılacak işlemlerle alakalı öneriler alabilir ve nihayetinde altyapının yapılandırılmasını ve çalışmasını otomatikleştirebilir. Gelecekte kurumsal şirketler, ağ gereksinimleri ve yönetim sistemleri açısından daha karmaşık bir yapıya sahip olacaktır. Teknoloji ilerledikçe şirketler, eğitimden iletişim sistemlerine kadar her konuda teknolojiyi kullanma ihtiyacı artacaktır. Tüm bu altyapının yönetim sürecinin giderek artan karmaşıklığı ile mücadele edebilmek için, insan müdahalesi gerek olmadan tamamen bağımsız, otonom yönetim sistemleri kullanılmaya başlanması kaçınılmaz bir gerçektir.

6. KAYNAKLAR

Al-Naymat, G., Al-kasassbeh, M. and Al-Hawari, E. (2018). Exploiting SNMP-MIB Data to Detect Network Anomalies using Machine Learning Techniques. *Intelligent Systems Conference 2018*, **869:** 991-1004.

Alkasassbeh, M., Al-Naymat, G., Hassanat, A., Almseidin, M. (2016). Detecting Distributed Denial of Service Attacks Using Data Mining Techniques. *International Journal of Advanced Computer Science and application*, **7**: 436-445.

Anonim, (1994). ANSI T1.215 OAM&P, Fault Management Messages for Interface between Operations Systems and Network Elements.

Anonim, (2000). Principles for a Telecommunications Management Network. ITU-T, Geneva.

Anonim, (2012). SNMP Reflected Amplification DDoS Attack Mitigation. BITAG, Denver.

Altıntaş, E., Özardıç, O., Talay, S. ve Ayav, T. (2003). Bir ağ yönetim sistemi: GuardiLAN. Proceedings of TBD 20th Informatics Workshop, http://hdl.handle.net/11147/2569.

Balta M. (2012). Sanal Ortam Üzerinde Oluşturulan Örnek Bir Kurumsal Ağ Topolojisinin Snmpv3 ile Topoloji Keşfi Uygulaması. Yüksek Lisans Tezi, Sakarya Üniversitesi, Fen Bilimleri Enstitüsü, Sakarya.

Binici E. (2006). Java İle Yapay Zekâ Mekanizmasına Sahip Bir Ağ Yönetim Sistemi Geliştirilmesi. Yüksek Lisans Tezi, Ege Üniversitesi, Fen Bilimleri Enstitüsü, İzmir

Case, J., Mundy, R., Partain, D. And Stewart, B. (2002). Introduction and Applicability Statements for Internet-Standard Management Framework, RFC 3410.

Clemm, A. (2006). Network Management Fundamentals. CiscoPress, Indianapolis, USA.

Demirbaş A. (2017). Ağ Üzerinde Bulunan Etkin Aygıtlardan Veri Toplamak İçin Bir Araç. Yüksek Lisans Tezi, Dokuz Eylül Üniversitesi, Fen Bilimleri Enstitüsü, İzmir.

Ding, J. (2010). Advances in Network Management. CRC Press, New York, 67-71.

Dixit, V.S. and Singh, V.B. (2012). Essentials of Computer Networks, Internet and Database Technologies. Alpha Science Intl. Ltd., 1. edition, New Delhi, India.

Hegering, H., Abeck, S. and Neumair, B. (1999). Integrated Management of Network Systems. Morgan Kaufmann Publishers, San Francisco, USA.

Honglei, Q., Zemin, Du. and Lihong, G. (2017). Computer Network Management Software. Computer System Networking and Telecommunications, http://ojs.whioce.com/index.php/csnt/article/download/545/419.

Iqbal, A. (2009). Monitoring Remote Financial Transaction Control Devices Using SNMP Over TCP. Electronic Thesis or Dissertation, Kent State University, Ohio.

Kara, S., Kırışoğlu, S. ve Özçelik, İ . (2018). Sanal yerel alan ağlarında ağ trafiği dengeleme için snmp tabanlı yeni bir algoritma. *Mühendislik Mimarlık Fakültesi Dergisi*, **34**: 365-380**.**

Kırışoğlu S. (2018). Kurumsal Ağların Sistematik Tasarımı İçin Yeni Bir Dinamik Vlan Yaklaşımı. Doktora Tezi, Düzce Üniversitesi, Fen Bilimleri Enstitüsü, Düzce.

Kijazi, A. and Michael, K. (2014). A Step on Developing Network Monitoring Tools. *Methodology*, **5**: 59-65.

McCloghrie, K. and Rose, M. (1991). Management Information Base for Network Management of TCP/IP-based internets: MIB-IIInternet, RFC-1213.

Rao, U.H. and Mohapatra, S. (2010). Deploying network management solutions in enterprises. *INC2010:6th International Conference on Networked Computing*, **28**: 1-6.

Rosen, C.E. and Rose, M. (1981). Vulnerabilities of Network Control Protocols: An Example, RFC 789.

Tün, M., Pekkan, E. ve Tunç, S. (2015). Yer Sarsıntı Haritalarının Üretilmesinde Sismik Ağ Yapısı: Eskişehir Örneği. *Harita Teknolojileri Elektronik Dergisi*, **7:** 1-14.

Verma, D.C. (2009). Principles of Computer Systems and Network Management. Springer Science Business Media, 1. edition, New York, USA.

Xiaoyu, T., Lu, Liu. and Ying, L. (2012). A New Generation Theory and Technology of Mobile Fusion Network, Posts and Telecommunications Press, China, 101-103.

Yang, L. and Wang, Q. (2013). Analysis of Network Management Technology and Development Trend In The Future. *Advances in Intelligent Systems Research*, **760**: 1192-1196

İnternet Kaynakları

1) https://www.statista.com/statistics/734527/worldwide-enterprise-network-infrastructure-market-by-technology/, 13.02.2019
2) http://reg.interop.com/stateofinfrastructure, 18.02.2019
3) https://enterprise.verizon.com/resources/articles/why-network-visibility-is-important-for-your-business/, 18.02.2019
4) https://www.computerhope.com/history/network.htm, 10.08.2018
5) http://edutechwiki.unige.ch/en/Networking_history, 10.08.2018
6) https://searchmobilecomputing.techtarget.com/definition/unified-network-management, 02.05.2019
7) https://www.technavio.com/report/global-network-management-system-nms-market-analysis-share-2018, 10.08.2018
8) https://searchnetworking.techtarget.com/survey/IT-Priorities-2017-survey-Virtualization-gains-in-networking-plans, 10.08.2018
9) https://searchnetworking.techtarget.com/feature/Enterprise-network-management-and-security-require-collaboration, 06.03.2019
10) https://www.networkmanagementsoftware.com/snmp-tutorial-part-2-rounding-out-the-basics/,04.02.2019
11) https://www.paessler.com/manuals/prtg/add_remote_probe, 05.09.2018
12) http://www.teksernet.com.tr/kategori.php?id=45/, 05.05.2019
13) http://bt.robit.com.tr/veri-merkezi/, 12.01.2019
14) https://www.connection.com/search/cisco/4294966758/, 08.05.2019

ÖZGEÇMİŞ

Adı Soyadı : Abdullah YILDIRIM

Doğum Yeri ve Tarihi : Kahramankazan 27.09.1993

Yabancı Dili : İngilizce

İletişim (Telefon/e-posta) : 05076087500 / yldrm.a@outlook.com

Eğitim Durumu (Kurum ve Yıl)

Lise : Gazi Anadolu Teknik Lisesi, (2007-2011)

Lisans : Ankara Üniversitesi, Bilgisayar ve Öğretim Teknolojileri Öğretmenliği, (2011-2015)

Yüksek Lisans : Afyon Kocatepe Üniversitesi, İnternet ve Bilişim Teknolojileri Yönetimi, (2016-2019)

Çalıştığı Kurumlar ve Yıl : Boru Hatları ile Petrol Taşıma A.Ş. (2014–Devam ediyor)