Niğde Ömer Halisdemir Üniversitesi Mühendislik Bilimleri Dergisi
Nigde Omer Halisdemir University Journal of Engineering Sciences

ISSN: 2564-6605

Araştırma / Research

BİR KURUMSAL GENİŞ ALAN AĞININ AĞ YÖNETİM SİSTEMİYLE ETKİLİ YÖNETİMİ

Said Mahmut ÇINAR[1,*], Abdullah YILDIRIM[2]

[1] *Afyon Kocatepe Üniversitesi, Mühendislik Fakültesi, Elektrik Mühendisliği Bölümü, Afyonkarahisar, Türkiye*
[2] *Afyon Kocatepe Üniversitesi, Fen Bilimleri Enstitüsü, İnternet ve Bilişim Teknolojileri Yönetimi ABD, Afyonkarahisar, Türkiye*

ÖZET

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, 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 verilerek örnek bir kurumsal geniş alan ağının modellemesi açıklanmıştır.

Anahtar kelimeler: Ağ yönetim sistemleri, Kurumsal geniş alan ağı, Ağ yönetim modeli,

EFFICIENT MANAGEMENT OF AN ENTERPRISE WIDE AREA NETWORK WITH NETWORK MANAGEMENT SYSTEMS

ABSTRACT

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 within infrastructure of network management system is analyzed and specifications of today's widely used network management systems are examined. In accordance with the benefits obtained in order to simplify the management, detailed information is given about specifications required for preferring an ideal network management system and establishing an enterprise wide area network, a sample of modelling enterprise wide area network has been explained.

Keywords: Network management systems, Enterprise wide area network, Network management model

1. GİRİŞ

Bilgisayar ağları, birden çok bilgisayarın çeşitli iletişim kanalları üzerinden kaynakları paylaşmak üzere birbirleri ile iletişim kurduğu sistemlerdir. Bilgisayar ağlarına ihtiyaç duyulmasının nedeni coğrafi konumdan bağımsız olarak fiziksel ve mantıksal kaynakları (yazıcı, program, veri vb.) ağdaki kullanıcıların erişimine sunmaktır. Kurumsal ağlar şirketler için oluşturulmuş özel bilgisayar ağları olarak tanımlanabilir. Kurumsal ağlar bir şirketin farklı coğrafi alanlarda faaliyet gösteren birimleri arasında iletişim sağlayabildiğinden dolayı çok fazla donanım ve yazılım kaynağını barındırabilmektedir. Bu durum kurumsal ağlarda yönetimsel sorunlarının ortaya çıkmasına sebep olmuştur. Bu yönetimsel sorunlar; i: hizmet kesintileri, ii: donanımsal arızalar, iii: performans problemleri, iv: siber tehditler şeklinde sıralanabilmektedir. Kurumsal ağlarda ortaya çıkan bu yönetimsel sorunlara ağa özel tasarlanmış ağ yönetim sistemleriyle zamanında ve etkili önlemler almak gerekmektedir. Literatürde ağ yönetim sistemleri üzerine yapılmış çalışmaların bir özeti aşağıda sunulmuştur;

Açık sistem arabağlantısı (Open Systems Interconnetion-OSI) modeliyle standardize edilmiş olan bilgisayar haberleşme sistemlerinin ağ katmanı cihazları, basit ağ yönetim protokolü (Simple Network Management Protocol-SNMP) ile yönetilmekte ve kontrol edilmektedir. Ancak artan ağ kullanıcısı ile birlikte ağın topolojik yapısının karmaşıklığı devamlı

* Sorumlu yazar / Corresponding author, e-posta / e-mail: smcinar@aku.edu.tr
Geliş / Recieved: 27.08.2019 Kabul / Accepted: 24.12.2019 doi: 10.28948/ngumuh.611668

artmakta ve ağın bant genişliğini arttıran kullanıcı uygulamaları çoğalmaktadır. Ağ yönetim sistemlerinde işleyişin ağ katmanından uygulama katmanına aktarılmaya başlanmasıyla birlikte ağ yönetimi teknolojilerinde kullanıcı uygulamalarına odaklanılmıştır [1]. Diğer bir model, yazılım tanımlı ağların (Software Defined Networking-SDN) OpenFlow protokolü ile kontrol edilmesidir. SDN kavramı, ağların yüksek verimle kullanılabilmesi, kullanıcılar için uçtan uca bağlantı sağlanması, bulut ve ağ sanallaştırma uygulamaları için ağ kaynaklarının dinamik yönetimine izin verilmesi gibi ihtiyaçların hayata geçirilmesi için ortaya çıkmıştır [2]. SDN, ağı programlanabilir hale getirmek ve yönetim karmaşıklığını azaltmak için etkili bir yoldur. Ancak mevcut SDN çözümleri, ağ yönetiminde kapsam belirlemedikleri için etkili bir yönetim gerçekleştirilememektedir. SDN tabanlı ağ yönetim sistemleriyle ilgili bu sınırlamaları aşmak için kurumsal ağların farklı sanal ağlara bölünerek yönetilmesi yaklaşımı geliştirilmiştir [3]. Bugün büyük ölçekli sistemlerde kullanımı sıklıkla görülen sanallaştırma teknolojileri (Hyper-v, Vmware) ele alınacak olursa, üzerinde barındırdıkları servisler ve hizmetlerde yaşanabilecek durma, kapanma, çalışmama, performans düşüklüğü gibi problemlerin takibi kritik seviyede önem arz etmektedir. Sanallaştırmada kullanan bulut sistemlerinde hata ve performans yönetimi de doğal olarak zorlaşmaktadır. Fiziksel ağlarda kullanılan kural tabanlı teknikler sanal ortamlarda etkili çalışmamaktadır. Bu sorunların üstesinden gelmek için derin öğrenme kapasitesine sahip yapay zekâ teknikleri kullanılmaktadır [4]. Yapay zekâ teknikleriyle otonom tarımsal traktör sistemleri [5], otoyol trafik sistemleri [6] gibi birçok farklı alanda yönetim çözümleri geliştirilmektedir. Kurumsal geniş alan ağlarının yönetimi içinde otonom ağ yönetim araçlarının kullanılması kaçınılmaz hale gelmektedir. Ancak otonom ağ yönetim sistemleri, ağ yönetimi araştırma alanında bir eğilimdir ve buradaki otonomdan kastedilen ağı yönetimini kolaylaştırmaktır [7].

Kurumsal ağlarda, ağ yöneticisinin görevini kolaylaştırmak için edinilen ağ yönetim araçları bulunmakla birlikte bunların kullanıcı dostu olması ve bu araçları verimli kullanabilmek için gerekli bilgilerin eksiksiz olması gereklidir [8]. Rao ve Mohapatra [9]'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 belirlenmiştir. Bu çalışmada personel eğitimi, ürün yenileme, yeni araçların sisteme dâhil edilmesi gibi birçok iyileştirici düzenleme yapılmıştır. Ağ sistemlerinde her şeyin yolunda gitmesini sağlamak ve ağ altyapısından daha fazla verim elde etmek için iyi bir ağ yönetimi günümüzde büyük önem kazanmıştır. Ağdaki kaynakların ve özellikle trafiğin ayarlanabilmesi, gerektiğinde ağ ölçeğinin genişletilmesi, ağ kullanımının en iyi duruma getirilmesi ve ağ altyapısının verimli kullanılabilmesi gereklidir [10].

Günümüzde bilgisayar ağlarının güvenliğini sağlamak önemli bir sorun haline gelmiştir. Güvenliğin tam anlamıyla sağlanması için kesintisiz trafik izleme, yapılandırma yönetimi, servis kayıtlarının alınması da dâhil olmak üzere bir dizi güvenlik uygulamaları yapılması gerekmektedir [11]. Kurumsal geniş alan ağının ölçeği büyüdükçe saldırı girişimlerinin takibi zorlaşmaktadır. SNMP tabanlı geliştirilen algoritmalar, bu tür saldırı girişimlerinin tespitinde büyük rol oynamaktadır [12]. SNMP, anlık veri gönderebilen ajan yapısıyla amaca uygun programları ağ yönetim sistemlerinin birçok alanında kullanımını sağlamıştır. Finans, yer bilimleri, telekomünikasyon, ulaşım ve enerji gibi birçok alanda bilgisayar ağlarının kullanılmaya başlanmasıyla birlikte ağ yönetim sistemleri kurumsal şirketlerin yönetiminin yanı sıra farklı amaç ve problemlerin çözümüne hizmet etmeye başlamıştır. Tün ve arkadaşları [13] geliştirdiği projede deprem anında yer sarsıntı haritaları ve olası hasar dağılım haritalarını, ağ yönetim sistemleri ve coğrafi bilgi sistemlerini bir arada kullanılarak elde etmiştir. Iqbal [14]'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 arttırılması ve aksama süresinin ise azaltılarak müşterilerine kaliteli hizmet sağlandığı sonuçlarına ulaşılmıştır. Siber saldırı türleri arasında hizmet dışı bırakma (Denial of Service/ Distributed Denial of Service-DOS/DDOS) saldırıları en tehlikeli saldırı türü olduğunu belirtilmiştir [15]. İnternetin ana tehditlerinden biri olan DOS/DDOS tipi saldırıları engellemek için izinsiz girişlerin hızlıca saptanması gerekmektedir. Bunun için kullanılabilecek en uygun yöntem, anormal etkinliğin normal bir ağ davranış profiliyle karşılaştırılmasıdır. Bu karşılaştırma sonucu tanımlama yapılarak ağ güvenliği korunabilmektedir. Al-Naymat ve arkadaşları [16] izinsiz girişlerin engellenmesine yönelik saldırı tespit sistemlerinde ağ cihazlarından toplanan ham verilerin analizi ile vakit kaybedilmesi yerine, cihazlardan toplanan işlenmiş verilerinin bulunduğu ağ yönetim yazılımı veri-tabanı kullanarak ağ saldırılarının tespiti ve saldırı türlerinin sınıflandırılması için etkili bir mekanizma tasarlamıştır. Bu sayede önemli bir işlem yükü ve geç tespit süresi ortadan kaldırılmıştır. Büyük coğrafi alana yayılmış enerji ve güvenlik gibi stratejik uygulamalarda ağ yönetiminin kullanılması hayati derecede öneme sahiptir.

Piyasada bireysel veya kurumsal ihtiyaçları karşılayabilecek birçok ağ yönetim yazılımının bulunmasından dolayı kullanım amacına en uygun yazılımın nasıl seçileceği sorusunun cevabı aranması gerekmektedir [17]. Yazılımın katabileceği kolaylıklar, kurumsal yapıya olan uygunluğu ve maliyeti konuları genellikle uzun araştırmalar ve denemeler sonucunda edinilebilecek bir bilgidir. Bunun yanında şirketler kendilerine özel ağ yönetim sistemi geliştirebilmektedir. Bilişim teknolojisi (Information Technology-IT) altyapılarının verimli ve düşük maliyetli yönetimlerine imkân sağlayacak bu yazılımın tasarımı, kodlaması ve bileşenlerinin hazırlanmasın da bilgisayar ve ağ varlıkları yönetimi (Computer and Network Asset Manager-CNAM) uygulaması yardımcı bir kaynaktır [18].

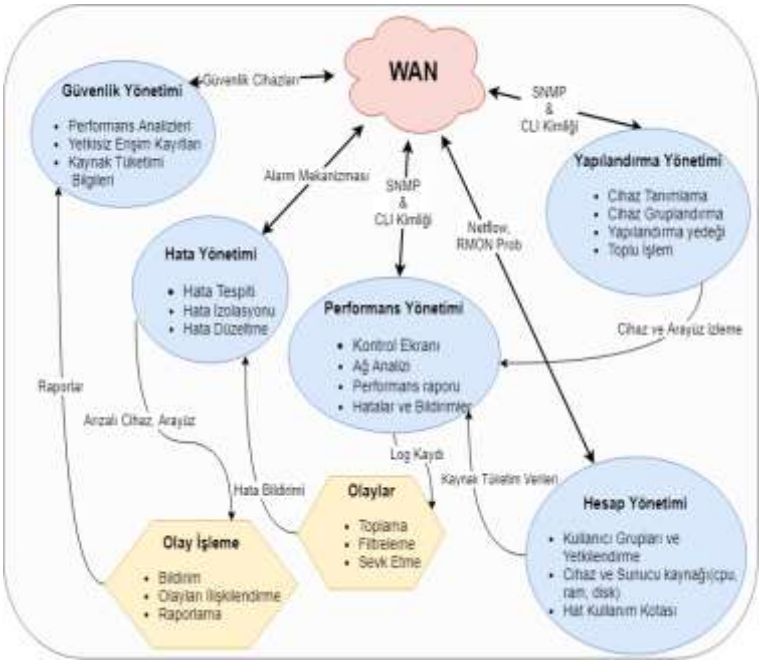
Bu çalışmada günümüzde daha fazla önem arz eden ağ yönetim sistemleriyle ilgili örnek bir sistem tasarımı yapılmış ve tasarımda kullanılabilecek yazılımların karşılaştırılması yapılmıştır. Aşağıda materyal ve metot bölümünde ağ yönetim sistemleri ve bileşenleri ayrıntılarıyla verildikten sonra ağ yönetim sistemlerinin tasarımda çok kullanılan bazı yazılımların özellikleri karşılaştırmalı olarak sunulmuştur. Bulgular bölümünde kurumsal bir ağ yönetim sisteminin taşıması gereken özellikler detaylandırılmış ve tasarlanan bir kurumsal ağda elde edilen sonuçlar verilmiştir. Son olarak elde edilen sonuçlar tartışılmıştır.

2. MATERYAL VE METOT

Bilgisayar ağları ve dağıtılmış sistemler kurumsal işletmelerin çoğunda kritik bir öneme sahiptir. İşletmeler çeşitli ihtiyaçlar nedeniyle daha fazla uygulama ve kullanıcıyı destekleyen büyük ve karmaşık ağlara yönelmektedir. Bunun sonucunda ağlar; bağlantılar, anahtarlar, yönlendiriciler, ana bilgisayarlar ve diğer aygıtlar içeren çok sayıda karmaşık ve birbiriyle etkileşimi olan donanım ve yazılım bileşenlerini içermektedir. Çok bileşenli bu ağlarda arıza olasılığının artabileceği, ağ bileşenlerinin yanlış yapılandırılabileceği ve ağ kaynaklarının fazladan kullanılabileceği buna bağlı olarak da ağın verimli bir şekilde işlev görmemesinin maliyetinin şirketler için yüksek olacağı açıktır. Şirketlerin geniş alana yayılmış çok sayıda ağ bileşeninin takibini yapabilmesi için merkezi bir noktadan ağın izlenmesine, yönetilmesine ve kontrolüne yardımcı olacak araçlara ihtiyacı olmaktadır. Hegering ve arkadaşları [19] ağ yönetimini, bir sistemin kurumsal hedeflere uygun olarak etkin ve verimli şekilde çalışmasını sağlayan işlemler bütünü olarak tanımlamaktadır. Bunu başarmak için ağ kaynaklarının denetlenmesi, ağ hizmetlerinin koordine edilmesi, ağ durumlarının izlenmesi ve ağ durumunun raporlanması gerekmektedir. Bir başka kabul edilebilir tanım olarak ağ yönetimi; ağa bağlı sistemlerin çalışması, yönetimi, bakımına ilişkin; faaliyetler, yöntemler, işlemler ve araçlar bütünü şeklinde ifade edilmektedir [20]. Aşağıda ağ yönetim sistemlerinde kullanılan; ağ yönetimi modeli, mimarisi ve protokolleri verildikten sonra piyasada çok kullanılan bazı ağ yönetim sistemi yazılımlarının özellikleri hakkında bilgiler verilmektedir.

2.1. Ağ Yönetim Modeli

Uluslararası standardizasyon örgütü (ISO), ağ yönetiminin yapısal bir çerçeveye yerleştirilmesi ve tutarlılık sağlaması amacıyla uluslararası bir ağ yönetim modeli oluşturmuştur. Bu model kısaca FCAPS (fault-management, configuration, accounting, performance, and security) olarak isimlendirilmiştir. FCAPS, ağ yönetimi için gereksinmeleri organize etmeyi sağlayabilen beş temel alanı belirlemektedir. Bunlar hata yönetimi, yapılandırma yönetimi, hesap yönetimi, performans yönetimi ve güvenlik yönetimidir.



Şekil 1. Ağ yönetiminde beş temel alanın ilişkisi

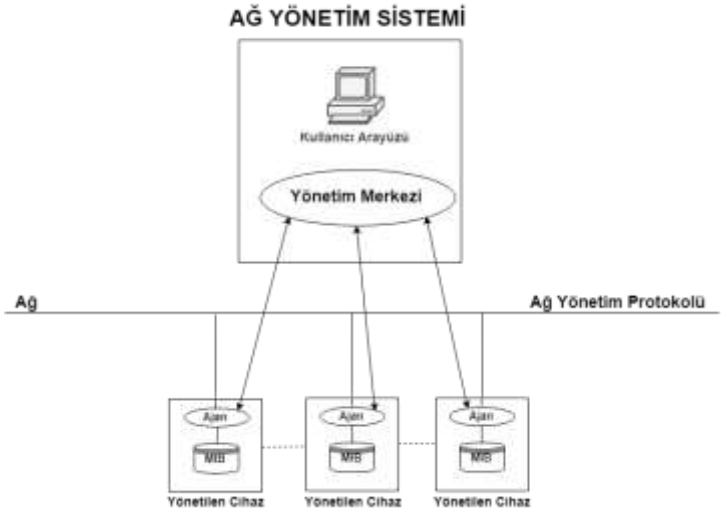
Şekil 1'de bu beş temel alanın kapsadığı işlemler ve birbirleriyle olan ilişkisi gösterilmiştir. Her bir alan diğer alanlardan doğrudan veya dolaylı olarak etkilenmektedir. Tüm işlemlerin sıralı ve doğru şekilde yapılması sonucunda etkili bir ağ yönetimi yapmak mümkün olabilmektedir.

2.2. Ağ Yönetim Sistemi Mimarisi

Ağ yönetim mimarisinin üç ana bileşeni bulunmaktadır (Şekil 2). Bu bileşenler; yönetim merkezi, yönetilen cihaz ve ağ yönetimi protokolü olarak bilinmektedir.

Yönetim merkezi; ağ yöneticisi ve araçlardan oluşur. Yönetici, ağ yöneticisinin ağ yönetimi işlevlerini gerçekleştirdiği konsoldur. Bu bir sunucuya kurulu yazılım veya doğrudan donanım şeklinde olabilir.

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



Şekil 2. Temel ağ yönetim mimarisi

Ağ yönetimi protokolü; yönetim merkezi ile yönetilen cihazlar arasında uygulanan bir politikadır. Bu protokol ile yönetim merkezinin yönetilen cihazların durumunun belirlenmesi sağlanır.

2.3. Ağ Yönetim Protokolleri

Protokoller, ağ yönetim sistemi ile yönetilen cihazlar arasındaki iletişimi sağlayan kurallar olarak tanımlanabilmektedir. Ağ yönetim sistemi, ağdaki cihazların durumunu sorgulayarak ajanlar aracılığıyla işlem yapmasına olanak sağlamaktadır. Ajanlar ağ da yaşanan alarmları ve hataları (bileşen arızaları, performans eşiklerinin aşılması vb.) yöneticiye bildirmek için ağ yönetim protokolünü kullanmaktadır. Ağ yönetim protokolleri ağı yönetmek için ağ yöneticisinin kullanacağı özellikleri sağlamaktadır.

İlk geliştirilen ağ yönetim protokolü kısaltması SNMP olan basit ağ yönetim protokolüdür. SNMP bir grup akademisyen tarafından tasarlanmıştır ve yeni sürümleriyle hâlen ağ yönetiminde kullanılan 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 arttırmaktadır. SNMPv3'de güvenlik ve yönetime odaklanmış olup kimlik doğrulama, gizlilik, yetkilendirme ve uzaktan yapılandırma özellikleri protokole kazandırılan özelliklerden bazılarıdır [21].

Daha sonra ortak yönetim bilgi protokolü (Common Management Information Protocol-CMIP) 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 [22]. CMIP, SNMP'ye göre yetenekleri daha gelişmiş bir protokoldür. Ancak bununla birlikte daha karmaşık bir yapıya sahiptir. Bir diğer önemli protokol ise SNMP'nin bir parçası olması ve gelişmiş ağ yönetim yeteneklerine izin vermesi için geliştirilen uzaktan ağ izleme (Remote Network Monitoring-RMON) protokolüdür. RMON, cihazları uzaktan keşfederek veri toplamak ve bu verileri işlemek için tasarlanmış bir protokoldür. Fakat CMIP ve RMON protokolleri karmaşık oldukları, daha fazla sistem kaynağı tükettikleri ve sonradan uygulamaya girmiş olmaları gibi nedenlerden dolayı beklenen ilgiyi görememişlerdir [23].

2.4. Ticari Pazarda Yer Alan Ağ Yönetim Sistemi Ürünleri

Ağ yönetim sistemleri (Network Management System-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. Ticari pazarda birçok üretici ağ planlaması, güvenlik kontrolü, döküm yönetimi ve trafik izleme gibi çeşitli yönetim faaliyetlerini destekleyen NMS çözümleri geliştirmektedir. Bu çalışma kapsamında çeşitli özeliklere sahip ve benzer sorunlara çözüm üretmek için geliştirilen dokuz ayrı ağ yönetim sistemi incelenmiştir. İncelenen ürünler; modüler yapıya sahip ürünler, donanım üreticilerinin geliştirdiği ürünler, ağdaki belli ihtiyaçlara yönelik geliştirilen ürünler ve ücretsiz ürünler olmak üzere dört ayrı gruba ayrılarak, NMS'lerin avantajlı ve dezavantajlı olduğu durumlar değerlendirilmiştir. Aşağıda Solarwinds, Manageengine Opmanager, Cisco Prime, Paessler PRTG, Infoblox NetMRI, OpenNMS, LibreNMS, Cacti ve Whatsup Gold isimli NMS yazılımları ortak özelliklerine göre gruplandırılarak tanıtılmıştır.

2.4.1. Solarwinds ve manageengine opmanager

Bu iki yazılımın birlikte ele alınmasının nedeni modüler yapıya sahip ve çok yönlü bir şekilde bilişim teknolojileri altyapısının yönetimini sağlayan NMS olmalarıdır. Ağ yönetimi, sunucu yönetimi, uygulama yönetimi, depolama ve veri-tabanı yönetimi gibi birçok yönetimsel faaliyeti yerine getiren araçlara sahiplerdir. İstenildiği takdirde bu modüllere yeni araçlar dâhil edilebilmesi sayesinde tek bir yönetim paneli üzerinden tüm sistemlerin yönetimi sağlanabilmektedir. Bu iki ürün seçilen modül ve yönetilecek ağ cihazı sayısı kadar ücret karşılığı satın alınabilmektedir.

2.4.2. Cisco prime

Cisco Prime, Hewlett Packard (HP) ve Huawei gibi donanım üreticisi firmalar, kendi ürettikleri ağ cihazlarıyla etkili çalışabilecek NMS ürünleri geliştirmektedir. Cisco Prime NMS yazılımı da bu amaca hizmet eden ürünlerin başında gelmektedir ve ürün ailesinde bulunan kablolu ve kablosuz donanımların, kendisine ait protokoller ile yönetim imkânı sağlamaktadır. Cisco Prime ve HP IMC (Internet Management Center-IMC) gibi NMS ürünlerinin dezavantajı ise diğer üreticilere ait cihazların yönetiminde başarısız bir performans sergilemeleridir. Bu tarz ürünlerde yine yönetilecek ağ cihazı adedi üzerinden ücretlendirme yapılarak satışı gerçekleşmektedir.

2.4.3. Paessler PRTG ve Infoblox NetMRI

Bazen sadece belli bir çözüm için kullanılmak üzere NMS'e ihtiyaç duyulabilmektedir. Paessler PRTG; ağ kaynaklarının (işlemci, bellek, bant genişliği vb.) performansının izlenmeye, Infoblox NetMRI; IP (Internet Protocol) adresi ve cihaz yapılandırma ayarlarını yönetmeye yönelik geliştirilen ürünlerdir.

Maliyetlerinin daha uygun olması ve istenen ihtiyaçları başarılı bir şekilde yerine getirmesi bu tarz yazılımların tercih edilme sebepleri sayılabilmektedir. Ağ yönetiminde oluşabilecek ihtiyaçlara yönelik yeni araçların yazılıma eklenemeyecek olması ve ayrıca tek bir ara-yüzden tüm sistemlerin yönetiminin mümkün olmaması daha dar yönetimsel çözümler sunan bu ürünlerin en büyük dezavantajı olarak değerlendirilmektedir.

2.4.4. OpenNMS, LibreNMS, Cacti ve Whatsup gold

Ağ yönetim sistemi tercih edilirken ücretli lisanslanan ürünler kullanılabileceği gibi, ücretsiz kullanımına izin verilen veya açık kaynak kodlu dağıtımı yapılan yazılımlar da tercih edilebilmektedir. Genellikle farklı çözümler için geliştirilen yazılımlar olmasından dolayı, ücretli ürünlerde olduğu gibi tek bir ekrandan bütün araçlara ulaşılabilecek bir ara-yüz yoktur. Etkili bir yapı kurulabilmesi için, en doğru yazılımların tercih edilmesi gereklidir. OpenNMS ve LibreNMS gibi ürünlerle ağ izleme ve hata yönetimi yapılabileceği gibi, Cacti ve Whatsup Gold gibi ürünlerle bant genişliği yönetimi ve topoloji takibi gibi temel kontrollere yönelik çözümler kullanılabilir.

Yukarıda dört temel grupta incelenen dokuz farklı ağ yönetim sistemi yazılımlarının özelliklerinin daha iyi ortaya çıkarmak ve seçim aşamasında tercihi kolaylaştırmak için Tablo 1'de 14 farklı kıstas üzerinden karşılaştırma yapılmıştır.

Tablo 1. Ağ yönetim sistemlerinin karşılaştırılması

NMS	Tek Arayüz	Yetkilendirme	Ağ Keşfetme	Hata Ayırt etme	Alarm Mekanizması	Yapılandırma Yönetimi	Toplu İşlem	Veri trafiği Takibi	Ağ İzleme	Log Analizi	Raporlama	Modüler yapı	Teknik Destek	Maliyet
Paessler PRTG	V	Y	V	Y	V	Y	Y	V	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	Y	V	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	V	Y	V	Y	V	-
Cacti	Y	Y	Y	Y	Y	Y	Y	V	V	Y	V	Y	Y	-
LibreNMS	V	V	Y	V	V	Y	V	V	V	V	Y	Y	Y	-

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

3. BULGULAR VE TARTIŞMA

Bu bölümde ilk olarak tasarımı yapılan bir kurumsal geniş alan ağının mimarisi, topolojisi, cihaz kurulum ve yapılandırmaları hakkında bilgiler verilecektir. Ardından söz konusu ağın yönetimi için tasarlanan NMS ile ilgili olarak; kullanılan NMS yazılımının nasıl seçildiği, hangi alarmların kurulduğu, yedekleme, raporlama ve güvenlik önlemleri gibi işlemlerin ne şekilde yapıldığıyla ilgili ayrıntılı bilgiler sunulacaktır. Son olarak tasarlanan NMS ile elde edilen sonuçlar verilmektedir.

3.1. Tasarlanan Bir Kurumsal Geniş Alan Ağı

Etkin bir ağ yönetimi tasarımına ağın kurulumundan başlanılması gerekmektedir. Şekil 3'de bir şirketin geniş alan ağı mimarisi görülmektedir. Burada veri kaynakları merkezi ofiste bulunan veri merkezinden uç noktalara dağıtacak şekilde bir ağ mimarisi tercih edilmiştir. Söz konusu ağda tüm altyapının kurulumu, planlaması ve yönetimi bu merkez ofis üzerinden yapılıp, uç noktaların merkeze erişimi iletişim hatları üzerinden sağlanmaktadır.

Kurumsal geniş alan ağının kurulum aşamasında veri merkezinde ve uç noktalardaki yerel alan ağlarında yapılması gereken işlemler şöyle sırlanabilir;

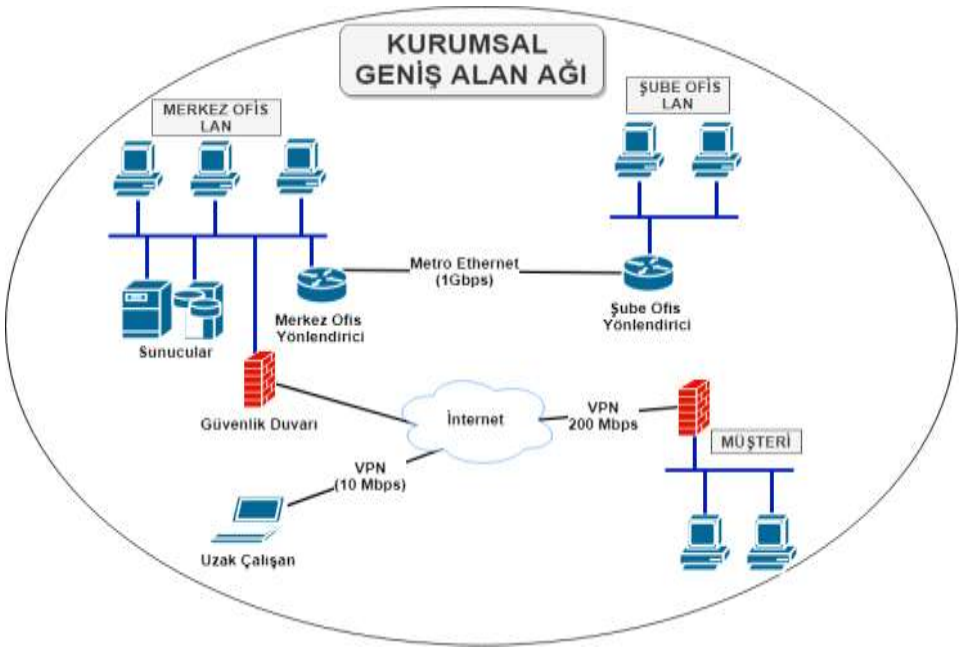
- İletişim hatlarının belirlenmesi
- Ağ topolojisi çıkarılması
- Cihazların kurulumu
- Cihazların doğru yapılandırılması
- Ağ yönetim sistemi seçimi
- Ağ yönetim sistemi kurulumudur

Yukarıdaki işlemler sırasıyla ve doğru planlanarak yapılması durumunda, kurulumu gerçekleşen ağın yönetimi daha kolay ve etkin biçimde gerçekleşebilmektedir.

Şekil 3. Merkezden yönetimi sağlanan kurumsal geniş alan ağı [24]

3.1.1. İletişim hatlarının belirlenmesi

Şekil 4'de merkez ofis ile uç noktalardaki şubeler, müşteriler ve çalışanların birbiriyle haberleşebilmeleri için iki farklı iletişim hattının kullanıldığı bir ağ topolojisi görülmektedir. Bu topolojide birinci ve daha az maliyetli olanı sanal özel ağ (Virtual Private Network-VPN) bağlantısı, diğeri ise kiralık (Metro Ethernet) iletişim hatlardır. Kurumsal geniş alan ağlarında hat seçiminde uç noktadaki ofislerde bulunan kullanıcıların yapacağı trafik tüketimi ve oluşacak maliyet göz önüne alınarak bir tercih yapılması gerekmektedir. Seçilecek iletişim hattının fizibilitesi doğru yapılması doğrudan şirketin bütçesini etkileyecektir. Bu sayede ölü yatırımların önüne geçilerek gerçek manada çözülmesi gerek ihtiyaçlara kaynak çıkarılacaktır.



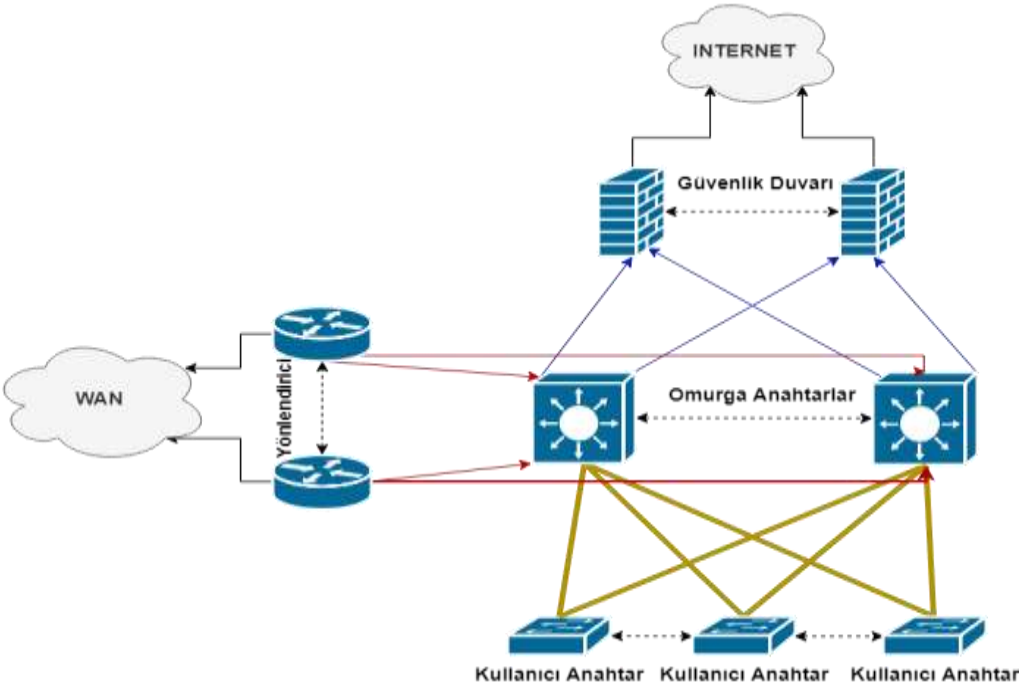
Şekil 4. Geniş alan ağında kiralık ve VPN hatlarını gösteren örnek topoloji

3.1.2. Ağ topolojisinin çıkarılması

Topolojiler ağın tanımlanması ve olası hataların giderilmesinde ağ operatörlerine yardımcı olan en temel araçlardır. Ağ topolojisi, ilk bakışta cihazlar ve ağ hakkında bilgi edinilmesini sağlayan, bir sorunla karşı karşıya gelindiğinde çözme süresini azaltan, cihazların bağlantı düğümlerini ortaya koyan çizimlerdir. Başka bir ifadeyle, ağ topolojisi veri merkezlerinin içerisindeki cihazların birbirleriyle olan bağlantının ve merkez ofis ile uç noktalar arasındaki hatların haritası niteliğindedir. En temel anlamda fiziksel ve mantıksal topoloji olmak üzere iki çeşit topoloji çizimi bulunmaktadır. Fiziksel topoloji, ağdaki cihazların kablo bağlantılarını gösteren çizimlerdir. Mantıksal topoloji ise ağda yer alan, ağ bölümlerinin ve cihazlarının çalışma trafiğini göstermektedir. Topolojinin mantıksal çizilmesi gruplar arasındaki veri akışının kablolu bağlantıdan bağımsız olarak gösterilmesidir. Topoloji çizimleri ağ kurulurken bir kere çizilip bırakılması yerine, ağda yapılan her değişiklik sonunda mutlaka güncellenmesi gerekmektedir. Ağ topolojilerinin çıkarılması ile personel bağımlılığı ortadan kaldırılarak, ekibe sonradan dâhil olabilecek uzman personelin geniş alan ağını daha hızlı anlamlandırabilmesi sağlanmıştır. Ayrıca bu topolojiler ağda yaşanan arızlara müdahale edilirken sorun giderme işlemlerinde yol gösterici haritalar niteliğinde olacaktır.

3.1.3. Cihazların kurulumu

Cihazlar kurulum aşamasında seçilecek olan topolojiye uygun şekilde konumlandırılmalıdır. Merkez ve uzak konumlarda bulunan yerel alan ağlarında yıldız topoloji tercih edilmeli ve omurga anahtarlar üzerinden kablo dağıtımı yapılmalıdır. Şekil 5'de görülen omurga anahtarlar etrafında takılacak olan diğer ağ cihazları ve sunucular düğüm (mesh) topoloji yapısına uygun olacak şekilde tam yedekli bir yapıda kurulmalıdır. Bu sayede aktif cihazlardan birisinde yaşanabilecek olası kesinti durumunda ağ yedek hattan hizmet vermeye devam edebilmektedir.



Şekil 5. Tam yedekli cihaz kurulumu

Ağdaki cihazların kurulumu aşamasında dikkat edilmesi gereken diğer bir konu da ağın parçalara bölünmesidir. Bölme işlemi sanal yerel alan ağı (Virtual Local Area Network-VLAN) teknolojisi ile yapılabilmektedir. Ağın parçalara bölme işlemi, ağdaki sorunları daha hızlı çözmeye ve çeşitli yönetimsel politikaların daha kolay uygulanmasına yardımcı olmaktadır.

3.1.4. 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 köprü niteliğindedir ve bu nedenle tüm

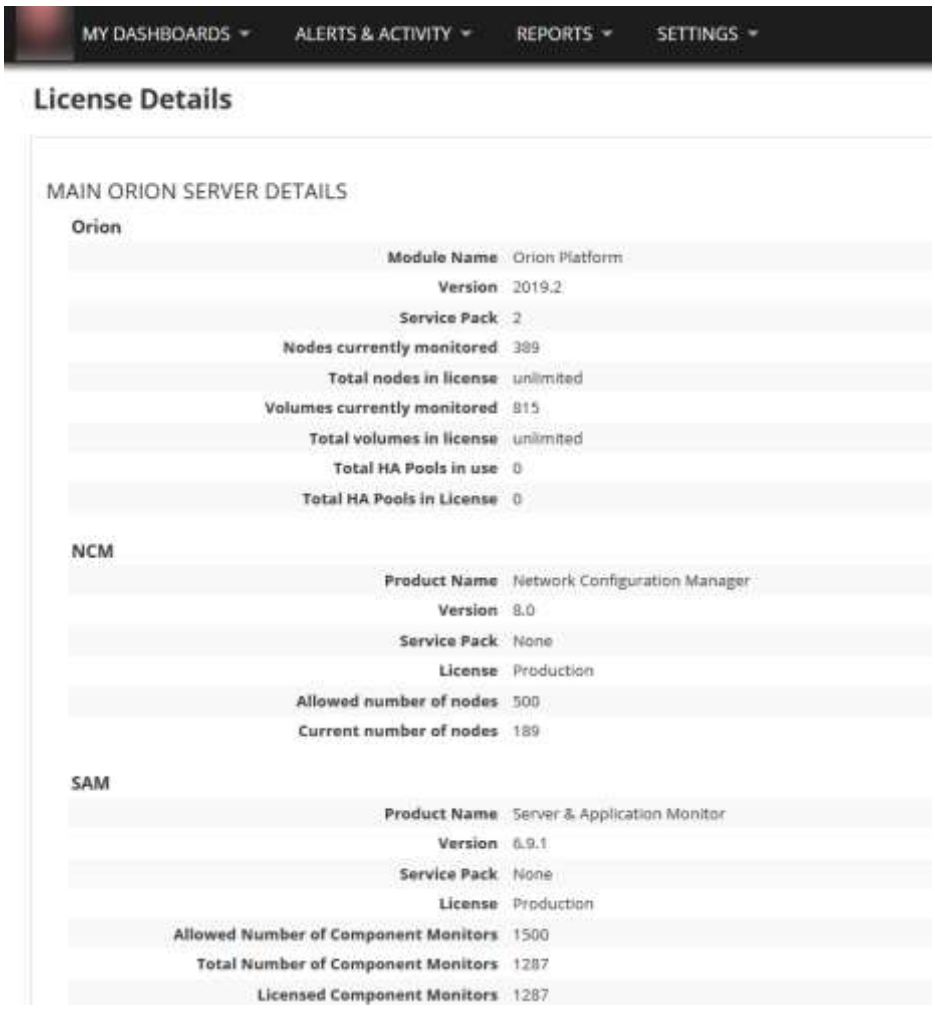
cihazlarda aktif hale getirilmesi gereklidir. Aynı şekilde ağ hizmetini etkileyecek veya cihazların çalışmasını durduracak saldırılara karşı güvenlik önlemlerinin alınması da gereklidir.

Ağ yönetim sistemlerinin döküm oluşturma ve cihaz yönetimi için kullandığı ağ yönetim protokolleri SNMP ve RMON'dur. Yönlendirici ve anahtar gibi aktif ağ cihazlarında bu işlem komut satırı ara-yüzü (Command Line Interface-CLI) ekranından yapılmaktadır. CLI ekranına, ağ cihazının uzaktan erişim ara-yüzünden (Secure Shell-SSH/ Telecommunication Network-TELNET) veya konsol portu üzerinden erişilerek gerekli yapılandırma ayarları yapılabilir. Ağ cihazlarının doğru yapılandırması ve gerekli güvenlik önlemlerinin alınması şirket içi veya dışarıdan (internet) yapılabilecek siber saldırılara karşı önlem sağlayacaktır. Özellikle MAC adres, DHCP ve DNS üzerinden yapılacak atakları engellemek için cihazlarda yapılan güvenlik yapılandırmaları hizmet kesintilerini önüne geçecektir. Ağ cihazlarına bağlantıların güvenli protokoller (SSH, HTTPS) üzerinden yapılması ise yetkisiz erişimleri ve araya girme (man in the middle) saldırılarının yapılmasını zorlaştıracaktır.

3.1.5. Ağ yönetim sistemi yazılımı seçimi

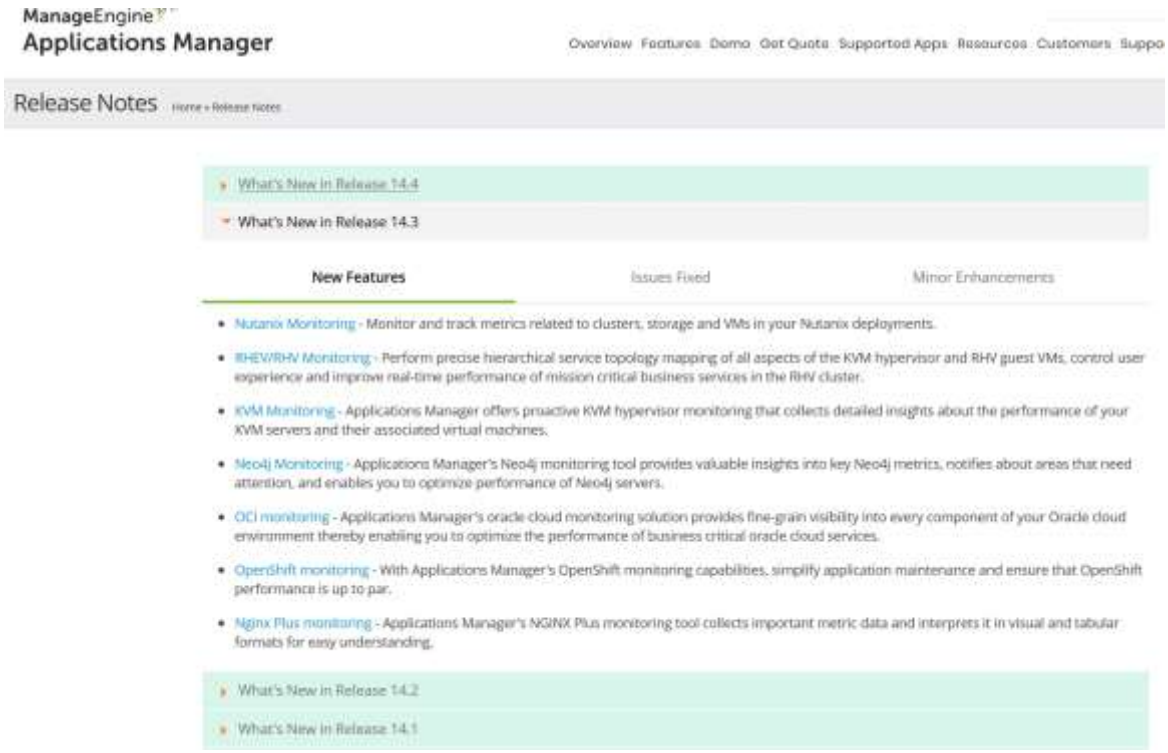
Ağ yönetim sistemi seçilirken ürünün hangi ölçüde, ne gibi çözümler sunduğu ve ne kadar maliyetle temin edilebileceği şirketler için önem arz etmektedir. Sadece protokol tabanlı ağ etkinliklerini izleyen basit bir ürün tercih edilebileceği gibi cihazları otomatik yoklayan, dağıtılmış bir veri tabanına 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. Ağ yönetim sistemi tercih ederken aşağıdaki beş etkeni göz önünde bulundurmak önemlidir.

- Kapsam: Düşünülecek ilk konu NMS'in neleri kapsadığıdır. Yazılım kurumsal geniş alan ağının yalnız bir bölümünde mi kullanılacak yoksa birden fazla yerde mi kullanılacak, NMS ile ağ cihazları dışında sunucu, servis veya sanal ortamlar gibi farklı sistemler yönetilecek mi gibi soruların yanıtları sonucunda kapsam belirlenmesi yapılmalıdır. . İncelemiş olan Cisco Prime ve Solarwinds NMS ürünleri ele alınacak olursa, gerçek ortamda yapılan deneyimlerde her ikisi de ağ cihazlarının keşfedilmesi, ağ cihazlarına toplu yapılandırma ayarı yapabilmesi, ağ performans değerlerinin takibi ve ağda yaşanan arızlara yarı otonom müdahalelerde bulunabilmeleri gibi işlemlerde aynı başarıyı göstermiştir. Bir ağ uzmanının ihtiyaçlarını başarıyla yerine getirmiştir. Ancak konu sunucu kaynaklarının (cpu, ram, disk vb.) takibi, depolama sistemlerinin yönetimi (storage), sanallaştırma yönetimi gibi farklı çözümler sunmaya geldiğinde Cisco Prime bu alanda varlık gösterememiştir. İnceleme sonucunda da görüldüğü gibi ürün tercih edilirken şirketin IT içerisinde bulunan sistem, ağ, güvenlik, yazılım ve hatta son kullanıcı desteği veren birimlerin ihtiyaçları göz önüne alınarak kapsam belirlenmelidir.
- Ölçeklenebilirlik: Yıllar geçtikçe ağın sürekli genişleyeceği ve iş gereksinimlerinin artacağı düşünülerek, bununla paralel NMS'in gelişen ihtiyaçlara cevap verebilmesi gereklidir. Şekil 6'da Solarwinds ağ yönetim sistemi ürünü lisans bilgileri görülmektedir. İncelediğimiz üründe görüldüğü gibi çeşitli kullanım değerleri (yönetilecek cihaz, kullanılacak sensör, izlenecek bileşen) sayısı üzerinden ürün lisanslanmıştır. Çalışma kapsamında incelediğimiz ücretli ürünlerin tamamında aynı şekilde lisanslama gerçekleştirilmektedir. Buradaki belirlenen lisans sayıları dolması halinde sisteme dâhil olacak yeni cihazların yönetimi yapılamayacaktır. Tüm bu bilgiler göz önüne alınarak ürün seçiminde gerekli lisans sayıları gelecek düşünülerek belirlenmelidir.
- 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. İnternet üzerinde genel bir tarama yapıldığında NMS üreticileri müşterilerin kendi bulut ortamları üzerinden ürünlerinin kullanımı için yıllık ücret talep etmektedir. Şirketin ürünü kısa vadeli kullanma gibi bir planı varsa bu yöntem doğrudan ürünü satın alıp ağa kurmaktan daha avantajlı fiyatlara gelmektedir. Ancak süre uzadıkça ve kapasiteler (yönetilecek cihaz sayısı, depolanacak veriler vb.) arttıkça yapılacak maliyet, ürününü satın alıp yerinde kullanma fiyatlarını aştığı görülmektedir. Bulut ortamının en önemli avantajı dünyanın her yerinden sisteminizi yönetme imkânı sunmasıdır. Dezavantaj ise şirketin internetin de yaşanabilecek kesintide NMS devre dışı kalacaktır. Diğer önemli bir sorun ise tüm IT altyapınızla ilgili bilgileri ve yönetimini başka bir şirketin erişebileceği ortam üzerinde tutmanızdır. Bu durum şirketin bilgi kaynaklarının kötü amaçlı kişilerin eline geçme riskini artırmaktadır. NMS hizmetini bulut ortamı üzerinden alımı kritik öneme sahip olamayan ve daha küçük ölçekli şirketlerin tercih etmesi daha isabetli bir seçim olacaktır.



Şekil 6. Solarwinds ağ yönetim sistemi ürünü lisans bilgileri ekranı

- Destek: Tercih edilecek olan ürünün üreticisi tarafından teknik desteğinin olması önemlidir. Yaşanabilecek yazılıma bağlı hataların düzeltilmesi, güncellemeler ile yenilikler yapılması ve ihtiyaç halinde yeni araçların yazılıma dâhil edilebilmesi gibi konularda gelişime ve yardıma açık bir NMS tercih edilmesi dikkat edilmesi gerekli bir husustur. Özellikle testlerini yapmış olduğumuz ürünlerden dağıtımı ücretsiz olanlarda böyle bir geliştirme görülmemektedir. Cacti ürünü ağdaki hatların kullanım trafiğini göstermek dışında bir çözüm sunmamaktadır. Ürünün geliştirildiği yıldan itibaren bakıldığında yeni bir özellik eklemesi veya geliştirme yapılmadığı görülmektedir. Aynı şekilde Whatsup Gold da yıllardır ağ cihazlarının ve sunucuların çalışma durumlarını göstermek dışında bir özellik sunmamaktadır. Diğer yandan Şekil 7'de görüldüğü gibi incelediğimiz ücretli bir ürün olan ManageEngine sürekli güncellemeler yayınlayarak, IT ihtiyaçlarına yönelik yeni özellikleri ürününe eklemektedir. Microsoft, Cisco, PaloAlto gibi birçok farklı üreticiye ait yeni servis ve hizmetlerin takibi, kullanımı ile ilgili özellikleri kullanıcılarına sunmaya çalışmaktadır.



Şekil 7. ManaeEngine ağ yönetim sistemi ürünü sürüm yeniliklerini gösteren resmi sayfası [25]

- Özellikler ve araçlar: Ağ yönetim sistemlerinin incelendiği ikinci bölümde verilen Tablo 1'de karşılaştırılan 14 kriterden yola çıkarak tercih edilecek NMS'de bulunması gereken özellikler ve araç listeleri oluşturulmalıdır. Tüm bu etkenlerin sonunda yine tablodaki maliyetler düşünülerek yazılım tercihi yapılmalıdır.

3.1.6. Ağ yönetim sistemi kurulumu

Ağ yönetim sistemini temel ayarları yapıldıktan sonra hesap, hata, yapılandırma, performans ve güvenlik yönetimleri için yapılması gerekli işlemler bulunmaktadır. İşlemlerin eksiksiz yapılması halinde, ağ yöneticilerin iş yükü büyük ölçüde azalmakta, ağda yaşanacak sorunlar hızlı çözümlenmekte, kurumsal sistemlerin güvenliği sağlanmakta ve kaynakların performansı verimli kullanılmaktadır. Yapılacak işlemler maddeler aşağıda halinde açıklanmıştır.

- Her bir yönetici için farklı kullanıcı giriş hesabı açılıp, sistemde sorumlu olduğu alanlar yetkilendirilmelidir. Bunun yapılabilmesi için kullanıcı grupları oluşturulup, NMS'e erişecek kullanıcıların yazılım içerisinde yapabilecekleri işlemler kısıtlanmalıdır.
- IP tanıtılması, VLAN yapılandırmaları ve protokolleri hazır hale getirilen aktif cihazlar NMS'e öğretilmelidir. Öğretilen cihazlar, yönetim açsından kolaylık sağlaması amacıyla üretici, cihaz türü, bulunduğu konum, durum bilgisi (açık/kapalı) gibi belirleyici gruplara ayrılmalıdır.
- Cihazların belli aralıklarla ve ayarlarda yapılan değişikliklerden sonra otomatik yedeklerinin alınması sağlanmalıdır. Alınan yedekler kayıt altında tutulup, ihtiyaç halinde geri dönülebilmelidir.
- Güvenlik yönetimi için gerekli tüm yapılandırma ayarları cihazlara uygulanmalıdır. Toplu yapılandırma özelliği kullanılarak cihazların tümüne şifre verilmesi, TELNET bağlantısının kapatılması, cihazlara yetkisiz erişim veya ağda yaşanabilecek sızmalara karşı cihaz erişim kontrol (Media Access Control-MAC) ve IP adresi tabanlı saldırıları önleyici ayarlar yapılmalıdır. Anahtar cihazlarında port security, dhcp snooping ve spanning tree protokolü güvenlik yapılandırmaları aktifleştirilmelidir. Bu ayarlar sayesinde şirket içerisinden gelebilecek saldırılar büyük ölçüde önlenecektir.
- Ağ ve sistemler üzerinde yaşanabilecek hataların alarm tanımları yapılmalıdır. Özellikle cihaz kaynak kullanım durumlarında (işlemci, bellek, ısı vb.) eşik değerleri verilmelidir. Son olarak alarm oluşması anında NMS'in yapması gerekli olayların (sorumlu birim yöneticilerine bildirimin sağlanması, ağ cihazı üzerinde yapılandırma değişikliğinin yapılması, port ara-yüz durumunun değiştirilmesi vb.) kuralları oluşturulmalıdır.

- Cihazların durumu, alarm bildirimleri ve ağda yaşanan tüm olayların takibi için kontrol ekranı hazırlanmalıdır. Görüntülenmesi önem arz eden nesnelerin alarm bildirimleri, bilgi grafikleri ve görselleri hazır hale getirilmelidir.
- Ağ ve sistemlerle ilgili günlük, haftalık, aylık raporlar ve sistem günlük (log) kayıtları dosya sunucularına yedeklenerek, yetkili yöneticilere mail yoluyla gönderilmelidir. Raporlama yapılırken özellikle cihazların, hatların ve uygulamaların kaynak kullanımına yönelik şablonlar hazırlanmalıdır.

3.2. Modellenen Kurumsal Ağ Yönetim Sisteminde Elde Edilen Sonuçlar

Kurumsal ağın anlatılan talimatlar doğrultusunda kurulup, ağ yönetim sistemiyle bütünleştirilmesiyle zaman, iş gücü, maliyet, güvenlik ve kaynak kullanımı gibi ağın işleyişini sağlayan birçok etkende fayda sağlanabilmektedir. Tablo 2'de yapılan işlemler ve sağlanan faydalar gösterilmiş olup, kurumsal geniş alan ağının tasarım ve yönetim bölümlerinde elde edilen sonuçlar değerlendirilmiştir.

Tablo 2. NMS kurulumunda yapılan işlemlerden elde edilen sonuçlar

Yapılan İşlem	**Sonuç**
Yedekli kurulum	Ağda yaşanabilecek olası hatalarda hizmetlerin sürekliliğini sağlamıştır. Bu durum hem problemlerin çözümünde zaman kazandırmış hem de maddi kayıpların önüne geçmiştir.
Cihazlara doğru yapılandırma ayarı yapma	NMS'in donanımlar ile iletişim kurmasını sağlamak ve ağ yönetim protokollerinden kaynaklı olabilecek siber tehditleri önlemek için yapılmıştır.
Ağ topolojileri oluşturma	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, 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.
Yapılandırma ayarı yedekleri alma	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. Ayrıca oluşabilecek donanım arızalarının ve hat bant genişliği doygunluğunun (saturation) önüne geçilmiştir.
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.
Kontrol ekranı düzenleme	Yöneticilerin ağı ve ağda oluşan olayların anlık takibini yapabilmeleri sağlanmıştır.
Cihaz log kayıtları tutma	Ağda oluşan hatanın hangi etkenden kaynaklandığının bulunması kolaylaşmış ve dolaylı yoldan yöneticilerin sorun giderme süreleri kısalmıştır.
Rapor şablonları hazırlama	Yöneticilerin ağ ve sistemler hakkında geçmişe dönük günlük, haftalık, aylık, yıllık hazırladıkları raporlar doğrultusunda şirketlerin yatırım maliyetlerini doğrudan etkileyecek veriler elde edilmiştir.

4. SONUÇLAR

Ağ yönetimi bilgisayar ve ağa bağlanan kullanıcılarının güvenliğinin temini açısından önemli bir konudur. Geniş ve birbirinden uzak yerlerde konumlanmış çok sayıda yönetim alanına sahip olabilen kurumsal ağlarda, güvenli ve yüksek performanslı ağ bağlantısı olan bilgisayar altyapıları kullanılmaktadır. Bu ağ yapılarında kullanılan cihazlarda donanım ve/veya yazılım kaynaklı arızalar ortaya çıkabilmekte ve bunun sonucunda ağ performansı düşebilmektedir. Bu makalede yapılan çalışma sonucunda;

- Ağın kurulum aşamasında planlı bir çalışma yapılması, ağın yönetimini doğrudan etkilediği görülmüştür.
- Ağ cihazlarının doğru yapılandırması ve gerekli güvenlik önlemlerinin alınması, donanımların bulunacağı veri merkezinin standartlara uygun inşa edilmesi, hiçbir işlem yapmadan önce ağın detaylı topolojisinin çıkarılması konularında yapılan işlemler sonucunda elde edilecek faydalar gösterilmiştir.
- Ağ yönetim sistemlerinin barındırdığı teknoloji ve mimari detaylı anlatılarak; bu kavramla ilgili standartlar, ağ yönetimi sistemi seçilirken bakılması gereken noktalar, ağ yönetim sistemi kurulurken yapılacak adımlar listelenerek ağ yönetiminde görev alacak uzmanlara yol gösterici bir içerik olarak sunulmuştur.
- Çalışma süresince incelenen ağ yönetim sistemleri her ne kadar yöneticilerin işini kolaylaştırsa da en önemli eksiklikleri tam otonom yapıya sahip olmamalarıdır.
- Bir otonom ağ yönetim sisteminden kendini en iyi duruma getirme, koruma, yapılandırma ve iyileştirme yeteneklerine sahip olması beklenmektedir.
- Bu beklentinin doğal bir sonucu olarak otonom bir ağ yönetim sisteminin; kullanılan ağı, cihazları ve meydana gelen olayları kendi kendine öğrenebilmesi ve analiz edebilmesi gereklidir.
- Kurumsal şirketlerin, teknoloji ile paralel olarak eğitimden pazarlamaya kadar her konuda ağ teknolojilerine duydukları ihtiyaç artması nedeniyle, gelecekte ağ altyapısı yönetiminin giderek artan karmaşıklığı ile mücadele edebilmek için, insan müdahalesi gerek olmadan tamamen bağımsız, otonom yönetim sistemleri kullanılmaya başlanması kaçınılmaz bir gerçektir.

KAYNAKLAR

[1] T. Xiaoyu, L. Lu, L. Ying, "A New Generation Theory and Technology of Mobile Fusion Network," Posts and Telecommunications Press, vol. 11, pp. 101-103, 2012.

[2] A. Hakiri, A. Gokhale, P. Berthou, D. C. Schmidt, and T. Gayraud, "Software-defined networking: Challenges and research opportunities for future internet," Computer Networks, vol. 75, part A, pp. 453-471, 2014.

[3] Y. Wang, and I. Matta, "Multi-layer virtual transport network management," Computer Communications, vol. 130, pp. 38-49, 2018.

[4] L. Gupta, T. Salman, M. Zolanvari, A. Erbad, and R. Jain, "Fault and performance management in multi-cloud virtual network services using AI: A tutorial and a case study," Computer Networks, vol. 165, 106950, 2019.

[5] H. Ramezani, H. ZakiDizaji, H. Masoudi, and G. Akbarizadeh, "A new DSWTS algorithm for real-time pedestrian detection in autonomous agricultural tractors as a computer vision system," Measurement, vol. 93, pp. 126-134, 2016.

[6] I. Rubin, A. Baiocchi, Y. Sunyoto, and I. Turcanu, "Traffic management and networking for autonomous vehicular highway systems," Ad Hoc Networks, vol. 83, pp. 125-148, 2019.

[7] R. M. da Silva Bezerra, and J. S. B. Martins, "Network autonomic management: a tutorial with conceptual, functional and practical issues," IEEE Latin America Transactions, vol. *12*(2), pp. 306-314, 2014.

[8] L. S. Yang, and Q. Wang, "Analysis of Network Management Technology and Development Trend In The Future," Advanced Materials Research, vol. 760, pp. 1192-1196, 2013.

[9] U. H. Rao, and S. Mohapatra, "Deploying network management solutions in enterprises," INC2010: 6th International Conference on Networked Computing, 2010, pp. 1-6.

[10] F. P. Tso, S. Jouet, and D. P. Pezaros, "Network and server resource management strategies for data centre infrastructures: A survey," Computer Networks, vol. 106, pp. 209-225, 2016.

[11] R. Sahay, W. Meng, and C. D. Jensen, "The application of Software Defined Networking on securing computer networks: A survey," Journal of Network and Computer Applications, vol. 131, pp. 28-108, 2019.

[12] H. K. Kalutarage, S. A. Shaikh, I. P. Wickramasinghe, Q. Zhou, and A. E. James, "Detecting stealthy attacks: Efficient monitoring of suspicious activities on computer networks," Computers & Electrical Engineering, vol. 47, pp. 327-344, 2015.

[13] M. Tün, E. Pekkan, ve S. Tunç, "Yer Sarsıntı Haritalarının Üretilmesinde Sismik Ağ Yapısı: Eskişehir Örneği," Harita Teknolojileri Elektronik Dergisi, vol. 7, pp. 1-14, 2015.

[14] A. Iqbal, "Monitoring Remote Financial Transaction Control Devices Using SNMP Over TCP," PhD thesis, Kent State University, Ohio, 2009.
[15] M. Alkasassbeh, G. Al-Naymat, A. B. Hassanat, and M. Almseidin, "Detecting distributed denial of service attacks using data mining techniques," International Journal of Advanced Computer Science and Applications, vol. 7, pp. 436-445, 2016.
[16] G. Al-Naymat, M. Al-Kasassbeh, and E. Al-Hawari, "Exploiting SNMP-MIB Data to Detect Network Anomalies using Machine Learning Techniques, Proceedings of SAI Intelligent Systems Conference, 2018, pp. 991-1004.
[17] Q. Honglei, D. Zemin, and G. Lihong, "Computer Network Management Software," Computer System Networking and Telecommunications, pp. 24-31, 2017.
[18] A. Roohi, K. Raeisifard, and S. Ibrahim, "An application for management and monitoring the data centers based on SNMP," In 2014 IEEE Student Conference on Research and Development, 2014, pp. 1-4.
[19] H. Hegering, S. Abeck, B. Neumair, "Integrated Management of Network Systems," In M. KAUFMANN, Saint Louis: Morgan Kaufmann Publishers, 1999, pp. 380-400.
[20] A. Clemm, Network Management Fundamentals. Indianapolis: CiscoPress, 2006.
[21] J. Case, R. Mundy, D. Partain, and B. Stewart, "Introduction and Applicability Statements for Internet-Standard Management Framework," IETF, RFC3410, 22 Dec., 2002.
[22] J. Ding, Advances in Network Management. New York: CRC Press, 2010.
[23] E. Binici, "Java İle Yapay Zekâ Mekanizmasına Sahip Bir Ağ Yönetim Sistemi Geliştirilmesi," Yüksek Lisans Tezi, Ege Üniversitesi, İzmir, 2006.
[24] Teksernet Ortak Kullanımlı Telsiz hizmetleri, "Sayısal Geniş Alan Kaplama Sistemleri (IPSC)," [Online]. Available: http://www.teksernet.com.tr/kategori.php?id=45/. [Accessed: Jan. 05, 2020].
[25] ManageEngine, "ManageEngine Applications Manager Release Notes," [Online]. Available: https://www.manageengine.com/products/applications_manager/release-notes.html. [Accessed: Jan. 05, 2020].