T.C.
BAHÇEŞEHİR ÜNİVERSİTESİ

ORTA ÖĞRETIM KURUMLARINDA ÜCRETSİZ YAZILIM KULLANARAK İNTERNET ÇIKIŞININ KONTROLÜ VE İNCELENMESİ

Yüksek Lisans Tezi

Murat Uğur ÖZÖREN

Istanbul, 2011

T.C.
BAHÇEŞEHİR ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
BİLGİ TEKNOLOJİLERİ PROGRAMI

ORTA ÖĞRETIM KURUMLARINDA ÜCRETSİZ YAZILIM KULLANARAK İNTERNET ÇIKIŞININ KONTROLÜ VE İNCELENMESİ

Yüksek Lisans Tezi

Murat Uğur ÖZÖREN

Tez Danışmanı : Yrd. Doç. Dr. Yalçin ÇEKİÇ

Istanbul, 2011

T.C.
BAHÇEŞEHİR ÜNİVERSİTERSİ
Fen Bilimleri Enstitüsü
Bilgi Teknolojileri Yüksek Lisans Programı

Tezin Başlığı :Orta Öğretim Kurumlarında Ücretsiz Yazılım Kullanarak İnternet Çıkışının Kontrolü ve İncelenmesi
Öğrencinin Adı Soyadı : Murat Uğur ÖZÖREN
Tez Savunma Tarihi : 26.01.2011

Bu yüksek lisans tezi Fen Bilimleri Enstitüsü tarafından onaylanmıştır.

Yrd. Doç. Dr. Tunç BOZBURA
Enstitü Müdürü V.

Bu Tez tarafımızca okunmuş, nitelik ve içerik açısından bir Yüksek Lisans tezi olarak yeterli görülmüş ve kabul edilmiştir.

Tez Sınav Jürisi Üyeleri :

Yrd. Doç. Dr. Yalçın ÇEKİÇ (Tez Danışmanı) :

Doç. Dr. Adem KARAHOCA :

Yrd. Doç. Dr. Mehmet Alper TUNGA :

ÖNSÖZ

Yüksek lisans öğrenimim sırasında ve tez çalışmalarım boyunca gösterdiği her türlü destek ve yardımlardan dolayı çok değerli hocam Yrd. Doç. Dr. Yalçın ÇEKİÇ'e en içten dileklerimle teşekkür ederim.

Bu çalışma boyunca yardımlarını ve sabrını esirgemeyen eşim Özlem ÖZÖREN'e, Anneme, Babama ve kardeşim Ali Rıza ÖZÖREN'e, Şişli Endüstri Meslek Lisesi Bilişim Teknolojileri Alanı öğretmenlerine ve arkadaşlarıma teşekkürü borç bilirim.

Ocak 2011

Murat Uğur ÖZÖREN

ÖZET

ORTA ÖĞRETIM KURUMLARINDA ÜCRETSİZ YAZILIM KULLANARAK İNTERNET ÇIKIŞININ KONTROLÜ VE İNCELENMESİ

Özören, Murat Uğur

Bilgi Teknolojileri Yüksek Lisans Programı

Tez Danışmanı: Yrd. Doç. Dr. Yalçın Çekiç

Ocak, 2011, 109 sayfa

İnternet, son yıllarda hızla gelişmesi ve yaygınlaşması ile günlük hayatımızın vazgeçilmez bir parçası haline gelmiştir. Bu gelişime paralel olarak da internet üzerinden çeşitli suçlar işlenmesi, yapılan internet erişim kayıtlarının tutulmasını gerekli kılmıştır. İnternet servis sağlayıcılar, kullanıcılarının internet erişim kayıtlarını, internet adresi - tarih eşlemesi şeklinde tutmaktadır. Ancak internetin toplu kullanılmasının sağlandığı ortamlarda, hangi kullanıcının internet bağlantısını kullanarak suça karıştığını belirlenmesi için internet erişim kayıtların tutulması görevi TCK'nın 5156 sayılı kanun ile internet servis sağlayıcısı abonesine verilmiştir.

Bu nedenle toplu internet kullanımı ortamlarından olan Milli Eğitim Bakanlığına bağlı eğitim kurumlarında da internet erişim kayıtlarının tutulması gerekliliği ortaya çıkmıştır. Ancak, okullar için sağlanan ödenekler çok kısıtlı olduğundan, erişim kayıtlarının tutulması ve saklanması işleminin ücretsiz yazılımlar kullanılarak yapılması daha uygundur. Bu amaçla bu tezde TCK'nın 5651 sayılı kanununun gerektirdiği internet trafiği bilgisinin kaydedilmesi ve saklanması işlemi, bir orta öğretim kurumunda gerçekleştirilmiştir. Tezin uygulama aşamasında, öncelikle orta öğretim kurumunun bilgisayar ağ altyapısı planlanarak, kurulmuş ve bunu takiben özgür yazılım dünyasında sıkça kullanılan ücretsiz programlardan olan IPCop ve untangle programları ile internet erişim kayıtları ayrı ayrı tutulmuştur.

Sonuç olarak her iki programın çeşitli yönlerden avantaj ve dezavantajları ortaya konularak orta öğretim kurumlarında internet erişim kayıtlarının tutulabilmesi için en uygun olan program tespit edilmiştir.

Anahtar Kelimeler: Erişim kaydı, IPCop, Untangle, İnternet suçları, 5651 sayılı kanun

ABSTRACT

THE CONTROL AND ANALYSIS OF INTERNET CONNECTION IN SECONDARY SCHOOLS BY USING A FREE SOFTWARE

Özören, Murat Uğur

M.S. in Information Technologies Graduate Program

Supervisor: Assist. Prof. Dr. Yalçın Çekiç

January, 2011, 109 pages

Internet has become an indispensable part of our lives, thanks to the recent developments and their penetration. Due to the increase in crimes resulting from the extensive usage of technologies, it has become essential to log the records. Internet Service Providers log the records of the users, in internet address-history format. However, in places where internet is for common share, the duty of logging the records and identifying which user has committed a crime through internet connection is given to the Internet Service Providers subscriber, by the authorization of the law of 5156.

As a result of this law, the necessity of logging the records of the Internet access in state schools, which are an example of common internet use, has emerged. However, as the financial contribution of the state to schools is not sufficient, it is a necessity to use free software to log the record. For the purposes of this dissertation, logging of Internet access was applied in a states secondary school in compliance with the law of 5156l. In the application part of this dissertation, firstly the network of the school was designed and started and followingly the records of Internet access are logged through Ipcop and untangle software, which are frequently found in free software world.

In conclusion, the advantages and the disadvantages of both programmes were discussed and the most convenient program for the end stated above was displayed.

Key words: Log, Access record, IPcop, Untangle, Netcrime, The law of 5651

İÇİNDEKİLER

TABLOLAR

ŞEKİLLER

KISALTMALAR

Alan Adı Sistemi (Domain Name System)	:	DNS
Asymmetric Digital Subscriber Line (Asimetrik Sayısal Abone Hattı)	:	ADSL
Bellek (Random Access Memory)	:	RAM
Central Processing Unit	:	CPU
Denial of Service	:	DoS
Dynamic Host Configuration Protocol	:	DHCP
File Transfer Protocol (Dosya transfer protokolü)	:	FTP
GigaByte	:	GB
International Organization of Standardization	:	ISO
International Specialty Products (İnternet Servis Sağlayıcı)	:	ISP
Internet Control Message Protocol (İnternet mesaj control protokolü)	:	ICMP
Internet Protocol (İnternet Protokolü)	:	IP
İletim Kontrol Protokolü (Transmission Control Protocol)	:	TCP
İnternet erişim kaydı.	:	Log
Kilobit per second	:	Kbps
Korumalı çiftbükümlü ağ kablosu	:	STP
Korumasız çiftbükümlü ağ kablosu	:	UTP
Küçük ofis/Ev ofisi	:	SOHO
Local Area Network (Yerel alan ağı)	:	LAN
Megabit per second	:	Mbps
MegaByte	:	MB
National Science Foundation	:	NFS
Open System Interconnection	:	OSI
Peer to peer	:	P2P

Sanal özel ağlar (Virtual Private Network)	:	VPN
Simple Mail Transfer Protocol	:	SMTP
Simple Network Management Protocol (Basit ağ yönetim protokolü)	:	SNMP
Türk Ceza Kanunu	:	TCK
Uniform Resource Location	:	URL
Wide Area Network (Geniş alan ağı)	:	WAN
World Wide Web	:	WWW
Zengin Metin İşaretleme Dili (Hyper Text Markup Language)	:	HTML

1. GİRİŞ

Bilindiği gibi internetin ortaya çıkması ve son yıllarda hızla yaygınlaşmasıyla, günlük hayatımızdaki birçok işin yapılması ve kullanıcıların bilgiye olan erişimi daha önce hiç olmadığı kadar kolaylaşmıştır. Bilgiye olan erişimi sağlamada sunduğu kolaylıklar nedeni ile internet, öğrenci ve öğretmenlerin okul kütüphanelerinde araştırma yapabilmesi için ve mesleki eğitimde araç olarak kullanılmaktadır. Buna ek olarak Milli Eğitim Bakanlığı tarafından oluşturulan e-Okul Veli Bilgilendirme Sistemi'ne yönetici ve öğretmenlerin bilgi girişi yapmaları için tüm eğitim kurumlarında kullanılmaktadır. Eğitim kurumları da dâhil olmak üzere bu kadar yaygın olarak kullanılan internetin maksadını aşan amaçlarla kullanılmasına engel olmak ve bu şekildeki kullanımları tespit etmek amacı ile yasal düzenlemelere gidilmiştir.

5651 sayılı "İnternet ortamında yapılan yayınların düzenlenmesi ve bu yayınlar yoluyla işlenen suçlarla mücadele edilmesi" yasasına göre, erişim sağlayıcı olan eğitim kurumları, sağladığı hizmetlere ilişkin trafik bilgilerini saklamakla ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlamakla yükümlüdür. İşte bu nedenle bu tezde amaçlanan, yasada belirtilen tedbirler kapsamında önlemler alabilmek için, bir orta öğretim kurumunun network yapısı planlanması, bu plan doğrultusunda yapılandırılıp, ücretsiz yazılımlar kullanılarak internet çıkışının kontrolü, elde edilen verilerin saklanması ve incelenmesi işlemi gerçekleştirilmesidir.

Tezin ikinci bölümde internet tanımlanarak, internetin toplu kullanımı için hukuki gereklilikler ele alınacaktır. Eğitim kurumlarındaki internet altyapıları konusunda giriş yapmak amacıyla, bilgisayar ağları ve ağ teknolojileri başlıkları teknik olarak incelenip, bir eğitim kurumunun network yapısı ele alınıp ve düzenlenecektir. Buna ek olarak yasa kapsamında istenilen kayıtların toplanabilmesi için gerekli sistemler değerlendirilecek, içlerinden en uygun olan vekil sunucu (proxy server) sistemi hakkında bilgi verilecektir.

Tezin üçüncü bölümünde ‘IPCop’ ve ‘untangle’ işletim sistemleri ile ilgili bilgi verilip, bir eğitim kurumunda bu sistemler kurularak yapılan uygulama hakkında bilgi verilecektir.

Sonuç bölümünde ise elde edilen bütün veriler ışığında bir eğitim kurumunun internet çıkışının kontrolünde kullanılabilecek en verimli kayıt tutma ve saklama yöntemi hakkında değerlendirme yapılacaktır.

2. BİLGİSAYAR AĞLARI

Bu bölümde internet, bilgisayar ağları ve güvenlik konularının rahatlıkla anlaşılabilmesi için gerekli olan genel bilgiler verilecektir. Bu bilgiler arasında internet, OSI referans modeli, TCP/IP referans modeli, ağ teknolojileri ve erişim kaydı (log) tutma işlemleri yer almaktadır.

2.1 İNTERNETİN TANIMI

İnternet, TCP/IP protokolüne bağlı olarak birçok bilgisayar ağının birbirine bağlanmasıyla oluşan bir ağ (network) sistemidir. Kısaca "ağların ağı" olarak da adlandırılan İnternet dünya çapındaki bilgisayar ağlarını ve bu ağlar üzerindeki bilgisayarları birbirine bağlayan bir yapıya sahiptir (Forcier 1999).

Bu ağın gelişmesine yönelik ilk girişimler soğuk savaş sırasında Amerika Birleşik Devletleri Savunma Bakanlığı (U.S. Department of Defense) tarafından başlatılmıştır. Ülkeye yönelik bir nükleer saldırı durumunda dahi işlevselliğini yürütebilecek bir iletişim ağının oluşturulması hedeflenmiştir (Forcier 1999). Böylece İnternet'in ilk temelleri ARPAnet (Advanced Research Projects Agency Network - İleri Düzey Araştırma Projeleri Kurum Ağı) olarak Amerika Birleşik Devletleri Savunma Bakanlığı'nın himayesinde, 1969 yılında atılmış oldu. 1970'lerde Amerika Birleşik Devletlerinde birçok merkezdeki bilgisayarlar ARPAnet'e bağlandı. 1980'li yıllara girildiğinde Amerika Birleşik Devletleri ordusu yeni bir bilgisayar ağı olarak MILITARY NET'i kurdu ve ARPAnet'ten ayrıldı. Bu sırada İletim Kontrol Protokolünün (TCP - Transmission Control Protocol) dört uyarlaması geliştirilip kullanılarak ARPAnet 'e bağlı bilgisayarlar arasındaki iletişim kolaylaştırılmıştır. 1983'te tüm ARPAnet kullanıcıları, İletim Kontrol Protokolü / İnternet Protokolü (TCP/IP - Transmission Control Protocol/İnternet Protocol) olarak bilinen yeni protokole geçiş yaptılar. 1990 yılında ARPAnet kullanımdan kaldırılarak yerini Amerika Birleşik Devletleri, Avrupa, Japonya, Pasifik ülkelerinde ticari ve hükümet işletimindeki omurgalara (backbone) bıraktı. ARPAnet'in kaldırılmasına rağmen, TCP/IP protokolü kullanılmaya ve geliştirilmeye devam edilmiştir. 1995'te Amerika

Birleşik Devletleri Bilimsel Araştırma Kurumu (NFS - National Science Foundation) bu yeni ağı, İnterneti, tanıtan bir bildiri yayınladı.

İnternet yapısına uygun olarak üniversiteler arasında yüksek-hız kapasitesine sahip bir bağlantı geliştirildi. Bu sayede evinden bir üniversite ağına bağlanan bir öğrenci ya da öğretim üyesi bu ağ ile bağlantısı olan diğer üniversite ağlarına da bağlanabilme olanağına sahip oldu. Bu bağlantı türü ağ geçidi (gateway connection) bağlantısı olarak adlandırıldı ve şu anda İnternet olarak bilinen ve dünya çapındaki bilgisayarları TCP/IP protokolüyle birbirine bağlayan ağın oluşmasına temel oluşturdu (Roblyer ve Edwards 2000). 1981'de sadece 213 bilgisayarın İnternet bağlantısı varken, 2000 yıllında bu sayı 400 milyona kadar ulaştı. 2010 yılında ise dünyadaki İnternet kullanıcısı sayısı 2 milyar kişiye ulaştığı kaydedilmiştir (http://www.internetworldstats.com).

Türkiye İnternetle ilk kez, 12 Nisan 1993'te Orta Doğu Teknik Üniversitesi'nden Ankara- Washington arasında kiralık hat kurularak yurtdışıyla sağlanan bağlantı sayesinde tanışmıştır. 1994'te kurumlara ve firmalara İnternet hesapları verilmeye başlanmasıyla, Sakarya Üniversitesi, Bilkent Üniversitesi, Boğaziçi Üniversitesi 1995 yılında, İstanbul Teknik Üniversitesi 1996 yılında internet bağlantılarını gerçekleşmiştir. 2010 yılı itibariyle MEB'ye bağlı ilköğretim okullarının yüzde 96'sında, orta öğretim okullarının da yüzde 100'ünde internet erişimini sağlandığı bildirilmiştir (MEB).

Günümüzde bir bilgisayar kullanıcısı internet aracılığı ile ağ bağlantısı olan milyarlarca bilgisayara bağlanıp, bu devasa ortamdaki bilgilerden yararlanabilir. İnternet aracılığı ile insanlar elektronik posta (e-posta) göndermenin yanı sıra, multimedya nesneleri kullanarak dünyanın çeşitli bölgelerindeki insanlarla eşzamanlı (senkron) ve eşzamansız (asenkron) olarak etkili ve ekonomik bir şekilde iletişimde bulunabilmektedirler. Ayrıca" www, Telnet, FTP, Portal" gibi temel internet uygulamaları ile de dünyanın herhangi bir yerindeki bilgiye kolaylıkla erişebilmektedirler.

2.1.1 İnternet Suçları ve İlgili Yasalar

İnternetin sosyal hayatın içine girmesiyle birlikte, birçok suç internet ortamında ya da internet aracılığıyla işlenir oldu. Bu sebeple TCK'nın onuncu bölümde bilişim alanında

suçlar tanımlanmış ve fiiller sınıflandırılmıştır. Bu kapsama giren 243. Madde'ye göre "Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren ve orada kalmaya devam eden kimseler bilgilere zarar vermeseler dahi suç işlemiş olurlar". Bir mail adresinin şifresini ele geçirerek içeriğini görüntülemek, bilgileri indirmek bu madde kapsamında işlenen bir suça örnek teşkil eder.

Bu bölümde yer alan 244. madde'ye göre ise "Bir bilişim sisteminin işleyişini engelleyen, bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi veya kişiler suç işlemiş olurlar." Bir internet sayfasına erişimi engelleme, içeriğini değiştirmek, halk arasında "Hackerlık" olarak nitelendirilir ve bu madde kapsamında işlenen suçlara bir örnektir.

Bu maddeleri takip eden 245. Madde'ye göre de "Başkasına ait bir banka veya kredi kartını, her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimse, kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın bunu kullanarak veya kullandırtarak kendisine veya başkasına yarar sağlarsa suç işlemiş olur". Başkasına ait bir kredi kartı ile internet üzerinden yapılacak olan alışveriş işlemi bu madde kapsamında değerlendirilen bir suçtur. Ayrıca bu fiil internet aracılığıyla işlenen, 142. madde'de yer alan "Nitelikli Hırsızlık" ve 158. madde'de yer alan "Nitelikli Dolandırıcılık" suçları kapsamında da değerlendirilir.

Bilişim suçları kapsamına girmemekle birlikte diğer suçların, örneğin TCK'nin 81. maddesi'nde tanımlanan "Kişilere Karşı Suçların" aydınlatılması sürecinde gerekli delillerin toplanması amacı için internet kullanılmaktadır. Bu bağlamda suça karışan kişilerin internet üzerinden yaptıkları işlem geçmişleri incelenmekte ve olayların aydınlatılması için gerekli veriler araştırılmaktadır.

Yukarıda da belirtildiği gibi internet hukuk kapsamında hem suç işlemek için bir araç hem de suçların aydınlatılmasında bir yardımcı olarak kullanılmaktadır. Suçların aydınlatılması sürecinde savcılar İnternet üzerinden yapılan iletişimin tarih, saat ve IP bilgileri ile servis sağlayıcı (ISP) şirketlerden iletişimin yapıldığı adrese ve hizmeti satın alan, suça iştirak etmiş gerçek veya tüzel kişilere ulaşır. Ulaşılan bu adresteki gerçek veya tüzel kişiler TCK'nin 5651 sayılı "İnternet ortamında yapılan yayınların düzenlenmesi ve bu yayınlar yoluyla işlenen suçlarla mücadele edilmesi" halındaki

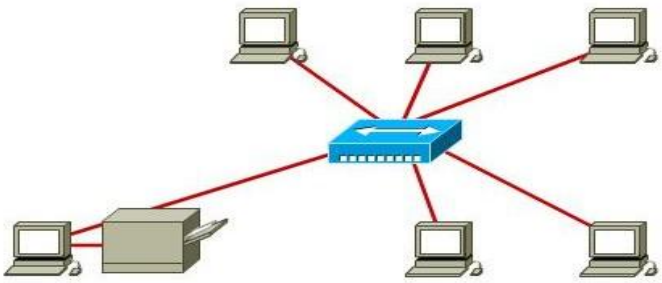
kanuna göre sağladıkları hizmetlere ilişkin trafik bilgilerini (Log) saklamakla ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlamakla yükümlüdürler (TCK).

2.2 BİLGİSAYAR AĞLARI VE AĞ TEKNOLOJİLERİ

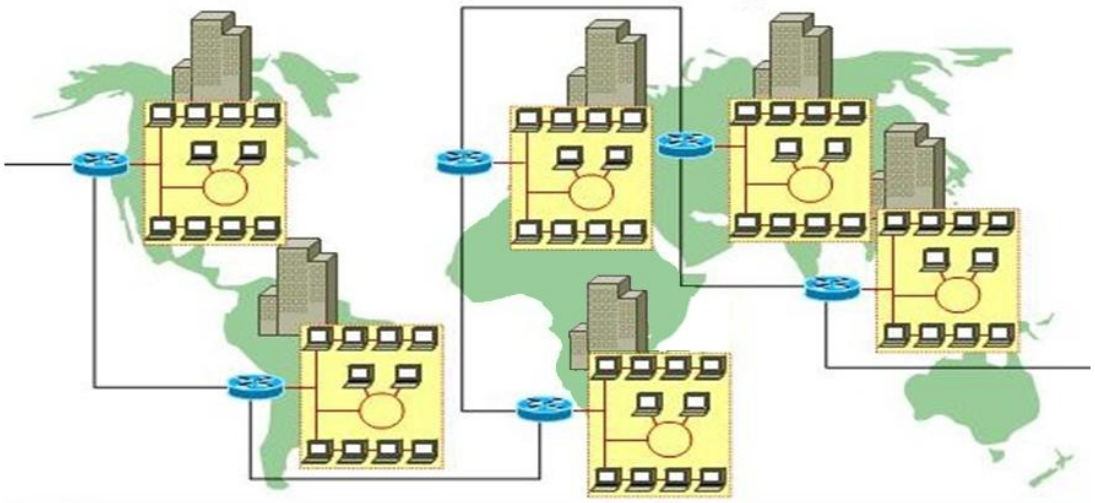
Ağ (Network) kavramı, var olan kaynakların kullanıcılar tarafından beraber kullanılması, bilgiye ortak ulaşılması ve buna bağlı olarak da maliyet ve zaman tasarrufu sağlanılması gereksiniminden ortaya çıkmıştır. Bu temel kuraldan hareketle oluşan ağlar, uzaktaki bilgiye erişim (Web), kişisel iletişim (E-posta, ICQ, IRC, Video-konferans), interaktif eğlence (Web-TV, oyunlar) gibi kavramlarla hayatımızda önemli bir yer kaplamaktadır (TAGEM).

Ağlar çok çeşitli boyutlarda olabilir. İki bilgisayardan oluşan basit ağlardan milyonlarca aygıtı bağlayan ağlara kadar pek çok boyutta ağ olabilir. Küçük ofislere veya evlere ve ev ofislerine yüklenen ağlara SOHO (Küçük ofis/Ev ofisi) ağları denir. SOHO ağları, yazıcı, belge, resim ve müzik gibi kaynakların birkaç yerel bilgisayar arasında paylaşılmasını sağlamaktadır. Şirket ağları ise bilgilerin ağ sunucularında birleştirilmesini, depolanmasını ve bu bilgilere erişilmesini sağlamanın yanı sıra e-posta ve IP-telefon gibi daha etkili ve daha uygun maliyetli servislerin kullanılmasına olanak veren ağlardır. Şirket ve SOHO ağları genellikle bir internet bağlantısının paylaşılmasını sağlamak için kullanılır.

Şekil 2.1 ve Şekil 2.2 ‘de görüldüğü gibi ağları yayıldıkları coğrafi alan açısından yerel alan (Local Area Network - LAN) ve geniş alan (Wide Area Network - WAN) ağları olarak ikiye ayırabiliriz.



Şekil 2.1 : Yerel alan ağları (Local Area Network: LAN)



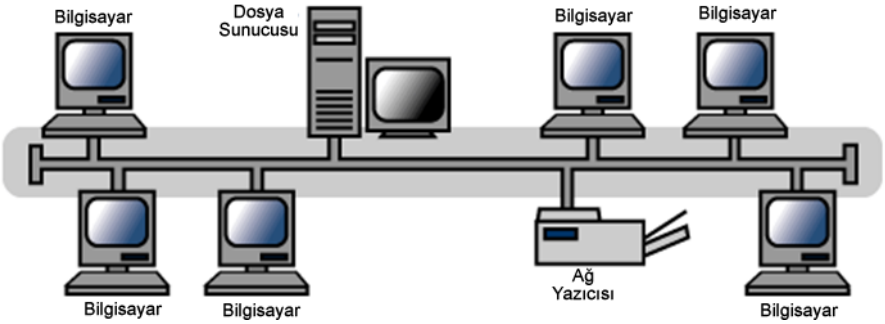
Şekil 2.2 : Geniş alan ağları (Wide Area Network: WAN)

2.2.1 Ağ Topolojileri

Topoloji, bilgisayar, yazıcı, ağ cihazları gibi donanımların birbirine fiziksel veya mantıksal bağlanma şekillerini tanımlayan genel bir terimdir. Temel olarak 3 topoloji vardır.

2.2.1.1 Doğrusal topoloji (Bus topology)

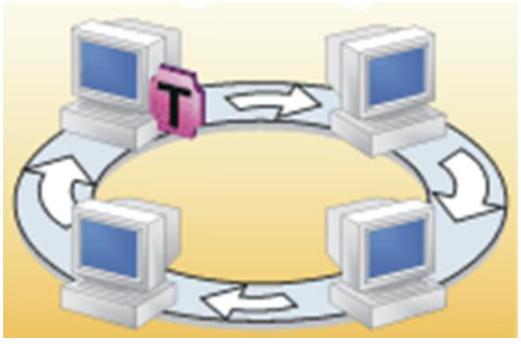
Doğrusal bir hat üzerinde kurulmuş bir yapıya sahiptir. Doğrusal topolojide bilgisayarlar Şekil 2.3'de görüldüğü üzere kabloya T-konnektörler aracılığıyla bağlanırlar. Kablo üzerinde sinyal yansımalarını engellemek için açıkta kalan iki uca sonlandırıcılar takılır. Bir makinede veya kablonun herhangi bir noktasında oluşan arıza tüm sistemin çalışmasını engeller. Bu topoloji, ağ performansı en düşük olan topolojilerden biridir. İki istasyon arası mesafe en fazla ince eş-eksenli kablo (thin coaxial) kullanıldığında 185 metre, kalın eş-eksenli kablo (thick coaxial) kullanıldığında 500 metre, en az ise 0,5 metredir. Doğrusal topoloji ağları 10Mbps hızda çalışır (Karris 2009, s.4-2).



Şekil 2.3 : Doğrusal topoloji (Bus topology)

2.2.1.2 Halka topoloji (Ring topology)

Halka topolojide Şekil 2.4'de görüldüğü gibi her istasyon halkanın bir elemanıdır ve halkada oluşan bilgi bütün istasyonlara ulaşır. Her istasyon, halkada oluşan bilgiyi ve hedef adresi alır. Hedef adres kendi adresi ise kabul eder. Aksi halde gelen bilgi işlem dışı kalır. Halkadaki bilgi akışı tek yönlüdür (Karris 2009, s.4-4). Halkaya dahil olan bilgisayarlar gelen bilgiyi iletmekle görevlidir. Ağda bulunan düşük hızlı bir kart tüm sistemi yavaşlatır. Kablonun herhangi bir noktasında oluşan arıza tüm sistemin çalışmasını engeller, En yaygın uygulaması IBM'e ait olan Token Ring topolojisidir. Bu topoloji 4Mbps veya 16Mbps hızda çalışır.

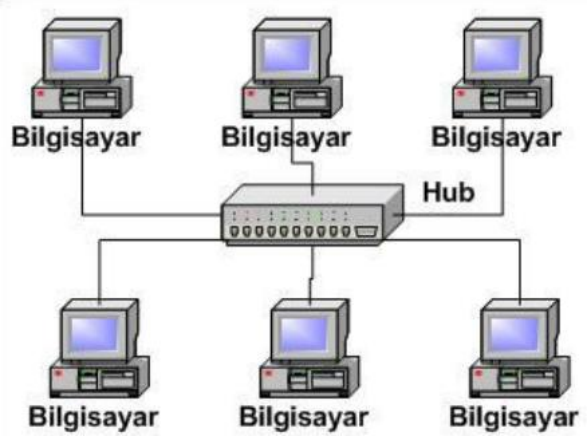


Şekil 2.4 : Halka topoloji (Ring topology)

2.2.1.3 Yıldız topoloji (Star topology)

Bu topolojide ağdaki iletişimin gerçekleşmesi için merkezi birim bulunur ve bütün istasyonlar Şekil 2.5'de görüldüğü gibi bu merkezi birime bağlanır (Karris 2009, s.4-3).

Bir istasyondan diğerine gönderilen bilgi önce bu merkezi birime gelir, buradan hedefe yönlendirilir. Ağ trafiğini düzenleme yeteneğine sahip bu merkezi birim, dağıtıcı (hub) ve anahtar (switch) olarak adlandırılan ağ cihazlarıdır. Bu topolojiye dayalı bir sistem kurulurken korumasız çift bükümlü (UTP - Unshieded Twisted Pair) veya korumalı çift bükümlü (STP - Shielded Twisted Pair) kablo kullanılır. İstasyonların merkezi birime olan uzaklığı en fazla 100 metredir. Kullanılan ağ kartına, ağ cihazına, kablo cinsi ve boyuna bağlı olarak 10Mbps ile 10Gbps arası hızlarda çalışabilir. Herhangi bir istasyonun arızalanması ağ trafiğini etkilemez ve ağa yeni bir istasyon eklemek çok kolaydır.



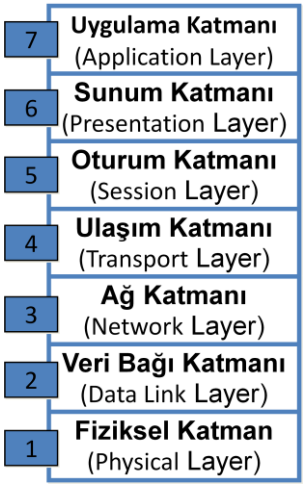
Şekil 2.5 : Yıldız topoloji (Star topology)

2.2.2 OSI (Open System Interconnect) Referans Modeli

İlk bilgisayar ağlarında farklı firmalar kendilerine özel teknolojilerle ağ sistemleri geliştirip satıyorlardı. Kendi başlarına düzgün çalışan bu ağlar farklı firmaların ağ sistemleri ile ortak çalışma yeteneğine sahip değildi çünkü her birinin kendilerine özel yazılımları ve donanımları vardı. Ağ sistemlerinin bu özel yapısı diğer donanım ve yazılım üreticilerinin ağlar için ortak ürün geliştirmesini de imkansız hale getiriyordu. Bir ağ sistemi kurmak istenildiğinde kablosundan ağ kartına, ağ cihazı ve ağ işletim sistemine kadar her şeyi üretici firmadan paket olarak çok yüksek bir fiyata alınıp bu firmaya bağımlı duruma geliniyordu. Ağ sistemlerine olan talebin artması ile ağ sistemlerinin işlevlerini tanımlayan ortak bir model oluşturulması gerektiği anlaşıldı. Bunu gerekli kılan bir diğer unsur ise ağ sistemlerini açıklamakta kullanılan terimlerin

üreticiden üreticiye değişiklik göstermesi, ağ üzerinde işlem gören yazılım ve donanım bileşenlerinin ne görev üstlendiklerinin standart halinde olmamasıydı. 1984 yılında Uluslararası Standartlar Organizasyonu (ISO) Şekil 2.6'da ki yedi katmanlı Open System Interconnection modelini (OSI) ortaya koydu.

OSI Modeli değişmez bir kanun değildir. İsteyen kendi başına bir ağ sistemi tasarlayabilir ve çalışır hale getirebilir. Ancak OSI modeli referans alınmadıysa diğer ağlarla iletişimi zor olacak, değişik üreticiler bu ağ sistemi için donanım ve yazılım üretemeyeceklerdir. OSI modeli, ağ iletişiminin karmaşık yapısını işlevsellik ve verdikleri hizmet açısından yedi ana katmana böler (Heap, Maynes 2002). Her katman yürüttüğü görevler ve hizmetler olarak kendi sorumluluğuna sahiptir. Böylece bir katmanda yapılan değişiklikler diğer katmanları etkilemez ve problemlerin tespiti ve çözümü kolaylaşır.



Şekil 2.6 : OSI (Open System Interconnect) referans modeli

2.2.2.1 Uygulama katmanı (Application layer)

Kullanıcının çalıştırdığı uygulama programları, doğrudan bu katmanda tanımlıdır. Dosya aktarımı (FTP), e-posta (SMTP), ağ yönetimi (SNMP), metin iletişim protokolü (HTTP) gibi protokoller kullanıcı programlarına hizmet verirler (Çölkesen ve Örencik, 2000).

2.2.2.2 Sunum katmanı (Presentation layer)

Bilginin iletimde kullanılacak biçiminin düzenlenmesini sağlar. Sıkıştırma - açma, şifreleme - şifre çözme, EBCDIC - ASCII dönüşümü ve ters dönüşümü gibi işlevlerin yerine getirildiği katmandır (Çölkesen ve Örencik, 2000).

2.2.2.3 Oturum katmanı (Session layer)

Uç düğümler arasında gerekli oturumun kurulması, yönetilmesi ve sonlandırılması işlerini kapsar. İletişimin mantıksal sürekliliğinin sağlanması için, iletişimin kopması durumunda bir senkronizasyon noktasından başlayarak iletimin kaldığı yerden devam etmesini sağlar.

2.2.2.4 Ulaşım katmanı (Transport layer)

Bilginin son alıcıda her türlü hatadan arındırılmış olarak elde edilmesini sağlar. Paketlerin içeriğini de kontrol eder. Herhangi bir arıza durumunda verileri değişik yollardan göndermeye çalışır. Ulaşım katmanın oluşturduğu bilgi bloklarına bölüm (segment) denir (Çölkesen ve Örencik, 2000).

2.2.2.5 Ağ katmanı (Network layer)

Veri paketlerinin bir uçtan diğer uç ağdaki çeşitli düğümler (yönlendirici, geçityolu) üzerinden geçirilip yönlendirilerek alıcısına ulaşmasını sağlayan işlevlere sahiptir. Buradaki bilgi bloklarına paket adı verilir. İnternet'in protokol kümesi olan TCP/IP'de IP protokolü bu katmana ait bir protokoldür (Çölkesen ve Örencik, 2000).

2.2.2.6 Veri bağı katmanı (Data link layer)

Gönderilecek bilginin hatalara bağışık bir yapıda lojik işaretlere dönüştürülmesi, alıcıda hataların sezilmesi, düzeltilemiyorsa doğrusunun elde edilmesi için göndericinin uyarılması gibi işlevleri vardır. Gönderilen - alınan lojik işaret bloklarına çerçeve (frame) denir (Çölkesen ve Örencik, 2000).

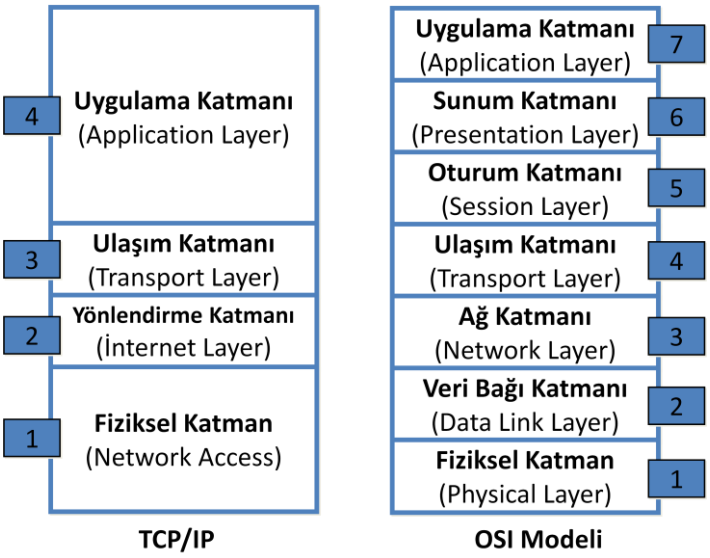
2.2.2.7 Fiziksel katman (Physical layer)

Verinin fiziksel olarak hat üzerinden aktarılması için gerekli işlevleri kapsar. Bu katman için tanımlanan standartlar taşıyıcı işaretin şekli, verici ve alıcı konumundaki uç noktaların elektriksel ve mekanik özelliklerini belirler. Kablo çeşitleri, konnektör standartları (UTP,RJ45,BNC…) bu katmanda belirlenir (Çölkesen ve Örencik, 2000).

2.2.3 TCP/IP (Transmission Control Protocol / Internet Protocol) protokolü

TCP/IP protokol grubu, 1970'lerin ortasında, Stanford Üniversitesi ve Bolt Beranek ve Newman (BB&N) tarafından geliştirilmiştir. Paket anahtarlamalı ağlarla devlet kuruluşları, üniversiteler ve araştırma kurumlarını birbirine bağlama projesinin bir ürünüdür. TCP/IP bir çok küçük protokolden oluşur. Adını en çok bilinen ikisinden (TCP ve IP) alır (Odom 2003). Özellikle İnternet ortamında TCP/IP protokol kümesinin kullanılması nedeniyle kullanımı yaygınlaşmıştır. TCP katmanı verilerin alıcıya ulaştırılmasından sorumludur. Hatalı yollanan verilerin tekrar yollanmasının kayıtlarını tutarak gerekli kontrolleri yapar. Eğer gönderilecek veri bir kerede gönderilemeyecek kadar büyük ise TCP onu uygun boydaki bölümlere (segment) böler ve bu bölümlerin karşı tarafa doğru sırada, hatasız olarak ulaşmalarını sağlar.

TCP/IP protokol kümesi dört katmanda incelenir. Bu katmanlar sırasıyla uygulama, taşıma, yönlendirme ve fiziksel katmanlarıdır. Taşıma katmanında TCP ve UDP protokolleri, yönlendirme katmanında IP, İnternet Kontrol Mesajı Protokolü (ICMP-Internet Control Message Protocol), Adres Çözümleme Protokolü (ARP-Address Resolution Protocol) tanımlıdır. Fiziksel katman için var olan tanımlar (Ethernet) geçerlidir. TCP/IP ve OSI katmanlarının karşılaştırması Şekil 2.7'de gösterilmiştir.



Şekil 2.7 : TCP/IP ve OSI modeli karşılaştırması

2.2.3.1 Uygulama katmanı (Application layer)

Uygulama katmanı TCP/IP'nin kullanıcıya en yakın katmanıdır. Uygulama programları çalıştıkları süre içinde TCP/IP protokol kümesinin uygulama katmanındaki protokoller ile etkileşim içerisindedirler. Bu protokoller sayesinde iletişim içerisinde bulunabilirler. TCP/IP protokol kümesindeki Uygulama Katmanı ile Ulaşım Katmanı arasında port olarak adlandırılan bir geçit tanımlıdır. Bu iki katman arasındaki iletişim portlar aracılığı ile gerçekleşmektedir. Her port 16 bitlik bir numaraya sahiptir. Bu numaraya port numarası adı verilmektedir. TCP/IP protokoller kümesinde toplam 65536 (2^{16}) adet port tanımlıdır. Port numaraları üç farklı kategoriye bölünmüştür.

0 dan 1023 e kadar olan portlar iyi bilinen portlardır (Well Known Port). Uygulama katmanı standart protokollerine bu gruptan HTTP için 80, FTP için 21, TELNET için 23, SMTP için 25, DNS için 53 gibi port numaraları tanımlanmıştır.

1024 den 49151'e kadar olan portlar kayıtlı portlardır. Bu portlar özel uygulamalar için geliştirilmiştir. 49152 ile 65535 arasındaki portlar ise dinamik ya da özel portlardır. Uygulama katmanı protokollerinin en çok kullanılanlarından bazıları aşağıda belirtilmiştir.

- FTP (File Transfer Protocol): Dosya transfer protokolüdür.

- SMTP (Simple Mail Transfer Protocol): E-posta yollamak için kullanılan protokoldür.
- HTTP (Hypertext Transfer Protocol):Web sayfalarının iletimi için oluşturulmuş protokoldür. Sunucu ve istemcilerin iletişimini sağlayarak kullanıcıların internet üzerinde dolaşabilmesine imkân tanır.
- TELNET (TCP/IP Terminal Emulation Protocol): Uzak sistemlere bağlanmak ve bu sistemler üzerinde komutlar çalıştırmak için kullanılan protokoldür.
- DNS (Domain Name System, yani Alan Adı Sistemi) alan adı verilen isimler ile IP adreslerini birbirine bağlayan sistemdir. Paylaştırılmış bir veritabanı olarak çalışır.

2.2.3.2 Ulaşım katmanı (Transport layer)

TCP/IP 'nin ulaşım katmanında TCP ve UDP olmak üzere iki protokol tanımlıdır. TCP (Transmission Control Protocol) veri gönderimini garanti eden bir protokoldür. İki bilgisayar iletişim kurmadan önce iletişim kurma istek ve onaylarını birbirlerine yollarlar. Böylece bilgi alışverişi için hazır hale gelmiş olurlar. Şekil 2.8' de görüldüğü gibi TCP, paketlerin başlık bilgisi içerisine sıra numarası ekleyerek paketleri sıralı göndermeyi garanti eder. Alındı bilgisi (acknowledgement) ile denetim yaparak bir paketin alıcıya ulaştığından emin olur. TCP kontrol bilgisi (checksum) ile paketlerin içeriğinin doğru bir şekilde gönderilmesini garanti eder.

<table>
<tr><td colspan="3">Kaynak Portu
(16bit)</td><td>Hedef Portu
(16bit)</td></tr>
<tr><td colspan="4">Sıra Numarası
(Sequence Number)
(32bit)</td></tr>
<tr><td colspan="4">Alındı Bilgisi Numarası
(Acknowledgement Number)
(32bit)</td></tr>
<tr><td>Veri Ofseti
(4bit)</td><td>Ayrılmış Bit
(6bit)</td><td>Bayraklar
(Flag)
(6bit)</td><td>Pencere (Window) Boyutu
(16bit)</td></tr>
<tr><td colspan="3">TCP kontrol bilgisi
Checksum
(16bit)</td><td>Acil işaretçiler
(Urgent Pointer)
(16bit)</td></tr>
<tr><td colspan="4">Opsiyonlar-Değişkenler
(32bit)</td></tr>
<tr><td colspan="4">Veri</td></tr>
</table>

Şekil 2.8 : TCP'de gönderilen bilgi paketi

UDP (User Datagram Protocol) verilerin hızlı bir şekilde iletiminin sağlayan bir protokoldür. İletişim başlamadan önce gönderici ve alıcı arasında bir anlaşma yapılmaz. Verilerin sıralı ve eksiksiz gönderilmesini değil, hızlı bir şekilde gönderilmesini sağlar. UDP bilgi paketi yapısı Şekil 2.9'da görülmektedir.

Kaynak Portu (16bit)	**Hedef Portu** (16bit)
Uzunluk *Lenght* (16bit)	**TCP control bilgisi** *Checksum* (16bit)
Veri	

Şekil 2.9 : UDP'de gönderilen bilgi paketi

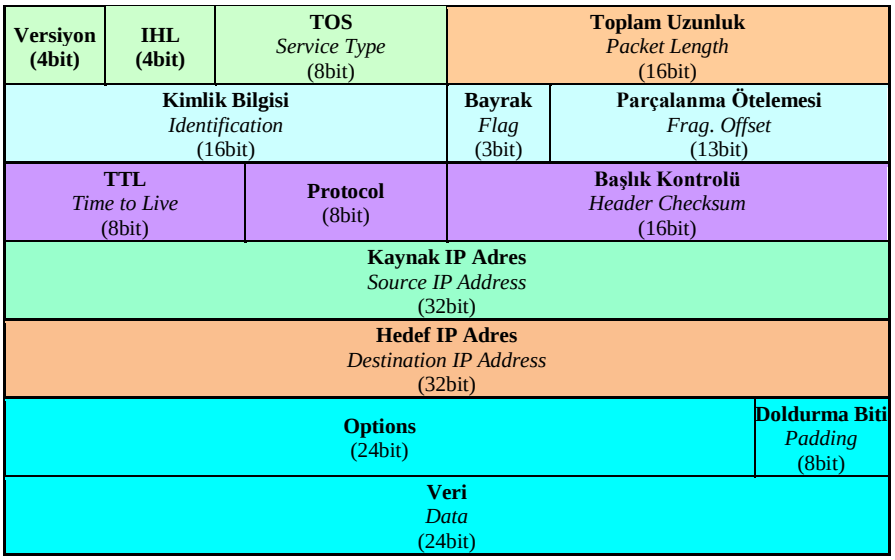
Her bir TCP veri paketi, 192bit başlık (header) bilgisi taşımakta ve iletimi hatalı olmuş olan paketleri tekrar göndererek doğruluğunu sağlamaktadır. UDP paketleri ise 64 bitlik başlık bilgisine sahiptir ve iletilen paketlerin doğruluğunu kontrol etmezler. Bu nedenle UDP daha hızlı bir protokol olup ses, video gibi gerçek zamanlı veri akışı gerektiren uygulamalarda ve bazı kontrol protokollerinde kullanılmaktadır.

Ulaşım katmanında UDP'nin oluşturduğu veri bütününe "datagram", TCP'nin oluşturduğu veri bütününe "segment" adı verilir. İkisi arasındaki temel fark, segmenti oluşturan veri grubunun başında sıra numarası bulunmasıdır. (Çay 2010)

2.2.3.3 Yönlendirme katmanı (Internet layer)

IP ve ICMP yönlendirme katmanının en bilindik protokolleridir. Yönlendirme katmanında global bir adresleme yapısı ile iletim için uygun büyüklüklere ayrılmış datagram paketlerini bir iletim yolu belirleyerek, alıcıya en kısa yoldan gönderme işlevi yerine getirilir.

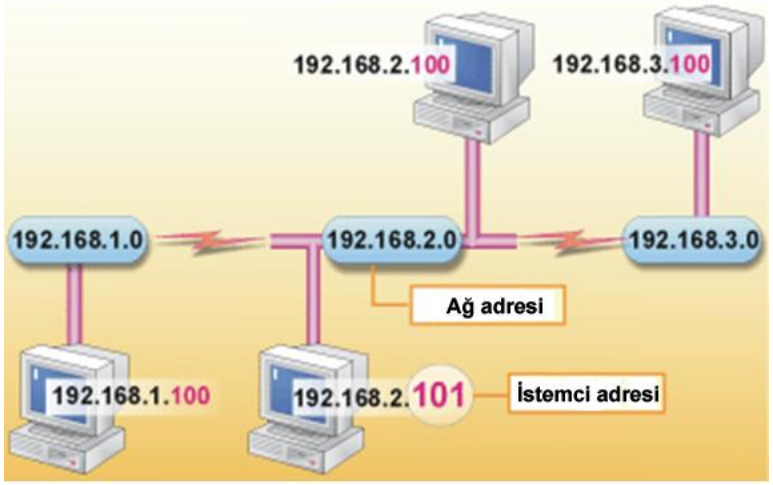
Ulaşım katmanı, hedef IP adresi bilgisi bulunan segmenti, yönlendirme katmanına verir. Yönlendirme katmanı bu segmenti alır herhangi bir diğer datagram veya segmentten önce veya sonra alıcıya iletim için bir yol belirler. Her bir datagram veya segment, yönlendirme katmanı tarafından kendi başlığı eklenerek Şekil 2.10'da görülen IP paketi haline getirilir ve her bir IP paketi birbirinden bağımsız olarak alıcıya gönderilir.



Şekil 2.10 : IP paket yapısı

Paketler üzerinde çok sınırlı hata kontrolü vardır. Yönlendirme katmanındaki 16bitlik başlık kontrolü (checksum) IP paketini alan alıcının IP başlığında bir bozulma olup olmadığını kontrol etmesini sağlar. Verinin internet katmanına bozuk ulaştığını değerlendirip yeniden gönderimini sağlayabilecek fonksiyona sahip değildir. Bu görev bir üst katmandaki TCP'de yapılır (Çay 2010).

TCP/IP protokolü kullanılan ağlarda, iletişim kuracak her cihaza Şekil 2.11'de görüldüğü gibi bir IP adresi atanır. Şu anda yaygın olarak IP sürüm 4 (IPv4) kullanılmaktadır. IPv4, 32 bit boyunda olup, noktalarla ayrılmış dört adet 8 bitlik sayıyla gösterilir. Paketler bir noktadan diğer noktaya iletilirken kaynak ve hedef mantıksal adresleri kullanılır.



Şekil 2.11 : Ağ IP adresleme

IP adresleri, bilgisayar ağlarını bölümlemek ve farklı büyüklüklerde bilgisayar ağları oluşturmak üzere sınıflandırılmıştır. Beş farklı adres formatı mevcuttur, bunlar; A, B, C, D ve E sınıfı adreslerdir.

A sınıfı adreslerde Şekil 2.12'de görüldüğü gibi ilk 8 bit, ağı tanımlamak için kullanılır. İlk bit 0'dır. Ondan sonraki 7 bit ağ adresini oluşturur. Geri kalan 24 bit, ağdaki host (makine) sayısını belirler. 16.777.214 adet bilgisayar içeren 126 adet altağ (subnet) kullanılabilir. 0.0.0.0 adresi varsayılan yönlendirme, 127.0.0.0 adresi ise yerel çevrim çin kullanılır. Geçerli ağ adresleri 1.0.0.0 ile 126.0.0.0 arasındadır (Odom 2003).

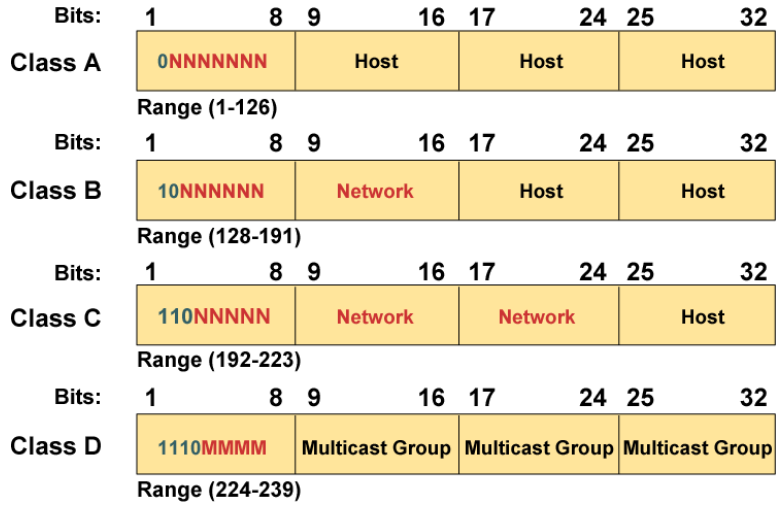
B sınıfı adreslerde Şekil 2.12'de görüldüğü gibi ilk 16 biti, ağı tanımlamak için kullanılır. İlk iki bit "10" şeklindedir. Sonraki 14 bit ağ adresini oluşturur, sonraki 16 bit ağdaki host sayısını belirler. Her biri 65.534 olmak üzere 16.384 adet altağa izin verir. 128.0.0.0 ile 191.254.0.0 adres aralığını kullanılır (Odom 2003).

C sınıfı adreslerde Şekil 2.12'de görüldüğü gibi ilk 24 biti, ağı tanımlar. İlk üç bit "110" şeklindedir. Sonraki 21 bit ağ adresini oluşturur. Kalan 8 bit ağdaki host sayısını belirler. 254 adet bilgisayar içeren 2.097.152 altağa izin verilir. 192.0.1.0 ile 223.255.254.0 aralığı kullanılır (Odom 2003).

D sınıfı adresler multicast adresleme için kullanılır. İlk dört biti "1110" şeklindedir. 224.0.0.0 ile 239.255.255.255 aralığındaki adresler bu sınıfa ait IP adresleridir (Odom 2003).

E sınıfı adresleme yedek olarak saklı tutulmaktadır. İlk dört biti "1111" şeklindedir. 240.0.0.0 ile 255.255.255.255 aralığındaki adresler bu sınıfa ait IP adresleridir (Odom 2003).

Yerel ağlarda kullanılmak üzere A sınıfından 10.0.0.0, B sınıfından 172.0.0.0 ve C sınıfından 192.168.0.0 ağ adresleri özel adres olarak ayrılmıştır (Odom 2003).



Şekil 2.12 : IP sınıfları

IPv4 standardına göre yapılan adreslemede, adreslerinin tamamı tükenmek üzere olduğundan IP adresleri IPv6 standartlarına göre verilmeye başlanacaktır. Bu adresleme tekniğinde IP adresleri 128 bitten oluşmaktadır (Odom 2003).

IP adresleri sistemlere dağıtılırken ağ daha küçük birimlere parçalanarak alt ağlar oluşturulur. Hostlara bağlı oldukları ağlarını tanımlayabilmek için alt ağ maskeleri kullanılır. Hostlar, bağlı oldukları ağları bulmak için alt ağ maskeleri ile IP adreslerini VE mantıksal işleminden geçirirler.

ICMP kontrol amaçlı bir protokoldür; genel olarak sistemler arası kontrol mesajları IP yerine ICMP üzerinden aktarılır. ICMP, IP ile aynı düzeyde olmasına karşın, aslında kendisi de IP'yi kullanır. ICMP mesajları IP üzerinden gönderilir. Bir çok ICMP mesaj tipi vardır. Bunlardan bazıları aşağıda belirtilmiştir.

- Alıcıya erişilemiyor (Destination Unreachable)
- Zaman Aşımı (Time Exceeded)
- Parametre Sorunu (Parameter Problem)
- Yansıma (Echo)
- Yansıma Karşılığı (Echo Reply)
- Zaman Damgası (Time Stamp)
- Zaman Damgası Karşılığı (Time Stamp Reply)

ICMP'nin en çok kullanılan uygulaması "ping" programıdır. Bir bilgisayardan karşıdaki bilgisayara ping mesajı gönderilerek o anda iletişimin var olup olmadığı öğrenilebilir. İletişim var ise Şekil 2.13'de görüldüğü gibi paket tur süreleri listelenir. Eğer ağ üzerinde adresi verilen alıcı yoksa veya o anda erişilemiyorsa alıcıya erişilemiyor mesajı alınır.

Şekil 2.13 : ICMP ping komutu kullanımı

2.2.3.4 Fiziksel katman (Network access)

Fiziksel katman, OSI'nin veri bağı ve fiziksel katmanlarını kapsamaktadır. Fiziksel katman için özel bir protokol tanımlanmamıştır. Ethernet, WiFi, modem üzerinden çevrimiçi bağlantı ve var olan fiziksel bağlantı türlerinin protokollerini kullanmaktadır.

2.2.4 Ağ Cihazları

Ağ cihazları, uç sistem konumunda olan bilgisayar veya benzeri sistemlerin birbirleriyle karşılıklı çalışmalarını, iletişim kurmalarını sağlayan uç ve ara cihazlardır. Bir ağ bulutu bu tür cihazların birbirine bağlanmasıyla oluşur.

2.2.4.1 Ağ kartı (NIC- Network Interface Card)

Bilgisayarları ve diğer cihazları ağa bağlamada kullanılan kartlara ağ kartı (NIC - Network Interface Card) denir. Ağ kartları iletilecek verileri elektrik, ışık veya radyo sinyalleri ile diğer bilgisayarlara iletebilir. Ağ kartları hız ve bağlantı yolları bakımından farklılık gösterir. PCI, USB, PCMCIA gibi bağlantı yuvalarını kullanarak bilgisayarlara takılan ağ kartları mevcuttur. Şekil 2.14'de kablolu ve kablosuz PCI ağ kartları görülmektedir.

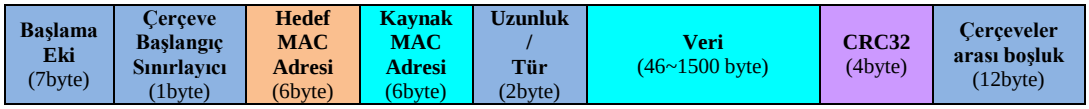
Her bir ağ kartının üzerindeki ROM içerisine üretim sırasında kaydedilen kendine özgü, MAC adresi (Media Access Control) denilen 48bitlik fiziksel bir adres tanımlanır. (00:05:A3:BF:D7:81). MAC adresinin İlk 24 biti IEEE (Institute of Electrica and Electronics Engineers) isimli kurum tarafından üretici firmaya verilen kısımdır. İkinci 24 bit ise, üretici firmanın her ürettiği karta verdiği adres kısmıdır.

Şekil 2.14 : Kablolu ve kablosuz PCI ağ kartı (NIC)

Bilgisayar ağlarında çoğunlukla ISO tarafından IEEE 802.3 standardı olarak belirlenen Ethernet standardı kullandığından bu ağlara bağlanmak için kullanılan ağ kartlarına Ethernet Kartı da denilmektedir.

1960'lı yıllarda Hawaii Üniversitesi tarafından geliştirilen ALOHA-NET' Ethernet ağlarının temeli olmuştur. 1980'li yıllarda XEROX firması CSMA/CD (Carrier Sense Multiple Access with Collision Detection) erişim kontrol protokolünü kullanan Ethernet standardını oluşturmuştur. CSMA/CD erişim kontrol protokolü ile her bilgisayar, ağı istediği zaman kullanabilmektedir. Bilgisayarlar ortak ilerim hattı olan ağa veri bırakmadan önce hattı kontrol eder, kullanılmadığından emin olduktan sonra hatta veri bırakır. Eğer aynı anda iki bilgisayar, ağın kullanılmadığını algılayıp ağ üzerinden veri gönderirlerse, bu veriler çarpışır (collision). Çarpışma CSMA/CD algoritmasını kullanarak tespit edildiğinde her iki bilgisayar da veri göndermeyi durdurup bir zaman sonra tekrar aynı veriyi ağa bırakırlar ve iletişim gerçekleşir. Ethernet standartları, çerçeve biçimi, çerçeve boyutu, zamanlama ve kodlama gibi ağ iletişiminin birçok yönünü de tanımlar (Spurgeon 2000). Ethernet ağında, belirtilen çerçeve düzenine göre iletilecek veriler biçimlendirilir. Çerçevelere, Protokol Veri Birimleri (PDU) de denir. Ethernet çerçevelerinde hedef ve kaynak MAC adresleri, sıralama ve zamanlama için başlama eki, çerçeve sınırlayıcının başlangıcı, çerçeve uzunluğu ve tipi, iletim hatalarını algılamak için de çerçeve kontrolü bilgileri bulunur. Ethernet çerçevelerinin boyutu, en az 64 bayt, en çok 1518 bayt olarak sınırlandırılmıştır. Bu sınırlamalara uymayan çerçeveler alıcı bilgisayar tarafından işlenmez. Ethernet ağlarının farklı kategori vardır:

- Ethernet: 10 Mbps hızında koaksiyel ve çift bükümlü kablolar üzerinde çalışır.
- Fast Ethernet: 100 Mbps hızında çift bükümlü kablolar üzerinde çalışır.
- Gigabit Ethernet: 1000 Mbps (1 Gbps) hızında fiber kablo ve çift bükümlü kablolar üzerinde çalışır.
- 10 Gigabit Ethernet: 10.000 Mbps (10 Gbps) hızında fiber kablo ve 33m de (STP – CAD7) kablo üzerinde çalışır.



Şekil 2.15 : 802.3 Ethernet çerçevesi yapısı

Ağ kartları kullanılacak kablolama çeşidine, konnektör tipi ile bağlanacakları ağ cihazlarının portlarının teknoloji ve hızlarına bağlı olarak seçilmelidir. Bazı kart ve ağ

cihazları üzerindeki portlar autosense özelliğine sahiptir. Bu özellik karşı tarafın hızına uyum sağlandığını belirtir. Ancak teknolojileri yine de aynı olmalıdır. Günümüzde en çok UTP kablo, RJ-45 konnektör ve kablosuz yapısına uygun ethernet kartları kullanılmaktadır.

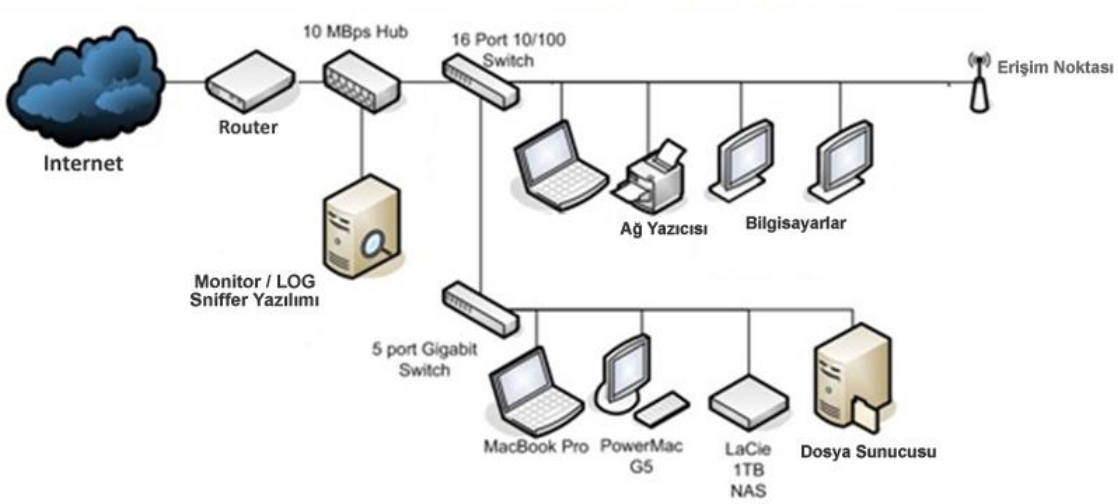
2.2.4.2 Dağıtıcı (Hub)

Ağ kartlarını dolayısıyla ağa bağlı cihazları birbirine bağlayan çok portlu en basit bağdaştırıcıdır. Dağıtıcı (Hub) bir potrundan kendisine gelen veriyi portlarına bağlı bütün bilgisayarlara, cihazlara yollar (Baykal N.). Bilgisayar gelen veriyi analiz ederek kendisine ait bir veri ise kabul eder. Hublar 4, 8, 12, 16, 24 portlu olarak üretilirler. Şekil 2.16'de 16 portlu Hub görülmektedir.

Dağıtıcı çalışırken herhangi bir portundan kablo çıkartılması veya takılması herhangi bir sorun çıkarmaz. Dağıtıcılar birbirlerine bağlanarak ağın daha da genişlemesi sağlanabilir.

Şekil 2.16 : 16 portlu dağıtıcı (Hub)

Dağıtıcı bir bilgisayar ağının internet bağlantısının trafik bilgililerinin tutulması için de kullanılabilir. Bu işlem için Şekil 2.17'de görüldüğü gibi dağıtıcının bir portuna gelen bilgiyi diğer portlarına çoklaması özelliğinden faydalanılır. İnternet bağlantısı ile LAN arasına konumlandırılacak bir dağıtıcı ve dağıtıcının boş portlarından birine bağlanacak içerisinde "sniffing" programı çalışan bir bilgisayar ile internet bağlantısı trafik bilgisi görüntülenip kaydedilebilir.



Şekil 2.17 : Trafik bilgisi için dağıtıcı kullanımı

2.2.4.3 Anahtar cihazı (Switch)

Anahtar (switch) akıllı bir dağıtıcı cihazıdır. Aynı anda birden fazla iletim yapma imkanı sağlar. Böylece aynı anda bir bilgisayar yazıcıyı kullanırken diğer ikisi kendi aralarında dosya transferi yapabilirler.

Şekil 2.18 : 8 portlu anahtar (Switch)

Anahtar, portlarına bağlanan bilgisayarları MAC adreslerine bakarak tanır. Anahtarlama işlemini gerçekleştirmek için MAC adreslerini yapısında bulunan tabloda tutar. Bu tabloda MAC adresinin hangi portuna bağlı olduğu bilgisi bulunur. Kendisine ulaşan veri paketlerinin MAC adreslerini inceler ve tüm portlara dağıtmak yerine, sadece hedef MAC adresine sahip olan bilgisayarın bağlı olduğu porta bırakır (Baykal N.). Böylelikle veri paketi sadece hedef bilgisayara ait portu ve kabloyu meşgul eder. Çakışmalar

engellenmiş olur ve ağ performansı artar. Anahtar OSI Referans modelinin ilk iki katmanında çalışır. Ağ güvenliğini sağlamak ve performansını arttırmak amacı ile kullanılmak üzere yönetilebilir anahtarlar da bulunmaktadır. Anahtarlar 8, 16, 24 portlu olarak üretilirler. Şekil 2.18' de 8 portlu bir anahtar görülmektedir.

2.2.4.4 Yönlendirici (Router)

Yönlendiriciler, OSI başvuru modelinin ilk üç katmanında çalışan aktif ağ cihazlarıdır. Temel olarak yönlendirme görevi yaparlar. LAN ve WAN arasında bağlantı kurmak amacıyla kullanılırlar (Baykal N.). Yönlendiricinin üzerinde LAN ve WAN bağlantıları için ayrı ayrı portlar bulunur. Bu portlar ile iki ağ arasında ki bağlantı sağlanır. Şekil 2.19'da CISCO marka bir yönlendirici görülmektedir.

Şekil 2.19 : Yönlendirici (Router)

2.2.4.5 Köprü (Bridge)

Aynı protokolü kullanan büyük ağların parçalanarak trafik yoğunluğu ayrıştırılmış küçük ağlara bölünmesinin sağlamak veya veri bağı katmanı tamamen farklı olan ağ teknolojileri ile kurulmuş ağ dilimlerini birbirine bağlamak için kullanılan ağ cihazlarıdır. Köprüler hangi veri paketlerini kabul edip diğer tarafa geçebileceğini, hangilerini kabul edemeyeceklerine karar vermek için IP adreslerini kullanırlar. Gerekli bilgiler içerilerindeki tablolarda tutulur.

2.2.4.6 Tekrarlayıcı (Repeater)

Kablonun kapasitesinden daha uzak mesafelere bağlantı kurulması gerektiğinde, bakırın direncinden dolayı oluşan veri zayıflaması ve parazitleri engellemek için kullanılan cihazlardır. Şekil 2.20'de görüldüğü üzere mesafesi uzatılacak ağın iki kablosunu uç uca ekler ve sinyalin parazitlerden temizlenerek tekrar güçlendirilmesini sağlar.

Şekil 2.20 : Tekrarlayıcı (Repeater)

2.2.4.7 Ortam dönüştürücü (Transciever)

Ortam dönüştürücüler farklı fiziksel yapıya sahip ağların birbirine bağlanması için kullanılır. Ortam dönüştürücülerin çok çeşitli türleri mevcuttur. Örneğin Şekil 2.21'de görülen Fiberden RJ45'e, AUI 'den RJ45'e, RJ45'ten BNC'ye gibi farklı biçimlerdeki ortamları birbirine dönüştürmek için kullanılırlar (Dean 2009, s.93).

Şekil 2.21 : Fiberden RJ45'e ortam dönüştürücü

2.2.4.8 Modem cihazı

Modemler, standart telefon hatlarını kullanarak, farklı yerlerdeki bilgisayarlar arasında bağlantı yapılmasını sağlayan aygıtlardır. Bu sayede, bir bilgisayardan diğerine veri aktarımı yapılabilir, ya da özel bazı protokoller ile internet servisleri kullanılabilir. Standart telefon hatları, normal şartlarda, sadece ses iletebilir. Modemler, bilgisayarlardaki dijital bilgiyi öncelikle ses sinyallerine (analog sinyal) dönüştürürler (MOdulation). Bu sinyalleri alan karşı taraftaki modem ise, analog sinyalleri ters dönüşümle bilgisayarların kullandığı dijital bilgiye dönüştürürler (DEModulation). Modem, ismi "Modülator" ve "Demodülator" kelimelerinin birleşiminden türetilmiştir (GÜ). Dahili ve harici olmak üzere çeşitleri bulunmaktadır.

Şekil 2.22'de bir örneği görülen dahili (internal) modemler bilgisayarın ana veri yoluna direkt monte edilebildiklerinden daha aktif görev yaparlar. Cihazın seri portlarını meşgul etmeyip yazılımsal COM port üzerinde de çalışabilirler. Sabit seri port kullanmadıkları için üzerlerindeki Jumperlar ile ayarlanmaları gerekmektedir (PnP ler hariç). Dahili modem gücünü cihazın güç kaynağından temin eder ve ses ayarları yazılım kontrollüdür. Bu modemler ile internet servis sağlayıcılarının (ISS) belirledikleri telefon numaraları çevrilerek internet bağlantısı sağlanır. Bu bağlantıya çevirmeli ağ (DialUP) denir. Geliştirilen protokoller ile önce karşıdaki modem ile eşleşir daha sonra oturumu açarlar. Dial Up modemlerin en büyük dezavantajı internete bağlı durumdayken telefon hattını meşgul etmeleridir (MEGEP).

Şekil 2.22 : Dahili (DialUp) modem

Harici Modemler Bilgisayara dışarıdan kabloyla bağlanan modemlerdir. Harici modemlerin üzerlerinde, telefon hattı girişi, besleme girişi ve modemin bilgisayarla

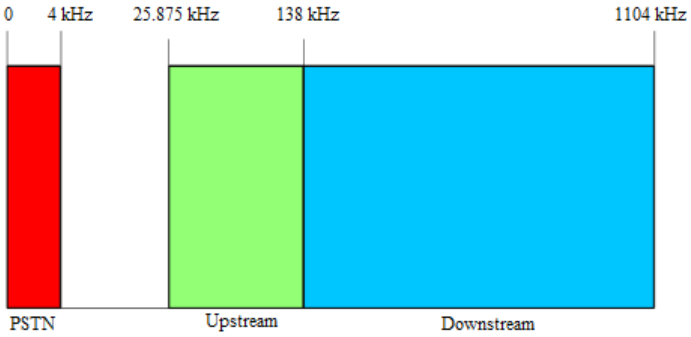
bağlantısını sağlayan Ethernet, USB veya COM giriş-çıkış birimleri bulunur. Harici modemlerin ön yüzlerinde, kullanıcılara modemin o anki durumuyla ilgili bilgi vermek amacıyla ışıklar yer almaktadır. Çeşitli bağlantı türleri için çeşitli modemler mevcuttur. Telefon hatları üzerinden DialUp bağlantı kurmayı sağlayan Harici DialUP modemler, Şekil 2.23'de görülen ADSL bağlantı kurmayı sağlayan ADSL modemler, Kablolu TV şebekesi üzeriden bağlantı kurmayı sağlayan kablo modemler mevcuttur.

ADSL modemler günümüzde internet bağlantısı için en çok kullanılan cihazlardır. ADSL Asymetric Digital Subscriber Line) Asimetrik Sayısal Abone Hattı kelimelerinin baş harflerinden oluşmuştur. Asimetrik kelimesi, veri transfer hızının, gönderim ve alım için eşit olmadığını belirtir. Kullanıcının veri alım hızı, gönderim hızından yüksek olabilir. ADSL modemler digital kodlama tekniği ile telefon hatlarını % 99 verimle kullanırlar. (MEGEP).

Şekil 2.23 : ADSL ve kablo modemler

ADSL teknolojisi 25KHz ile 1,1MHz frekans aralığını kullanır. Bu aralık konuşma amaçlı olarak kullanılan 0KHz ile 4 KHz frekans aralığından farklı bir frekans bandı olduğu için internete bağlantısı sağlandığında telefon hattı meşgul edilmemiş olur ve aynı anda hat üzerinden telefon görüşmesi de yapılabilir. Görüşme kalitesinin etkilenmemesi için ayırıcı (splitter) cihazı ile telefon ADSL sinyallerinden filtrelenmelidir. Şekil 2.24'de görüldüğü üzere ADSL teknolojisinde 25KHz ile 1,1MHz frekans aralığının 25KHz ile 200Khz aralığını upload (kullandığımız bilgisayardan

internete bilgi göndermek) ve 200 Khz ile 1,1 MHz aralığını da download (internetten kullandığımız bilgisayara bilgi indirmek) için tahsis edilmiştir (Sezlev 2008).



Şekil 2.24 : ADSL frekans aralığı bölümleri

2.2.5 Kablolama

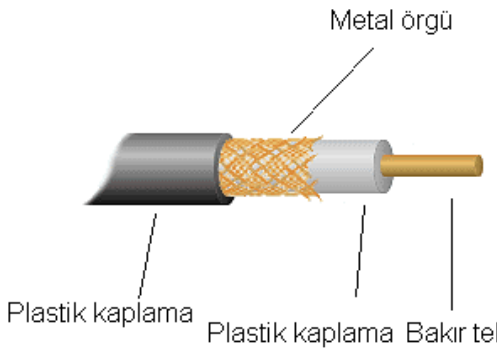
Bilgisayarlar arasındaki bilgi alışverişi Ağ kartları ve bunları birbirine bağlayan kablolar aracılığıyla gerçekleşir. Etkili bir iletişim için bu kabloların doğru şekilde seçilmiş ve kullanılmış olması gerekir (ITU). Ethernet kablo teknolojileri standartları aşağıda belirtilmiştir.

- 10Base2: İnce koaksiyel kablo ile 10Mbps hızında Ethernet ağı oluşturmak için kullanılır. İnce kablo kullanıldığı için ince Ethernet (ThinNet) olarak da adlandırılır. 2 rakamı maksimum 185m olan kablo uzunluğunu ifade etmektedir.
- 10Base5: Kalın koaksiyel kablo ile 10Mbps hızında Ethernet ağı oluşturmak için kullanılır. Kalın kablo kullanıldığı için Kalın Ethernet (ThickNet) olarak da adlandırılır. 5 rakamı maksimum 500m olan kablo uzunluğunu ifade etmektedir.
- 10Base36: Broadcast yayın yapan kablo ile 10Mbps hızında Ethernet ağı oluşturmak için kullanılır. Kablo uzunluğu maksimum 3600 metre olabilir.
- 10BaseT: Korumasız çift bükümlü (unshielded twisted pair) kablo üzerinde 10Mbps hızında Ethernet ağı oluşturmak için kullanılır. T ifadesi çift bükümlü kablo kulanıldığını (twisted pair) belirtmektedir. Ethernet olarak da anılır.

- 100BaseT: Korumasız çift bükümlü (unshielded twisted pair) kablo üzerinde 100Mbps hızında Ethernet ağı oluşturmak için kullanılır. Fast Ethernet olarak da anılır.
- 1000BaseT: Korumalı çift bükümlü (shielded twisted pair) kablo üzerinde 1000Mbps hızında Ethernet ağı oluşturmak için kullanılır. Gigabit Ethernet olarak da anılır.
- 10GBaseT: Korumalı çift bükümlü (shielded twisted pair) kablo üzerinde 10Gbps hızında Ethernet ağı oluşturmak için kullanılır. 10Gigabit Ethernet olarak da anılır.
- 10BaseF: Fiber optik kablo ile 10Mbps hızında Ethernet ağı oluşturmak için kullanılır..
- 100BaseFX, 100BASE-SX: Fiber optik kablo ile 100Mbps hızında Ethernet ağı oluşturmak için kullanılır.
- 1000BASE-LX, 1000BASE-SX, 1000BASE-LX: Fiber optik kablo ile 1000Mbps hızında Ethernet ağı oluşturmak için kullanılır.
- 10GBASE-SR, 10GBASE-LR, 10GBASE-LX4, 10GBASE-ZR: Fiber optik kablo ile 10Gbps hızında Ethernet ağı oluşturmak için kullanılır.

2.2.5.1 Koaksiyel (Coaxial) kablo

Koaksiyel (Coaxial) kablo Şekil 2.25'de görüldüğü üzere bir iletken metal telin üzerine plastik bir koruyucu, ardından bir metal örgü ve bir dış plastik kaplamadan oluşan kablo cinsidir. Metal örgü koruma katı iletilen verinin dış etkenlerden (electrical interference) korunmasını sağlar.

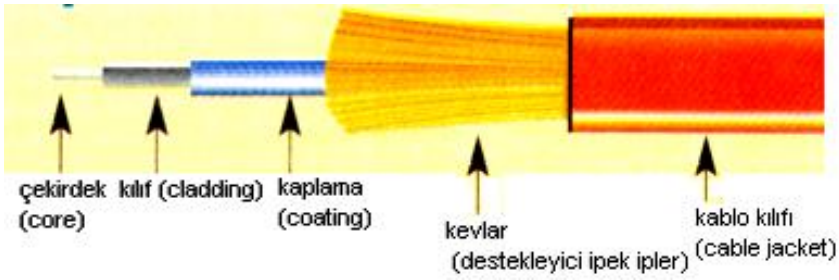


Şekil 2.25 : Koaksiyel (Coaxial) kablo yapısı

10Base2 olarak bilinen ThinNet RG-58 kablo tipi ile maksimum 185m mesafeye sinyal taşınabilir ve 30 bilgisayar birbirine bağlanabilir. 10Base5 olarak bilinen ThickNet RG-6 ve RG11 kablo tipi ile maksimum 500m mesafeye sinyal taşınabilir ve 100 bilgisayar birbirine bağlanabilir. Koaksiyel kablolar BNC konnektör ile sonlandırılır (Mueller 2003). Günümüzde bu tip kablo, ağ kurmak için kullanılmamaktadır.

2.2.5.2 Fiber optik kablo (FO)

Fiber optik kablo ile veriler, ışık formunda taşınır. Veri taşınmasında ışık kullanıldığı için kayıpsız ve elektriksel gürültüden (electrical interference) etkilenmeden yüksek kapasitede ve hızda veri akışı sağlanır. Şekil 2.26'de görüldüğü gibi ışık iletimi yapan çekirdek (core) 9, 50 veya 62,5 mikron kalınlıkta olmasına rağmen kırılgan yapısından dolayı üzerindeki koruma katları olan kılıf, kaplama, kevlar, kablo kılıfı ile kablo kalınlığı en az 0,5cm ye ulaşır (İÜBUYAMER).



Şekil 2.26 : Fiber optik (FO) kablo yapısı

Yapılarına göre en iyi performansı gösteren fiber optik kablo çekirdek ve kılıfı camdan imal edilmiş olanıdır. Daha ucuz, performansı daha verimsiz olan fiber optik kablo cam çekirdek, plastik kılıfa sahip olanıdır. En ucuz, performansı en zayıf olan fiber optik kablo ise çekirdek ve kılıfı plastikten üretilmiş olanıdır. Fiber tipine göre; Tek modlu (Single Mod), Çok modlu kademe indeksli (Multi Mode Step-Index), Çok modlu derece indeksli (Multi Mode Graded Index) çeşitleri mevcuttur. Ağ kurulurken kullanılacak olan fiber optik kablonun yapısı, tipi ve ağda kullanılan cihazlara (modül) bağlı olarak, veri iletimi 80km ye kadar mesafelere ve 30Gbps hızlarına kadar çıkılabilmektedir. Çekirdek kolaylıkla kırılabileceğinden, çizilebileceğinden ve optik iletimin

hassasiyetinin ışık iletim kalitesini etkilediğinden dolayı kurulum esnasında fiber optik kabloların sonlandırılmasına çok özen gösterilmelidir. Kurulum maliyetinin yüksek olması sebebi ile mesafe ve hız gereksinimi olmayan LAN'larda öncelikle bir bakır kablo olan çift bükümlü kablo (UTP ve STP) kullanılmaktadır.

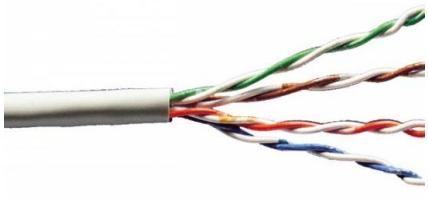
2.2.5.3 Çift bükümlü kablo (UTP ve STP)

Üzeri plastik kılıflı 8 bakır telin hem kendi aralarında hem de dış ortamdan oluşabilecek sinyal bozulmalarını engellemek amacıyla farklı turlarda çiftler halinde sarılarak elde edilen 4 sarmal çiftin birbirlerine sarılması ve kaplanması ile oluşturulmuş, ethernet teknolojisinde veri iletimi için kullanılan kablolara çift bükümlü (Twisted Pair) kablo denir. Çift bükümlü kablolar ile 100m mesafeye kadar veri iletimi yapılabilmektedir. Korunmasız çift bükümlü kablo (UTP-Unshielded Twisted Pair) ve korunmalı çift bükümlü kablo (STP-Shielded Twisted Pair) olmak üzere iki tür çift bükümlü kablo mevcuttur. Mevcut kullanılan çift bükümlü kablolar aşağıda belirtilmiştir.

- Category 5 kablo, 100 MHz band genişliği ile maksimum 100Mbps hızında verileri taşımak için kullanılmaktadır.
- Category 5e kablo, 100 MHz band genişliği ile maksimum 1Gbps hızında verileri taşımak için kullanılmaktadır.
- Category 6 kablo, 250 MHz band genişliği ile maksimum 1Gbps hızında verileri taşımak için kullanılmaktadır.
- Category 7 kablo, 600 MHz band genişliği ile maksimum 10Gbps hızında verileri taşımak için kullanılmaktadır (http://discountcablesusa.com).

2.2.5.3.1 Korumasız çift bükümlü kablo (UTP – Unshielded Twisted Pair)

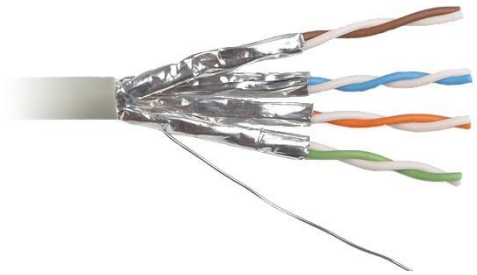
UTP, hem kendi aralarında hem de dış ortamdan oluşabilecek sinyal bozulmalarını engellemek amacıyla Şekil 2.27'de görüldüğü gibi birbirine sarılmış dört çift kaplamalı bakır telden ve en dışta da plastik bir kılıftan oluşur. UTP kablolar, kolay döşenebileleri ve maliyetlerinin düşük olması sebebiyle yerel ağ uygulamalarında en yaygın olarak kullanılan kablo türüdür.



Şekil 2.27 : Korumasız çift bükümlü kablo (UTP) yapısı

2.2.5.3.2 Korumalı çift bükümlü kablo (STP – Shielded Twisted Pair)

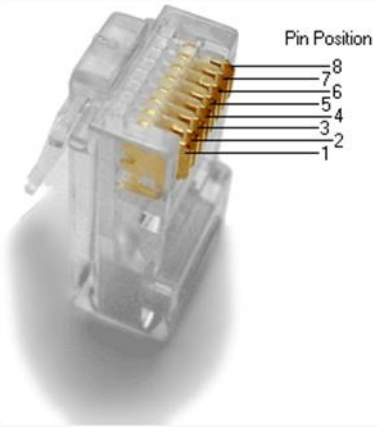
STP kablo Şekil 2.28'de görüldüğü gibi dış ortamdan kaynaklanan elektromanyetik gürültülerden (electrical interference) etkilenmemesi amacıyla UTP kablonun koaksiyel kablodakine benzer bir dış iletken koruyucu metal tabaka ile kaplanarak üretilmiş olanıdır. STP Kablo elektromanyetik gürültüyü koruma tabaksında toplayarak toprağa aktarılmasını sağlamaktadır. Korumanın gerçekleşebilmesi için STP ağ kablosu iki taraftan da, ağ cihazları üzerinden toprak hattıyla ilişkilendirilmelidir (Shinder 2000, s.205).



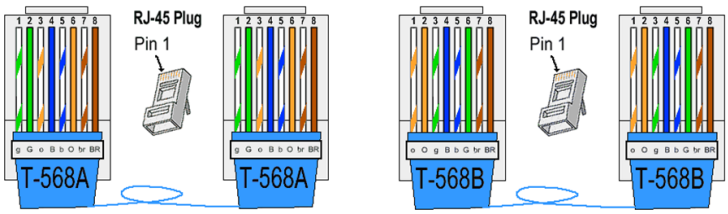
Şekil 2.28 : Korumalı çift bükümlü kablo (STP) yapısı

UTP ve STP kablolar Telekomünikasyon Endüstrisi Kurumu (TIA - Telecommunications Industry Association) ve Elektronik Endüstrisi Birliği (EIA - Electronic Industries Alliance) tarafından kabul edilen Tablo 2.1'deki TIA/EIA-568-A ve TIA/EIA-568-B standartlarına bağlı kalarak RJ-45 konnektör ile sonlandırılırlar.

Tablo 2.1: TIA/EIA-568-A ve TIA/EIA-568-B standartları

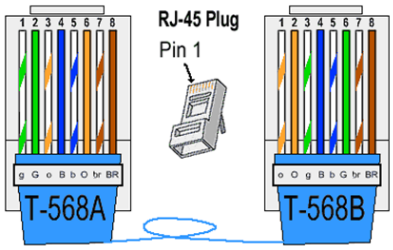
Pin	T568A	T568B	RJ-45 konnektör pin numaraları
1	Yeşil / Beyaz	Turuncu / Beyaz	
2	Yeşil	Turuncu	
3	Turuncu / Beyaz	Yeşil / Beyaz	
4	Mavi	Mavi	
5	Mavi / Beyaz	Mavi / Beyaz	
6	Turuncu	Yeşil	
7	Kahverengi / Beyaz	Kahverengi / Beyaz	
8	Kahverengi	Kahverengi	

UTP ve STP kablo ile bir bilgisayar ya da yönlendiriciden bir ağ cihazına bağlantı yapılacak kablonun her iki ucundaki konnektör de Şekil 2.29'da görüldüğü gibi aynı standart ile sonlandırılmış bir şekilde hazırlanmalıdır. (568A-568A yada 568B-568B). Bu şekilde hazırlanan kabloya düz kablo (Straight-Through Ethernet Cable) denir.



Şekil 2.29 : Düz kablo (Straight-Through ethernet cable)

Eğer kablo bir ağ cihazından diğer bir ağ cihazına ya da bir bilgisayardan diğer bir bilgisayara takılacaksa o zaman Şekil 2.30'da görüldüğü gibi kablonun uçlarındaki konnektörler birbirinden farklı standartta sonlandırılarak hazırlanmalıdır (568A-568B yada 568B-568A). Bu şekilde hazırlanan kabloya çapraz kablo (Crossover Ethernet Cable) denir.



Şekil 2.30 : Çapraz kablo (Crossover ethernet cable)

2.3 LOG TUTMA VE YÖNTEMLERİ

Herhangi bir olay ile ilgili geçmişe dönük tutulan kayıtlara log denilmektedir. İnternet erişim kayıtları ifadesi ile internet trafik logları aynı anlama gelmektedir. İnternet erişim kayıtlarının tutulabilmesi için birden çok yöntem mevcuttur.

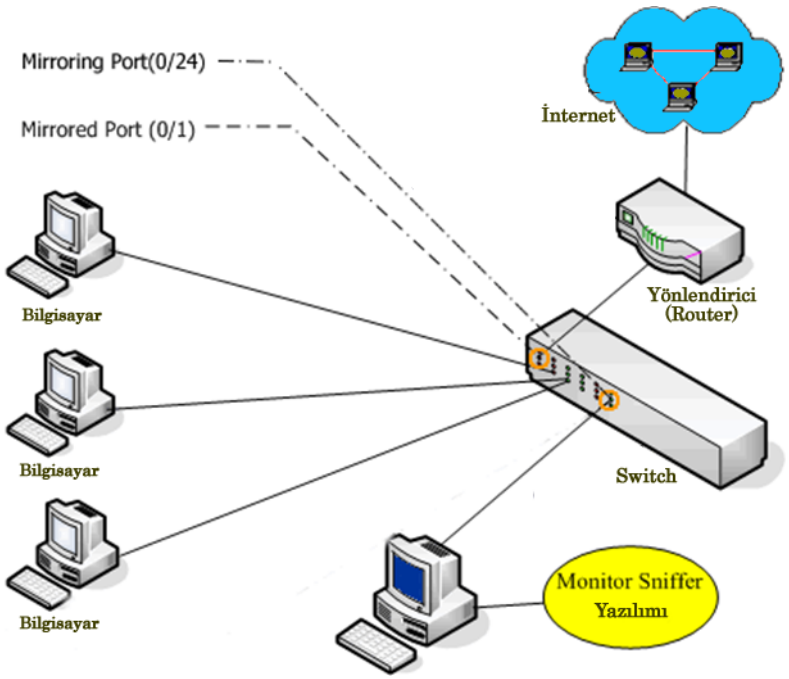
2.3.1 Sniffing

Ethernet protokolü kullanılan bir ağda ağ kartları ilk önce ağ üzerinden kendisine ulaşan veri paketinin başlığında bulunan hedef MAC adresi bölümünü kontrol eder. Hedef MAC adresi kendi adresi değil ise bu paketi reddeder. Sniffer, network kartını seçici olmayan moda (promiscuous mode) geçirerek alıcı adresi kendi MAC adresi olmasa da gelen paketleri alıp incelemesini sağlayan programdır (Connolly 2003). Network Traffic Analyser, Ethereal, Snort, Wireshark, Nast, Advanced Packet Sniffer, Network-I çeşitli sniffing programlarıdır.

Aynı ağ içerisinde iki bilgisayar arasında yapılan veri alış-verişini yakalamaya "sniffing" denilir. Bilindiği gibi dağıtıcı çalışırken herhangi bir portundan gelen bilgi paketini tüm portlarına yayınlamaktadır. Dağıtıcının portlarından birine Sniffing programı çalışan bir bilgisayar bağlanarak ağ trafiği kolaylıkla görüntülenip kaydedilebilecektir.

Bir yerel ağın internet çıkışından giden ve gelen paketleri analiz etmek söz konusu olduğunda ise yerel ağı oluşturan anahtar ile ağ geçidi görevi gören yönlendirici arasına bir dağıtıcı yerleştirilerek portlarından birine de Sniffing yapacak olan bilgisayar bağlandığında ağ trafiğinin analizi ve kaydı kolaylıkla yapılabilir. Şekil 2.31'de

görüldüğü gibi bu işlem için özel olarak üretilmiş veya ayarlanabilir "port mirorring" özelliği ile anahtarlanan tüm veri paketlerini bir portuna da gönderen anahtarlar mevcuttur.



Şekil 2.31 : Sniffing ile ağ trafiği log tutumu

2.3.2 Vekil Sunucu (Proxy Server) – Transparan Proxy

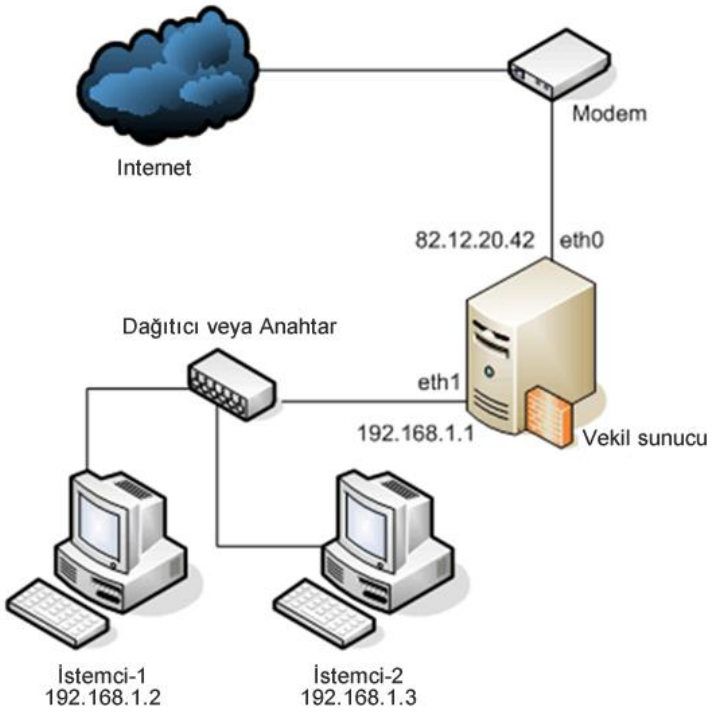
Çoğunlukla okul, şirket gibi toplu internet kullanımı olan kurum ve kuruluşlarda ağ kullanıcılarının internete erişimi sırasında kullanılan bir ara sunucudur. Vekil sunucu, ağ istemcilerin (client) internete çıkışları sırasında ağ geçidi (gateway) görevi görür. Ağ üzerindeki istemciler web isteklerini vekil sunucuya yaparlar, vekil sunucuda bu istekleri istemciler adına internet bağlantısı üzerinden hedef sunuculara iletir (Akkuş 2003). İsteklere karşılık sunucular tarafından gönderilen paketler vekil sunucu tarafından istek sahibi ağ istemcilerine gönderir. Vekil sunucu kullanmanın, birçok avantajı vardır (Şeker 2007).

Ekstra hız: Vekil sunucu, ağ istemcilerin ziyaret ettiği sayfaları bir süreliğine önbelleğine (cache) alır. Daha önce başka bir ağ istemcisi tarafından ziyaret edilen bir sayfa başka bir ağ istemcisi tarafından ziyaret edilmek istendiğinde vekil sunucu bu sayfanın içeriğini internet bağlantısı üzerinden yeniden almak yerine önbelleğinden istemciye gönderir. Bu özelliği sayesinde vekil sunucu internet bant genişliği aynı veri paketleri ile işgal edilmemiş olur. Ayrıca ağ istemcilerin web sayfası isteklerinin önbellekten alınması internet kullanımında hızlanmayı da beraberinde getirir (Şeker 2007).

Ekstra kontrol: Vekil sunucu, istenen sayfalara erişim verip istenmeyenlere erişim vermeyebilir. İçerik bazlı filtreleme (content based filtering) ile bütün paketler vekil sunucudan geçtiği için vekil sunucu geçen paketlerin içeriklerine bakarak istenilmeyen bilgi veya adres taşımaları durumunda paketlerin engellenmesi sağlanmaktadır. Bu yaklaşımda vekil sunucularda kara liste (black list) üzerinde yazılı olan kelimeleri içeren adreslere girilmesi engellenmiş olur. Örneğin site içerisinde "oyun" kelimesi geçiyorsa ve engellenmesi isteniyorsa, sunucunun kara listesine oyun kelimesi eklenir (Yılmaz 2005).

Ekstra güvenlik: Ağda bulunan istemcilerin internete direkt erişimi olmadığı ve tüm internet istekleri vekil sunucu tarafından yapıldığı için hangi istemcinin hangi web sayfası isteğinde bulunduğu ve hangi içeriği aldığı adres (IP, domain), saat, tarih bilgileri olarak kayıt altına alınır ve belirli bir süre vekil sunucu tarafından saklanabilir. Ayrıca vekil sunucu ağdaki tüm istekleri üstlendiğinden internet tarafından bakıldığında ağda tek bir istemci olarak görülür, bu da ağdaki bilgisayarların dışarıdan izole dilerek gelebilecek saldırılara karşı korunmasını sağlar. Bunun dışında vekil sunucu, virüslü dosyaları otomatik olarak temizleyebilir. (Yılmaz 2005)

CCProxy, lighttpd, WinGate Proxy, Nginx, Polipo,Privoxy, Squid, Tinyproxy, Varnish, Ziproxy çeşitli vekil sunucu programlarıdır.



Şekil 2.32 : Vekil (Proxy) server kullanımı

Vekil sunucular kurulum tiplerine göre saydam (transparent) veya saydam olmayan (non-transparent) şeklinde sınıflandırılabilirler. Saydam sunucular istemcinin hiçbir ayarlama yapmasına gerek duymadan internet paket trafiğini kendi üzerilerine alırlar ve paket kontrolünü kendi üzerilerinden gerçekleştirirler. Saydam olmayan vekil sunucular ise tam tersi şekilde istemcilerde bir sunucu ayarlaması yapılmasını ve hatta kullanıcı adı ve şifre girilmesini gerektirirler.

3. UYGULAMA

Bu bölümde bir orta öğretim kurumunun internet bağlantısı ve erişim kayıtlarının tutulabilmesi için gerekli ağ yapısı planlaması yapılacaktır. Daha sonra internet erişim kayırlarının tutulabilmesi için untangle ve IPCop programları kurularak programlardan elde edilen veriler incelenecektir.

3.1 UYGULAMA ORTAMI

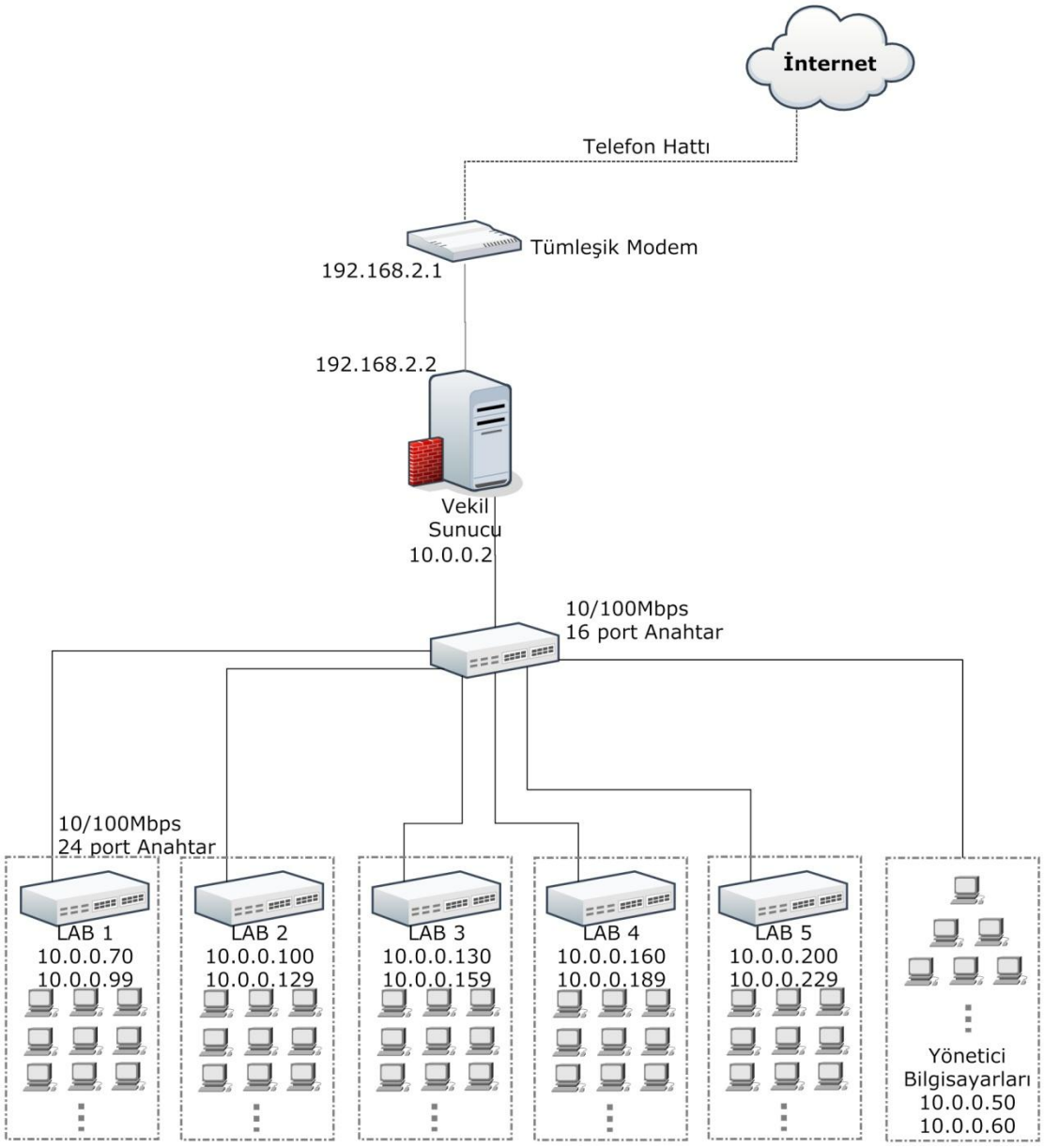
Uygulamanın yapılacağı eğitim kurumunda 100Mbps hızında ağ cihazları ve UTP kablo kullanılarak yıldız topolojisi bir ağ oluşturulmuştur. Eğitim kurumunda Windows tabanlı işletim sistemine sahip 10 adet yönetici (idare) bilgisayarı ve 5 adet 20+1 bilgisayardan oluşan laboratuar mevcuttur. Eğitim kurumunun internet bağlantısı TTNET internet servis sağlayıcısına ADSL bağlantısı ile sağlanmaktadır.

3.1.1 Uygulama Ortamının Ağ Yapısının Planlanması

Eğitim kurumu 4 portlu bir ADSL modem ile internet hizmeti almakta ve modemin bir portuna bağlı olan 16 portlu anahtar cihazı ile internet bağlantısını kurum içerisindeki yönetici, laboratuar bilgisayarlarına paylaştırılmaktaydı. Kurum içerisinde A sınıfı 10.0.0.0 ağ adresi kullanılmış ve IP adresleri el ile verilmişti. ADSL modem'e 10.0.0.3 IP adresi ayarlanmıştı. Yönetici bilgisayarlarına 10.0.0.50'den 10.0.0.60'a kadar olan IP aralığı, Laboratuar 1 bilgisayarlarına 10.0.0.70'den 10.0.0.99'a kadar olan IP aralığı, Laboratuar 2 bilgisayarlarına 10.0.0.100'den 10.0.0.129'a kadar olan IP aralığı, Laboratuar 3 bilgisayarlarına 10.0.0.130'dan 10.0.0.159'a kadar olan IP aralığı, Laboratuar 4 bilgisayarlarına 10.0.0.170'den 10.0.0.199'a kadar olan IP aralığı ve Laboratuar 5 bilgisayarlarına 10.0.0.200'den 10.0.0.229'a kadar olan IP aralığı ayarlanmıştı.

Planlanan ağ yapısı Şekil 3.1'de görülmektedir. İnternet erişim kayıtlarının tutulabilmesi için çift ağ kartına sahip bir sunucu bilgisayar hazırlanmıştır. Sunucu bilgisayar ADSL modem ile 16 port anahtar cihazının arasına bağlanmıştır. Böylelikle tüm internet trafiğinin sunucu bilgisayar üzerinden geçmesi sağlanmıştır.

Mevcut IP yapısında çok fazla değişiklik yapmamak için sunucu bilgisayarın LAN a bakan ağ kartının IP adresi ADSL modemin eski adresi olan 10.0.0.3 adresi şeklinde ayarlanmıştır. Böylelikle tüm istemci bilgisayarlarının IP, Ağ geçidi ve DNS sunucu adresi ayarlamalarının yeniden yapılmasına gerek kalmamıştır. Sunucunun diğer ağ kartı ADSL modemin bir portuna bağlanarak oluşan ağa C sınıfı 192.168.2.0 ağ adresi gurubunda bir IP adresi atanmıştır. ADSL modem'e 192.168.2.1, Sunucu bilgisayara ise 192.168.1.2 IP adresleri atanmıştır.



Şekil 3.1 : Planlanan ağ yapısı

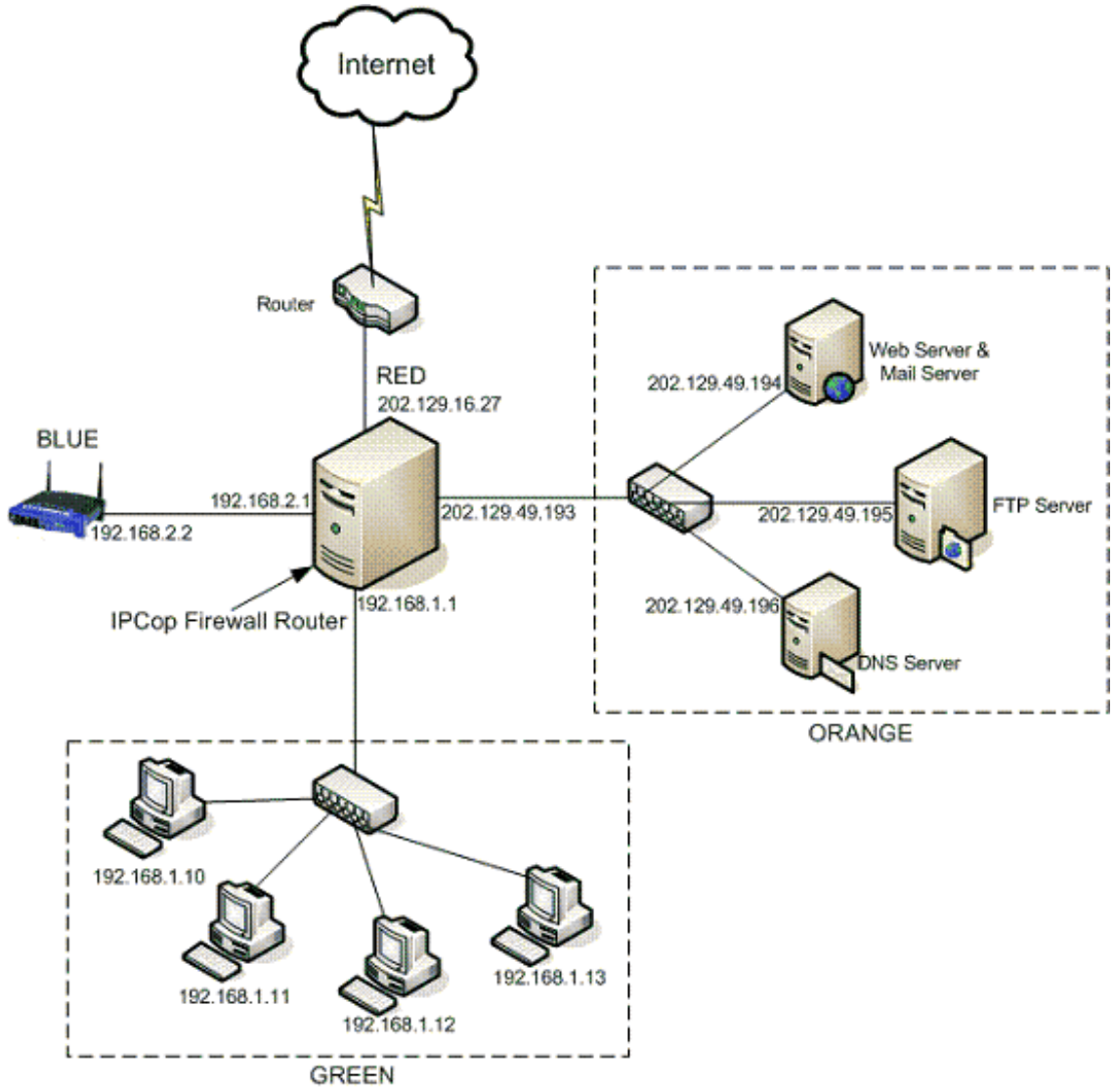
3.2 İNTERNET ERİŞİM KAYITLARININ TUTULMASI

Ağ yapısı planlanıp uygulandıktan sonra sunucuya ilk önce IPCop programı kurularak internet erişim kayıtları tutulmuş, daha sonra untangle programı kurularak aynı işlem tekrarlanmıştır.

Erişim kayıtlarının tutulabilmesi için kullanılacak olan sunucu; İntel Core2 Quad core 2,83GHz mikroişlemciye, 6GB ram'e ve 2TB sabit disk donanımına sahiptir. Ancak kullanılacak programlar sunucu içerisine sanallama ile oluşturulan sanal sunucular içerisine kurulacaktır.

3.2.1 IPCop Programı

IPCop açık kaynak Linux çekirdeği kullanan SOHO lar için ideal bir firewall (güvenlik duvarı) yazılımıdır (ipcop). Ipcop'un kurulumu sırasında Şekil 3.2 de görüldüğü üzere RED, GREEN, BLUE, ORANGE olmak üzere 4 bölge için 4 ağ kartı tanımlanabilir. RED olarak tanımlanan ağ kartına internet veya güvenilmeyen ağ bağlantısı, GREEN olarak tanımlanan ağ kartına korunacak yerel ağ, BLUE olarak tanımlanan ağ kartına isteğe bağlı olarak kablosuz ağlar, ORANGE olarak tanımlanan ağ kartına ise isteğe bağlı olarak silahsızlandırılmış bölgede (DMZ) yapılandırılan Web sunucusu, Dosya sunucusu, DNS sunucusu gibi internete servis sunan sunucular bağlanabilir. İhtiyaçlar doğrultusunda RED+GREEN, RED+GREEN+BLUE veya RED+GREEN+BLUE+ORANGE bölgeleri kullanılabilir.



Şekil 3.2 : IPCop bölgeleri

IPCop, üzerinde çalıştırılabilecek birçok uygulama ile aşağıdaki hizmetleri yerine getirebilmektedir.

- Firewall Görevi: Yerel ağ ile internet arasında bir firewall olarak kullanabilir ve yerel ağın internet ortamına güvenle çıkmasını sağlar. Aynı şekilde internet ortamından erişimi güvenli hale getirir.
- DHCP Sunucusu: Yerel ağda bulunan bilgisayarlar için DHCP sunucusu görevi yaparak IP, DNS ve ağ geçidi bilgilerini otomatik olarak atayabilir.

- Web Proxy: Vekil sunucu ile internet bant genişliğinin maksimum seviyede kullanılmasını sağlar. Ayrıca ek paketlerle URL (web sayfası) filtrelemesi de yapar.
- Virüsleri Engelleme: Gerek URL ile gelen gerekse de e-postalarla gelen virüsleri tarayarak yerel ağa internet ortamından virüslerin ulaşmasını engelleyebilir.
- Yönlendirici (Router): Sunucuların (web, e-posta v.b) güvenli bir şekilde internet ortamında hizmet vermesini sağlar.
- NAT (Network Address Translation): Birden fazla gerçek IP adresini kolayca yönetip, kullanılmasını sağlar.
- Güncelleme Proxy: Microsoft, Adobe, Symantec gibi firmaların yazılımlarının güncellemelerini önbelleğinde (cache) tutarak yerel ağdaki istemcilerin güncelleme verilerine internet yerine IPCop üzerinden daha hızlı bir şekilde ulaşıp güncelleme yapmalarına olanak sağlayabilir.
- PAT (Port Address Translation): Verilerin kaynak ve hedef portlarının adres çevirimlerini gerçekleştirir.
- Layer 7 (Uygulama) Seviyesinde Kısıtlama: İnternet politikası doğrultusunda network kullanıcılarının hangi işletim sistemini, web tarayıcısını ve hatta internet uygulamalarını kullanabileceklerine kadar gerekli kısıtlamaların yapılmasını sağlayabilir.
- Log: Tüm işlemler için ayrı ayrı log tutarak geriye dönük izlemeler, istatistiki veriler ve analizler yapılmasını sağlayabilir.
- Hız Limiti Belirleme: İstemci bazında Download ve Upload hız limitinin belirlenmesini sağlayabilir.

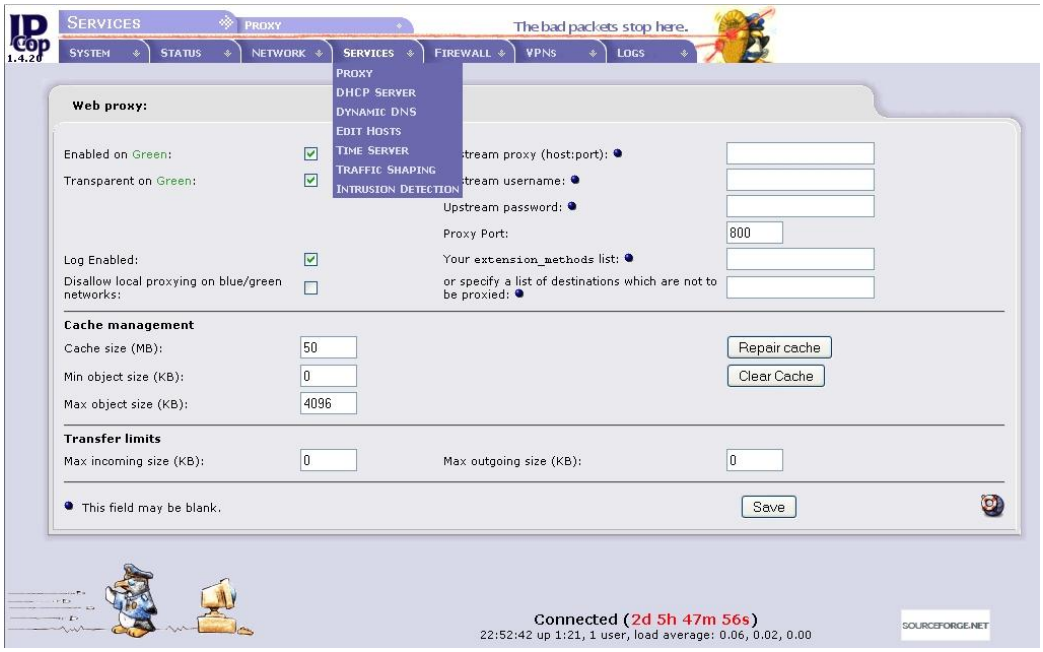
IPCop'un grafik arayüzü olmaması sebebi ile çok düşük konfigürasyonlu donanımlara dahi kurulabilmektedir. IPCop'un grafik ara yüzü yoktur ancak ayarların yapılabilmesi için web üzerinden hizmet veren bir web arayüz kontrol paneline sahiptir. Web arayüzüne ulaşmak için GREEN bölgedeki bir istemcinin web tarayıcısından https://IPCop GREEN ağ kartı IP adresi:445 adresine bağlanılması gerekir.

3.2.1.1 IPCop programı kurulumu

IPCop programının yükleme CD imajı olan ipcop-1.4.20-install-cd.i386.iso, http://garr.dl.sourceforge.net/project/ipcop/IPCop/IPCop%201.4.19%20_%201.4.20/ipcop-1.4.20-install-cd.i386.iso adresinden indirildi. Sunucunun içerisine 2GB sabit disk, 256MB ram, bir çekirdek mikroişlemci ve iki ağ kartı donanımına sahip bir sanal sunucu oluşturuldu. İndirilen ipcop-1.4.20-install-cd.i386.iso dosyası sanal bilgisayarın CD sürücüsüne yüklenip **EK A1 IPCop kurulumu** adımları gerçekleştirilerek IPCop programı kuruldu.

3.2.1.2 Uygulama

Kurulum gerçekleştirildikten sonra IPCop web arayüzüne bağlanılıp Şekil 3.3'de görülen SERVICES (Hizmetler) sekmesi altındaki PROXY (Web vekil sunucu) menüsünden "Enabled on Green", "Transparent on Green" ve "Log Enabled" seçenekleri işaretlenip kaydedilerek (Save) vekil sunucu şeffaf mod da aktif hale getirildi. Vekil sunucu üzerinden geçen yerel ağdaki istemcilerin trafik bilgisi bu şekilde kaydedilmeye başlandı.

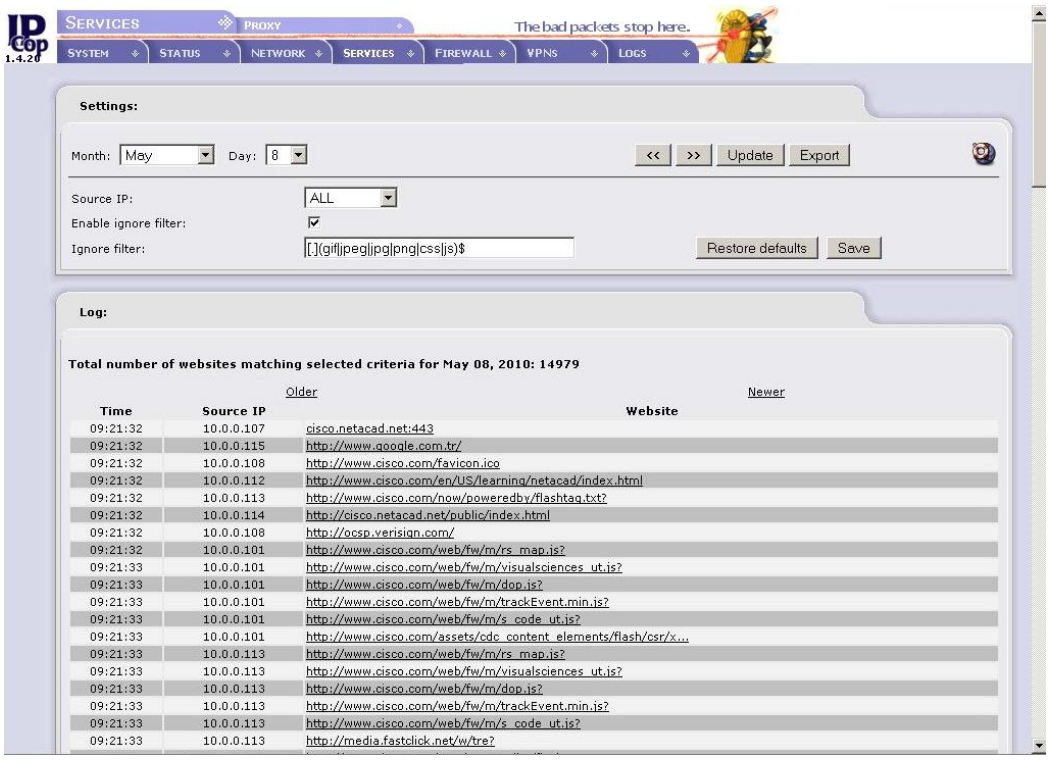


Şekil 3.3 : IPCop web arayüzü vekil sunucu menüsü

Bu işlemin ardından IPCop sadece yerel ağ istemcilerinin internet erişim kayıtlarını tutmakla kalmaz ayrıca, vekil sunucu önbellek (cache) hizmeti kullanımına başlar.

IPCop üzerinde kaydedilmeye başlanan internet erişim kayıtlarının ihtiyaç olan tarih ve saat deki kısmını "LOGS" sekmesi altındaki "PROXY LOG" menüsünden görüntüleyebiliriz.

Şekil 3.4' de görüldüğü gibi internet erişim kaydı tarih, saat, istemci IP adresi ve erişilen web sitesi adresi şeklinde görüntülenir. İhtiyaç olan tarih seçilip "Update" tıklandığında o tarihe ait tüm erişim listesi ekrana listelenir. Saat seçimi ise "Older" ve "Newer" seçenekleri ile yapılır.



Şekil 3.4 : IPCop web arayüzü erişim kayıt listesi menüsü

Şekil 3.4'de görülen menü içerisindeki "Ignore filter" seçeneği ile trafik içerisindeki veriler dosya uzantılarına bağlı olarak filtrelenir. Bu şekilde erişim kaydı listesi sadeleştirilerek istenilen trafik bilgisine daha kolay ulaşılabilir.

3.2.1.3 Sonuçlar

IPCop ile internet erişim kayıtlarının tutulması uygulaması üç ay boyunca sürdürülmüştür. Bu üç aylık süre boyunca geçmişe dönük internet erişim kayıtlarının tutulmasında ve raporlanmasında herhangi bir sıkıntı yaşanmamıştır.

Kullanıcılar, yapılan görüşmelerde internet hızının, sunucunun kullanılmadığı döneme göre arttığını bildirmişlerdir. Kullanıcıların internet hızında artış hissetmelerinin sebebi IPCop programının internet erişim kayıtlarını tutmak için kullandığı squid vekil sunucu eklentisinin önbellek desteği sunmasıdır.

Gün içerisinde en az 60 istemcinin aynı anda interneti kullandığı, yoğun internet trafiğinin oluştuğu saatlerde sunucunun performansını gösteren "top" komutu ile yapılan kontrollerde alınan sonuçlardan ortalama bir tanesi Şekil 3.5'de görülmektedir.

```
top - 11:34:36 up  3:35,  1 user,  load average: 0.27, 0.12, 0.02
Tasks:  45 total,   1 running,  44 sleeping,   0 stopped,   0 zombie
Cpu(s):   0.0% user,   7.3% system,   0.0% nice,  92.7% idle
Mem:    256804k total,   142992k used,   113812k free,    25988k buffers
Swap:    32764k total,        0k used,    32764k free,    74636k cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
 3338 squid     16   0 18624  18m 2068 S  3.7  7.2   1:24.80 squid
   57 root       9   0     0    0    0 S  0.3  0.0   0:06.12 kjournald
 3345 squid      9   0 18624  18m 2068 S  0.3  7.2   0:00.10 squid
 3367 root       9   0  1040 1040  848 R  0.3  0.4   0:01.49 top
    1 root       8   0   568  568  500 S  0.0  0.2   0:03.53 init
    2 root       9   0     0    0    0 S  0.0  0.0   0:00.03 keventd
    3 root      19  19     0    0    0 S  0.0  0.0   0:00.59 ksoftirqd_CPU0
    4 root       9   0     0    0    0 S  0.0  0.0   0:00.00 kswapd
    5 root       9   0     0    0    0 S  0.0  0.0   0:00.00 bdflush
    6 root       9   0     0    0    0 S  0.0  0.0   0:00.28 kupdated
   14 root       9   0     0    0    0 S  0.0  0.0   0:00.16 kjournald
   35 root       9   0     0    0    0 S  0.0  0.0   0:00.02 kapmd
   40 root       9   0     0    0    0 S  0.0  0.0   0:00.00 khubd
   56 root       9   0     0    0    0 S  0.0  0.0   0:00.00 kjournald
   99 syslogd    9   0   664  664  576 S  0.0  0.3   0:00.29 syslogd
  101 klogd      9   0  1208 1208  576 S  0.0  0.5   0:00.30 klogd
  373 root       8   0   708  708  620 S  0.0  0.3   0:00.05 fcron
  378 root       8   0  2248 2248 2052 S  0.0  0.9   0:00.07 httpd
```

Şekil 3.5 : IPCop ortalama "top" komutu sonucu

"top" komutu sunucunun anlık durumunu listeledikten sonra her 2-3 saniyede bir ekranı yenileyerek son durumu dinamik bir biçimde ekrana aktarır. "top" komutu ile çalışan süreçler (uygulamalar), süreçlerin ID numaraları, kullanıcıları ve kullandıkları bellek

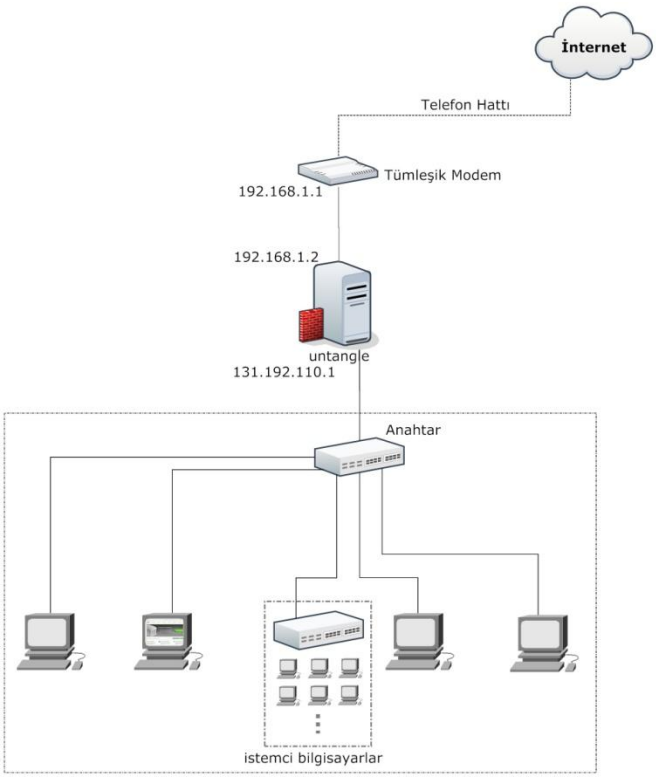
miktarı ile işlemci kullanımı oranı, bellek kulanım miktarı anlık olarak görüntülenmektedir. Ayrıca 1, 5 ve 15 dakika öncesi load average (ortalama işlemci yük durumu) bilgileri görüntülenmekte olup bu değerin %1 altında olması beklenir.

Şekil 3.5'de görüldüğü üzere sunucu son 1 dakika içinde ortalama %27, son 5 dakika içinde ortalama %17 ve son 15 dakika içinde ortalama %2 oranında kullanılmıştır. Sunucu anlık olarak tüm süreçler için işlemeci gücünün %7,3'ünü, Squid vekil sunucu uygulaması ise işlemci gücünün %4 ünü kullanmaktadır. 256804k olan toplam bellek miktarını %7,2 si Squid vekil sunucusu tarafından kullanmakta olup tüm sistem 142992k bellek kullanmaktadır. Sunucu üzerindeki belleğin 113812k'sı boş olup ek belleğe ihtiyaç duyulmadığından 32764k olan sanal bellek (swap) kullanımda değildir.

Bu sonuçlara bakıldığında load average ın %1,00 in altında ve fiziksel belleğin yeterli olması IPCop un sunucu üzerinde sorunsuz, sınırlar içerisinde hizmet verdiğini göstermektedir.

3.2.2 Untangle Programı

Üretici firmanın adı ile anılan untangle, ayrıca bir işletim sistemine gerek duymaksızın DEBAIN 5 Linux çekirdeğe sahip işletim sistemi üzerinde çalışan, çeşitli uygulamalardan oluşan çok fonksiyonlu bir güvenlik duvarı programıdır (untangle). Kurulacağı sunucuda başka bir işletim sistemine gerek yoktur. Untangle'nin kurulup çalıştırılacağı sunucu iki ağ kartına sahip olmalıdır. Şekil 3.6'de görüldüğü gibi ağ kartlarından biri yerel ağa diğeri ise ağ geçidine bağlanmalıdır.



Şekil 3.6 : Untangle sunucunun ağ üzerindeki yeri

Untangle işletim sistemi ve üzerinde çalışan temel uygulamaları kapsayan "Lite Package" paketi ücretsizdir. Daha kapsamlı güvenlik ve detaylı kısıtlamalara (filtreleme) ihtiyaç duyulduğunda ise bu uygulamaları kapsayan "Premium Package", "Standard Package", "Education Premium", "Education Standard" paketleri yıllık kullanım ücretleri ile kullanılabilmektedir. Untangle üzerinde çalışan çeşitli uygulamalar ve işlevleri aşağıda belirtilmiştir.

Lite paketin ücretsiz kullanılabilen uygulamaları;

- Web Filtre: 16 Kategoride internet sitesini tanır ve filtreler.
- Attack Blocker: DoS atakların önlenmesi için kullanılır.
- Captive Portal: Belirli koşullarda internet erişimine izin verir.
- Phish Blocker: Internet üzerinde kredi kartı ve kişisel bilgilerin çalınmaması için kullanılır.
- Spam Blocker: İstenmeyen e-postaları engellemek için kullanılır.
- Spyware Blocker: Casus yazılımlardan korunmak için kullanılır.

- Virus Blocker: Internet üzerinden virüs girişlerini engeller.
- Protocol Control: P2P, Mesajlaşma vb. tüm protokolleri kontrol etmek ve engellemek için kullanılır.
- Firewall: Güvenlik duvarı ile iç ve dış ağı ayırarak, kurallara göre geçiş kontrolü sağlar.
- Intrusion Prevention: Internet üzerinden ağa olan saldırıları tespit ederek engeller.
- OpenVPN: Ağa VPN üzerinden bağlanabilmeyi sağlar.
- Reports: Sistem ve ağdaki kullanıcılar ile ilgili ayrı ayrı ve çok detaylı raporlama yapar.

Ücretli paketler ile kullanılabilen bazı uygulamalar;

- eSoft Web Filter: 53 Kategoride 450 Milyon internet sitesini tanır ve filtreler.
- Directory Connector: RADIUS veya Microsoft Active Directory sunucusunu kullanarak kullanıcı bazlı kural yazılmasını ve raporlamasını sağlar.
- Policy Manager: Sınırsız kullanıcı için zaman bazlı erişim kontrolleri ve uzaktan bağlantı sınırlaması gibi kural setlerinin tanımlanmasını sağlar.
- Kaspersky Virus Blocker: Anti-virüs üreticilerinin lider markalarından biri olan Kaspersky ile daha fazla koruma sağlar.
- Commtouch Spam Booster: Genişletilmiş spam önleme özelliği ile spam mesajları %98 oranında azaltır.
- WAN Balancer: 6 farklı internet bağlantısına kadar, internet trafiğini farklı hatlara bölüp optimize etmeyi sağlar.
- WAN Failover: Bağlantı kopukluklarını algılayarak yedek hatta otomatik geçiş yapılmasını sağlar.
- Bandwidth Control: Ağ üzerindeki tüm trafiği, kullanıcı, kota, site bazlı olarak sınırlanmasını, izlenmesini ve kural yazılmasını sağlar.
- Live Support: Canlı teknik destek alınabilmesini sağlar.
- Configuration Backup: Untangle ayarlarının, untangle data merkezinde her gece yedeklenmesini sağlar. Bu sayede yeniden yüklenmesi gerekirse zahmetsizce geri yükleme yapılabilir.

Untangle, hizmet vereceği yerel ağdaki kullanıcıların sayısına bağlı olarak Tablo 3.1'deki donanım gereksinimini karşılayan bir sunucuya kurulmalıdır.

Tablo 3.1: Donanım gereksinimi tablosu

Kullanıcı sayısı	İşlemci	Hafıza	Sabit Disk	NIC
En az	Intel / AMD (800 + Mhz)	512 MB	20 GB	2
1-50 Kullanıcılar	Pentium 4 veya daha büyük	1 GB	80GB	2 veya daha fazla
51-150 Kullanıcılar	Dual Core	2 GB	80GB	2 veya daha fazla
151-500 Kullanıcılar	Dual Core veya daha fazla	2 GB veya daha fazla	80GB	2 veya daha fazla
501-1500 Kullanıcılar	Quad Cores	4 GB	80GB	2 veya daha fazla
1501-5000 Kullanıcılar	Quad Cores veya daha fazla	4 GB veya daha fazla	80GB	2 veya daha fazla

Untangle kurulu sunucuyu ayarlamak ve rapor almak için web arayüzü de kullanılabilmektedir. Web arayüze erişebilmek için web tarayıcısından https://sunucunun IP adresi adresine bağlanılması gerekir.

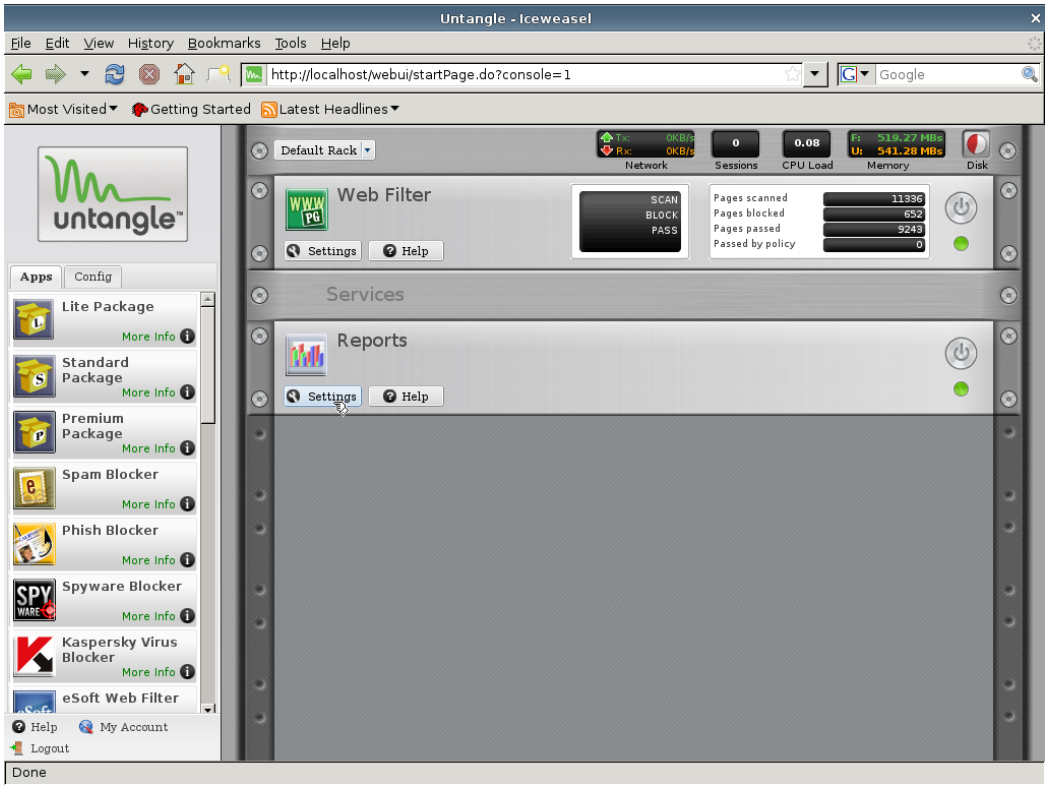
3.2.2.1 Untangle programı kurulumu

Untangle programının yükleme CD imajı olan untangle_800_x32.iso, http://download.untangle.com/get.php?file=untangle_800_x32.iso&var=10ds82 adresinden indirildi. Sunucunun içerisine 8GB sabit disk, 1GB ram, bir çekirdek mikroişlemci ve iki ağ kartı donanımına sahip bir sanal sunucu oluşturuldu. İndirilen untangle_800_x32.iso dosyası sanal bilgisayarın CD sürücüsüne yüklenip **EK B1 Untangle kurulumu** adımları gerçekleştirilerek untangle programı kuruldu.

3.2.2.2 Uygulama

Untangle'ın kurulumu gerçekleştikten sonra internet erişim kayıtlarının tutulabilmesi için Web filtre eklentisi, gün içinde veya geçmiş tarihte yapılan internet erişimlerinin kayıtlarına ulaşabilmek için ise rapor eklentisi kurulup yapılandırılmalıdır. **EK B2**

Untangle web filter eklentisi kurulumu ve **EK B3 Untangle reports eklentisi kurulumu** işlemleri ile bu iki eklenti kurulup yapılandırılarak internet erişim kayırları tutulmaya başlanmıştır.

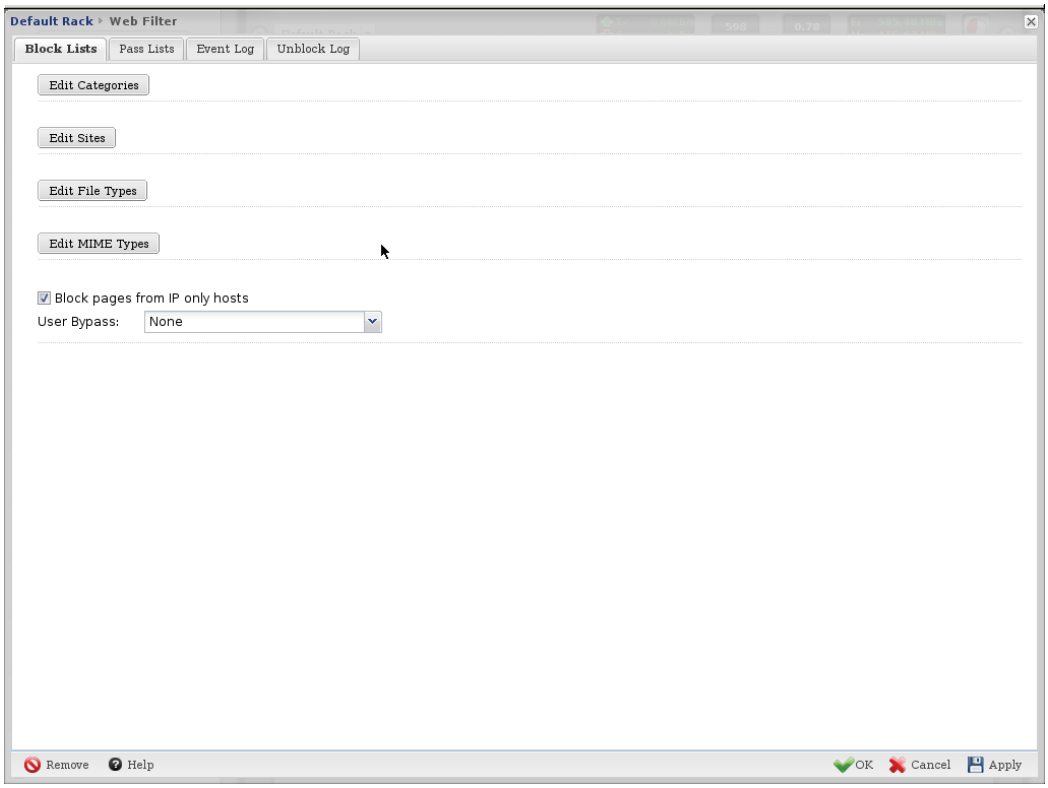


Şekil 3.7 : Untangle web arayüzü

Sunucu çalışmaya başladıktan sonra yerel ağ içerisindeki herhangi bir bilgisayardan Şekil 3.7 : Untangle web arayüzü'de görülen web arayüzüne bağlanarak sunucu yapılandırılması, ayarları ve raporlama yapılabilir. Untangle kullanımı kolay, kullanıcıya tam denetim sağlayan ve sunucu ile ilgili tüm verilerin görüntülenebildiği oldukça gelişmiş bir web arayüzüne sahiptir.

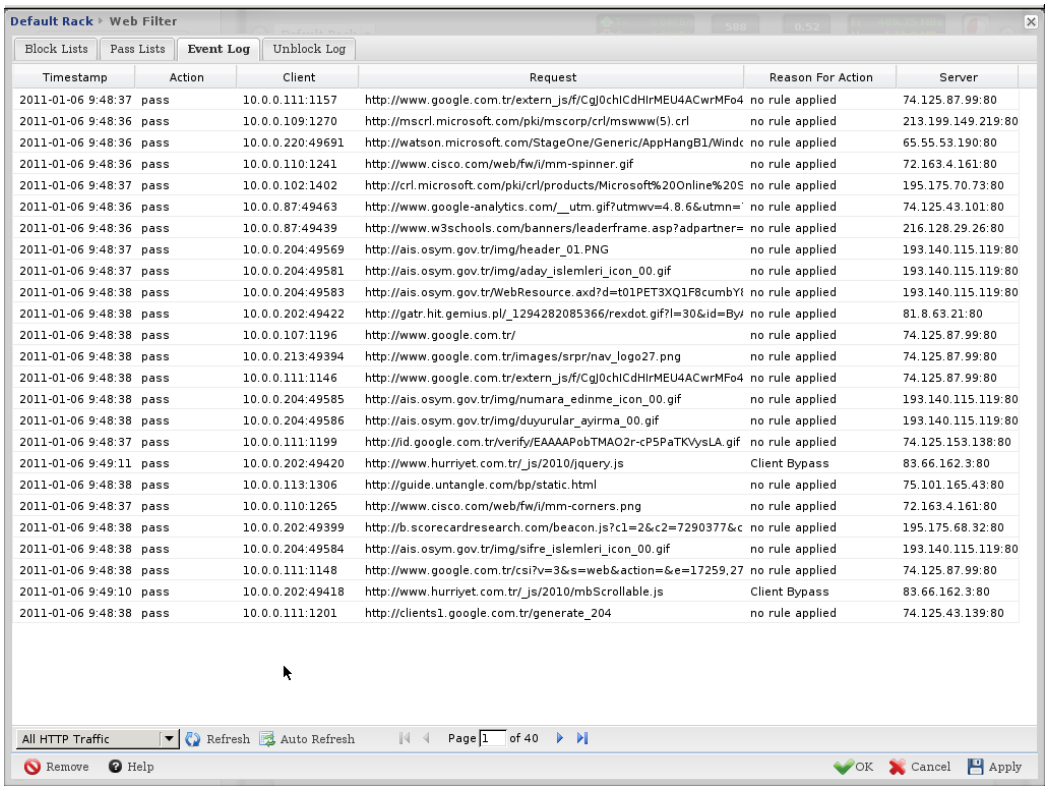
İnternet erişiminin kategori veya URL ye göre filtrelenmesi ayarlamaları ile günlük, anlık internet erişim kayıtlarını görüntülemek için "Web Filter" eklentisi üzerindeki "Settings" düğmesine tıklanarak Şekil 3.8'de görülen "Web Filter" menüsüne geçilmelidir. Şekil 3.8'de görülen "Web Filter" menüsü içerisindeki "Block Lists"

sekmesi internet erişiminin filtrelenmesi ayarlarının yapılmasında, Şekil 3.9'de görülen "Event Log" sekmesi ise anlık internet erişim kayıtlarının görüntülenmesinde kullanılır.



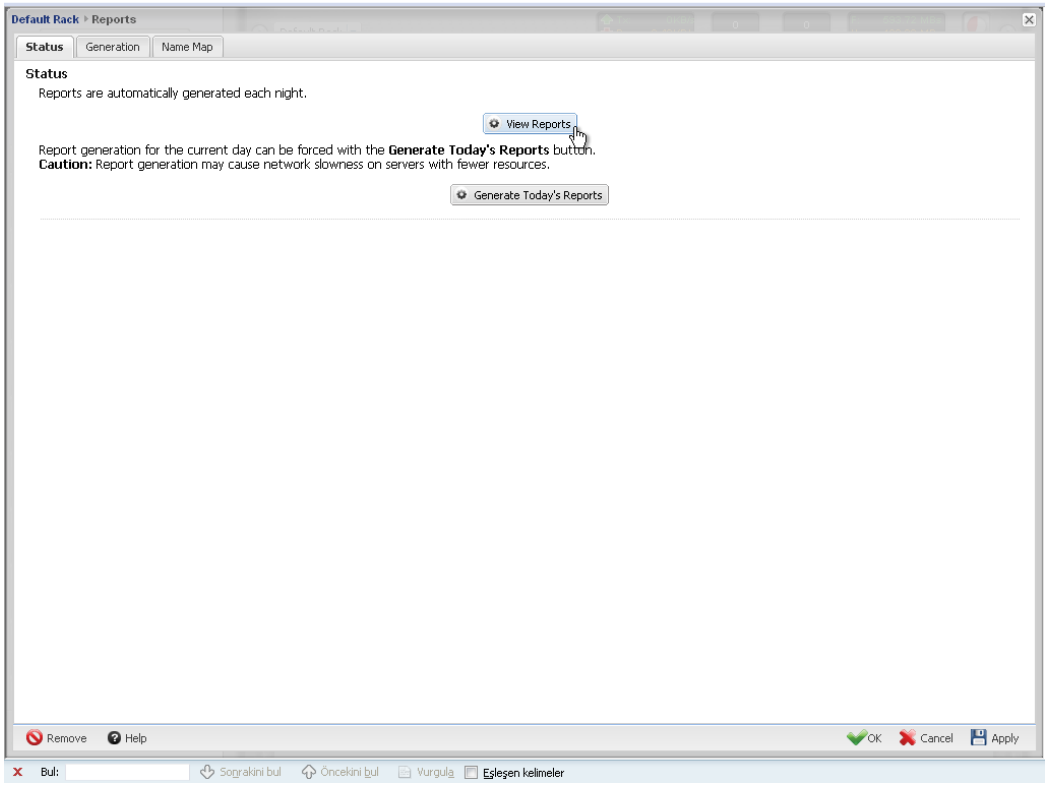
Şekil 3.8 : Untangle web arayüzü "Web Filter" menüsü "Block Lists" sekmesi

Anlık internet erişim kayıtlarının ekrana listelenebilmesi için "Event Log" sekmesinde "All HTTP Traffic" seçilip "Refresh" düğmesine tıklanmalıdır. Şekil 3.9 : Untangle web arayüzü "Web Filter" menüsü "Event Log" sekmesi gibi anlık internet erişim kaydı erişim tarihi, erişim saati, istemci IP adresi, erişilen web sitesi adresi ve erişilen web sunucu IP adresi şeklinde ekrana listelenecektir. Aşağıda bulunan "Page" bölümünün iki yanındaki oklar yardımı ile istenilen bir zaman dilimine ait internet erişim kaydı görüntülenebilinir.



Şekil 3.9 : Untangle web arayüzü "Web Filter" menüsü "Event Log" sekmesi

Geçmiş tarihte yapılan internet erişimlerinin kayıtlarını görüntülemek için ise web arayüzü içerisinde ki "Reports" menüsü kullanılır. Web ara yüzünde "Reports" eklentisi üzerinde bulunan "Settings" düğmesine tıklanarak Şekil 3.10'de görülen "Reports" menüsüne geçilmelidir.



Şekil 3.10 : Untangle web arayüzü "Reports" menüsü

"Reports" menüsü içerisinden geçmiş tarihlere ait internet erişim kayıtlarının yanı sıra sunucu ile ilgili tüm performans bilgileri, internet bant genişliği kullanımı, yoğunlukta kullanılan web sayfaları, "Firewall" gibi diğer eklentilere ait raporlar görüntülenebilmektedir. Gün içerisinde tutulan tüm kayıtlar gece yarısı rapor olarak oluşturulur. Eğer içinde olunan günün raporu gece yarısından önce oluşturulmak isteniyor ise "Generate Today's Reports" düğmesi ile bu işlem başlatılabilir. Ancak bu işlemin sistem kaynaklarını yoğun bir şekilde kullandığı unutulmamalıdır. Bu sebepten "Reports" eklentisi geçmiş tarihli kayıtların görüntülenebilmesi için kullanılır.

"Reports" menüsünden "View Reports" düğmesi ile Şekil 3.11'de görülen raporlama penceresine geçiş yapılır.

Şekil 3.11 : Untangle web arayüzü "Reports" penceresi

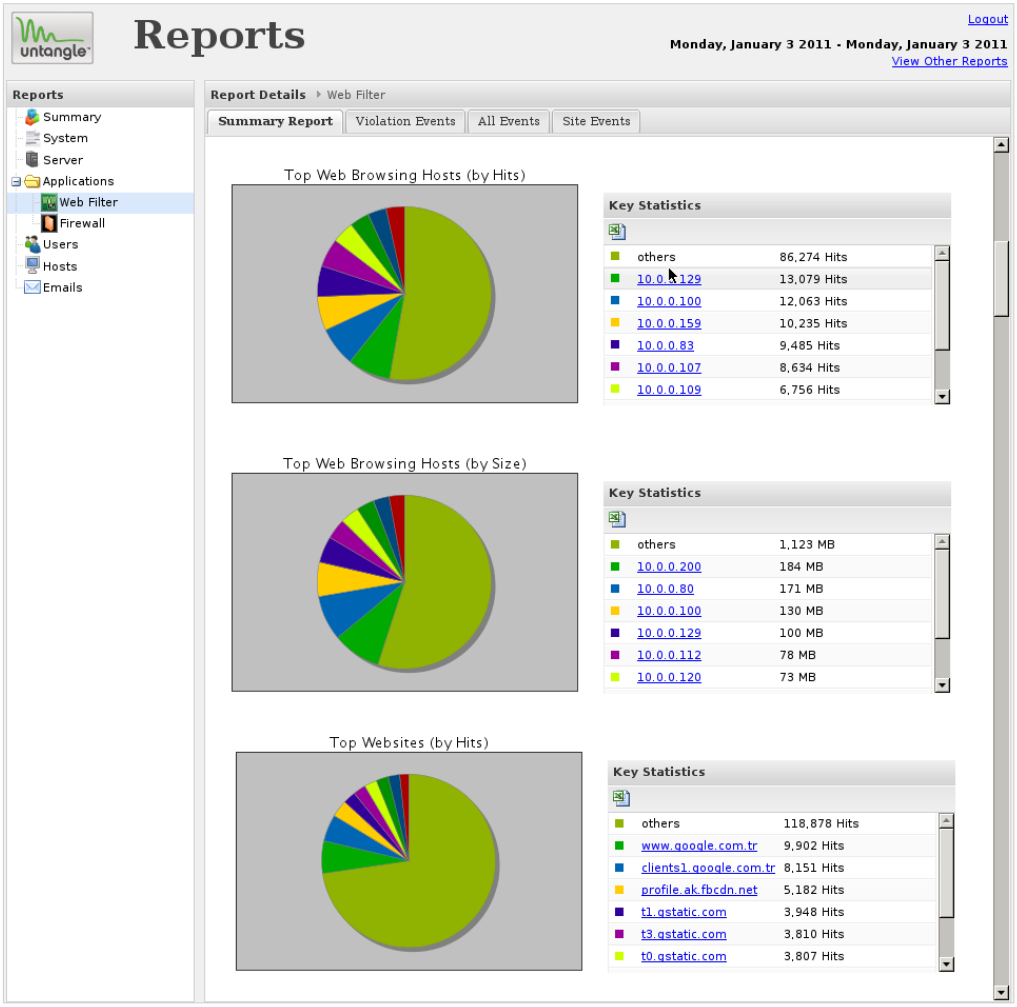
Bu pencereden geçmiş tarihlere ilişkin sunucu ile ilgili tüm kayıtlara erişilebilir. Geçmiş tarihlere ilişkin internet erişim kayıtları "Web Filter" bölümünden görüntülenmektedir.

Pencerenin sağ üst köşesinde raporun ait olduğu tarih bulunmaktadır. Başka bir tarihe ait kayıtları görüntülemek için "View Other Raports" düğmesi ile ilgili tarihin raporlarına erişilir.

3.2.2.3 Sonuçlar

Untangle ile internet erişim kayıtlarının tutulması uygulaması iki ay boyunca sürdürülebilmiştir. Bu iki aylık süre boyunca geçmişe dönük internet erişim kayıtlarının tutulmasında ve raporlanmasında herhangi bir sıkıntı yaşanmamıştır.

Şekil 3.12'de görüldüğü gibi internet erişim kayıtlarına ilişkin en çok internet adresi ziyaret eden kullanıcılar, en çok veri indiren kullanıcılar, en çok ziyaret edilen siteler gibi çeşitli istatistiki bilgiler de elde edilebilmektedir.



Şekil 3.12 : Untangle web arayüzü Web Filter menüsü rapor sekmesi

Kullanıcılar, yapılan görüşmelerde internet trafiğinin yoğun olduğu saatlerde sunucu kullanılmadığı ve IPCop sunucusunun kullanıldığı dönemlere göre internet hizmetinin yavaşladığını, sık sık kesilmeler olduğunu bildirmişlerdir.

Gün içerisinde en az 60 istemcinin aynı anda interneti kullandığı, yoğun internet trafiğinin oluştuğu saatlerde sunucunun performansını gösteren "top" komutu ile yapılan kontrollerde alınan sonuçlardan ortalama bir tanesi Şekil 3.13'de görülmektedir.

```
top - 09:46:02 up 37 min,  1 user,  load average: 4.31, 4.44, 3.18
Tasks:  84 total,   4 running,  80 sleeping,   0 stopped,   0 zombie
Cpu(s): 81.2%us, 12.5%sy,  0.0%ni,  0.0%id,  0.0%wa,  1.0%hi,  5.2%si,  0.0%st
Mem:   1035692k total,  1015036k used,    20656k free,    23532k buffers
Swap:  1381580k total,        0k used,  1381580k free,   532068k cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
 4867 root      20   0  663m 240m 8772 S 99.9 23.8  18:20.84 java
 8899 postgres  20   0 44884 7136 5508 S  2.0  0.7   0:02.58 postgres
 3404 dnsmasq   20   0  2328  600  460 S  1.0  0.1   0:01.93 dnsmasq
 7424 kiosk     20   0  172m  78m  18m S  1.0  7.7   1:46.68 firefox-bin
15496 root      20   0  2388 1120  884 R  1.0  0.1   0:00.14 top
    1 root      20   0  2100  688  588 S  0.0  0.1   0:01.70 init
    2 root      15  -5     0    0    0 S  0.0  0.0   0:00.00 kthreadd
    3 root      RT  -5     0    0    0 S  0.0  0.0   0:00.00 migration/0
    4 root      15  -5     0    0    0 S  0.0  0.0   0:00.05 ksoftirqd/0
    5 root      RT  -5     0    0    0 S  0.0  0.0   0:00.02 watchdog/0
    6 root      15  -5     0    0    0 S  0.0  0.0   0:00.13 events/0
    7 root      15  -5     0    0    0 S  0.0  0.0   0:00.00 khelper
   41 root      15  -5     0    0    0 S  0.0  0.0   0:01.14 kblockd/0
   43 root      15  -5     0    0    0 S  0.0  0.0   0:00.00 kacpid
   44 root      15  -5     0    0    0 S  0.0  0.0   0:00.00 kacpi_notify
  175 root      15  -5     0    0    0 S  0.0  0.0   0:00.00 kseriod
  212 root      20   0     0    0    0 S  0.0  0.0   0:00.00 pdflush
  213 root      20   0     0    0    0 S  0.0  0.0   0:00.91 pdflush
  214 root      15  -5     0    0    0 S  0.0  0.0   0:00.00 kswapd0
  215 root      15  -5     0    0    0 S  0.0  0.0   0:00.00 aio/0
  779 root      15  -5     0    0    0 S  0.0  0.0   0:00.00 ksuspend_usbd
  783 root      15  -5     0    0    0 S  0.0  0.0   0:00.00 khubd
  955 root      15  -5     0    0    0 S  0.0  0.0   0:00.00 scsi_eh_0
 1003 root      15  -5     0    0    0 S  0.0  0.0   0:00.00 ata/0
 1005 root      15  -5     0    0    0 S  0.0  0.0   0:00.00 ata_aux
 1100 root      15  -5     0    0    0 S  0.0  0.0   0:03.14 kjournald
 1290 root      16  -4  2284  796  488 S  0.0  0.1   0:00.08 udevd
```

Şekil 3.13 : Untangle ortalama "top" komutu sonucu

Şekil 3.13'de görüldüğü üzere sunucunun yük durumu son 1 dakika içinde ortalama %431, son 5 dakika içinde ortalama %444 ve son 15 dakika içinde ortalama %318 oranındadır. Load average'nin %100 den büyük olduğu durumlarda süreçlerin %100 den büyük olan kısmı ötelenip sıraya konarak gerçekleştirilmektedir. Bu ötelemeler sonucu süreçlerin gerçekleştirilmesinde gecikmeler olacaktır. Bu sonuç göz önünde bulundurulduğunda kullanıcıların internet erişimlerinin kesilme sebebi anlaşılmaktadır. Ayrıca 1035692k olan toplam bellek miktarının %98 i olan 10150636k bellek kullanımdadır. Sunucu üzerindeki belleğin 20656k'sı boş olup ek belleğe ihtiyaç duyulmadığından 1381580k olan sanal bellek (swap) kullanımda değildir.

Bu sonuçlara bakıldığında load average ın %1,00 in çok çok üstünde olması mikroişlemcinin yetersiz geldiğini, fiziksel belleğin %95 ler civarında kullanılıyor

olmasının untangle işletim sisteminin çok fazla sistem kaynağına ihtiyaç duyduğunu göstermektedir.

4. SONUÇ

Çağımızın vazgeçilemez iletişim ortamı olan internet birçok işlemin yapılmasını ve kullanıcıların bilgiye erişimini kolaylaştırdığı gibi suç unsuru barındıran erişimler ve işlemler için de kullanılabilmektedir. Bu uygunsuz kullanımın tespiti için TCK'nın 5651 sayılı kanununda belirtildiği üzere erişim trafik bilgilerinin kaydedilmesi çok önemlidir.

Milli Eğitim Bakanlığına bağlı eğitim kurumlarında ödeneklerin çok kısıtlı olması sebebi ile erişim kayıtlarının tutulması ve saklanması işleminin ücretsiz yazılımlar kullanılarak yapılması daha uygundur. Bu nedenle bu araştırmada TCK'nın 5651 sayılı kanunun gerektirdiği erişim trafik bilgisinin kaydedilmesi ve saklanması işlemi, toplu kullanım ortamına örnek olarak seçilen bir orta öğretim kurumunda gerçekleştirilmiştir.

Özgür yazılım dünyasında ağ yönetimi ve internet erişimi kontrolü gibi uygulamalar için sıkça kullanılan ücretsiz yazılımlardan olan IPcop ve untangle programları ile trafik bilgisinin nasıl tutulacağı ve en verimli trafik bilgisi tutma programının tespitine yönelik karşılaştırma yapılmıştır.

Öncelikle orta öğretim kurumunun ağ yapısı amaca yönelik olarak planlanmıştır. Bunu takiben her iki program ile de yapılan çalışmada, trafik bilgilerinin tutulabilmesi işlemi değerlendirilmiştir. Bunun yanında kullanılan programın internet trafiğine etkisi, kullanım kolaylığı, donanım gereksinimi, performansı ve maliyeti de göz önünde bulundurulmuştur.

Yapılan çalışma sonucunda erişim trafiği bilgisi kayıt kabiliyeti ele alındığında her iki programın da erişim trafik bilgisini saat, tarih, kaynak ve hedef adresi olarak tespit edip, saklayabildiği görülmüştür. Ayrıca zamana bağlı trafik bilgisi sorgulandığında, her iki programın da web arayüzünden kolaylıkla rapor alındığı gözlemlenmiştir. Ancak çalışma konumuz dışında da olsa geçmişe dönük sistem bilgileri, bant genişliği veya istatistiki erişim trafik bilgisi gibi bilgilere ihtiyaç duyulduğunda untangle'ın bu tür raporlamaları da yapabildiği görülmüştür.

Tablo 4.1: IPCop ve Untangle programlarının "top" performans değerleri

	Yük durumu (1dk önce)	Yük durumu (5dk önce)	Yük durumu (15dk önce)	Task total	Task running	Task sleeping	Kullanılan CPU (user)	Kullanılan CPU (system)	Kullanılmayan CPU	Toplam Bellek	Kullanılan Bellek (RAM)		Kullanılmayan Bellek (RAM)	Mem Buffers
IPCop	0,27	0,12	0,02	45	1	44	0,0%	7,3%	92,7%	256804k	142992k	55,7%	113812k	25988k
untangle	4,31	4,44	3,18	84	4	80	81,2%	12,5%	0,0%	1035692k	1015036k	98,0%	20656k	23532k

Programların sistem performansı

Tablo 4.1'de ki ortalama "top" komutu verileri ile değerlendirilmiştir. Buna göre 1, 5 ve 15 dakikalık yük durumlarına bakıldığında IPCop'un 0,27, 0,12 ve 0,02 değerleri ile mikroişlemci kullanımı normal sınırlar içerisindeyken, untangle'ın 4,31, 4,4 ve 3,18 değerleri ile mikroişlemci gücünün yetersiz geldiği tespit edilmiştir. Bellek kullanımları bakımından incelendiklerinde IPCop'un %55,7 ile 142992k bellek kullandığı buna karşın untangle'ın %98,0 ile 1015036k bellek kullandığı tespit edilmiştir. Elde edilen bellek kullanım değerlerine bakıldığında IPCop, untangle'a göre çok az miktarda bellek alanına ihtiyaç duymaktadır. Sonuç olarak bu veriler değerlendirildiğinde IPCop'un daha az sistem kaynağına ihtiyaç duyduğu tespit edilmiştir.

Bu programların internet trafiğine etkileri bakımından değerlendirildiklerinde, untangle programının mikroişlemci kullanımını çok yüksek değerlere ulaştırarak sistem kaynaklarını çok fazla kullandığı ve bu durumun da internet trafiğinde aksamalara neden olduğu tespit edilmiştir. IPCop programı ise sistem kaynaklarını çok düşük seviyelerde kullanmaktadır. Ayrıca IPCop'un erişim trafik bilgilerini tutabilmesi için kullandığı transparan vekil sunucu eklentisinin, önbellek hizmeti sayesinde istemcilerin internet hizmeti performansında gözle görülür bir artış olduğu görülmüştür.

Mali açıdan karşılaştırıldığında, her iki program da erişim trafik kaydını oluşturacak eklentileri ile birlikte ücretsiz olarak temin edilip kullanılabilmektedir. Fakat IPCop, üzerinde önbellek desteği olan bir vekil sunucu bulunduruyor olmasına karşın untangle bu özelliği yıllık kullanım bedeli olan program paketleri ile sunmaktadır. Bununla

birlikte donanım gereksinimi açısından bakıldığında IPCop, untangle'a göre performansı daha düşük dolayısıyla daha ucuz donanımlarda da hizmet verebilmektedir.

Sonuç olarak düşük seviyeli ve maliyetli sunucularda çalışabildiği, kullanıcıların internet kullanım hızını arttırdığı, bir yerel ağın gerek duyabileceği hizmetleri yerine getiren çeşitli eklentilere sahip olduğu ve ücretsiz olarak edinilebildiği için ödenekleri sınırlı olan eğitim kurumlarında internet erişim trafiğinin kontrolü ve incelenmesi işleminde IPCop programının kullanılması uygun olacaktır.

KAYNAKÇA

Kitaplar

Baykal, N., 2005. *Bilgisayar Ağları.* Ankara: Sas Bilişim Yayınları

Connolly, K. J., 2003. *Law of Internet Security and Privacy.* NY: Aspen Law & Business

Çölkesen, R. ve Örencik, B., 2002. *Bilgisayar Haberleşmesi ve Ağ Teknolojileri.* İstanbul: Papatya Yayıncılık

Dean, T., 2009. *Network+ Guide to Networks.* Boston:Course Technology

Forcier, R.C., 1999. *The computer as an educational tool.* NJ: Prentice-Hall, Inc.

Heap, G., & Maynes, L., 2002. *CCNA practical studies*. Indianapolis: Cisco Press

Karris, S.T., 2009. *Network Design and Management.* California: Orchard Publications

Mueller, S., 2003. *Upgrading and Repairing PCs*. USA: Que Publishing

Odom, W., 2003. *Cisco CCNA 640–647 sınavı sertifikasyon rehberi.* İstanbul: Sistem Yayıncılık

Roblyer, M.D. & Edwards, J., 2000. *Integrating educational technology into teaching.* NJ: Prentice-Hall, Inc.

Shinder, D. L., 2000. *Computer networking essentials.* Indianapolis: Cisco Press

Spurgeon, C. E., 2000. *Ethernet: The Definitive Guide*. California: O'Reilly Media Inc.

Diğer Yayınlar

Akkuş, D., 2003, Güvenlik Duvarı Kavramları [online], Linux Belgelendirme Çalışma Grubu, http://www.belgeler.org/howto/proxy-fw_concepts.html#proxy-fw_proxy [Ziyaret Tarihi: 14 Kasım 2010]

Çay, K., 2010, TCP / IP protokol grubu tarihçesi [online], Turkcenet, http://www.turkcenet.org/index.php?option=com_content&task=view&id=256&Itemid=55&limit=1&limitstart=0. [Ziyaret Tarihi: 17 Eylül 2010].

Ethernet Cables Comparison between CAT5, CAT5e, CAT6, CAT7 Cables. 2010. http://discountcablesusa.com/ethernet-cables100.html [Ziyaret Tarihi: 14 Kasım 2010]

GÜ, Gazi Üniversitesi BL211 Bilgisayar Ağ Sistemleri Bilgisayar Teknolojisi ders notu, 2010, http://uemyo.uegazi.edu.tr/DERSler/bilgisayar_teknolojisi/BIL-211.pdf [Ziyaret Tarihi: 15 Eylül 2010].

Internet Usage in Europe. 2010. http://www.internetworldstats.com/stats4.htm [Ziyaret Tarihi: 03 Eylül 2010].

ITU, Ethernet Kablo Tipleri ve Kablo Hazırlanışı, 2010, http://www.bidb.itu.edu.tr/?d=372 [Ziyaret Tarihi: 14 Kasım 2010]

ipcop, IPCop, http://www.ipcop.org [Ziyaret Tarihi: 20 Nisan 2010].

İÜBUYAMER, Fiber optik kablo, 2010, http://buyamer.istanbul.edu.tr/index.asp?grp=egitim&no=8 [Ziyaret Tarihi: 14 Kasım 2010]

MEB, Fatih Projesi, 2010, http://www.meb.gov.tr/haberler/haberayrinti.asp?ID=8285 [Ziyaret Tarihi: 22 Kasım 2010].

MEGEP, Mesleki eğitim ve öğretim sistemini geliştirme projesi, http://www.megep.meb.gov.tr [Ziyaret Tarihi: 15 Ağustos 2010].

Sezlev, M., 2008, ADSL Hakkında. Bilgi Teknelojileri [online], UMS Bilgi teknolojileri, http://www.umsbilgi.com.tr/index.php?option=com_content&view=article&id=3&Itemid=3 [Ziyaret Tarihi: 15 Ekim 2010].

Şeker, Ş.E., 2007, vekil sunucu [online], Bilgisayar kavramları, http://www.bilgisayarkavramlari.com/2007/12/12/vekil-sunucu-proxy-server. [Ziyaret Tarihi: 20 Kasım 2010].

TAGEM, Temel ag kavramlari, 2010, http://www.cizgi-tagem.org/resource/vfiles/tagem/dms_file/223/temel_ag_network_kavramlari.pdf [Ziyaret Tarihi: 10 Eylül 2010].

TCK, Türk Ceza Kanunu, 2004, http://www.mevzuat.gov.tr/Metin.Aspx?MevzuatKod=1.5.5237&sourceXmlSearch=&MevzuatIliski=0 [Ziyaret Tarihi: 12 Ekim 2010].

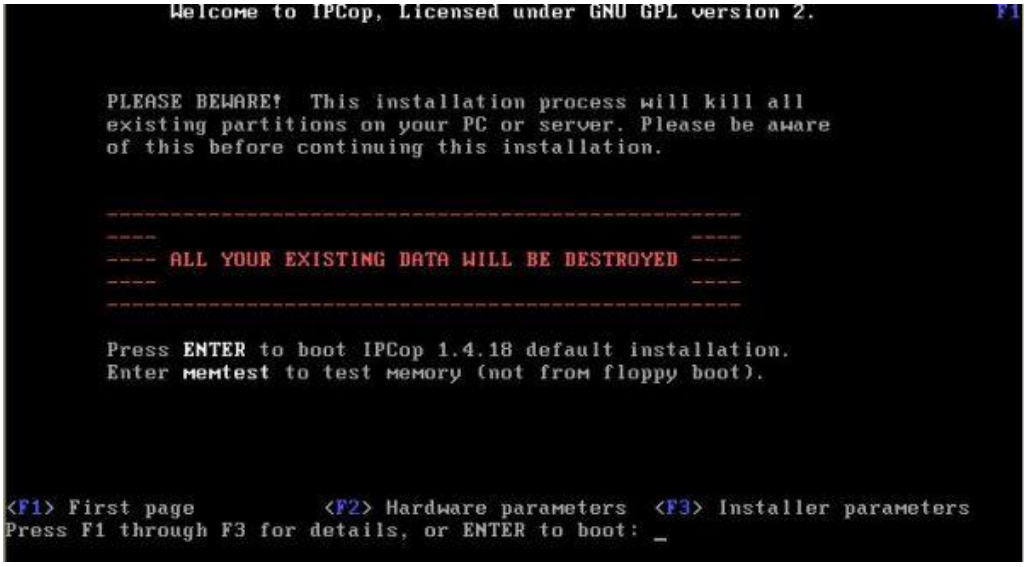
untangle, Untangle Lite Package, http://www.untangle.com/Products/untangle-libitem-lite-package. [Ziyaret Tarihi: 15 Eylül 2010].

Yılmaz, E., 2005, Bilgisayar güvenliği makalesi [online], Doctus, http://doctus.org/showthread.php?t=263. [Ziyaret Tarihi: 21 Kasım 2010].

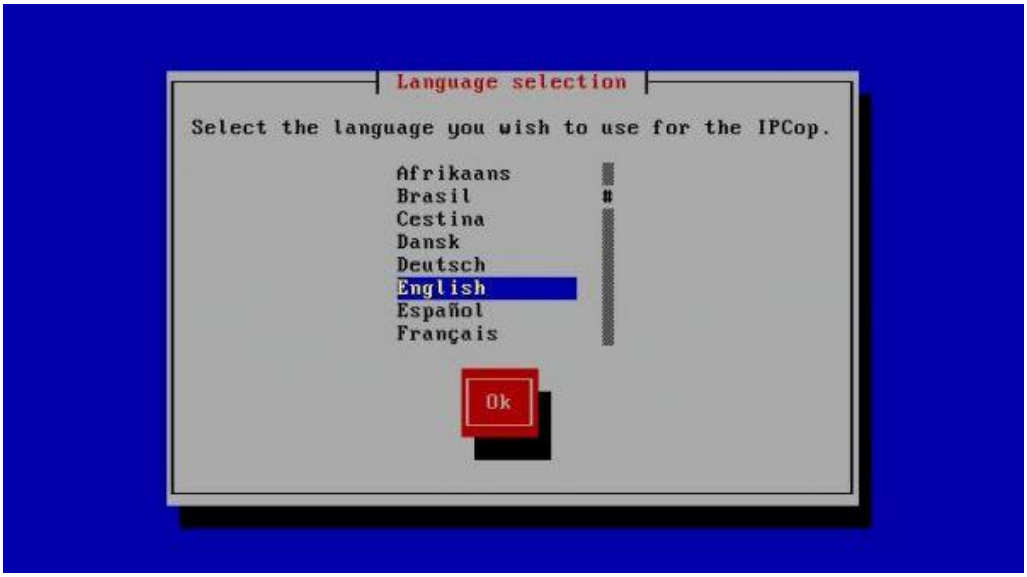
EKLER

EK A1 IPCop kurulumu

Sunucu kurulum CD ile açıldığında karsımıza gelen ilk ekran aşağıdaki gibi olacaktır.

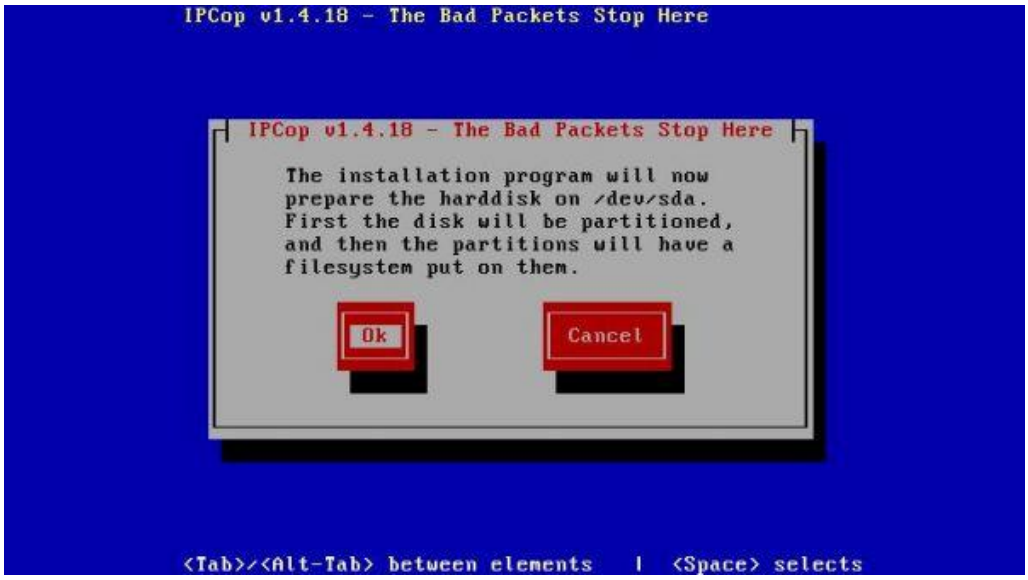


Şekil A1.1 : Bu ekranda ENTER a basarak kurulumu başlatıyoruz.

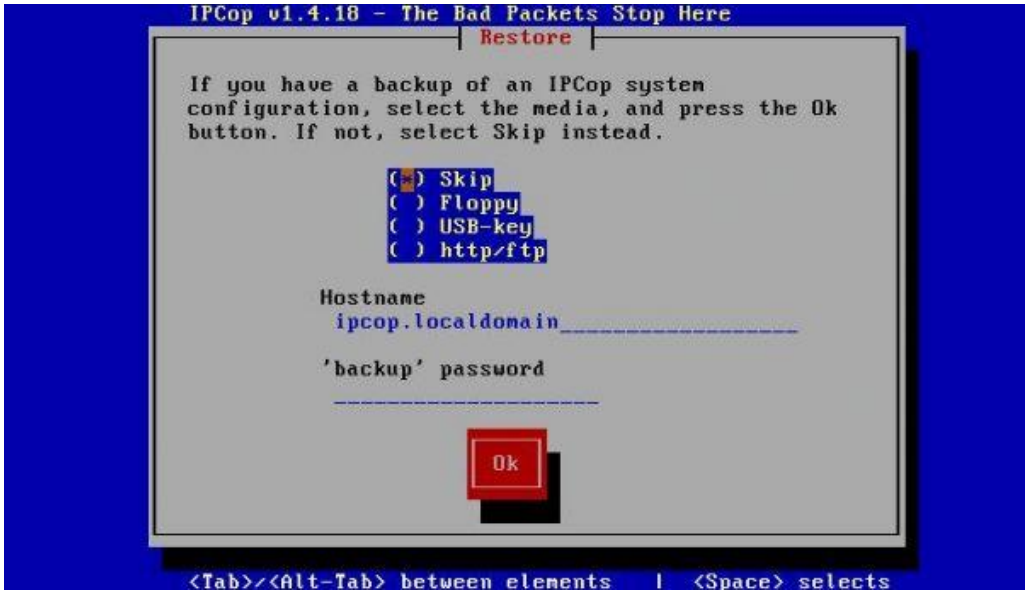


Şekil A1.2 : Kurulum dilini *"English"* seçip *"OK"* butonu ile bir sonraki adıma geçiyoruz. (Kurulum dili olarak Türkçe de seçilebiliyor fakat karakterleri göstermede problem çıkıyor.)

Şekil A1.3 : Karşımıza çıkan diğer ekran bize kurulumun nereden yapılacağını sormaktadır. (HTTP/FTP yi seçtiğimizde network kartının driver ı istenmektedir.) Biz programı CD-ROM'dan kuracağımız için bu ekranı *"OK"* diyerek geçiyoruz.



Şekil A1.4 : IPCop'un sabit diski kendine göre bölümlendireceğini belirtmektedir. *"OK"* seçiyoruz.

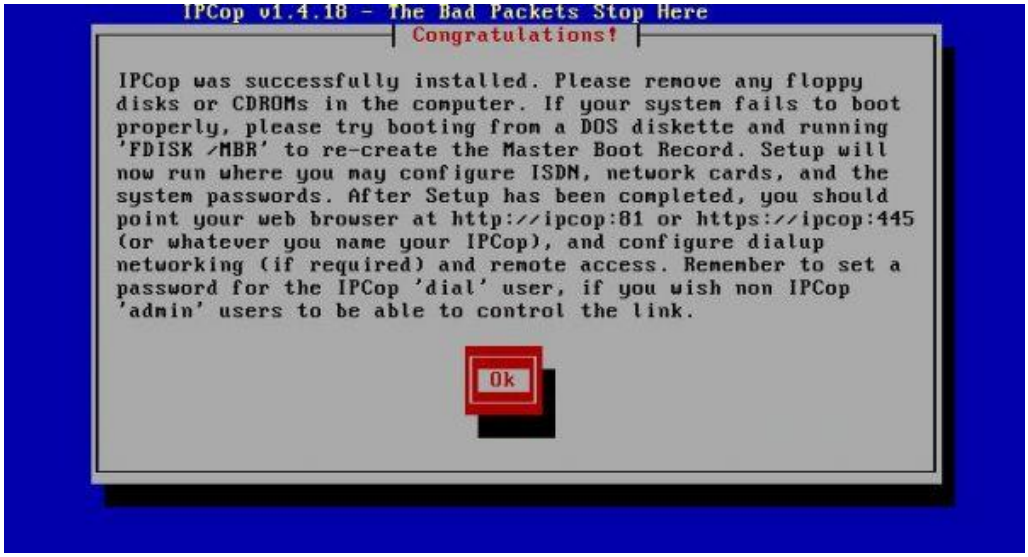


Şekil A1.5 : Biz ilk kez kurulum yaptığımız için *"Skip"* i seçiyoruz.

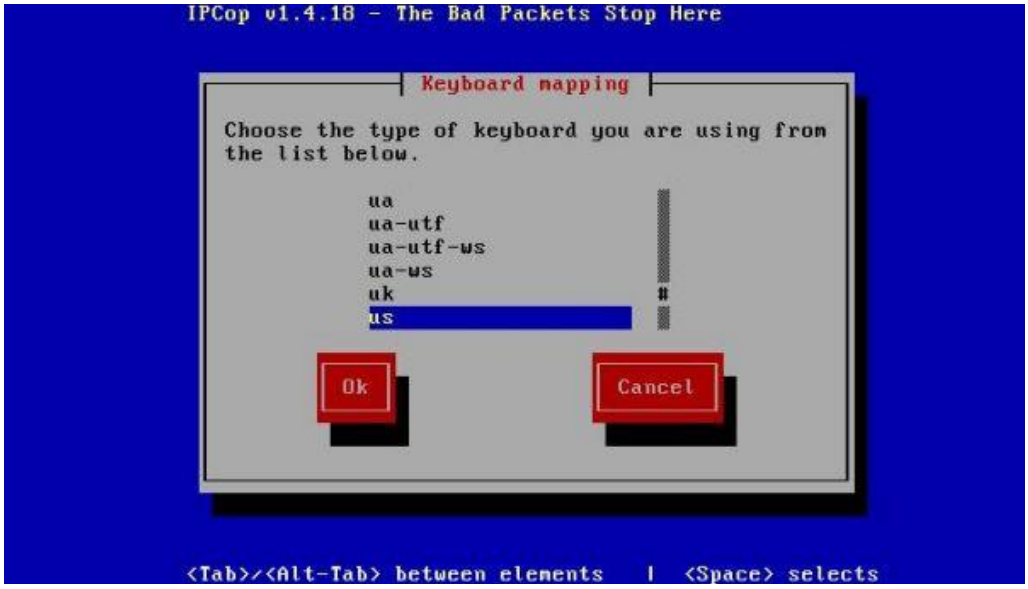
Şekil A1.6 : Sunucumuzdaki ağ kartlarının otomatik bulunması için *"Probe"* butonunu seçiyoruz.

Şekil A1.7 : Sunucuda takılı bulunan kartlar tarandıktan sonra bulunan ilk kartı listelenecektir. Bu kart Green kartıdır. *"OK"* seçiyoruz.

Şekil A1.8 : Green kartına atayacağımız IP numarasını ve alt ağ maskesini yazmamız gerekiyor. (Burada vereceğimiz IP adresi kurulum tamamen bittikten sonra web arayüze bağlanmak için kullanacağımız ve istemcilerimize ağ geçidi olarak atayacağımız adrestir.)

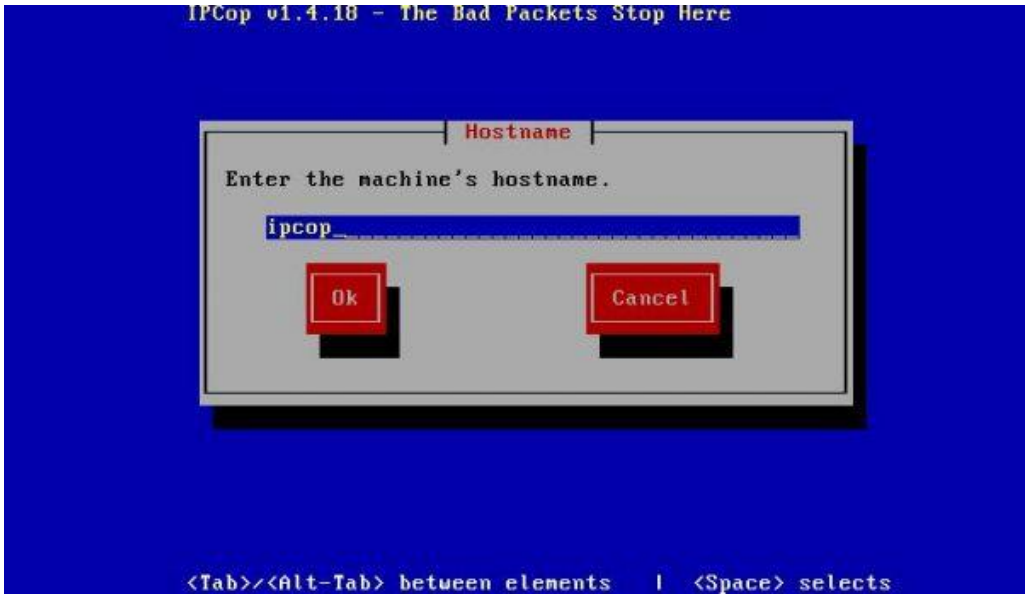


Şekil A1.9 : Kurulum başarı ile gerçekleşti. CD çıkarıldıktan sonra ayarlamalara devam etmek için *"OK"* seçilir.

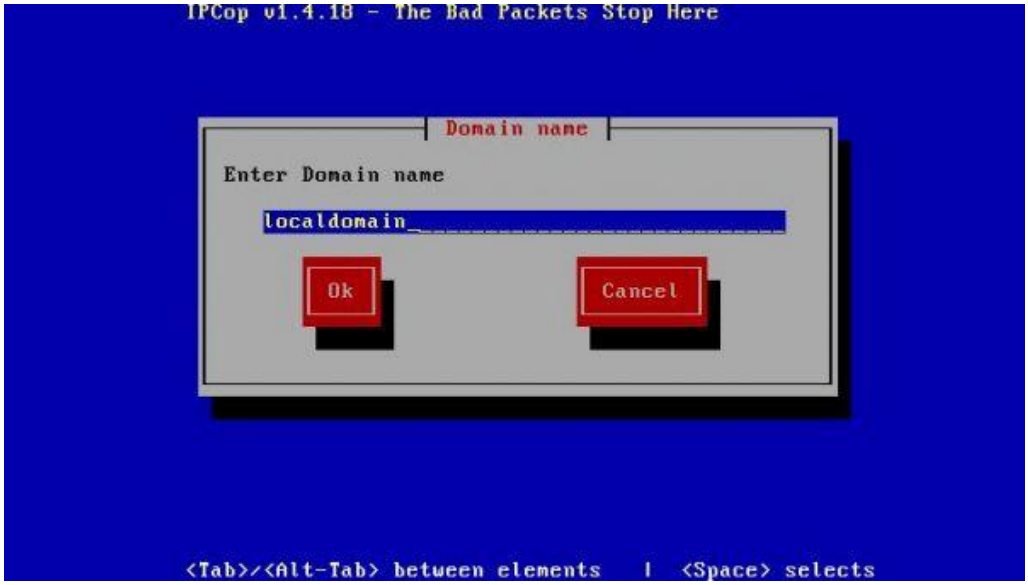


Şekil A1.10 : Burada Türkçe Q klavye için trq seçeneği seçilir.

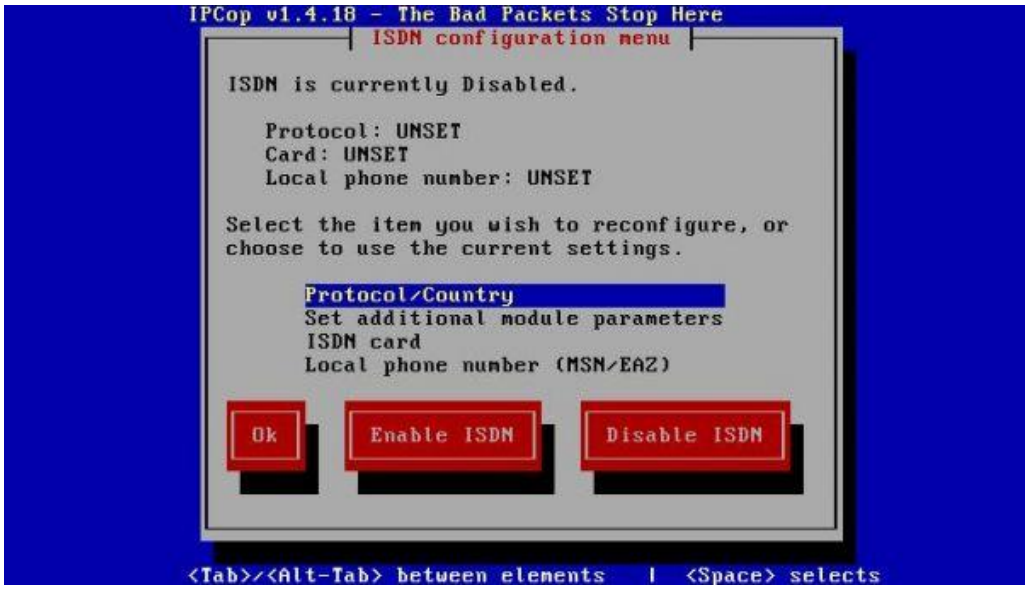
Şekil A1.11 : Zaman bölgemizi seçmemiz gerekiyor *"Turkey"* i seçilir.



Şekil A1.12 : Sunucuya vermek istediğimiz ismi burada yazıyoruz.

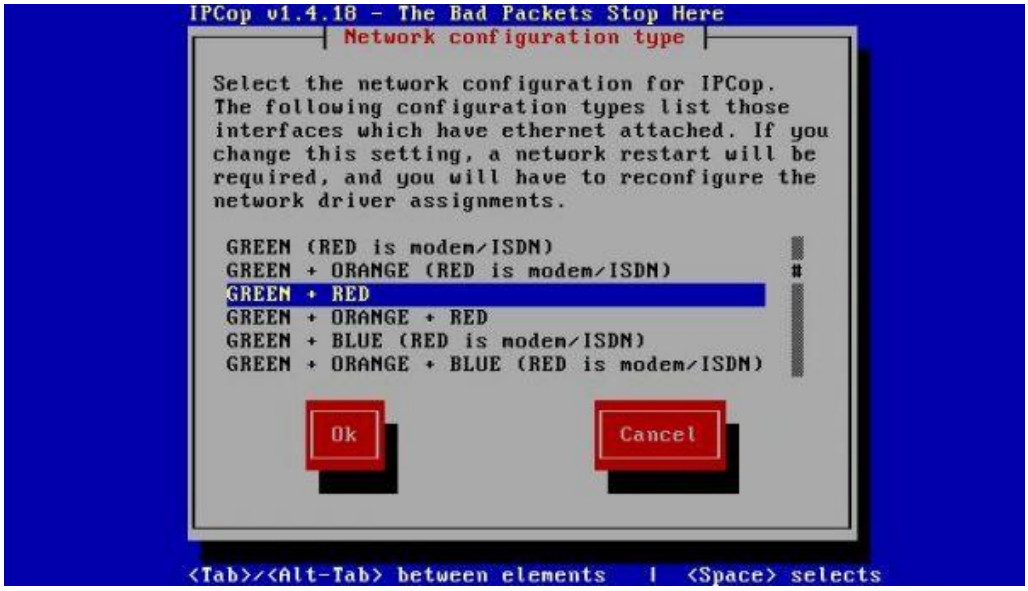


Şekil A1.13 : Domain isminizi bu alanda yazıyoruz.

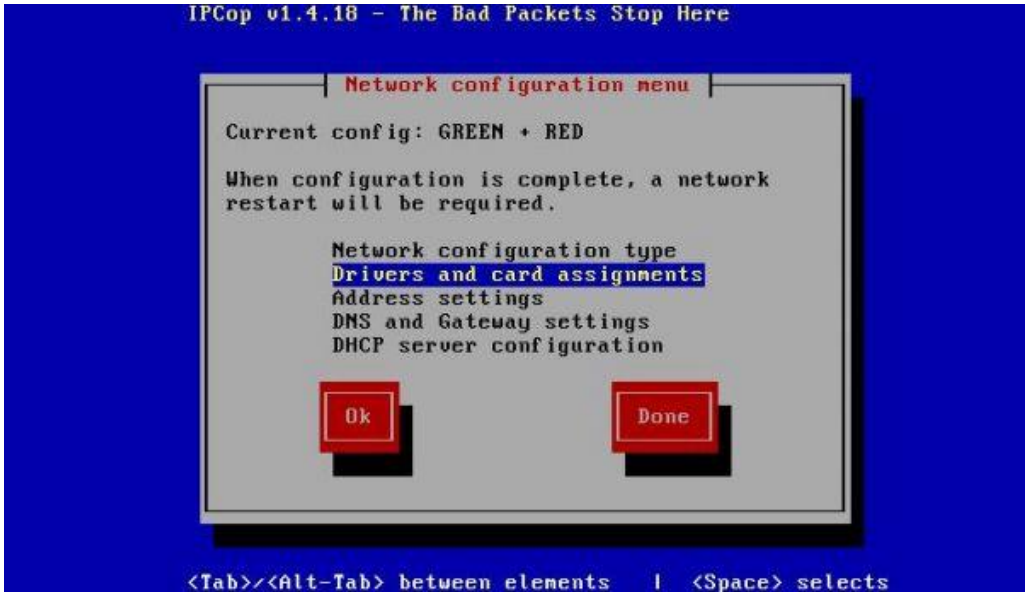


Şekil A1.14 : ISDN hat kullanmadığımız için bu kısımda *"Disable ISDN"* i seçiyoruz.

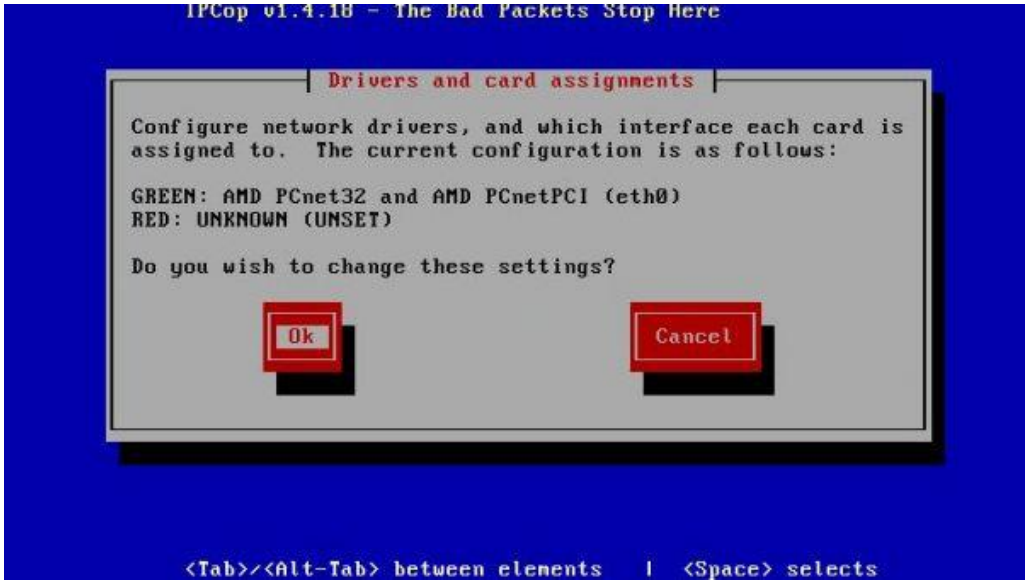
Şekil A1.15 : Ağ ayarlarını yapacağımız için *"Network configration type"* ı seçiyoruz.



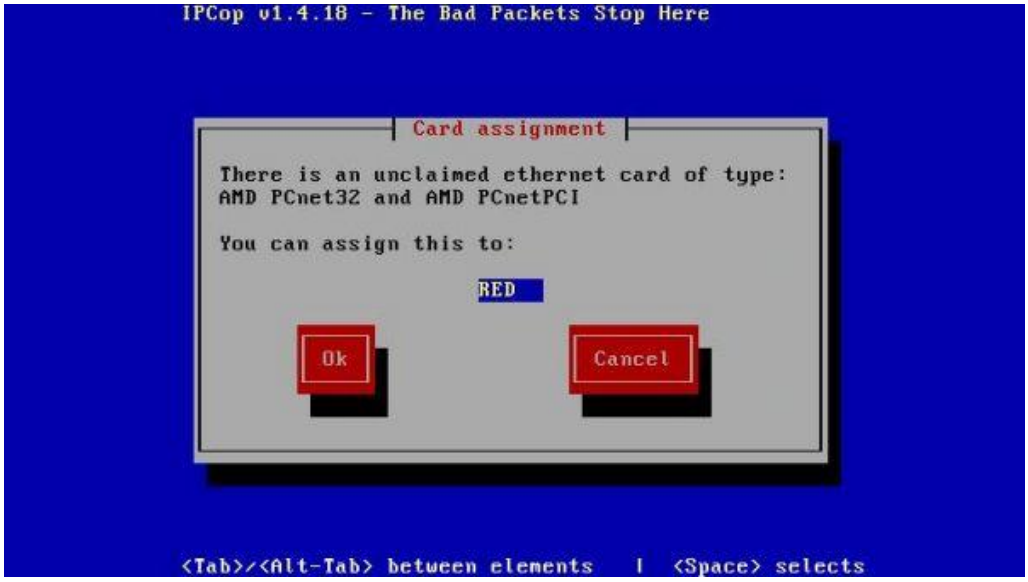
Şekil A1.16 : Sunucumuzu *"Green+Red"* olarak kullanacağımızdan bu seçeneği seçiyoruz.



Şekil A1.17 : RED ağ kartını seçmek için *"Drivers and card assignments"* ı seçiyoruz.

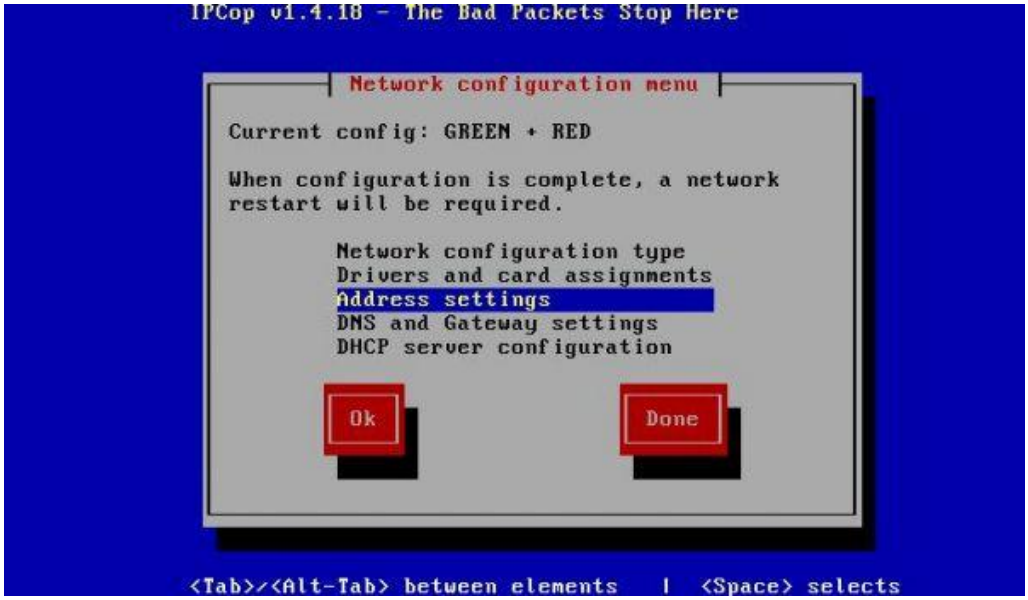


Şekil A1.18 : Green için atanan kart görünürken, Red için ise herhangidir kart atanmamıştır. *"OK"* seçiyoruz.



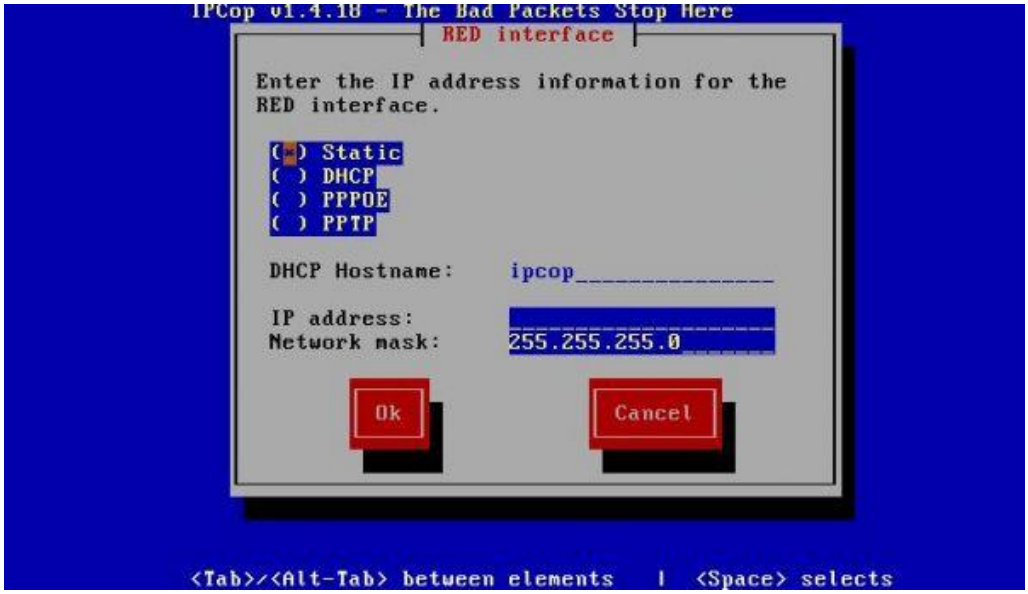
Şekil A1.19 : Sunucuya takılı olan bir kart daha bulundu. Bu kartı Red olarak seçiyoruz.

Şekil A1.20 : Tüm kartların atandığını görüyoruz. *"OK"* seçilir.

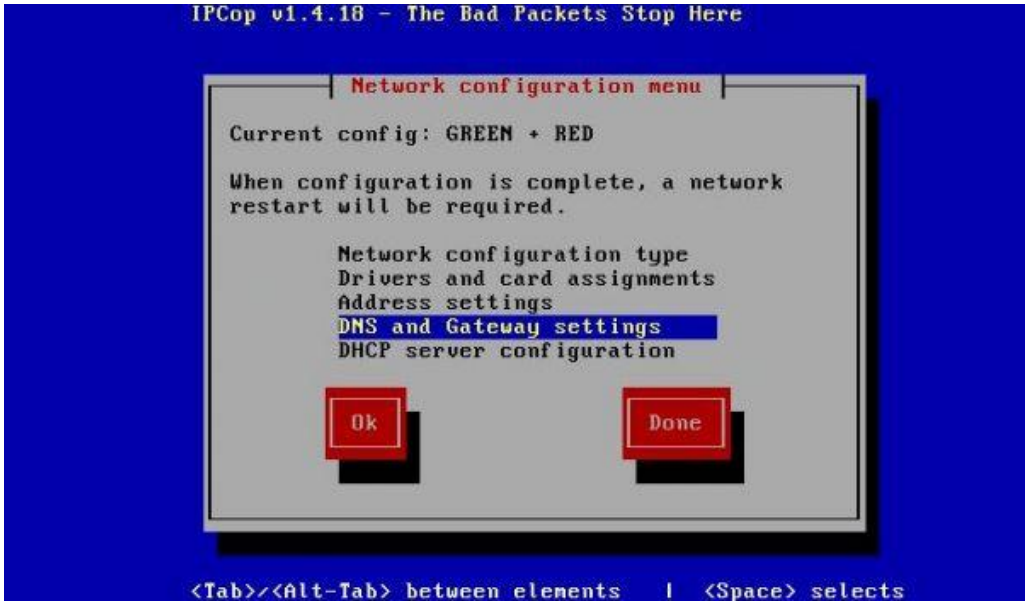


Şekil A1.21 : Red ağ kartını ayarlamak için *"Address setting"* seçiliyor.

Şekil A1.22 : RED kısmını seçip *"OK"* e basıyoruz.

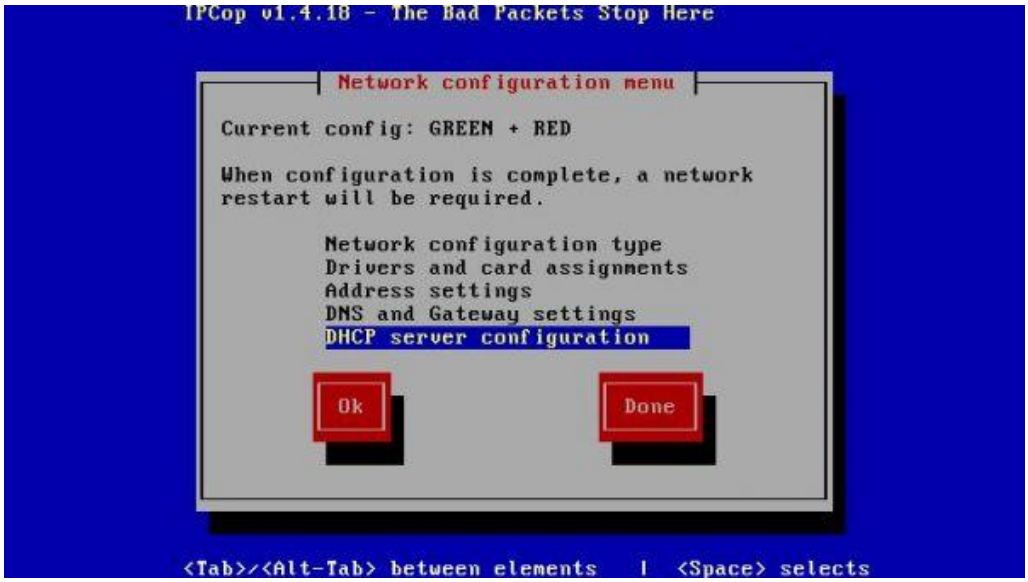


Şekil A1.23 : IP adresi sabit olduğu için *"Static"* kısmı seçilerek ADSL modeme bağlı olan kartımıza atayacağımız IP adresini ve ağ maskesini yazarak *"OK"* seçilir.



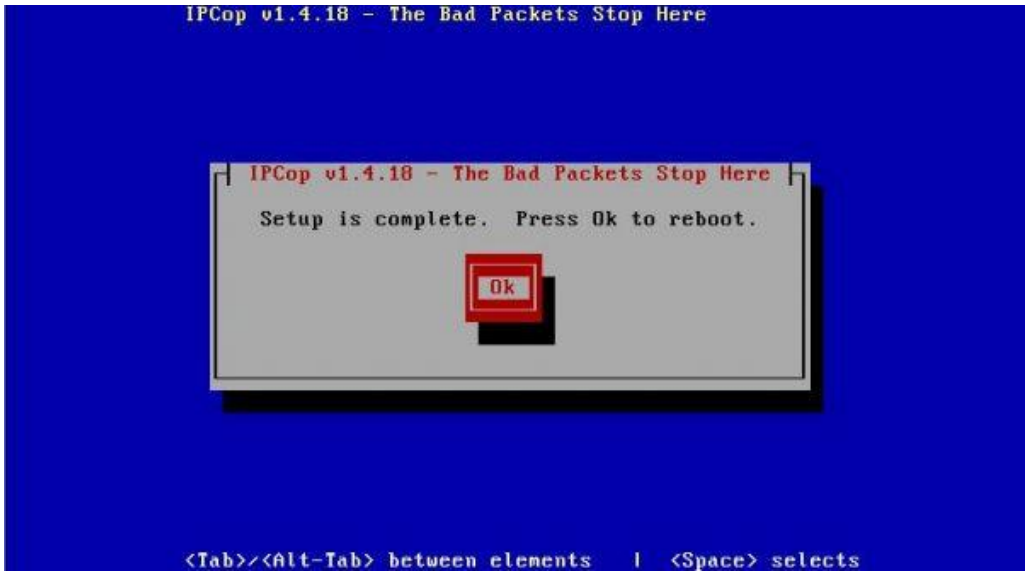
Şekil A1.24 : DNS ve Ağ geçidini ayarlamak için *"DNS and Gateway setting"* seçilir.

Şekil A1.25 : Birinci ve ikinci DNS adresi ve Varsayılan ağ geçidi bilgilerimizi buradaki kısımlara doldurulup *"OK"* seçilir.

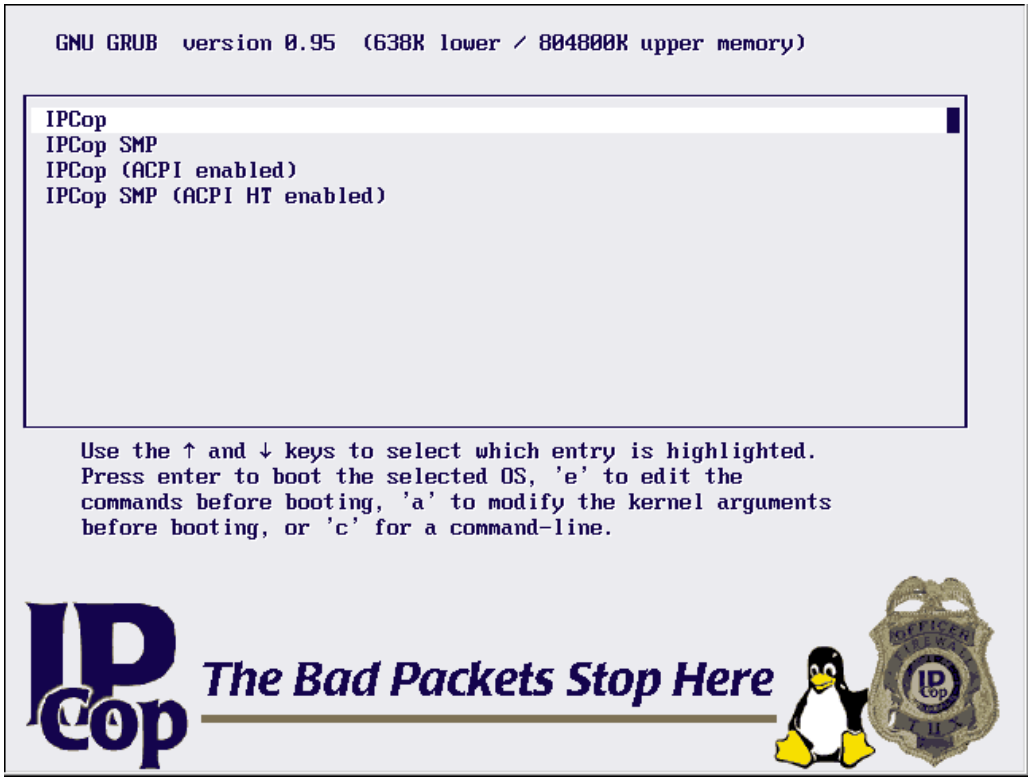


Şekil A1.26 : Yerel ağa IP dağıtmak istenir ise DHCP ayarları da yapılabilir. Ayarları tamaladığımız için *"Done"* seçilir.

Şekil A1.27 : 'root', 'admin' ve 'backup' için şifre bilgileri girilerek *"OK"* seçilir.



Şekil A1.28 : Kurulum tamamlanmıştır.

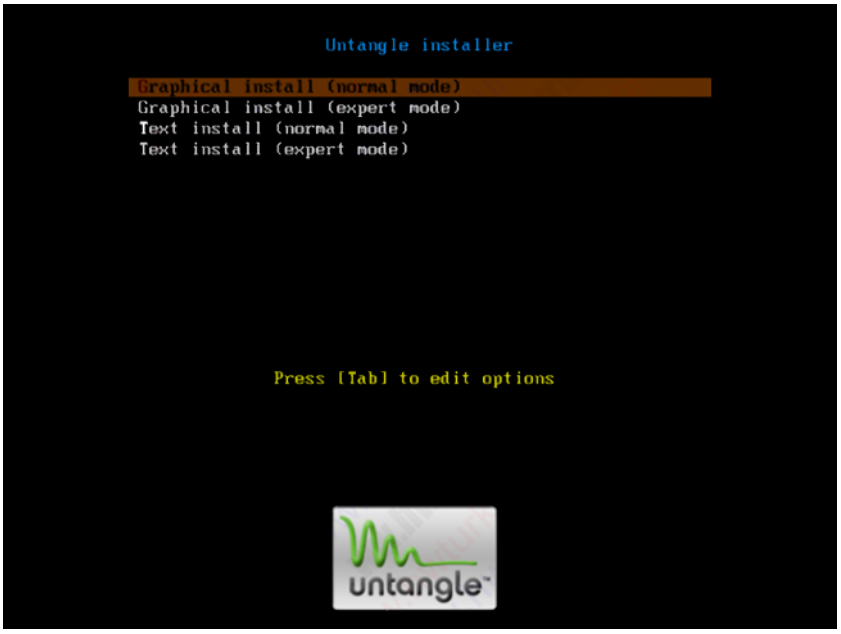


Şekil A1.29 : Sunucu yeniden başlatılırken karşımıza gelecek olan ekran yukarıdaki gibi olacaktır.

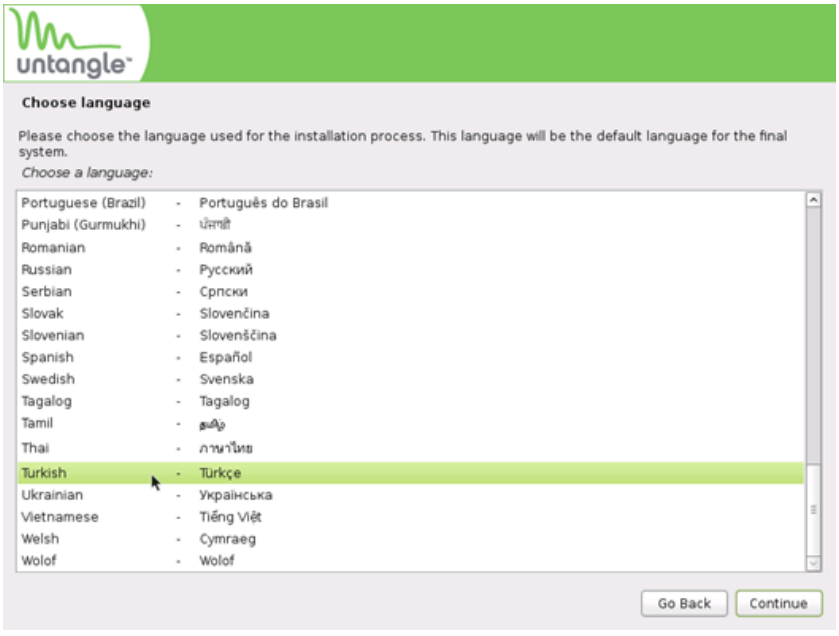
Web arayüzüne ulaşmak için https://[ipcop'a verdiginiz Green ip adresi]:445 adresi kullanılır.

EK B1 Untangle kurulumu

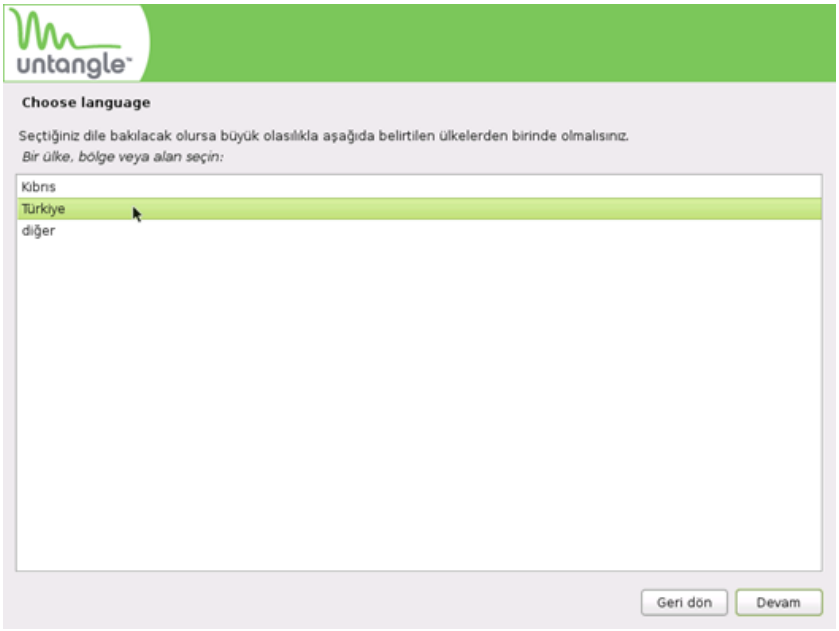
Sunucu kurulum CD ile açıldığında karsımıza gelen ilk ekran aşağıdaki gibi olacaktır.



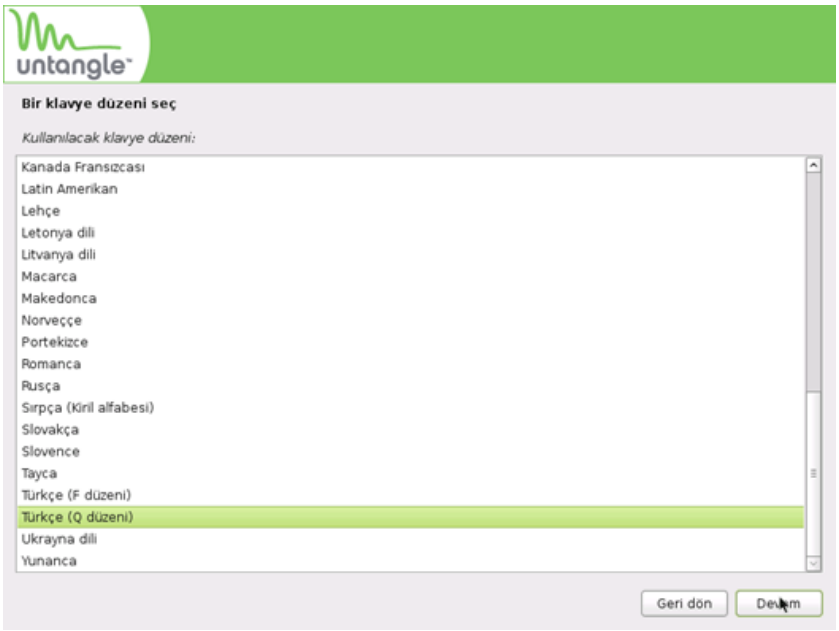
Şekil B1.1 : Untange Installer menüsünde "Graphical Install" seçeneği seçilerek kurulum başlatılır.



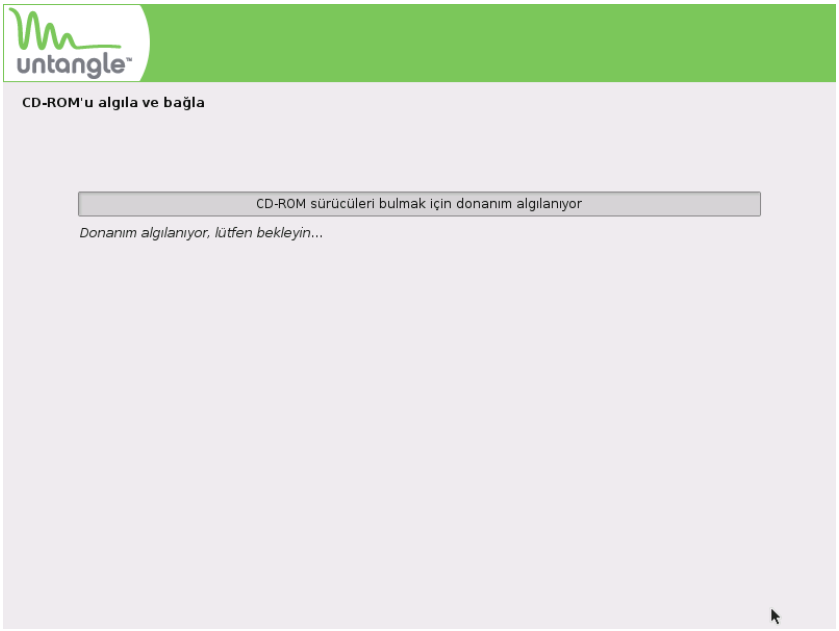
Şekil B1.2 : Kurulum dilini "Turkish" seçip "OK" ile bir sonraki adıma geçiyoruz. (Bu seçim ile bazı uygulamalar Türkçe olamayabilir.)



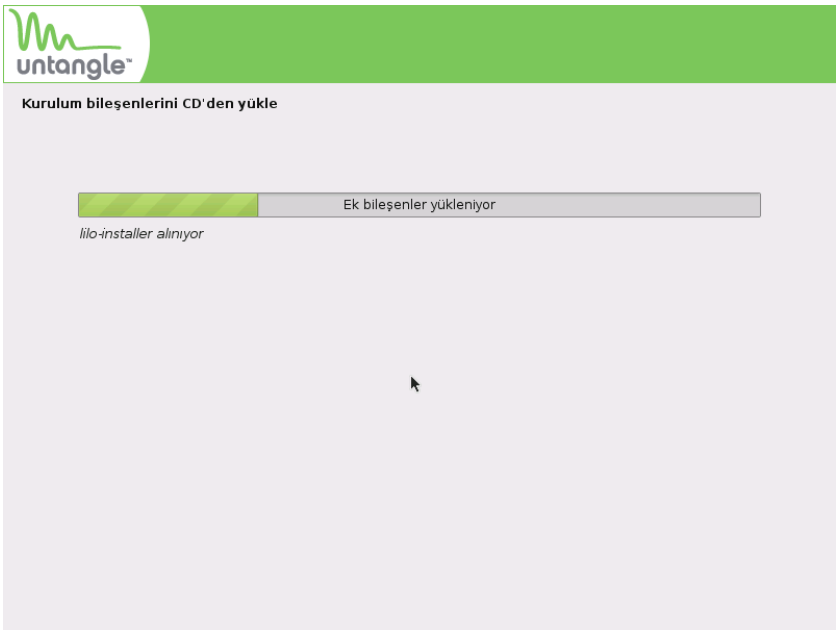
Şekil B1.3 : Bölgemizi Türkçe olarak seçip devam ediyoruz.



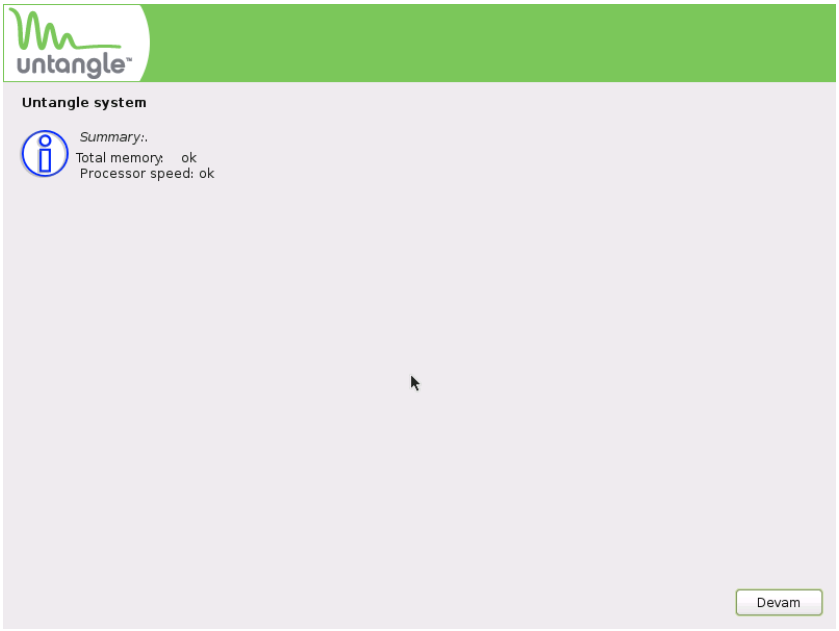
Şekil B1.4 : Klavye düzenimizi seçtiğimiz ekran Türkçe (Q düzeni) seçilir.



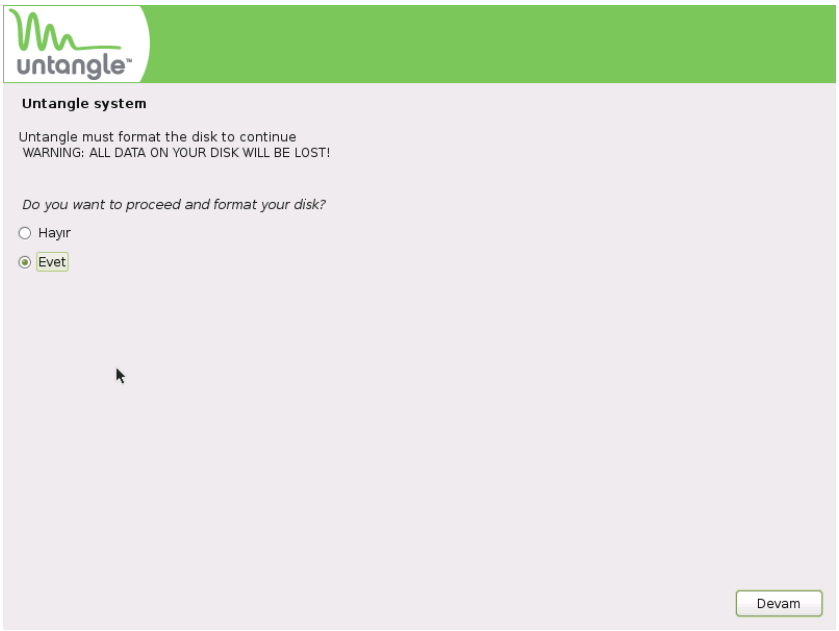
Şekil B1.5 : Untangle'ın donanımı algılaması beklenir.



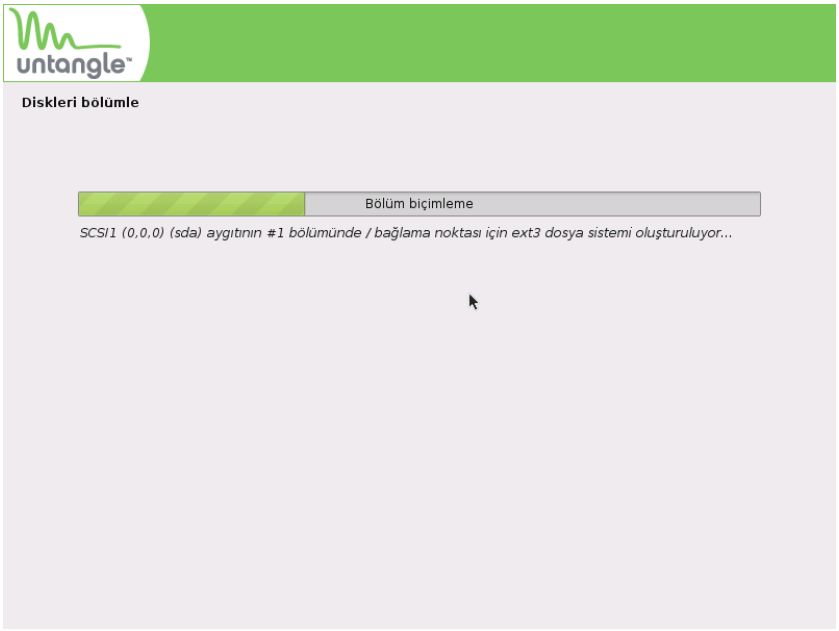
Şekil B1.6 : Kurulum bileşenleri yükleniyor beklemeliyiz.



Şekil B1.7 : Sistemimizin untangle'ın gereksinimlerini karşıladığını "ok" ifadesinden anlaşılır ve devam edilir.

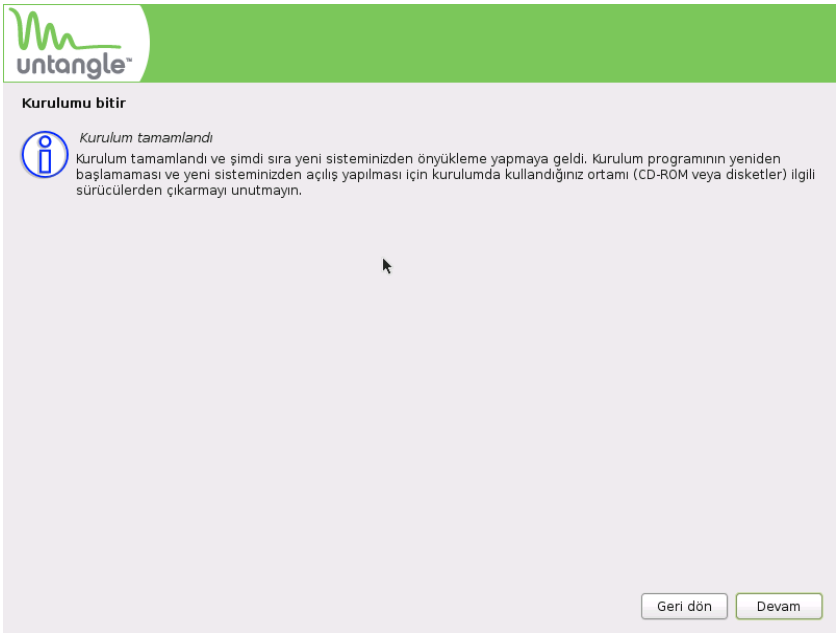


Şekil B1.8 : Bu ekran diskin formatlanacağını ve tüm verilerinizin silineceğini bildiriyor. "Evet" seçerek devam edilir.



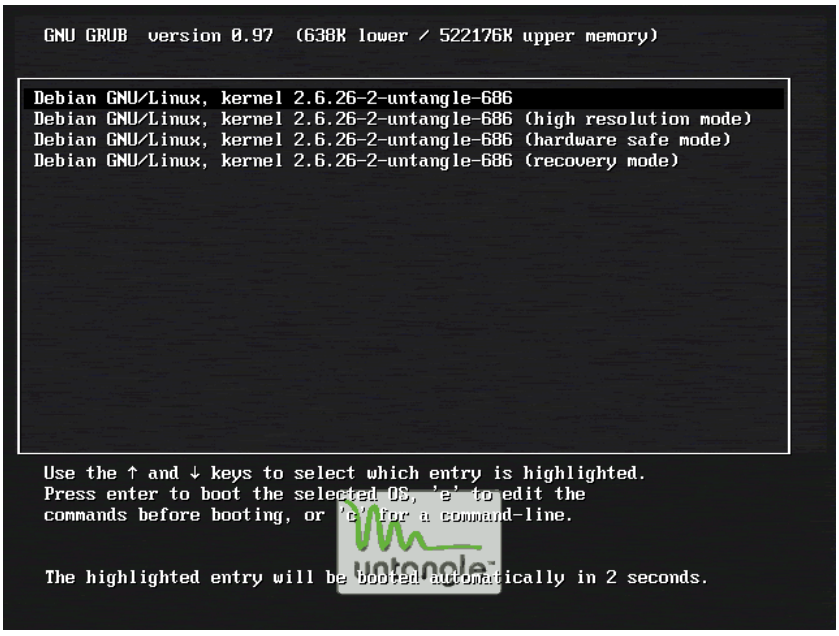
Şekil B1.9 : Untangle otomatik olarak tüm diski kullanacak şekilde biçimlendirir.

Şekil B1.10 : Temel sistem kuruluyor. Sunucunuzun performansına göre biraz zaman alabilir.

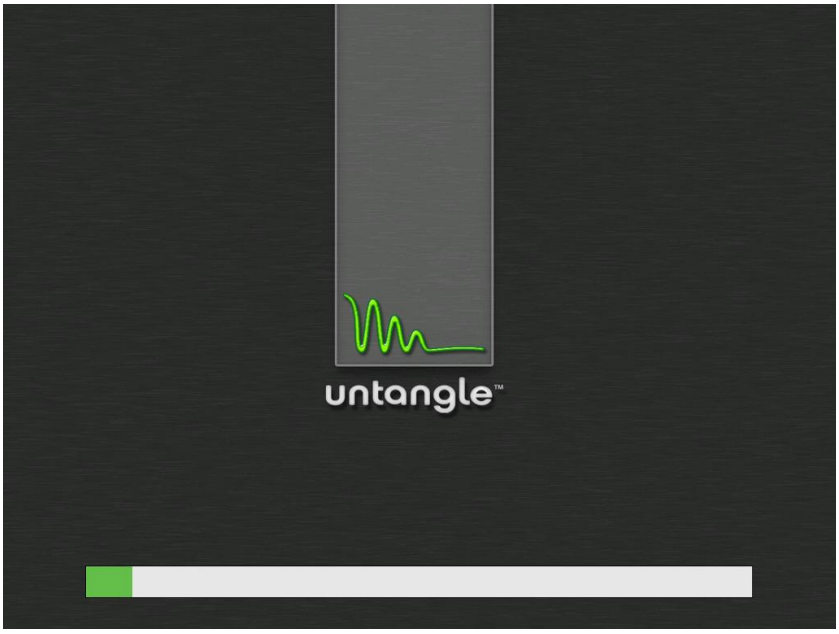


Şekil B1.11 : Untangle işletim sisteminin sunucumuza kurulumu tamamlandı.

Untangle kurulum CD sini çıkararak sunucu yeniden başlatılır.

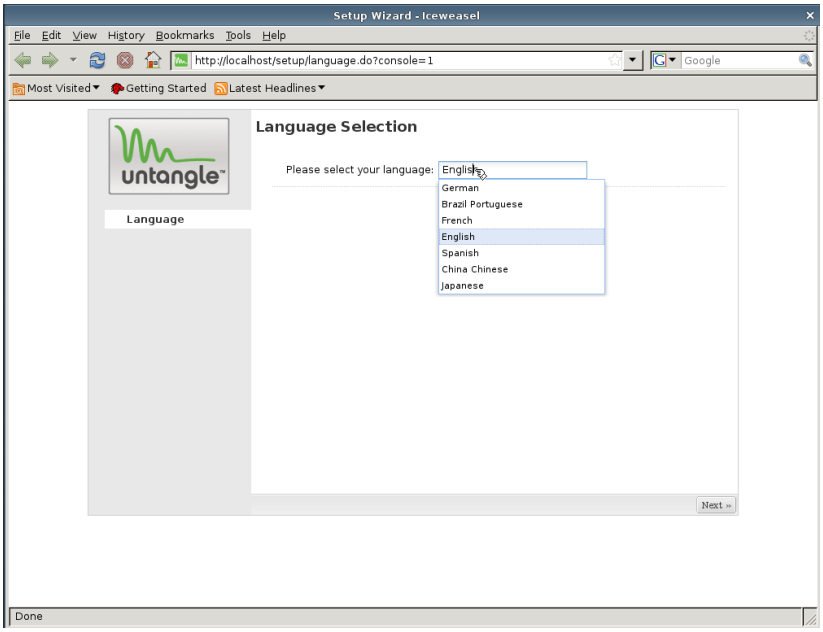


Şekil B1.12 : Sunucu yeniden başlatıldığında untangle açılış ekranı.

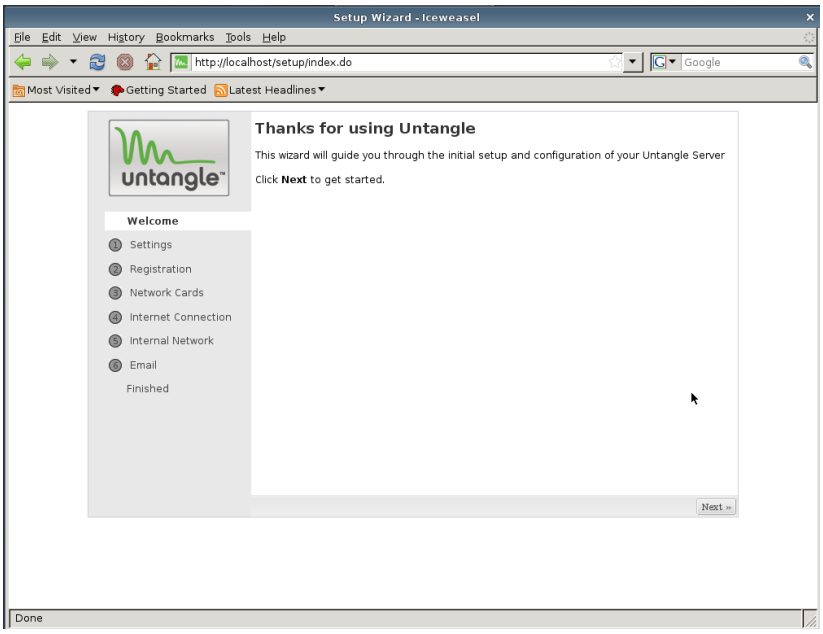


Şekil B1.13 : Yeşil çubuk ilerlerken untangle arka planda servis ve uygulamalarını çalıştırır.

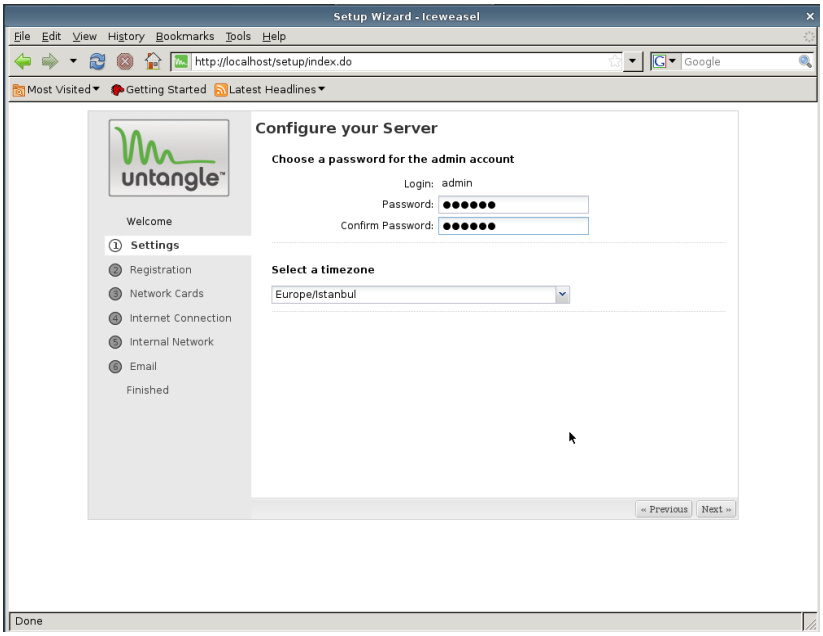
Kurulumdan sonra sistem ilk açıldığında bir takım ayarların yapılması gerekmektedir.



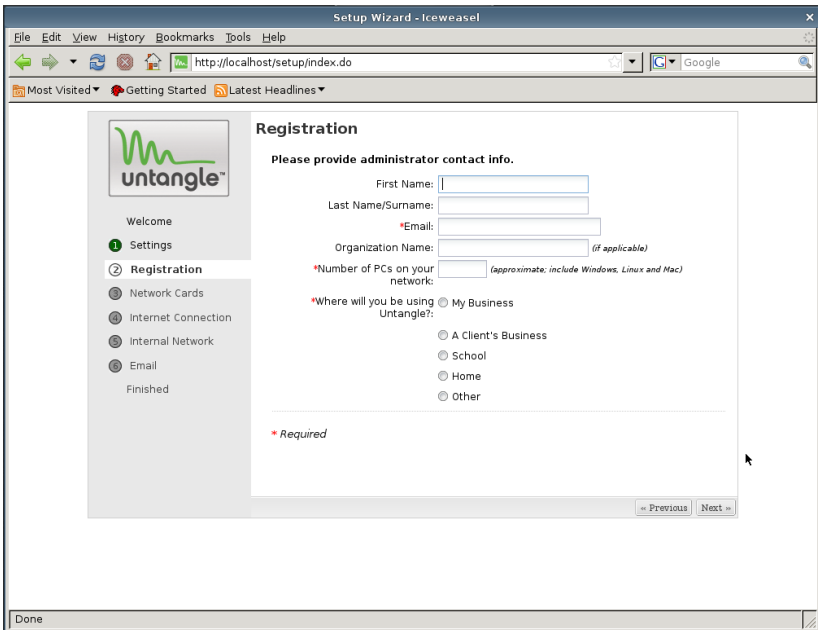
Şekil B1.14 : Untangle'ı kurarken kullanacağımız dili seçiyoruz. (Buradaki seçenekler arasında Türkçe bulunmamaktadır.)



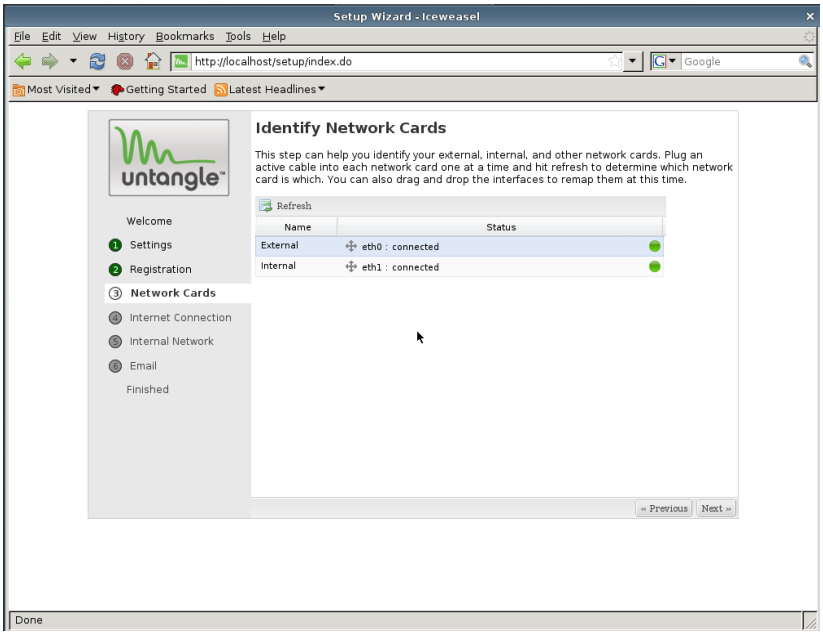
Şekil B1.15 : Untangle sunucunun başlatılması için "Next" e tıklanır.



Şekil B1.16 : Burada yönetim ekranına (web arayüz) girmek için kullanacağımız şifre ve bulunduğumuz saat dilimi belirlenir.

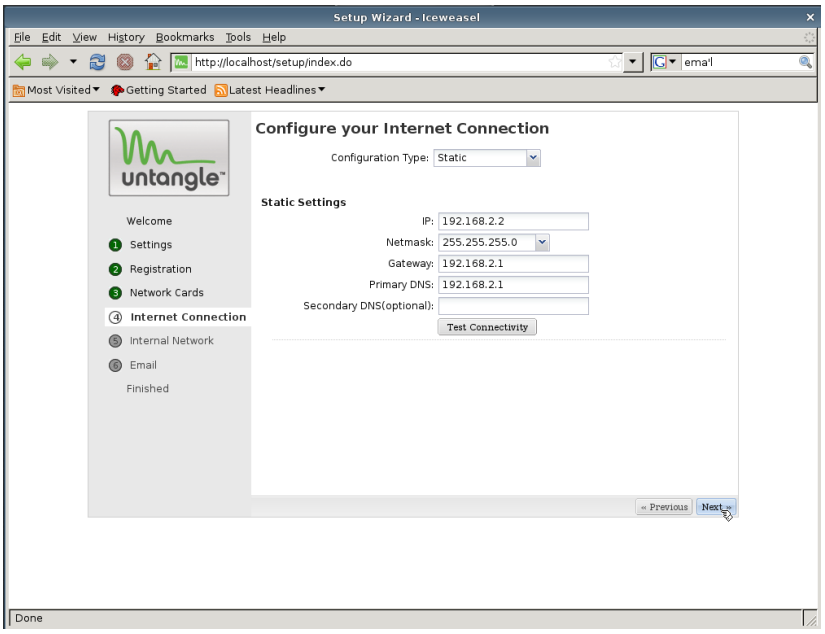


Şekil B1.17 : Kayıt işlemi gerçekleştirilerek ilerlenir.

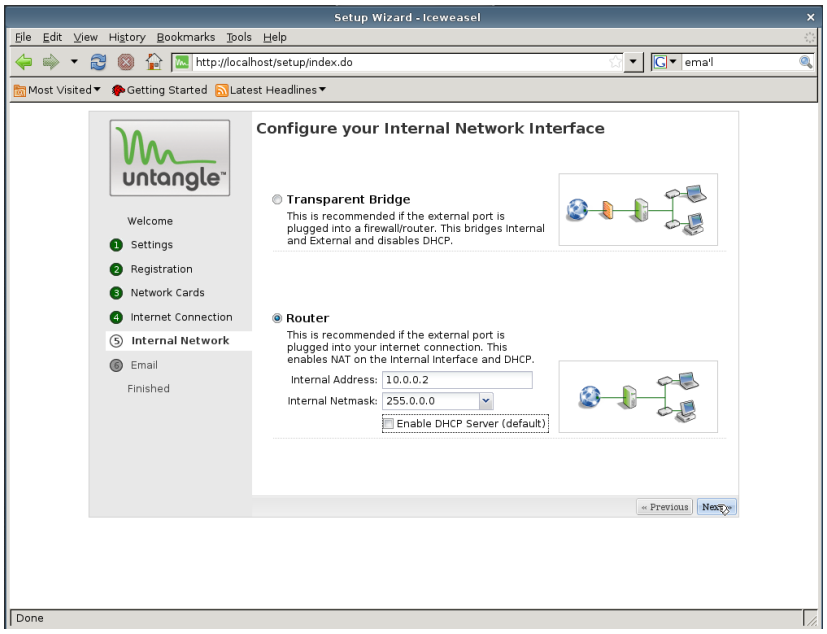


Şekil B1.18 : Untangle sistemimizde algıladığı ağ kartlarını ve durumlarını listeler.

Yeşil olmaları bağlı ve aktif olduklarını gösterir. Burada External (dış bacak) ve internal (iç bacak) ağ kartları yer değiştirilebilir. Ağ kartına bağlı ağ kablosu çıkarılıp, refresh yapıldığında yeşillerden bir gri renk olacaktır. Bu kartın hangisi olduğu bu şekilde belirlendikten sonra yer değiştirilmek istendiğinde dört yönlü ok simgesinden diğerinin üzerine sürüklediğimizde kartların görevleri değiştirilmiş olur.

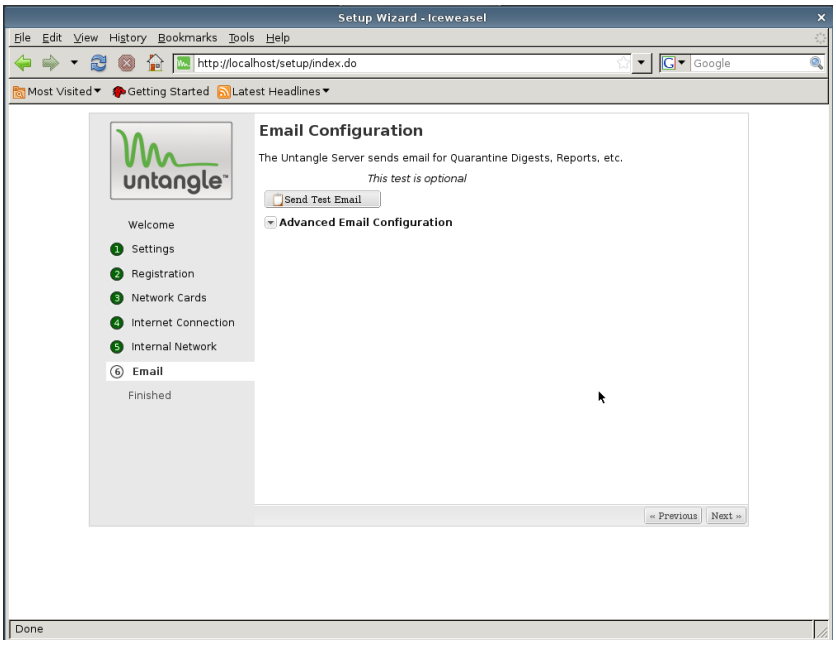


Şekil B1.19 : İnternete bağlı (External) ağ kartının IP adresi, DNS ve Ağ geçidi bilgileri burada ayarlanır.

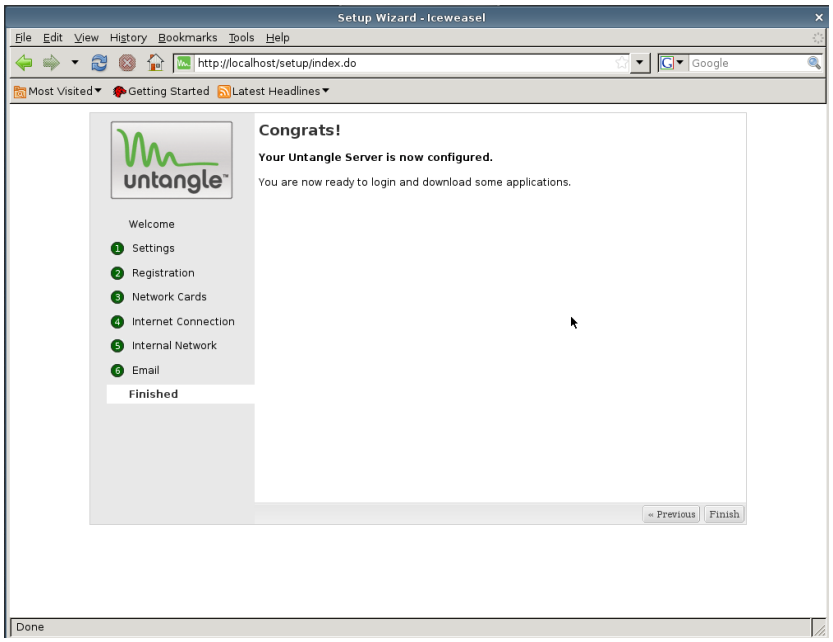


Şekil B1.20 : Untangle sunucunun yerel ağ üzerinde nasıl çalışacağı belirlenmelidir.

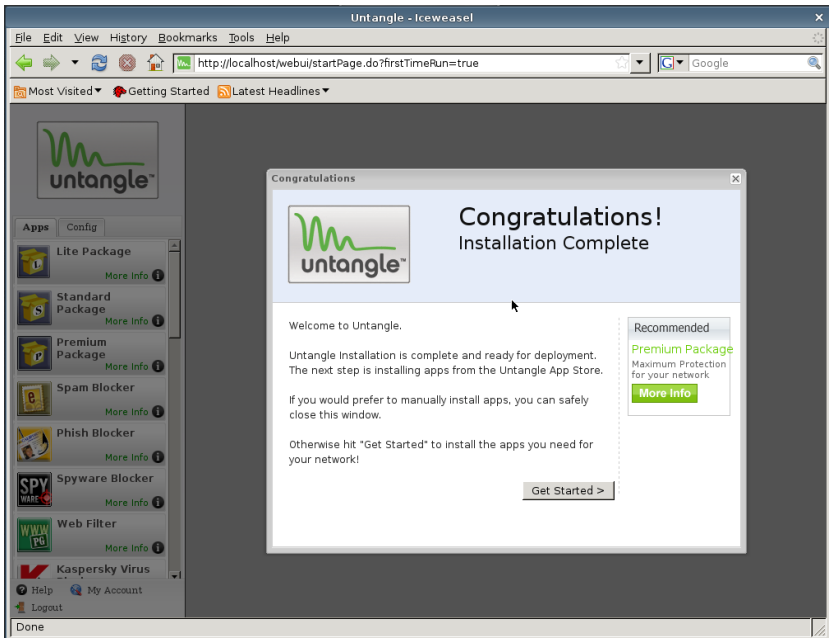
Ağımızda başka bir güvenlik duvarı (firewall) olmadığından "Router" seçeneğini seçilerek IP adresi ayarlanır.



Şekil B1.21 : Untangle'nin otomatik olarak rapor gönderebilmesi için mail sunucusu ayarlarının yapılması gerekir.

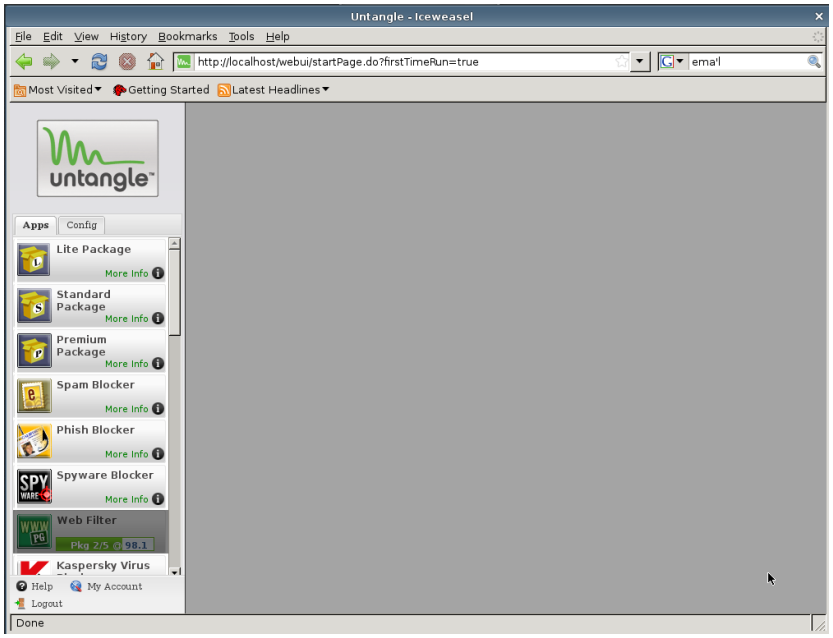


Şekil B1.22 : Tüm temel ayarlamalar tamamlandı. untangle kullanıma hazır durumdadır.



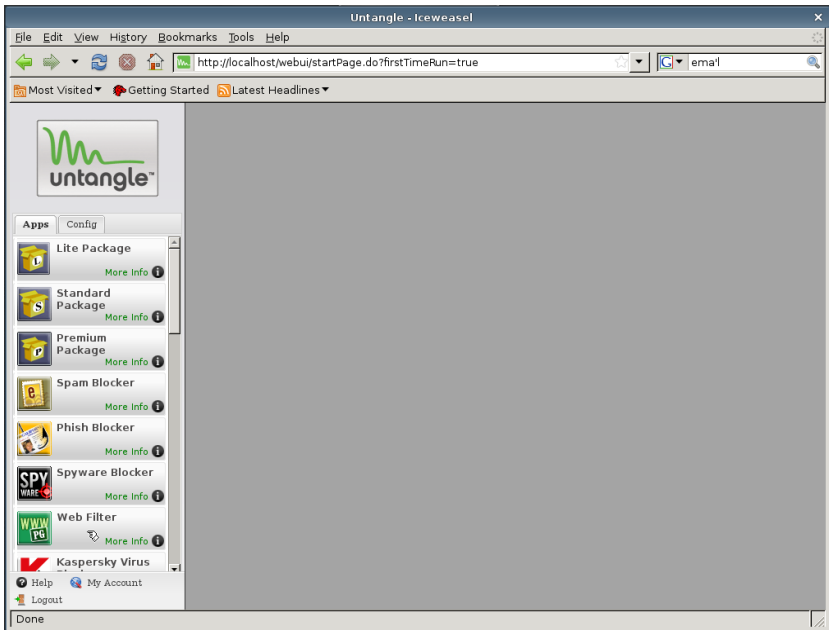
Şekil B1.23 : "Get Started" ile eklentiler planlanmaktadır.

Başlatılacak sihirbazı ile untanglenin hangi amaçlar için kullanılacağı ve mevcut ağ hakkında birkaç soru yanıtlanarak, gerekli eklentilerin kurulması sağlanılabilir. (Sihirbazı kullanmayacağız.)

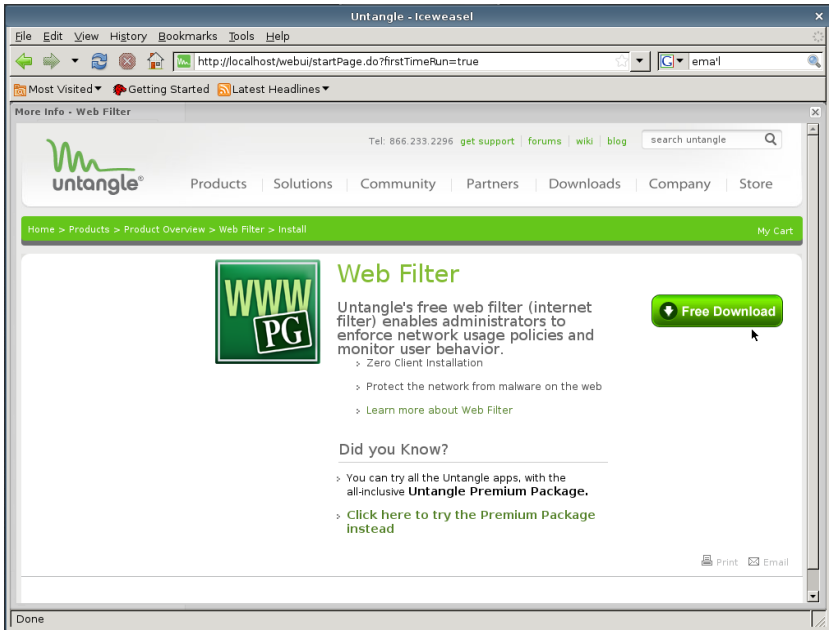


Şekil B1.24 : Artık untangle kullanıma hazır. İhtiyacımız olan eklentileri kurmalıyız.

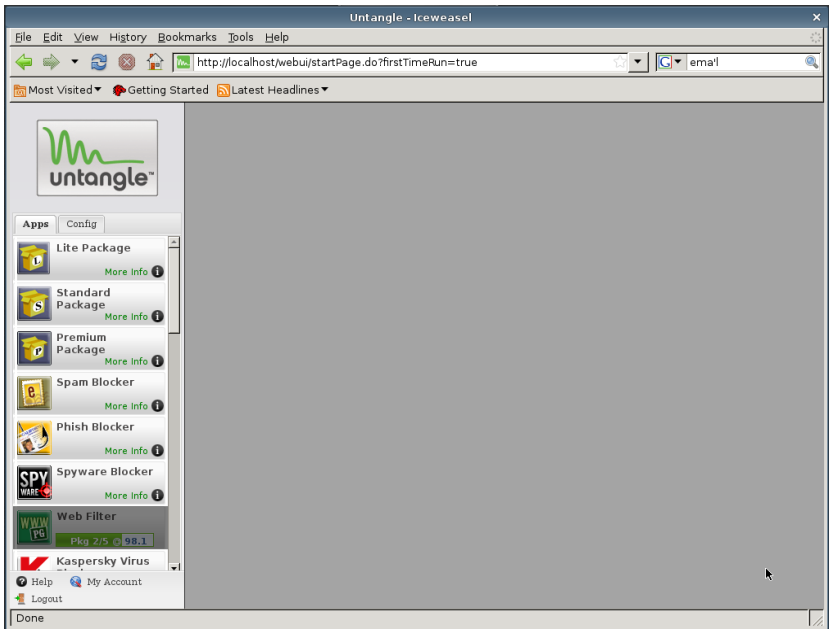
EK B2 Untangle web filter eklentisi kurulumu



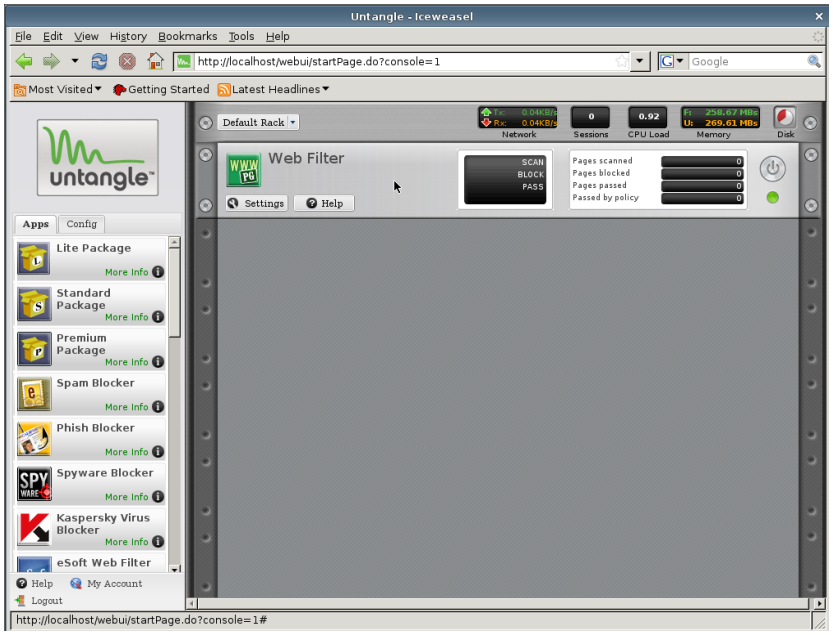
Şekil B2.1 : "Apps" menüsünden "Web Filter" eklentisi seçilerek kuruluma başlanır.



Şekil B2.2 : Eklentiye internet bağlantısı üzerinden erişilir ve sisteme indirilmeye başlanır.



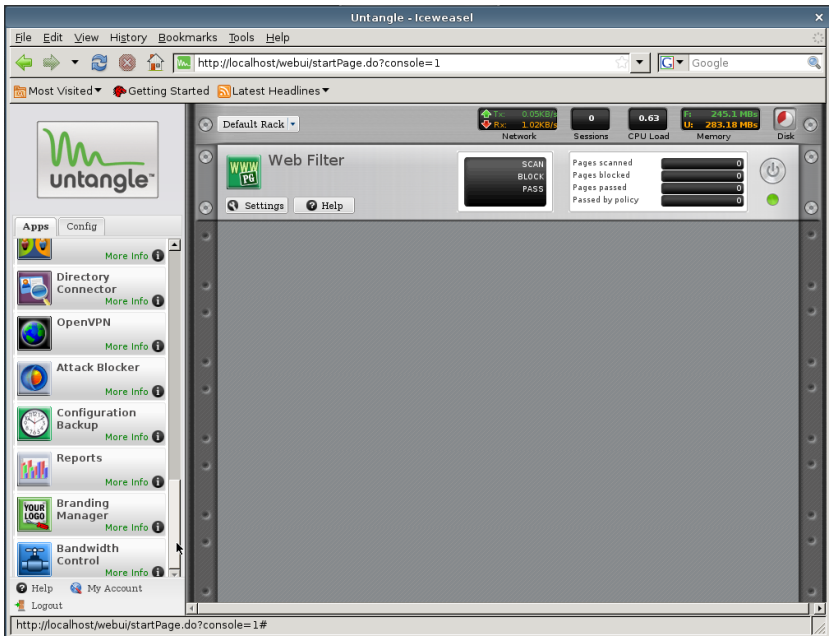
Şekil B2.3 : İndirme ve kurulum işlemlerinin safhaları yeşil çubukda görünmektedir.



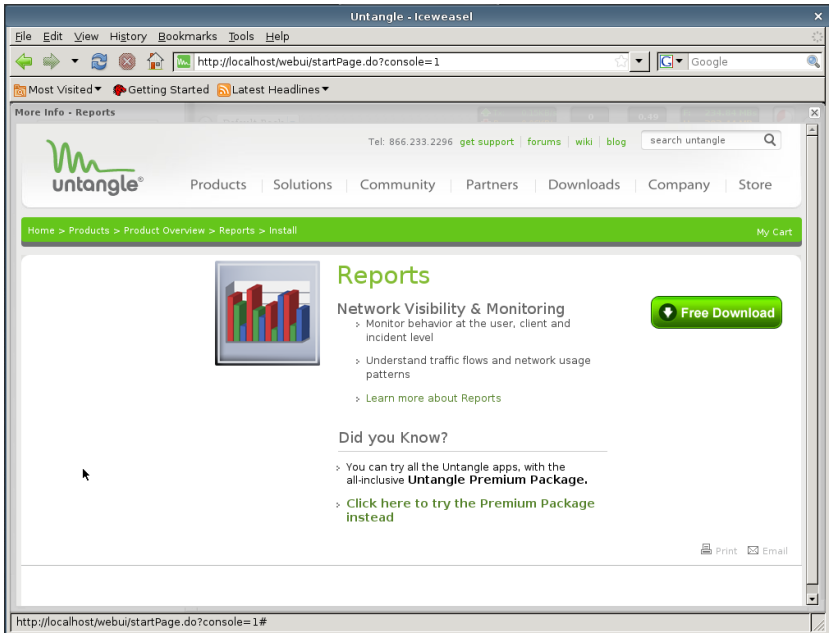
Şekil B2.4 : Web Filter başarı ile kuruldu ve çalışmaya başladı.

Web fliter ile istenilmeyen içerik barındıran web sayfaları kategori veya adres tabanlı filtrelenmektedir. Ayrıca internet erişim kayıtları da bu eklenti tarafından tutulmaktadır.

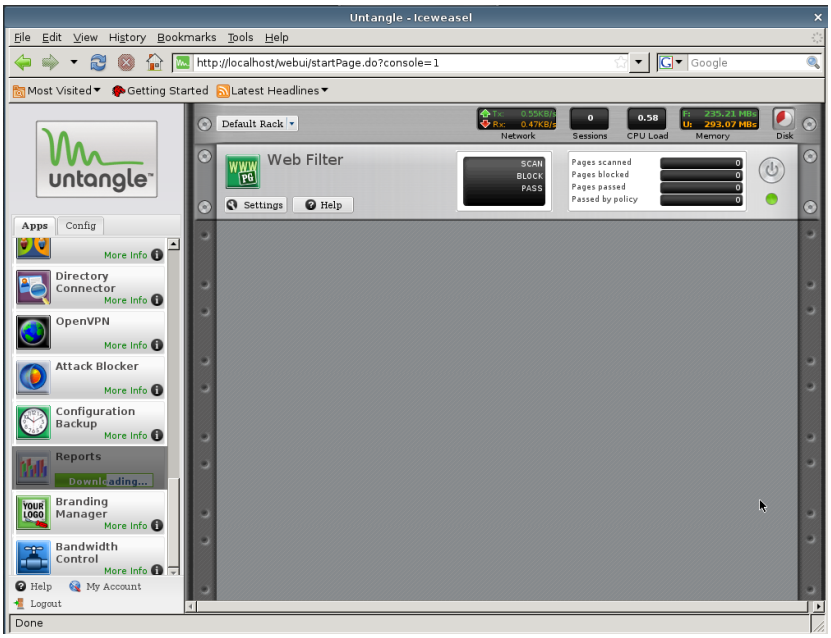
EK B3 Untangle reports eklentisi kurulumu



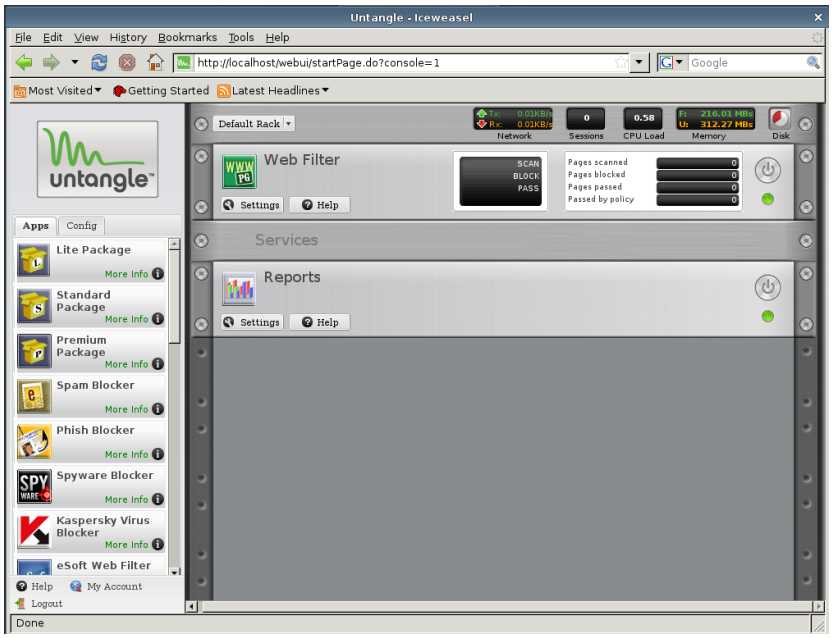
Şekil EK.B.3.1 : "Apps" menüsünden "Reports" eklentisi seçilerek kuruluma başlanır.



Şekil EK.B.3.2 : Eklentiye internet bağlantısı üzerinden erişilir ve sisteme indirilmeye başlanır.



Şekil EK.B.3.3 : İndirme ve kurulum işlemlerinin safhaları yeşil çubuk da görünmektedir.



Şekil EK.B.3.4 : Reports eklentisi başarı ile kuruldu ve çalışmaya başladı.

Geçmişe dönük internet erişim kayıtları ve daha birçok raporlamaya "Reports" eklentisinden ulaşılmaktadır.

ÖZGEÇMİŞ

Adı Soyadı: Murat Uğur ÖZÖREN

Sürekli Adresi : ŞİŞLİ E.M.L. Abide-i Hürriyet cad. No:316 Şişli / İSTANBUL

Doğum Yeri ve Yılı: İSTANBUL, 1979

e-posta: ugurozoren@yahoo.com

İlk Öğretim : 19 Mayıs İlköğretim Okulu 1985 – 1993

Orta Öğretim : Şişli Endüstri Meslek Lisesi 1993 – 1996

Lisans : Sakarya Üniversitesi – Tek.Eğitim Fakültesi – Elektronik Öğret. 1997 – 2001

Yüksek Lisans : Bahçeşehir Üniversitesi – Bilgi Teknolojileri 2009 – Devam ediyor

Enstitü Adı : Fen Bilimleri Enstitüsü

Program Adı : Bilgi Teknolojileri

Çalışma Hayatı:

- Şişli Endüstri Meslek Lisesi İSTANBUL, Öğretmen, 2007 – Devam ediyor
- Vali Kemal Nehrozoğlu İ.Ö.O. Midyat/MARDİN, Öğretmen, 2004 – 2007
- BİMTAŞ A.Ş., 2002 – 2004
- Boğaziçi Bilgisayar Sanayi ve Ticaret A.Ş., 1995-1996