



2. Hafta

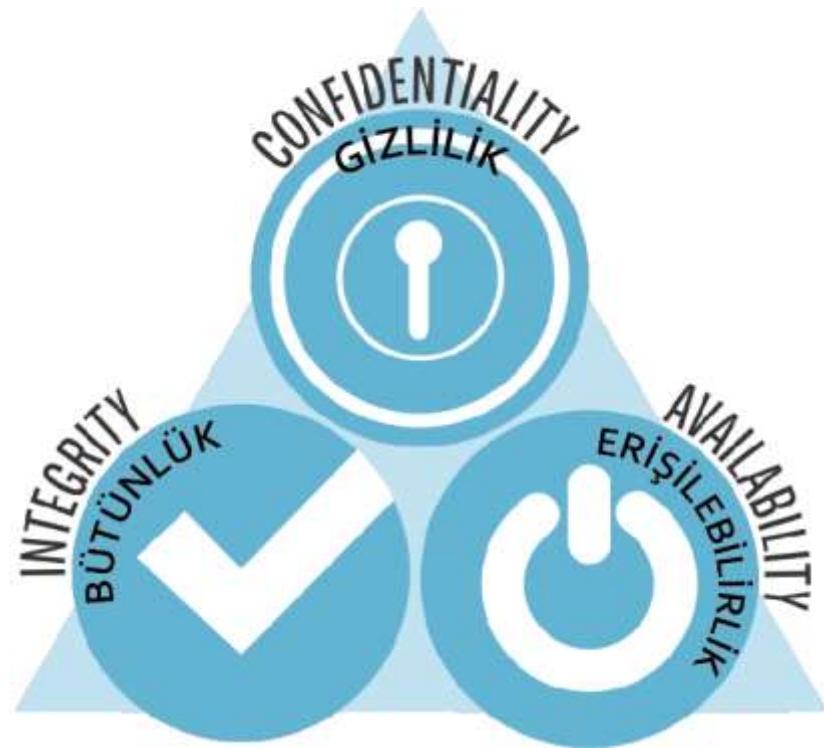
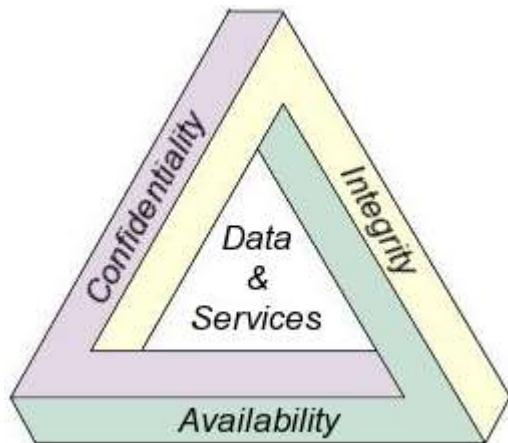
BİLGİ GÜVENLİĞİ NEDİR? SİBER GÜVENLİK NEDİR? NASIL? HACKER KİMDİR? HACKING NEDİR?

Bilgi Güvenliği

- **Bilgi:** Bir kurumun kuruluşun veya organizasyonun faaliyetlerini yürütmekte kullandıkları verilerin anlam kazanmış haline denir.
- **Bilgi Güvenliği:** Öneme sahip bilginin korunması, bütünlüğünün sağlanması, erişebilir ve ulaşabilir olmasının sağlanması için alınan gerekli, önemler ve tedbirlerdir.
- Bilgi Güvenliği Yönetim Sistemi Standardı (ISO 27001)

CIA Üçlüsü (CIA Triad)

- Confidentiality - Gizlilik
- Integrity - Bütünlük
- Availability - Erişilebilirlik
(Kullanılabilirlik)



Bilgi Güvenliği

- **Gizlilik:** Bilgilerin yetkisiz erişime karşı korunması
- **Bütünlük:** Bilgilerin eksiksiz, tam, tutarlı ve doğru olması
- **Erişilebilirlik:** Bilgilere yetkililerce ihtiyaç duyulduğunda erişilebilir olması

Bilgi Güvenliği



- **Gizlilik - Confidentiality**
Herşeyi herkesten gizlemek değil, veriye/bilgiye sadece yetkisi onların ulaşılabilmesini sağlamak. Şifreleme gibi..
- **Bütünlük - Integrity**
Yetkisiz ve izinsiz değişikliklerin engellenmesi, verinin amacına uygun derecede doğru olması.
- **Erişilebilirlik - Availability**
Veriyi iletmek, depolamak ve işlemekten sorumlu hizmetlerin devamlılığının sağlanması.
- Bilgi güvenliğinin sağlanmasından **herkes sorumludur.**
(Bilginin sahibi, kullanan, sistemi yöneten, vb..)

*Yetki **paylaşılır**, sorumluluk **paylaşılmaz**. Bilgi ise **paylaşıldıkta artar**.*

Bilgi Güvenliği Kategorileri

- **Ağ güvenliği** (Network security)
- **Uç/Son nokta** veya **Kullanıcı güvenliği** (Endpoint security)
- **Veri güvenliği** (Data security)
- **Uygulama güvenliği** (Application security)
- **Kimlik ve Erişim Yönetimi** (Identity and access management)
- **Güvenlik yönetimi** (Security management)
- **Sanallaştırma ve bulut** (Virtualization and cloud)

Bilgi Güvencesi

- Information Assurance, IA

Bilgi sistemlerinin ;

- Kullanılabilirliğini,
- Bütünlüğünü,
- Doğrulanmasını,
- Gizliliğini ve
- İnkar edememe

Özellikini sağlar. Bilgi güvenliğini de içine alır.



Siber Güvenlik

- Siber uzayda organizasyon ve kullanıcıların varlıklarını korumak amacıyla kullanılan araçlar, politikalar, güvenlik kavram ve önlemleri, kurallar, risk yönetimi yaklaşımları, eylemler, eğitimler, uygulamalar ve teknolojilerin bütünüdür.

Kaynak: Uluslararası Telekomünikasyon Birliği (ITU)

Siber Güvenlik (Cyber Security)

- Kurum, kuruluş ve kullanıcıların varlıkları, bilgi işlem donanımlarını, personeli, altyapıları, uygulamaları, hizmetleri, telekomünikasyon sistemlerini ve siber ortamda iletilen ve/veya saklanan bilgilerin tümünü kapsamaktadır.
- Siber güvenlik, kurum, kuruluş ve kullanıcıların varlıklarına ait güvenlik özelliklerinin siber ortamda bulunan güvenlik risklerine karşı koyabilecek şekilde oluşturulmasını ve idame edilmesini sağlamayı amaçlamaktadır.

Hack

- Kırmak,
- Küçük parçalar koparmak,
- Açık yönlerini ortaya çıkarmak,
- Açıklığı kullanmak.

Anlamlarında kullanılır.

Hacking

- Sistem veya programın açığından yararlanıp erişim sağlamak, değiştirmek veya silmek.
- Açıklığı kullanma işlemidir.



Hacker

- Siber korsan,
- İnternet ve ağ alt yapısı bilgisine sahip,
- Programlama dili bilen,
- Ağ veya sisteme sızmayı başarabilen,
- Verilere-bilgilere ulaşabilen,
- Tüm işlemleri fark edilmeden yapabilen,
- İleri düzey bilgiye sahip kişidir.

Hacker

- Sistemlere sizabilme yeteneğine sahip, programlama bilgisi üst düzeyde olan ağ ve sistemlerin işleyişini iyi bilen, gerektiğinde sosyal mühendislik yapabilen, hacking araçlarını tanıyan ve bunları gerektiği zaman geliştirebilen kişilerdir.

Siber Korsanlar

- Etik, kültür, etnik veya siyasi özelliklerine göre farklılar göstermektedir.
- Siyah Şapkalı Hacker,
- Gri Şapkalı Hacker,
- Beyaz Şapkalı Hacker,
- Haktivist,
- Cracker,
- Phreaker,
- Lamer,
- Script Kiddie



Hackerlar ve Şapkaları

- Amaç ve faaliyetlerine göre;
- Siyah Şapkaklı, Gri Şapkaklı ve Beyaz Şapkaklı



Siyah Şapkalı Hacker

- Kötü amaçlı, zarar vermek veya para odaklı,
- Sistemleri ele geçirmek veya yok etmek için,
- Saldırı gerçekleştiren, tehlikeli bilgisayar korsanıdır.
- Sisteme erişimi engelleme, bilgi değiştirme, gizli bilgi çalma gibi faaliyetlerde bulunurlar.



Beyaz Şapkalı Hacker

- Etik hacker,
- Aynı bilgi ve beceriye sahip, iyi niyetli,
- Açıklığı tespit eden, uyarın veya önleyen,
- Sistem güvenliğinden sorumlu personel,
- Ahlaklı siber korsandır.



Gri Şapkali Hacker

- Sistemlere sızma ve giriş yapan,
- Kötü amaç olmayıp, merak için,
- Yasallık sınırlarında saldırganlık faaliyeti olan,
- Zaman zaman tehlikeli faaliyetler içerisinde,
- Yaptıkları hukuk karşısında suç teşkil eden,
(Sisteme sızma, girme vb.) Siber korsanlardır.



Cracker

- Bilgisayar programlarının kopya korumalarını kırrarak, bu programların izinsiz olarak dağıtımına imkan veren veya bu yolda çıkar sağlayan kişilere denir. (Yazılım korsanı)
- Lisansların iptali veya serial-key temini,



Hacktivistler

- Hacker + Aktivist = Hacktivist
- Kendilerine göre, toplumsal sorun veya yanlış politik durum olarak gördükleri konulara dikkat çekmek için sistemlere saldıran kişi veya gruplardır. (sanal protestocu)
 - Wikileaks,
 - Anonymous,
 - RedHack,
 - Cyber-Warrior,
 - Ayyıldız Tim,
 - SEA vb.



Lamer

- Başkalarının önceden yazdığı betik(script) kodları veya programları çalıştırır, övünür,
- Ağ, sistem, yazılım, programlama gibi konularda bir bilgiye sahip olmadan,
- Atak yapmaya çalışan kişilerdir.

(Lamer: Özenti, basit)



Script Kiddie

- Yeterli bilgisi olmadan hazır araçlarla saldırı düzenleyen (genelde genç yaşta-çocuk) kişilere verilen isimdir. (Betikçiler-BetikKerataları)
- Tıpkı lamer'lar gibi ama bir miktar bilgi sahibi,
- Kötü niyetli, zarar verme amaçlı,
- Teknik detay ve programın nasıl çalıştığını bilmez, ama kullanımını bilenlerdir.



Phreaker

- Telefon iletişim hatlarına erişip,
- Uzun süreli Ücretsiz görüşme, vb. amaçlı,
- Telefon kırıcılarıdır.



NewBie

- Çaylak, okula yeni başlayan,
- Bilişimde veya programla da yenilere denilir,
- Betik keratalarından bir basamak üstte,
- Kendini öğrenmeye adamış bilişim korsanı adaylarıdır.



3. Hafta

İŞLETİM SİSTEMLERİ VE LINUX (KALI LINUX)

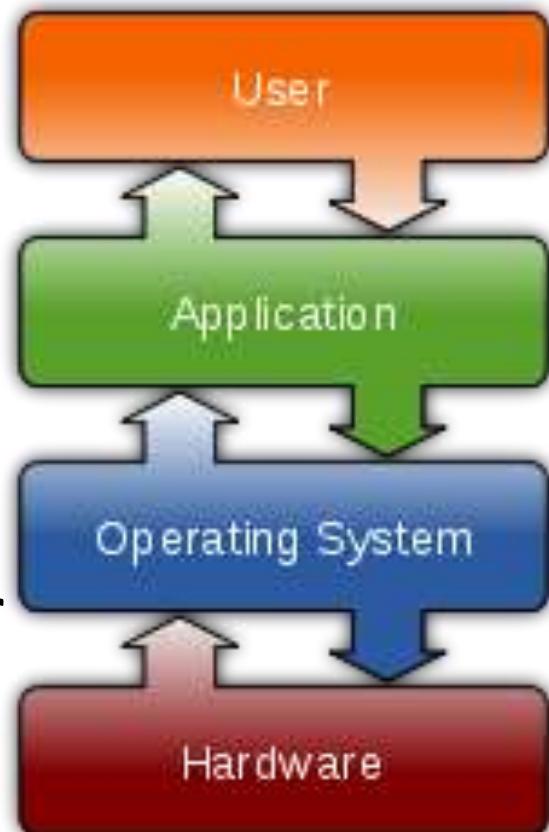


İşletim Sistemi

Operating System

Donanımın doğrudan denetimi ve yönetiminden, temel sistem işlemlerinden ve uygulama programlarını çalıştırırmaktan sorumlu olan sistem yazılımıdır.

Donanım <-> Çekirdek <-> Kabuk <-> Uygulamalar



İşletim Sistemi

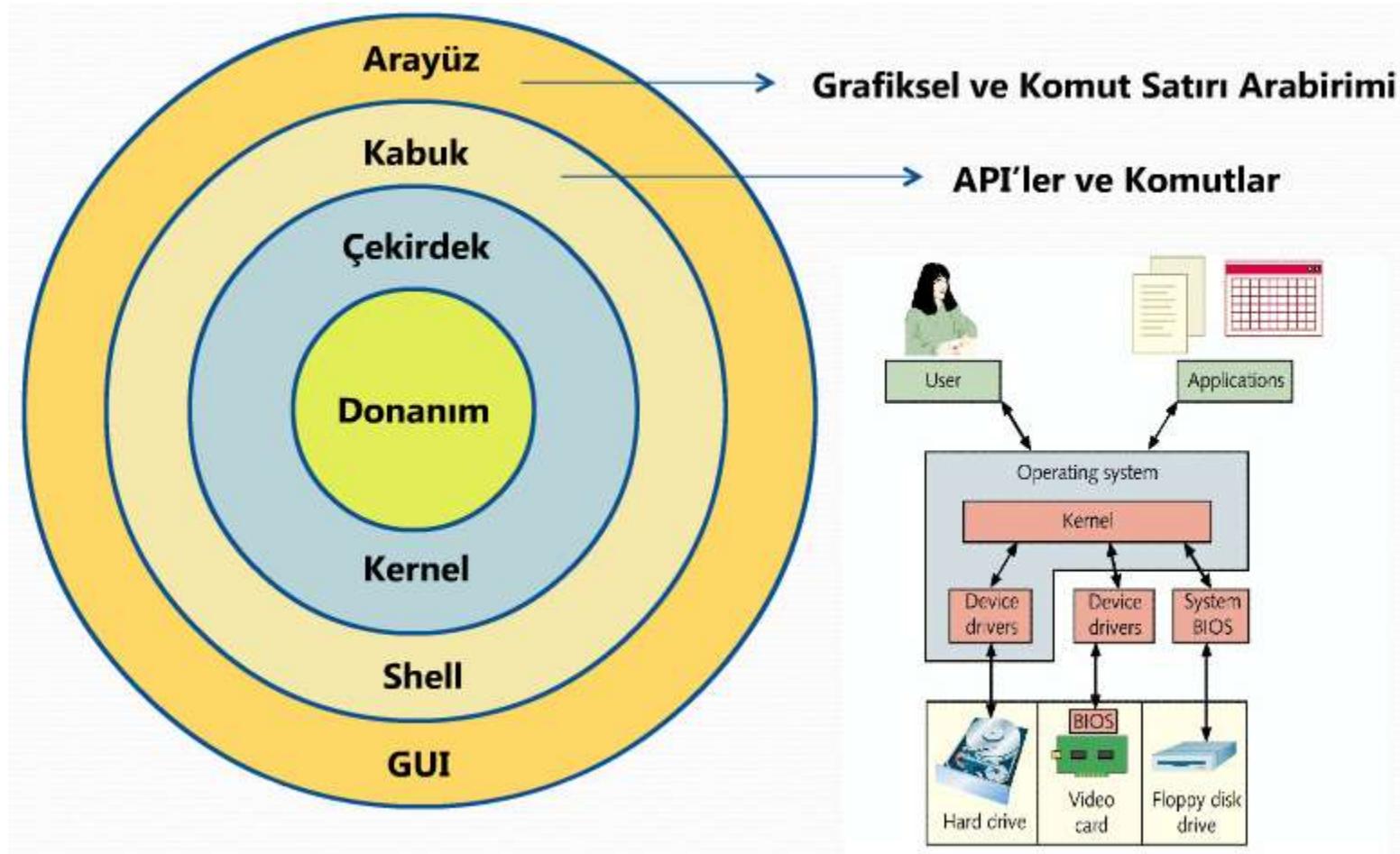
Donanım ile kullanıcı arasında bir arayüz (interface) görevini, aynı zamanda donanım ile yazılım birimlerinin etkin bir biçimde kullanılmalarını sağlayan sistem programları topluluğudur.



İşletim Sistemi Mimarileri



İşletim Sistemi Mimarileri



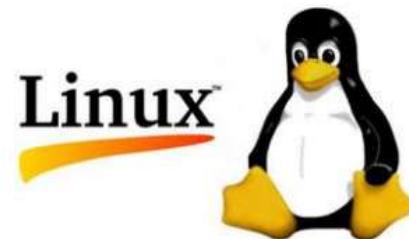
İşletim Sistemi Türleri

- Kişisel bilgisayar(PC),
- Sunucu (Server),
- Anaçatı (Mainframe),
- Çok işlemcili (Parallel computing),
- Gerçek zamanlı (Real-time),
- Gömülü (Embedded),

işletim sistemleri..

İşletim Sistemi Çeşitleri

- Unix ve çeşitleri
- Linux ve dağıtımları
- Windows ve sürümleri
- Apple OS ve IOS sürümleri
- Android ve sürümleri

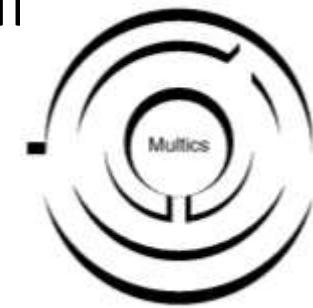


android

Unix



- 1969'da Ken Thompson ve Dennis Ritchie katılımı ile AT&T Bell Laboratuvarları'nda geliştirildi.
- Geliştirme süreci sonunda **UNIX** adını aldı
- MULTICS'in versiyonu olan PDP-7 mini bilgisayarı üzerinde UNICS'i yazdı.
- DEC PDP-7'lerde 8K bellekler ile çalıştırıldı.
- İlk olarak Assembly dilinde yazıldı.



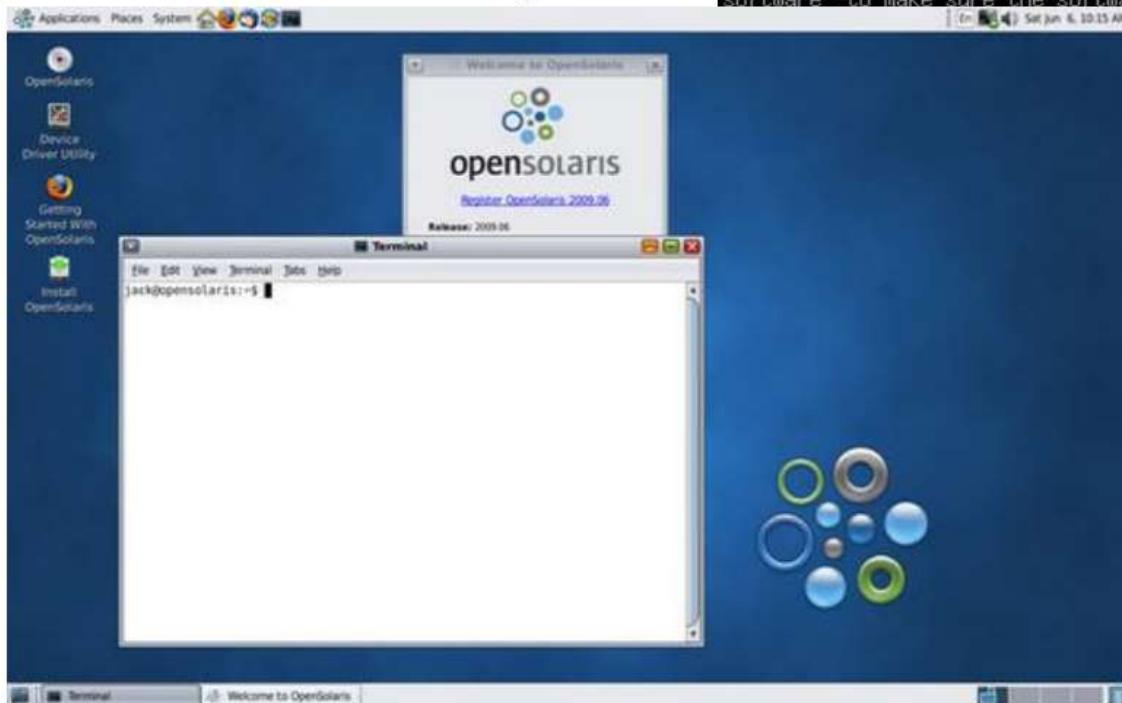
Unix

- 60'lı yılların sonunda “C” diliyle yazılmıştır.
- Çok kullanıcılı (*multiuser*) ve aynı anda birçok işi yapabilen (*multitasking*) bir işletim sistemidir.
- Komut yorumlayıcı programlar (*shell*) aracılığı ile kullanıcı ve bilgisayar sisteminin iletişimini sağlanır.
- 1980 lerde Unix ~ fiyatı 1300-1850\$..
- Pek çok Unix çeşidi vardır.
 - BSD Unix, OpenSolaris, HP-UX, AIX, SCO Unix, Sun OS...



Unix

Grafik Kullanıcı Arayüzü



```
zimos@PDP-8:~  
GNU GENERAL PUBLIC LICENSE  
Version 2, June 1991  
  
Copyright (C) 1989, 1991 Free Software Foundation, Inc.  
51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA  
Everyone is permitted to copy and distribute verbatim copies  
of this license document, but changing it is not allowed.  
  
Preamble  
  
The licenses for most software are designed to take away your  
freedom to share and change it. By contrast, the GNU General Public  
License is intended to guarantee your freedom to share and change free  
software--to make sure the software is free for all its users. This  
most of the Free Software  
other program whose authors commit to  
are Foundation software is covered by  
cense instead.) You can apply it to  
  
we are referring to freedom, not  
es are designed to make sure that you  
pies of free software (and charge for
```

Metin Tabanlı Arayüz



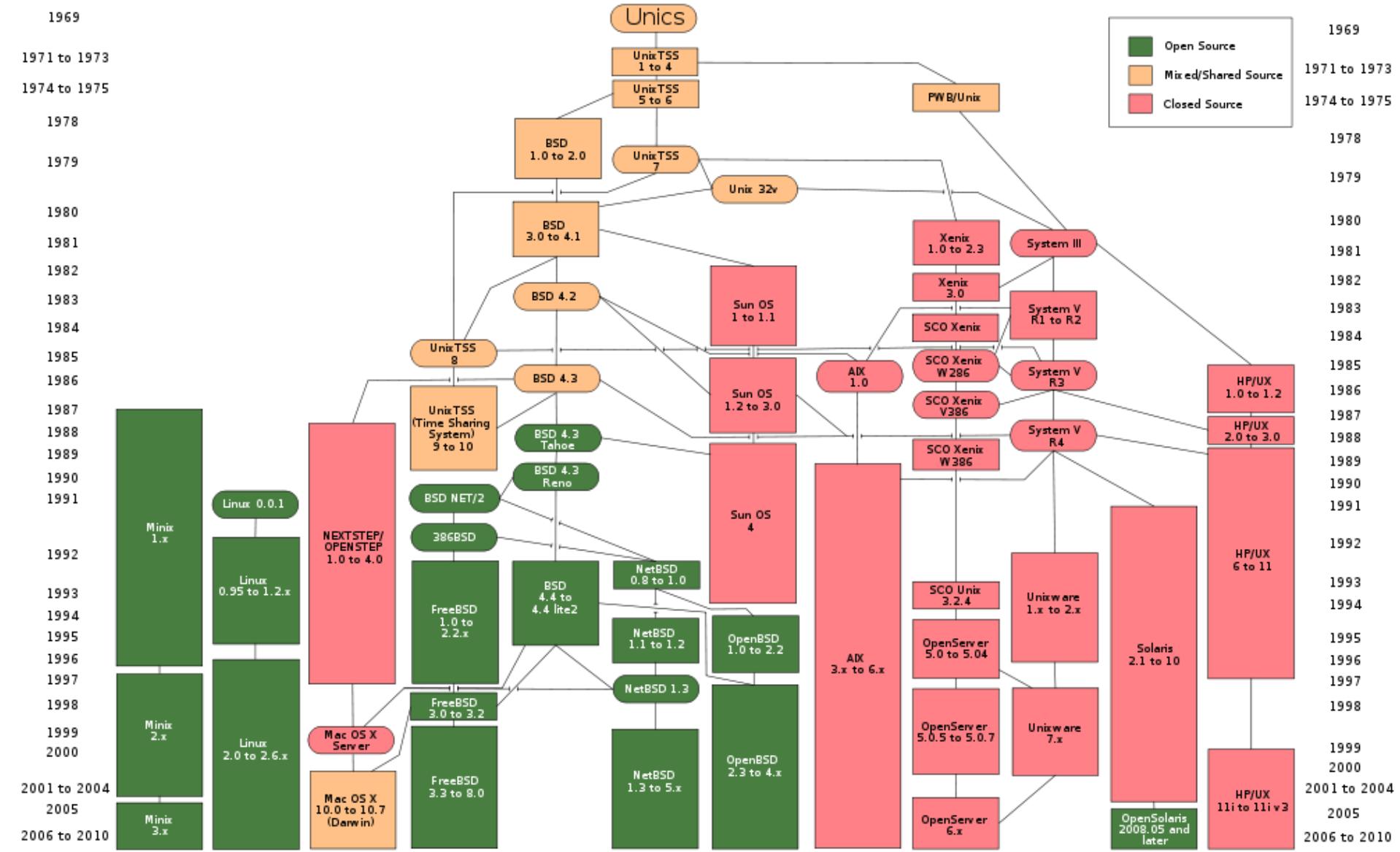
Unix



- BSD Unix
- Solaris
- OpenSolaris
- Linux
- HP-UX
- AIX
- Minix
- SCO Unix
- Sun OS
- DigitalUnix / Tru64 Unix

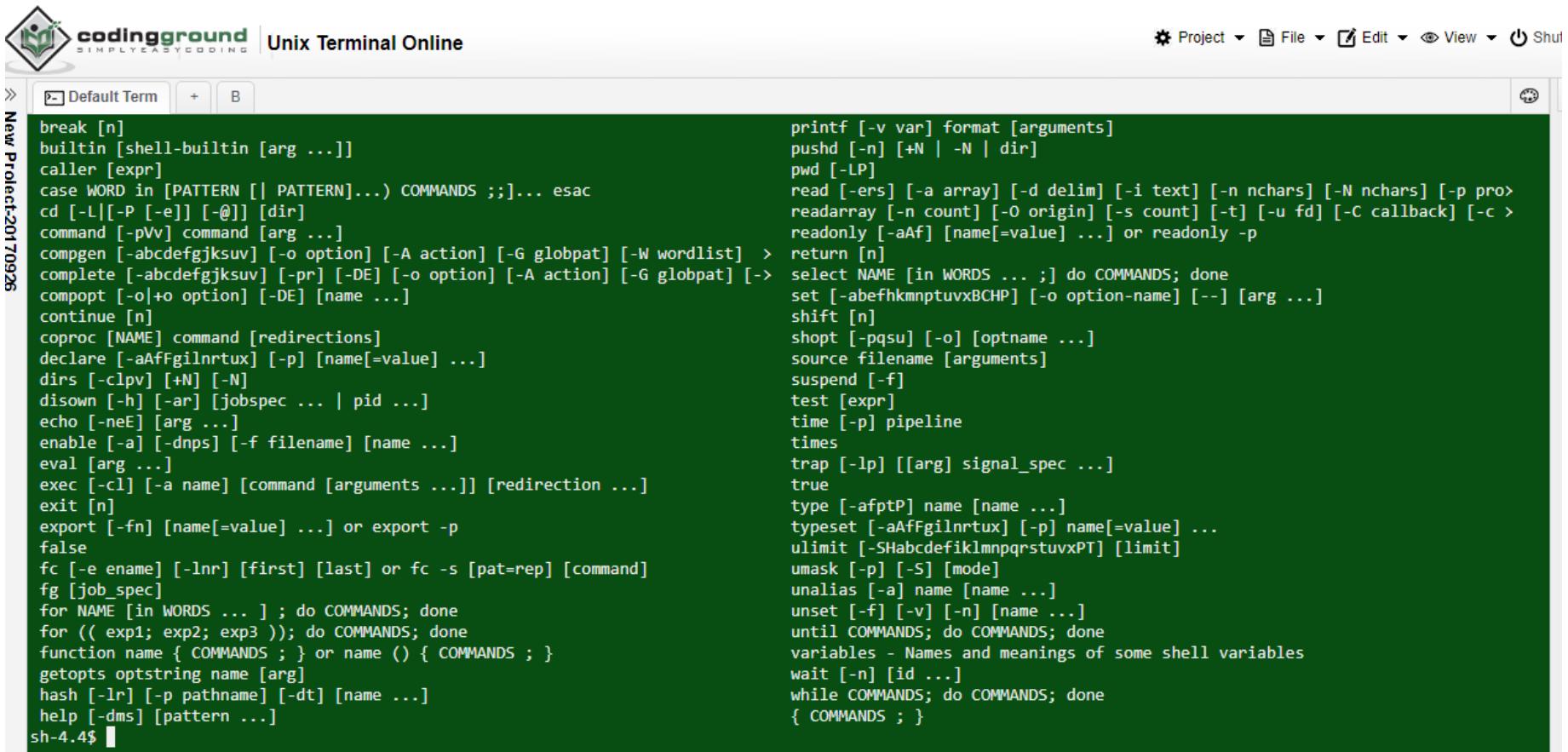


Unix



Online Unix Terminal

http://www.tutorialspoint.com/unix_terminal_online.php



The screenshot shows a web-based terminal interface from CodingGround. The top navigation bar includes links for Project, File, Edit, View, and Shutdown. On the left, there's a sidebar with a 'New Project' section showing '20170926'. The main area has tabs for 'Default Term', '+', and 'B'. The terminal window displays a large amount of shell command documentation, starting with 'break [n]' and ending with '{ COMMANDS ; }'. The text is color-coded for syntax highlighting.

```
break [n]
builtin [shell-builtin [arg ...]]
caller [expr]
case WORD in [PATTERN [| PATTERN]...] COMMANDS ;;; esac
cd [-L|[-P [-e]] [-@]] [dir]
command [-pVv] command [arg ...]
compgen [-abcdefgjksuv] [-o option] [-A action] [-G globpat] [-W wordlist] >
complete [-abcdefgjksuv] [-pr] [-DE] [-o option] [-A action] [-G globpat] [->
compopt [-o+o option] [-DE] [name ...]
continue [n]
coproc [NAME] command [redirections]
declare [-aAfFgilnrtux] [-p] [name[=value] ...]
dirs [-clpv] [+N] [-N]
disown [-h] [-ar] [jobspec ... | pid ...]
echo [-neE] [arg ...]
enable [-a] [-dnpS] [-f filename] [name ...]
eval [arg ...]
exec [-cl] [-a name] [command [arguments ...]] [redirection ...]
exit [n]
export [-fn] [name[=value] ...] or export -p
false
fc [-e ename] [-lnr] [first] [last] or fc -s [pat=rep] [command]
fg [job_spec]
for NAME [in WORDS ... ] ; do COMMANDS; done
for (( exp1; exp2; exp3 )); do COMMANDS; done
function name { COMMANDS ; } or name () { COMMANDS ; }
getopts optstring name [arg]
hash [-lr] [-p pathname] [-dt] [name ...]
help [-dms] [pattern ...]
sh-4.4$
```

```
printf [-v var] format [arguments]
pushd [-n] [+N | -N | dir]
pwd [-LP]
read [-ers] [-a array] [-d delim] [-i text] [-n nchars] [-N nchars] [-p pro>
readarray [-n count] [-O origin] [-s count] [-t] [-u fd] [-C callback] [-c >
readonly [-aAf] [name[=value] ...] or readonly -p
return [n]
select NAME [in WORDS ... ;] do COMMANDS; done
set [-abefhkmnptuvxBCHP] [-o option-name] [--] [arg ...]
shift [n]
shopt [-pqsu] [-o] [optname ...]
source filename [arguments]
suspend [-f]
test [expr]
time [-p] pipeline
times
trap [-lp] [[arg] signal_spec ...]
true
type [-afptP] name [name ...]
typeset [-aAfFgilnrtux] [-p] name[=value] ...
ulimit [-SHabcdefiklmnpqrstuvxPT] [limit]
umask [-p] [-S] [mode]
unalias [-a] name [name ...]
unset [-f] [-v] [-n] [name ...]
until COMMANDS; do COMMANDS; done
variables - Names and meanings of some shell variables
wait [-n] [id ...]
while COMMANDS; do COMMANDS; done
{ COMMANDS ; }
```



GNU - GPL

- Richard M. Stallman yazılımların koşullarını kabullenmek istemiyor..
- 1984 GNU projesini başlatıyor..
- GNU = **G**NU is **N**ot **U**nix
- 1985'de Free Software Foundation  **FREE SOFTWARE FOUNDATION** (Özgür Yazılım Vakfı) kuruluyor..
- 1991'de **G**eneral **P**ublic **L**icence (Genel Kamu Lisansı)
- Özgür ve açık kaynak kodlu..
- Kaynak kodlar üzerinde herkes istediği değişikliği yapabilir, dağıtabilir, satabilir.
- Yapılan değişikliğinde kodları paylaşılmalı..

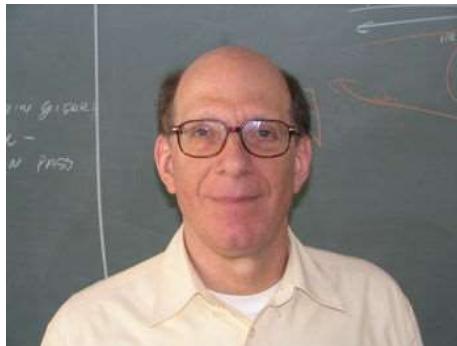


Minix

- Helsinki Üniversitesi’nde Dr.Andrew Stuart "Andy" Tanenbaum, Minix işletim sistemini geliştirmiştir.
- Öğrencilerine Unix yerine Minix üzerinde eğitim-uygulama yaptırmıştır.



HELSINGIN YLIOPISTO
HELSINGFORS UNIVERSITET
UNIVERSITY OF HELSINKI



```
Executing in 32-bit protected mode.

Building process table: pm fs rs ds tty mem log init.
Physical memory: total 263068 KB, system 5788 KB, free 197368 KB.
PCI: video memory for device at 0.15.0: 134217728 bytes
Root device name is /dev/cd0p8#8
MT-D0: multiword DMA modes supported: 0 1 2
MT-D1: little DMA modes supported: 0 1 2
MT-D9: Ultra DMA mode selected: 2
Replacing root

Multiuser startup in progress ...: is cmos.
/dev/cd0p8#8 is read-write mounted on /usr
/dev/cd0p8#1 is read-only mounted on /home
Starting services: random lance lntf printer.
Starting daemons: update cron syslogd.
Starting networking: dhcpcd named.
Alarm call
Unable to obtain an IP address.
Local packages (start): done.
/dev/rescue is read-write mounted on /boot/rescue

Minix Release 3 Version 1.2a (console)

145-116-229-112.uilenstede.casema.nl: login: _
```

Minix



Minix

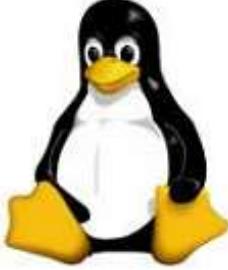
```
Executing in 32-bit protected mode.

Building process table: pm fs rs ds tty mem log init.
Physical memory: total 203060 KB, system 5700 KB, free 197360 KB.
PCI: video memory for device at 0.15.0: 134217728 bytes
Root device name is /dev/c0d0p0s0
AT-D0: Multiword DMA modes supported: 0 1 2
AT-D0: Ultra DMA modes supported: 0 1 2
AT-D0: Ultra DMA mode selected: 2
Replacing root

Multiuser startup in progress ...: is cmos.
/dev/c0d0p0s2 is read-write mounted on /usr
/dev/c0d0p0s1 is read-write mounted on /home
Starting services: random lance inet printer.
Starting daemons: update cron syslogd.
Starting networking: dhcpcd nonamed.
Alarm call
Unable to obtain an IP address.
Local packages (start): done.
/dev/rescue is read-write mounted on /boot/rescue

Minix Release 3 Version 1.2a (console)

145-116-229-112.vilenstede.casema.nl login: _
```



Linux

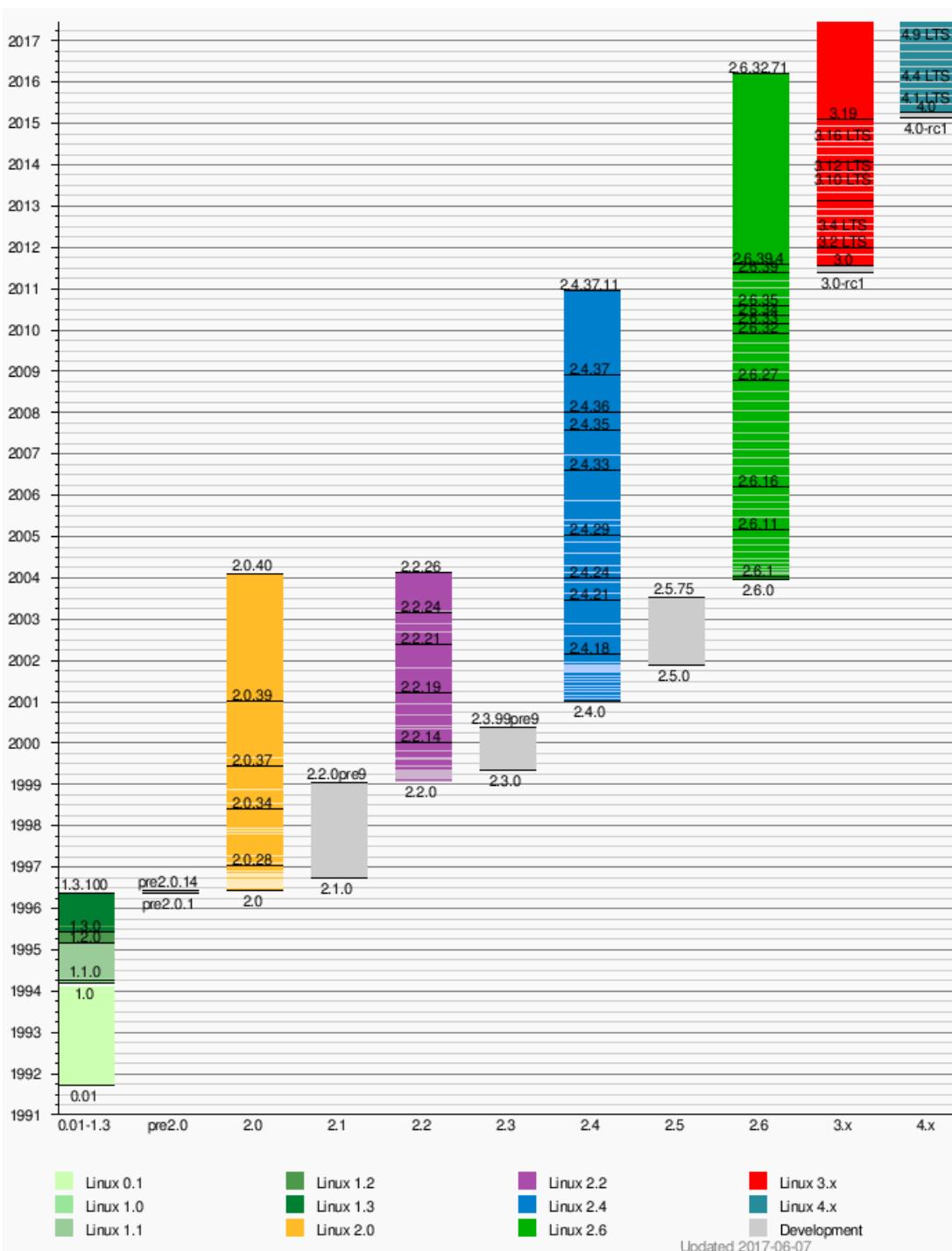
- Helsinki Üniversitesi'nde 23 yaşında, Finlandiyalı bir öğrenci,
- **Linus Torvalds,**
- Minix'ten esinlenerek Linux işletim sistemini (çekirdeği) oluşturmuştur..
- 5 Ekim 1991 – Linux 0.02 internet ve haber gruplarında yer alıyor..
- GNU-GPL Lisansı ile dağılıyor..



Linux Çekirdeği

- Multitasking
- Virtual Memory
- Protected Mode (Korumalı Mod)
- Hızlı TCP/IP
- Çoklu kullanıcı ortamı
- Modüler Yapı
- İstenilen şekilde yapılandırma yeteneği
- Modern bir işletim sistemi
çekirdeğinden beklenenek pek çok
özellik ve daha da fazlası

Linux Çekirdeği (Kernel) Zaman Çizelgesi



Açık Kaynak (Open Source)

- Kaynak kodu isteyen herkese açık olan yazılımdır.
- Kullanıcıya değiştirme özgürlüğü sağlar.



Özgür Yazılım (*Free software*)

Kullanıcısına;

- Çalıştırma,
- Kopyalama,
- Dağıtma,
- İnceleme,
- Değiştirme ve
- Geliştirme

özgürlükleri tanıyan **yazılım** türüdür.





Özgür Yazılım

- Herhangi bir amaç için yazılımı **çalıştırma** özgürlüğü (0)
- Her ne istiyorsanız onu yaptırmak için programın nasıl çalıştığını öğrenmek ve onu **değiştirme** özgürlüğü (1)
(Yazılımın kaynak koduna ulaşmak, bu iş için önkoşuldur.)
- Kopyaları **dağıtma** özgürlüğü. Böylece komşunuza yardım edebilirsiniz (2)
- Tüm toplumun yarar sağlayabileceği şekilde programı **geliştirme** ve geliştirdiklerinizi (ve genel olarak değiştirilmiş sürümlerini) **yayınlama** özgürlüğü (3).
(Kaynak koduna erişmek, bunun için bir önkoşuldur.)
- **Kaynak ve Ayrıntılar:** <https://www.gnu.org/philosophy/free-sw.tr.html>

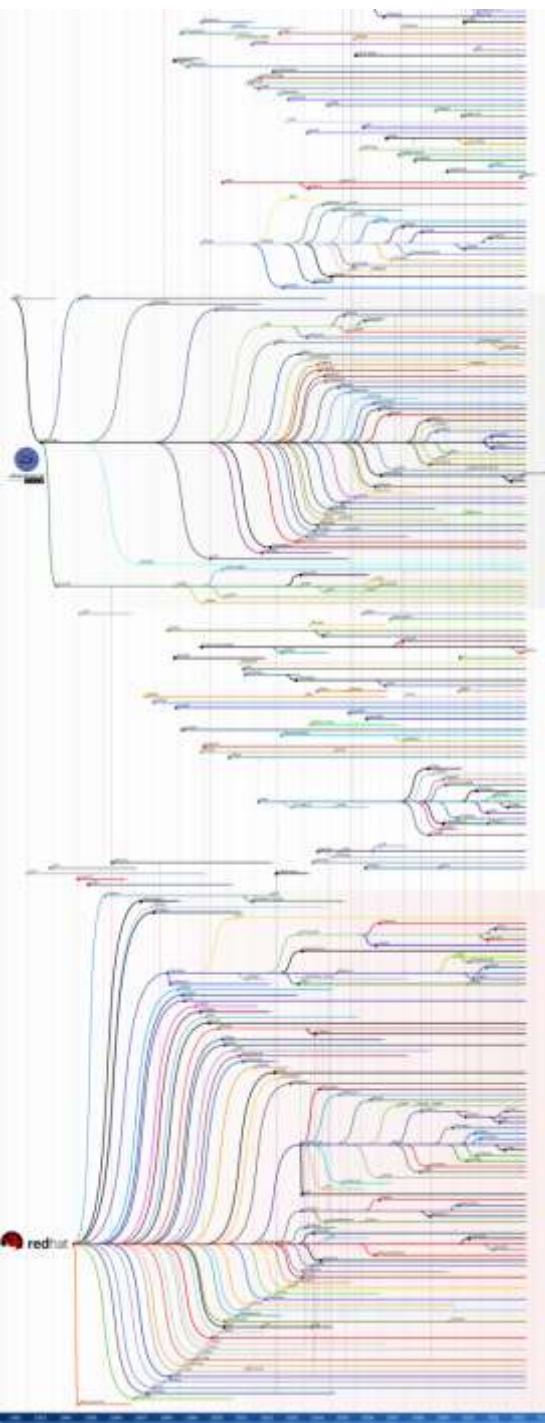
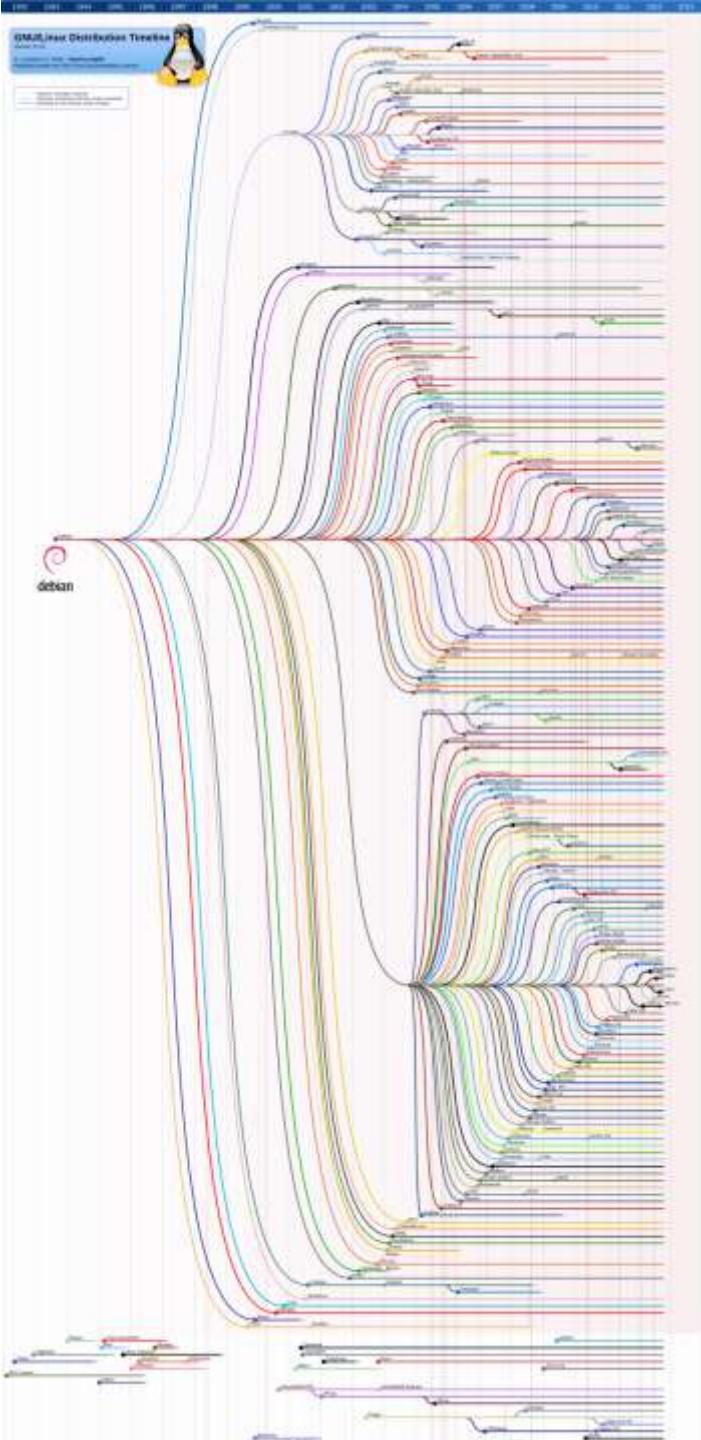
Linux Dağıtımları

- Dağıtım, bir GNU/Linux sistemini kurmayı ve yönetmeyi kolaylaştırmayı amaçlayan yazılımlar bütünüdür.



DistroWatch.com

Put the fun back into computing. Use Linux, BSD.



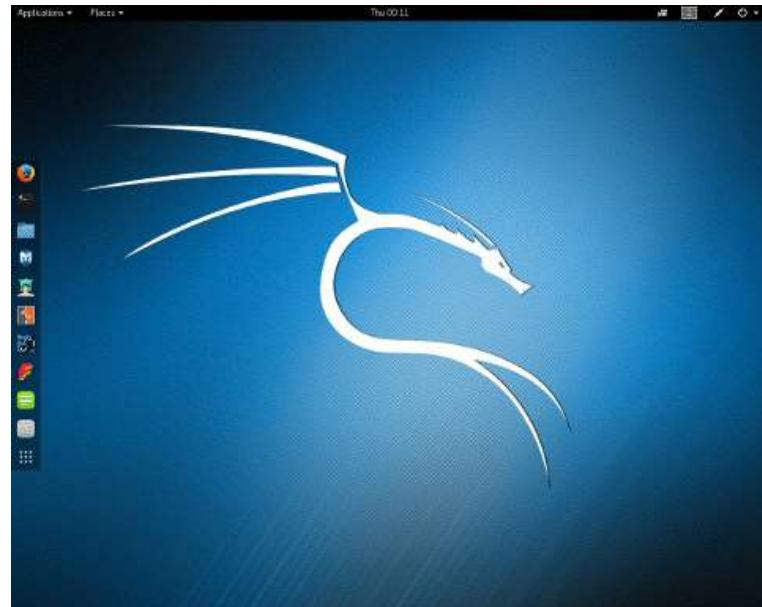
Kali Linux

- Penetrasyon Test ve Güvenlik Denetimi amaçlı bir Debian tabanlı Linux dağıtımidır.
- Offensive Security Ltd. firması tarafından geliştirilmektedir.
- 2004 yılında BackTrack ile başlayan geliştirme,
- 2013 den itibaren Debian tabanı ile yeniden geliştirilmiştir ve Kali adı verilmiştir.



Kali Linux

- Arayüz: GNOME
- Paket Yönetimi: Deb
- Site: www.kali.org
- Sürüm: 2017.2
- Platform: 32 – 64 bit
- Kurulum dosya: ISO image



Kali Linux – Applications Menüsü



Kali Linux – Uygulamalar_(Applications) Menüsü

- Information Gathering (Bilgi Toplama Araçları)
- Vulnerability Analysis (Zafiyet Tarama Araçları)
- Web Applications Analysis (Web Güvenlik Açığı Tarayıcıları)
- Database Assessment (Veritabanı Değerlendirmesi)
- Password Attacks (Şifre Atakları)
- Wireless Attacks (Kablosuz Ağ Atakları)
- Reverse Engineering (Tersine Mühendislik)
- Exploitation Tools (Sömürüm Araçları)
- Sniffing & Spoofing (Koklama ve Sahtecilik)
- Post Exploitation (Sömürüm Sonrası)
- Forensics (Adli Bilişim Araçları)
- Reporting Tools (Raporlama Araçları)
- System Service (Sistem Hizmeti)

Kali Linux - Araçlar

Information Gathering

- acccheck
- ace-voip
- Amap
- Automater
- bing-ip2hosts
- braa
- CaseFile
- CDPSnarf
- cisco-torch
- Cookie Cadger
- copy-router-config
- DMitry
- dnmap
- dnsenum
- dnsmap
- DNSRecon
- dnstracer
- dnswalk
- DotDotPwn
- enum4linux
- enumIAX
- Faraday
- Fierce
- Firewalk
- fragroute

Vulnerability Analysis

- BBQSQL
- BED
- cisco-auditing-tool
- cisco-global-exploiter
- cisco-ocs
- cisco-torch
- copy-router-config
- DBPwAudit
- Doona
- DotDotPwn
- HexorBase
- Inguma
- jSQL
- Lynis
- Nmap
- ohrwurm
- Oscanner
- Powerfuzzer
- sfuzz
- SidGuesser
- SIPArmyKnife
- sqlmap
- Sqlninja
- sqlsus
- THC-IPV6

Wireless Attacks

- Aircrack-ng
- Asleap
- Bluelog
- BlueMaho
- Bluepot
- BlueRanger
- Bluesnarfer
- Bully
- coWPAtty
- crackle
- eapmd5pass
- Fern Wifi Cracker
- Ghost Phisher
- GISKismet
- Gqrx
- gr-scan
- hostapd-wpe
- kalibrate-rtl
- KillerBee
- Kismet
- mdk3
- mfduk
- mfoc
- mfterm
- Multimon-NG

Web Applications

- [apache-users](#)
- Arachni
- BBQSQL
- BlindElephant
- Burp Suite
- CutyCapt
- DAVTest
- deblaze
- DIRB
- DirBuster
- fimap
- FunkLoad
- Gobuster
- Grabber
- jboss-autopwn
- joomscan
- jSQL
- Maltego Teeth
- PadBuster
- Paros
- Parsero
- plecost
- Powerfuzzer
- ProxyStrike
- Recon-ng

Kali Linux - Araçlar

- fragrouter
- Ghost Phisher
- GoLismero
- goofile
- hping3
- ident-user-enum
- InTrace
- iSMTP
- lbd
- Maltego Teeth
- masscan
- Metagoofil
- Miranda
- nbtscan-unixwiz
- Nmap
- ntop
- p0f
- Parsero
- Recon-ng
- SET
- smtp-user-enum
- snmp-check
- SPARTA
- sslaudit
- SSLsplit
- sslstrip
- SSLLyze
- THC-IPV6
- theHarvester

Exploitation Tools

- tnscmd10g
- unix-privesc-check
- Yersinia
- Armitage
- Backdoor Factory
- BeEF
- cisco-auditing-tool
- cisco-global-exploiter
- cisco-ocs
- cisco-torch
- Commix
- crackle
- exploitdb
- jboss-autopwn
- Linux Exploit Suggester
- Maltego Teeth
- Metasploit Framework
- RouterSploit
- SET
- ShellNoob
- sqlmap
- THC-IPV6
- Yersinia
- PixieWPS
- Reaver
- redfang
- RTLSDR Scanner
- Spooftooth
- Wifi Honey
- wifiphisher
- Wifitap
- Wifite
- Binwalk
- bulk-extractor
- Capstone
- chntpw
- Cuckoo
- dc3dd
- ddrescue
- DFF
- diStorm3
- Dumpzilla
- extundelete
- Foremost
- Galleta
- Guymager
- iPhone Backup Analyzer
- p0f
- Skipfish
- sqlmap
- Sqlninja
- sqlsus
- ua-tester
- Uniscan
- Vega
- w3af
- WebScarab
- Webshag
- WebSlayer
- WebSploit
- Wfuzz
- WPScan
- XSSer
- zaproxy

Forensics Tools

- ## Stress Testing
- DHCPig
 - FunkLoad
 - iaxflood
 - Inundator
 - inviteflood
 - ipv6-toolkit
 - mdk3
 - Reaver
 - rtpflood

Kali Linux - Araçlar

Sniffing & Spoofing

- Burp Suite
- DNSChef
- fiked
- hamster-sidejack
- HexInject
- iaxflood
- inviteflood
- iSMTP
- isr-evilgrade
- mitmproxy
- ohrwurm
- protos-sip
- rebind
- responder
- rtpbreak
- rtpinsertsound
- rtpmixsound
- sctpscan
- SIPArmyKnife
- SIPp
- SIPVicious
- SniffJoke
- SSLsplit
- sslstrip
- THC-IPV6
- VolPHopper

Password Attacks

- acccheck
- Burp Suite
- CeWL
- chntpw
- cisco-auditing-tool
- CmosPwd
- creddump
- crunch
- DBPwAudit
- findmyhash
- gpp-decrypt
- hash-identifier
- HexorBase
- THC-Hydra
- John the Ripper
- Johnny
- keimpx
- Maltego Teeth
- Maskprocessor
- multiforce
- Ncrack
- oclgausscrack
- PACK
- patator
- phrasendrescher
- polenum

Maintaining Access

- CryptCat
- Cymothoa
- dbd
- dns2tcp
- http-tunnel
- HTTPTunnel
- Intersect
- Nishang
- polenum
- PowerSploit
- pwnat
- RidEnum
- sbd
- U3-Pwn
- Webshells
- Weevily
- Winexe

Reverse Engineering

- apktool
- dex2jar
- diStorm3
- edb-debugger
- jad
- javasnoop
- JD-GUI
- OllyDbg
- smali
- Valgrind
- YARA

Reporting Tools

- CaseFile
- CutyCapt
- dos2unix
- Dradis
- KeepNote
- MagicTree
- Metagoofil
- Nipper-ng
- pipal

Hardware Hacking

- android-sdk
- apktool
- Arduino
- dex2jar
- Sakis3G

Pentest Linux Dağıtımları

- BlackArch - <https://blackarch.org>
- Parrot Security - <https://www.parrotsec.org>
- Komutan Linux - <https://www.komutan.org>
- Pentoo – <http://www.pentoo.ch>
- BackBox - <https://backbox.org>
- Bugtraq-II - <http://bugtraq-team.com>
- Cyborg Linux - <http://cyborg.ztrela.com>
- Weakerthan - <http://www.weaknetlabs.com>

Security-Forensic Linux Dağıtımları

- Parrot Security - <https://www.parrotsec.org>
- CAINE - <http://www.caine-live.net>
- Tails - <https://tails.boum.org>
- Samurai WTF - <http://www.samurai-wtf.org>
- NST - <http://www.networksecuritytoolkit.org>
- Matriux - <http://www.matriux.com>
- DEFT - <http://www.deftlinux.net>
- Kodachi - <https://www.digi77.com/linux-kodachi>
- Urix - <http://urix.us>

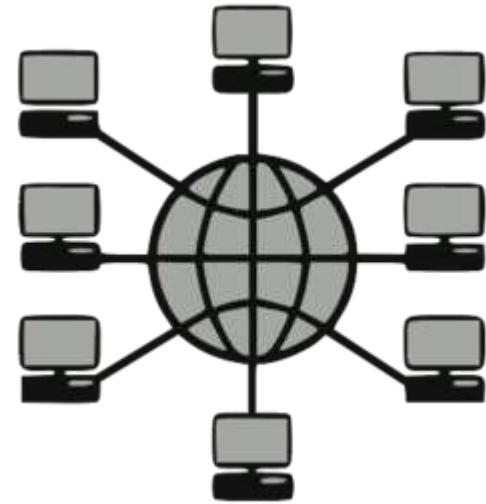
Online Linux Terminal

Linux Terminal (Üyelik)

- <http://www.webminal.org/terminal/>

Linux Terminal (JavaScript)

- <https://bellard.org/jslinux/>



4. Hafta

BİLGİSAYAR AĞLARI (NETWORK) VE SUNUCU SİSTEMLERİ

OSI Model

Open Systems Interconnection

(Açık Sistem Arabağlantısı Modeli)

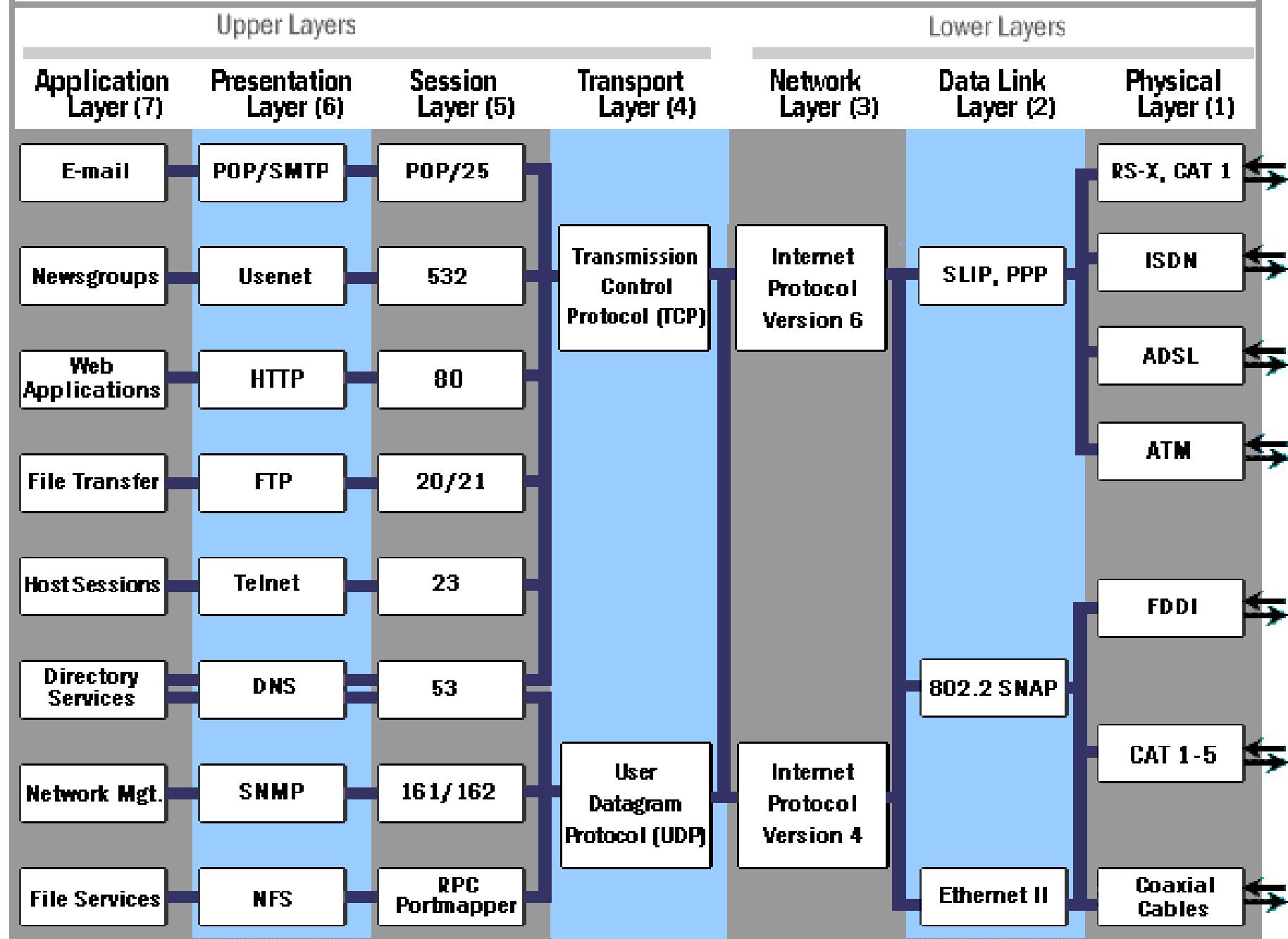
- ISO (International Organization for Standardization) (Uluslararası arası Standartlar Kuruluşu) tarafından geliştirilmiştir.

OSI Modeli

7	Uygulama Katmanı(Application Layer)	Uygulama katmanıdırular, Genellikle Yazılım ile gerçekleşirler, En üst katman kullanıcıya en yakındır.
6	Sunum Katmanı(Presentation Layer)	
5	Oturum Katmanı (Session Layer)	
4	İletim Katmanı (Transport Layer)	Veri iletim işlemlerini gerçekler.
3	Ağ Katmanı(Network Layer)	Fiziksel ve Veri iletim katmanları yazılım veya donanım ile gerçekleşir.
2	Veri Bağlantı Katmanı(Data Link Layer)	
1	Fiziksel Katman(Physical Layer)	

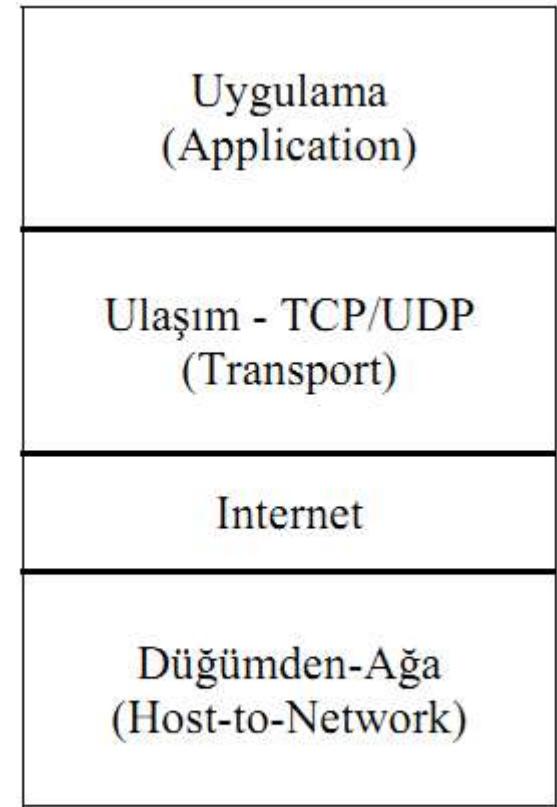
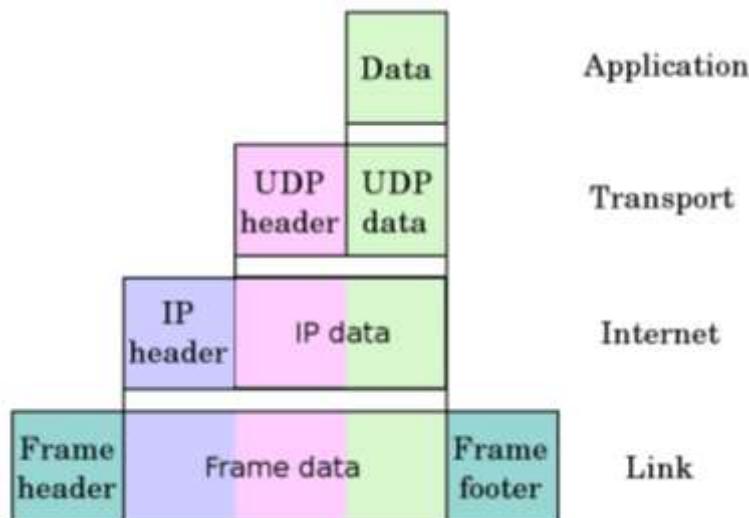
OSI Modeli	Katman	Açıklama
Uygulama	7	Uygulamalara ağ hizmetleri sağlamakla yükümlüdür
Sunum	6	Uygulama katmanı için standart bir arayüz sağlamak üzere veri biçimlerini dönüştürür
Oturum	5	Yerel ve uzak uygulama arasındaki bağlantıları oluşturur, yönetir ve sonlandırır.
Taşıma	4	Ağ üzerinde güvenilir taşıma ve akış denetimi sağlar
Ağ	3	Mantıksal adreslemeden ve yönlendirme etki alanından sorumludur
Veri Bağı	2	Fiziksel adresleme ve ortam erişim yordamları sağlar
Fiziksel	1	Aygıtlar için tüm elektriksel ve fiziksel özellikleri tanımlar

Open Systems Interconnection (OSI) Reference Model



TCP/IP Model

- TCP/IP Modeli Amerikan Savunma Bakanlığı tarafından heterojen ağlarda kesintisiz bağlantılı iletişim için geliştirilmiştir.
- 4 katmandan oluşur.

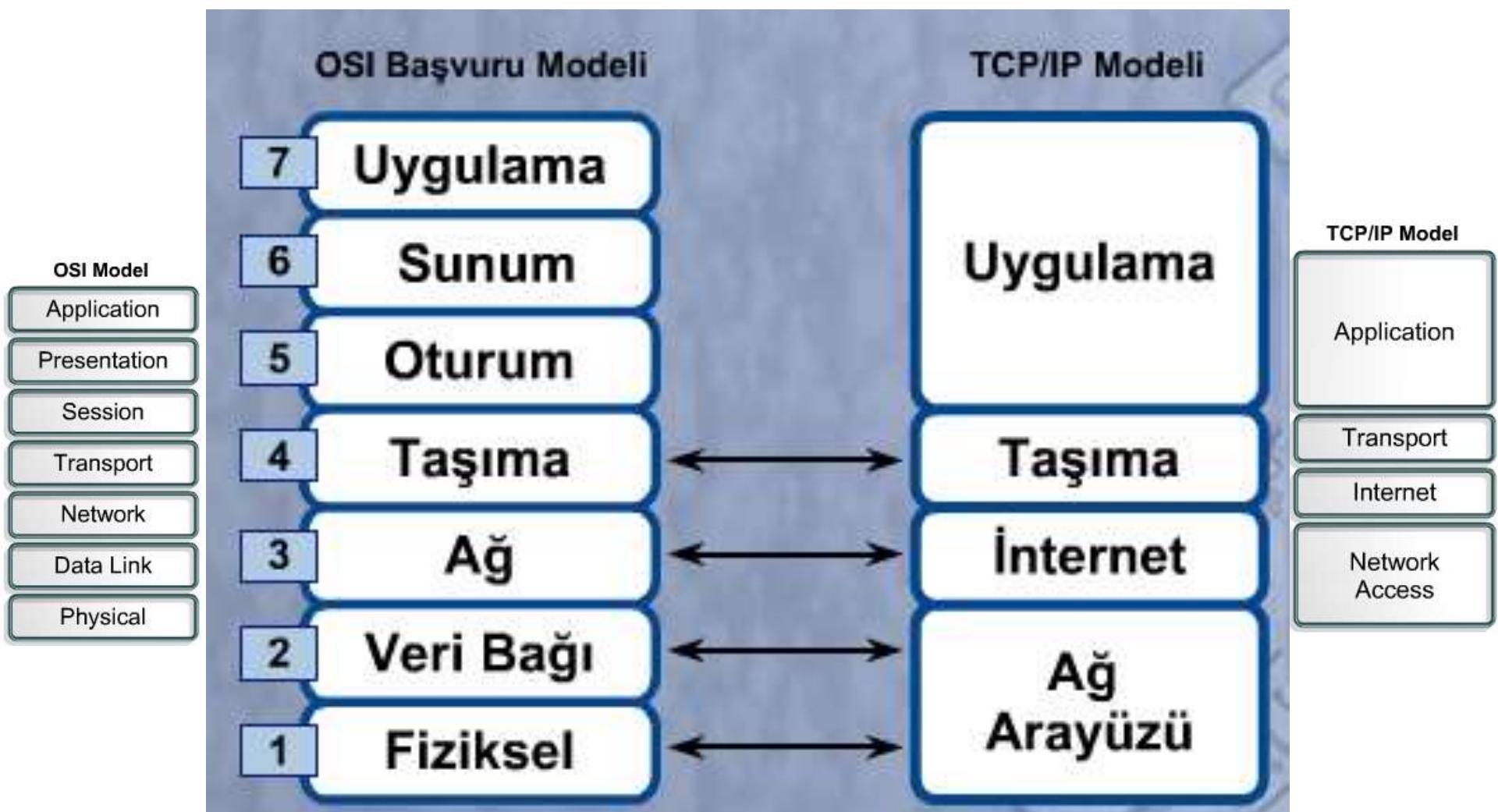


Şekil 8.4 TCP/IP Referans modeli

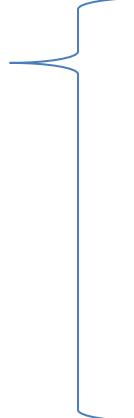
TCP/IP

Katman	Açıklama	Protokoller
Uygulama	TCP/IP uygulama protokollerini ve ana bilgisayar programlarının ağı kullanmak için taşıma katmanı hizmetleriyle nasıl bir arabirim oluşturacağını tanımlar.	HTTP, Telnet, FTP, TFTP, SNMP, DNS, SMTP, X Windows, diğer uygulama protokoller
Taşıma	Ana bilgisayarlar arasında iletişim oturumu yönetimi sağlar. Veri taşınırken kullanılan bağlantının hizmet düzeyini ve durumunu tanımlar.	TCP, UDP, RTP
Internet	Verileri IP veri birimleri olarak paketler. Bu paketler, veri birimlerini ana bilgisayarlar ve ağlar arasında iletmek için kullanılan kaynak ve hedef bilgilerini içerir. IP veri birimlerinin yönlendirilmesini gerçekleştirir.	IP, ICMP, ARP, RARP
Ağ arabirim	Koaksiyel kablo, optik fiber veya çift bükümlü bakır kablo gibi bir ağ ortamıyla doğrudan arabirim oluşturan donanım aygıtları tarafından bitlerin elektriksel olarak nasıl işaret haline getirileceği de dahil olmak üzere verilerin fiziksel olarak ağ içinden nasıl gönderileceğini belirtir.	Ethernet, Token Ring, FDDI, X.25, Frame Relay, RS-232, v.35

OSI ve TCP/IP

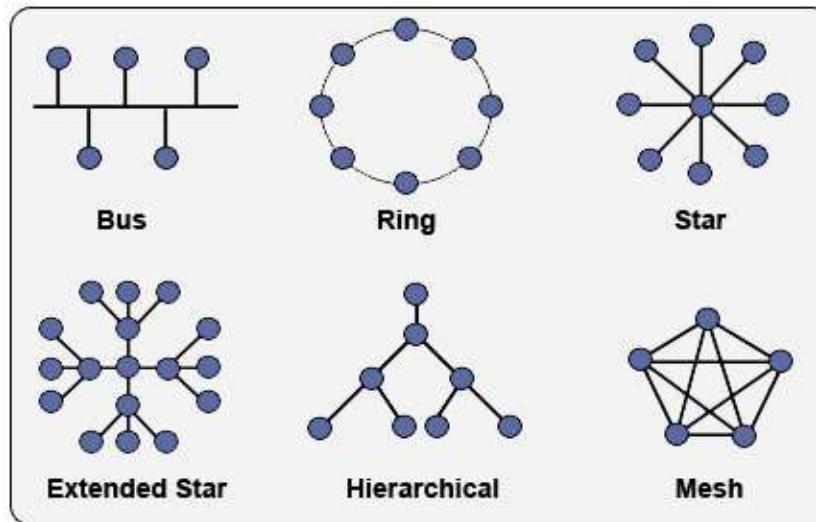


Ağın Sınıflandırılması

- Coğrafi koşullara göre;
 - LAN, MAN, WAN
 - Topolojilerine göre;
 - Bus, Ring, Star, Tree, Mesh
 - Ortamlarına göre;
 - OSI, TCP/IP
 - Ethernet, Token Ring, FDDI, ATM
 - İletim Yöntemleri;
 - Aktif (Ağ Cihazları);
 - Modem, NIC, Repeater, Hub, Switch, Router
 - Pasif (Kablolar);
 - Coaxial, UTP, STP, Fiber
- 

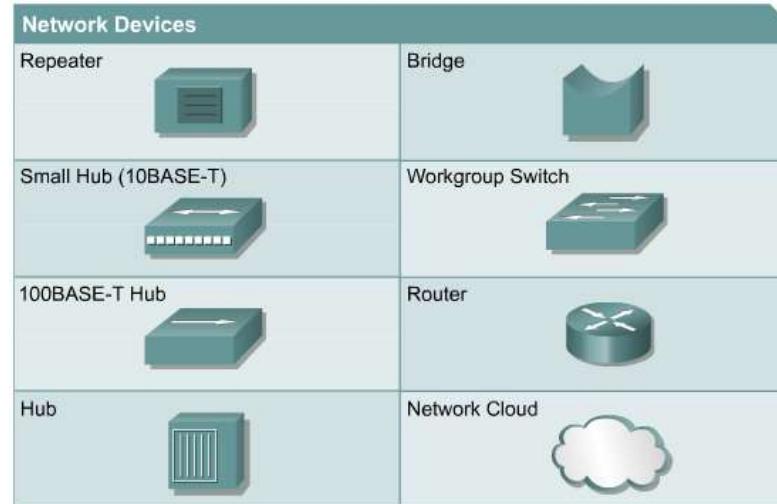
Ağ Topolojileri

- Bir ağdaki bilgisayarların nasıl yerleşeceğini, nasıl bağlanacağını, veri iletiminin nasıl olacağını belirleyen genel yapıdır.
 - Fiziksel topoloji: Ağın fiziksel olarak nasıl görüneceğini belirler (Fiziksel katman)
 - Mantıksal topoloji: Bir ağdaki veri akışının nasıl olacağını belirler (Veri iletim katmanı)



Ağ Donanımları(Cihazları)

- NIC – Network Interface Card(Ağ Arabirim Kartı)
- Repeater (Tekrarlayıcı-Yenileyici)
- Hub (Dağıtıcı)
- Switch (Anahtar)
- Bridge (Köprü)
 - Brouter (Köprü-Yönlendirici)
- Router (Yönlendirici)
- Gateway (Ağ Geçidi - Geçityolu)
- Firewall (Ateş Duvarı)



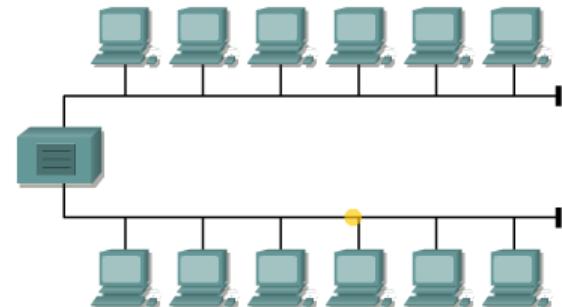
NIC – Network Interface Card (Ağ Arabirim Kartı)

- Ağ adaptörü veya ağ kartı (ethernet) kartı olarak adlandırılır.
- Sinyalleri alma gönderme işlemlerini yapar.
- Veri paketlerini parçalara ayırma birleştirme işlemlerini yapar.
- Fiziksel adrese sahiptir (MAC Adresi) 48 bittir. (16 lık)
- OSI de Fiziksel(1) ve Veri iletim(2) katmanlarında yer alır.
- Ethernet, ATM, FDDI, TokenRing, ISDN kullanılan teknolojilerdir.
- PCI, USB, PCMCIA bağlantı yuvalarına takılırlar.



Repeater(Tekrarlayıcı-Yineleyici)

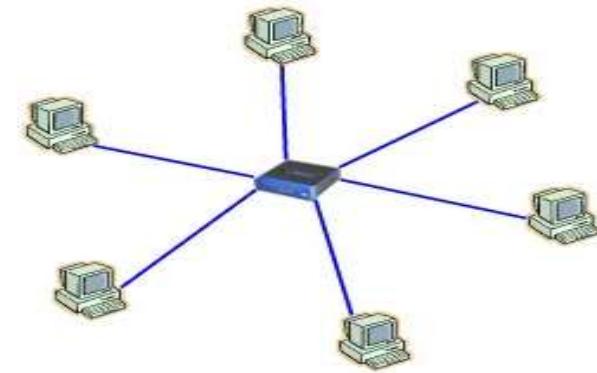
- Ağın genişletilmesinde kullanılır.
- Sinyallerin daha uzun mesafelere ulaştırılmasını sağlar.
- Farklı kablo türlerinde farklı mesafelerde kullanılır.
- Verileri sadece aktarır
- OSI de fiziksel katmanda yer alır.



The purpose of a repeater is to regenerate and retime network signals at the bit level. This allows them to travel a longer distance on the media.

Hub (Dağıtıcı)

- Kablolar ile ağ birimlerinin (bilgisayar vb.) birbirlerine bağlanmasını sağlar.
- Paylaşılan bir yol sunar.
- OSI de Fiziksel katmanda yer alır.
- Port sayısına göre,
- 10/100/1000 Mbps,
- LAN da kullanılır.
- BNC/RJ45.
- Star topoloji.

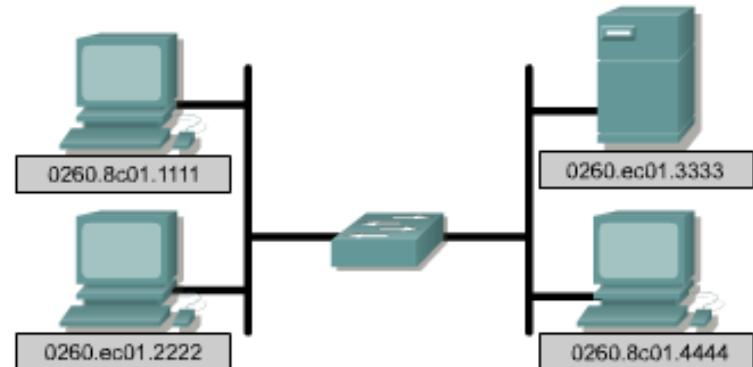


Switch (Anahtar)



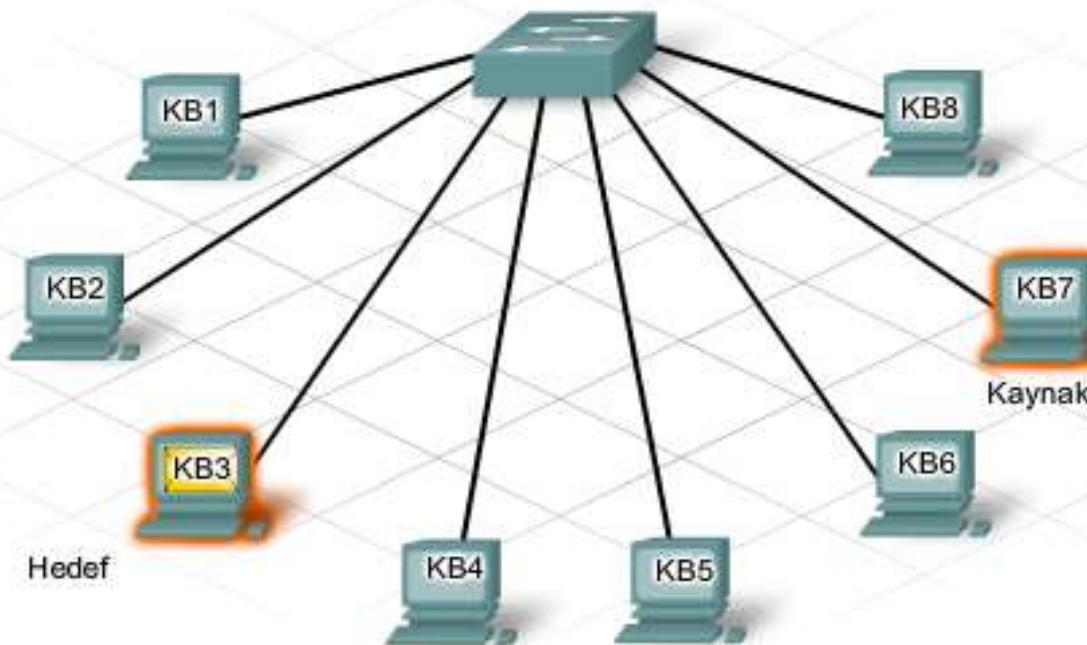
- Kendisine bağlı cihazlara anahtarlamalı bir yol sunar. 8, 12, 16, 24, 36 portlu olabilirler.
- Paket aktarımında MAC adreslerini kullanır.
- Adreslerine göre sadece iki cihazın birbirleri ile haberleşmesine olanak sağlar diğer cihazlar paket trafiginden etkilenmez.
- Diğer cihazlar kendi aralarında trafiğe devam edebilirler.
- OSI de genelde ikinci katmanda çalışırlar (bazen 3)
- Ethernet, ATM teknolojilerini kullanırlar.

Interface	MAC Address
E0	0260.8c01.1111
E0	0260.ec01.2222
E1	0260.ec01.3333
E1	0260.8c01.4444



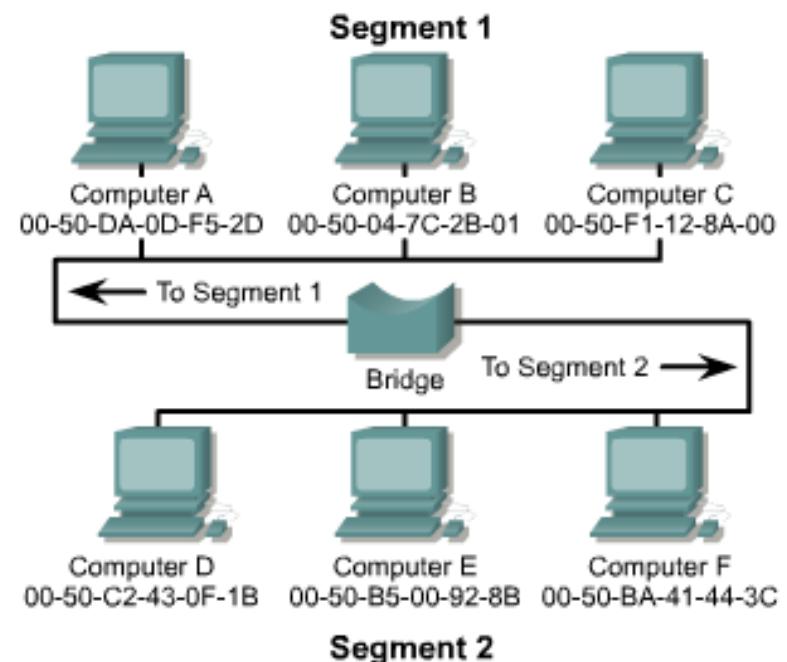
Switch MAC Tablosu

MAC Tablosu			
fa0/1	fa0/2	fa0/3	fa0/4
260d.8c01.0000	260d.8c01.1111	260d.8c01.2222	260d.8c01.3333
fa0/5	fa0/6	fa0/7	fa0/8
260d.8c01.4444	260d.8c01.5555	260d.8c01.6666	260d.8c01.7777



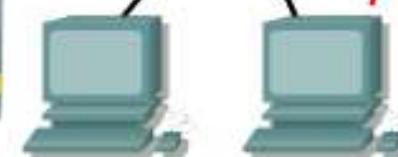
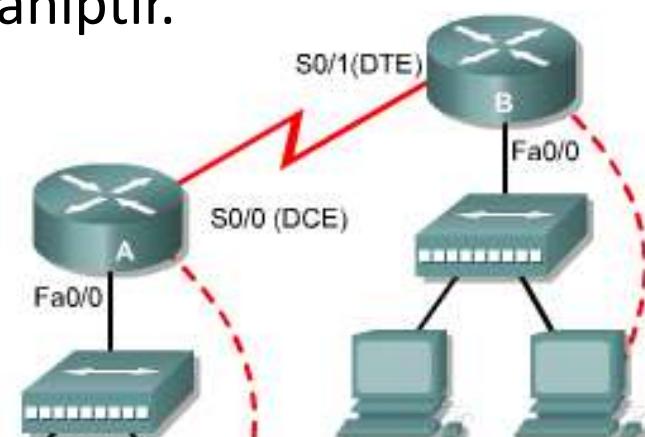
Bridge (Köprü)

- Ağları böümlere ayırmaya veya birleştirmede kullanılır. (farklı topolojide olsa)
- MAC adreslerini kullanır.
- OSI de veri iletim katmanında yer alır.
- Trafik yoğunluğunu azaltmayı sağlar.
- Kaynak, Saydam ve çevrimli yöntemleri vardır.
- 10 / 100 Mbps.



Router (Yönlendirici)

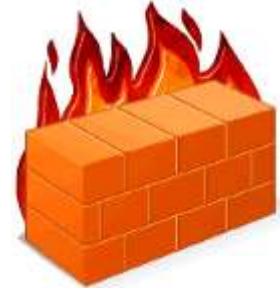
- Ağın ve paketlerin yönlendirilmesini sağlar.
- IP adreslerini kullanır. OSI de 3.katmandadır.
- En iyi yolun bulunması işlevini yapar.
- Ağlar arası haberleşme için ara bağlantı sağlar.
- LAN-LAN, LAN-MAN, LAN-WAN da işlev yapar.
- Cihaz, işlemci, ram ve işletim sistemine sahiptir.
- Yönlendirme tablosuna sahiptir.
- Konfigürasyonu yapılabilir. Kurallar vb..
- Farklı portlara (şaseler) sahiptir.
- Statik, Dinamik yönlendirme.



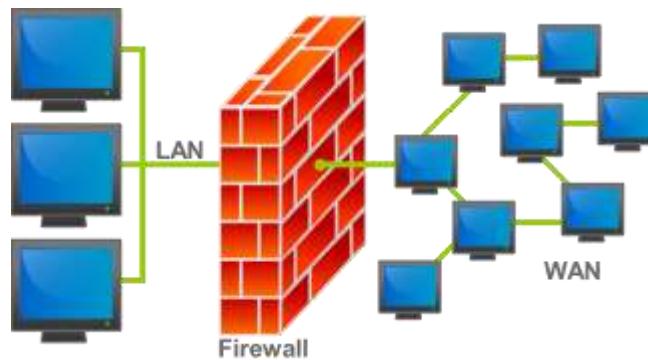
Gateway (Ağ Geçidi)

- Geçityolu olarak da adlandırılır.
- Protokol dönüşümü veya haritalama olanağı sağlayan donanım veya yazılımdır.
- Genelde Routerlar üzerinden tanımlanır.
- Farklı protokol kullanan ağlarda iki yönlü protokol dönüşümü yaparak bağlantı yapılmasını sağlar.
- OSI de tüm katmanları içerir.

Firewall(Ateş Duvarı)

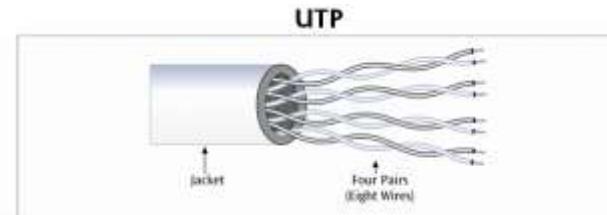
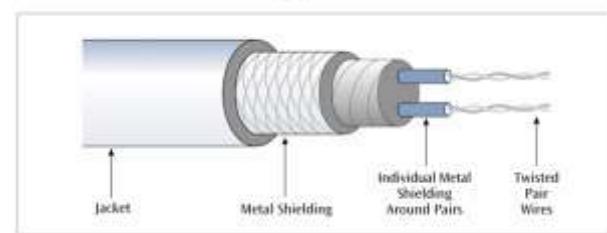


- Ağ erişimine ilişkin içерden veya dışarıdan yetkisiz her erişime engel olmak için veya paketleri süzmek için kullanılan güvenlik amaçlı donanım veya yazılımdır.
- Kurallar tanımlanır. IP ler tanımlanır.
- Portlar kullanılır. Servislere erişim ayarlanır.
- Genelde izin ver veya yasakla prensibine göre çalışır.



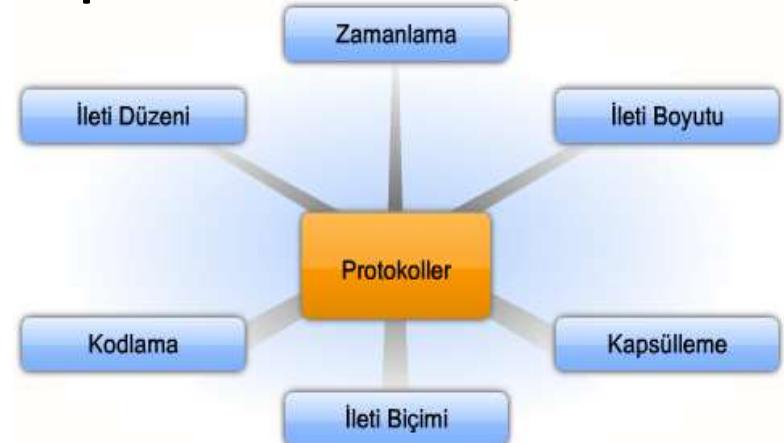
Kablolama Sınıflamaları

- Coaxial (Koaksiyel – Eş eksenli) [BNC]
 - Thin (thinnet) (İnce)
 - Thick (thicknet) (Kalın)
- Twisted-Pair (Çift-bükümlü) [RJ45]
 - STP (Korumalı Çift-bükümlü)
 - UTP (Korumasız Çift-bükümlü)
 - Straight-through (Düz)
 - Cross-over (Ters)
 - Rollover ()
- Fiber-Optik [ST /SC / MT-RJ]



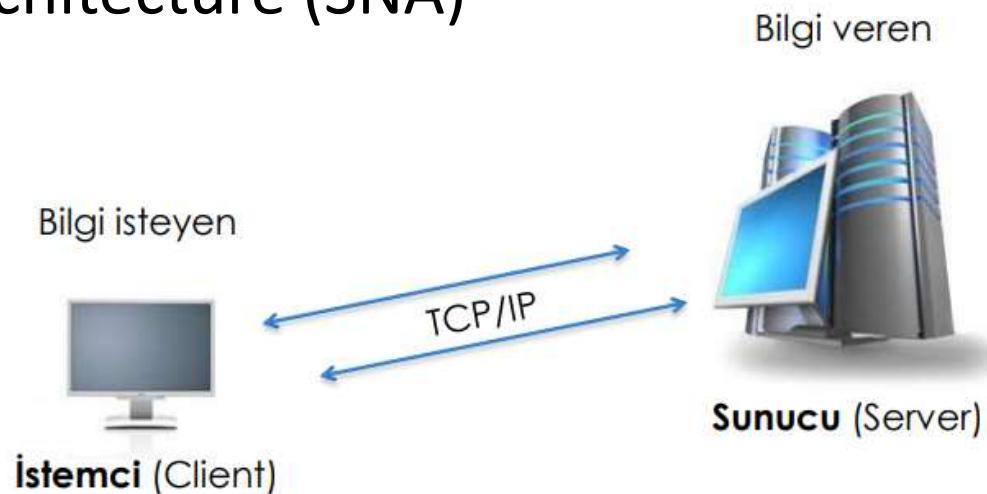
Protokol

- Protokoller, bilgisayarlar arası iletişimde kullanılan ağ dilleridir. (kurallarıdır.)
- Ağ protokolleri verinin cihazlar arasında nasıl taşınacağını ve ekstra olarak veri ile hangi bilgilerin gönderileceğini belirler.
- En sık kullanılan ve bilinen protokol TCP/IP protokol grubudur.
 - Internet erişimi tamamen TCP/IP'ye dayanır.



Protokol Kümeleri(Yığınları)

- IBM System Network Architecture (SNA)
- Digital DECnet
- Novell Netware
- Apple AppleTalk
- NetBEUI
- IPX/SPX
- TCP/IP
 - TCP (Transmission Control Protocol)
 - UDP (User Datagram Protocol)
 - IP (Internet Protocol)
 - ICMP (Internet Control Message Protocol)
 - IGMP (Internet Group Management Protocol)
 - ARP (Address Resolution Protocol)



OSI Modeli

PROTOKOLLER

KATMANLAR



OSI Model Layers

Application Layer

Presentation Layer

Session Layer

Transport Layer

Network Layer

Data-Link Layer

Physical Layer

TCP/IP Protocol Architecture Layers

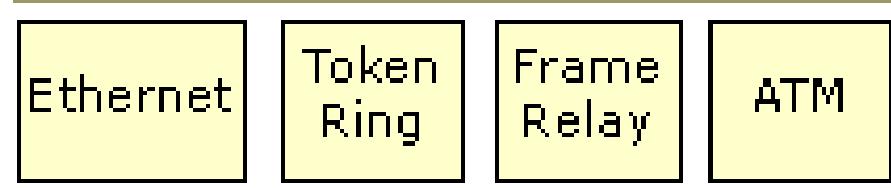
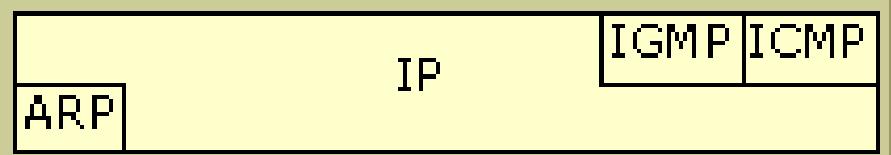
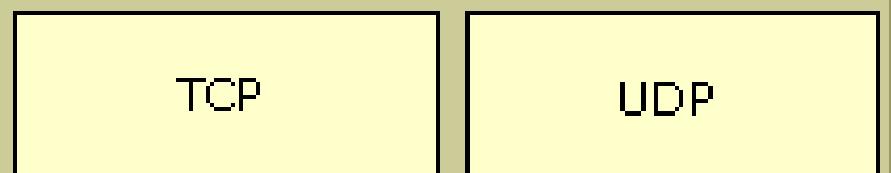
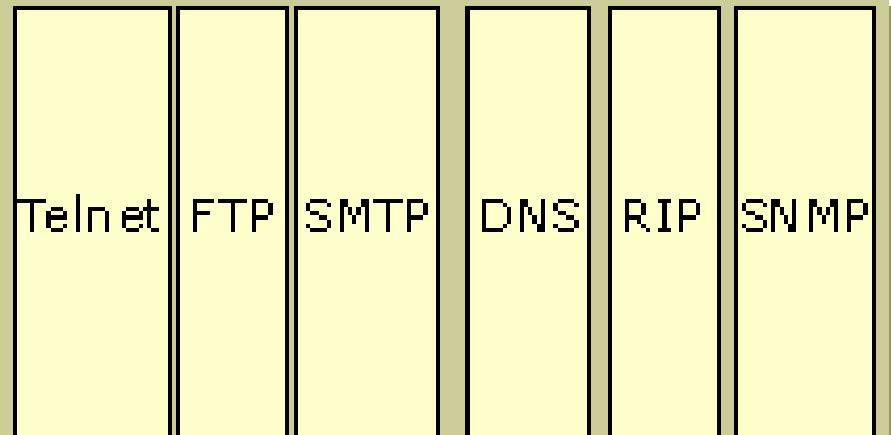
Application Layer

Host-to-Host Transport Layer

Internet Layer

Network Interface Layer

TCP/IP Protocol Suite



Application

Transport

Internet

Network
Access

File Transfer

- TFTP ♦
- FTP ♦
- NFS

E-mail

- SMTP

Remote Login

- Telnet ♦
- rlogin

Network Management

- SNMP ♦

Name Management

- DNS ♦
- used by the router

Application

Transport

Internet

Network
Access

Transmission Control Protocol (TCP)

Connection-Oriented

User Datagram Protocol (UDP)

Connectionless

Application

Transport

Internet

Network
Access

Internet Protocol (IP)

Internet Control Message Protocol (ICMP)

Address Resolution Protocol (ARP)

Reverse Address Resolution Protocol (RARP)

Application

Transport

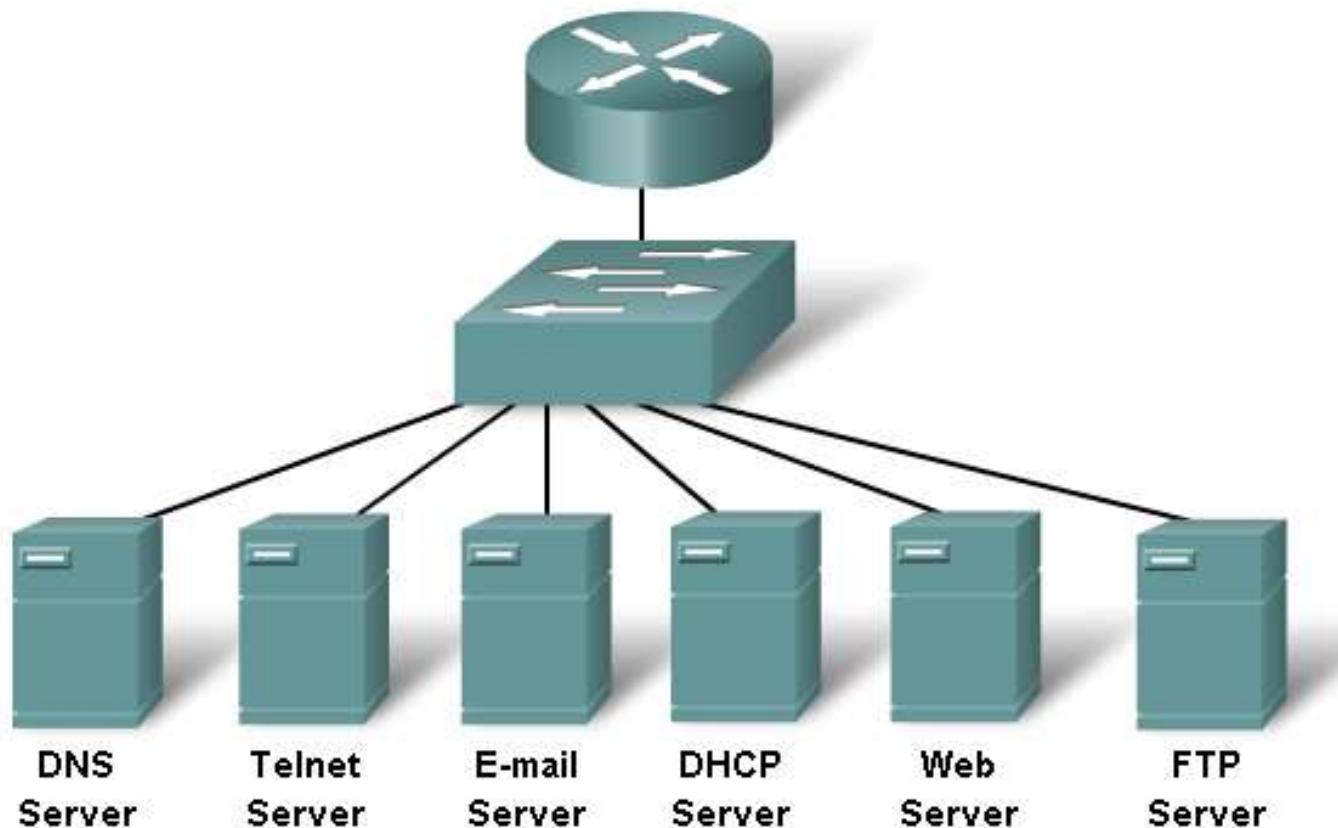
Internet

Network
Access

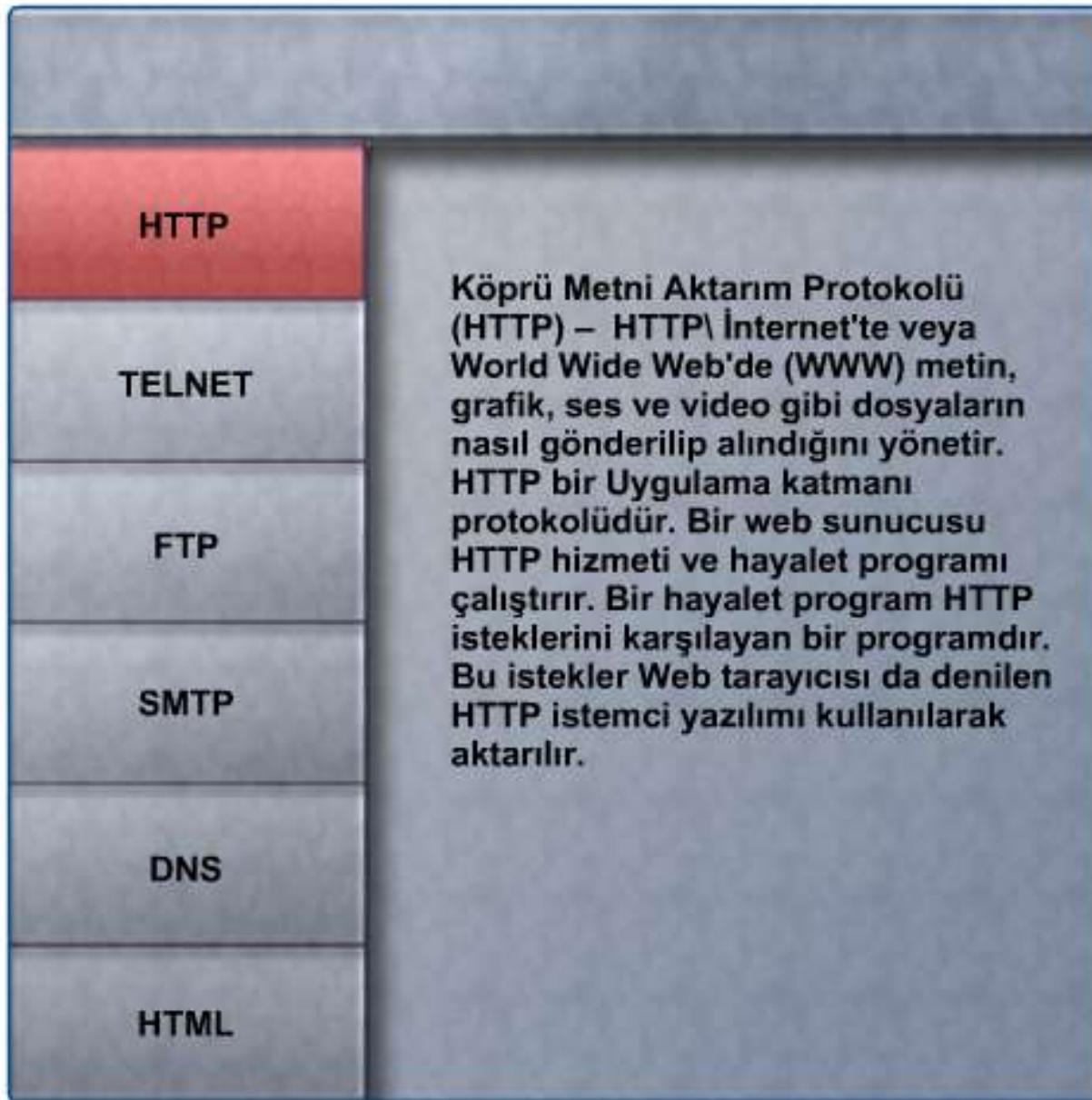
- Ethernet
- Fast Ethernet
- SLIP & PPP
- FDDI
- ATM, Frame Relay & SMDS
- ARP
- Proxy ARP
- RARP

İnternet İletişimi

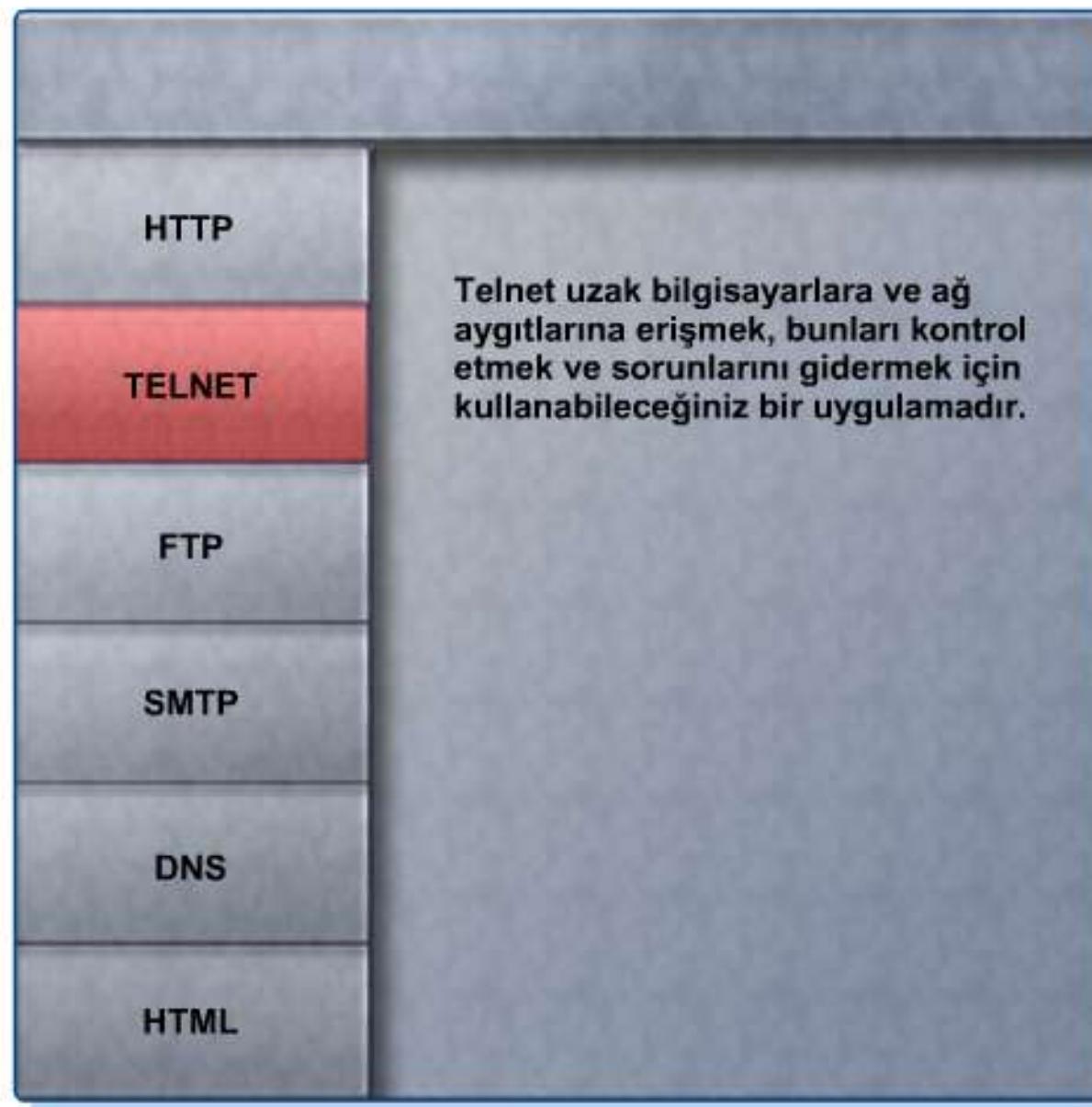
- TCP / IP
- IP Adresi
- DHCP
- HTTP
- DNS
- E-mail
- FTP
- SNMP



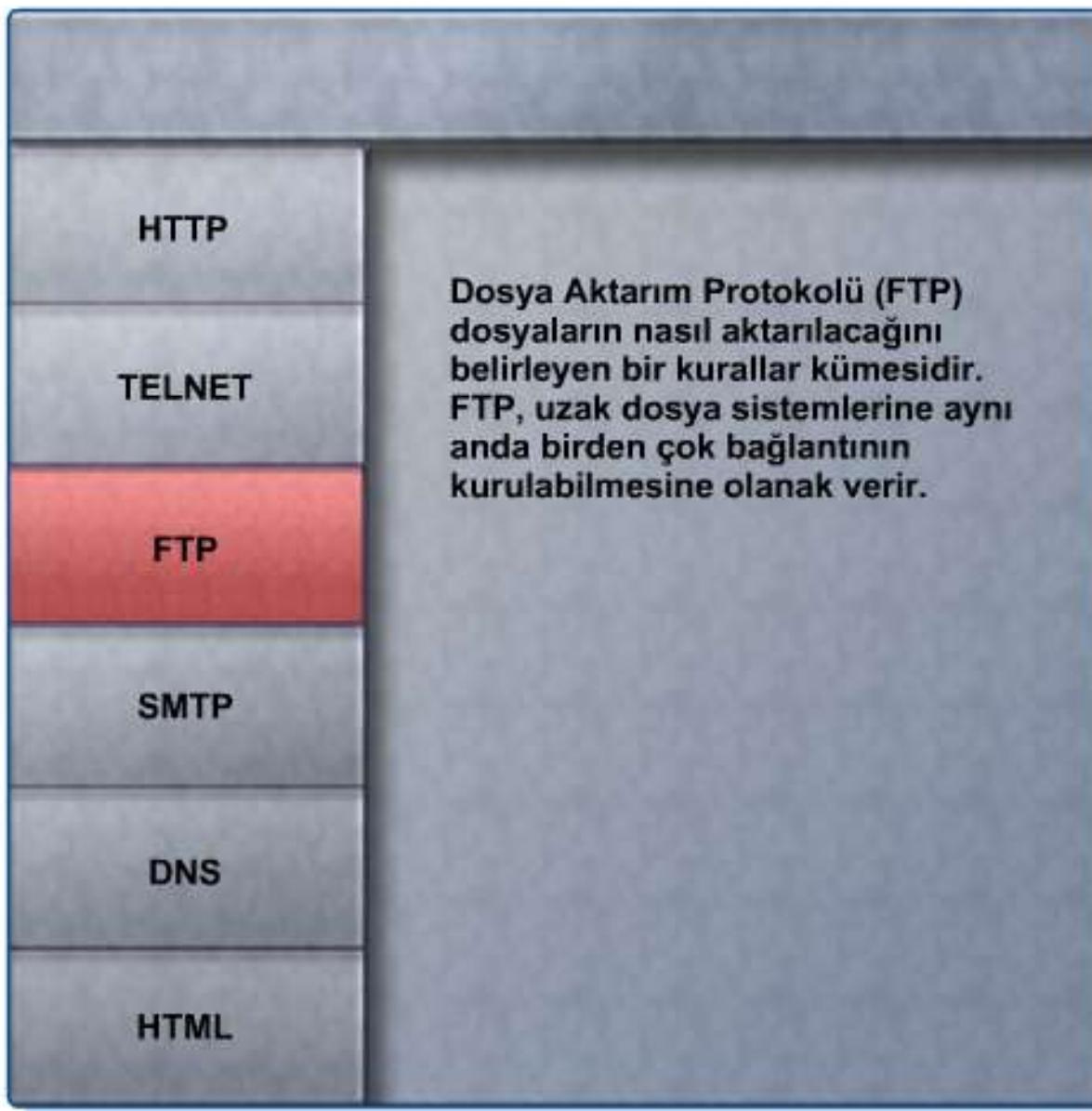
TCP/IP Uygulama Katmanı Protokollerİ



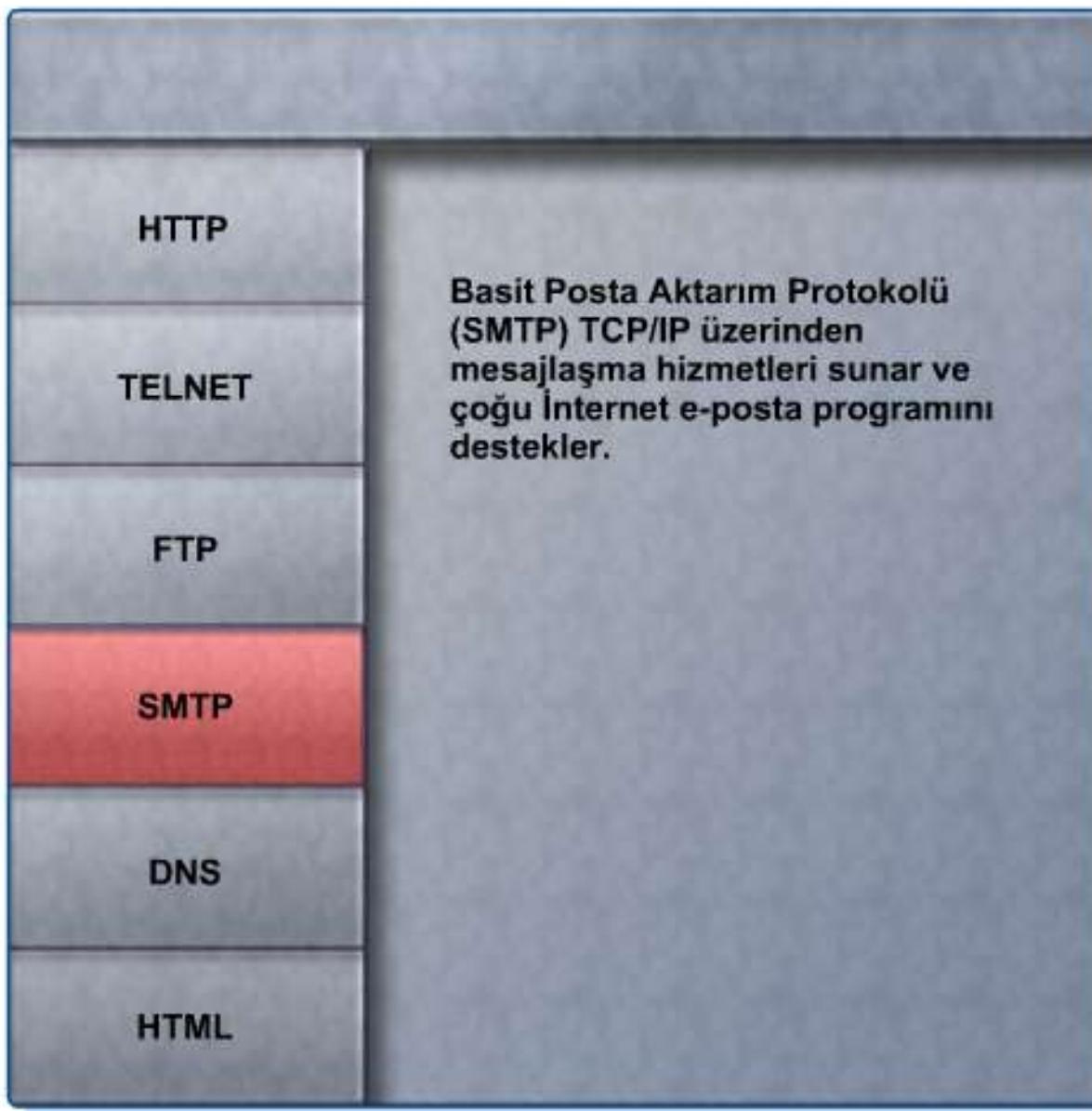
TCP/IP Uygulama Katmanı Protokollerİ



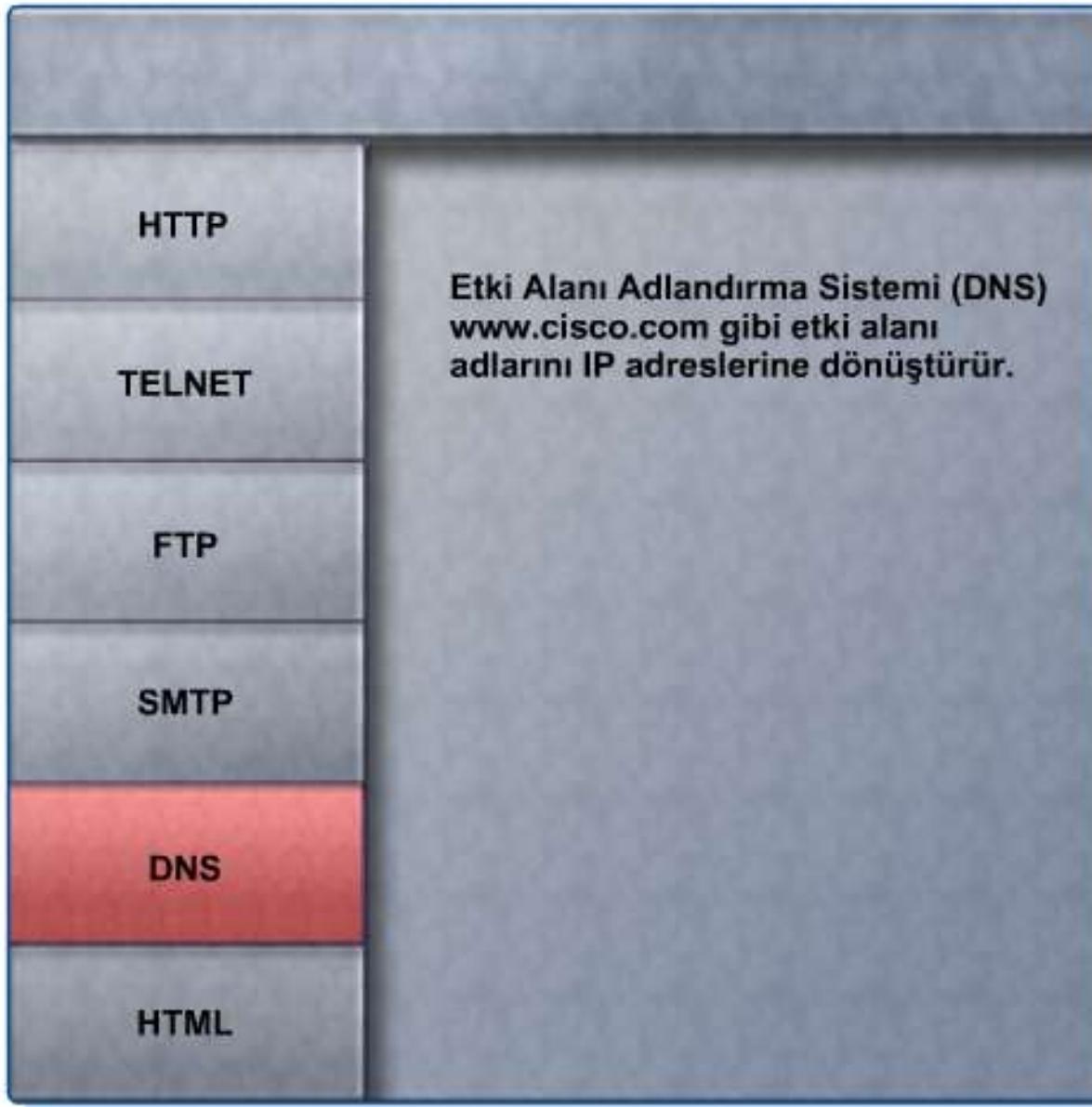
TCP/IP Uygulama Katmanı Protokollerı



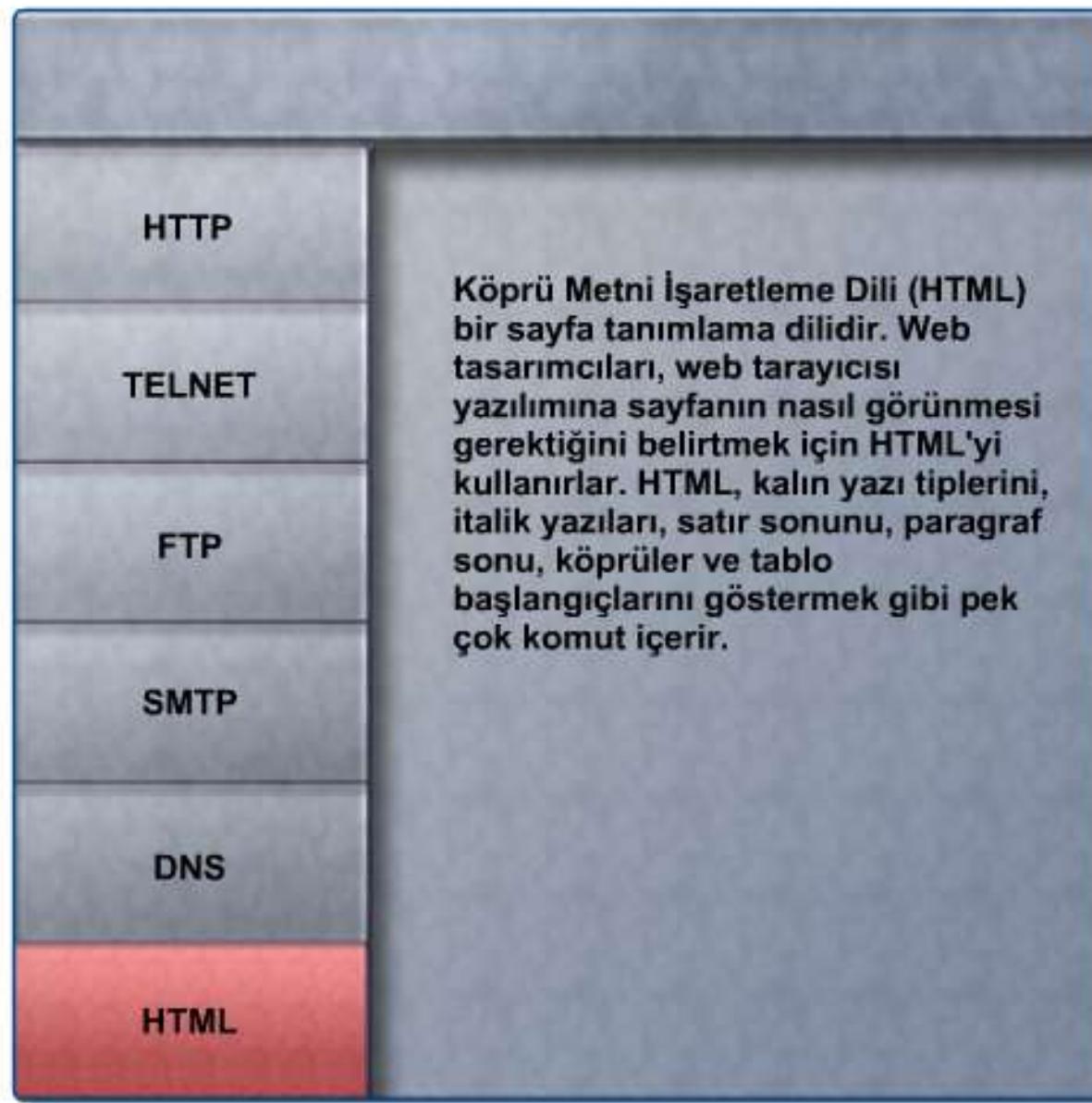
TCP/IP Uygulama Katmanı Protokollerı



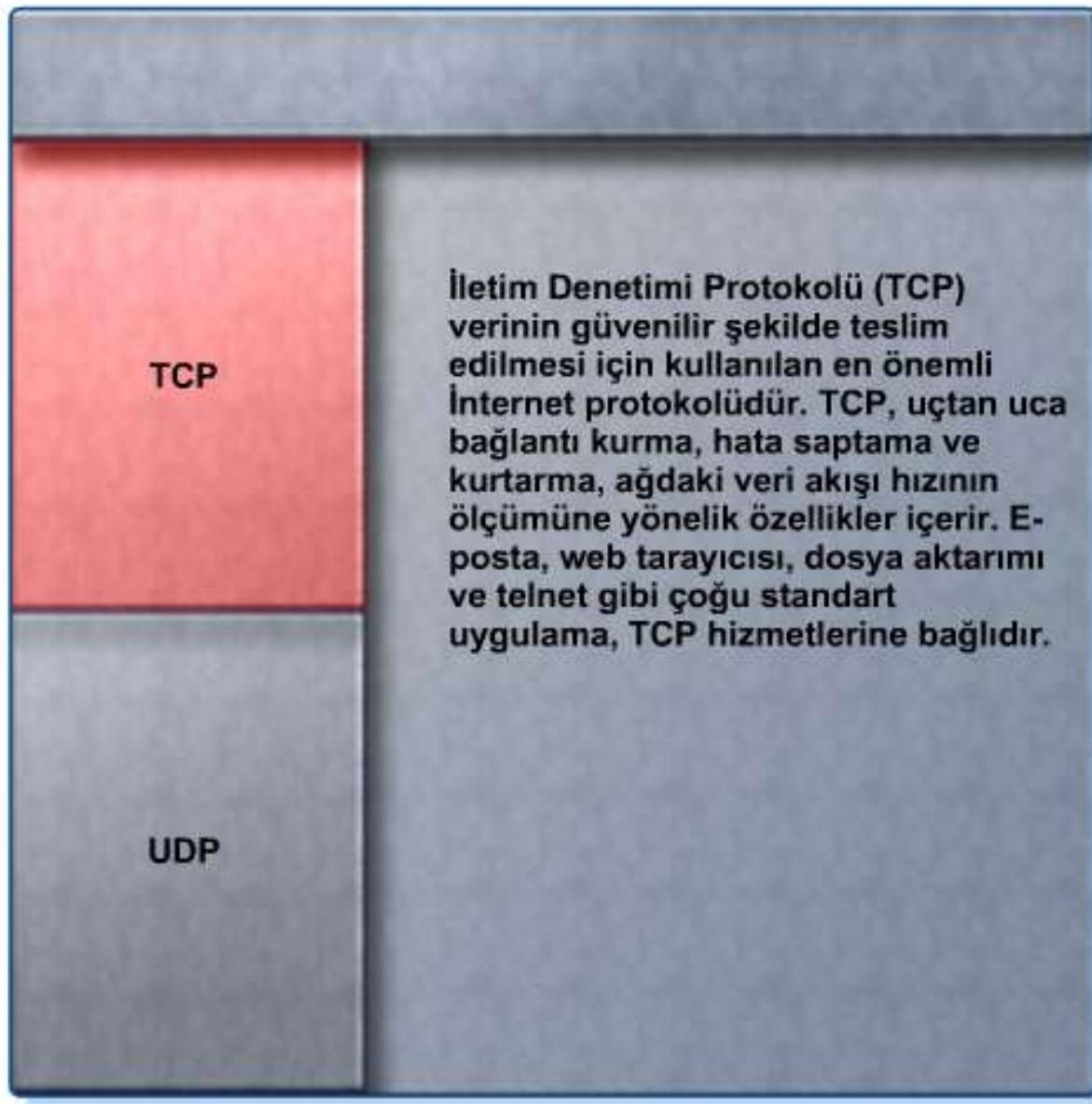
TCP/IP Uygulama Katmanı Protokoller



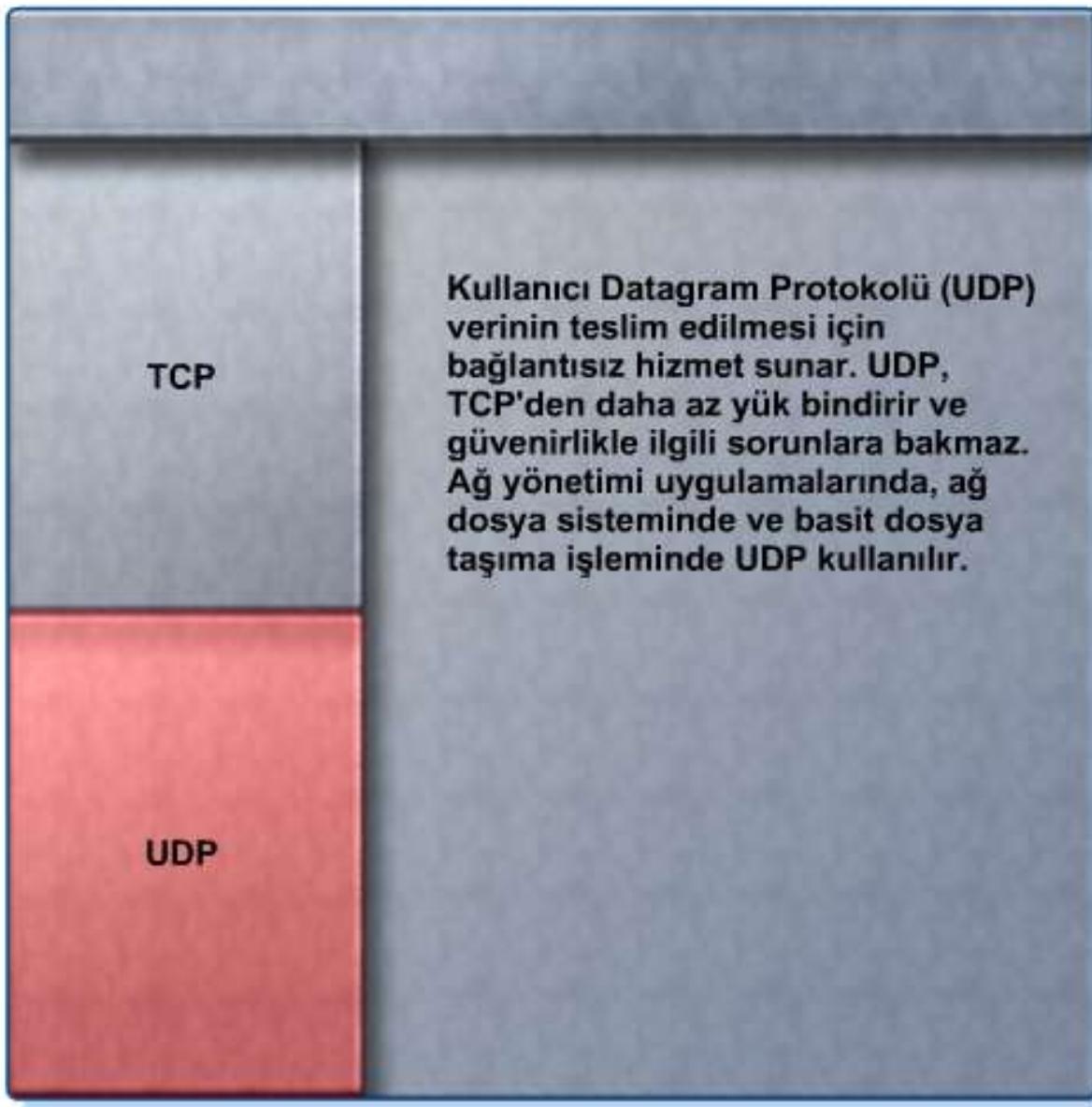
TCP/IP Uygulama Katmanı Protokollerı



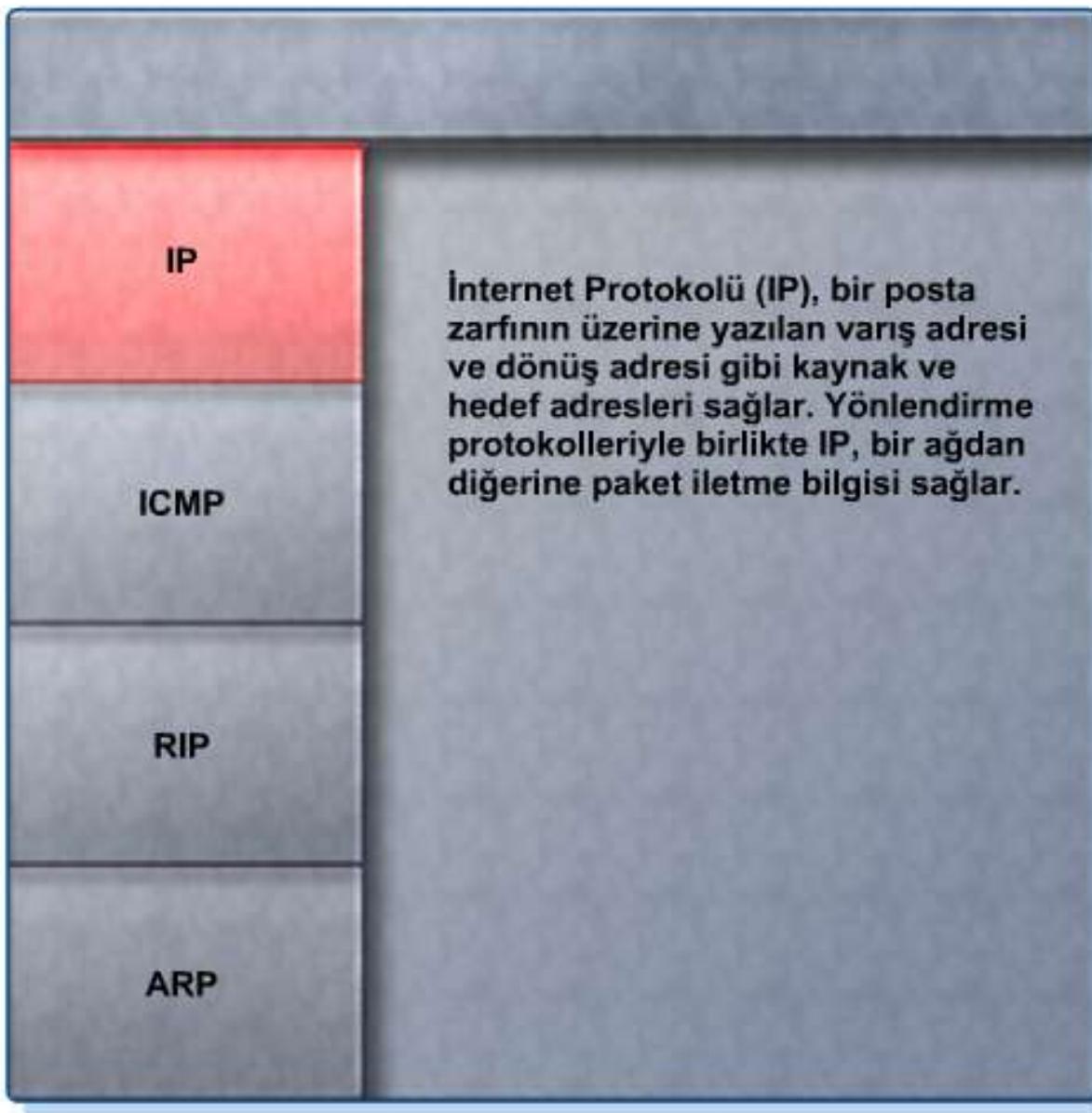
TCP/IP Taşıma Katmanı Protokollerı



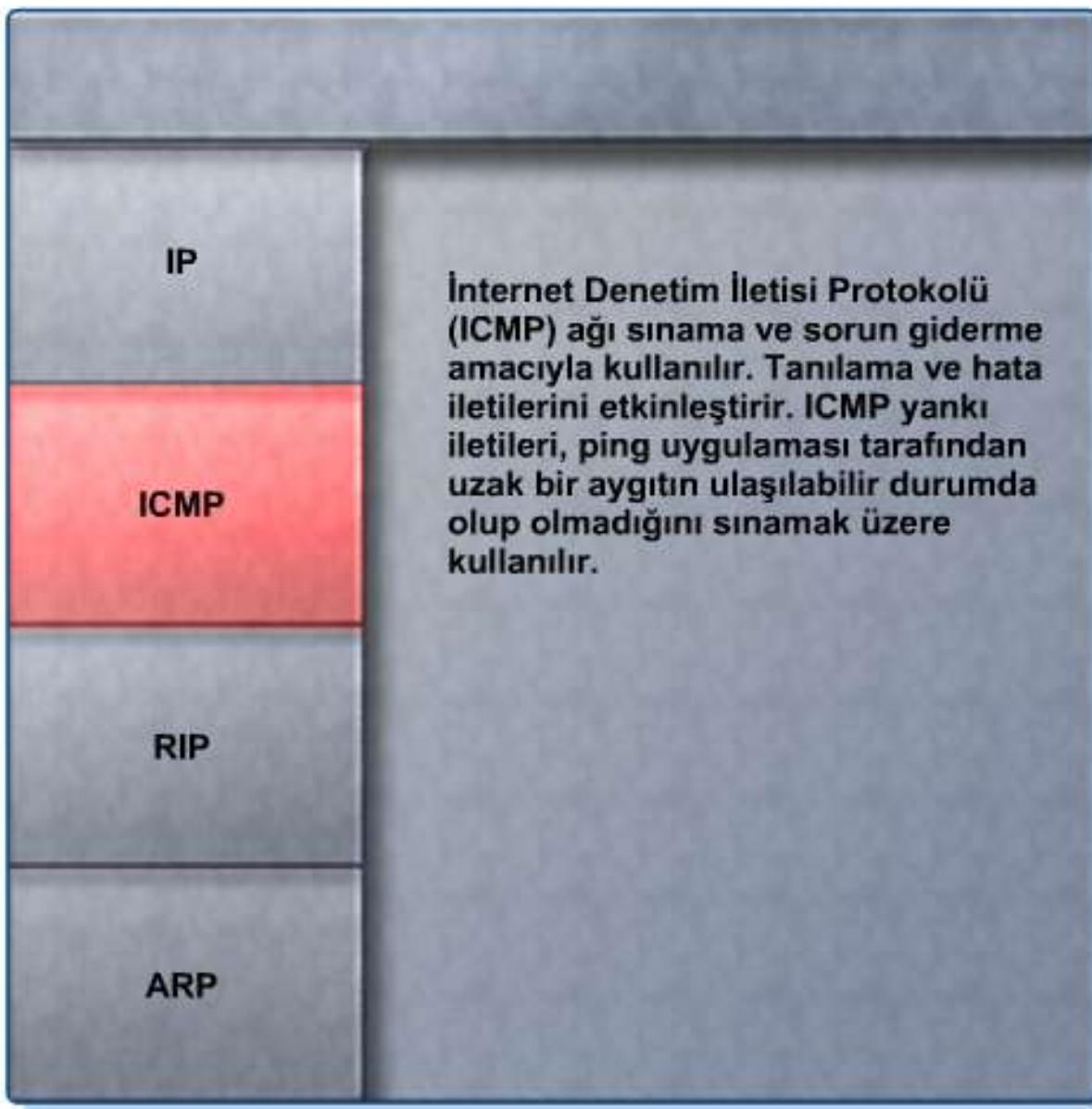
TCP/IP Taşıma Katmanı Protokollerİ



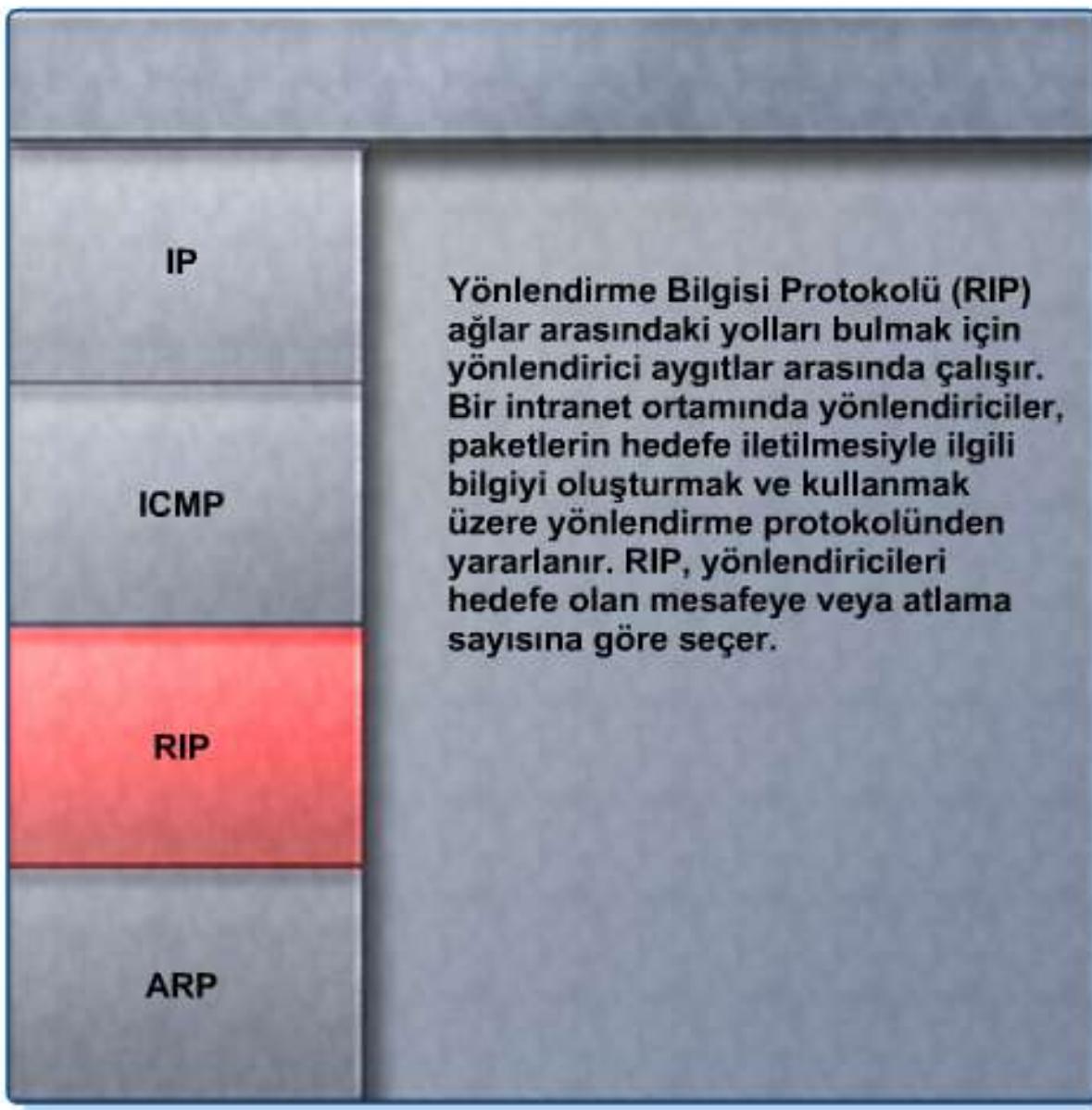
TCP/IP Internet Katmanı Protokollerİ



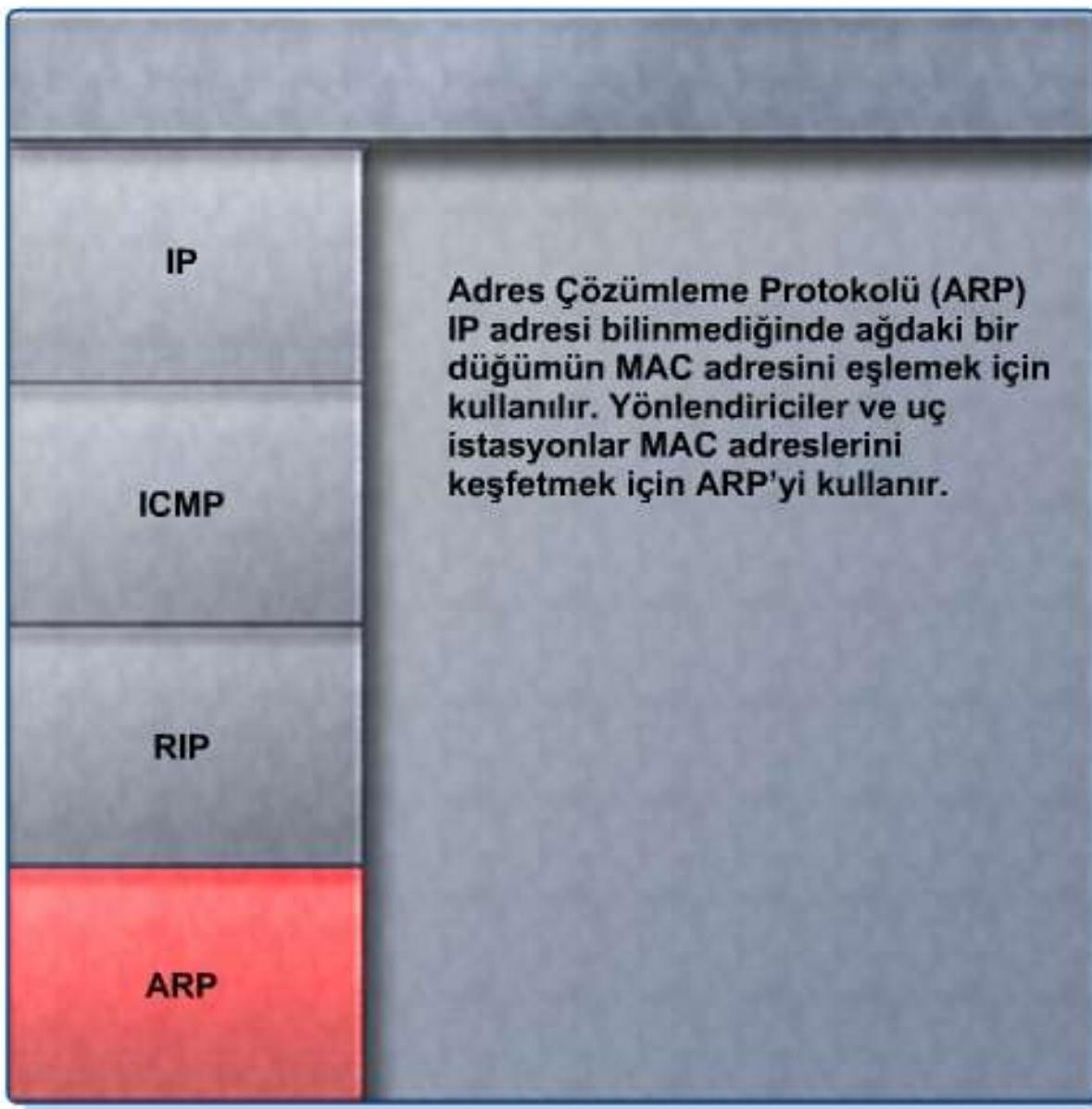
TCP/IP Internet Katmanı Protokoller



TCP/IP İnternet Katmanı Protokollerİ



TCP/IP İnternet Katmanı Protokollerleri



Protokol Bağlantı Noktaları

Protokol	Bağlantı Noktası	Amaç
HTTP	Bağlantı noktası 80	Web sayfalarını TCP/IP ağı üzerinde taşıır
HTTPS	Bağlantı noktası 443	Web sayfalarını TCP/IP ağı üzerinde güvenli bir şekilde taşır
SMTP	Bağlantı noktası 25	TCP/IP ağı üzerinden e-posta gönderir
Telnet/SSH	Bağlantı noktası 23/22	Bilgisayarlara TCP/IP ağı üzerinden bağlantı sağlar
FTP/TFTP	Bağlantı noktası 20 veya 21	Dosyaları TCP/IP ağı üzerinde taşıır
DNS	Bağlantı noktası 53	URL'leri IP adreslerine çevirir
DHCP	Bağlantı noktası 67	Bir ağ üzerinde IP adreslerinin atanmasını otomatikleştirir.

E-posta Protokollerini Karşılaştırma

Protokol	Avantajlar	Dezavantajlar	Bağlantı Noktası	Posta Gönderme	Posta Alma
SMTP	E-postayı bir sunucundan diğerine gönderir Doğrudan hedefe posta gönderebilir	Yalnızca istemci yüklemesi yapılabilir	25	E	H
POP	Basittir Kesintili bağlantıları destekler	Yalnızca indirme işlemi yapılabilir Postalar sunucu üzerinde yönetilemez	110	H	E
IMAP	Basittir POP'tan daha fazla özelliğe sahiptir Sunucuda posta depolar POP'tan daha hızlıdır Birden fazla istemcinin erişimine olanak verir	Daha fazla disk alanı ve CPU kaynağı gerektirir	143	H	E

LAN Teknolojileri

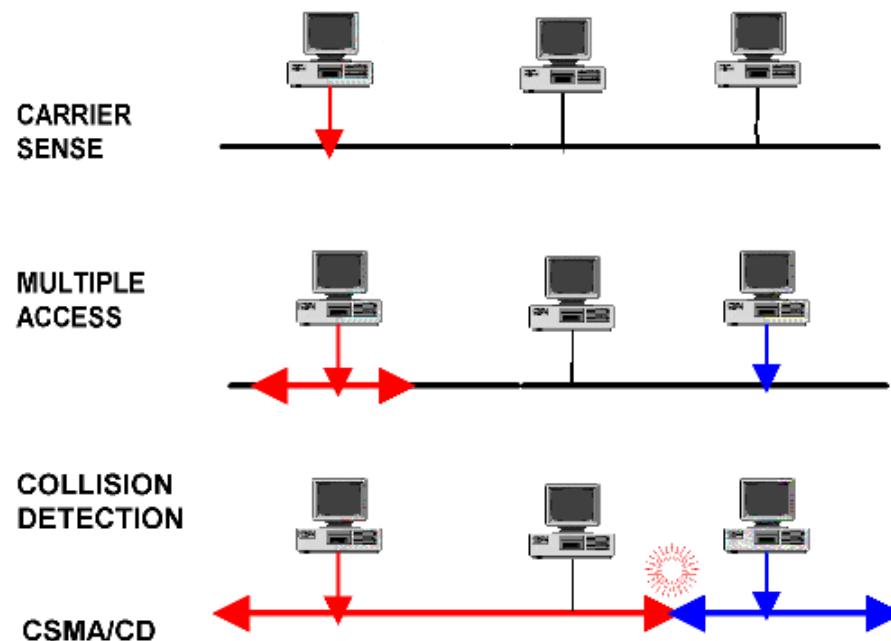
- Ethernet (IEEE 802.x)
 - CSMA/CD
 - Fast Ethernet
 - Gigabit Ethernet
- Jetonlu Halka(Token Ring)
- Jetonlu Halka(Token Bus)
- ATM
- FDDI LAN

IEEE 802 Standards	
802.1	Bridging & Management
802.2	Logical Link Control
802.3	Ethernet - CSMA/CD Access Method
802.4	Token Passing Bus Access Method
802.5	Token Ring Access Method
802.6	Distributed Queue Dual Bus Access Method
802.7	Broadband LAN
802.8	Fiber Optic
802.9	Integrated Services LAN
802.10	Security
802.11	Wireless LAN
802.12	Demand Priority Access
802.14	Medium Access Control
802.15	Wireless Personal Area Networks
802.16	Broadband Wireless Metro Area Networks
802.17	Resilient Packet Ring

CSMA / CD

Carrier Sense Multiple Access / Collision Detect
(Taşıyıcı Sezme Çoklu Algılama / Çatışma Denetimi)

(Çarpışma Algılayıcıyla Taşıyıcı Dinleyen Çoklu Erişim)



Geniş Alan Ağları

Sınıflandırma

- Bağlantı Durumuna göre
 - Noktadan noktaya
 - Çoklu bağlantı teknolojisi
- Anahtarlama Yöntemine göre
 - Devre anahtarlama
 - Paket anahtarlama
 - Hücre anahtarlama
- Topolojik Yapışma göre
 - Hiyerarsık topoloji
 - Örgü topoloji

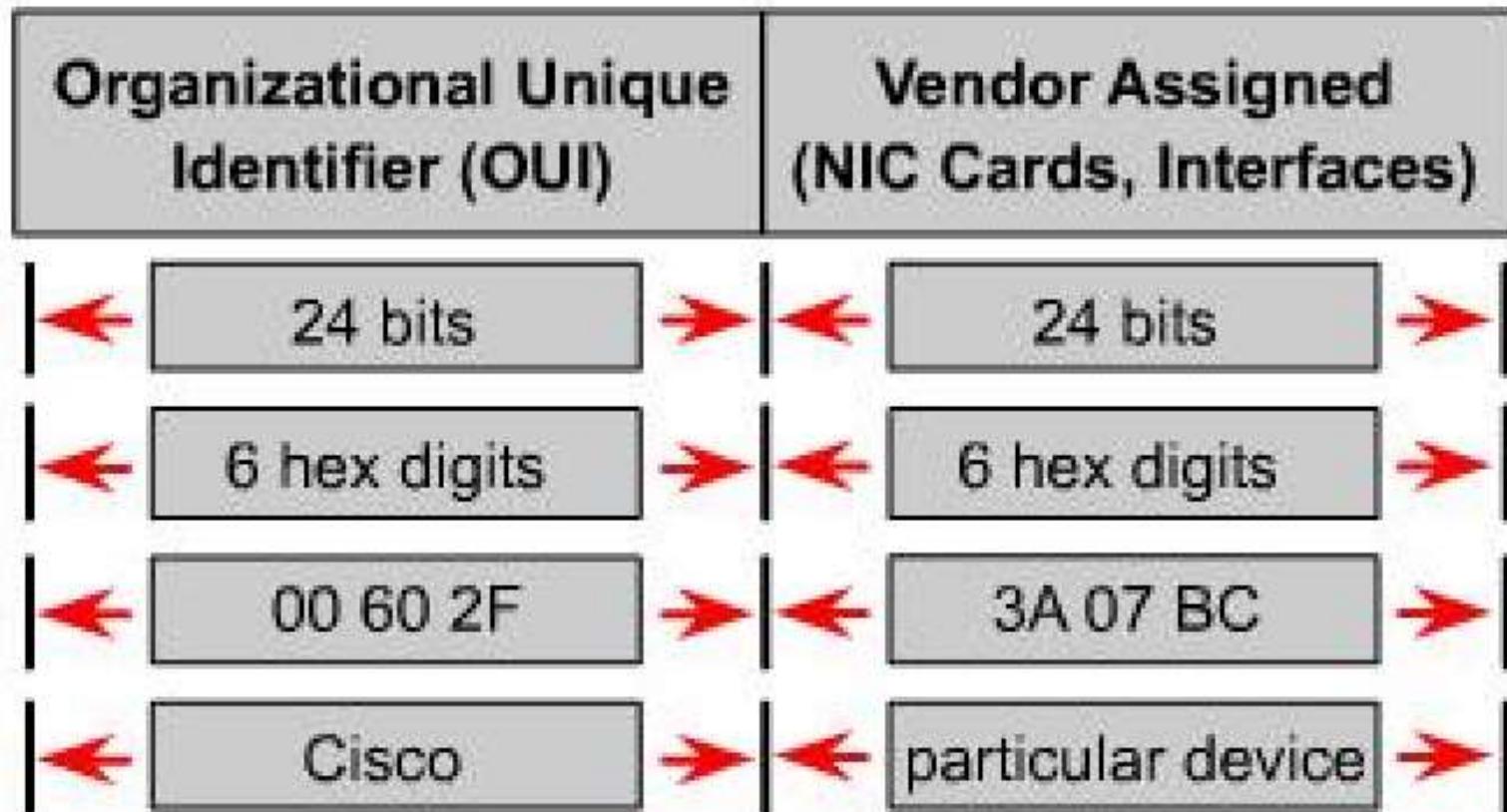
Teknolojiler

- Modem(dial-up)
- Kiralık hat
- X.25
- Frame Relay (FR)
- ISDN
- xDSL
- ATM
- SMDS

xDSL'ler

- ADSL (Asymmetric Digital Subscriber Line)
- HDSL (High bit-rate Digital Subscriber Line)
- HDSL2 (High bit-rate Digital Subscriber Line - 2)
- IDSL (ISDN Digital Subscriber Line)
- RADSL (Rate Adaptive Digital Subscriber Line)
- SDSL (Symmetric Digital Subscriber Line)
- SHDSL (Symmetric High-data-rate Digital Subscriber Line)
- VDSL (Very-High-Bit-Rate Digital Subscriber Line)
- G.SHDSL (G.991.2 Symmetric High-data-rate Digital Subscriber Line)
- MSDSL (Multi-Speed Digital Subscriber Line)
- METALOOP

MAC



IP Adresi ve Sınıflandırması

- IP adresi belli bir ağa bağlı cihazların ağ üzerinden birbirlerine veri yollamak için kullandıkları haberleşme yöntemidir.
- (Internet Protocol Address)

1 0 0 0 0 0 1 1 0 1 1 0 1 1 0 0 0 1 1 1 1 0 1 0 1 1 0 0 1 1 0 0

32 Bits

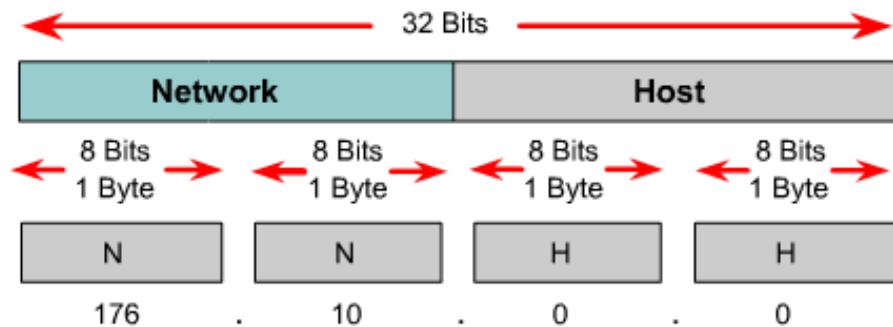
Binary : 11000000.10101000.00000001.00001000 and 11000000.10101000.00000001.00001001

Decimal : 192.168.1.8 and 192.168.1.9

IP v4

- IPV4 adresleri 4 hanelidir. Ve aralarında nokta bulunur.
- Örnek : 192.168.2.1
- Her hane 256 adet ip no barındırır.
- Teorik olarak $256 \times 256 \times 256 \times 256 = 4$ Milyar
- Tükenmek üzeredir ve birçok güvenlik açığı barındırmaktadır.

IP



Network Address (host bits = all zeros)



Broadcast Address (host bits = all ones)

Class A	Network	Host		
Octet	1	2	3	4
Class B	Network		Host	
Octet	1	2	3	4
Class C	Network			Host
Octet	1	2	3	4
Class D	Host			
Octet	1	2	3	4

1 0 0 0 0 0 1 1 0 1 1 0 1 0 0 0 1 1 1 1 1 0 1 0 1 1 0 0 1 1 0 0

← 32 Bits →

Binary : 11000000.10101000.000000001.00001000 and 11000000.10101000.00000001.00001001

Decimal : 192.168.1.8 and 192.168.1.9

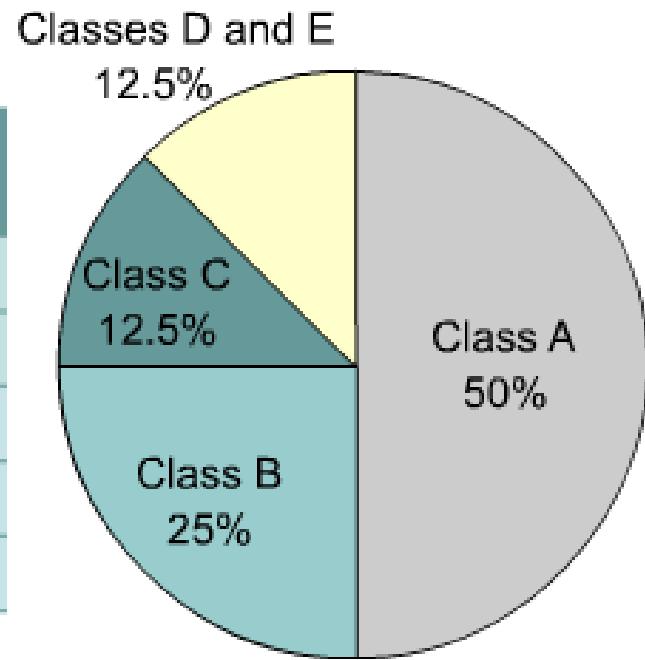
IP v4 Sınıflaması

IP Address Class	High Order Bits	First Octet Address Range	Number of Bits in the Network Address
Class A	0	0 - 127 *	8
Class B	10	128 - 191	16
Class C	110	192 - 223	24
Class D	1110	224 - 239	28

IP address class	IP address range (First Octet Decimal Value)
Class A	1-126 (00000001-01111110) *
Class B	128-191 (10000000-10111111)
Class C	192-223 (11000000-11011111)
Class D	224-239 (11100000-11101111)
Class E	240-255 (11110000-11111111)

Public(Genel) ve Private(Özel) IP

IP address class	IP address range (First Octet Decimal Value)
Class A	1-126 (00000001-01111110) *
Class B	128-191 (10000000-10111111)
Class C	192-223 (11000000-11011111)
Class D	224-239 (11100000-11101111)
Class E	240-255 (11110000-11111111)



Class	RFC 1918 internal address range
A	10.0.0.0 to 10.255.255.255
B	172.16.0.0 to 172.31.255.255
C	192.168.0.0 to 192.168.255.255

Loopback 127.0.0.1 (localhost)

IP v6



- **Internet Protokol Version 6** (*Internet Protokol sürüm 6*)
- 32 bitlik bir adres yapısına sahip olan IPv4'ün adreslemede artık yetersiz kalması ve ciddi sıkıntılar meydana getirmesi üzerine geliştirilmiştir.
- IPV6 adresleri 8 hanelidir.
- Araları ":" ile ayrılır. Her hane hexadecimal olarak ifade edilir.
- IPV6'da IPV4'de olduğu gibi IP sıkıntısı yaşanmayacaktır.
- Her hane 65536 adet ipv6 adresini barındırır.
- En küçük adres 0 en büyük adres FFFF'dir.
- Örnek : 2001:a98:c040:111d:0:0:1

IP v4 / IP v6

$2^{128} = 340.282.366.920.938.463.463.374.607.431.768.211.456 \asymp 3,4 \cdot 10^{38}$ adet IPv6 adresi demektir. 32 bitlik adres (IPv4) yapısı demek

$2^{32} = 4.294.967.296 \asymp 4,3 \cdot 10^9$ adet IPv4 adresi demektir.

An IPv6 address

(in hexadecimal)

2001:0DB8:AC10:FE01:0000:0000:0000:0000

↓ ↓ ↓ ↓ └─────────────────
2001:0DB8:AC10:FE01:: Zeroes can be omitted

0010000000000001:0000110110111000:1010110000010000:1111111000000001:
0000000000000000:0000000000000000:0000000000000000:0000000000000000

IP v4 / IP v6

IPv4	IPv6
8 Bitlik alanlardan oluşur	16 bitlik alanlardan oluşur
4 farklı alandan meydana gelen bir mimarisi vardır.	8 farklı alandan meydana gelen mimari ile hazırlanmıştır.
Toplamda 32 bit adresleme yapabilir	Toplamda 128 bit adresleme yapabilir
Adresler sadece sayılarından oluşmaktadır.	Adreslerde harflerinde kullanımı vardır.
NAT (Network Address Translator) yapılmaktadır.	NAT (Network Address Translator) yapılmaktadır.
IPSec desteği isteğe bağlı kullanılabilir	IPSec kullanımı zorunludur

Anahtar(Switch) Cihazı

- Anahtar OSI'ye göre 2.katmanda çalışır,
- Veri bağı - Data link - Layer2,
- MAC adresleri ile çalışır,
- Tabloları ile gerekli işlevi sağlar,
- 3.katman anahtarlar

Bir anahtarın. MAC adres tablosu

Alicı MAC Adresi	Bağlı Olduğu Port
08-00-02- 1a-3c-b2	1.port
00-a0-24-1a-3c-b2	5.port
08-00-21-a4-c8-92	7.port
08-00-02-1a-3c-33	8.port
08-00-24-1 a-3c-b2	8.port
00-00-02-1a-3c-b2	2.port
00-00-25-1 a-3c-ae	4.port

Anahtarlama Yöntemleri (Switching)

- **Store and forward (Depola ve ilet)**

- Paketi giriş portundan aldıktan sonra buffer'a atar.
- Ardından paketi ilgili çıkış portuna gönderir.
- Paketteki hataları kontrol etmez, daha hızlıdır.
- Ancak bozuk paketler ağda ilerler.

- **Cut-through (Kestirme)**

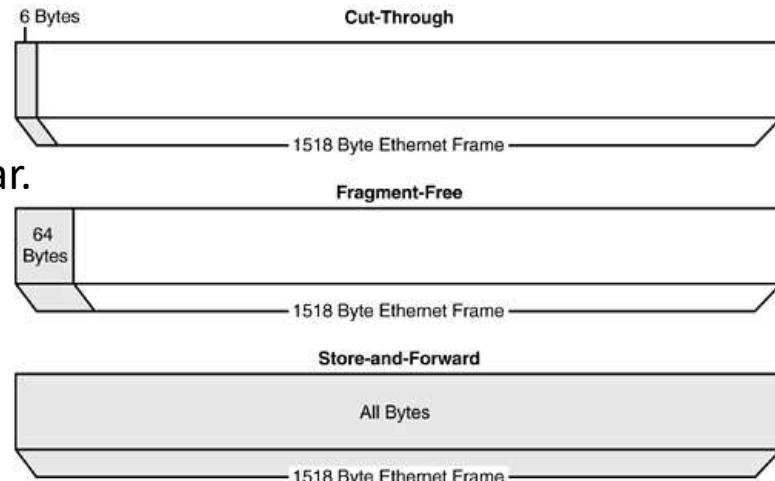
- Paketi iletmeden önce hedef adresi belirler, sonra adresin çıkış portuna bu paketi iletir.
- Pakette hata olup olmadığını kontrol eder. Hatalıysa iletmez.

- **Fegment Free (Serbest parça)**

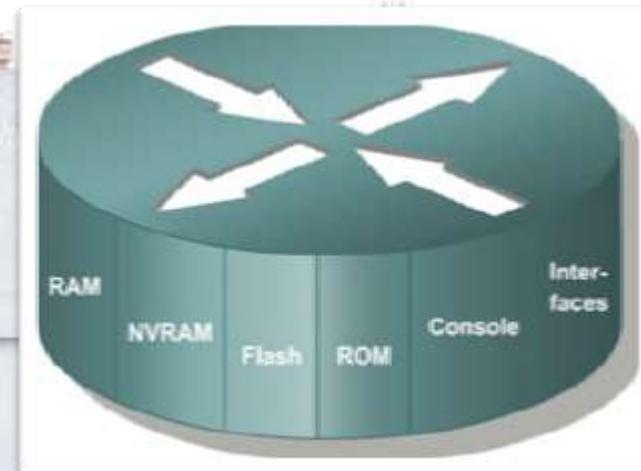
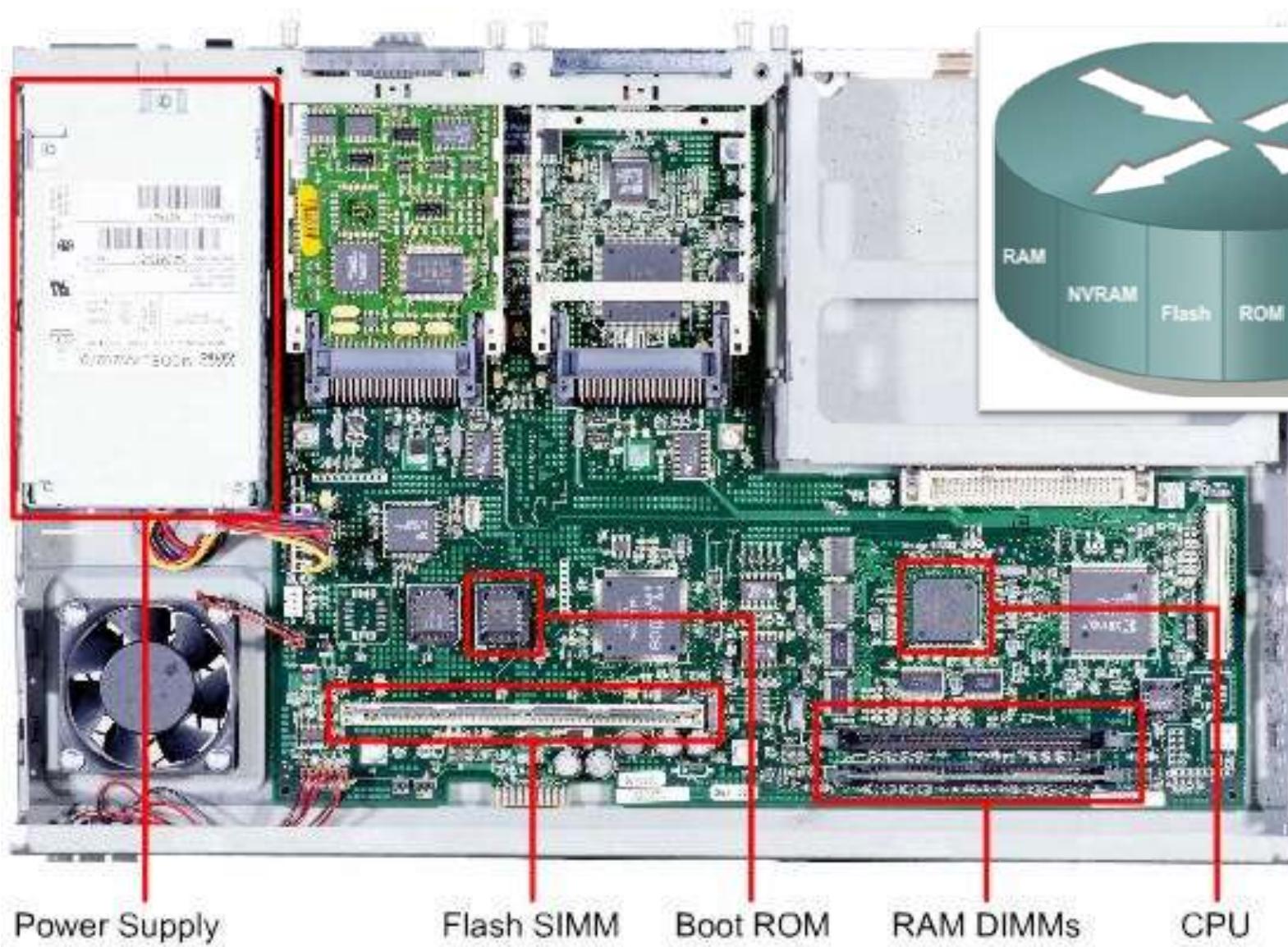
- Paketin ilk 64 byte'ı okunur ve paket kontrol toplamı oluşturulmadan ilettilir.

- **Adaptive switching (Uyarlamalı anahtarlama)**

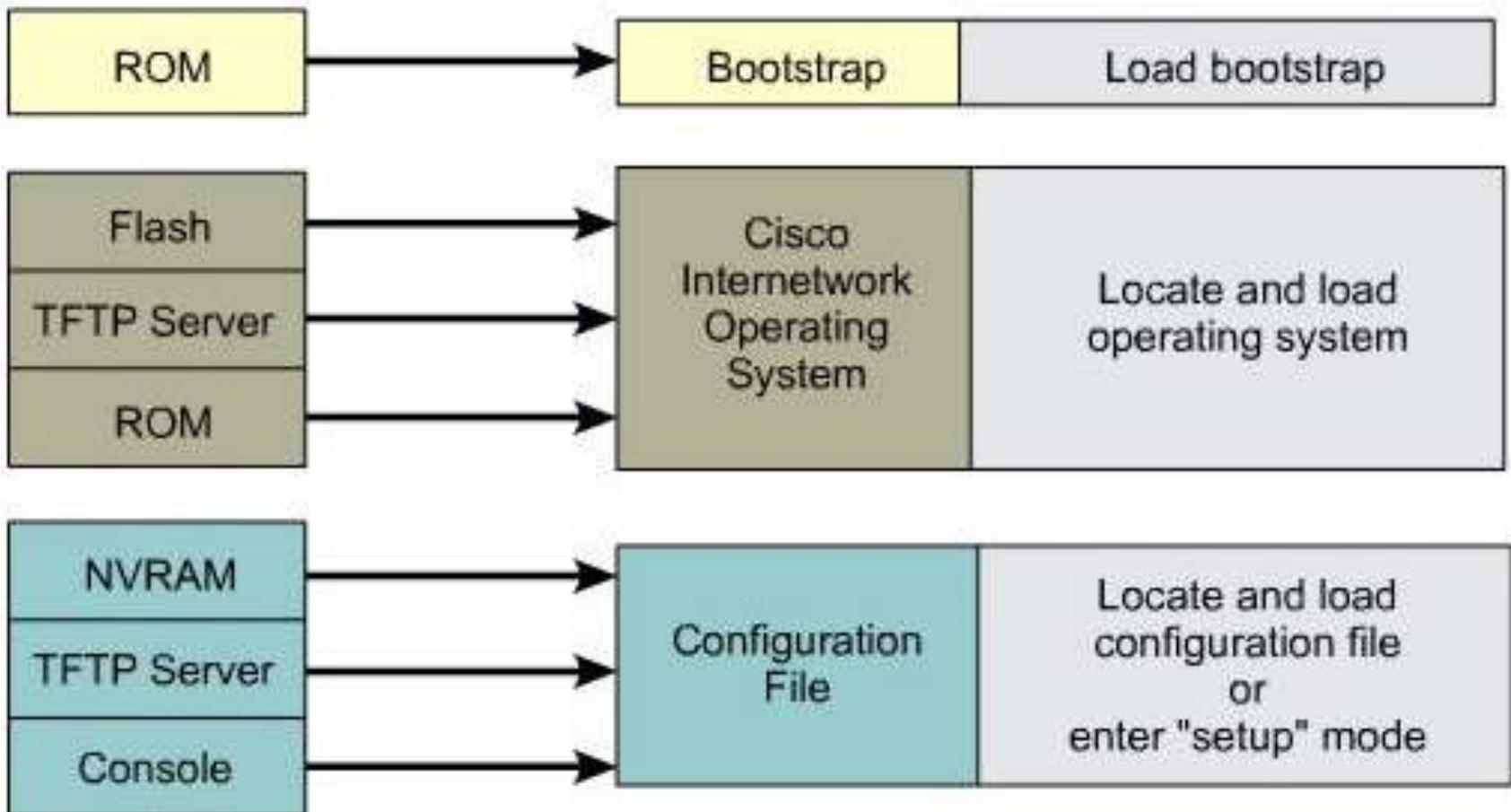
- Yukarıdaki üç yöntem arasında kendi kendine seçim yapan bir yöntemdir.



Router (Yönlendirici)



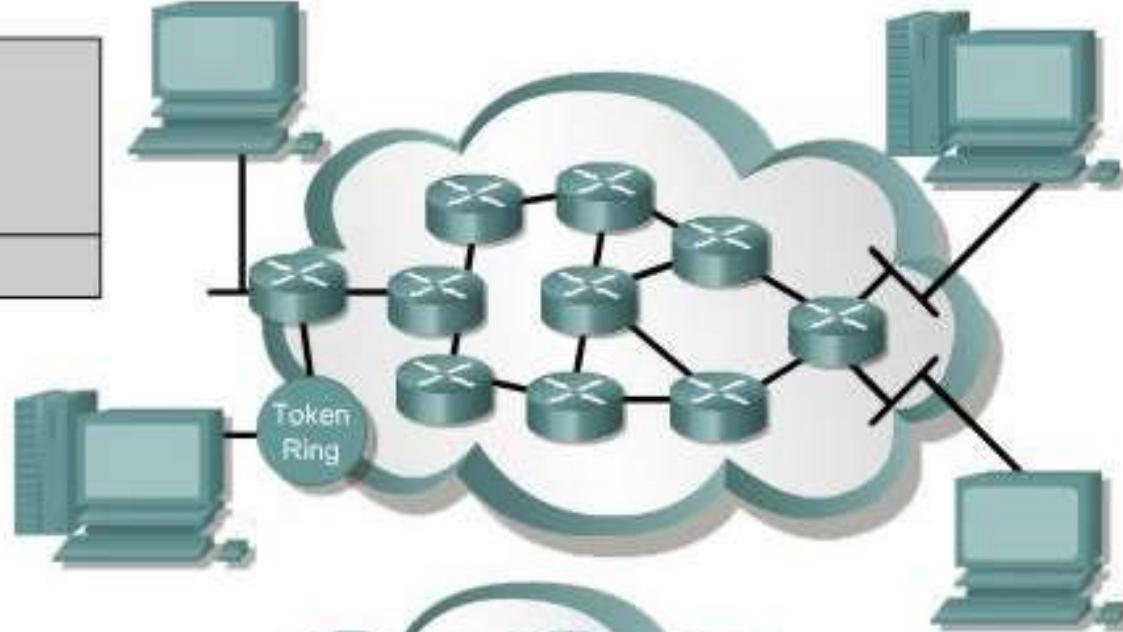
Router



Routing

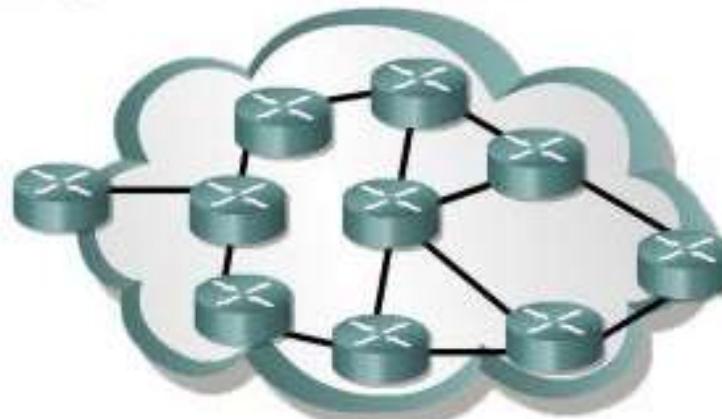
Routed protocol
used between
routers to direct
user traffic

Examples: IP and IPX

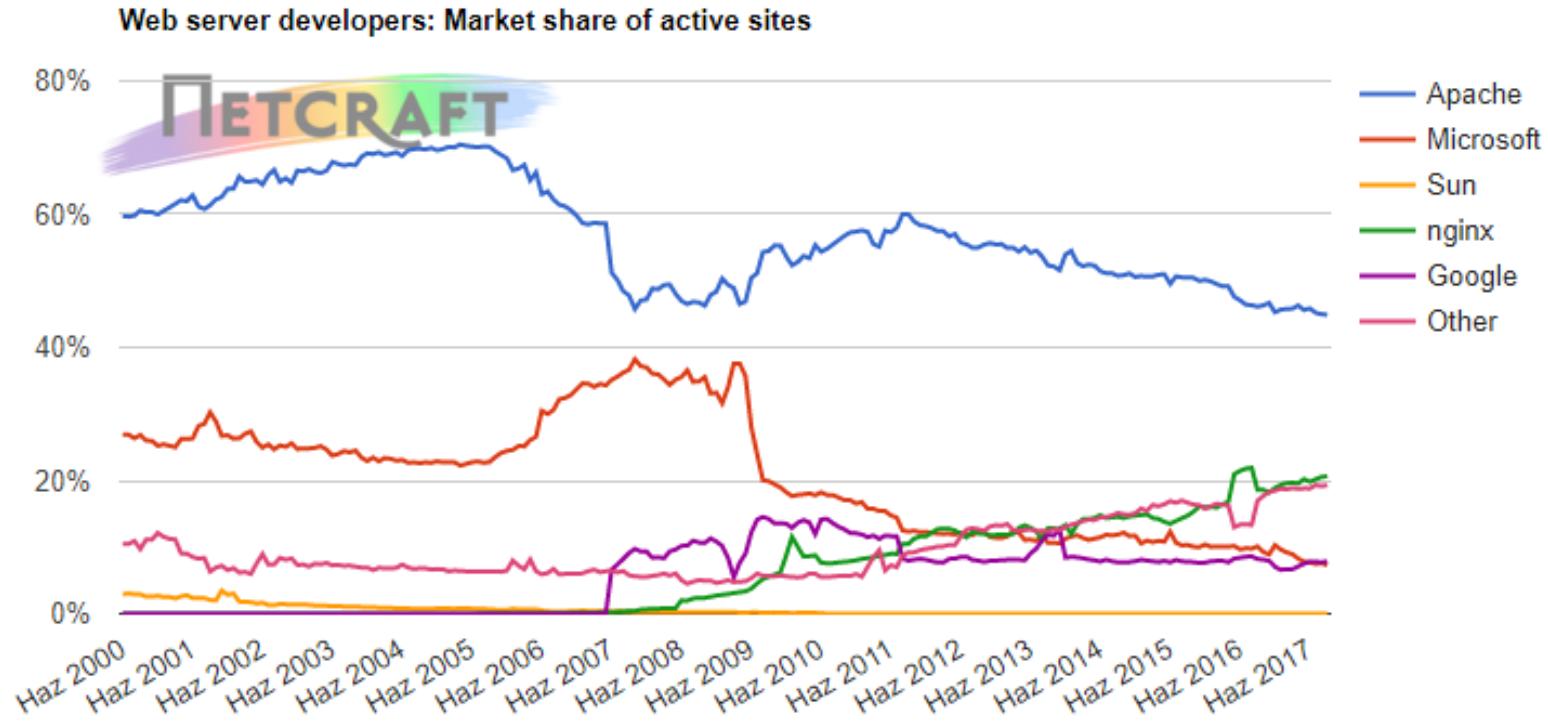


Routing protocol
used between
routers to maintain
tables

Examples: RIP, IGRP, OSPF



Web Server



Developer	August 2017	Percent	September 2017	Percent	Change
Apache	77,916,218	44.99%	77,487,531	44.89%	-0.10
nginx	35,566,579	20.54%	35,640,320	20.65%	0.11
Google	13,376,490	7.72%	13,561,655	7.86%	0.13
Microsoft	13,136,286	7.58%	12,629,582	7.32%	-0.27

5. Hafta

KRIPTOLOJİ VE ŞİFRELEME



Acaba Nedir? (*Dersin Özeti*)

w5bEn3JlbmNplGhhesSxciBvb
GR1xJ91bm RhIMO2xJ9yZXRtZ
W4gZ8O2csO8bmVjZWt0aXlu
VGhIIEJ1ZGRoYQ==

Terimler ve Kavramlar

Kriptografi: Gizli yazışma sanatı anlamına gelmektedir.

Yunancada *gizli* anlamına gelen **kripto/kryptos** ve yazılmış bir şey yazmak anlamına gelen **grafi/graphein** kelimelerinden oluşur.

Kriptoloji: Kriptografi biliminin çalışma disiplinine Kriptoloji denir.

(*Kriptoloji:* Şifre Bilimidir.)

Terimler ve Kavramlar

- **Kriptografi:** Veriyi yalnızca okuması istenen şahısların okuyabileceği bir şekilde saklamak ve göndermek amacıyla kullanılan teknikler bütünüdür.
- **Kripto algoritması:** Verinin matematiksel yöntemler kullanılarak kodlanması ve okunamayacak hale getirilmesidir.

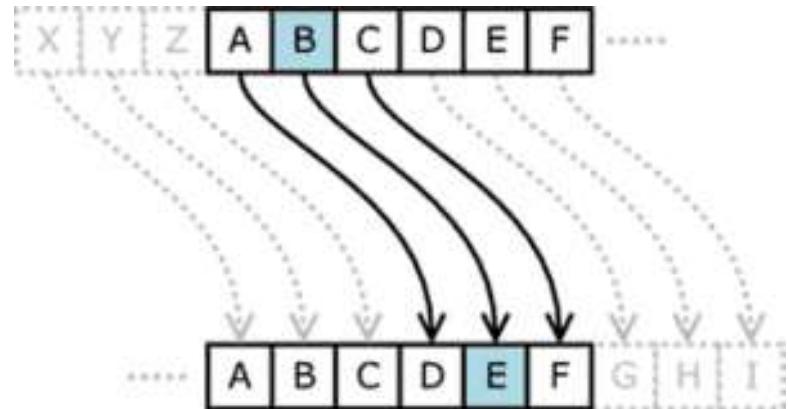
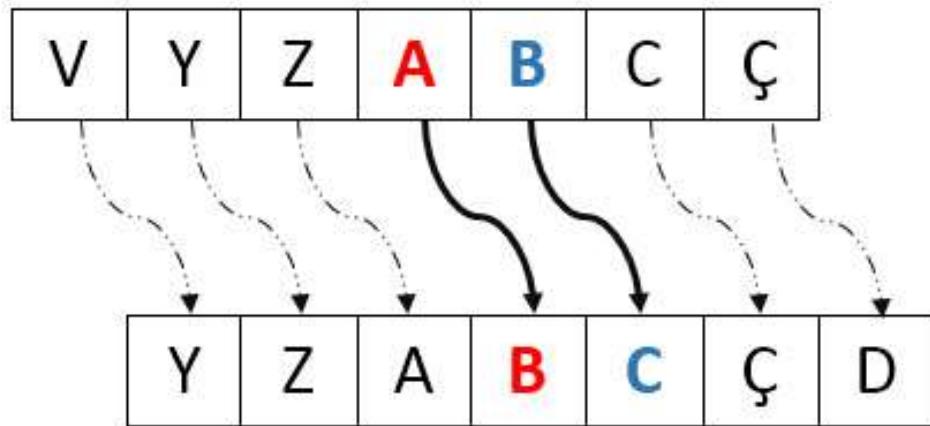
Terimler ve Kavramlar

- **Kriptoanaliz:** Bir şifreleme sistemini veya sadece şifreli mesajı inceleyerek, şifreli mesajın açık halini elde etmeye çalışan kriptoloji disiplinidir.
- **Encoding:** Verinin başka bir forma dönüştürülmesidir. (şifreleme yapılmamaktadır.) **base64** gibi.
- **Stenografi:** Verinin başka veri içerisinde saklanmasıdır. (Bilgi şifrelenmez, gizlenir.)
 - Stenografi alfabesi ile yazılması şeklinde kullanılır.

Atbash şifrelemesi

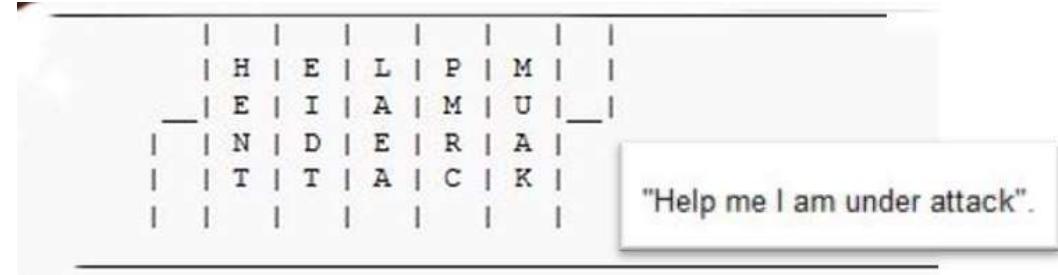
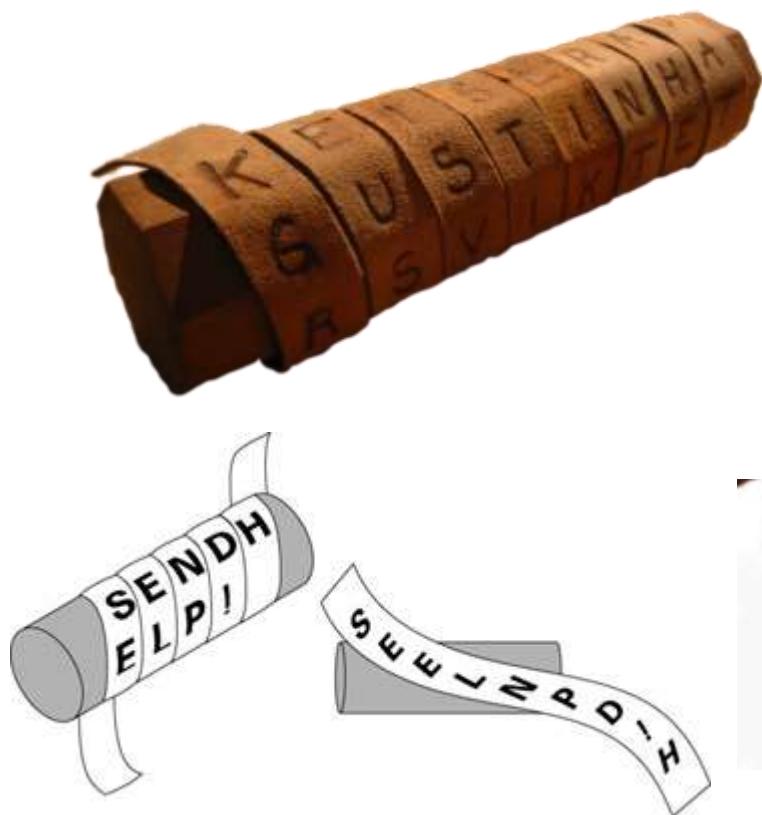
A	B	C	D	E	F	G	H	I	J	K	L	M
Z	Y	X	W	V	U	T	S	R	Q	P	O	N
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
M	L	K	J	I	H	G	F	E	D	C	B	A

Sezar Şifresi (Çevrimisel Alfabe)



- Kaba kuvvet (brute-force) saldırısıyla çok kolay çözülür.
- Çünkü, Şifreleme/Şifre çözme yöntemi gizli değildir.
- Sadece 25 farklı deneme yeterlidir. (Anahtar uzayı 25 elemanlıdır.)
- Düz metin (plaintext) ve formatı gizli değildir.
- Harf değiştirme şifrelemelerinde toplam $26!$ farklı şifre tablosu vardır.

Scytale Cipher (Sarmal Şifrelemesi)



Çok Alfabeli (Polyalphabetic) Şifreleme

Çok alfabeli şifreleme(polyalphabetic Cipher): 1467 yılında Leon Battista Alberti tarafından bulunmuştur. Yerdeğiştirmeye dayalı bir şifrelemedir. Bunların en bilineni vigenere şifresidir.

Örnek (Türk alfabetesine göre):

Düz Metin : S A L D I R I Ş A F A K T A

Anahtar : L İ M O N L İ M O N L İ M O

Şifreli Metin : F İ A S V E S Ğ O Ş L U H O

Base64

- Verinin başka bir forma dönüştürülmesidir.
(Encoding) Şifreleme yapılmamaktadır.
- ASCII karakterlerini kullanan ortamlarda iletilmesine ve saklanmasına olanak tanıyan bir kodlama şemasıdır.

Base64 Encoding Table

Value	Char	Value	Char	Value	Char	Value	Char
0	A	16	Q	32	g	48	w
1	B	17	R	33	h	49	x
2	C	18	S	34	i	50	y
3	D	19	T	35	j	51	z
4	E	20	U	36	k	52	0
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	J	25	Z	41	p	57	5
10	K	26	a	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	s	60	8
13	N	29	d	45	t	61	9
14	O	30	e	46	u	62	+
15	P	31	f	47	v	63	/

Stenografi

Orijinal Resim



Gizlenmiş Resim



<http://stylesuxx.github.io/steganography/>

Terimler ve Kavramlar

- **Açık Metin**(clear text): Şifrelenmemiş, bir insanın okuyabileceği yazı veya verilerdir.
- **Şifreli Metin**(ciphered text): Bir kripto algoritması kullanılarak herkesin okuyamayacağı bir şekilde kodlanmış bilgiye denir.
- **Şifreleme**: Açık metinden şifreli metne geçme işlemidir.
- **Şifre Çözme**: Şifreli metinden açık metne geçme işlemidir.

Şifreleme -> Deşifreleme

(Encryption -> Decryption)

Açık Metin
(Plaintext)



Şifreleme
(Encryption)

Şifreli Metin
(Ciphertext)



Deşifreleme
(Decryption)

Açık Metin
(Plaintext)

Terimler ve Kavramlar

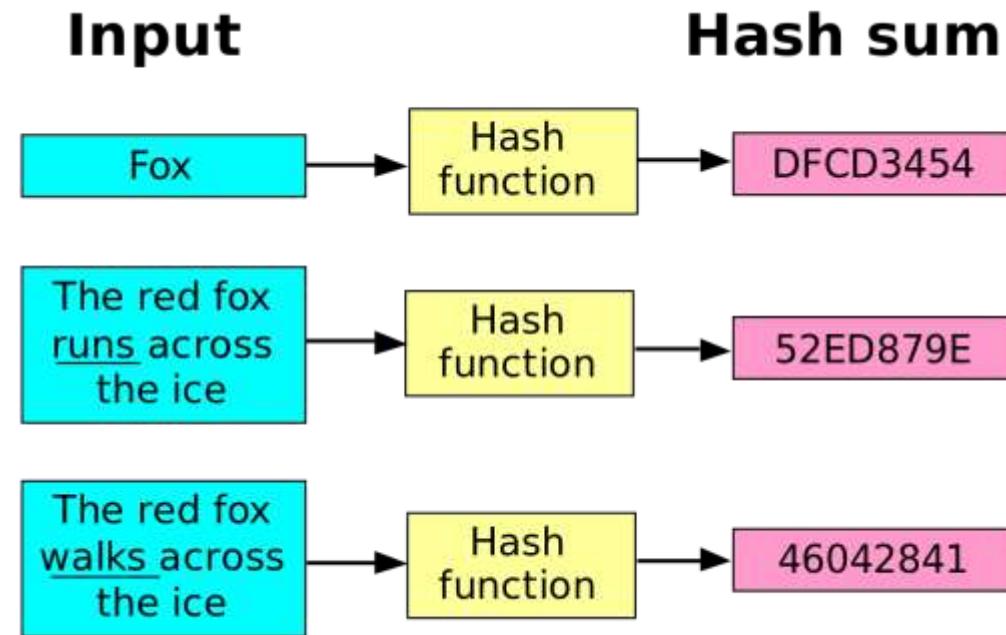
- **Simetrik Şifreleme:** Hem şifreleme hem de deşifreleme için aynı anahtarı kullanan kripto sistemleridir.
- **Asimetrik Şifreleme:** Kişiye genel ve özel anahtarı ile şifrelenip gönderilir, kişi kendi özel anahtarı ile deşifre eder.

Kripto(Kriptografik) Sistemler

- Anahtarsız Şifreleme (Keyless Encryption)
 - MD5, SHA-1, RIPEMD-160, ..
- Simetrik (Gizli) Anahtarlı Şifreleme (Private Encryption)
 - Blok Şifre Sistemleri (AES, DES, IDEA, Camellia..)
 - Akan Şifre Sistemleri (RC4(Wep), A5/1(Gsm), A5/2..)
- Asimetrik (Açık) Anahtarlı Şifreleme (Public Encryption)
 - İmzalama Algoritmaları (DSA, ECDSA, RSA..)
 - Anahtar Paylaşım Algoritmaları (RSA, DH, Eliptik..)

Hash (Özet Fonksiyon)

Hash fonksiyonu, değişken uzunluklu veri kümelerini, sabit uzunluklu veri kümelerine haritalayan algoritma veya alt programdır.



MD5

MD5 (Message-Digest Algorithm 5),

- Bir şifreleme yöntemi değil, bir hash fonksiyonudur.
- Herhangi bir uzunlukta verilen mesajı (veya dosyayı) alıp fazla uzun olmayan bir harf ve sayı dizisine çevirir.
- (Kısaca, Girilen verinin boyutundan bağımsız olarak, 128-bit özet değeri üretir.)

Hash ve Salting (Özet+Tuzlama)

	Kullanıcı 1	Kullanıcı 2	Kullanıcı 1	Kullanıcı 2
Password	bob	bob	bob	bob
Salt	-	-	et52ed	ye5sf8
Hash	f4c31aa	f4c31aa	lvn49sa	z32i6t0

Acaba Nedir? (*Dersin Özeti*) - **CEVAP**

w5bEn3JlbtNplGhhesSxciBvbGR1xJ91bm
RhIMO2xJ9yZXRtZW4gZ8O2csO8bmVjZWt0aXlu
VGhIEJ1ZGRoYQ==

Base 64 – Encode

Öğrenci hazır olduğunda öğretmen görünecektir.

The Buddha

6. Hafta

ADLI BİLİŞİM (FORENSIC)



Adli Bilişim

- Adli Bilişim
- (Computer Forensics) [Digital Forensics]
- Forensic, “mahkemeye ilgili, adli”
- Bilgisayar Kriminalistiği bilimi,
- Bir bilişim sisteminde bulunan bilgilerin mahkemedede/soruşturma biriminde suçun veya suçsuzluğun ispatlanmasıında kullanılmak üzere incelenmesi olarak tanımlanmaktadır .

Adli Bilişim

Elektromanyetik ve elektro optik ortamlarda muhafaza edilen veya bu ortamlarca iletilen ses, görüntü, veri, bilgi veya bunların birleşiminden oluşan her türlü bilişim nesnesinin, mahkemede sayısal delil niteliği taşıyacak şekilde tanımlanması, elde edilmesi, saklanması, incelenmesi ve mahkemeye sunulması çalışmaları bütündür.

Adli Bilişim Alt Dalları

- **Bilgisayar Adli Bilimi (Computer Forensics)**
- **Dosya Sistemi Adli Bilimi (File System Forensics)**
 - FAT12, FAT16, FAT32 Forensics
 - NTFS Forensics
 - exFAT Forensics
 - HFS+ Forensics
 - EXT2, EXT3, EXT4 Forensics
- **İşletim Sistemi Adli Bilimi (OS Forensics)**
 - Windows Adli Bilimi (Windows Forensics)
 - Unix&Linux Adli Bilimi (Unix&Linux Forensics)
 - MacOSx Adli Bilimi (MacOSx Forensics)
- **Ağ Adli Bilimi (Network Forensics)**
- **Mobil Cihaz Adli Bilimi (Mobile Forensics)**
- **Kötü Yazılım Adli Bilimi (Malware Forensics)**
- **Geçici Bellek Adli Bilimi (Memory Forensics)**

Suç veya Delil

- Bilgisayar Sistemlerine Yetkisiz Erişim,
- Sistemi Bozma,
- Bilgisayar Sabotajı,
- Bilgisayar Yoluyla Dolandırıcılık,
- Bilgisayar Yoluyla Sahtecilik,
- Bilgisayar Yazılımlarının İzinsiz Kullanımı,
- Şirket İçi Yolsuzlukların Tespiti,
- Boşanma Davalarında Eşlerin Aldatmasının İspatlanması,
- Vb..

Hukuki Açıdan Adli Bilişim

TCK (Bilişim Suçları)

- Madde 243. - Yetkisiz Erişim - Sisteme Girme
- Madde 244. - Verileri Engelleme, Bozma, Değiştirme, Yok etme.
- Madde 245. - Kredi Kartı ve Banka'ya karşı işlenen suçlar .

TCK (Bilişim Vasıtalı Suçlar)

- Madde 124. - Haberleşmenin engellenmesi
- Madde 125. - Hakaret
- Madde 132. - Haberleşmenin Gizliliğini İhlal.
- Madde 133. - Kişiler arası konuşmaların dinlenmesi ve kayda alınması.
- Madde 135. - Kişisel verilerin kaydedilmesi.
- Madde 136. - Verileri hukuka aykırı olarak verme veya ele geçirme
- Madde 142. - Nitelikli Hırsızlık.
- Madde 158. - Nitelikli Dolandırıcılık.
- Madde 226. - Müstehcenlik.

Fikir ve Sanat Eserleri Kanunu

- Madde 71 - Manevi Haklara Tecavüz.
- Madde 72 - Mali Haklara Tecavüz.
- Madde 73 - Diğer Suçlar.



Ceza Muhakemesi Kanunu

- Madde 134. - Bilgisayarlarında, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve el koyma.

Dijital Delil (e-delil)

Dijital/elektronik delil (e-delil),

- Bir elektronik araç üzerinde saklanan veya bu araçlar aracılığıyla iletilen soruşturma açısından değeri olan bilgi ve verilerdir .



Dijital Deliller (e-delil)

- Fotoğraflar
- Video görüntüleri
- Office, Pdf vb. dosyalar
- Çeşitli bilgisayar programları (hack programları)
- İletişim kayıtları (SMS, Skype, Whatsapp, vb. kayıtları)
- Gizli ve şifreli dosyalar
- Dosyaların oluşturulma, değiştirilme ve erişim tarih kayıtları
- Son girilen ve sık kullanılan internet siteleri
- İnternet ortamından dosyalar
- Silinmiş dosyalar
- Haritalar / GPRS cihazları

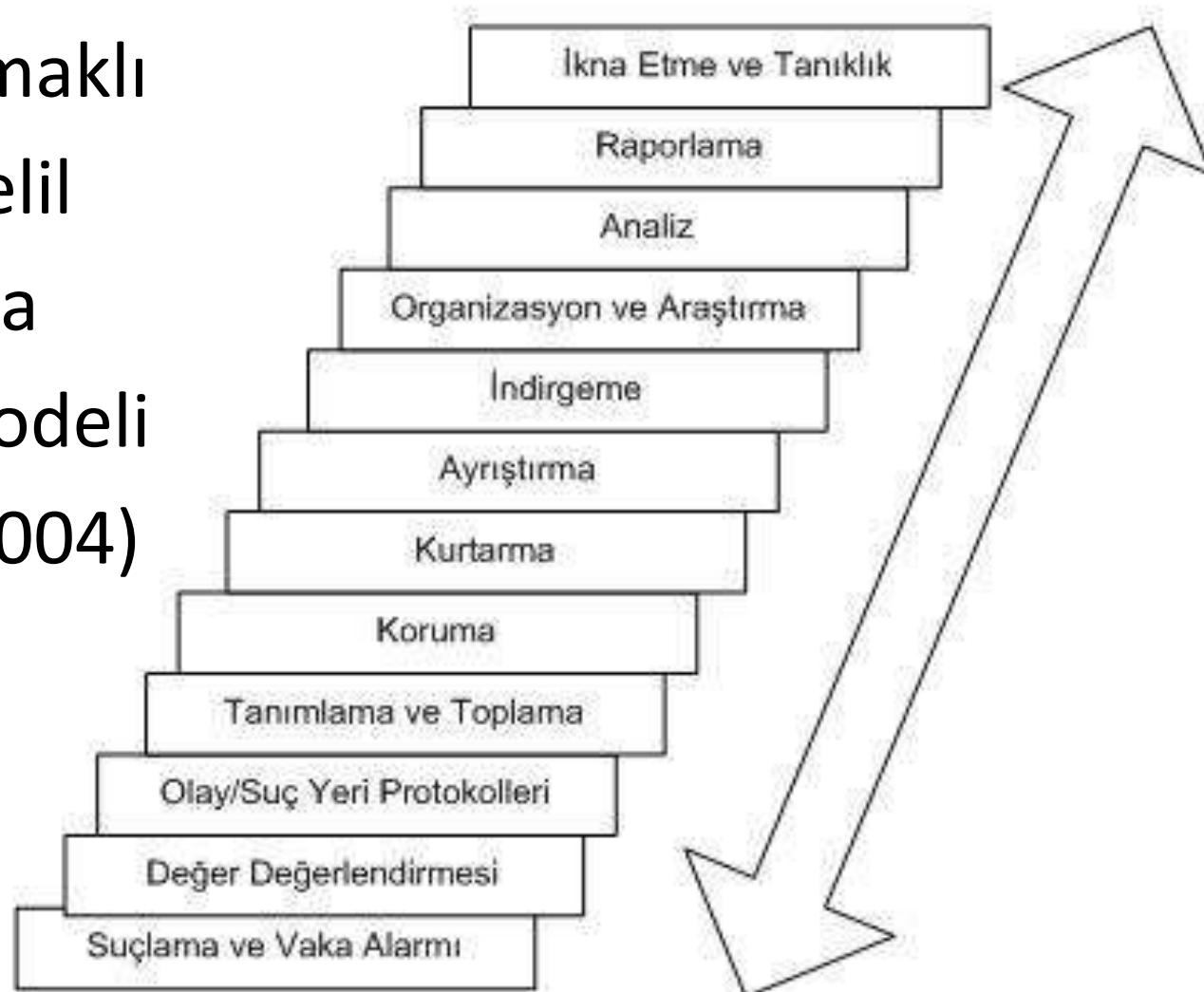
Dijital Delil Ortamları

- Depolama
 - Sabit Disk (HDD)
 - Usb Flash
 - Hafıza Kartı
 - CD/DVD
 - Floppy
 - Telefon/SIM kart
 - Yazıcı
 - Modem
 - Oyun konsolu
- Uçucu Veriler
 - RAM
 - Protokol, Port, IP
 - Sistem tarihi/saatı
 - Kullanıcı adı, işlemler, açık/çalışan dosyalar
 - Pagefile.sys dosyası



Dijital Delil Süreç Modeli

12 basamaklı
Dijital Delil
Araştırma
Süreç Modeli
(Casey 2004)



Adli Bilişim Süreçleri/Safhaları

- Olaya müdahale
 - Toplama (Collection)
 - Korumaya alma
 - Delil tespiti
 - Elde etme
- Laboratuvar incelemesi
 - İnceleme (Examination)
 - Çözümleme (Analysis)
 - Raporlama (Reporting)

Delil Toplamadan Önce..

- İncelenenek Bilgisayar **Kapalı** ise;
 - Fotoğrafı çekilir, kablolar işaretlenir,
 - Elektrik, Kesintisiz güç kaynağı, batarya kontrol edilip fişi çekilmelidir. (*Bilgisayar Açılmamalıdır.*)
- İncelenenek Bilgisayar **Açık** ise;
 - Ekran görüntüsünün fotoğrafı çekilir,
 - Ram imajı alınmalı,
 - Uzak erişim engellenmeli,
 - Açıkta erişim, hesap, sosyal medya vb. var ise kontrol edilmeli,
 - Veri uçuculuğu sırasına göre inceleme yapılmalı

Olay Yerinde YapılmaMASı Gerekenler

- Bilgisayarı çalıştırılmak, veya bir uygulamayı Açımak/Kapatmak
- Bilgisayarın sahibinden yardım istemek,
- Virüs kontrolü yapmak,
- Yazıcı çıktısı almaya çalışmak,
- Delil nakliye önlemi almamak,

Paketleme-Nakliye-Muhafaza

- Isıya,
- Rutubete,
- Fiziksel şoklara,
- Statik elektriğe,
- Manyetik kaynaklara



Duyarlı önlemlerle, veri bütünlüğünü bozmayacak şekilde, belgelendirip nakliyesi sağlanmalıdır.

İnceleme (Tanımlama)

- Adli kopya (İmaj Alma) işlemi sonrası orijinal veri/yapı üzerinde hiçbir işlem yapılmaz.
- İmaj üzerinde incelemeler yapılır.
- Disk yazma koruması yapılmalıdır.
- Disk sürücülerinin (verilerin) bütünlüğünü tek yönlü veri akışı ile koruyup yazma engellenmelidir.

Disk Yazma Koruma İşlemi

- Disk ile arasında köprü vazifesi görür ve incelemeye yazmaya engel olur.
- Donanımsal
- Yazılımsal



İmaj Alma

- Adli bilişimde yapılan birebir kopyalama işlemine imaj / adli kopya (forensic image) denilmektedir.
- Düşük seviye bit bazında kopyalama yapılması gereklidir.
- Silinmiş verilere de erişim imkanı sağlar.
- İmajın birebir aynı olması Hash değeri ile korunur. (MD-5, SHA-1)

Adli Kopya (İmaj Alma)

- Donanımsal
 - TABLEAU- TD1, TD2 ve TD3
 - Ditto
 - ATOLA
 - DEEPSPAR
 - ICS - SOLO 4
 - LOGICUBE
 - Yazılımsal
 - Forensic Toolkit (**FTK**)
 - Safeback
 - (DOS) “dd”, Linux “dd”
 - **Encase**
 - Forensic Replicator
 - PDA Seizure
 - Pdd (Palm dd, Windows, Free)
 - WinHex
 - Image (DOS)
 - SMART (Linux Redhat)
 - ByteBack (DOS)
 - Anadisk
 - ILook
 - Automated Image & Restore
- 

Çözümleme/Analiz

- Mevcut Dosyaların Çıkarılması
- Silinmiş Dosyaların Çıkarılması
- Unallocated alandaki verilerin çıkarılması
- İnternet Aktivitelerinin Tespit Edilmesi
- Gizlenmiş Verilerin Bulunması
- Şifreli ve Encrypted Dosyaların Çözülmesi
- Stegonografi Uygulanmış Verilerin Tespiti
- Geçici Dosyaların analizi
- Swap Alanın İncelenmesi
- Log İncelemeleri
- Zararlı Kodların İncelenmesi
- Kelime Arama İşlemleri
- Sisteme Neler Kurulmuş ve Hangi
- Donanımlar Takılı Olduğu



Çözümleme/Analiz Yazılımları

- ENCASE
- FTK
- XWAYS FORENSİC
- FORENSIC EXPLORER
- IEF
- GET DATA
- ACTIVE PARTITION RECOVERY
- WINHEX
- OXYGEN FORENSIC
- CD/DVD INSPECTOR



X-Ways

Çözümleme/Analiz Donanımları

- Cellebrite
- Salvation Data
- Atola
- Deepspar
- PC3000



Raporlama

- Ayrıntılı olarak dijital delillerin nasıl elde edildiğine ilişkin teknik boyutu ve adli bilişimin hangi metodlarının kullanıldığı da anlaşılır bir dille belirtilmesi gerekmektedir .
- Raporda araştırmancının yapıldığı zaman dilimi, incelenen elektronik deliller ve araştırma sonunda ele geçen bulgulara ilişkin bilgiler yer almalıdır.

Anti-Forensic

- Deliller üzerinde adli bilişim süreçlerinin başarılı olmaması için geliştirilen yöntemlerdir.
 - Dosya gizleme,
 - Dosya silme(geri dönüşsüz),
 - Dosya bozma,
 - Forensic uygulamasını devre dışı bırakma
 - Vb..

Adli Bilişim Sertifikasyonları

- EnCase Certified Examiner (ENCE) Guidance Software
- Certified Forensic Computer Examiner (CFCE)
- AccessData Certified Examiner (ACE)
- Certified Computer Examiner (CCE)
- Computer Hacking Forensic Investigator (CHFI)
- Certified Computer Crime Investigator (CCCI)
- Certified Cyber Forensics Professional – (CCFP)
- GIAC Certified Forensic Analyst and Examiner (GCFA & GCFE)



Yazılım Hazırlık

1. VirtualBox (<https://www.virtualbox.org/wiki/Downloads>)

2. Vmware Workstation Player

(https://my.vmware.com/en/web/vmware/free#desktop_end_user_computing/vmware_workstation_player/14_0)

3. Kali Linux .iso (<https://www.kali.org/downloads/>)





7. Hafta

SANAL SİBER GÜVENLİK ORTAMI LABORATUVAR VE KURULUMLARI

Sanallaştırma (Virtualization)

Birden fazla işletim sisteminin aynı fiziksel ekipman kaynaklarını paylaşarak çalışmasını ifade eder.

Türleri;

- Sunucu Sanallaştırma (Server Virtualization)
- Depolama Sanallaştırma (Storage Virtualization)
- Ağ Sanallaştırma (Network Virtualization)
- Masaüstü ve Dizüstü Sanallaştırma (Desktop & Laptop Virtualization)
- Uygulama Sanallaştırma (Application Virtualization)

Sanallaştırma Yazılımları

- VMware (VMware)
- VirtualBox (Oracle)
- Hyper-V (Microsoft)
- XenServer (Citrix)
- Xen Project
- OpenVZ



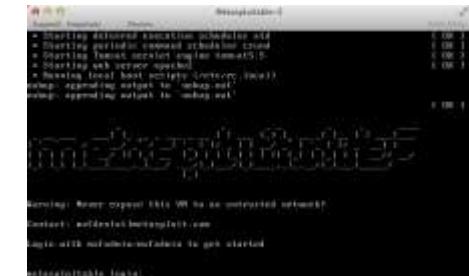
<https://www.virtualbox.org/wiki/Downloads>



Laboratuvar Ortamı

Sanallaştırma yazılımı ile oluşturulan sanal makinaların oluşturduğu ortamdır. Bir Siber Güvenlik Sanal Laboratuvar ortamında bulunabilen sistemler;

- Linux İşletim Sistemleri (Dağıtımları)
 - **Kali**, Debian, Fedora, Ubuntu, Suse, vb..
- Zafiyet Çatı Sistemleri (Vulnerable)
 - **Metasploitable**, Holynix, Kiopritx, Hack2net, vb..
- Microsoft İşletim Sistemleri
 - Windows 7-8-10, 2008-2012-2016 vb..
- Veritabanı Sistemleri
 - MySQL, Ms SQL, Oracle, Postgresql , Nosql , vb..
- Ağ ve Güvenlik Sistemleri
 - Firewall(Checkpoint, Pfsense), IPS/IDS(Suricata, Snort), Roter(Cisco, Juniper), GNS3, vb..
- Kurumsal Uygulama Sunucu Mimarileri
 - Sharepoint, Weblogic, SAP, Apache tomcat, vb..
- Unix İşletim Sistemleri
 - FreeBSD, OpenBSD, Solaris, vb..
- İstemci Uygulamaları
 - Java, PDF, Flash, Browser(Tarayıcılar), vb..
- İçerik Yönetim Sistemleri
 - Wordpress, Joomla, Drupal, vb..
- Antivirüs Sistemleri
 - Kaspersky, Symantec, Bitdefender, McAfee, vb..
- Ağ Hizmetleri
 - DNS, Eposta, FTP, Web-www, VPN, vb..



Kurulumlar

- Sanallaştırma Yazılımı
 - **VMware** Workstation Player (VMware)
veya
 - VirtualBox (Oracle)
- **Kali Linux** Dağıtımı
- Metasploitable2

VMware Workstation Player (14.0.0) Kurulumu

https://my.vmware.com/en/web/vmware/free#desktop_end_user_computing/vmware_workstation_player/14_0 adresinden Vmware indirilir.

The screenshot shows the VMware download page for the Workstation Player. At the top, there's a navigation bar with links for Home, All Downloads, VMware Workstation Player, US, Login, Training, and Help. Below the navigation is a large blue header with the text "Download VMware Workstation Player". Underneath, there are dropdown menus for "Major Version: 14.0 (latest)" and "Minor Version: 14.0.0 (latest)". A navigation menu at the bottom includes "Product Downloads", "Drivers & Tools", and "Open Source". The main content area displays two download options: "VMware Workstation 14.0.0 Player for Windows 64-bit Operating Systems." (exe | 90.73 MB) and "VMware Workstation 14.0.0 Player for Linux 64-bit." (bundle | 110.17 MB). Each option has a "Show Details" link and a prominent blue "Download" button with a downward arrow icon.

https://my.vmware.com/en/web/vmware/free#desktop_end_user_computing/vmware_workstation_player/14_0

Home > All Downloads > VMware Workstation Player

Download VMware Workstation Player

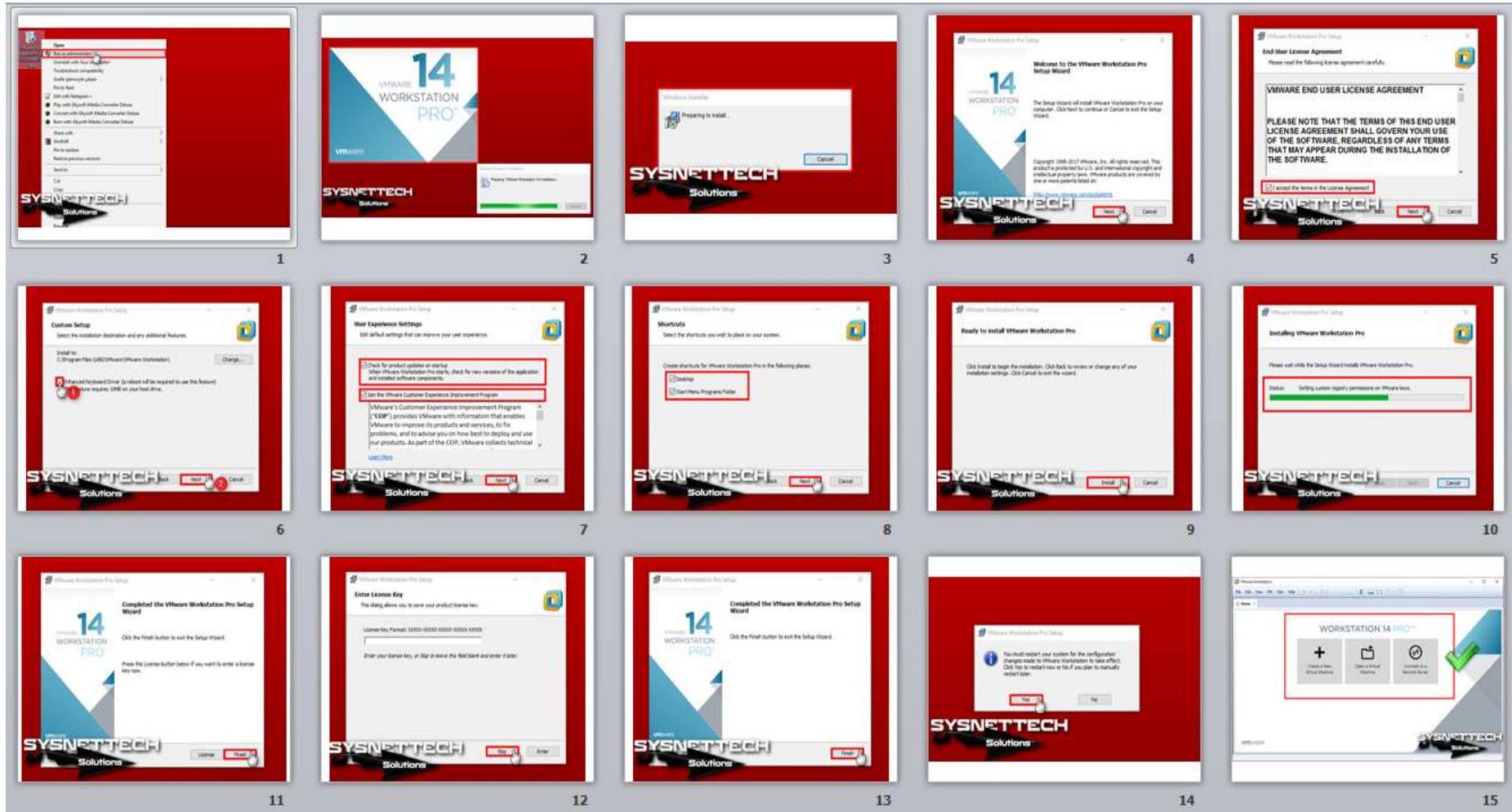
Major Version: 14.0 (latest) ▾ Minor Version: 14.0.0 (latest) ▾

Product Downloads Drivers & Tools Open Source

VMware Workstation 14.0.0 Player for Windows 64-bit Operating Systems.
(exe | 90.73 MB)
Show Details Download

VMware Workstation 14.0.0 Player for Linux 64-bit.
(bundle | 110.17 MB)
Show Details Download

VMware Workstation Player (14.0.0) Kurulumu



Kali Linux (2017.2) Kurulumu

www.kali.org adresinden downloads kısmından .iso imaj dosyası indirilir.

The screenshot shows the official Kali Linux website at <https://www.kali.org/downloads/>. The page features the Kali logo and navigation links for Blog, Downloads, Training, and Documentation. The main content is titled "Kali Linux Downloads" and includes a section for "Download Kali Linux Images". A table lists available image files, with the "HTTP" link for the Kali 32-bit download highlighted by a red box.

Image Name	Download	Size	Version	sha256sum
Kali 64 bit	HTTP Torrent	2.8G	2017.2	4556775bfb981ae64a3cb19aa0b73e8dcac6e4ba524f31c4bc14c9137b99725d
Kali 32 bit	HTTP Torrent	2.9G	2017.2	7f5000d8f55469264399a8bb7358fc22bec87fb1dc8a51b87f26876634e3effc



Player ▾



Home



Metasploitable2-Linux



Kali 2017.2



Windows 7 x64



Parrot

Welcome to VMware Workstation 14 Player



Create a New Virtual Machine

Create a new virtual machine, which will then be added to the top of your library.



Open a Virtual Machine

Open an existing virtual machine, which will then be added to the top of your library.



Upgrade to VMware Workstation Pro

Get advanced features such as snapshots, virtual network management, and more.



Help

View online help.



This product is not licensed and is authorized for non-commercial use only. For commercial use, purchase a license. [Buy now.](#)

Select a Guest Operating System

Which operating system will be installed on this virtual machine?

Guest operating system

- Microsoft Windows
- Linux
- Novell NetWare
- Solaris
- Other

Version

Debian 8.x



Help

< Back

Next >

Cancel

Specify Disk Capacity

How large do you want this disk to be?

The virtual machine's hard disk is stored as one or more files on the host computer's physical disk. These file(s) start small and become larger as you add applications, files, and data to your virtual machine.

Maximum disk size (GB): 

Recommended size for Debian 8.x: 20 GB

- Store virtual disk as a single file
- Split virtual disk into multiple files

Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.

Help

< Back

Next >

Cancel

Ready to Create Virtual Machine

Click Finish to create the virtual machine. Then you can install Debian 8.x.

The virtual machine will be created with the following settings:

Name:	Kali-kurulum
Location:	C:\Users\ KullanıcıAdı \Belgeler\Virtual Machines\Kali...
Version:	Workstation 14.x
Operating System:	Debian 8.x
Hard Disk:	25 GB, Split
Memory:	512 MB
Network Adapter:	NAT
Other Devices:	CD/DVD, USB Controller, Printer, Sound Card

Customize Hardware...

Virtual Machine Settings



Hardware Options

Device	Summary
Memory	512 MB
Processors	1
Hard Disk (SCSI)	25 GB
CD/DVD (IDE)	Using file D:\Siber Güvenlik\İ...
Network Adapter	NAT
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

Device status

 Connected Connect at power on

Network connection

 Bridged: Connected directly to the physical network Replicate physical network connection state

Configure Adapters

 NAT: Used to share the host's IP address Host-only: A private network shared with the host Custom: Specific virtual network

VMnet0

 LAN segment:

LAN Segments...

Advanced...

Add...

Remove

OK

Cancel

Help

KALI

"the quieter you become, the more you are able to hear"

Boot menu

Live (amd64)

Live (amd64 failsafe)

Live (forensic mode)

Live USB Persistence

Live USB Encrypted Persistence

Install

Graphical install

Install with speech synthesis

Advanced options

(check kali.org/prst)

(check kali.org/prst)



Select a language

Choose the language to be used for the installation process. The selected language will also be the default language for the installed system.

Language:

Slovenian	- Slovenščina
Spanish	- Español
Swedish	- Svenska
Tagalog	- Tagalog
Tajik	- Тоҷикӣ
Tamil	- தமிழ்
Telugu	- తెలుగు
Thai	- ภาษาไทย
Tibetan	- བོད་ཡື່ງ
Turkish	- Türkçe
Ukrainian	- Українська
Uyghur	- ئۇيغۇرچە
Vietnamese	- Tiếng Việt
Welsh	- Cymraeg

[Screenshot](#)

[Go Back](#)

[Continue](#)

VMware Tools enables many features and improves mouse movement, video and performance. Log in to the guest operating system and click "Install Tools".

[Install Tools](#)

[Remind Me Later](#)

[Never Remind Me](#)



Ağı yapılandır

Lütfen bu sistemin makine adını girin.

Makine adı, sisteminizi ağa tanıtan tek bir sözcükten oluşmaktadır. Makine adınızın ne olduğunu bilmiyorsanız, sistem yöneticinize başvurun. Eğer kendi ev ağınıizi kuruyorsanız herhangi bir ad kullanabilirsiniz.

Makine adı:

kali



Ağrı yapılandırır

Alan adı, size ait internet adresinin bir bölümündür ve makine adının sağ tarafında yer alır. Bu ad genellikle .com, .net veya .org şeklinde biter. Eğer bir ev ağınız varsa herhangi bir ad seçebilirsiniz; fakat tüm makinelerde aynı alan adını kullandığınızdan emin olun.

Alan adı:

Kullanıcıları ve parolaları oluştur

Sistem yönetici 'root' için bir parola girmeniz gerekiyor. Kötü niyetli veya yetersiz kabiliyetleri olan bir kullanıcının root haklarına sahip olması çok kötü sonuçlar yaratabilir. Bu yüzden kolayca tahmin edilemeyecek bir root parolası seçmeye özen göstermelisiniz. Bu parola sözlükte bulunan ya da sizinle olan alâkasından dolayı kolaylıkla bulunabilecek bir sözcük olmamalıdır.

İyi bir parola harfler, rakamlar ve noktalama işaretlerinin uygun bir kombinasyonundan oluşmalı ve düzenli aralıklarla değiştirilmelidir.

root kullanıcısının parolası boş olamaz. Eğer bu alanı boş bırakırsanız root hesabı devre dışı bırakılacak ve sistemde oluşturulacak ilk normal kullanıcı hesabının "sudo" komutuyla root haklarına sahip olması sağlanacaktır.

Parolayı yazarken parolanın görünmeyeceğini unutmayın.

Root parolası:

Parolayı Göster

Lütfen hatasız yazdığınıizi doğrulamak için aynı root parolasını tekrar girin.

Doğrulamak için parolayı tekrar girin:

Parolayı Göster

Diskleri bölümle

Kurulum programı disk bölümleme konusunda (standart bölümleme şemaları kullanarak) size yardım edebilir; ya da tercih ederseniz elle bölümleme yapabilirsiniz. Bölümleme yardımcısı eşliğinde bölümleme yaparsanız işlemin sonunda hâlâ sonuçları gözden geçirme ve değiştirme şansınız olacaktır.

Eğer bütün bir diskin bölümlenmesinde bölümleme yardımcısını kullanmayı seçmişseniz bir sonraki adımda hangi diskin kullanılacağı size sorulacaktır.

Bölümleme yöntemi:

Yardımcı ile - diskin tamamını kullan

Yardımcı ile - diskin tamamını kullan ve LVM'yi ayarla

Kılavuzla - diskin tamamını şifrelenmiş LVM ile kullan

Elle



Diskleri bölümle

Dikkat! Seçtiğiniz diskteki bütün veriler silinecektir. Fakat bu işlem ancak diskte yapılacak değişiklikleri siz onaylandığınızda gerçekleşecektir.

Bölümlenecek diski seçin:

SCSI1 (0,0,0) (sda) - 26.8 GB VMware, VMware Virtual S



Diskleri bölümle

Bölümlenecek alanı seçin:

SCSI1 (0,0,0) (sda) - VMware, VMware Virtual S: 26.8 GB

Disk birkaç farklı şekilde bölümlenebilir. Emin değilseniz, birinci şemayı seçin.

Bölümleme şeması:

Tüm dosyalar tek bölümde (yeni kullanıcılarla önerilir)

Ayrı /home bölümü

Ayrı /home, /var ve /tmp bölümleri



Diskleri bölümle

Devam etmeniz halinde aşağıda sıralanan bütün değişiklikler disklere kaydedilecektir. Aksi halde bundan sonraki değişiklikleri elle yapacaksınız.

Şu aygıtların bölümleme tabloları değiştirilecek:

SCSI1 (0,0,0) (sda)

Aşağıdaki bölümler biçimlenecek:

SCSI1 (0,0,0) (sda) aygıtının 1 numaralı bölümü ext4 türünde

SCSI1 (0,0,0) (sda) aygıtının 5 numaralı bölümü takas türünde

Değişiklikler diske kaydedilsin mi?

Hayır

Evet



Paket yöneticisini yapılandır

Ağ yansısı CD-ROM'dakilere ilave yazılımlar kurmak için kullanılabilir. Ayrıca mevcut yazılımların yeni sürümlerine de erişmeniz mümkün olacaktır.

Bir ağ yansısı kullanılsın mı?

- Hayır**
- Evet**

GRUB önyükleyiciyi bir sabit diske kur

Görünen o ki bu yeni kurulum bu bilgisayardaki tek işletim sistemi olacak. Eğer öyleyse önyükleyici GRUB'u birincil sabit diskin ana önyükleme kaydına (MBR) kurmanız uygun olacaktır.

Uyarı: Kurulum programı, bilgisayarınızda bulunan diğer bir işletim sistemini algılamakta başarısız olursa, ana önyükleme kaydının değiştirilmesi bu işletim sisteminin geçici olarak açılamamasına yol açacaktır. Bununla birlikte sisteminizin bu işletim sisteminden açılması için GRUB'u daha sonra elle yapılandırabilirsiniz.

GRUB önyükleyici ana önyükleme kaydına (MBR) kurulsun mu?

- Hayır**
- Evet**

GRUB önyükleyiciyi bir sabit diske kur

Şimdi, önyükleme yapılabilecek bir aygıta GRUB önyükleyici kurularak yeni kurulan sistem açılabilir hale getirilecek. Bunu yapmanın alışılmış yolu, GRUB'ı birincil sabit diskinizin ana önyükleme kaydına (MBR) kurmaktır. İsterseniz, GRUB'ı diskte başka bir yere, başka bir diske, hatta bir diskete de kurabilirsiniz.

Önyükleyicinin kurulacağı aygit:

Aygitı elle gir

/dev/sda



Sistem kur

Sistem kuruluyor...

Veriler diske kopyalaniyor...





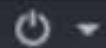
Kurulumu bitir

Kurulum bitiriliyor

remove-live-packages çalıştırılıyor...

Kullanıcı Adı:

Sonraki



Parola:

••••| 

 İptal



Giriş



Metasploitable

<https://sourceforge.net/projects/metasploitable/files/Metasploitable2/>

The screenshot shows the SourceForge project page for 'Metasploitable'. The URL in the address bar is <https://sourceforge.net/projects/metasploitable/files/Metasploitable2/>. The page features the SourceForge logo and navigation links for 'Search', 'Browse', 'Enterprise', and 'Blog'. Below the header are 'SOLUTION CENTERS' and other resource links like 'Resources', 'Newsletters', 'Cloud Storage Providers', and 'Business VoIP Providers'. The main content area displays the project title 'Metasploitable' with a file icon, a brief description stating it's an intentionally vulnerable Linux virtual machine, and credit to 'Brought to you by: rapid7user'. A red box highlights the download link 'Download metasploitable-linux-2.0.0.zip (873.1 MB)'.

[Home](#) / [Browse](#) / [Security & Utilities](#) / [Security](#) / [Metasploitable](#) / [Files](#)



Metasploitable

Metasploitable is an intentionally vulnerable Linux virtual machine
Brought to you by: [rapid7user](#)

[Summary](#) | [Files](#) | [Reviews](#) | [Support](#) | [Wiki](#)

Looking for the latest version? [Download metasploitable-linux-2.0.0.zip \(873.1 MB\)](#)

[Home](#) / [Metasploitable2](#)

Name	Modified	Size	Downloads / Week
Parent folder			
README.txt	2012-06-13	569 Bytes	207 
metasploitable-linux-2.0.0.zip	2012-05-21	873.1 MB	6,375 
Totals: 2 Items		873.1 MB	6,582

VMware Workstation 14 Player (Non-commercial use only)

Player ▾ | ▶ ⌂ ⌃ ⌄ ⌅

 Home

 Kali-Linux-2-TR

 Metasploitable2-Linux

 Puupy

 Pardus

Welcome to VMware Workstation 14 Player

 **Create a New Virtual Machine**
Create a new virtual machine, which will then be added to the top of your library.

 **Open a Virtual Machine**
Open an existing virtual machine, which will then be added to the top of your library.

 **Upgrade to VMware Workstation Pro**
Get advanced features such as snapshots, virtual network management, and more.

 **Help**
View online help.

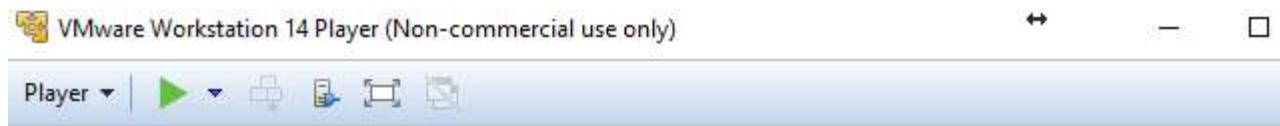
> Metasploitable2-L... ▾ 🔍 Ara: Metasploitable2-Linux 🔎

☰ ?

Ad	Değiştirme tarihi	Tür
Metasploitable.vmx	24.10.2017 23:44	VMware v

All supported files (*.vmx; *.vmc)

Aç İptal



Metasploitable2-Linux

State: Powered Off

OS: Ubuntu

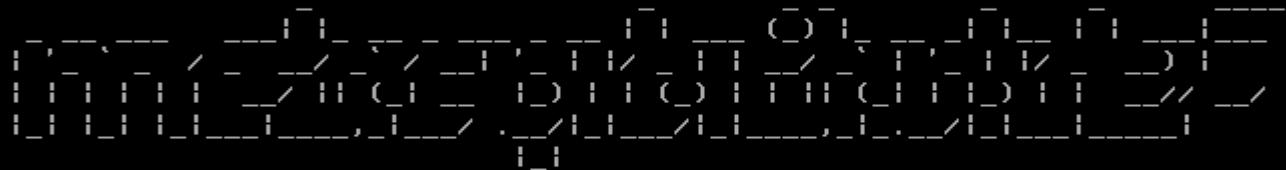
Version: Workstation 6.5-7.x virtual machine

RAM: 512 MB

Play virtual machine

Edit virtual machine settings

```
* Starting deferred execution scheduler atd [ OK ]
* Starting periodic command scheduler crond [ OK ]
* Starting Tomcat servlet engine tomcat5.5 [ OK ]
* Starting web server apache2 [ OK ]
* Running local boot scripts (/etc/rc.local)
nohup: appending output to 'nohup.out'
nohup: appending output to 'nohup.out' [ OK ]
```

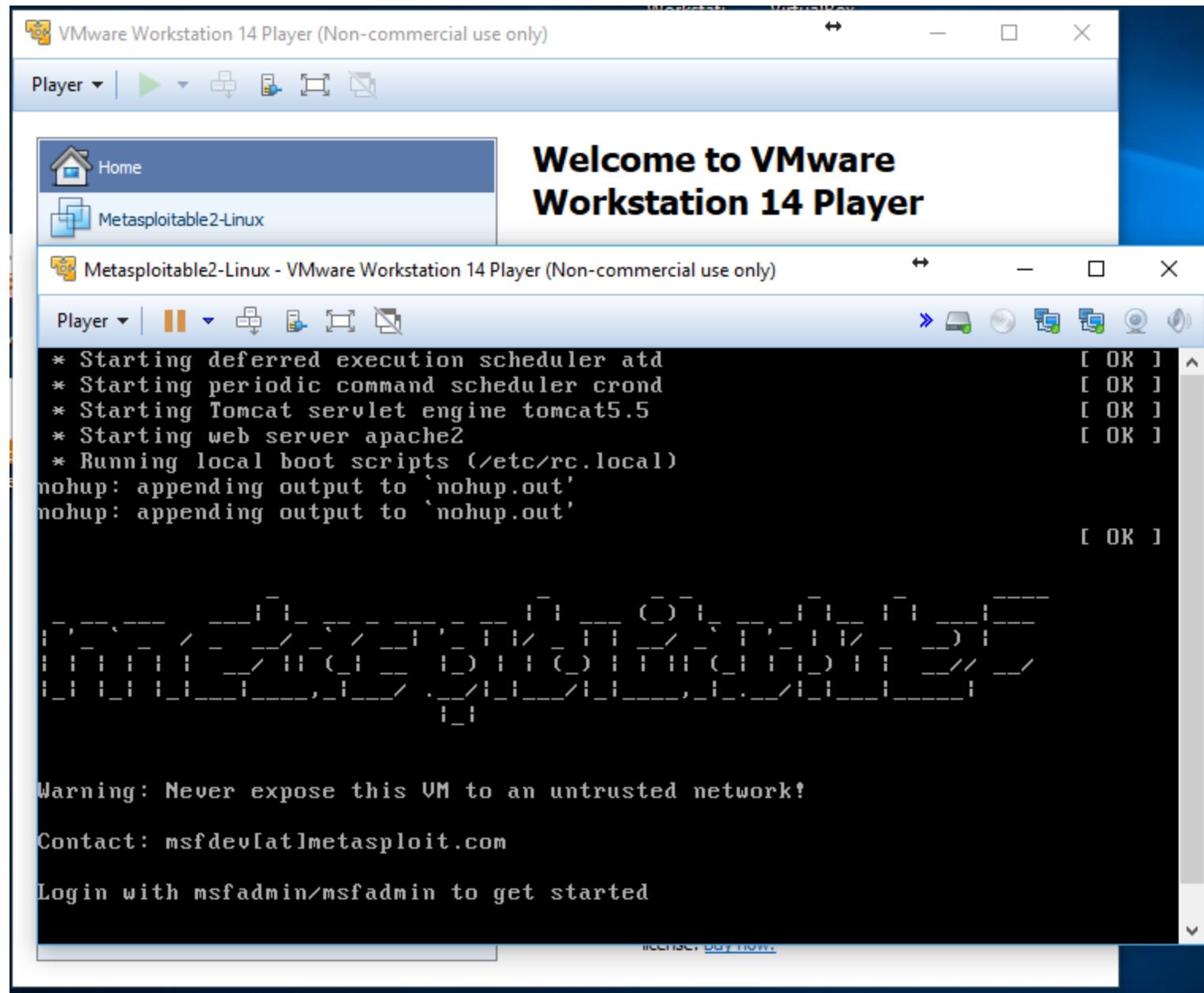


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

metasploitable login:



```
Login with msfadmin/msfadmin to get started
```

```
metasploitable login: msfadmin_
```

```
Login with msfadmin/msfadmin to get started
```

```
metasploitable login: msfadmin  
Password:
```

```
Contact: msfdev[at]metasploit.com
```

```
Login with msfadmin/msfadmin to get started
```

```
metasploitable login: msfadmin
```

```
Password:
```

```
Last login: Tue Oct 24 16:38:24 EDT 2017 on tty1
```

```
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
```

```
The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*copyright.
```

```
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.
```

```
To access official Ubuntu documentation, please visit:
```

```
http://help.ubuntu.com/
```

```
No mail.
```

```
To run a command as administrator (user "root"), use "sudo <command>".  
See "man sudo_root" for details.
```

```
msfadmin@metasploitable:~$ _
```

Metasploitable2 - Linux

192.168.72.130

Google



Most Visited ▾ Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng



Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

- [TWiki](#)
- [phpMyAdmin](#)
- [Mutillidae](#)
- [DVWA](#)
- [WebDAV](#)