**T.C.**

**TRAKYA ÜNİVERSİTESİ**

**FEN BİLİMLERİ ENSTİTÜSÜ**

**OSI – Oturum ve Sunum Katmanları**

**KENAN BAYSAL**

**BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİMDALI**

**EDİRNE,2011**

İçindekiler Tablosu

[1 Giriş 1](#_Toc310374164)

[2 Sunum Katmanı 2](#_Toc310374165)

[2.1 Ortak Uygulama Servis Elemanı (CASE) 3](#_Toc310374166)

[2.2 Özel Uygulama Servis Elemanı (SASE) 3](#_Toc310374167)

[2.3 Protokoller 4](#_Toc310374168)

[2.3.1 Apple Filling Protocol - AFP 4](#_Toc310374169)

[2.3.2 Independent Computing Architecture – ICA 4](#_Toc310374170)

[2.3.3 Lightweight Presentation Protocol –LPP 5](#_Toc310374171)

[2.3.4 NetWare Core Protocol – NCP 5](#_Toc310374172)

[2.3.5 Network Data Representation – NDR 5](#_Toc310374173)

[2.3.6 Telnet 5](#_Toc310374174)

[2.3.7 External Data Representation - XDR 6](#_Toc310374175)

[2.3.8 X.25 7](#_Toc310374176)

[2.3.9 Abstract Syntax Notation One - ASN.1 8](#_Toc310374177)

[3 Oturum Katmanı 9](#_Toc310374178)

[3.1 Protokoller 10](#_Toc310374179)

[3.1.1 AppleTalk Data Stream Protocol - ADSP 10](#_Toc310374180)

[3.1.2 AppleTalk Session Protocol – ASP 11](#_Toc310374181)

[3.1.3 H.245 11](#_Toc310374182)

[3.1.4 ISO-SP (X.225, ISO 8327) 12](#_Toc310374183)

[3.1.5 Internet Storage Name Service - iSNS 13](#_Toc310374184)

[3.1.6 Layer 2 Forwarding Protocol – L2F 14](#_Toc310374185)

[3.1.7 Layer 2 Tunneling Protocol – L2T 14](#_Toc310374186)

[3.1.8 NetBIOS – Network Basic Input/Output System 15](#_Toc310374187)

[3.1.9 Password Authentication Protocol -PAP 16](#_Toc310374188)

[3.1.10 Point-to-Point Tunneling Protocol – PPTP 16](#_Toc310374189)

[3.1.11 Remote Procedure Call – RPC 17](#_Toc310374190)

[3.1.12 Real-Time Transport Control Protocol – RTCP 19](#_Toc310374191)

[3.1.13 Short Message Peer-to-Peer Protocol – SMPP 20](#_Toc310374192)

[3.1.14 SOCKS Protocol 20](#_Toc310374193)

[3.1.15 Zone Information Protocol – ZIP 20](#_Toc310374194)

[3.1.16 Sockets Direct Protocol – SDP 21](#_Toc310374195)

[4 Sonuç 21](#_Toc310374196)

**Şekiller Listesi**

[Şekil 1.1 7 Katmanlı OSI Referans Modeli 1](#_Toc309488141)

[Şekil 2.1 X25 Ağ Mimarisi 7](file:///C%3A%5CUsers%5CKenan%20BAYSAL%5CDesktop%5COSI%5CKenan%20BAYSAL%20Sunum%20ve%20Oturum%20Katman%C4%B1.docx#_Toc309488142)

[Şekil 3.1 AppleTalk OSI Referans Modelinde Protokol Dağılımı 10](file:///C%3A%5CUsers%5CKenan%20BAYSAL%5CDesktop%5COSI%5CKenan%20BAYSAL%20Sunum%20ve%20Oturum%20Katman%C4%B1.docx#_Toc309488143)

[Şekil 3.2 iSNS sunucu ve istemcileri ile bir IP depolama ağı 13](file:///C%3A%5CUsers%5CKenan%20BAYSAL%5CDesktop%5COSI%5CKenan%20BAYSAL%20Sunum%20ve%20Oturum%20Katman%C4%B1.docx#_Toc309488144)

[Şekil 3.3 L2F Paket Yapısı 14](#_Toc309488145)

[Şekil 3.4 L2TP Paket Yapısı 15](#_Toc309488146)

[Şekil 3.5 RPC mimarisi 17](#_Toc309488147)

# Giriş

Bilgisayar teknolojisinin baş döndürücü bir hızla geliştiği günümüzde, artan bilgisayar sayısı ile birlikte bu bilgisayarların iletişim kurma ihtiyacına yönelik olarak ağ bağlantı protokolleri geliştirilmiştir.

Ağ mimarilerinin bilimsel temelini oluşturan “Açık Sistemler Ara bağlantısı Başvuru Modeli *(Open System Intercorrect Referance)*” ya da kısa adıyla OSI, 1983 yılında ISO tarafından yayınlanmıştır. [1]

Bu ağ mimarisi modeli yedi katmanlı bir yapıdan oluşmaktadır. Protokol, hizmet, arayüz ve diğer bir dizi işlem bu katmanlı yapıda sistematik olarak tanımlandırılmıştır. Her işlev için ihtiyaca göre farklı hizmet ve protokoller oluşturulabilir durumdadır. [2]

Şekil 1,1’de OSI 7 katmanı gösterilmiştir. [3]

Şekil . 7 Katmanlı OSI Referans Modeli

# Sunum Katmanı

Yedi katmanlı OSI referans modelinde Sunum Katmanı altıncı katman olarak Uygulama Katmanının hemen altında yer alır ve veri dönüştürücü olarak görev yapar. Gelen ve giden verileri iki tarafında anlayacağı standart bir gösterime dönüştürür.

Sunum katmanı, uygulama katmanına veri işleme veya görüntüleme için veri ulaşımı ve veri düzenleme işlerinden sorumludur. Son kullanıcı için veri sunumu yapacak olan uygulama katmanına gönderilecek olan verinin sözdizimsel farklılıklarını düzenler. Örneğin EBCCDIC kodlanmış bir bilgisayar dosyasını ASCII koduna dönüştürerek uygulama katmanına sunar. Yalın veri yapıları (sayı, tarih vb.) gösterimler ile birlikte karmaşık veri yapıları (alındı, fatura vb.) üzerinde de bu dönüştürme işlemlerini yapabilmektedir. Veri formatlarında MPEG, GIF, JPEG örnekleri de verilebilir.[4]

Şifreleme işlemi de bu katmanda yapılabildiği gibi uygulama, oturum, ulaşım veya ağ katmanında da yapılabilir. Bu katmanlardaki şifreleme işleminin kendine göre avantaj ve dezavantajları mevcuttur. Şifre çözme işlemi de sunum katmanında gerçekleştirilir. Örneğin banka hesabınıza internet şubesi aracılığı ile oturum açtığınızda veri alındığı gibi şifre çözme işlemi sunum katmanında gerçekleştirilir.

Kullanılan uygulama ve protokollerin geniş bir çoğunluğu uygulama ve sunum katmanı arasında bir ayrım yapmaz. Örneğin genellikle uygulama katmanı protokolü olarak tanımlanan HTTP uygun dönüşüm için karakter kodu tanımlaması kabiliyetine sahip sunum katmanına sahiptir.[5][6]

Sunum katmanı iki alt katmandan meydana gelir;

* CASE *(Ortak Uygulama Servis Elemanı - Common Application Service Element)*
* SASE *(Özel Uygulama Servis Elemanı – Specific Application Service Element)*

## Ortak Uygulama Servis Elemanı (CASE)

CASE alt katman olarak uygulama katmanı için ve oturum katmanı için hizmet sağlar ve oturum katmanı için istek hizmetlerine cevap verir. ACSE, ROSE, CCR, RTSE gibi ortak uygulama servislerine destek sağlar. Bu uygulama servislerinin kısaca işlevleri şunlardır;

* ACSE *(Association Control Service Element)*; iki uygulama programı arasında bağlantı oluşturmak için kullanılan bir OSI metodudur.
* ROSE *(Remote Operation Service Element)*; uzaktan kontrol etme yeteneği sağlar.
* CCR *(Commitment Concurrency and Recovery)*; dağıtılmış sistemler arasında atomik işlemler oluşturmak amacıyla kullanılan bir OSI metodudur.
* RTSE *(Reliable Transfer Service Element)*; toplu verileri sekizli diziler haline dönüştürerek güvenli iletim ortamı oluşturur.

## Özel Uygulama Servis Elemanı (SASE)

SASE alt katmanı uygulamalara özel servisler sunar. Bu servislerden bazıları şöyledir;

FTAM *(File Transfer, Access and Managment Protocol)*; istemci ile sunucu arasında açık bir ortamda dosya transfer hizmeti sağlar. FTAM ayrıca farklı sistemler arasında dosya erişim ve yönetimine destek sağlar. TCP/IP ortamındaki FTP (File Transfer Protocol) ve NFS (Network File System) benzeri bir yapıdır. FTAM sistemde kullanıcı hakkındaki bağlantı bilgisi oturum bitirilinceye kadar sunucu tarafından devam ettirilir.

VT *(Virtual Terminal)*; klavye, ekran ve yazıcı benzeri cihazlar ile terminal kontrol etmeyi sağlayan host uygulamaları sağlar.

MOTIS (*Message Orinted Text Interchange Standart);* TCP/IP’deki Simple Mail Transfer Protocol (SMTP) benzeri bir işlev görür.

CMIP *(Common Management Information Protocol)*; ağ yönetim uygulamaları ve yönetim aracıları arasında iletişim kurulmasını sağlar.

JTM *(Job Transfer and Manipulation)*; iş transferi ve veri işleme görevi gerçekleştirir.

MMS *(Manufacturing Messaging Service)*; gerçek zamanlı veri işleme için mesajlaşma sistemi, ağ araçları ve bilgisayar programları arasında gözetimli denetim bilgileri sağlar.

RDA *(Remote Database Access)*; veri tabanı erişimi için protokol standardıdır.

DTP *(Disturbuted Transaction Processing)*; iki veya daha fazla ağ sunucusunun dâhil olduğu işlemler topluluğudur. Genellikle işlem yöneticisi, bütün işlemleri kapsayan genel işlem yönetimi ve oluşturulmasından sorumluyken host işlem kaynaklarını sağlar.

## Protokoller

### Apple Filling Protocol - AFP

Mac işletim sistemine dosya paylaşım servisi sağlayan ağ protokolüdür. MAC OS 9 ve öncesinde AFP öncelikli dosya hizmeti protokolü idi. [7]

### Independent Computing Architecture – ICA

ICA, CITRIX firması tarafından geliştirilmiş uygulama sunucu sistemi için özel olarak geliştirilmiş bir protokoldür. Bu protokol istemci ile sunucu arasında geçen verinin özelliklerini hiçbir platforma bağlı kalmadan ortaya koyar. ICA, CITRIX’s WinFrame, CITRIX XenApp ve CITRIX XenDesktop ürünleri için uygundur. Microsoft’un RDP *(Remote Desktop Protocol)* eşdeğeri bir hizmet sunar. Birçok platformda RDP’den daha iyi hizmet sunmaktadır. Çalıştırıldığı sunucu üzerinden istemde bulunan bir sistemin altyapısı üzerinde ayrım yapmaz, Windows, Linux, Mac her türlü durumda ICA sayesinde sunucu üzerinden istemci olarak bağlantı kurabilirler.[8]

### Lightweight Presentation Protocol –LPP

OSI uygulama hizmetlerine çizgi akımı yaklaşım desteği sunan bir protokol olarak tanımlanabilir.

### NetWare Core Protocol – NCP

NCP bazı Novel firması ürünlerinde kullanılan bir ağ bağlantı protokolüdür. Genellikle NetWare işletim sistemi ile ilişkilendirilir. Ancak bazı parçaları Windows NT, Linux ve Unix’in çeşitli biçimlerinde uygulanmıştır.

Dosya erişimi, yazdırma işlemleri, dizin işlemleri, saat senkronizasyonu, mesajlaşma, uzaktan komut yürütme ve benzeri diğer ağ hizmetleri işlemlerinde kullanılır. NCP, Novel eDirectory tarafından sunucular arasındaki dizin hizmetleri ağacı arasındaki veri değişimlerini senkronize etmek için kullanılmaktadır.

### Network Data Representation – NDR

OSI sunum katmanın bir bileşenedir. Ara yüz tanımlama dili *(IDL)* veri tiplerini sekizli dizileri üzerine eşleme tanımlaması yapar.

### Telnet

İnternet veya yerel ağ bağlantısı üzerinden Virtual Terminal bağlantı kullanımında metin odaklı iki yönlü interaktif iletişim hizmeti sunan ağ bağlantı protokolüdür. Uzak bilgisayar üzerinde oturum açma izni sağlar. Protokol sayesinde oturum açılan bilgisayar klavye ve ekranı sanki bağlanılan bilgisayarın bir uçbirimiymiş görev yapar. İlk olarak 1969 yılında RFC 15 başlangıcı ile birlikte geliştirilmiş ve ilk internet standartlarından biri olan, IETF *(Internet Engineering Task Force)* Internet Standart STD 8 olarak standartlaştırılmıştır.

Telnet güvenli bağlantıya yönelik transfere dayanan bir istemci-sunucu protokolüdür. Genellikle bu protokol bir parola eşitleme programının dinlediği TCP port 23 te bağlantıyı tasdik etmek için kullanılır, bununla birlikte telnet TCP/IP den daha eskidir ve ilk olarak NCP(Network Control Program) de çalışmıştır.

5 Mart 1973 ten önce, Telnetin resmi olmayan tanımı bir ad-hoc (router kullanmadan bilgisayarlar arasındaki direk bağlantı kurma) protokolü olarak açıklanıyordu. Aslında Telnet 7 bitlik ASCII verisini göndermek için 8 bitlik kanal kullanıyordu. Yüksek bit setiyle her byte özel bir Telnet karakteriydi. 5 Mart 1973 tarihli UCLA toplantısında "Yeni Telnet" iki NIC dokümanıyla tanımlandı: Telnet Protocol Spesification NIC #15372, ve Telnet Option Spesifications, NIC #15373. Şu anda kullanılan protokol eski telnet protokolü değil bu yeni protokoldür. Bu protokolün internet protokolü olarak benimsenen birçok eklentisi vardır.[9][10]

### External Data Representation - XDR

XDR, bilgisayar ağlarında kullanılan veri kodlama ve tanımlama standart protokolüdür. Farklı bilgisayar mimarileri arasında veri transferi yapma konusunda oldukça kullanışlıdır. Sun Workstation, VAX, IBM-PC, ve Cray gibi birbirinden farklı mimarilere sahip makineler arasında iletişim sağlamakta kullanılmaktadır.

XDR veri formatı tanımlama dili kullanır. Bu dil sadece veri tanımlama işlevi görür, herhangi bir programlama dili gibi bir işlevi yoktur.

Sun Microsystem tarafından 1980’lerin ortasında geliştirilmiş ve 1987’de piyasaya sunulmuştur. 1995 yılında IETF standartlarına girmiştir. [11]

XDR veri türleri;

* Boolean
* İnt-32 bit integer
* Unsigned int – unsigned 32 bit integer
* Hyper – 64 bit integer
* Unsigned Hyper – unsigned 64 bit integer
* IEEE float
* IEEE double
* Quadruple
* Enumeration
* Structure
* String
* Fixed length array
* Variable length array
* Union – discriminated union
* Fixed length opaque data
* Variable length opaque data
* Void – zero byte quantity

### X.25

X.25, anahtarlamalı geniş alan ağları *(WAN – Wide Area Network)* için uygun ITU-T *(International Telecommunication Union)* standart protokolüdür. Hata oranı yüksek, hızı düşük olan şebekeler üzerinde gerçekleştirilen ilk paket anahtarlamalı geniş alan ağ servislerinden biridir. Geniş alan servisini sağlayanın kontrolü altında bulunan donanım olan DCE *(Data Circuit Terminating Equipment)* ile kullanıcı taraflı terminal veya bağlantıyı sağlayacak donanım olan DTE arasında tanımlanan bir servistir. Eğer DTE *(Data Terminal Equipment)* X.25 servisinin gerektirdiği fonksiyonları yerine getiremeyen bir donanım ise araya yine ITU-T standartlarında X.3, X.28, X.29 ile tanımlanmış bir PAD donanımı yerleştirilir. Hizmete sunulduğu yıllarda şebeke hata oranlarının yüksek olması sebebiyle her paket anahtarlama noktasının veri bağı katmanında hata kontrolü yapıldığından dolayı veri paketlerinin gecikmesi ve dolayısıyla servis hızının düşmesine sebep oluyordu. Bu sebeplerden dolayı X.25 üst hızı sadece 64Kbps seviyesi ile sınırlı kalmıştır.[12][4]



DTE

DCE

DTE

DCE

DCE

DCE

DTE

DTE

PDA

PSE

PSE

PSE

PSE

X.25 Ağı

Şekil . X25 Ağ Mimarisi

### Abstract Syntax Notation One - ASN.1

OSI referans modelinin sunum katmanında kullanılan, verilerin nasıl gösterildiği, kodlandığı, yollandığı, alındığı ve okunduğunu anlatmaya yarayan standart genişletilebilir bir dildir.

1984 yılında CCITT X.409’un bir parçası olarak ISO ve ITU tarafından standardı sunulmuş, 1988 yılında da X.680 olarak kendi standardına kavuşmuştur.[6]

ASN.1 iki ana bölüm içerir;

* *Özet sözdizimi*; veri yapılarını kesin bir dille tanımlar. Bu sözdizimi programcıya, bit ve byte kavramları ile uğraşmak yerine doğrudan *“integer”*, *“character string”*, *“structer”* cinsinden tanımlama yapmaya imkân sağlar.
* *Transfer sözdizimi*; bir akışını ASN.1 veri nesnesi olarak kodlama tanımlaması yapar.

Genel yapısı itibari ile ASN.1 ileri seviye programlama dilleri ile benzerlik gösterir. Örneğin C dilinde bir struct veri yapısı ile ASN.1 dilinde aynı tip verinin tanımlanması aşağıda görülmektedir.

*C dilinde;*

struct Student {

 char name[50];

 int grad;

 float gpa;

 int id;

 char bday[8];

}

*ASN.1 dilinde;*

Student ::= SEQUENCE{

 name OCTET STRING,

 grad BOOLEAN,

 gpa REAL,

 id INTEGER,

bday OCTET STRING,

}

# Oturum Katmanı

Yedi katmanlı OSI referans modelinde Oturum Katmanı beşinci katman olarak Sunum Katmanının hemen altında yer alır. İki bilgisayarın üzerindeki uygulamaların birbirini tanımladığı katmandır. Bilgisayarlar arası gerekli oturumun kurulması, yönetilmesi ve sonlandırılması işlevlerini yerine getirir. İletişimin mantıksal sürekliliğinin sağlanması için iletişim kopması durumunda bir senkronizasyon noktasından başlayarak iletimin kaldığı yerden devam etmesini sağlar. Gönderilecek bilgi senkronizasyon noktaları ile sınırları belirlenmiş bloklara ayrılır. Karşı ucun oturum katmanı bir bloğun tamamını doğru olarak elde edip bir üst katmana teslim ettikten sonra blokla ilgili işlemi tamamladığını veriyi gönderene bildirir. Gönderen taraf ise bloğu belleğinden silebilir. İletişimin koptuğu durumlarda bağlantı kurulduğunda son senkronizasyon noktasından başlayarak bilgi gönderilir. Birim segmenttir. X.235 veya ISO8327 standartlaştırılmış isimler ile de bilinir. [2] [5]

Oturum katmanı şu hizmetleri sağlar;

* *İletişim Yönetimi*; kimin iletişim sırası olduğuna karar verir.
* *Senkronizasyon*; iki oturum varlığını bilinen bir duruma taşır.

Şekil . AppleTalk OSI Referans Modelinde Protokol Dağılımı

Uygulama

Sunum

Oturum

İletim

Ağ

Veri Bağı

Fiziksel

AFP

ASP

ZIP

ADSP

ATP

AEP

NBP

RTMP

 DDP .

LLAP

ELAP

TLAP

FDDI

LocalTalk

Ethernet Driver

Token ring

 Driver

FDDI

Driver

* *Faaliyet Yönetimi*; faaliyet olarak adlandırılan mantıksal birimler halinde kullanıcıya veri sınırlandırma izni verir.
* *İstisna İşleme*; genel bir hata raporlama mekanizmasıdır.

## Protokoller

### AppleTalk Data Stream Protocol - ADSP

AppleTalk Apple firması tarafından bilgisayarlar arası ağ bağlantısı için özel olarak geliştirilen bir uygulamadır. ADSP, AppleTalk OSI modelinde Oturum katmanında yer alan protokoldür. ADSP kullanılarak istemci uzak uç ile bir bağlantı oluşturabilir, veri gönderebilir veya veri alabilir ve bağlantıyı sonlandırabilir. Ayrıca ADSP, istemcinin kendi içinde kullanabileceği, uyarı mesajı mekanizması sağlar. [4][7]

### AppleTalk Session Protocol – ASP

ASP, AppleTalk uygulamasının oturum katmanında merkezini oluşturur. Biri iş istasyonu biri de sunucu olmak üzere iki ağ varlığı aralarında ASP oturumu oluşturabilirler. Bu iki varlık arasındaki lojik iletişim eşsiz oturum tanımlayıcıları ile tanımlanır. Bağlantı oturum süresince iş istasyonu sunucuya komutlar dizisi gönderir.

ASP hizmetleri ve özellikleri;

* Oturum açma ve oturum kapatma.
* Açık bir oturumda sunucuya komut gönderimi ve dönen komutların yanıtlanması.
* Oturum sonunda iş istasyonundan sunucuya veri blokları yazımı
* Sunucudan iş istasyonuna uyarı gönderimi
* Oturum açılmadan sunucudan hizmet durum bilgisi alınması

ASP komut yorumlama çalıştırma işi yapmaz.

### H.245

H.245,H.323 ve H.324 iletişim oturumları ile birlikte kullanılan ve telefon sinyali olmayan sinyal hat iletimini de içeren kanal kontrol protokolüdür. H.245, şifreleme, akış kontrol, öncelik istekleri ve medya akışında kullanılan lojik kanalların açılıp kapanması gibi multimedya iletişiminde ihtiyaç duyulan bilgi taşıma konusunda kabiliyetlidir.

Sinyalizasyon arama prosedürü aracılığı ile bağlantı kurulduğunda, H245 arama kontrol protokolü arama kurulmadan önce, medya türün çözmek ve medya akışı oluşturmak için kullanılır. Arama kurulduktan sonra da yönetime devam eder. İşlem adımları şu şekildedir; [13][14]

* *Master-Slave Tanımlama İşlemi:* Arama esnasında master ayrımının yapılmasında kullanılır ve arama süresi boyunca hat kontrol çatışmalarının önlenmesini sağlar.
* *Değişim Kapasitesi Prosedürü:* Her bitiş noktası bir sonrakini hangi tür bilginin gönderme ve alma konusunda kapasitesi olduğu konusunda uyarır.
* *Lojik Kanal Prosedürü:* Çoklanmış yollar arası veri transferinde kullanılan bitiş noktaları arasında lojik kanal açma veya kapama için kullanılır.
* *İstek Kipi Komutu:* Konferans boyunca herhangi bir alınan bitiş noktası göndericinin iletim kapasitesi kipini sağlayan iletim bilgi kipinde değişim istediğinde kullanılır.
* *Akış Kontrol Komutu:* Herhangi bir lojik kanalda iletim bit genişliğinde limit aşımı durumunda alıcı tarafından onarım amacıyla kullanılır.
* *İletişim Kipi Mesajları:* Çoklu kontrolör tarafından, çoklı konferans işlemi sırasında ortak kip seçimi için kullanılır.
* *Konferans İstek ve Yanıt Mesajları:* Çoklu konferans işlemi sırasında şifre istekleri gibi verileri kontrol altında tutmak amacıyla kullanılır.
* *Gidiş-Dönüş Gecikme Komutları:* Kontrol kanalı üzerinde iki bitiş noktası arasında gecikme süresini ölçmek için kullanılır.
* *Hızlı Görüntü Güncelleme Komutu:* Veri kaybı durumunda görüntü çerçevelerini hızlıca güncellenmesini sağlar.
* *Oturum Bitiş Komutu:* Bu komutun ardından bitiş noktaları bütün lojik kanalları kapatır.

### ISO-SP (X.225, ISO 8327)

ISO-SP, OSI oturum katmanında, oturum açma kapama gibi konularda oturum yönetimi sağlar. Bağlantının kopması durumunda yeniden bağlantı oluşturmayı sağlar. Eğer oturum uzun bir süre kullanılmadıysa, oturumu bir sonraki kullanıma kadar kapatır. Bu olay üst katmanlarda şeffaf olarak gerçekleşir. Oturum değişim paketlerinin akışında senkronizasyon noktası sağlar.

### Internet Storage Name Service - iSNS

iSNS sunucularda, IP depolama anahtarlarında ve hedef aygıtlarda dağıtılabilir hafif bir keşif protokolü olarak tasarlanmıştır. Bölgeleme ve durum değişim yönetimi olarak da bilinen, IP depolama kaynaklarının kayıt, keşif ve yönetimi sağladığı olanaklardır. İsim kayıt servisi nitelik ve adreslerini analogdan fiber kanala olacak şekilde kayıt edilmesi için IP depolama aygıtlarını aktif hale getirir. Olası hedeflerin kimliklerini iSNS sorgular. Bölgeleme keşif domainleri tarafından sağlanır.

Şekil . iSNS sunucu ve istemcileri ile bir IP depolama ağı





Yönetim platformu

iFCP geçidi

iFCP geçidi

FC anahtarı

FC diskleri

FC sunucu

FC sunucu

iFCP geçidi

iSNS

IP Network

iSCSI aygıtı

iSCSI aygıtı

Şekilde görüldüğü gibi iSNS sunucusu, iFCP ve iSCSI istemcileri tarafından erişilebilir olarak, IP network ile herhangi bir yerde bulunabilir. Bir veya daha fazla yönetici iş istasyonu iSNS sunucusuyla iletişim halinde olabilir. [15]

### Layer 2 Forwarding Protocol – L2F

Cisco System tarafından, özel sanal ağ bağlantıları kurmak amacıyla geliştirilmiş bir tarama protokolüdür. L2F kendi başına şifreme veya gizlilik sağlamaz. L2F özellikle Point to Point Protocol (PPP) trafik taraması için tasarlanmıştır.

|  |  |  |  |
| --- | --- | --- | --- |
| Bit 0-12 | 13-15 | 16-23 | 24-31 |
| F | K | P | S | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | C | Ver | Protokol | Sequence (opt) |
| Çoklanmış Kimlik | İstemci Kimliği |
| Uzunluk | Ofset Yükü |
| Paket Anahtarı |
| Yük |
|  | L2F Kontrol |

Şekil . L2F Paket Yapısı

### Layer 2 Tunneling Protocol – L2T

Sanal özel ağların (VPNs) desteğinde kullanılan tarama protokolüdür. L2F gibi bu protokol de kendi başına şifreleme veya gizlilik desteği sağlamaz. Şifreleme desteği sağlayan protokol üzerinde bulunur. 1999 yılında RFC2661 standardı ile sunulmuştur. L2F ve PPTP’nin daha yeni sürümü olarak sayılabilir.

L2TP taraması PPP oturumu veya iki bölümlü bir oturumun bir bölümü boyunca genişletilebilir. Bu biçimde dört farklı tarama modeli olarak isimlendirilir.[4]

* İstemli tarama
* Mecburi tarama – gelen arama
* Mecburi tarama – uzaktan arama
* L2TP multi-hop bağlantı

|  |  |
| --- | --- |
| **Bits 0-15** | **Bits 16-31** |
| Bayraklar ve sürüm bilgisi | Uzunluk |
| Tarama kimliği | Oturum kimliği |
| Ns | Nr |
| Offset boyu | Offset pad |
| Playload Veri |

Şekil . L2TP Paket Yapısı

### NetBIOS – Network Basic Input/Output System

NetBIOS (Network Basic Input/Output System), bir yerel ağ (LAN) üzerindeki farklı bilgisayarların birbirleriyle iletişim kurmasını sağlayan (veri aktarımı vs.) bir sistemdir. IBM tarafından ilk masaüstü bilgisayarlar için oluşturulan NetBIOS, daha sonra Microsoft tarafından Windows işletim sistemlerine uyarlanmıştır.
NetBIOS üzerinden aynı ağ üzerindeki bilgisayarların iletişimi, temel olarak WINS (Windows Internet Name Service) Sunucusunun bilgisayarların NetBIOS isimlerini IP adreslerine çözümlemesiyle gerçekleşir.

Bir bilgisayara işletim sistemi kurulduğunda bu bilgisayara bir NetBIOS ismi atanır. NetBIOS ismi, 16 adet ASCII karakterden oluşur. Bu isim tek parçadan oluşmaktadır. Yani etki alanı isimleri gibi (sunucu1.sirket.com.tr)  değil de  ”sunucu1”  gibi nokta kullanılmadan oluşturulan isimlerdir.  Ancak Microsoft bu adı 15 karaktere sınırlandırmıştır ve 16. karakteri NetBIOS son eki (NetBIOS  Suffix) olarak ayırmıştır (Bilgisayar ismi 15 karakterden azsa, 15. karaktere kadar boşluk karakterleriyle doldurulur).  Bu son ek,  Microsoft ağ yazılımı tarafından kayıtlı bilgisayarlarda kurulu olan hizmetlerin fonksiyonunu belirlemek için kullanılır.[4][5]

En sık kullanılan NetBIOS son ekleri şunlardır:

* 00: İş İstasyonu Hizmeti (Workstation Service)
* 03: Haberci Hizmeti (Messenger Service)
* 20: Dosya Hizmeti  (File Service )
* 1B: Temel Etki Alanı Tarayıcısı  ( Domain Master Browser )
* 1C: Bir Etki Alanı İçin Etki Alanı Denetçileri (Domain Controllers For a Domain)
* 01: Temel Tarayıcı (Master Browser)
* 1E: Tarayıcı Hizmet Seçimleri (Browser Service Elections)

### Password Authentication Protocol -PAP

Şifre kullanan bir kimlik doğrulama protokolüdür. PAP, kullanıcıların sunucu kaynaklarına erişmelerinden önce PPP tarafından kullanılır. Hemen hemen bütün ağ işletim sistemi uzak sunucuları tarafından desteklenen bir protokoldür. Şifrelenmemiş ASCII şifreler bütün ağ boyunca PAP tarafından iletilir ve bu nedenle güvensiz kabul edilir. Bu yüzden uzak sunucuların CHAP ve EAP gibi güçlü kimlik doğrulama protokollerini desteklememesi durumunda kullanılmaktadır.[4]

### Point-to-Point Tunneling Protocol – PPTP

Internet üzerinden erişimi sağlayan protokoldür. PPTP teknolojisi çok protokollü sanal bir network yaratır. RAS Sunucularına modemler aracılığıyla ulaşılır. PPTP ise RAS sunuculara Internet üzerinden erişimi sağlar.

 PPTP protokolü PPP paketlerinin TCP/IP networkleri üzerinden yönlendirilmesini sağlar. PPTP, TCP/IP, IPX ve NetBUEI protokollerini destekler. Ancak uzak network bir TCP/IP network’ü olmalıdır.

 PPTP iletişiminde önce istemcisi Dial-Up Network ile Internet birimini arar. Doğrulama işleminin ardından istemcinin RAS sunucuya erişimine izin verilir.

PPTP tünelleri PPP tünelleri ile aynıdır. Fakat istemci makinada PPP programının elle başlatılmasına gerek yoktur. Sadece sunucu tarafında gerekli programın çalışması yeterlidir. PPTP kullanmanın en büyük faydalarından biri WİNDOWS ve MAC OS X işletim sistemlerinin PPTP VPN tünelleri oluşturmayı ön tanımlı olarak desteklemesi ve bağlantı kurulumu için kullanımı kolay ara yüzlere sahip olmasıdır.[4]

### Remote Procedure Call – RPC

Sunucu üzerindeki servisleri kontrol ettiğimizde karşımızı çıkan RPC (remote procedure call) arka planda haberimiz olmadan birçok şeyi gerçekleştiren bir servistir.
RPC temel anlamda istemci ve sunucu arasında yapılan işlemlerin iletişimi için tasarlanmıştır. Bir işlemin gerçekleşmesi için bir gönderici ve birde alıcı vardır. Örneğin Microsoft Outlook ve Exchange sunucu ikilisi gibi. Aynı şekilde sunucu üzerindeki bir çok serviste bu mimariyi kullanarak birbirleriyle haberleşirler. Bu haberleştirmeyi güvenli kılan ve kolaylaştıran şey RPC’dir.[3] [5]

NDR64

NDR20

Rpcrt4.dll

RPC Stubs

İstemci Sunucu Process

RPC

CDP

Runtime API

Connecting RPC

Datagram RPC

Local RPC

TCP

SPX

Named Pipes

HTTP

UDP

CDP

Network

Kernel

Registry

Win32 API

SSPI

EPM

Active Directory

User Mode

Kernel Mode

Şekil . RPC mimarisi

* *Client or Server process*;Bir RCP isteğini başlatan yada yanıt veren program yada servistir.
* *RPC stubs*RPC isteğini başlatmak için istemci yada sunucu tarafından kullanılan programdır
* *Marshalling engine(NDR20 or NDR64);*RPC istemci ve sunucuları arasında ortak bir RPC arayüzü oluşturur.NDR20 32 bit mimarisi için, NDR64 ise 64 mimarisi için tasarlanmıştır. İstemci ve sunucu bu marshalling engine sayesinde iletişim için karşılıklı anlaşmayı sağlarlar.
* *Runtime application programming interface (API);* Sunucu yada istemci’a RPC için direk bir arayüz oluşturur. RPC istemci ve sunucuları RPC’yi başlatmak içnin runtime API yi çağırırlar.
* *Connection RPC protocol engine;*RPC bir connection oriented protocol isteğinde bulunduğunda kullanılır. Burada RPC nin dışarıya doğru bir bağlantıda mı yoksa dışarıdan içeriye doğru bir bağlantıda mı olduğu tasarlanır.
* *Local RPC protocol engine;* Sunucu ve istemci aynı host içerisinde barınıyorsa kullanılır.
* *Registry*;RPC servisinin ilk yüklemesinde erişim sağlanır. Buradaki registry anahtarları, RPC kullanıldığı ip port aralıklarını yada network aygıtlarının isimlerini barındırır.
* *Win32 APIs(kernel32.dll, advapi32.dll, ntdll.dll);*Kernel32.dll , sistem servislerinin hafıza yada kaynak yönetimlerini sağlayan Windows NT tabanlı bir API istemci dynamic-link library (DLL) dosyasıdır.
Advapi32.dll, gelişmiş bir Windows 32 base API DLL dosyasıdır. Güvenliği destekler. Ntdll.dll , Windows NT nin sistem fonksiyonlarını kontrol eder.
* *SSPI(secur32.dll)*; RPC için bir güvenlik ara yüzü oluşturur. Kerberos, NTLM, ve Secure Sockets Layer (SSL) ın kimlik doğrulama ve şifreleme için kullanımını sağlar.

RPC Yapımında Temel Adımlar;

* İstemci taslağa çağrıda bulunur. Bu çarı normal yolla [stack](http://tr.wikipedia.org/w/index.php?title=Stack&action=edit&redlink=1)'e itilen parametreli yere prosedür çağrısıdır.
* İstemci taslağı parametreleri bir mesaja paketler ve mesajı göndermek için bir sistem çağrısı yapar. Paketlenmiş parametreler [marshalling](http://tr.wikipedia.org/w/index.php?title=Marshalling&action=edit&redlink=1) diye adlandırılır.
* Çekirdek istemci makineden sunucu makineye mesajı yollar.
* Çekirdek gelen paketleri sunucu taslağa iletir.
* Son olarak, sunucu taslak sunucu prosedürünü çağırır.

### Real-Time Transport Control Protocol – RTCP

Real-Time Transport Protocol (RTP)’nin bir alt protokolüdür. RTP ile RTCP birlikte çalışırlar. RTP gerçek zamanlı veri iletimi ile ilgilenirken; RTCP veri iletimini monitör eder. RTCP sayesinde veri alıcısı herhangi bir paket kaybının olup olmadığını tespit eder, ya da jitter gecikmelerini gidermeye çalışır. Bu iki protokolde Transport ve Network katmanlarından ayrı olarak çalışır.

Veri iletimi esnasında iki uç arası bir RTP oturumu kurulur. Bu oturum IP adresleri ve RTP ve RTCP ye ait portlardan oluşur. Bu oturum içerisindeki cihazlar veri alıp gönderebilirler. Her bir medya türü için cihazlar arası ayrı bir oturum oluşturulur. Böylelikle oturum içerisindeki kişilerin hangi medya tipinden veri almak istemelerine imkân sağlanmış olur. Örneğin bir kullanıcı yayınlanan bir filmin sadece sesini almak isteyebilir. Bu durumda alıcının video yayınını engellemesi yeterli olacaktır. Burada bir önemli husus ta eğer UDP ile birlikte çalışıyorsa RTP protokol tanımlamasında RTP portunun bir çift sayıya denk gelmesi gerektiğidir. RTCP portu ise o oturuma ait RTP portundan sonraki elverişli olan ilk tek port numarasıdır. RTP ve RTCP genellikle 1024-65535 arası portları kullanır.

RTCP şunları içerir;

* Kayıp paket sayısını,
* Jitter verilerini, bitlerin kaynak ile hedef arasında gidiş-dönüş süresini gösteren round-trip time bilgisini içeren  QoS Feedback (Servis kalitesi geri bildirim);
* Oturumdan ayrılan kullanıcıların BYE bilgisi göndererek diğer kullanıcıları haber ettiği oturum kontrol;
* Oturumdaki kullanıcıların bilgilerini içeren kimlik;
* Ayrı ayrı transfer edilmiş ses ve görüntü bilgilerinin eşlenmesini sağlayan ortam eşlemesi bilgileri

### Short Message Peer-to-Peer Protocol – SMPP

SMPP (Short Message Peer-to-Peer Protocol), SMS gönderici ve alıcıları arasında SMS alışverişini sağlamak üzere tasarlanmış uluslararası bir telekomünikasyon protokolüdür.

Genellikle GSM operatörleri ve katma değerli servis sağlayıcılar arasında toplu SMS gönderimlerinde kullanılır.

Bir dış SMS servisi SMPP kullanarak TCP/IP veya X.25 üzerinden kendi uygulama katmanında bir Servis Mesajı Merkezi ile SMS alışverişinde bulunabilir.

SMPP küçük bir İrlanda teknoloji firması olan Aldiscon tarafından geliştirildi. Aldison daha sonra Logica tarafından satın alındı. SMPP 1999'dan beri SMS Forum adlı organizasyon tarafından geliştirilmektedir. Günümüzde SMPP sürüm 5.0 olsa da en sık kullanılan sürümler 3.3 ve 3.4 sürümleridir.

### SOCKS Protocol

SOCKS, istemci-sunucu uygulamalarının şeffaf bir biçimde network güvenlik duvarı servislerini kullanmasına izin veren bir internet protokolüdür. SOCKS, SOCKETS in kısaltılmış şeklidir.

Bu protokol MIPS Computer Systems sistem müdürü David Koblas tarafından geliştirilmiştir. MIPS firmasının Silicon Garphics tarafından 1992yılında devralınmasından sonra Koblas aynı yılın Usenix Security sempozyumunda bir sunum gerçekleştirerek SOCKS kullanımı herkese açık hale getirildi. Protokol, 4. sürümü NEC firmasından Ying-Da Lee tarafından getirildi. SOCKS referans mimarisi ve istemcisi Permeo Technologies'e aittir. SOCKS, OSI modelinin oturum katmanında işler.

### Zone Information Protocol – ZIP

AppleTalk ağı numaralarının bölge isimleri ile ilişkilendiren bir protokoldür. En önemli özelliklerinden birisi yönlendirici olmayan düğümlere sağladığı şeffaflık hizmetidir. Yönlendirici olmayan düğümler başlangıç işlemi süresince bölgelerini seçmek için ZIP’un küçük bir alt kümesini kullanılır, ayrıca bu süreçte internetin bölge yapısı bilgisini elde eder. ZIP üç büyük temel hizmet sunar;

* İnternetin ağ bölge ismi haritalanmasına bakım hizmeti
* Düğüm tarafından seçilen bölge ismine destek hizmeti
* Çeşitli komutlara destek hizmeti

### Sockets Direct Protocol – SDP

Software Working Group tarafından yüksek performanslı bilgi işlem ihtiyacını gidermek için tasarlanan bir ağ protokolüdür. Başlangıçta InfiBand (IB) için tasarlanan SDP, Uzaktan Doğrudan Bellek Erişimi (RDMA) için bir ulaşım agnostik protokolü olarak yeniden oluşturulmuştur. Bu önemli performans artışı sonucunda uzakta bulunan başka bir bilgisayara, doğrudan bir bilgisayarın hafızasından veri akışı sağlar.

# Sonuç

Bilgisayar ağ bağlantı mimarilerinde yedi katmanlı OSI modelinde Sunum ve Oturum katmanlarında kullanılan protokoller ağ iletişiminde güvenlik, yönetim, veri denetimi ve iletimi gibi konularda bir omurga vazifesi görmektir.

**Kaynaklar**

1. Harmancı A. E.; 2006; “Türkiye Bilişim Ansiklopedisi”; Papatya Yayıncılık; Türkiye; s53
2. Serpanos D., Wolf T.; 2011; “Architecture of System Networks”; Elsevier Inc.; USA; s12 - s162
3. Stallings W.; 2009; “Business Data Communications”; Pearson Prentice Hall; USA; s125 - s167
4. Harwood M.; 2003; “Network +”; Que Certification; USA; s79- s131- s86 -s139 - s155 – s136
5. Hura G. S., Singhal M.; 2001; “Data and Computer Communications – Networking and Internetworking”; UK; s659 - s629 – s261 – s1002
6. Shinde S. S.; 2009; “Computer Network”; New Age International Publishers; New Delhi; s314 –s315
7. Sidhu G. S., Andrews R. W., Oppenhiemer A. B.; 1990; “Inside Apple Talk”; Addison-Wesley Publishing Company Inc; USA; s13 – s288
8. 2007; Citrix Presentation Server Administrator’s Guide; Citrix Systems; USA; s201
9. R. Khare; May June 1998; “Telnet : The Mother of All (Application) Protocols”; IEEE Internet Computing; USA Ca; s91
10. R. Deregözü; 1997; “Telnet”; İTÜ Bilgi İşlem Merkezi; İstanbul
11. M. Eisler; 2006; “XDR: External Data Representation Standart”; The Internet Society; RC:4506
12. M. Harwood; 2010; “CompTIA Network+”; Pearson; USA; s293
13. ITU-T; 2006; “H.245”; Telecommunication Standardization Sector of ITU
14. E. Yavuz; 2004; “İnternet Protokolü Üzerinden Ses Haberleşmesinde Servis Kalitesine Etki Eden Parametrelerin Analizi”; Süleyman Demirel Üniversitesi Fen Bilimleri Enstitüsü Elektronik ve Haberleşme Mühendisliği Anabilim Dalı Yüksek Lisans Tezi; Isparta; s27
15. K. Gibbons, J. Tseng, C. Monia, F. Trovostino, K. Hirata, M. Bakke, J. Hafner, H. Hall; 2001; “Internet Storage Name Servise – A Technical Overview”; Nishan Systems; CA,USA