Point-To-Point Protocol(PPP)

Hamza CANBAZ
Bilgisayar Mühendisliği Bölümü Lisans Öğrencisi
Yıldız Teknik Üniversitesi
İstanbul, Türkiye
hamza.canbaz@std.yildiz.edu.tr

Gürol Berkay ÇINAR
Bilgisayar Mühendisliği Bölümü Lisans Öğrencisi
Yıldız Teknik Üniversitesi
İstanbul, Türkiye
berkay.cinar@std.yildiz.edu.tr

İbrahim ÇOLAKGİL
Bilgisayar Mühendisliği Bölümü Lisans Öğrencisi
Yıldız Teknik Üniversitesi
İstanbul, Türkiye
ibrahim.colakgil@std.yildiz.edu.tr

Evren İSPİROĞLU
Bilgisayar Mühendisliği Bölümü Lisans Öğrencisi
Yıldız Teknik Üniversitesi
İstanbul, Türkiye
evren.ispiroglu@std.yildiz.edu.tr

Muhammed Said YARGIN
Bilgisayar Mühendisliği Bölümü Lisans Öğrencisi
Yıldız Teknik Üniversitesi
İstanbul, Türkiye
said.yargin@std.yildiz.edu.tr

***Abstract*—Bu çalışmada, seri bir iletim ortamı üzerinden paketlerin aktarılmasını sağlayan noktadan noktaya protokolün-PPP için ağlar üzerinde ihtiyacın doğuşu, tarihsel gelişimi, çözdüğü problemler ve uygulamaları ele alınmıştır.**

***Index Terms*—Noktadan noktaya Protokol, PPP, seri hatlarda ağ çözümleri, PPP uygulamaları**

I. GİRİŞ

Bilişim sistemlerinde tarihsel süreç boyunca en önemli konulardan biri haberleşme konusu olmuştur. Kullanıcılar arttıkça ve ağlar büyüdükçe gelişmiş haberleşme protokollerine ihtiyaç doğmuştur. PPP bu ihtiyaca cevap vermek için geliştirilmiş protokollerden biridir. PPP, IP katmanının yanı sıra diğer ağ katmanlarının da bağlantısını yönetebilecek Network Control Protocols (NCP), genişletilmiş Link Control Protocol ve kapsülleme özellikleri ile birlikte geliştirilmiştir.

II. PPP'NIN TARIHÇESI

A. Tarihsel Süreç

Noktadan noktaya protokolün (Point to Point - PPP) tarihi 1980'lerin sonuna yani "Serial Line Net Protocol" (SLIP)'un seri internet protokol uygulamaları için fiili standart olduğu zamanlara dayanmaktadır [1].

PPP ile ilgili ilk resmi "The Internet Engineering Task Force" (IETF) belgesi, 1989'da yayınlanan "Request for Comments 1134" (RFC-1134) idi. RFC, standardın kendisi değil, 1990'da ilerleyen zamanda ilk ana PPP standardı olarak tanımlanacak olan RFC 1171 için bir öneriydi.

IETF, PPP'yi sıfırdan geliştirmeye çalışmak yerine, başlangıçta IBM tarafından geliştirilen ISO Üst Düzey Veri Bağlantı Kontrolü ("High-Level Data Link Control" - HDLC) protokolüne dayandırılmasına karar verdi. HDLC, Eşzamanlı Veri Bağlantı Kontrolü ("Synchronous Data Link Control" - SDLC) protokolünün bir türevidir. PPP'nin geliştiricileri, çerçeveleme yapısını ve genel işleyişinin bir kısmını HDLC protokolünden uyarladı.

Microsoft tarafından kullanılan resmi uygulama, RFP 1990'dan gelmektedir. Yetenekler eklenmiş ve standarda müteakip değişiklikler yapılarak bugünkü PPP'ye ulaşılmıştır. 1994 yılında, RFC 1717'de "PPP Çoklu Bağlantı Protokolü" için belgelenmiş bir standart önerildi. O zamanlar, veri akışlarını bit seviyesinde (temelde bir donanım çözümü) birleştirmek için başka öneriler vardı. Bu teklif, birden çok veri akışını tek bir veri akışında birleştirme ihtiyacı için yazılım tabanlı bir çözümü tanımlıyordu [2].

B. Noktadan Noktaya Protokolüne Neden İhtiyaç Duyduk?

SLIP, sadece temelde üçüncü katmandaki IP ile birinci katmandaki bir seri bağlantı arasındaki boşluğu doldurmak ihtiyacını karşılamaktaydı. Bu yaklaşım iş görmekteydi ancak cihazlar arasında doğrudan bağlantılar için güçlü bir protokolde beklenen özelliklerin hiçbirini karşılamıyordu.

PPP, yalnızca IP'yi değil, diğer ağ katmanı protokollerinin iletimini de desteklemek için tam işlevli ikinci katman bağlantısını etkinleştirecek eksiksiz bir protokol paketi olacak şekilde geliştirildi.

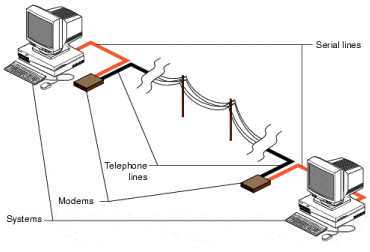

Fig. 1. SLIP [3]

C. Ana Problem Neydi?

Seri Hat İnternet Protokolü (SLIP), bazı eksiklikler barındırdığı için noktadan noktaya protokolü ortaya çıkmıştır. IP için temel katman iki çerçeveleme sağlar, ancak çoklu kullanım için oldukça basittir. Yaptığı tek şey her datagramın sonunu çerçevelemek olduğundan, seri bağlantılar üzerinden güvenilir, emniyetli ve yüksek performanslı operasyon için gerçekten ihtiyaç duyduğumuz özelliklerin çoğunu sağlamaz. Bu, özellikle çoğu seri bağlantının kısa LAN kabloları olmadığı, nispeten uzun mesafelerde çevirmeli WAN bağlantıları olduğu günümüzde geçerlidir.

D. Probleme Çözüm Neydi?

PPP'nin temel amacı seri bir iletim ortamı üzerinden paketlerin aktarılmasıdır. Böylece PPP sayesinde, iki iletişime uygun cihazın özel olarak yapılandırılmış veri paketleri (datagram) sayesinde bilgi değişimi yapması sağlanmış olur. Çalışma mekanizmasını; Kapsüllenme (Encapsulation), Bağlantı Kontrol Protokolü (Link Control Protocol) ve Ağ Kontrol Protokolü (Network Control Protocol) olmak üzere üç ana bölümde incelemek mümkündür [4].

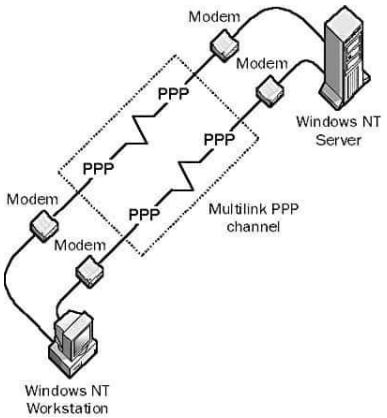

Fig. 2. Point to Point Protocol (PPP)[[5]

III. TEKNİK AÇIDAN PPP

A. PPP Nedir?

PPP, byte tabanlı bir veri katmanı protokolüdür. Birbirlerine direkt bağlı olan 2 cihaz arasında veriyi iletmek ve kontrol etmek için kullanılır [6].

B. Servisler

1-PPP'nin sağladığı servisler:

- Cihazlar arası aktarımda kullanılacak frame yapısını belirler.
- Ağ katmanının veri katmanı içinde encapsulate edilmesini sağlar.
- Birden çok bağlantılara imkan sağlar.
- Yetkilendirmeyi yerine getirir.

2-PPP'nin sağlamadığı servisler:

- Akış kontrolü sağlamaz
- Hata kontrol sistemi basittir. Hata düzeltme sağlayamaz.
- Çok bağlantılı yapıları yönetmek için sofistike bir adresleme yapısına sahip değildir.

C. Frame Formatı

Flag: 01111110. Frame'in başlangıcını ve bitişini belirleyen 1 byte'lık bayrak.

Adress: 11111111. Cihazlar arası direkt bağlantılar kullandığından dolayı her zaman broadcast olarak belirtilen 1 byte'lık kısım. Cihazlar arası anlaşılarak atlanabilir.

Control: 11000000 Akış kontrolü ve hata düzeltmesi olmadığından sabittir. Cihazlar arası anlaşılarak atlanabilir.

Protocol: 1 veya 2 byte olabilir. Payload'da olan verinin tipini belirler.

Payload: Ağ katmanının verisini taşıyan kısımdır.. Varsayılan maksimum değeri 1500 byte'dır ve bu değer cihazlar arası anlaşma ile küçültülebilir. Eğer gönderilecek veri maksimum değerden küçükse padding ile doldurulur. İçerisinde flag sekansı varsa byte stuffing ile veri tutarlılığı sağlanır.

Frame Check Secquence: CRC ile hata kontrolü yapar. 2 veya 4 byte boyutunda olabilir.

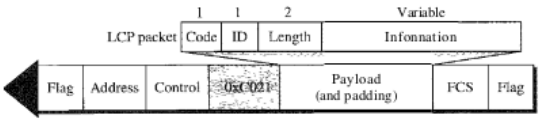

Fig. 3. Frame [7]

D. İletişim Aşamaları

- Dead: Hat boştur.
- Establish: Cihazlardan biri iletişime başlar, seçenkler için anlaşma sağlanır. Eğer gerekliyse kimlik doğrulama gerçekleştirilir.
- Authenticate: Cihazlar birbirlerine doğrulama amaçlı paketler gönderirler. Eğer hata oluşursa iletişim bitirilir.
- Network: Ağ katmanı protoklü belirlenir. Eğer ağ katmanında birden fazla protokol kullanılıyorsa alıcı cihaz hangi prokolün kullanıldığını bilmelidir. Veri iletişimi cihazlardan biri sonlandırana kadar devam eder.

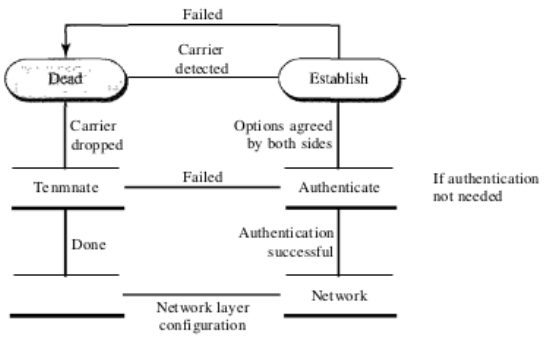

Fig. 4. Aşamalar [7]

E. Multiplexing

PPP bir veri katmanı protokolü olmasına rağmen başka protokolleri de kullanır.

1 - Link Control Protocol (LCP):

- Bağlantıların kurulması, devam ettirilmesi , ayarlanması ve sonlandırılmasından sorumludur.
- Protocol: 21h'dır.
- Code: Paket tipini belirler.
- ID : İstek ve cevapların bilgisini tutar.
- Length: Bütün LCP paketinin boyutunu tutar.
- Information: Cihazların kendi aralarında kararlaştıracağı kısımlar için kullanılır.

2 - Authentication Protocols:

Password Authentication Protocol (PAP):

- Kullanıcı sisteme bir kimlik ve şifre gönderir.
- Sistem bilgilerin geçerliliğini kontrol eder. Bağlantıyı sağlar veya reddeder.

Challenge Handshake Authentication Protocol (CHAP):

- Sistem kullanıcıya biri diğerine bir challenge paketi gönderir.
- Kullanıcı bu paketi ve şifresini önceden belirlenmiş bir fonksiyondan geçirierek bir değer elde eder. Elde ettiği değeri sisteme gönderir.
- Sistem kullanıcıya gönderdiği değer ve kullanıcının şifresi ile aynı işlemi uygular. Sistemin sonucu kullanıcının gönderdiği değer ile uyuşuyorsa erişime izin verir.

Network Control Protocols: PPP birçok ağ katmanı protokolü içerebileceğinden ağ katmanı veri paketi taşıyabilir. Bunun için PPP içinde farklı ağ protokolleri için ağ kontrol protokolü belirler. IPCP paketi taşıyan bir PPP paketi örneği:

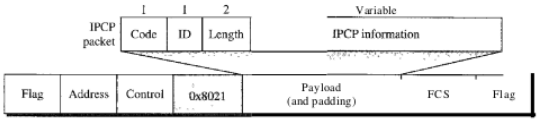

Fig. 5. IPCP [7]

F. Multilink

PPP başlangıçta tek kanallı uçtan uca fiziksel bağlantı için tasarlanmıştı. Tek bir bağlantıdan birden çok kanalın bulunabilmesi için Multilink PPP (MPPP) geliştirildi. Bu durumda bir logical PPP frame'i Daha küçük PPP frame'lerine bölünür.

IV. PPP ve Kullanim Alanlari

Point to Point Protokolünün yaygın olarak ilk kullanım alanı Dial-up bağlantılardır. Sonrasında PPPoE, PPPoA, PPTP, L2TP gibi protokollerde kullanılmaya başlanmıştır [8].

A. Dial-up connection nedir?

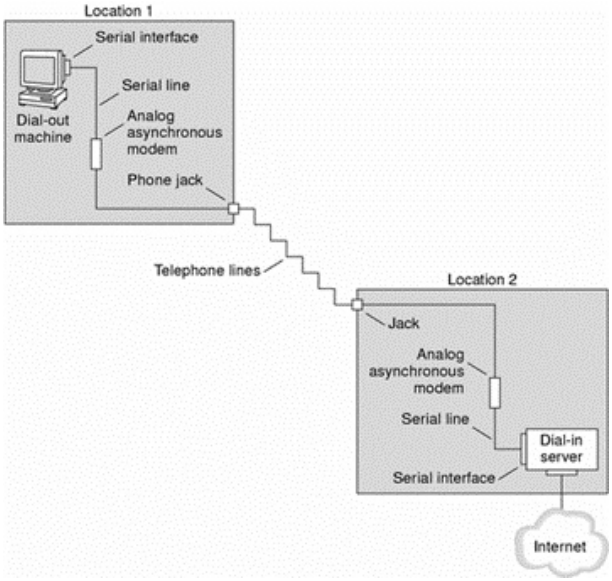

Fig. 6. Dial-Up [10]

Türkçeye çevirmeli bağlantı olarak geçmiştir. Dial-up bağlantı 56 Kbps'ye kadar veri aktarım hızlarında İnternet'e erişmek için standart bir telefon hattı ve analog modem kullanır. Internete ulaşmanın en ucuz ve en yavaş yöntemidir. Gelen çağrıları almak üzere ISP(Internet Servis Sağlayıcısı) ile bağlantı kuran bilgisayar buna örnek olarak verilebilir. Başka bir örnek olarak kullandığımız makineden farklı bir yerdeki makineye PPP bağlantısı üzerinden veri iletilmesi verilebilir. Bu bağlantıda dial-up bağlantıyı bağlatan makine dial-out makine, bu makinenin hedef eşi ise dial-in makine olarak adlandırılır.

Dial-up bağlantı gerçekleşirken aşağıdaki adımlar gerçekleşir.

- Dial-out makinesi modeme bağlanır ve bu modem karşı tarafa iletilecek analog sinyalleri dijital sinyallere dönüştürmekle görevlidir.
- Kullanıcı daha sonra standart bir telefon veya özel bir çevirmeli modem kullanarak internet servis sağlayıcısı (ISP) tarafından sağlanan bir telefon numarasını çevirir.
- Bağlantı kurulduktan sonra, ISP'nin telefon hattının ucundaki modem analog sinyalleri tekrar dijital sinyallere dönüştürür ve bunları internete yönlendirir.

- Kullanıcının bilgisayarı veya cihazı daha sonra modem tarafından kurulan bağlantı üzerinden internete erişebilir.

2010 yılında Birleşik Krallık'ta yaklaşık 800.000 civarı kullanıcı dial-up bağlantıyı kullanmaktaydı. 2013 yılında ise BT Group bu kullanımı kaldırdı. Dial-up bağlantılar yerini Broadband bağlantılara bırakmıştır. Broadband bağlantılar dial-up bağlantılara göre daha hızlı, güvenli ve yüksek bant genişlikli aktivitelere uygundur. Internete bağlanmak için telefon hattına ihtiyaç duymaz.

DSL, Cable, Fiber, Satellite, Mobile bağlantıları örnek olarak verilebilir. Günümüzde geniş bant genişlikli bağlantı altyapısının olmadığı yerlerde veya yedek bağlantı türü olarak kullanılabilir.

B. PPPoE ve Kullanımı

PPPoE protokolü Ethernet bağlantısını kullanarak bilgisayar ile ISP arasında bağlantı kurmaya olanak sağlayan bir protokoldür. PPPoE, Internet Servis Sağlayıcıların DSL bağlantısı ile müşterilere internet erişimi sağlamada kullanılır. (Digital Subscriber Line, verileri bir telefon hattı üzerinden iletmek için kullanılan bir teknolojidir. Genellikle ISP tarafından müşterilere yüksek hızlı internet erişimi sağlamak için kullanılır.) [9]

Ethernet, cihazların LAN veya WAN'a bağlanması için kullanılan bir ağ teknolojisidir. Bilgisayarlar, routerlar, switchler ve diğer cihaz türleri gibi ağ cihazları için yaygın olarak kullanılan bir standarttır.

PPPoE'yi kullanmak için bir bilgisayarda PPPoE istemcisinin kurulu olması gerekir. İstemci, genellikle ISP tarafından çalıştırılan PPPoE sunucusu ile iletişim kurar. Bağlantı kurulduktan sonra, PPPoE istemcisi PPPoE bağlantısı üzerinden veri gönderebilir ve alabilir. PPPoE Windows, MacOS, Linux gibi birçok işletim sistemi tarafından desteklenir ve bu işletim sistemlerinde yaygın olarak kullanılmaktadır. Linux'deki pppd komutu, PPPoE sunucusuyla bağlantı kurmayı sağlar.

C. PPTP ve Kullanım Alanları ?

İki bilgisayar veya ağ arasında güvenli bir bağlantı kurmak için kullanılan bir PPP türüdür. PPTP, bir ağdan gelen veri paketlerini başka bir ağın paketlerine kapsülleyerek çalışır, bu da verilerin genel bir ağ üzerinden güvenli bir şekilde iletilmesini sağlar. Bağlantının güvenliğini sağlamak için şifreleme ve kimlik doğrulama gibi özellikler içerir. Genellikle VPN bağlantılarında kullanılır. PPTP protokolü hızlı ve kullanımı kolay bir protokol olarak kabul edilir. Nispeten zayıf bir şifreleme kullanması ve ihlallere karşı diğer protokoller kadar koruma sağlayamamasından ötürü diğer VPN protokolleri kadar güvenli değildir. Yerini daha modern protokoller olan OpenVPN, L2TP/IPSec, IKEv2, WireGuard gibi protokollere bırakmıştır.

D. PPTP nasıl çalışır?

İstemci, sunucuya bir istek göndererek PPTP bağlantısını başlatır. Sunucu istemcinin kimliğini doğrular ve TCP (İletim Kontrol Protokolü) ve PPTP kontrol mesajı protokolünü kullanarak bir kontrol bağlantısı kurar. İstemci ve sunucu daha sonra veri bağlantısı için kullanılacak şifreleme ve sıkıştırma yöntemleri üzerinde anlaşmaya varır. İstemci ve sunucu, veri paketlerini bir tünelleme protokolünde kapsülleyen GRE (Generic Routing Encapsulation) protokolünü kullanarak bir veri bağlantısı kurar. Veri bağlantısı, üzerinde anlaşmaya varılan yöntemler kullanılarak şifrelenir ve sıkıştırılır. İstemci ve sunucu artık güvenli, şifrelenmiş bağlantı üzerinden veri gönderip alabilir.

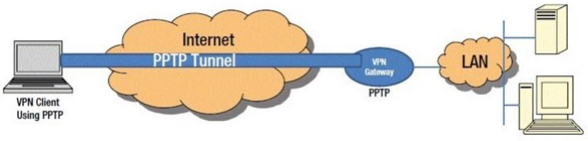

Fig. 7. PPTP [11]

E. L2TP ve PPTP'nin karşılaştırılması

- L2TP (Layer-to Tunneling Protocol) de PPTP gibi güvenli bir bağlantı kurulmak için kullanılan, sanal özel ağları destekleyen Cisco ve Microsoft tarafından geliştirilen bir protokoldür.
- L2TP, IPSec olarak bilinen kompleks bir şifreleme protokolü kullanır. Bu sayede PPTP'ye göre daha güvenli bir bağlantı sunar.
- PPTP resmi olarak kabul edilen ilk VPN protokol olma özelliğine sahiptir.PPTP, L2TP'ye göre daha hızlı bir bağlantı sunar.
- PPTP, L2TP'ye göre daha hızlı bir bağlantı sunar.

REFERENCES

[1] C. M. Kozierok, (n.d.). "PPP Overview, History and Benefits. The TCP/IP Guide - PPP Overview, history and benefits." Retrieved December 24, 2022, from

[2] Walls, C. (no date) "Point-to-point protocol, Point-to-Point Protocol - an overview — ScienceDirect Topics". Available at: https://www.sciencedirect.com/topics/computer-science/point-to-point-protocol (Accessed: December 25, 2022).

[3] "Editor (2021) Serial line internet protocol (SLIP), Network Encyclopedia. Available" at: https://networkencyclopedia.com/serial-line-internet-protocol-slip/ (Accessed: December 25, 2022).

[4] Seyir defteri. Point to Point Protocol (Noktadan Noktaya Protokolü). (n.d.). Retrieved December 25, 2022, from https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/07/point-to-point-protocol-(noktadan-noktaya-protokol

[5] Editor (2021) Point-to-point protocol (PPP), Network Encyclopedia. Available at: https://networkencyclopedia.com/point-to-point-protocol-ppp/ (Accessed: December 25, 2022).

[6] B. Foruzan, "Introduction to Data Communications" & Networking, 2007, Fourth Edition.

[7] https://www.geeksforgeeks.org/difference-between-byte-stuffing-and-bit-stuffing/

[8] https://docs.oracle.com/cd/E19683-01/817-1717/pppsvrconfig.intro-41/index.html#:~:text=The%20most%20commonly%20used%20PPP,number%20to%20initiate%20the%20link

[9] https://en.wikipedia.org/wiki/Dial-up_Internet_access#:~:text=Despite%20the%20rapid%20decline%2C%20dial,or%20copper%20may%20be%20uneconomical\end{thebibliography}

[10] https://docs.oracle.com/cd/E19683-01/817-1717/pppsvrconfig.intro-41/index.html#:~:text=The%20most%20commonly%20used%20PPP,number%20to%20initiate%20the%20link

[11] https://www.hideipvpn.com/learning-center/what-is-pptp/