

İkili El Sıkışma (Two-Way Handshake) Nedir?

Ağ iletişiminde "El Sıkışma" (Handshake), iletişim kuracak iki cihazın veya yazılımın, veri alışverişine başlamadan önce birbirlerinin varlığını doğruladığı, temel parametreler üzerinde anlaştığı ve iletişim kanalını kurduğu bir dizi ön adımdır.

İkili El Sıkışma (Two-Way Handshake) ise, bu sürecin sadece iki adımda tamamlandığı, yani istemci ve sunucu arasında yalnızca iki mesajın gidip geldiği en basit formudur.

1. Nedir? (Tanım ve Kullanım Alanı)

İkili el sıkışma, iletişim başlatmanın en yalın şeklidir ve daha çok basit, durumsuz (stateless) veya güvenilirlik kaygısının düşük olduğu iletişim protokollerinde kullanılır.

- **Tanım:** İstemcinin bir istek gönderdiği (1. adım) ve sunucunun bu isteğe bir cevap göndererek bağlantıyı onayladığı (2. adım) bir dizi mesajlaşma modelidir.
- **Kullanım Alanı:** En yaygın olarak, **UDP (User Datagram Protocol)** tabanlı uygulamaların başlangıç süreçlerinde veya çok basit, yüksek hız gerektiren ama kayıp toleransı olan durumlarda görülür. Ancak genellikle en bilinen protokol olan **TCP'de kullanılmaz**, çünkü TCP güvenilirliği garanti etmek için daha karmaşık bir yönteme (Üçlü El Sıkışma) ihtiyaç duyar.

2. Ne İşe Yarar? (Ana İşlevi)

İkili el sıkışmanın temel işlevi, iletişim kuracak cihazların karşılıklı olarak **iletişim başlatma niyetlerini** bildirmeleridir.

- **İstek Gönderimi:** İstemci, sunucuya "Ben hazırım ve konuşmak istiyorum" mesajını iletir.
- **Cevap Alımı:** Sunucu, istemciye "Mesajını aldım ve ben de hazırım" mesajını ileterek bağlantıyı onaylar.

Bu süreç, hızlı bir şekilde kanal açmak için idealdir, ancak önemli bir dezavantajı vardır: **Güvenilirlik garantisi vermez.**

3. Ne Amaçla Kullanılır? (Hız Odaklı Senaryolar)

İkili el sıkışma, genellikle güvenilirliğin hızdan daha az önemli olduğu senaryoları desteklemek için tasarlanmıştır.

- **Hız Avantajı:** Üçlü el sıkışmaya göre daha az paket alışverişi olduğu için (2 yerine 3 paket), iletişim daha hızlı kurulur. Bu, özellikle her milisaniyenin önemli olduğu durumlarda faydalıdır.
- **Durumsuz İletişim:** İki cihaz arasında uzun süreli bir oturumun (session) korunmasına gerek olmayan, tek seferlik istek ve cevap modellerinde tercih edilebilir. Örneğin, bir cihazın hızlıca bir bilgi sorgulayıp alması gerektiğinde.
- **DDoS Saldırıları Riski:** TCP'nin Üçlü El Sıkışması, İkili El Sıkışmaya göre çok daha güvenlidir. Çünkü İkili El Sıkışma, sunucunun sadece bir istek aldığı anda kaynak ayırmasına neden olabilir. Bu da sunucuyu, sahte isteklerle kolayca kaynakları tüketmeye zorlayan **DDoS (Hizmet Engelleme) saldırılarına** karşı daha savunmasız hale getirir.

4. Örnekler (Adımlar ve Mesajlar)

İkili el sıkışmanın adımları basit ve nettir. Protokol ne olursa olsun, mantık hep aynıdır:

Adımlar:

Adım	Kim Gönderir?	Mesaj (Sembolik İsim)	Açıklama
1	İstemci (Client)	İSTEK (REQUEST)	"Konuşmak istiyorum."
2	Sunucu (Server)	ONAY (ACKNOWLEDGEMENT / ACK)	"İsteğini aldım, başlayabiliriz."

E-Tablolar'a aktar

Senaryo Örneği:

İki yazılımın basit bir bilgi sorgulaması yaptığını varsayalım:

1. **İstemci (Client) → Sunucu (Server):** "Bana hava durumu verilerini gönder."
2. **Sunucu (Server) → İstemci (Client):** "Tamam, verileri gönderiyorum."

Bu noktadan sonra veri alışverişi başlar. Ancak bu modelde, **istemcinin sunucunun cevabını gerçekten alıp almadığı garanti edilmez**. Eğer Sunucudan gelen Onay mesajı yolda kaybolursa, Sunucu "Bağlantıyı kurdum" zannederken, İstemci hala bekliyor olabilir.

Önemli Not: Ağ mühendisliği ve temel protokoller bağlamında, veri iletiminin **güvenilirliğini** sağlayan protokol olan **TCP** kesinlikle **İkili El Sıkışma** kullanmaz; bunun yerine güvenliği artırılmış olan **Üçlü El Sıkışma (Three-Way Handshake)** yöntemini kullanır. İkili El Sıkışma, daha çok teorik veya TCP/IP dışında özel ağ yapılarında karşımıza çıkar.