10. Hafta ders notlarına dayanarak oluşturulan sınav soruları ve uzun cevapları:

1. **Tek Bit Hatası ve Burst Hatasının Tanımı Nedir?**
   - Tek bit hatası, veri iletimi sırasında yalnızca bir bitin değerinin değişmesidir. Burst hatası ise arka arkaya gelen çok sayıda bitin hatalı iletimi anlamına gelir ve genellikle gürültü nedeniyle meydana gelir.

2. **Redundancy'nin Hata Tespiti ve Düzeltmedeki Rolü Nedir?**
   - Redundancy, ekstra bitlerin eklenmesiyle gerçekleştirilir ve bu bitler hata tespiti ve düzeltme için kullanılır. Gönderilen veri ile birlikte bu kontrol bitleri, alıcıda hataların tespit edilmesini ve düzeltilmesini sağlar.

3. **Mod-2 Aritmetiğinin Veri İletişimindeki İşlevi Nedir?**
   - Mod-2 aritmetiği, iki ikili sayının XOR işlemiyle toplanmasını içerir. Bu yöntem, veri iletişiminde hata kontrolü için kullanılır, özellikle CRC (Cyclic Redundancy Check) gibi algoritmaların temelini oluşturur.

4. **Blok Kodlamada Dataword ve Codeword Arasındaki İlişki Nedir?**
   - Blok kodlamada, orijinal veri (dataword) belirli sayıda bitlere bölünür ve her bir bloğa ekstra kontrol bitleri (redundant bitler) eklenir. Bu işlem sonucunda elde edilen yeni dizilim codeword olarak adlandırılır.

5. **Hata Tespiti ve Düzeltmede Hamming Distance'ın Önemi Nedir?**
   - Hamming distance, iki kelime (word) arasındaki farklı bit sayısını ifade eder. Hata tespiti ve düzeltmede, iletilen ve alınan veriler arasındaki Hamming distance, hatalı bitlerin sayısını ve konumunu belirlemekte kullanılır.

6. **Hamming Kodlarının Hata Düzeltme Kapasitesi Nedir?**
   - Hamming kodları, genellikle en az 3 olan minimum Hamming distance ile tasarlanır ve 2 bit hatayı tespit edebilir, 1 bit hatayı düzeltebilir. Bu özellik, veri iletiminde güvenilirliği artırır.

7. **Checksum'un Veri İletişimindeki Rolü Nedir?**
   - Checksum, veri bütünlüğünü kontrol etmek için kullanılır. Gönderici, veri bloklarının toplamını hesaplar ve bu toplamı veriyle birlikte gönderir. Alıcı, aynı hesaplamayı yaparak gönderilen ve hesaplanan toplamları karşılaştırır.

8. **Cyclic Kodlar ve CRC'nin Veri İletişimindeki Kullanımı Nedir?**
   - Cyclic kodlar, özel lineer blok kodlardır ve döngüsel (cyclic) özellikleri sayesinde hata kontrolünde etkilidir. CRC, bu tür kodları kullanarak veri iletiminde oluşabilecek hataları tespit eder ve en çok LAN ve WAN ağlarında kullanılır.

9. **Lineer Blok Kodların Temel Özellikleri ve Kullanım Alanları Nelerdir?**
   - Lineer blok kodlar, XOR işlemiyle iki codeword arasında başka bir geçerli codeword üretebilme özelliğine sahiptir. Bu kodlar, veri iletişiminde hata kontrolü için yaygın olarak kullanılır.

10. **Two-Dimensional Parity Check'in Avantajları ve Kullanımı Nedir?**
    - Two-dimensional parity check, veri dizilerinde hem satır hem de sütun bazında parity bitler ekleyerek hata kontrolü sağlar. Bu yöntem, özellik

1. **Veri Bağı Katmanının İki Temel İşlevi**: Veri bağı katmanının iki temel işlevi, hata tespiti ve akış kontrolüdür. Hata tespiti, veri paketlerinin bozulmadan doğru bir şekilde alıcıya ulaştığından emin olmak için kullanılır. Akış kontrolü ise veri iletim hızını düzenleyerek gönderici ve alıcı arasında veri yoğunluğunun dengelenmesini sağlar.

2. **Framing Süreci**: Framing süreci, veri akışını anlamlı paketler halinde bölerek veri iletiminde sıralama ve organizasyon sağlar. Bu, veri bağlantısının her iki ucundaki cihazların, iletilen verilerin başlangıç ve bitiş noktalarını anlamasına yardımcı olur.

3. **Byte Stuffing Yaklaşımı**: Byte stuffing, özel kontrol karakterlerinin veri içinde doğal olarak ortaya çıkması durumunda iletim hatalarını önlemek için kullanılır. Bir kontrol karakteri veri akışında ortaya çıktığında, belirli bir kaçış karakteri eklenir, böylece alıcı bu karakterleri veri olarak değil, kontrol karakterleri olarak tanır.

4. **Karakter Temelli ve Bit Temelli Framing**: Karakter temelli framing, veri paketlerinin karakter sınırlarına göre düzenlenmesidir, örneğin ASCII karakterleri. Bit temelli framing ise veri bitlerinin dizilimine dayanır ve her frame bit düzeyinde sınırlanır.

5. **Akış Kontrolünün Rolü ve Önemi**: Akış kontrolü, gönderici ve alıcının veri işleme kapasiteleri arasındaki uyumu sağlamak için gereklidir. Bu kontrol, veri kaybını önlemek ve verimli bir iletim sağlamak için ağ trafiğini düzenler.

6. **Simplest Protocol**: Simplest Protocol, temel bir veri iletim protokolüdür ve genellikle hata olasılığının düşük olduğu ve basit iletimlerin gerektiği durumlarda kullanılır. Bu protokol, gönderici ve alıcının sırayla tek bir mesaj göndermesini ve almasını sağlar.

7. **Stop-and-Wait Protokolü**: Stop-and-Wait protokolü, bir paket gönderildikten sonra onay alınıncaya kadar yeni bir paket göndermeyi durduran bir yöntemdir. Bu protokol, düşük verimlilik ve yüksek güvenilirlik sunar ve özellikle düşük hata oranı olan ağlarda etkilidir.

8. **Gürültüsüz ve Gürültülü Kanallar için Protokoller**: Gürültüsüz kanallar için basit protokoller yeterlidir. Gürültülü kanallarda ise daha gelişmiş ARQ (Automatic Repeat Request) protokollerine ihtiyaç duyulur.

9. **ARQ Sistemlerinin İşlevi ve Çalışması**: ARQ sistemleri, iletilen verilerin doğruluğunu kontrol eder ve hata tespit edildiğinde yeniden iletim yapılmasını sağlar. Bu sistemler, veri bütünlüğünü ve güvenilir iletimi sağlar.

10. **Piggybacking Tekniği**: Piggybacking, bir ACK sinyalinin veri paketi içine yerleştirilmesi yöntemidir. Bu, veri iletiminde verimliliği artırır çünkü ayrı bir ACK paketi gönderme ihtiyacını ortadan kaldırır.

Go-Back-N ARQ ve Stop-and-Wait ARQ, veri iletişiminde hata kontrolü ve akış kontrolü için kullanılan iki yöntemdir.

Stop-and-Wait ARQ:
- Bu yöntemde, bir veri paketi gönderildikten sonra gönderici, karşı taraftan onay (ACK) veya negatif onay (NAK) alana kadar bekler.
- Gönderici, her paket için karşı taraftan yanıt alana kadar sıradaki paketi göndermez.
- Bu yöntemin basit yapısı, düşük veri hızı ve yüksek gecikme süreleri ile ilişkilendirilir.
- Verimlilik, özellikle uzun gecikme süreleri olan ağlarda düşüktür.

Go-Back-N ARQ:
- Bu yöntemde, gönderici birden fazla paket gönderebilir ve belirli bir pencere boyutu içinde onay bekler.
- Bir hata tespit edildiğinde, hatalı paketten sonraki tüm paketler yeniden gönderilir (geriye giderek).
- Yüksek veri hızları ve daha az gecikme sürelerine sahiptir.
- Verimlilik, paket kayıplarının düşük olduğu ve yüksek bant genişliğine sahip ağlarda artar.

Karşılaştırma:
- **Verimlilik**: Go-Back-N, Stop-and-Wait'e göre daha verimlidir çünkü birden fazla paketi arka arkaya gönderebilir.
- **Kaynak Kullanımı**: Stop-and-Wait daha az kaynak kullanır ancak Go-Back-N daha fazla bellek ve işlem gücü gerektirir.
- **Uygulama Karmaşıklığı**: Stop-and-Wait daha basit bir yapıya sahiptir; Go-Back-N daha karmaşıktır.
- **Tercih Edilen Kullanım Senaryoları**: Düşük bant genişliği ve yüksek gecikme süreleri olan ortamlarda Stop-and-Wait, yüksek bant genişliği ve düşük gecikme süreleri olan ortamlarda Go-Back-N tercih edilir.

1. **High-level Data Link Control (HDLC) Protokolünün Ana İşlevi**: HDLC, veri bağı katmanında güvenilir veri iletimi sağlamak için tasarlanmıştır. Veri çerçevelerinin bütünlüğünü ve düzgün sıralamasını koruyarak, hata tespiti ve kontrolü yapar.

2. **HDLC'de Kullanılan İki Yaygın İletim Modu**:
   - Normal Response Mode (NRM): Ana istasyonun kontrolünde, ikincil istasyonların sadece ana istasyondan izin aldığında veri gönderebildiği bir mod.
   - Asynchronous Balanced Mode (ABM): Her iki yönde de eşit haklara sahip istasyonlar arasında kullanılır, herhangi bir istasyonun diğerine göre üstünlüğü yoktur.

3. **NRM ve ABM Arasındaki Temel Farklar**:
   - NRM, genellikle bir ana istasyon ve birden fazla ikincil istasyon arasında kullanılır. Ana istasyon kontrolü elinde tutar.
   - ABM'de ise, her istasyon diğerine karşı eşit haklara sahiptir ve bağımsız olarak çalışabilir.

4. **HDLC Framelerinin Temel Türleri**:
   - Information Frames (I-frames): Veri taşıyan ve akış kontrolü sağlayan çerçeveler.
   - Supervisory Frames (S-frames): Hata kontrolü ve akış kontrolü için kullanılır, veri taşımazlar.
   - Unnumbered Frames (U-frames): Sistem yönetimi ve hata düzeltme işlemlerinde kullanılır.

5. **HDLC Frame Yapısının Bileşenleri**:
   - Flag: Çerçevenin başlangıcı ve sonunu belirtir.
   - Address Field: İstasyon adresini tanımlar.
   - Control Field: Çerçeve tipini ve kontrol bilgilerini içerir.
   - Data Field: Taşınan veriyi içerir.
   - Frame Check Sequence (FCS): Hata kontrolü için kullanılır.

6. **PPP ve HDLC Arasındaki Temel Farklar**:
   - HDLC, daha genel ve esnek bir protokoldür. PPP ise özellikle noktadan noktaya bağlantılar için tasarlanmıştır.
   - PPP, ağ katmanı protokollerini taşıyabilirken, HDLC genellikle sadece çerçeveleme ve hata kontrolü için kullanılır.

7. **PPP'nin Sağladığı ve Sağlamadığı Hizmetler**:
   - Sağladığı: Veri çerçevelemesi, hata kontrolü, çoklu protokol desteği, bağlantı kurma ve sonlandırma.
   - Sağlamadığı: Hız ayarlama veya paket sıralama gibi daha üst düzey işlevler.

8. **PPP'de Byte Stuffing**:
   - Byte stuffing, özel kontrol bayraklarının veri içinde yanlışlıkla tanınmasını önlemek için kullanılır. Belirli karakterlerin önüne kaçış karakteri eklenerek bu yanılgıyı önler.

9. **PPP'nin Kimlik Doğrulama İçin Kullandığı İki Protokol**:
   - Password Authentication Protocol (PAP): Basit, iki yönlü el sıkışma protokolü.
   - Challenge Handshake Authentication Protocol (CHAP): Daha güvenli, periyodik doğrulama yapan bir protokol.
   - Fark: CHAP, PAP'e göre daha güvenli ve dinamik bir kimlik doğrulama sunar.

10. **Multilink PPP**:
    - Multilink PPP, birden fazla fiziksel bağlantı üzerinden tek bir lojik bağlantı kurarak bant genişliğini artırır.
    - Genellikle yüksek hız gerektiren veya birden fazla bağlantı yolu olan senaryolarda kullanılır.

1. **Çoklu Erişim Protokollerinin Temel Amacı**:
   Çoklu erişim protokollerinin temel amacı, bir iletişim kanalının birden fazla kullanıcı veya cihaz tarafından etkili ve adil bir şekilde paylaşılmasını sağlamaktır. Bu protokoller, veri çakışmalarını yönetir ve tüm kullanıcıların verilerini uygun bir şekilde iletebilmeleri için kurallar koyar.

2. **ALOHA Protokolünün Temel Prensipleri**:
   ALOHA protokolü, herhangi bir zamanlama veya koordinasyon olmaksızın, kullanıcıların rastgele zamanlarda veri göndermelerine izin verir. Gönderilen veri çakıştığında, belirli bir gecikme süresi sonrasında yeniden deneme yapılır.

3. **Pure ALOHA ve Slotted ALOHA Arasındaki Fark**:
   Pure ALOHA'da kullanıcılar herhangi bir zamanda veri gönderebilirken, Slotted ALOHA zaman aralıklarını (slotları) kullanarak veri gönderimini düzenler. Bu zamanlama, veri çakışmalarını azaltır ve verimliliği artırır.

4. **Slotted ALOHA'nın Verimliliğini Artıran Özellik**:
   Slotted ALOHA'nın verimliliği, zaman aralıklarının (slotların) kullanımıyla artırılır. Bu, aynı anda birden fazla kullanıcının veri göndermesi ihtimalini azaltır ve böylece çakışma olasılığını düşürür.

5. **CSMA Protokolünün Temel İşlevi**:
   Carrier Sense Multiple Access (CSMA), bir kullanıcı veri göndermeden önce iletim kanalını dinleyerek başka bir kullanıcının veri gönderip göndermediğini kontrol eder. Bu, çakışma riskini azaltır.

6. **CSMA'nın Çakışmayı Azaltmak İçin Kullandığı Yöntemler**:
   CSMA, kanalı dinleyerek çakışmaları önlemeye çalışır. Eğer kanal meşgulse, veri gönderimi bir süre ertelenir.

7. **CSMA Türleri Arasındaki Farklar**:
   - **1-Persistent CSMA**: Kanal boşaldığında hemen veri gönderir, çakışma olasılığı yüksektir.
   - **Non-Persistent CSMA**: Kanal meşgulse, rastgele bir süre bekler ve sonra yeniden kontrol eder.
   - **p-Persistent CSMA**: Kanal boşsa, belirli bir olasılıkla veri gönderir veya bekler.

8. **CSMA/CD Protokolünün İşleyişi**:
   Carrier Sense Multiple Access with Collision Detection (CSMA/CD), veri gönderimi sırasında olası çakışmaları algılar. Çakışma tespit edildiğinde, gönderim durdurulur ve belirli bir süre sonra yeniden deneme yapılır.

9. **CSMA/CD'de Çakışma Tespiti**:
   Gönderici, veri gönderirken aynı zamanda kanalı dinleyerek herhangi bir çakışma olup olmadığını kontrol eder. Eğer çakışma algılanırsa, iletim durdurulur ve yeniden deneme için rastgele bir zamanlama kullanılır.

10. **CSMA/CA Protokolü ve CSMA/CD'den Farkı**:
    Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA), çakışmaları önlemeye odaklanır. Çakışmaları algılamak yerine, CSMA/CA, veri göndermeden önce kanalın boş olduğundan emin olmak için ekstra adımlar atar. Bu, özellikle kablosuz ağlarda kullanılır, çünkü kablosuz ortamda çakışmaları algılamak daha zordur.

14. Hafta ders notlarına dayanarak oluşturulan sınav soruları ve cevapları:

1. **Ethernet Nedir ve Ana Özellikleri Nelerdir?**
   - Ethernet, yerel ağlarda (LAN) veri iletimi için kullanılan bir teknolojidir. Basit, ucuz ve zamanla hızı artan bir yapıya sahiptir. Günümüzde anahtarlamalı (switched) yapısı ile çarpışma (collision) sorunlarını ortadan kaldırmıştır.

2. **Ethernet Çerçeve Yapısının Özellikleri Nelerdir?**
   - Ethernet çerçevesi, gönderenin ve alıcının MAC adreslerini, veri yükünü (payload) ve hata kontrolü için CRC'yi içerir. Preamble kısmı alıcı ve gönderici saatlerini senkronize etmek için kullanılır.

3. **Ethernet'in Bağlantısız ve Güvenilmez Yapısı Nasıl Tanımlanır?**
   - Ethernet bağlantısız bir yapıya sahiptir; yani paketler gönderilirken el sıkışma işlemi yapılmaz. Ayrıca güvenilir değildir; alıcı NIC, ACK veya NACK sinyalleri göndermez.

4. **Ethernet Switchlerin İşlevi ve Özellikleri Nelerdir?**
   - Ethernet switchler, Ethernet çerçevelerini alır, depolar ve MAC adresine göre iletir. Şeffaf yapılıdır, yani hostlar switch'in varlığından haberdar değildir ve kendiliğinden öğrenme yeteneğine sahiptir.

5. **Port Tabanlı VLAN Nedir ve Avantajları Nelerdir?**
   - Port tabanlı VLAN, tek fiziksel LAN üzerinde birden çok sanal (mantıksal) LAN tanımlamak için kullanılır. Trafik yalıtımı sağlar ve switch portlarına göre dinamik üyelik sağlar.

6. **MPLS'nin Amaçları ve Avantajları Nelerdir?**
   - MPLS, yüksek hızlı IP yönlendirmesi için sabit uzunluklu etiketleri kullanır. Daha hızlı arama sağlar ve IP datagramında IP adresi bulunsa da yönlendirmede kullanılmaz.

7. **MPLS Yönlendirmesinde Kullanılan Sinyalleme Protokolleri Nelerdir?**
   - MPLS, OSPF ve IS-IS gibi link-state protokollerini kullanır. Giriş MPLS routeri, RSVP-TE protokolünü kullanarak MPLS yönlendirmesini yol üzerindeki routerlarda kurar.

8. **Veri Merkezi Ağlarının Temel Özellikleri Nelerdir?**
   - Veri merkezi ağları, çok sayıda sunucuyu bir araya getirir ve yüksek kullanıcı sayısı, uygulama çeşitliliği, güvenilirlik gereksinimleri ve yük yönetimi gibi zorlukları içerir.

9. **Veri Merkezlerinde Sunucu Diziliminin Avantajları Nelerdir?**
   - Sunucular, raflara dizilir ve her rafta bir dolap başı anahtarı (TOR switch) bulunur. Bu yapı, sunucular arası verimli bağlantı sağlar ve dışarıyla iletişim için sınır yönlendiricileri kullanılır.

10. **Veri Merkezi Ağlarında Yük Dengelemenin İşlevi Nedir?**
    - Yük dengeleyiciler, dışarıdan gelen istekleri alır ve veri merkezi içindeki iş yükünü uygun sunuculara yönlendirir. Böylece veri merkezinin iç işleyişini dış istemcilerden gizler.