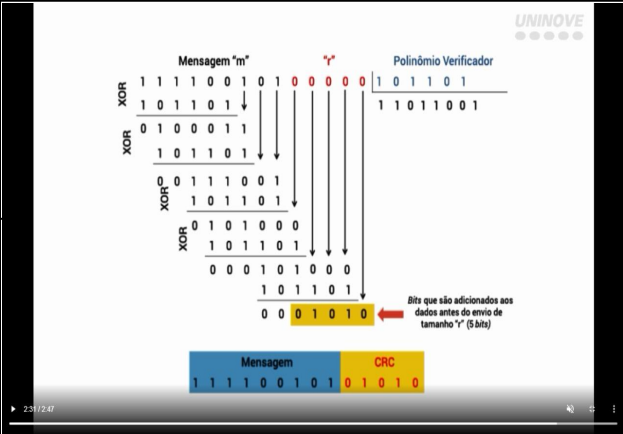
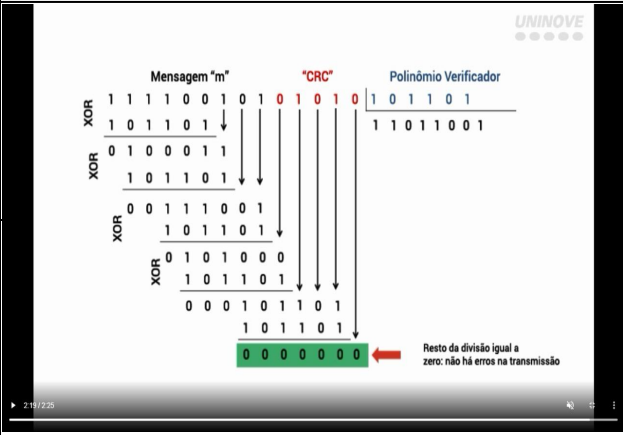


ENLACE - TRATAMENTO DE ERROS DE ENLACE		ENLACE - TRATAMENTO DE ERROS DE ENLACE	
Como a Camada de Enlace auxilia no tratamento de erros de transmissão nas Redes?		A camada de Enlace utiliza protocolos e métodos de detecção e resolução de falhas de transmissão . Como ela faz o intercâmbio entre a camada de rede (Pacote IP) e o camada Física (Bit a Bit), ela acaba se tornando responsável por ordenar os pacotes em quadros que poderão ser facilmente transformados em bits. Junto a essa transformação, essa camada deve usar métodos que façam com que os pacotes não se percam durante a transmissão fim-a-fim. Códigos de comparação de paridade , a subcamada LLC e o protocolo CSMA são usados pela camada de Enlace para impedir que essas falhas aconteçam.	
Que Métodos de Detecção de Erros são os mais utilizados pela Camada de Enlace?		Entre os métodos mais usados, temos: - Paridade Par a Par ; - Detecção de Erros CRC ; - Código Hamming ; - Subcamada LLC ; - Métodos de Controle de Fluxo ; - Protocolo CSMA ;	
Como funciona o método de detecção de erros por Paridade Par a Par ?		O método de medição por Paridade Par a Par é o mais simples, ele compara o número de casas binárias enviados pelo transmissor com os número de casas recebido pelo receptor . Ele faz essa comparação bit a bit, caso um bit não tenha outro para fazer a comparação, a mensagem é interrompida. Por exemplo: Tx = 11010 Rx = 1101_ (Está faltando o último bit) Resultado = Mensagem não enviada	
O que é o método de detecção de erros por CRC (Cyclic Redundancy Code) ?		O método CRC ou Cyclic Redundancy Code (Ciclo de Código de Redundância) é mais seguro que o Paridade Par a Par, pois utiliza um número verificador (é um número aleatório usado pelo algoritmo da transmissão), esse número será utilizado como pólimonio (pólimonios são números que, apesar de terem vários algarismos, usam seus algarismos como coeficientes independentes para fazer uma operações sobre os algarismos de um número variável). Os polimônios do CRC são sempre 6 dígitos , eles operam sobre a mensagem binária da esquerda para a direita com o objetivo de chegar a um resultado binário de 5 algarismos que serão acrescidos a mensagem binária, e usados como número CRC.	
Como funciona o CRC ?		O CRC funciona em 2 etapas , a primeira tem o objetivo de gerar o número CRC que será usado posteriormente pelo receptor para verificar se o CRC combina com o número polimônial usado para a geração dele. Como o número CRC é gerado? Primeiro são acrescidos a mensagem binária 5 dígitos "0" (esses dígitos serão transformados no CRC no final da operação). Depois começa a comparação por através de porta XOR (OU Exclusivo) da mensagem binária e do polinômio de 6 dígitos, sempre pegando os 6 primeiros dígitos à esquerda da mensagem binária, depois é acrescido ao resultado o próximo bit à direita (ou bits caso o resultado dê menos de 6 bits). No final, os últimos 5 dígitos serão transformados em número CRC , que será acrescido a mensagem que será enviada, quando chegar no receptor, ele usará o número CRC para verificar se bate com o número verificador.	
Ilustre como ocorre a 1ª etapa do CRC			
<i>- reservado para a questão acima -</i>			
Como funciona a 2ª etapa do CRC ?		Na segunda etapa a mensagem recebida junto com o número CRC deverá ser comparada polinomialmente com o número verificador de 6 dígitos, igual aconteceu na 1ª etapa. Essa operação deverá ser feita também utilizando portas XOR, a diferença agora está no resultado, o resultado deverá ser totalmente "0" ao final da operação . Isso mostra que a mensagem veio correta, sem acrescentar e nem faltar nenhum bit.	
Ilustre como ocorre a 1ª etapa do CRC			
<i>- reservado para a questão acima -</i>			

ENLACE - TRATAMENTO DE ERROS DE ENLACE	ENLACE - TRATAMENTO DE ERROS DE ENLACE
O que é o método de detecção de erros Código Hamming ?	O método Hamming foi criado por Richard Hamming em 1950 . O objetivo do método Hamming é não apenas mostrar que uma mensagem está errada e interromper uma transmissão, mas além disso consertar a falha para que a mensagem seja enviada corretamente . Ele faz isso por através de algoritmos de comparação XOR que não apenas fazem uma comparação bit a bit, mas fazem uma comparação entre os bits , gerando equações que conseguem identificar a falha e corrigi-la trocando o valor do bit defeituoso pelo valor correto.
Como o protocolo LLC auxilia na detecção e reparação de erros de transmissão?	O protocolo LLC ou Logical Link Control (Controle de Ligação Lógica) é uma subcamada da camada de Enlace. A sub-camada LLC é responsável por separar os dados do pacote IP em frames para que possam ser interpretados pela camada Física, além de interligar vários protocolos de ordenação e fluxos de dados operando na rede . Além disso, o LLC fornece 3 tipos de serviço de transmissão de acordo com a velocidade e segurança da integridade dos dados. E por fim, fornece o controle de fluxo de transmissão , evitando sobrecarga na rede, perca de pacotes e gerenciando a forma como os hosts se comunicam entre si.
Quais são os 3 tipos de Serviço de Controle de Transmissão oferecidos pelo LLC?	Os 3 tipos de Serviços de Controle de Transmissão, são serviços que fornecem conexão lógica entre os hosts e confirmação de recebimento do host receptor. Mas esse fornecimento vai depender do tipo de serviço e da empregabilidade do serviço na aplicação, os 3 são: - Sem Conexão / Sem Confirmação ; - Sem Conexão / Com Confirmação ; - Com Conexão / Com Confirmação ;
Como os 3 Tipos de Serviço de Controle de Transmissão LLC funcionam e em que aplicações eles são melhor empregados ?	- Sem Conexão / Sem Confirmação : não oferece confirmação de conexão host a host, nem de recebimento dos pacotes, é rápida e apropriada para aplicações de tempo real onde a integridade das informações não é importante. Nesses casos geralmente a integridade das informações fica a cargo das camadas superiores; - Sem Conexão / Com Confirmação : não oferece confirmação de conexão, mas exige a confirmação de recebimento dos pacotes por parte dos receptores, é mais empregado em conexões Wi-fi, onde o transmissor tem um timer de espera pela resposta do receptor, que se ultrapassado faz com que a mensagem seja reenviada; - Com Conexão / Com Confirmação : Funciona em 3 etapas - 1ª Estabelece-se a conexão entre hosts; 2ª O ocorre a transmissão dos quadros ordenadamente; 3ª A conexão é encerrada com confirmação, buffers e demais recursos são liberados;
- reservado para a questão acima -	
Como o LLC controla o fluxo de transmissão entre hosts?	O fluxo de uma transmissão precisa ser controlado e uma forma que os hosts receptores não recebam mensagens ao mesmo tempo ocasionando colisão de pacotes, e nem recebam informações além do que os buffers são capazes de aguentar . Por isso, o LLC utiliza 2 processos para controlar o fluxo: - Controle de Fluxo Baseado em FeedBack : Onde o host Receptor deixa os hosts Transmissores cientes da sua situação atual; - Controle de Fluxo Baseado em Velocidade : Onde o Transmissor, com base nas informações do Receptor, consegue calcular o tempo adequado para transmitir sua mensagem sem congestionar o Receptor;
O que é o CSMA ?	O CSMA ou Carrier-Sense Multiple Access (Capacidade de Dedução de Múltiplos Acessos) é um protocolo utilizado pelo LLC para controlar o fluxo de transmissão por através dos processos baseados em FeedBack e Velocidade de Transmissão. O CSMA utiliza algoritmos que tomam ações diferentes de acordo com a carga da rede e a sua velocidade atual de transmissão. Ele faz isso por através do recebimento constante de mensagens de aviso sobre o fluxo da rede.
Quais são os Algoritmos utilizados pelo CSMA?	O CSMA utiliza os seguintes algoritmos: - CSMA No-Persistent : nesse algoritmo enquanto os hosts Tx observam que Rx está ocupado, eles entram em modo de espera com um timer aleatório. Sua desvantagem é que eles não são avisados quando a rede desocupa, se derem sorte eles a encontram desocupada; - CSMA Persistent : o Tx fica escutando a rede todo o tempo, na espera por uma brecha para enviar a mensagem, assim que a brecha é aberta ele envia. A desvantagem é que se dois Tx estiverem no modo CSMA Persistent eles vão enviar a mensagem ao mesmo tempo assim que a brecha for aberta, gerando então a colisão de pacote; - CSMA P-Persistent : o Tx fica escutando a rede todo o tempo na espera por uma brecha, mas além disso, ele também fica escutando alertas de colisão (CSMA/CD ou CSMA/CA), se ele escutar uma alerta de colisão, ele recalcula o tempo de envio de acordo com o timer da colisão para que sua mensagem não colida futuramente. - CSMA/CD (Collision Detector) : o CSMA/CD (Detector de Colisões) é um algoritmo usado em conjunto com os outros, ele fica procurando por colisões na rede, quando as encontra ele envia por toda a rede uma mensagem de 48 bits onde informa qual foi a colisão e quanto tempo os hosts devem esperar para realizar uma retransmissão sem que uma futura colisão ocorra. Esse algoritmo também é conhecido por LWT (Listen While Talk), ele é mais utilizado em redes Ethernet. - CSMA/CA (Collision Avoidance) : o CSMA/CA (Preventiva de Colisão) é um algoritmo também utilizado em conjunto com outros algoritmos, que em vez de detectar colisões que já aconteceram, procura prevenir colisões por enviar quadros RTS (Solicitação de Envio) e só enviar a mensagem quando recebe um CTS (Confirmação de Transmissão). Ele é comumente usado em redes Wi-fi.
- reservado para a questão acima -	
- reservado para a questão acima -	