Why is the guard band necessary to use in FDM and not in TDM?

In Frequency Division Multiplexing (FDM), the available bandwidth is divided into multiple frequency bands, with each band assigned to a different communication channel. A guard band is a narrow frequency range that separates two ranges of wider frequency. This ensures that simultaneously used communication channels do not experience interference, which would result in decreased quality for both transmissions1. In Time Division Multiplexing (TDM), time slots are assigned to the signal at the initial level, so there is no need for guard bands to prevent inter-channel crosstalk2.

How does DSSS achieve bandwidth spreading and provides privacy?

Direct-sequence spread spectrum (DSSS) is a spread-spectrum modulation technique primarily used to reduce overall signal interference. The direct-sequence modulation makes the transmitted signal wider in bandwidth than the information bandwidth. After the despreading or removal of the direct-sequence modulation in the receiver, the information bandwidth is restored, while the unintentional and intentional interference is substantially reduced3. DSSS spreads signal over wide bandwidth to obtain multipath and interference rejection. DSSS rejects narrowband interference power by roughly the spreading gain and multipath by the spreading code autocorrelation evaluated at the multipath delay. So this autocorrelation is the key to multipath rejection4.

Four functions of the data link layer. The four functions of the data link layer are:

Framing: The data link layer receives packets from the network layer, divides them into frames, and sends those frames bit-by-bit to the physical layer5.

Addressing: The data link layer encapsulates the source and destination’s MAC address/physical address in the header of each frame to ensure node-to-node delivery5.

Error Control: The data link layer detects errors in transmitted data and corrects them using error detection and correction techniques5.

Flow Control: The data link layer synchronizes the sender’s and receiver’s speeds and establishes flow control between them to prevent overflow in the receiver’s buffer and loss of frames5.

Discuss the importance of calculating the minimum Hamming distance during the making of codewords in Blocking coding technique. The minimum Hamming distance between two codewords is defined as the number of positions in which they differ. It is an important parameter in block coding because it determines how many errors can be detected and corrected by a code. A code with a larger minimum Hamming distance can detect and correct more errors than a code with a smaller minimum Hamming distance. For example, if a code has a minimum Hamming distance of d, it can detect up to d-1 errors and correct up to floor((d-1)/2) errors6.

What is “Taking Turns” MAC protocols? How is Polling better than CSMA/CD, state three points.

“Taking Turns” MAC protocols are media access control protocols that coordinate transmissions from different stations by taking turns. There are two main types of “Taking Turns” MAC protocols: Polling and Token Passing. In Polling, a master node invites slave nodes to transmit in turn7. Polling can be better than CSMA/CD (Carrier Sense Multiple Access with Collision Detection) because:

It eliminates collisions that can occur when multiple stations transmit simultaneously.

It avoids empty slots that can occur when no station has data to transmit.

It can provide more predictable performance because transmission opportunities are scheduled.

Channelization protocols do not require any central controller to ensure multiple access resolution - True/False? Justify. True. Channelization protocols such as Frequency Division Multiple Access (FDMA), Time Division Multiple Access (TDMA), Code Division Multiple Access (CDMA), Space Division Multiple Access (SDMA), and Orthogonal Frequency Division Multiple Access (OFDMA) do not require any central controller to ensure multiple access resolution. Instead, they coordinate transmissions from different stations by dividing the available channel resources such as frequency, time, code or space among multiple users8.

How can you calculate the vulnerable time of CSMA? In Carrier Sense Multiple Access (CSMA), vulnerable time is considered as propagation time (Tp). Propagation time is defined as the time it takes for a signal to travel from one end of a transmission medium to another end9.

In CSMA/CD, what happens when two nodes sense the carrier at the same time? How can we stop the nodes from sensing the channel at the same time? In Carrier Sense Multiple Access with Collision Detection (CSMA/CD), if two nodes sense that the carrier is idle at the same time, they may both start transmitting simultaneously, resulting in a collision. When this happens, both nodes will detect the collision and stop transmitting their frames immediately. They will then transmit jam signals to ensure that all other nodes on the network detect the collision before waiting for a random backoff period and attempting to retransmit their frames10. To prevent nodes from sensing the channel at the same time, various techniques such as exponential backoff or priority schemes can be used to introduce randomness or differentiation in the transmission attempts of different nodes.

Suppose, you are using fiber optic cable and you want the density of the core to remain constant from the center to the edges. Illustrate the diagram. What will the figure look like if you vary the densities? I’m sorry, but I don’t have enough information to accurately answer this question. Could you please provide more context or clarify what you mean by “density of the core”?

What is the difference between CSMA/CD and CSMA/CA? Explain with examples.

CSMA/CD (Carrier Sense Multiple Access with Collision Detection) and CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) are both media access control protocols used in local area networks. The main difference between them is how they handle collisions. In CSMA/CD, when a collision is detected, the transmitting stations immediately stop transmitting and wait for a random backoff period before attempting to retransmit their frames. This approach is commonly used in wired Ethernet networks10. In contrast, CSMA/CA attempts to avoid collisions altogether by using techniques such as InterFrame Spacing (IFS), Contention Window (CW), and Acknowledgments (ACK) to coordinate transmissions from different stations. This approach is commonly used in wireless networks such as Wi-Fi11.

List some strategies in CSMA/CA that are used to avoid collision. Some strategies used in Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) to avoid collisions include:

InterFrame Spacing (IFS): Stations wait for a period of time called IFS after sensing that the channel is idle before attempting to transmit.

Contention Window (CW): Stations choose a random backoff period from a contention window before attempting to transmit.

Acknowledgments (ACK): Positive acknowledgments and retransmission mechanisms are used to ensure successful transmission of frames.

Request to Send/Clear to Send (RTS/CTS): Stations can use RTS and CTS control frames to reserve the channel for transmission of data frames