**ID:\_\_\_\_\_\_\_\_\_\_\_\_ Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**DCAN202 Week 11 Tutorial – Data Communication and Networking**

**1. What is the difference between error prevention, error detection, and error control?**

Ans: Error prevention refers to techniques applied to prevent errors from occurring in the first place. These include proper shielding of cables to reduce interference, replacing older media and equipment with new digital components, proper use of digital repeaters and analog amplifiers, and observing the stated capacities of media.

Error detection involves adding extra information to data signals to identify when errors have occurred during transmission. This requires adding an error detection code to the original data. Three basic techniques exist for detecting errors: parity checking, arithmetic checksum, and cyclic redundancy checksum.

Error control encompasses the actions taken once an error has been detected. The receiver can choose from three basic options: simply discard the frame or packet, return a message to the transmitter requesting retransmission of the corrupted data, or correct the error without requiring retransmission using forward error correction techniques.

**2. What are the three basic forms of error control?**

Ans: The three basic forms of error control are: first, doing nothing by simply tossing the corrupted frame or packet; second, returning a message to the transmitter asking it to resend the data packet that was in error; and third, correcting the error without retransmission using techniques such as forward error correction with Hamming codes.

**3. What is white noise and how does it affect a signal?**

Ans: White noise, also known as thermal or Gaussian noise, is a relatively continuous type of noise similar to the static heard when tuning a radio between stations. It depends on the temperature of the transmission medium, with noise levels increasing as temperature rises due to increased electron activity. If white noise becomes too strong, it can completely disrupt the signal, making data transmission unreliable or impossible.

**4. What is crosstalk and how does it affect a signal?**

Ans: Crosstalk represents unwanted coupling between two different signal paths, similar to hearing another conversation while talking on the telephone. This interference is relatively constant and occurs when signals from adjacent transmission lines interfere with each other. Crosstalk can degrade signal quality by introducing unwanted information into the intended signal path, but it can be reduced with proper measures such as improved cable design and spacing.

**5. What is echo and how does it affect data transmission?**

Ans: Echo is the reflective feedback of a transmitted signal as it moves through a medium, much like how a voice echoes in an empty room. In data communications, a signal can hit the end of a cable, bounce back through the wire, and interfere with the original signal. Echo occurs most often on coaxial cable systems. If severe enough, echo can interfere with the original signal, causing data corruption. However, echo is relatively constant and can be significantly reduced through proper system design.

**6. What is jitter and why is it a digital signal problem?**

Ans: Jitter results from small timing irregularities during the transmission of digital signals and occurs when digital signals are repeated over and over. If serious enough, jitter forces systems to slow down their transmission rates to maintain signal integrity. Jitter is particularly problematic for digital systems because it can cause video devices to flicker, audio transmissions to click and break up, and transmitted computer data to arrive with errors, disrupting the precise timing requirements of digital communications.

**7. Will proper shielding of a media increase or decrease the chance of errors?**

Ans: Proper shielding of media will decrease the chance of errors. Shielding reduces interference from external electromagnetic sources, which is one of the primary error prevention techniques. By protecting the transmission medium from external noise sources, proper shielding significantly improves signal quality and reduces the likelihood of data corruption during transmission.

**8. What types of errors will simple parity not detect?**

Ans: Simple parity will not detect even numbers of bit errors. For example, if two bits are corrupted during transmission, the parity check will still show the correct even or odd count, failing to detect the error. This represents the main weakness of simple parity checking, as it only catches odd numbers of bit errors while missing all even-numbered error combinations.

**9. What types of error will longitudinal parity not detect?**

Ans: While longitudinal parity is better at catching errors than simple parity, it still cannot catch all possible error combinations. Specifically, it may fail to detect certain patterns of multiple bit errors that maintain the correct parity in both rows and columns. Additionally, longitudinal parity requires adding too many check bits to a block of data, making it less efficient for practical implementation compared to more advanced error detection methods.

**10. Frame relay practices which form of error control?**

Ans: Frame relay practices the "do nothing" form of error control, where it simply tosses corrupted frames without returning any error message. Frame relay assumes that a higher-level protocol such as TCP/IP will detect the missing frame and request retransmission, delegating error recovery responsibilities to upper protocol layers.

**11. How many packets can be sent at one time using stop-and-wait error control?**

Ans: Stop-and-wait allows only one outstanding packet per transmission channel. After sending a frame, the transmitter awaits an acknowledgment (ACK) before proceeding. While simple to implement, this method underutilizes bandwidth, especially in high-latency networks.

**12. What is the function of an ACK in the stop-and-wait error control?**

Ans: An ACK (positive acknowledgment) in stop-and-wait error control serves to confirm successful receipt of a frame. When the receiver sends an ACK, it signals to the transmitter that the frame was received correctly and that the next frame can be transmitted. This provides confirmation that data transmission was successful and allows the communication process to continue.

**13. What is the function of a NAK in the stop-and-wait error control?**

Ans: A NAK (negative acknowledgment) in stop-and-wait error control signals that an error was detected in the received frame. When the receiver sends a NAK, it indicates to the transmitter that the frame contained errors and needs to be retransmitted. This triggers the transmitter to send the same frame again, ensuring data integrity through retransmission.

**14. What condition must be met for error correction to be performed?**

Ans: For error correction to be performed, a large amount of redundant information must accompany the original data. This redundant information allows the receiver to determine the location and nature of errors and make corrections without requiring retransmission from the sender. This type of error control is called forward error correction and typically involves sophisticated coding schemes such as Hamming codes.

**15. What is impulse noise and why is it the most disruptive?**

Ans: Impulse noise is a noncontinuous noise that represents one of the most disruptive forms of interference in data communications. It typically manifests as an analog burst of energy that occurs sporadically. Impulse noise is considered the most disruptive because it is difficult to remove from analog signals, as it may be hard to distinguish from the original signal. Additionally, impulse noise can damage more bits when data is transmitted at faster rates, as the bits are closer together temporally, allowing a single noise burst to affect multiple data bits simultaneously.