Quiz 1

Past Questions

With CSMA/CD, a sender can be sure that there is no collision at 2τ time units after the start of the transmission. What are the parameters affecting τ?

The propagation delay τ can be derived from the signal propagation delay and the maximum length of the wire (channel).

In order to detect a collision reliably, it is necessary that frames have a minimum size. How can the required minimum size of a frame be determined from τ?

The minimum frame size is the number of bits needed to fill the channel until 2τ time units have passed. In other words, the minimum frame size is $\frac{2\tau}{b}$ where b is the bit width (transmission time for a single bit).

Briefly explain the term "p-persistent" CSMA/CD and why it is useful to choose $p < 1$

With p-persistent CSMA/CD, a sender sensing an unused channel will start sending data with probability p. Choosing $p < 1$ is useful for reducing collisions in situations where multiple senders wait for a longer transmission to finish.

Let τ be the propagation delay between two stations with maximum distance. Why can a sender be sure that there is no collision after 2τ time units after the start of the transmission?

In the worst case, a collision happens close to one of the senders, that is after close to τ time units. Since the broken signal needs to travel back to both sender's involved, the worst case for both senders to be aware of a collision is close to 2τ time units.

Classic Ethernet uses in general 1-persistent CSMA/CD but not after a collision. Why is 1-persistent CSMA/CD not used always?

With 1-persistent CSMA/CD after a collision, the likelihood of repeated collisions would be very high and significantly reduce the throughput.

Explain briefly how the CSMA/CD media access control scheme works

To gain access to the medium, stations first sense a carrier signal. If the medium is not busy, a station starts to transmit data and listens for possible collisions. If a collision has been detected, the procedure is repeated after a backoff time.

Why does CSMA/CD not work well on a wireless network?

In wireless networks, collisions can occur close to a receiver while the involved senders do not detect this collision due to attenuation

Explain the meaning of the end-to-end argument, one of the design principles of the Internet protocol suite.

All functions which require knowledge of the state of end-to-end communication should be realized at the endpoints of a network and not within the network. This simplifies the network core and enables scalability of the core network.

Explain the term Autonomous System and how it relates to Interior Gateway (Routing) Protocols and Exterior Gateway (Routing) Protocols.

An *Autonomous System* is a set of routers and networks under the same administration. An Interior Gateway (Routing) Protocol is used within an Autonomous System to calculate routes while an Exterior Gateway (Routing) Protocol is used to find routes that cross Autonomous Systems.

Give an example of an ordered, decentralized, dynamic, time division multiplexing media access control mechanism

Token passing (e.g., as used by an IEEE 802.5 network) is an example of an ordered, decentralized, dynamic, time division multiplexing media access control mechanism.

What is the main difference between CSMA and CSMA-CD?

CSMA-CD allows the sender to terminate the transmission as soon as a collision has been detected and thus recovers the channel faster

Why does CSMA-CD not work well in wireless networks?

CSMA-CD relies on the assumption that all nodes can hear each other within a bounded amount of time. In wireless networks, the set of nodes in range of a sending node is not the same for all nodes of the network and thus there can be collisions that can not be observed by all nodes.

True/False

T	F	Problem
X		CSMA/CD is not required on a full-duplex ethernet link

T	F	Problem
	X	The hidden station problem is solved by CSMA/CD
	X	Slotted Aloha is a time division multiplexing media access control mechanism
	X	In case of MACA, all stations receiving RTS must send a CTS

Summary

Internet Concepts and Design

Internet Design Principles

- Connectivity is its own reward
- All functions which require knowledge of the state of end-to-end communication should be realized at the endpoints (end-to-end arguments)
- There is no central instance which controls the internet and is able to turn it off
- Addresses should uniquely identify endpoints
- Intermediate systems should be stateless if possible
- Implementations should be liberal in what they accept and stringent in what they generate
- Keep it simple

Autonomous Systems

- The global Internet consists of a set of inter-connected autonomous systems
- An *Autonomous System* (AS) is a set of routers and networks under the same administration
- Autonomous Systems are historically identified by 16-bit numbers, called the AS numbers (now 32-bits)
- IP packets are forwarded between autonomous systems over paths that are established by an *Exterior Gateway Protocol* (EGP)
- Within an autonomous system, IP packets are forwarded over paths that are established by an *Interior Gateway Protocol* (IGP)

Internet - A Scale-free Network?

- **Scale-free**: The probability $P(k)$ that a node in the network connects with k other nodes is roughly proportional to $k^{-\gamma}$
- Examples: social networks, collaboration networks etc
- Properties: short paths, robust against random failures, sensitive to targeted attacks

Classification and Terminology

Network Classifications

- **Distance**
  - Local Area Network (LAN), Wide Area Network (WAN), ...
- **Topology**
  - Star, Ring, Bus, Line, Tree, Mesh, ...
- **Transmission Media**
  - Wireless Network, Optical Network, ...
- **Purpose**
  - Industrial control network (SCADA), media distribution network, access network, aggregation network, backbone network, cloud network, ...
- **Ownership**
  - Home network, National Research Networks (NRENs), Google's network, ...

Communication Modes

- Unicast: Single sender and single receiver (1:1)
- Multicast: Single sender and multiple receivers (1:m)
- Concast: Multiple senders and single receiver (n:1)
- Multipeer: Multiple senders and multiple receivers (n:m)

- Anycast: Single sender and nearest receiver out of a group of receivers
- Broadcast: Single sender and all receivers attached to a network
- Geocast: Single sender and all receivers attached to a network

Communication Protocol

- A *protocol* is a set of rules and formats that govern the communication between communicating peers
  - set of valid messages (syntax of messages)
  - meanings of each message (semantics of messages)
- A protocol is necessary for any function that requires cooperation between communicating peers
- A protocol provides ideally a well-defined service
- It is often desirable to layer new protocols on already existing protocols in order to reuse services

Circuit vs Packet Switching

- **Circuit switching**
  - Communication starts by creating a (virtual) circuit between sender and receiver
  - Data is forwarded along (virtual) circuit
  - Communication ends by removing the (virtual) circuit
  - Example: Traditional telecommunications networks
- **Packet switching**
  - Data is carried in packets

    - Every packet carries information identifying the destination
    - Every packet is routed independently of other packets to its destination
    - Example: Internet

Connection-oriented vs Connection-less Services

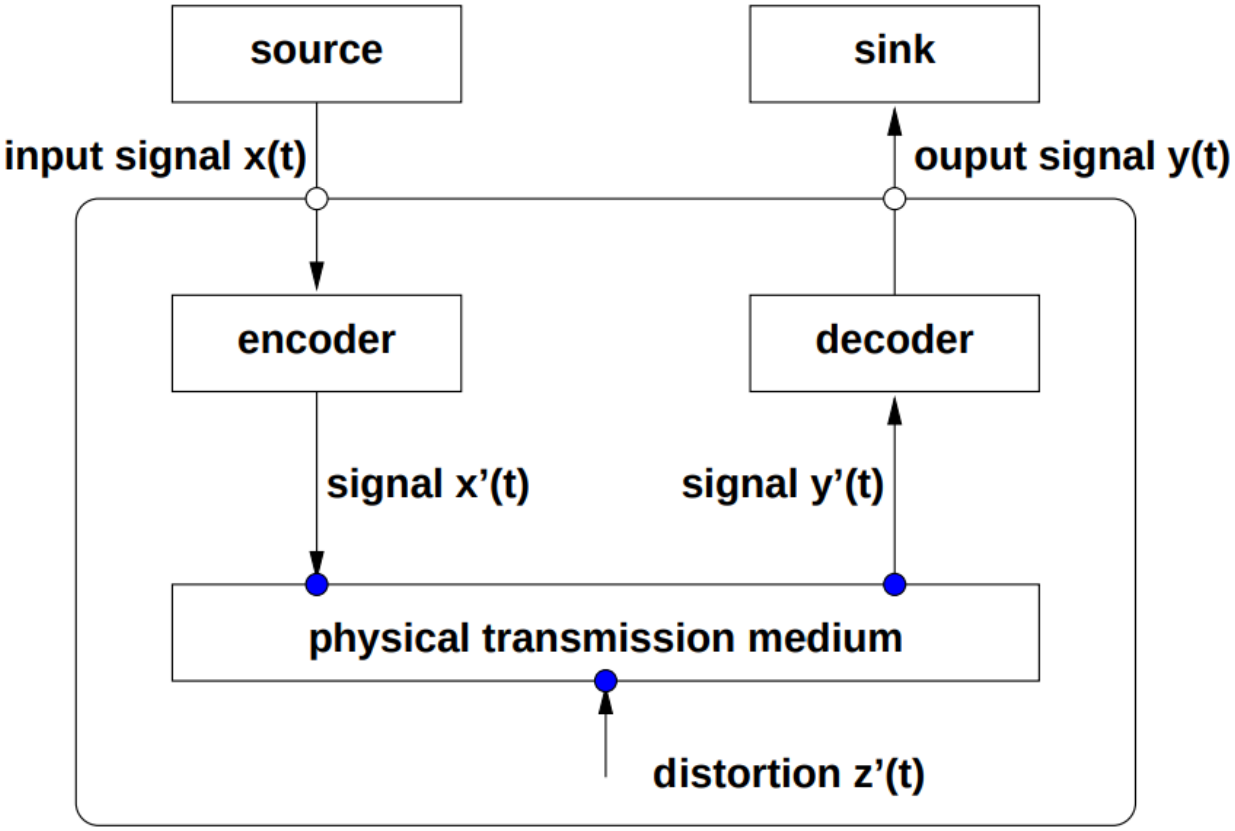
- **Connection-oriented**
    - Usage of a service starts by creating a connection
    - Data is exchanged within the context of a connection
    - Service usage ends by terminating the connection
    - State may be associated with connections (stateful)
    - Example: fetching a web page on the Internet
- **Connection-less**
    - Service can be used immediately
    - Usually no state maintained (stateless)
    - Example: Internet name lookups

Data vs Control vs Management Plane

- **Data Plane**
    - Concerned with the forwarding of data
    - Acting in the resolution of milliseconds to microseconds
    - Often implemented in hardware to achieve high data rates
- **Control Plane**
    - Concerned with telling the data plane how to forward data
    - Acting in the resolution of seconds or sub-seconds
    - Traditionally implemented as part of routers and switches
    - Recent move to separate the control plane from the data plane
- **Management Plane**
    - Concerned with the configuration and monitoring of data and control planes
    - Acting in the resolution of minutes or even much slower
    - May involve humans in decision and control processes

Channels and Transmission Impairments

Communication Channel Model

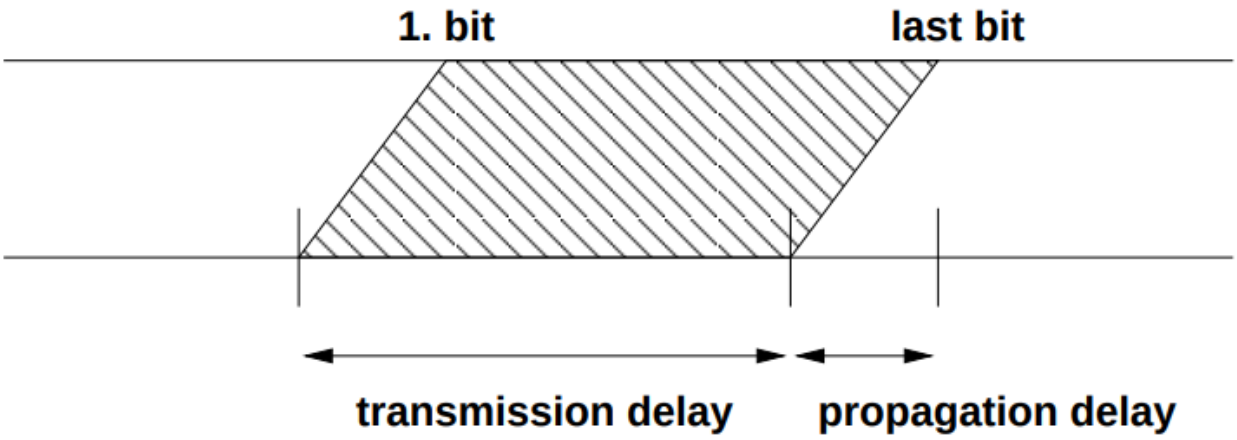


Transmission Impairments

- **Attenuation**
  - The strength of a signal falls off with distance over any transmission medium
  - For guided media, attenuation is generally an exponential function of the distance
  - For unguided media, attenuation is a more complex function of distance and the makeup of the atmosphere
- **Delay Distortion**
  - Delay distortion occurs because the velocity of propagation of a signal through a guided medium varies with frequency
  - Various frequency components of a signal will arrive at the receiver at different times
- **Noise**
  - Thermal noise (white noise) is due to thermal agitation of electrons ans is a function of temperature
  - Inter-modulation noise can occur if signals at different frequencies share the same transmission medium
  - Crosstalk is an unwanted coupling between signal paths
  - Impulse noise consists of irregular pulses or noise spikes of short duration and of relatively high amplitude

Channel Characteristics

- **Data rate** (bit rate) describes the data volume that can be transmitted per time interval (eg. 100Mbit/s)
- **Bit time** is the time needed to transmit a single bit (eg., 1 microsecond for 1 Mbit/s)
- **Delay** is the time needed to transmit a message from the source to the sink. It consists of *propagation delay* and the *transmission* delay
- **Bit error rate** is the probability of a bit being changed during transmission



Media Access Control

Frequency Division Multiplexing (FDM)

Signals are carried simultaneously on the same medium by allocating to each signal a different frequency band.

Wavelength Division Multiplexing (WDM)

- Optical fibers carry multiple wavelength at the same time
- WDM can achieve very high data rates over a single optical fiber
- Dense WDM is a variation where the wavelengths are spaced close together, which results in an even larger number of channels

Time Division Multiplexing (TDM)

- Signals from a given sources are assigned to specific time slots
- time slot assignment might be fixed (synchronous) of dynamic (statistical)

Pure Aloha

- Sender sends data as soon as data becomes available
- Collisions are detected by listening to the signal
- Retransmit after a random pause after a collision
- Not very efficient (18% of the channel capacity)

Slotted Aloha

- Senders do not send immediately but wait for the beginning of a time slot
- Time slots may be advertised by short control signals
- Collisions only happen at the start of a transmission
- Avoids sequences of partially overlaying data blocks

- Slightly more efficient (37% of the channel capacity)

Carrier Sense Multiple Access (CSMA)

- Sense the media whether it is unused before starting a transmission
- Collisions are still possible (but less likely)
- 1-persistent CSMA: sender sends with probability 1
- p-persistent CSMA: sender sends with probability p
- non-persistent CSMA: sender waits for a random time period before it retries if the media is busy

CSMA with Collision Detection (CSMA-CD)

- Terminate the transmission as soon as a collision has been detected (and retry after some delay)
- Let τ be the propagation delay between two stations with maximum distance
- Senders can be sure that they successfully acquired the medium after 2τ time units
- Used by the classic Ethernet developed at Xerox Parc

Multiple Access with Collision Avoidance (MACA)

- A station which is ready to send first sends a short RTS (ready to send) message to the receiver
- The receiver responds with a short CTS (clear to send) message
- Stations who receives RTS or CTS must stay quiet
- Solves the hidden station and exposed station problem

Token

- A token is a special bit pattern circulating between stations - only the station holding the token is allowed to send data
- Token mechanisms naturally match physical ring topologies - logical rings may be created on other physical topologies
- Care must be taken to handle lost or duplicate token

Transmission Error Detection

How to rate networks

- Speed
    - Bitrate
    - Goodput
- Last long
- Reliable
- Cost

Token ring vs CSMA

Token Ring	CSMA

You can calculate the longest delay (deterministic)	If one machine is disconnected there wont be any problems
Better speed	Cheaper
Token needs to be passed constantly, only one at all times.	Longest delay cannot be reliably calculated
If a machine detaches that currently owns the token, the whole network is blocked	

Transmission Error Detection

- Simple parity bits can be added to code words to detect bit b_nb_{n-1}...b_1b_0errors, however, aren't very strong in detecting errors which affect multiple bits
- Computation of error check codes must be efficient

Cyclic Redundancy Check (CRC)

A bit sequence (bit block) $b_n b_{n-1} \dots b_1 b_0$ is represented as a polynomial $B(x) = b_n x^n + b_{n-1} x^{n-1} + \dots + b_1 x + b_0$. A generator polynomial $G(x) = g_r x^r + \dots + g_1 x + g_0$ with $g_r = 1$ and $g_0 = 1$ is agreed upon between the sender and the receiver. The sender transmits $U(x) = x^r \cdot B(x) + t(x)$ with $t(x) = (x^r \cdot B(x)) \mod G(x)$. Then the receiver tests whether the polynomial corresponding to the received bit sequence can be divided by $G(x)$ without a remainder.

- Efficient hardware implementation possible using XOR gates and shift registers
- Only errors divisible by $G(x)$ will go undetected

Choosing Generator Polynomials

- $G(x)$ detects all single-bit errors if $G(x)$ has more than one non-zero term
- $G(x)$ detects all double-bit errors, as long as $G(x)$ has a factor with three terms
- $G(x)$ detects any odd number of errors, as long as $G(x)$ contains the factor $(x + 1)$
- $G(x)$ detects any burst errors for which the length of the burst is less than or equal to r
- $G(x)$ detects a fraction of error bursts of length $r + 1$; the fraction equals to $1 - 2^{-r}$
- $G(x)$ detects a fraction of error bursts of length greater than $r + 1$; the fraction equals to $1 - 2^{-r}$

Internet Checksum

Properties

- Summation is commutative
- Computation independent of the byte order
- Computation can be parallelized on processors with word sizes larger than 16-bit
- Individual data fields can be modified without having to recompute the whole checksum

- Can be integrated in a copy loop
- Often implemented in assembler or special hardware

Further Error Situations

- Despite bit errors, the following transmission errors can occur:
    - Loss of complete data frames
    - Duplication of complete data frames
    - Receipt of data frames that are never sent
    - Reordering of data frames during transmission
- The sender must adapt its speed to the speed of the receiver (end-to-end flow control)
- The sender must react to congestion situations in a network (congestion control)