CAN

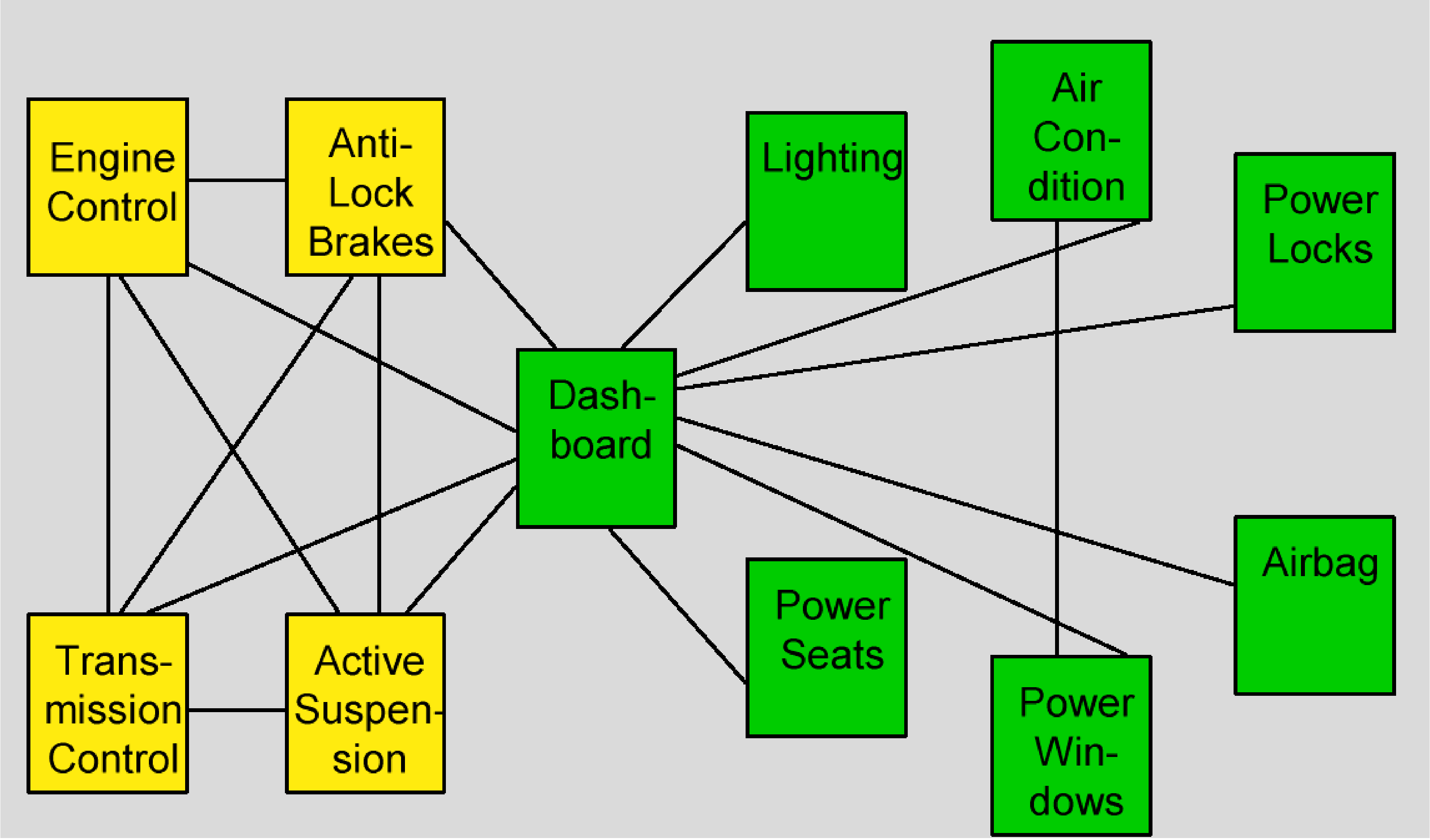
ECE 3710

only three letter
acronyms/initialisms allowed, apparently

If at first you don't succeed, then skydiving definitely isn't for you.

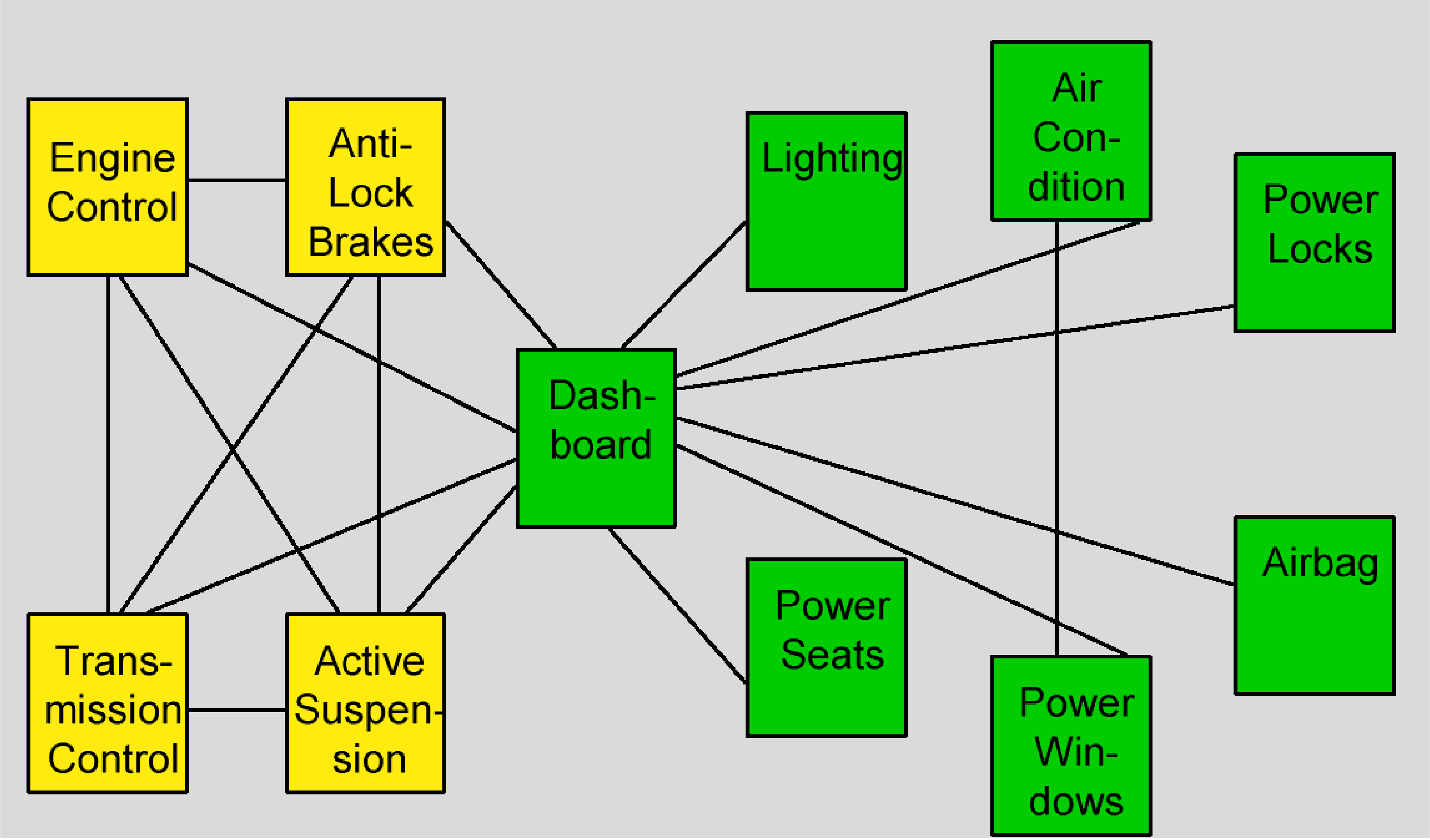
- Steven Wright

networked systems in a vehicle:



Q: problems?

networked systems in a vehicle:



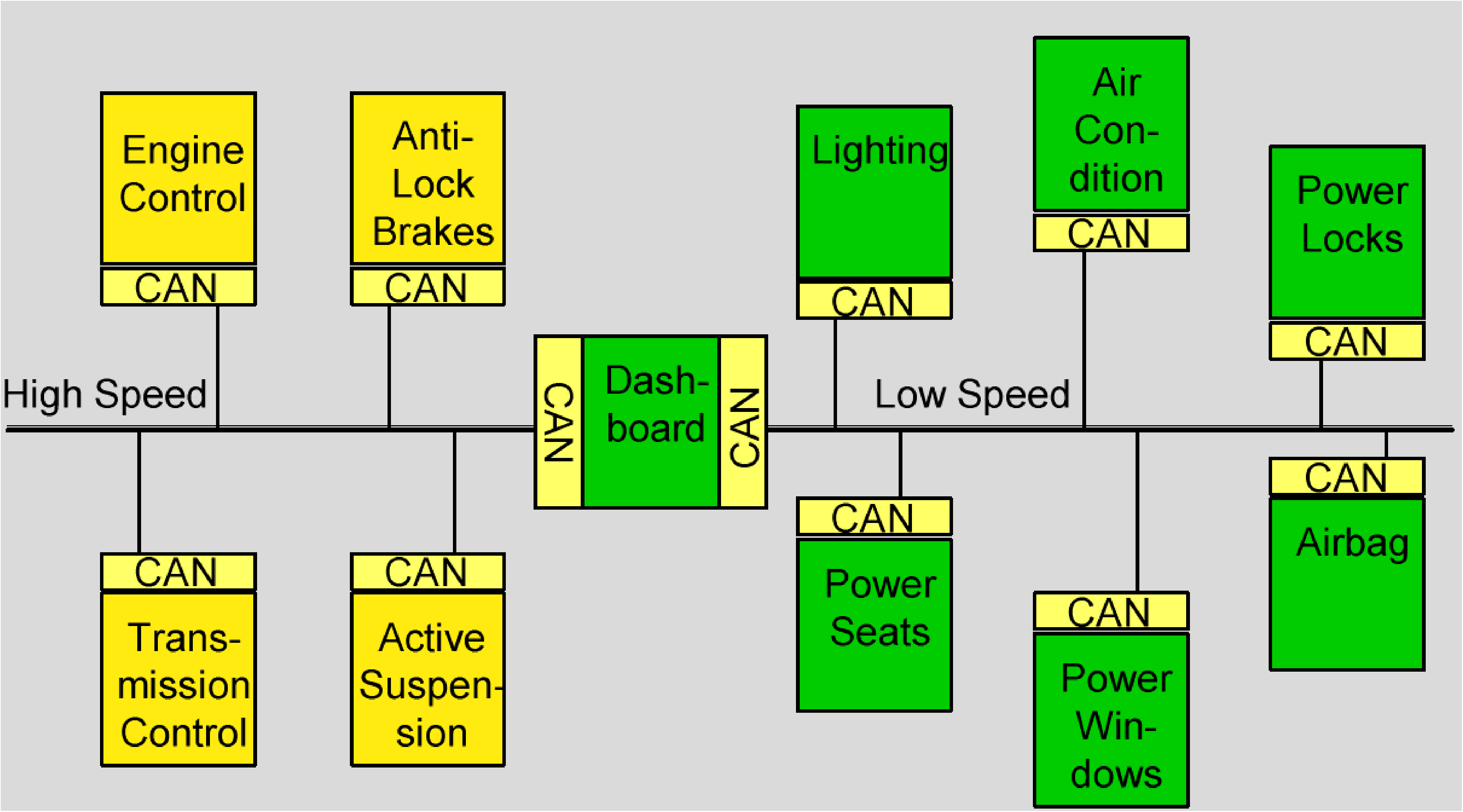
Q: problems?

A:

1. new system, new wires
2. multiple ways to cause catastrophic problem

(multiple points of failure)

Controller **A**rea **N**etwork:



1. originally for vehicle control systems
2. any system where multiple entities (uC, etc) need to communicate

simplification of embedded systems networks:

CAN

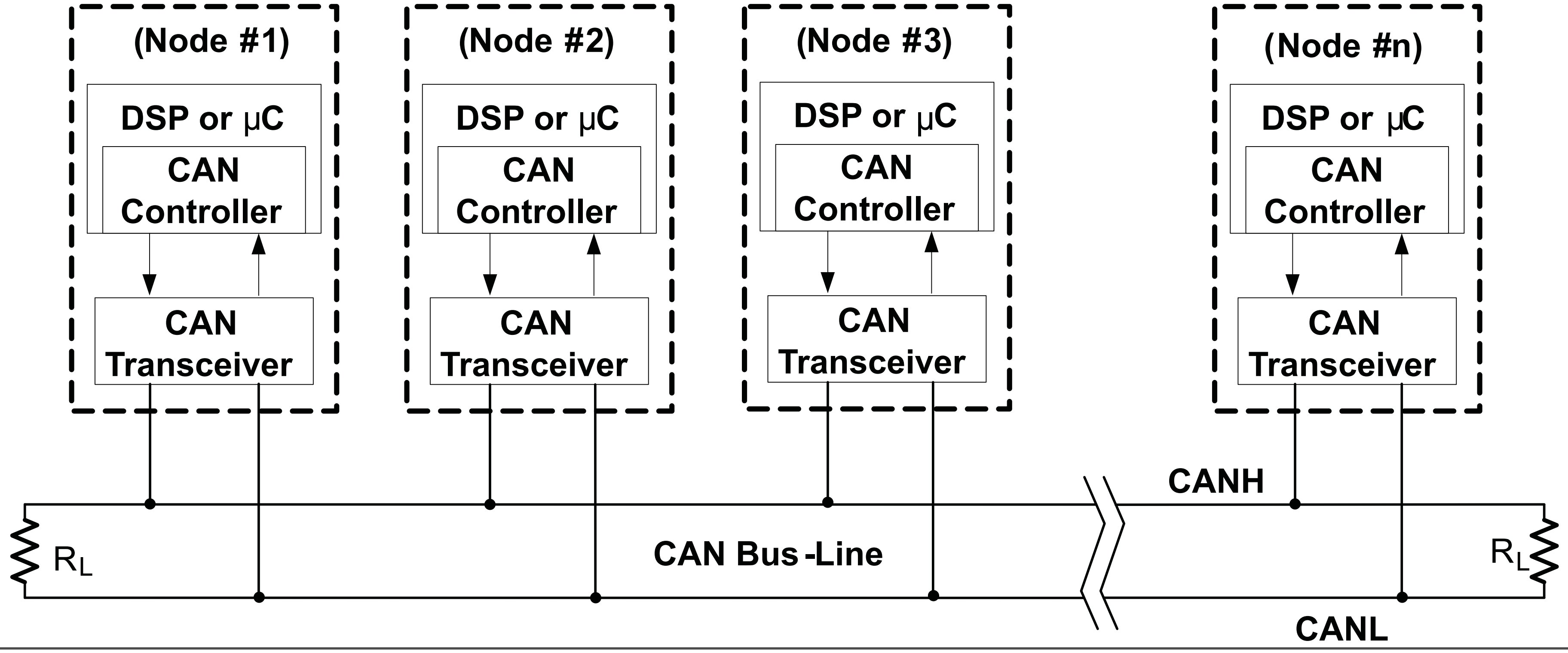
data is broadcast and devices decide if they need to respond

features:

1. no addresses
2. priorities
3. multiple access w/o central authority

more important data sent first

each device monitors line, stops transmitting if higher priority data



two or one wire

(if short, no termination)

CAN data frame

(three others)

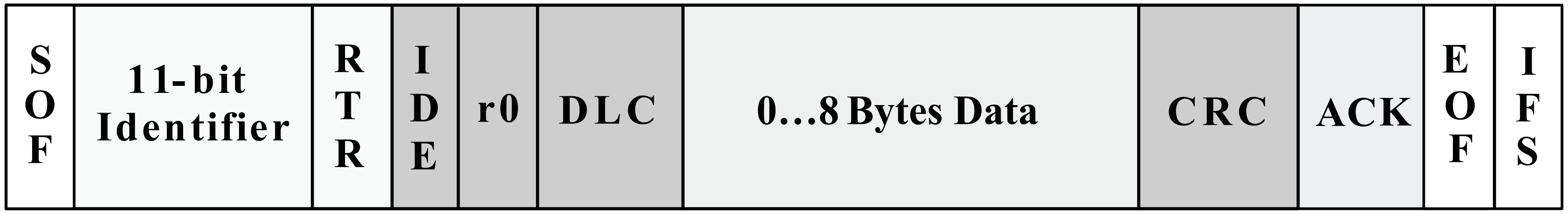
1. what is data about

2. priority

(lower is higher priority)

standard or extended frame

checksum for error detection



start of frame

request data from another device

unused bit

how many bytes of data follow

ack: next slide

end of frame

delay until next frame

CAN data frame

(three others)

ack:

each node (device on network) must acknowledge error-free RX or sender retransmits

how?
all in the signalling
(think open drain bus)

CAN data frame

(three others)

in data frame

problem: too many 1's or 0's
in a row

(clocks lose sync)

solution

bit stuffing:

1. after five 1's add zero
2. after five 0's add one

e.g.,

TX: 11111101 becomes TX: 111110101

TX: 00000111 becomes TX: 000001111

receiver: sees five X's, discards next bit

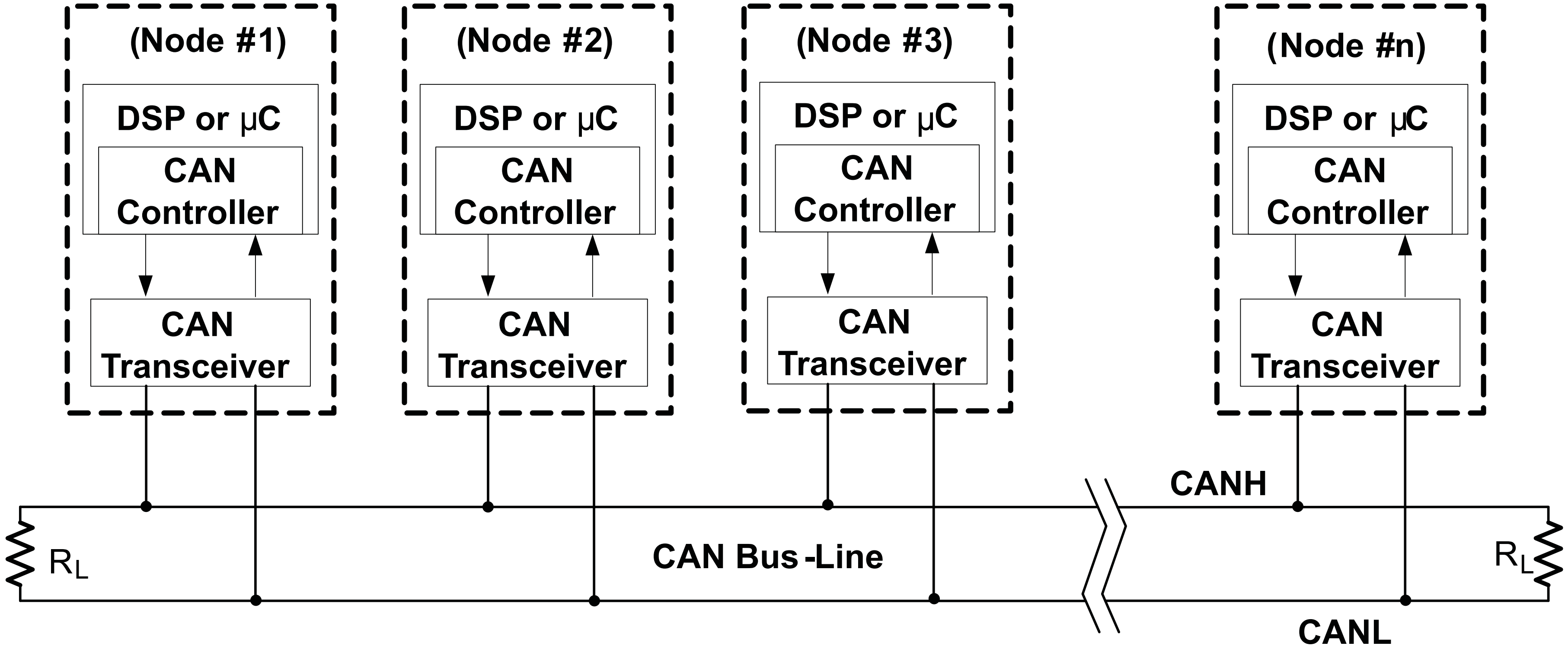
CAN physical layer

for resiliency to interference
(wired Ethernet, too)

to determine
logic value
(at receiver)

differential signal:
bit = CANH - CANL

active low:
0: if CANH - CANL = 2 V
1: if CANH - CANL = 0 V



assume
5V CAN

CAN physical layer

CANH:

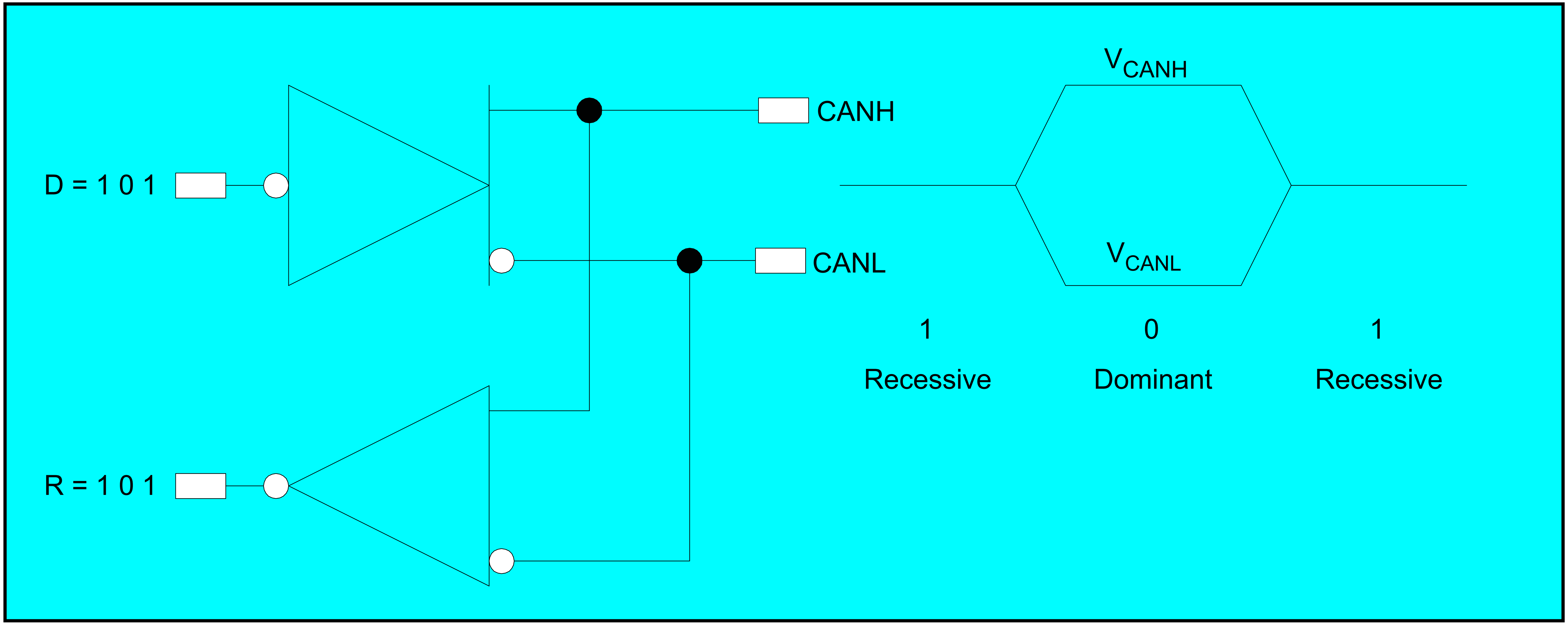
if ‘1’ output 2.5 V

if ‘0’ output 3.5 V

CANL:

if ‘1’ output 2.5 V

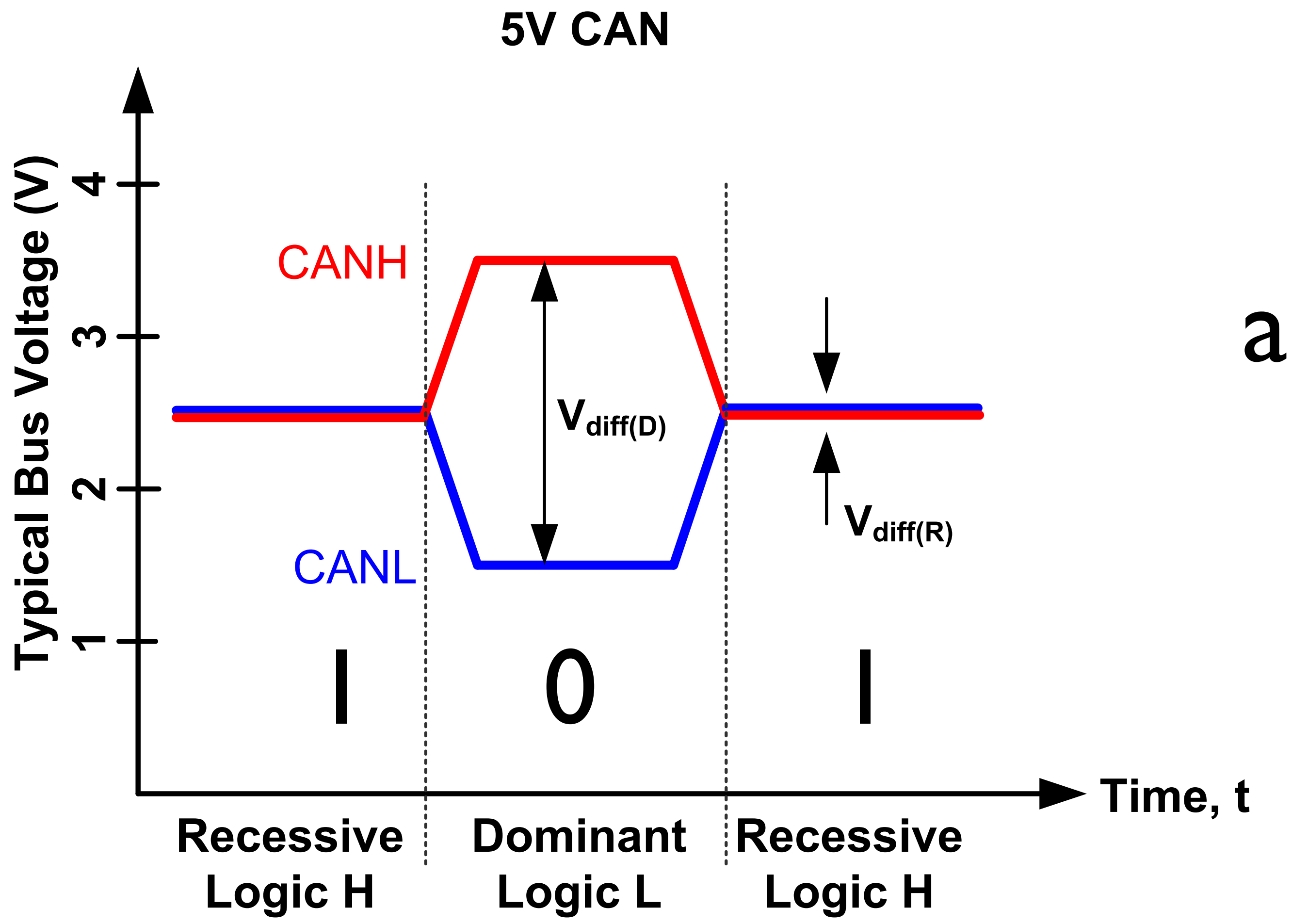
if ‘0’ output 1.5 V



CAN physical layer

CANH/L pins behave like open drain:

1. default of both is 2.5 V
2. CANH can be brought higher
3. CANL can be brought lower



active low:

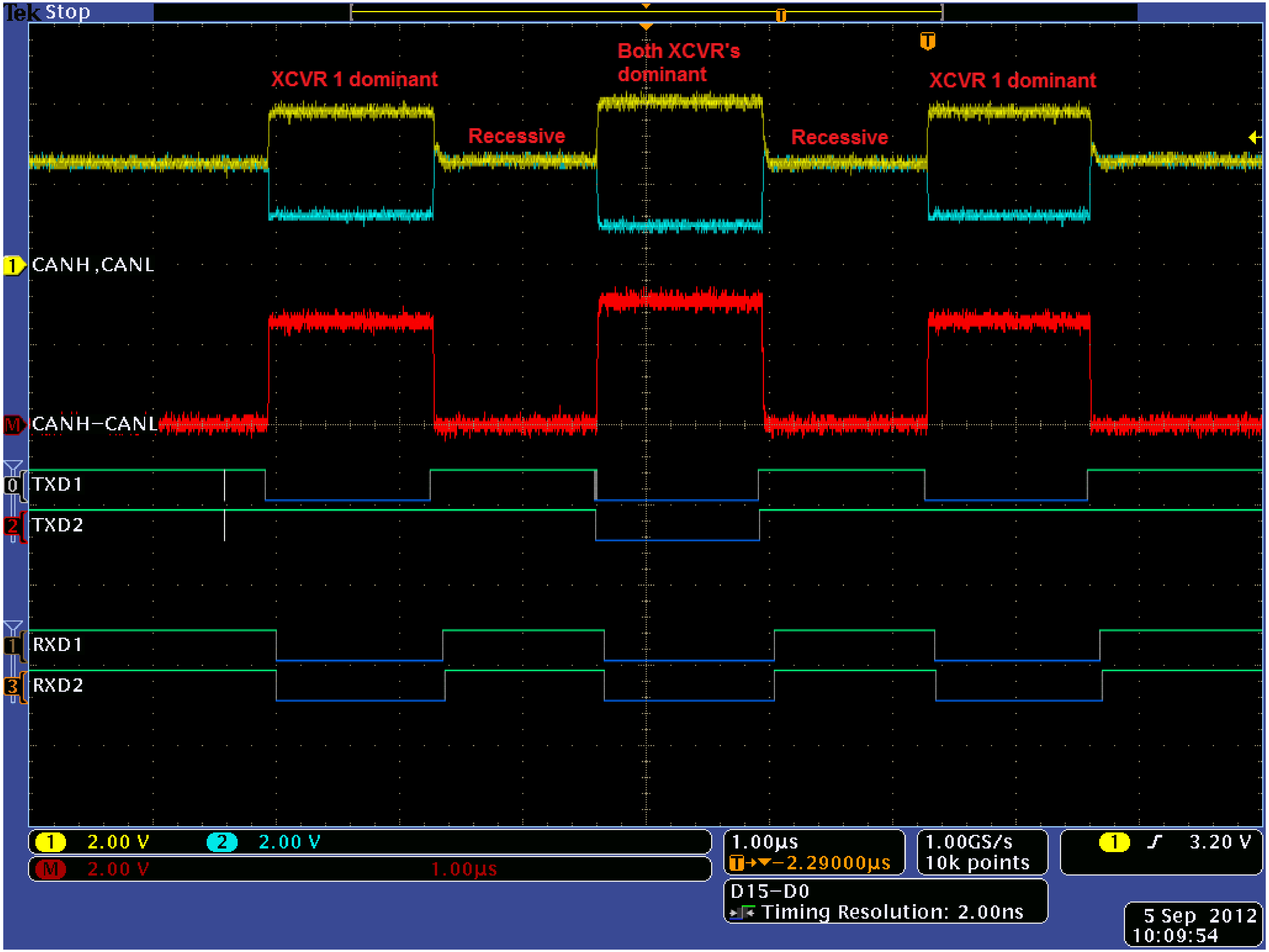
0: if CANH - CANL = 2 V

(3.5-1.5=2)

1: if CANH - CANL = 0 V

(1.5-1.5=0)

CAN physical layer



bus
(CANH/L)

differential calc at receiver

device1 TX
device2 TX

device1 RX
device2 RX

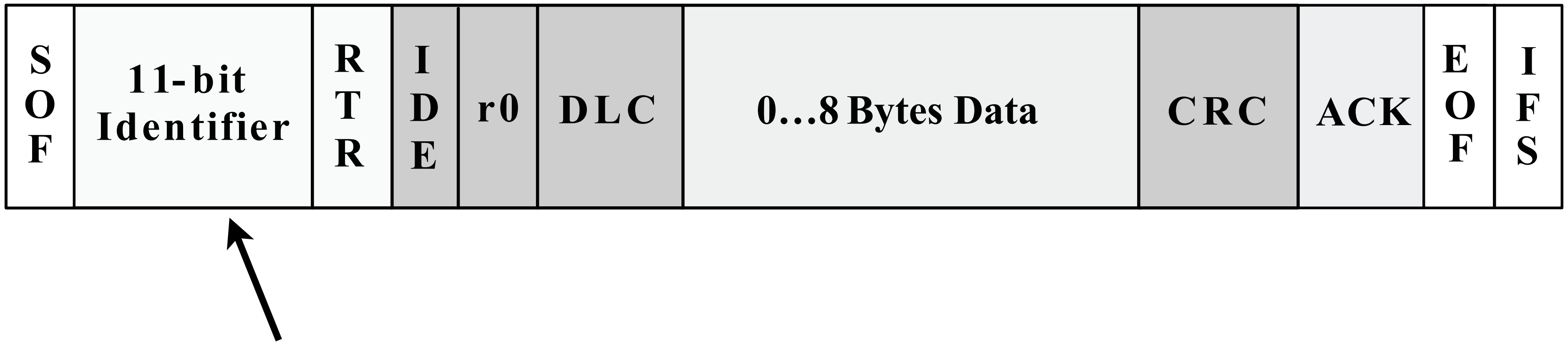
what RX sees during TX

CAN priorities

device1 and device2 TX
at same time

←

IDs of frame
are different
(ID1=1010101, ID2=1110111)

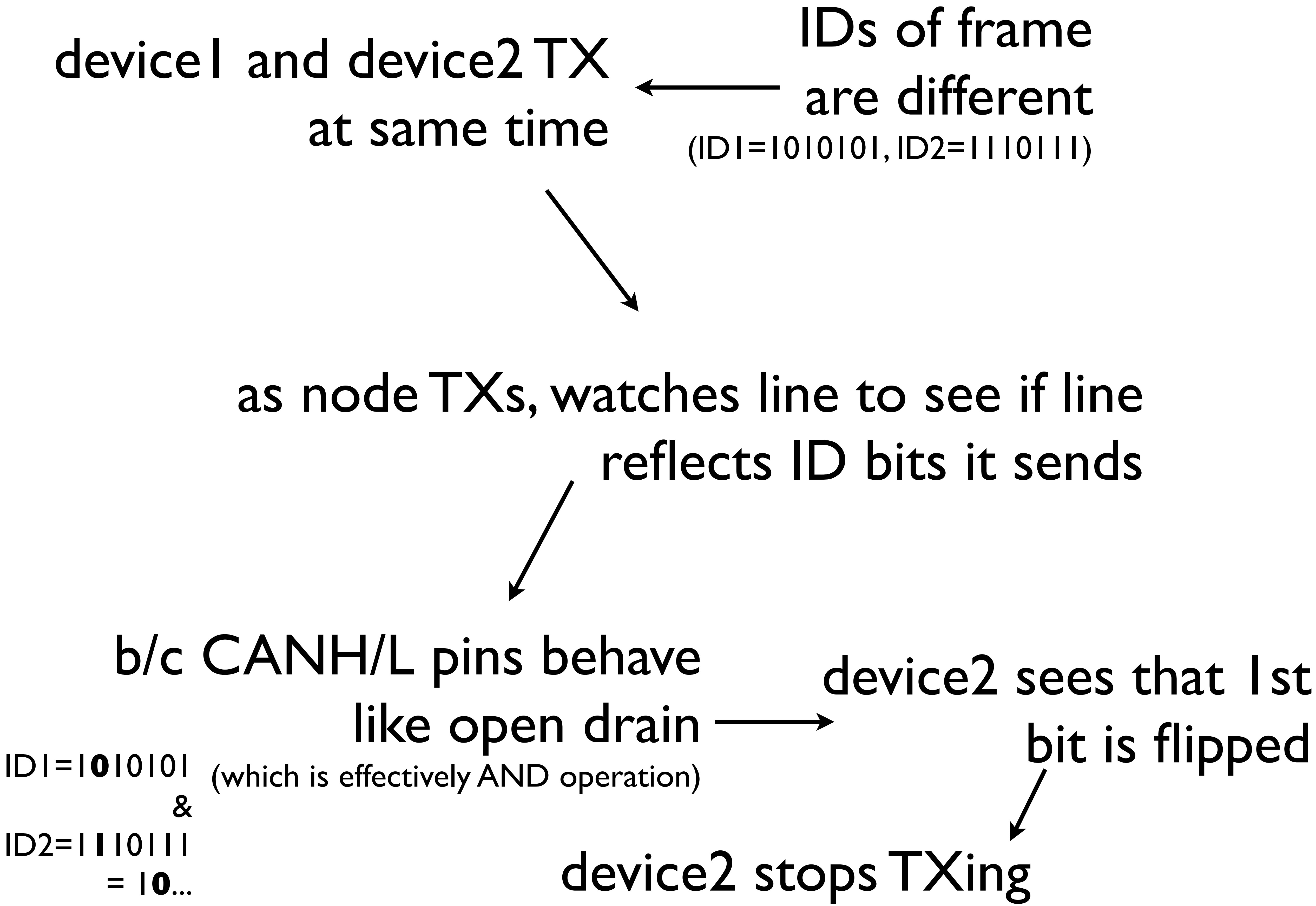


SOF	11-bit Identifier	RTR	IDE	r0	DLC	0…8 Bytes Data	CRC	ACK	EOF	IFS

MSB TX first

CAN priorities

(MSB TX first)



device1 and device2 TX at same time

IDs of frame are different (ID1=1010101, ID2=1110111)

as node TXs, watches line to see if line reflects ID bits it sends

b/c CANH/L pins behave like open drain (which is effectively AND operation)

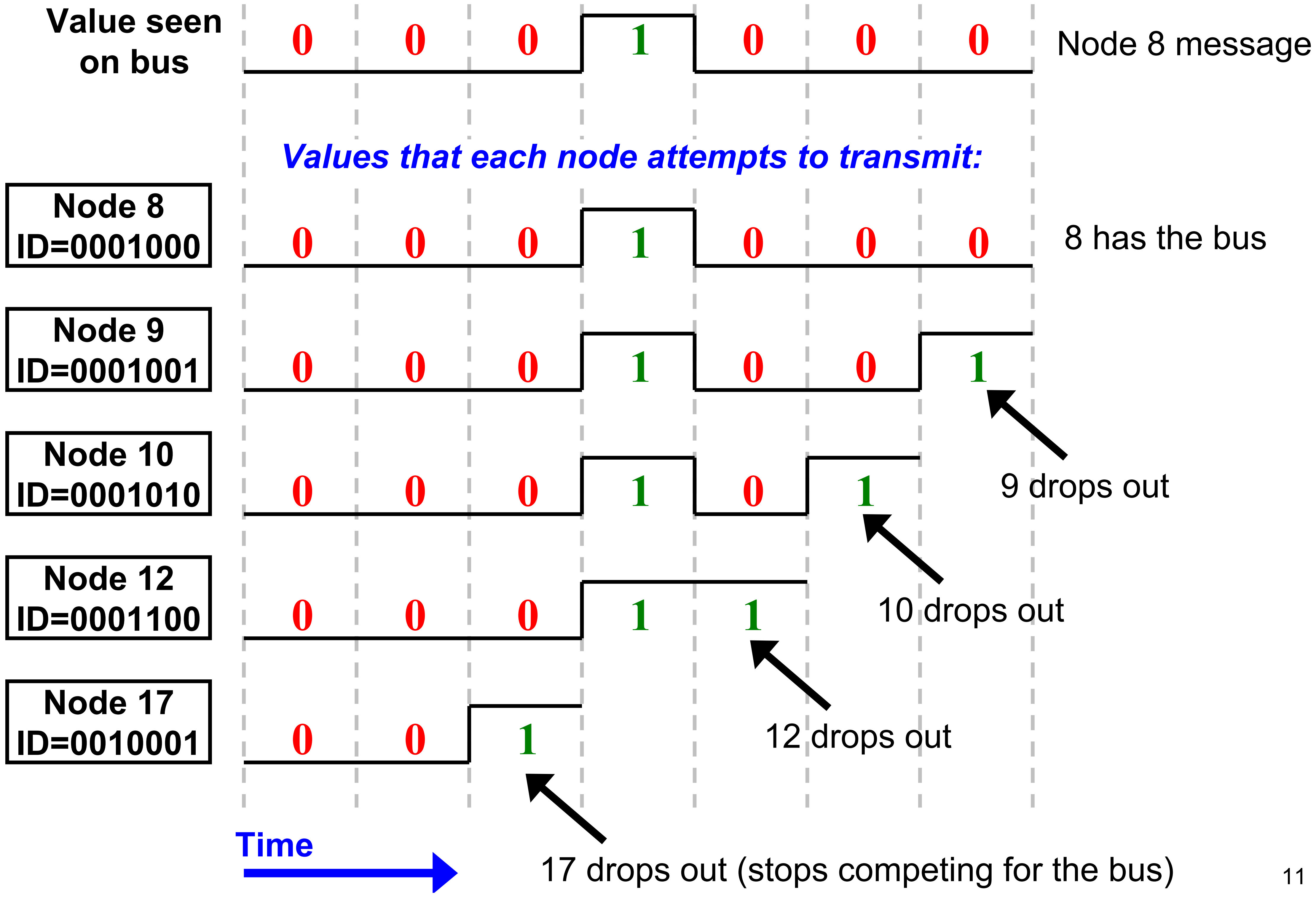
ID1=1**0**10101
&
ID2=1**1**10111
= 1**0**...

device2 sees that 1st bit is flipped

device2 stops TXing

CAN priorities

(MSB TX first)



Value seen on bus

0 0 0 1 0 0 0

Node 8 message

Values that each node attempts to transmit:

Node 8 ID=0001000

0 0 0 1 0 0 0

8 has the bus

Node 9 ID=0001001

0 0 0 1 0 0 1

9 drops out

Node 10 ID=0001010

0 0 0 1 0 1

10 drops out

Node 12 ID=0001100

0 0 0 1 1

12 drops out

Node 17 ID=0010001

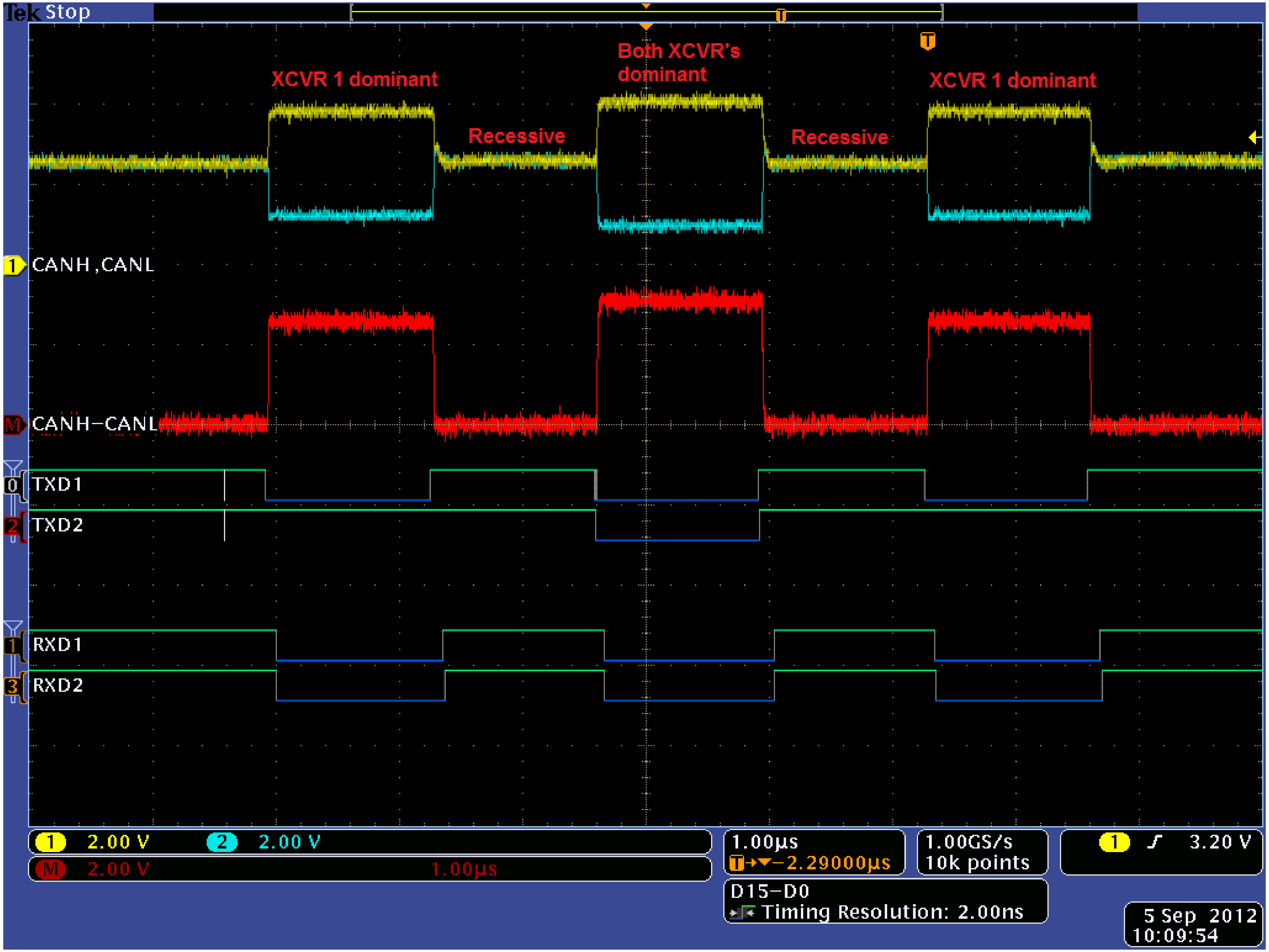
0 0 1

17 drops out (stops competing for the bus)

Time

lowest ID will always win ⟶ lower ID, higher priority

CAN physical layer



1 2.00 V 2 2.00 V

M 2.00 V 1.00µs

1.00µs T→▼−2.29000µs

1.00GS/s 10k points

1 ʃ 3.20 V

D15−D0 Timing Resolution: 2.00ns

5 Sep 2012 10:09:54

bus (CANH/L)

differential calc at receiver

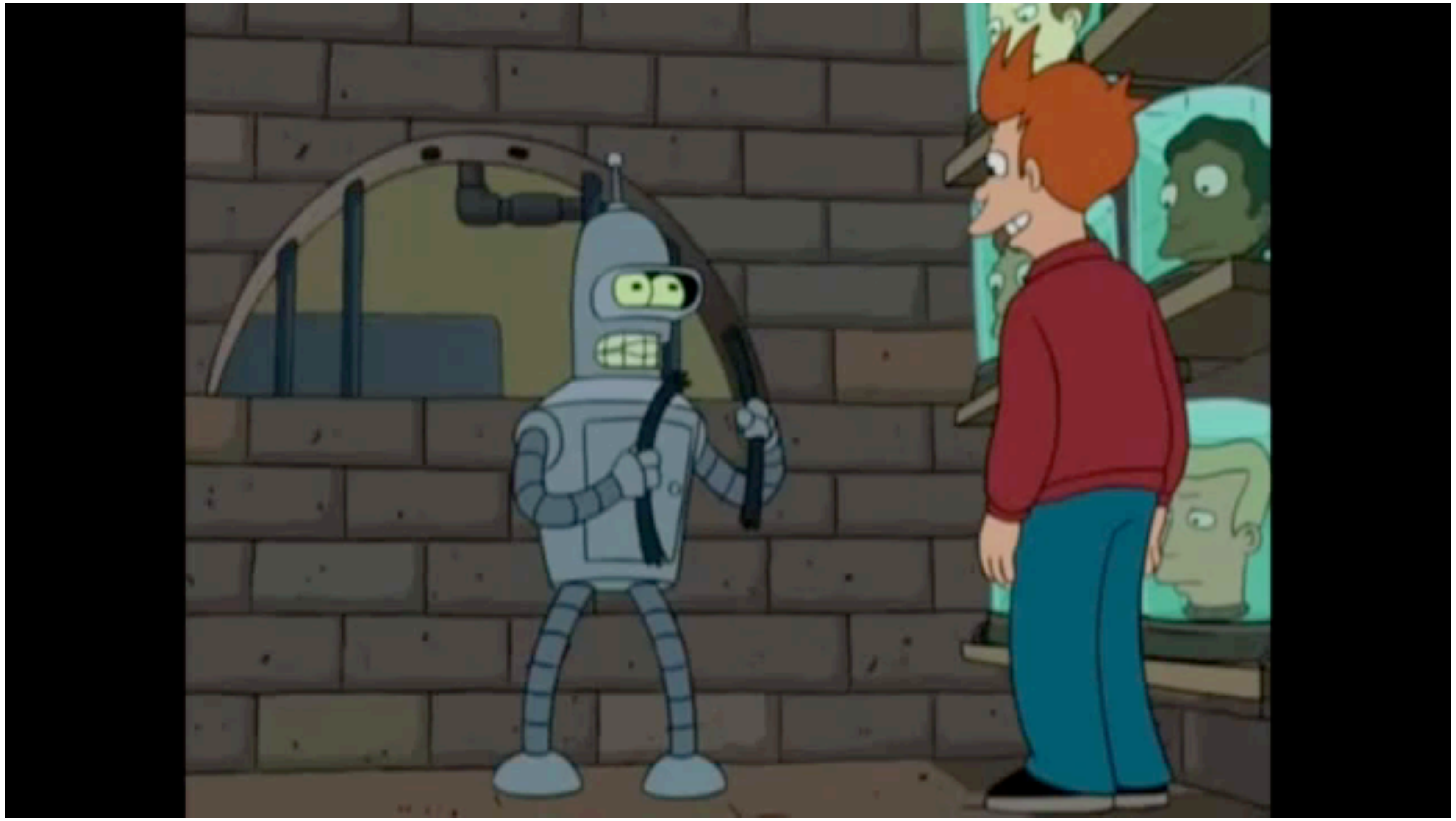
device1 TX
device2 TX
(active high)

device1 RX
device2 RX
(active high)

what RX sees during TX

D1 wins

CAN?



CAN

I try not to think about the implications...

everyone sees what is sent

problems:

1. no confidentiality
2. no authentication
3. can't guarantee availability

anyone can impersonate anyone else

can prevent critical messages from being sent

local access (mechanic)

Experimental Security Analysis of a Modern Automobile by Koscher et al.

remote access (OnStar)

Comprehensive Experimental Analyses of Automotive Attack Surfaces by Checkoway et al.