Impact of the $x^{43} + 1$ Scrambler on the Error Detection Capabilities of the Ethernet CRC

IEEE 802.3 HSSG Meeting, Montreal

July 5-9, 1999

Norival Figueira

Nortel Networks

nfigueir@nortelnetworks.com

NORTEL NETWORKS™

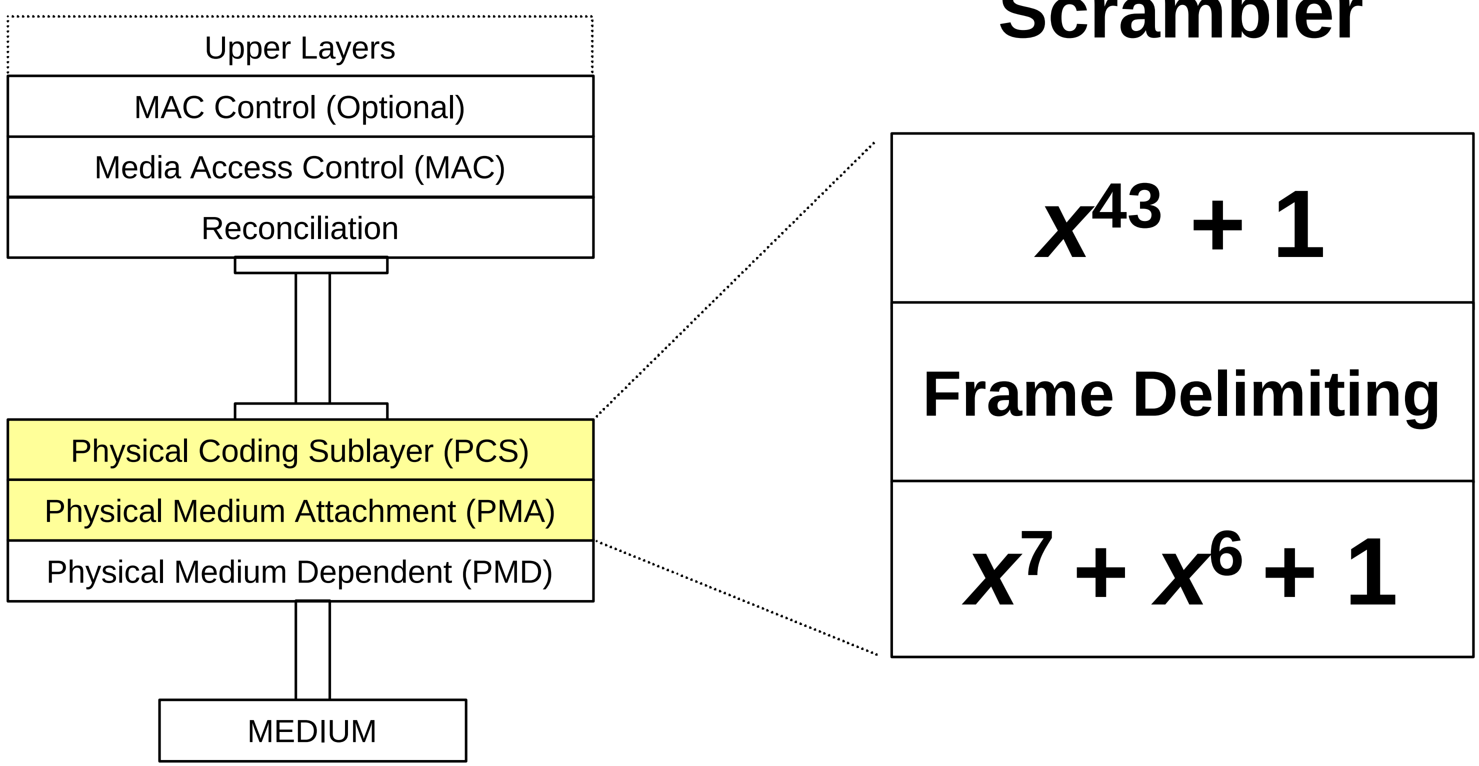
Agenda

- **Scrambled encoding**
- **Error multiplication in self-synchronous scramblers**
  — $x^{43} + 1$ scrambler duplicates bit errors
- **Overall error detection capabilities of Ethernet CRC are not reduced**
  — Given a random error, the probability of undetected errors is the same whether there is an $x^{43} + 1$ scrambler or not

A Scrambler PCS Layer

10 Gigabit Ethernet Reference Model

Scrambler



Scrambler Proposal

- **Two polynomial scrambler system**
  - $x^7 + x^6 + 1$ over all data
  - $x^{43} + 1$ from MAC DA through MAC CRC

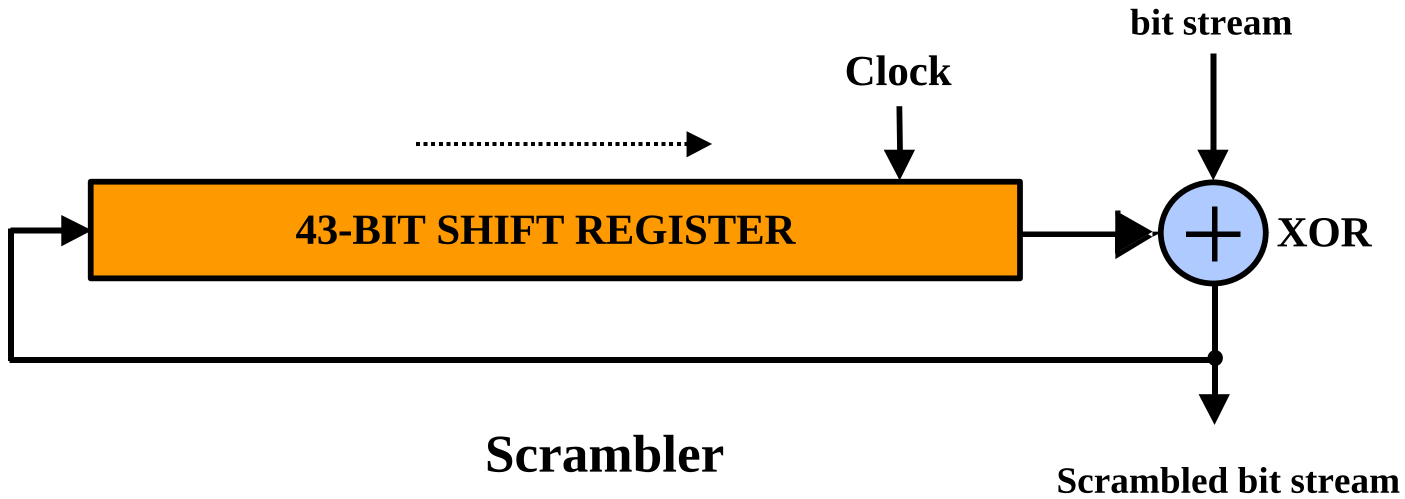
- **Perform frame delimiting using <length> <type><hcs> pointer chains**

- **$x^7 + x^6 + 1$ is periodically resynchronized**

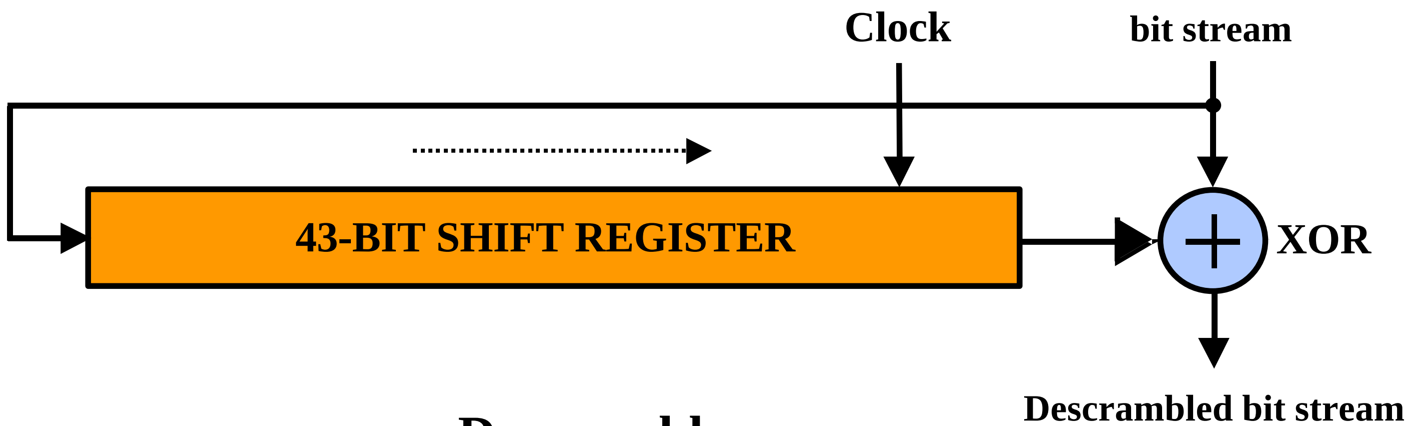
- **$x^{43} + 1$ self synchronizing**

NORTEL NETWORKS™

x^{43} + 1 Scrambler/Descrambler



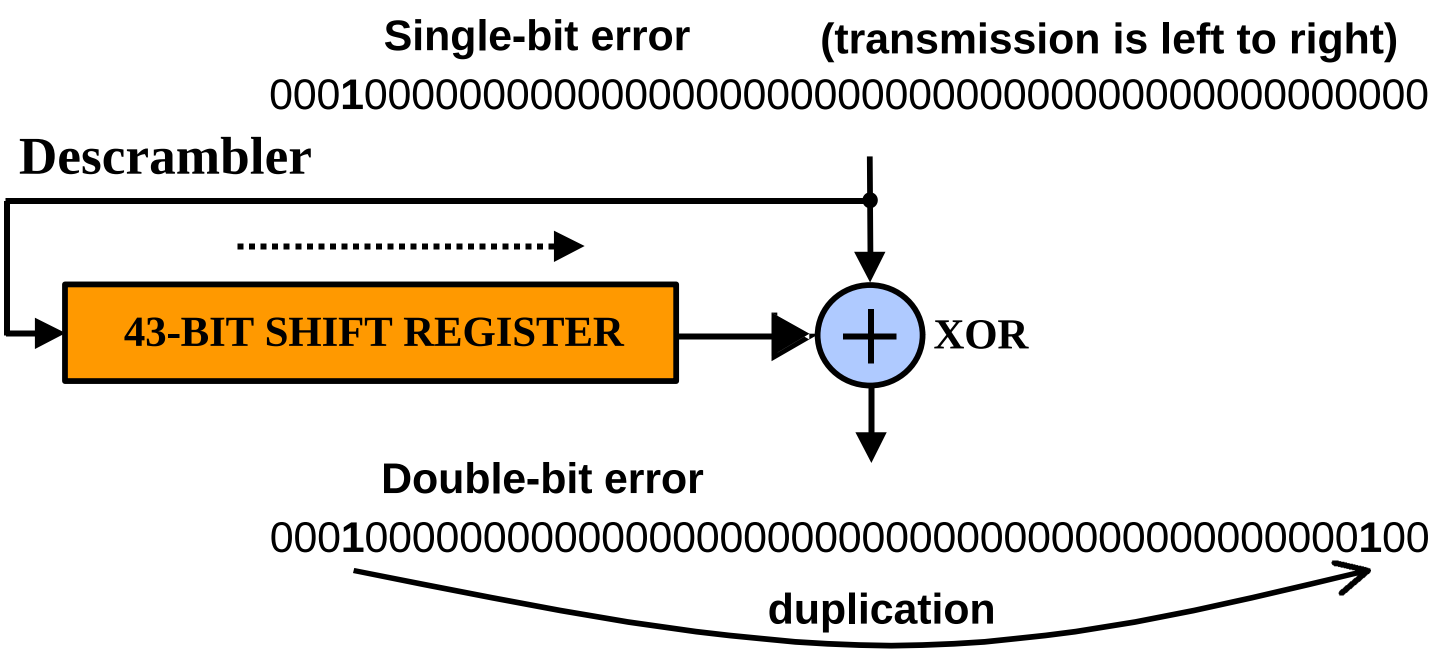
Scrambler



Descrambler

Error Duplication

- **Bit errors are delayed in the 43-bit shift register and appear again 43 bits later**
- **Every bit error duplicates itself 43 bits later**



Messages and Polynomials

- **An *n*-bit message can be represented as an *n* - 1 degree polynomial, where each bit is the coefficient for each term in the polynomial**
  - 10011011 corresponds to the polynomial M(*x*) = $x^7 + x^4 + x^3 + x^1 + 1$

- **Multiplication, division, and addition of polynomials are performed *module 2***
  - Module 2 addition is the same as subtraction = XOR of bit patterns
  - 10011011 + 1 = 10011011 XOR 00000001 = 10011010
  - (10011011)(11) = 110101101

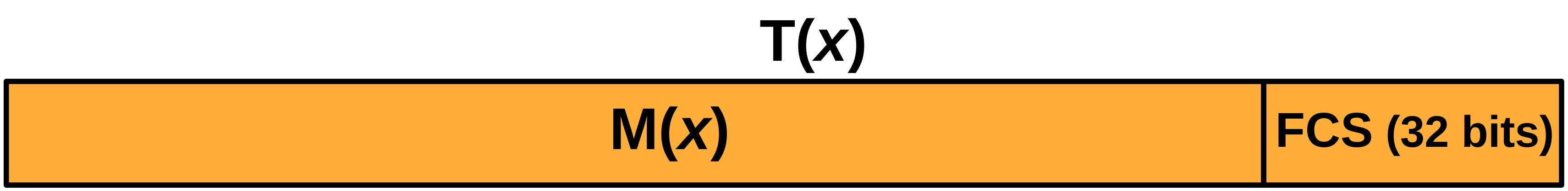
$$\begin{array}{r} 10011011 \\ \times\ 11 \\ \hline 10011011 \\ 10011011+ \\ \hline 110101101 \end{array}$$

Ethernet CRC

- **$G(x) = x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^{8} + x^{7} + x^{5} + x^{4} + x^{2} + x + 1$**

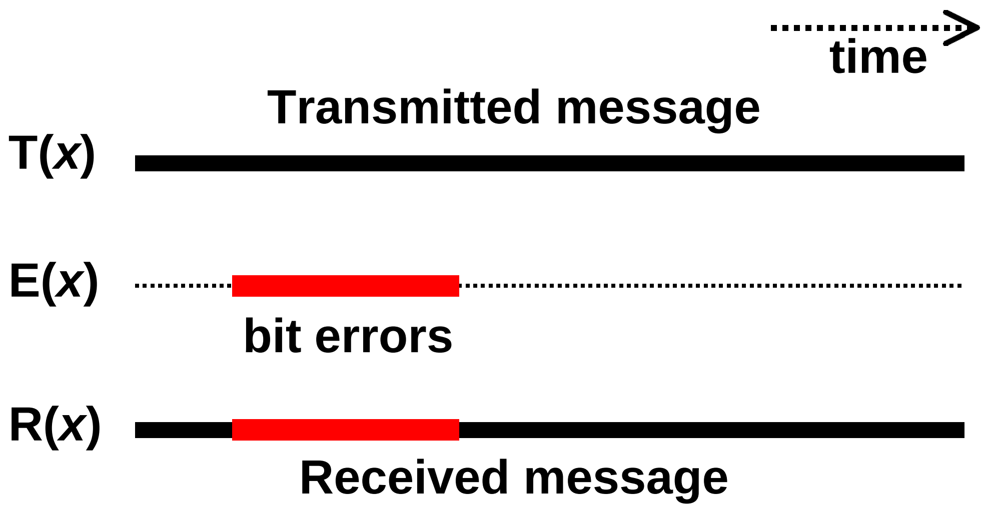
- **FCS = remainder of $M(x)x^{32}$ / $G(x)$**
  - — **$M(x)x^{32}$ = $M(x)$ followed by 32 zeroes**

- **Transmitted message: $T(x) = M(x)x^{32} + \text{FCS}$**
  - — Remainder of $T(x)$ / $G(x)$ is zero



Received Message

- **R(*x*) = T(*x*) + E(*x*)**



How a CRC Code Detects Errors

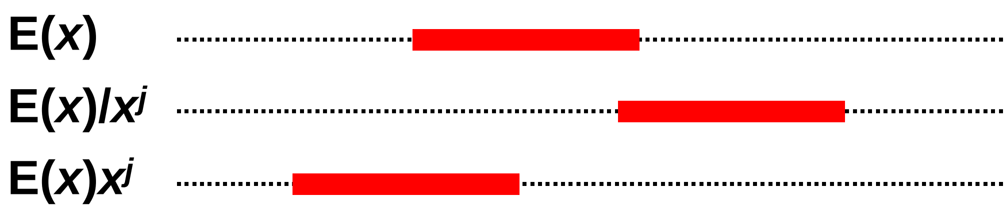
- **R(x) = T(x) + E(x)**

- **Received message R(x) is <u>assumed</u> correct if R(x) is divisible by G(x)**
  - — i.e., remainder of R(x) / G(x) = 000…0

- **Remainder of R(x) / G(x) = remainder of E(x) / G(x)**
  - – Since remainder of T(x) / G(x) = 000…0

- **Error is detectable if remainder of E(x) / G(x) $\neq$ 000…0**
  - — Some error patterns are undetectable (e.g., E(x) = G(x))

Position of Bit Errors is not Important



- **Error detection capability does not change if E(x) is <u>shifted</u> to the right or left without loosing bit errors**
  — If E(x) is detectable, $E(x)/x^j$ and $E(x)x^j$ are detectable
  — Multiplying or dividing E(x) by x^j does not make it a multiple of G(x)
  — Multiples of G(x) have all the factors of G(x), and x^j has none

- **Definition:**
  — F(x) is a factor of G(x) if G(x) is divisible by F(x) and F(x) is only divisible by itself and 1

Ethernet CRC Detects

- **All single-bit errors**
  - — Since G(x) has the terms x^{32} and 1
- **All double-bit errors**
  - — Since G(x) has a factor with at least three terms
  - — (also verified by enumeration of all possible cases)
- **All triple-bit errors**
  - — verified by enumeration of all possible cases (up to 1518 bytes)
- **All burst errors with length up to 32 bits**
  - — In this case, remainder of E(x) / G(x) $\neq$ 000…0

Ethernet CRC Detects (cont.)

- **All 33-bit burst errors except E(*x*) = G(*x*)x^j**
  - There are 2^{31} possible 33-bit burst errors
  - If error patterns are random, G(*x*) can detect 99.999999953% of all 33-bit burst errors

- **Ethernet CRC does <u>not</u> detect all <u>odd</u> number of bit errors**
  - E(*x*) = G(*x*)x^j is undetectable and has 15 bits in error!
  - If G(*x*) had (*x* + 1) as a factor, it would detect all odd number of bit errors
  - (*x* + 1) not being a factor of the Ethernet CRC is actually good, as we will show later

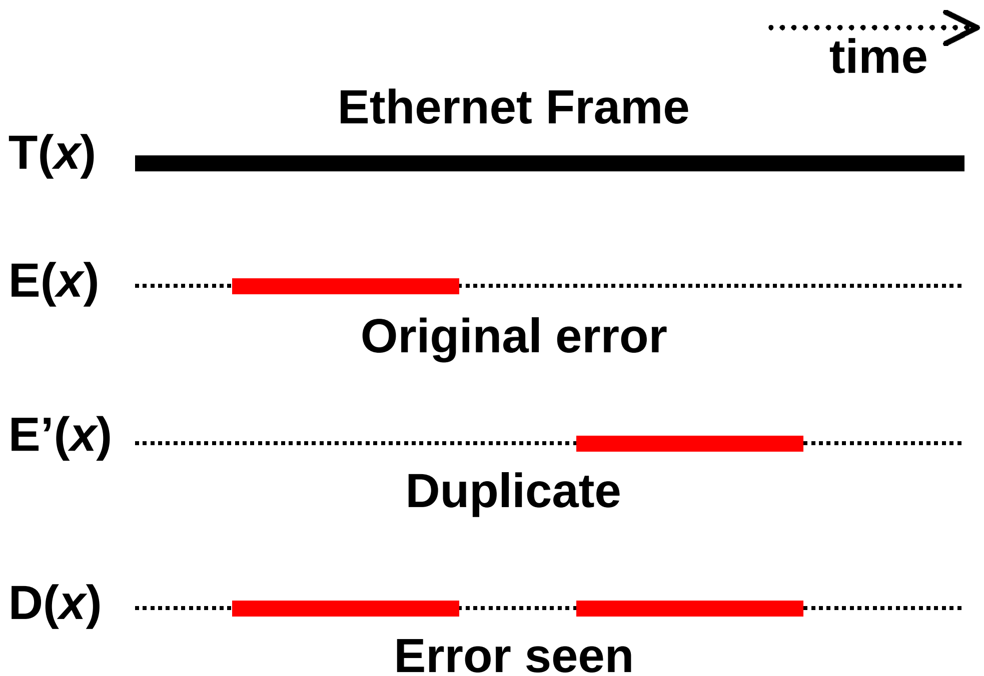
References

- **Stallings, W., “Data and Computer Communications,” 3rd Edition, Macmillan Publishing Company, c1991, pp. 127-132**
  - Overview of CRC codes and their general properties
  - Brief proofs for some properties and references to primary sources for other proofs

- **Tanenbaum, A. S., “Computer Networks,” Prentice Hall, 1996, pp. 128-132**
  - Same

Error Duplication

- **Errors are duplicated by the $x^{43} + 1$ scrambler**
- **The error seen at the frame is $D(x) = E(x) + E'(x)$**



Error Duplication (cont.)

- **D(x) can be expressed as**
  - — D(x) = E'(x)(x^{43} + 1)
  - — example:
    - – E(x) = 1010…0000, where E(x) ends with 43 zeros
    - – E'(x) = 0000…0101
    - – D(x) = 1010…0101

```
  10000000000000000000000000000000000000000001   x^43 + 1
                                          × 101   E'(x)
-----------------------------------------------
  10000000000000000000000000000000000000000001
 00000000000000000000000000000000000000000000
+10000000000000000000000000000000000000000001
-----------------------------------------------
1010000000000000000000000000000000000000000101   D(x)
```

Ethernet CRC is Immune to Error Duplication

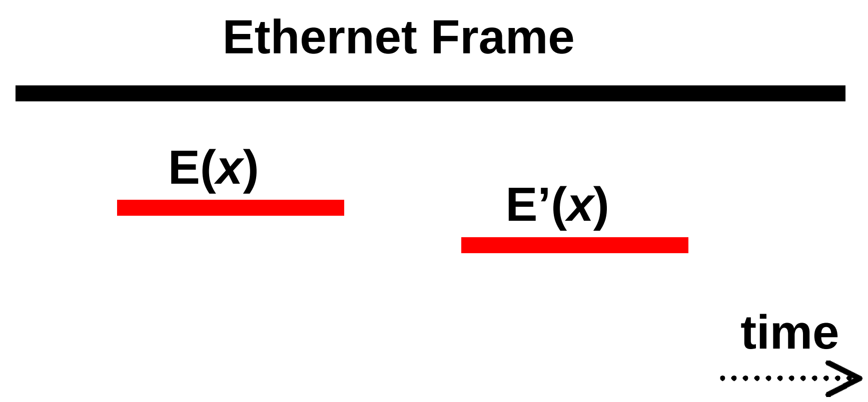
- **Ethernet CRC detects a duplicated error if $D(x) = E'(x)(x^{43} + 1)$ is <u>not</u> a multiple by $G(x)$**

- **But $(x^{43} + 1)$ has no <u>factors</u> in common with $G(x)$**
  - — $(x^{43} + 1)$ factors: (11) (10011111111001) (10101001001010 1) (11010001000101 1)
  - — Ethernet CRC factor: itself $\Rightarrow$ $(x + 1)$ is not a factor!

- **Conclusion: $D(x)$ is divisible by $G(x)$ <u>if and only if</u> $E'(x)$ and, consequently, $E(x)$ are divisible by $G(x)$**
  - — i.e., There is no change in error detection capabilities

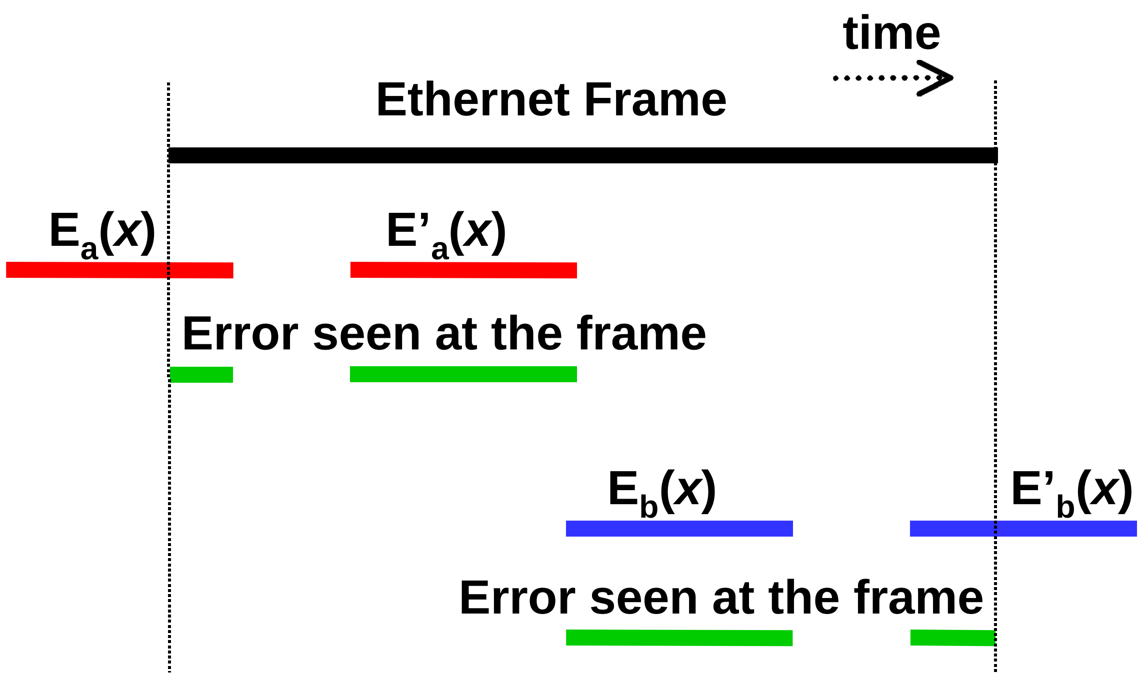
A Few Boundary Cases

- **Previous analysis assumes that E(*x*) and E'(*x*) are entirely contained inside the frame**



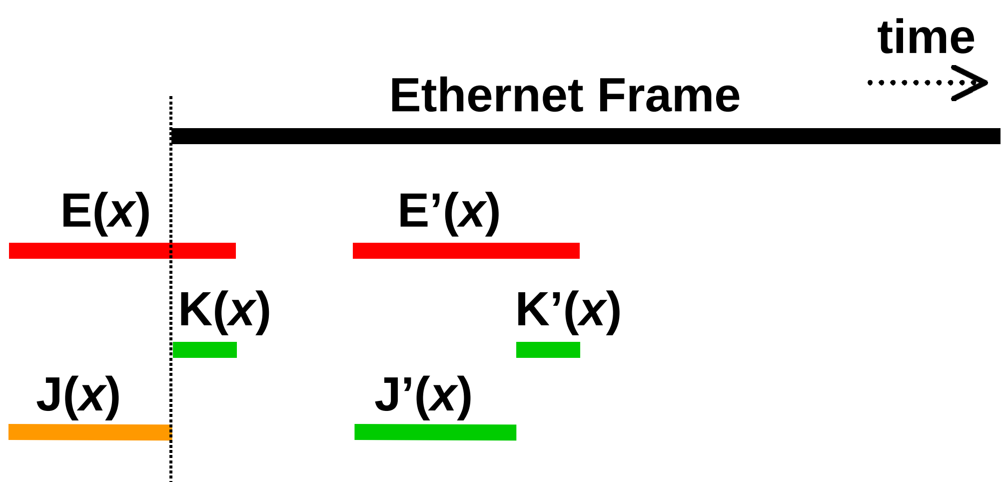
Errors/Duplications May Cross Frame Boundaries

- $E(x)$ or $E'(x)$ can be partially outside the frame
- Is the resulting error detectable?



Errors Crossing the Beginning of the Frame

- **Let $E(x) = J(x) + K(x)$**
  - $J(x)$ is the part of $E(x)$ that is originally outside the frame
- **$J'(x)$ and $K'(x)$ are the duplicates of $J(x)$ and $K(x)$, respectively**
- **Error seen at the frame: $K'(x)(x^{43} + 1) + J'(x)$**



NORTEL NETWORKS™

Probability of Undetected Errors = 2.3×10^{-10}

(Errors Crossing the Beginning of the Frame)

- **Case 1: J'(x) and K'(x) are undetectable**
  - Probability of D(x) being undetectable = $(1 / 2^{32})\ (1 / 2^{32})$
- **Case 2: J'(x) is detectable and K'(x) is undetectable**
  - Probability of D(x) being undetectable = 0
- **Case 3: J'(x) is undetectable and K'(x) is detectable**
  - Probability of D(x) being undetectable = 0
- **Case 4: J'(x) and K'(x) are detectable**
  - Probability of D(x) being undetectable is equal to the probability of K'(x) being detectable and K'(x)(x^{43} + 1) having the same remainder as J'(x). It is then $(1 - 1 / 2^{32})(1 / 2^{32})$
- **Probability of undetected errors = $1 / 2^{32}$ = 2.3×10^{-10}**

NORTEL NETWORKS™

Probability of Undetected Errors is the Same
(Errors Crossing the Beginning of the Frame)

- **For errors crossing the beginning of the frame, the probability of undetected errors is <u>exactly</u> the same as the one without the scrambler, i.e., $1 / 2^{32} = 2.3 \times 10^{-10}$**

NORTEL NETWORKS™

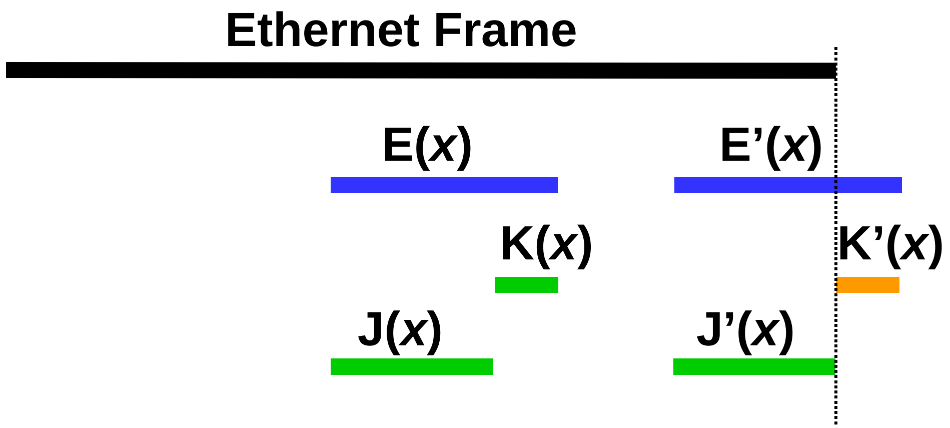
All Errors $\leq$ 29 Bits Long are Detectable
(Errors Crossing the Beginning of the Frame)

- **List of all undetectable errors**
  - (Left of "-" is outside the frame)
  - (30 bits) 1011 **-** 0 **-** 1111100100001101110111001 (2 cases)
  - (31 bits) 1000110100111110011111 **-** 100111001
  - (31 bits) 1 **-** 101101101000000001001000000101
  - (31 bits) 11101 **-** 10000101100010110011001011
  - (32 bits) 10100001011101111011 **-** 0 **-** 101000101001 (2 cases)
  - (32 bits) 101110101011101011101110011 **-** 0 **-** 0 **-** 111 (3 cases)
  - (32 bits) 1100000010011101 **-** 1111000110110111
- **For errors $\leq$ 32 bits long, the probability of undetected errors is increased (from 0) to 8.4×10^{-11}**
  - $2/(29 \times 2^{32}) + 3/(30 \times 2^{32}) + 6/(31 \times 2^{32}) = 0.36 / 2^{32} = 8.4 \times 10^{-11}$

NORTEL NETWORKS™

Duplication Partially Outside the Frame

- **Let $E(x) = J(x) + K(x)$**
- **$J'(x)$ and $K'(x)$ are the duplicates of $J(x)$ and $K(x)$, respectively**
  - — $K'(x)$ is the part of $E'(x)$ that is outside the frame
- **Error seen at the frame: $J'(x)(x^{43} + 1) + K(x)$**



Probability of Undetected Errors = 2.3 $\times$ 10^{-10}

(Duplication Partially Outside the Frame)

- **Case 1: J'(*x*) and K(*x*) are undetectable**
  - — Probability of D(*x*) being undetectable = $(1 / 2^{32})$ $(1 / 2^{32})$
- **Case 2: J'(*x*) is undetectable and K(*x*) is detectable**
  - — Probability of D(*x*) being undetectable = 0
- **Case 3: J'(*x*) is detectable and K(*x*) is undetectable**
  - — Probability of D(*x*) being undetectable = 0
- **Case 4: J'(*x*) and K(*x*) are detectable**
  - — Probability of D(*x*) being undetectable is equal to the probability of J'(*x*) being detectable and J'(*x*)(x^{43} + 1) having the same remainder as K(*x*). It is then $(1 - 1 / 2^{32})(1 / 2^{32})$
- **Probability of undetected errors = 1 / 2^{32} = 2.3 $\times$ 10^{-10}**

NORTEL NETWORKS™

Probability of Undetected Errors is the Same
(Duplication Partially Outside the Frame)

- **For errors whose duplications cross the end of the frame, the probability of undetected errors is <u>exactly</u> the same as the one without the scrambler, i.e., $1 / 2^{32} = 2.3 \times 10^{-10}$**

All Errors $\leq$ 29 Bits Long are Detectable
(Duplication Partially Outside the Frame)

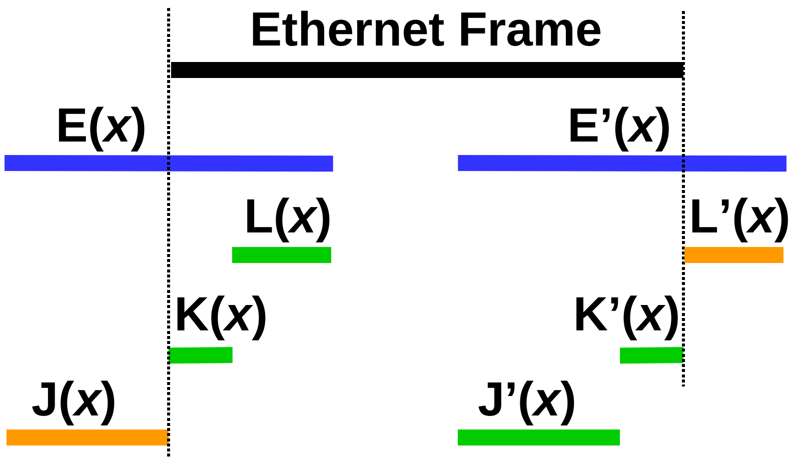
- **List of all undetectable errors**
  - (Right of "-" is duplicated outside the frame)
  - (30 bits) 110111 - 100110110010100111110011
  - (32 bits) 1110101001 - 1101100101000000000001
  - (32 bits) 1001 - 1101111100010000001011010001
  - (32 bits) 1 - 0 - 101000011001011001001100000111 (2 cases)
  - (32 bits) 11010110011001100000100111 - 100111

- **For errors $\leq$ 32 bits long, the probability of undetected errors is increased (from 0) to 4.6×10^{-11}**
  - $1/(29 \times 2^{32}) + 5/(31 \times 2^{32}) = 0.196 / 2^{32} = 4.6 \times 10^{-11}$

NORTEL NETWORKS™

Errors and Duplications at Frame Boundaries

- **Let E(*x*) = J(*x*) + K(*x*) + L(*x*)**
- **J'(*x*), K'(*x*), and L'(*x*) are the duplicates of J(*x*), K(*x*), and L(*x*), respectively**
  - L'(*x*) is the part of E'(*x*) that is outside the frame
  - J(*x*) is the part of E(*x*) that is outside the frame
- **Error seen: D(*x*) = K'(*x*)(x^{43} + 1) + J'(*x*) + L(*x*)**



This is a rare case!

Probability of Undetected Errors = 2.3×10^{-10}
(Errors and Duplications Extending Across Frame Boundaries)

- **Case 1: L(x) is undetectable**
  - Probability of D(x) being undetectable = $(1 / 2^{32})\ (1 / 2^{32})$
    = probability of K'(x)(x^{43} + 1) + J'(x) and L(x) being undetectable
    (the former is derivable from the first boundary case)
- **Case 2: L(x) is detectable**
  - Probability of D(x) being undetectable = $(1 - 1 / 2^{32})\ (1 / 2^{32})$
    = probability of K'(x)(x^{43} + 1) + J'(x) being detectable and
    K'(x)(x^{43} + 1) + J'(x) having the same remainder as L(x)
    (the former is derivable from the first boundary case)
- **Probability of undetected errors = $1 / 2^{32} = 2.3 \times 10^{-10}$**

NORTEL NETWORKS™

Probability of Undetected Errors is the Same

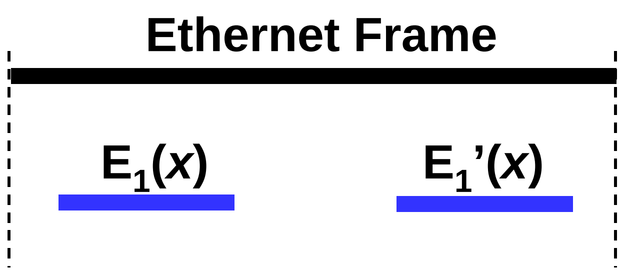
(Errors and Duplications Extending Across Frame Boundaries)

- **When error and duplication cross frame boundaries, the probability of undetected errors is <u>exactly</u> the same as the one without the scrambler, i.e., $1/\,2^{32} = 2.3 \times 10^{-10}$**

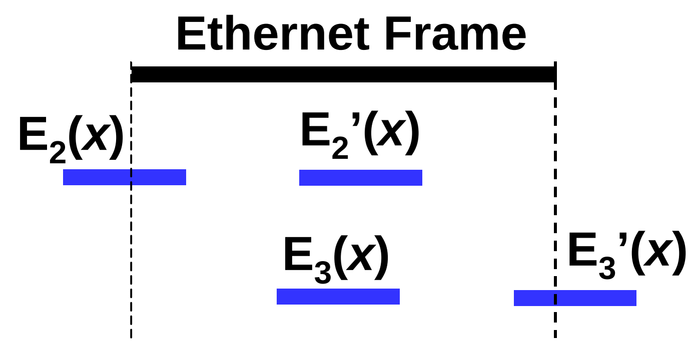
  — Note: Errors $\leq$ 32 bits long are not applicable in this case (frames are not that short)

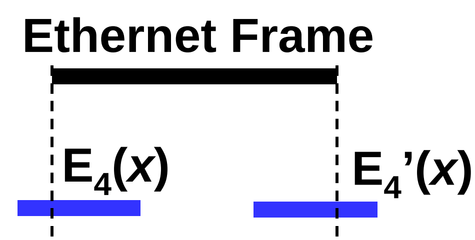
Summary of Cases

- **Base case**
  - Error detection capabilities of the Ethernet CRC are unchanged



- **Boundary Cases**
  - Probability of undetected errors is the same as the one without the scrambler, i.e., $1 / 2^{32} = 2.3 \times 10^{-10}$





Probability of Undetected Errors

Case Type	E(x) frame position	E'(x) frame position	1-bit error	2-bit error	Bursts ≤ 29 bits	Bursts ≤ 32 bits	Bursts > 32 bits
Without scrambler	inside	N/A	0	0	0	0	2.3×10^{-10}
Base	inside	inside	0	0	0	0	2.3×10^{-10}
Boundary	across beginning	inside	0	0	0	8.4×10^{-11}	2.3×10^{-10}
Boundary	inside	across end	0	0	0	4.6×10^{-11}	2.3×10^{-10}
Boundary	across beginning	across end	0	0	0	0	2.3×10^{-10}

Summary

- **The x^{43} + 1 scrambler does <u>not</u> change the overall probability of undetected errors of the Ethernet CRC**

  — For errors entirely contained inside the frame, error duplication does <u>not</u> affect the error detection capabilities of the Ethernet CRC

  — For random errors, the overall probability of undetected errors is the same whether there is an x^{43} + 1 scrambler or not

  — For errors or duplications that are not entirely contained inside the frame, the probability of undetected errors is the same as the one without the scrambler, i.e., $1 / 2^{32} = 2.3 \times 10^{-10}$

  — All errors 29 bits long or less are detectable

NORTEL NETWORKS™