INSTITUTO POLITÉCNICO NACIONAL

Escuela Superior de Cómputo

Unidad de Aprendizaje

Redes de Computadoras

Tarea 8:

CRC-32 Código de redundancia cíclica

Profesora:

Sandra Ivette Bautista Rosales

Grupo:

2CV10

Alumna:

Luciano Espina Melisa

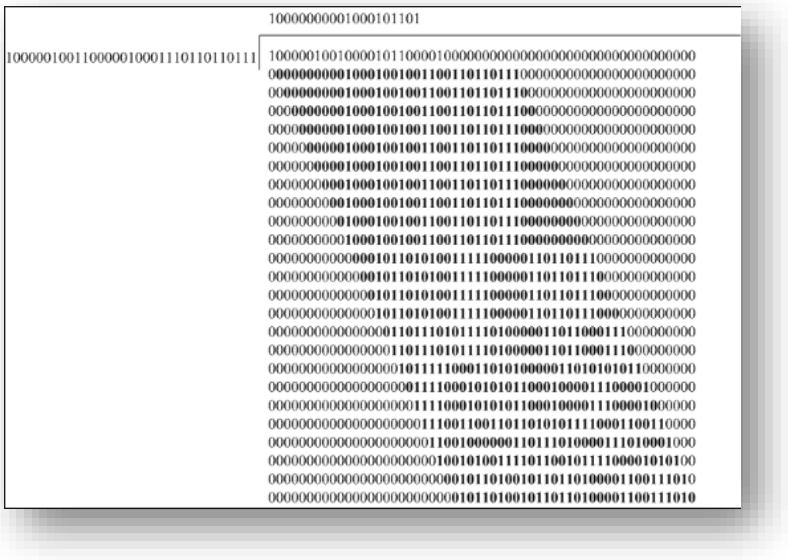
Fecha de Entrega:

23/Mayo/2018

CRC

El CRC es una técnica usada para marcar los errores. El CRC utiliza un valor numérico calculado para detectar los errores en los datos transmitidos. El remitente de una trama de datos calcula la secuencia de verificación de tramas (FCS). El remitente añade el valor FCS al final del fichero a los mensajes salientes. El receptor recalcula el FCS, y compara el valor con el FCS del remitente.

Si existe una diferencia, el receptor asume que ocurrió un error de transmisión, y envía una petición al remitente de volver a enviar la trama. La retención del valor verdadero de un bastidor es importante asegurarse de que el destino interpreta correctamente los datos que usted comunica.



La Solicitud de comentarios (RFC) 2615 define el uso del Point-to-Point Protocol (PPP) sobre SONET/el Synchronous Digital Hierarchy (SDH). Aquí es cómo este RFC especifica cuando una interfaz POS puede utilizar el CRC de 16 bits (CRC-16) y cuando puede utilizar el CRC de 32 bits (CRC-32):

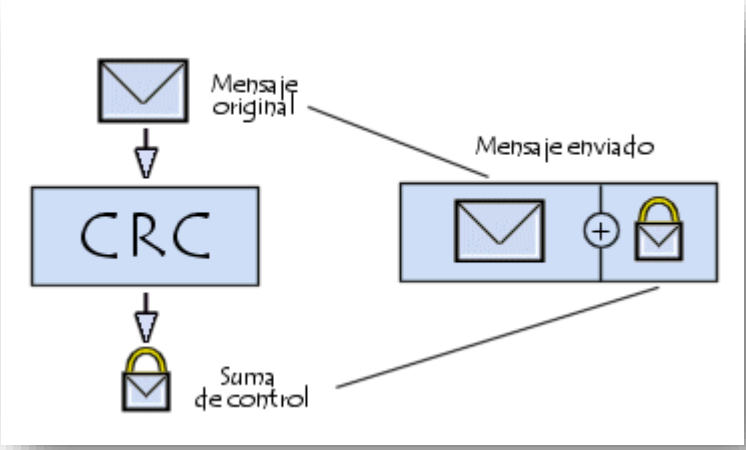
“Con respecto a la longitud del FCS, con una excepción, el FCS de 32 bits se debe utilizar para todas las tarifas SONET/SDH. Para la señal de transporte sincrónica (ingeniería del proceso de los sistemas STS)-3c- (SPE)/VC-4 solamente, el FCS de 16 bits puede ser utilizado, aunque se recomiende el FCS de 32 bits. La longitud del FCS es fijada disposición y no negociada.”

El RFC 2615 requiere (y recomienda) el CRC de 32 bits. El CRC de 32 bits es lejos superior en la detección de tipos determinados de errores que un CRC de 16 bits. El CRC-16 menos robusto puede no poder detectar un error de bit en los links que pueden transmitir los Gigabits de datos por segundo. [1]

Verificación de redundancia cíclica

La verificación de redundancia cíclica (abreviado, **CRC**) es un método de control de integridad de datos de fácil implementación. Es el principal método de detección de errores utilizado en las telecomunicaciones.

La verificación de redundancia cíclica consiste en la protección de los datos en bloques, denominados *tramas*. A cada trama se le asigna un segmento de datos denominado *código de control* (al que se denomina a veces FCS, *secuencia de verificación de trama*, en el caso de una secuencia de 32 bits, y que en ocasiones se identifica erróneamente como CRC). El código CRC contiene datos redundantes con la trama, de manera que los errores no sólo se pueden detectar, sino que además se pueden solucionar.



El concepto de CRC consiste en tratar a las secuencias binarias como polinomios binarios, denotando polinomios cuyos coeficientes se correspondan con la secuencia binaria. Por ejemplo, la secuencia binaria 0110101001 se puede representar mediante un polinomio, como se muestra a continuación:

$$0*X^9 + 1*X^8 + 1*X^7 + 0*X^6 + 1*X^5 + 0*X^4 + 1*X^3 + 0*X^2 + 0*X^1 + 1*X^0$$

siendo

$$X^8 + X^7 + X^5 + X^3 + X^0$$

o

$$X^8 + X^7 + X^5 + X^3 + 1$$

De esta manera, la secuencia de bits con menos peso (aquella que se encuentra más a la derecha) representa el grado 0 del polinomio (X0 = 1), (X0 = 1), (X0 = 1), el 4º bit de la derecha representa el grado 3 del polinomio (X3), y así sucesivamente.

Luego, una secuencia de n- bits forma un polinomio de grado máximo n-1. Todas las expresiones de polinomios se manipulan posteriormente utilizando un módulo 2.

En este proceso de detección de errores, un polinomio predeterminado (denominado polinomio generador y abreviado G(X)) es conocido tanto por el remitente como por el destinatario. El remitente, para comenzar el mecanismo de detección de errores, ejecuta un algoritmo en los bits de la trama, de forma que se genere un CRC, y luego transmite estos dos elementos al destinatario. El destinatario realiza el mismo cálculo a fin de verificar la validez del CRC. [2]

Polinomio generador común

CRC-32 (Ethernet): $= X^{32} + X^{26} + X^{23} + X^{22} + X^{16} + X^{12} + X^{11} + X^{10} + X^8 + X^7 + X^5 + X^4 + X^2 + X + 1$

Bibliografía

- [1] S/A |Cisco.com [Online] Available: https://www.cisco.com/c/es_mx/support/docs/optical-networking/ons-15454-sonet-multiservice-provisioning-platform-mspp/13565-crc.pdf
- [2] S/A Verificación de errores | CCM [Online] Available: https://es.ccm.net/contents/59-verificacion-de-errores