Network Working Group
Request for Comments: 1624
Updates: 1141
Category: Informational

A. Rijsinghani, Editor
Digital Equipment Corporation

May 1994

Computation of the Internet Checksum via Incremental Update

Расчет контрольной суммы Internet с помощью инкрементального обновления

Статус документа

Этот документ содержит информацию для сообщества Internet. Документ не задаёт стандартов Internet, а его распространение не ограничивается ничем.

Аннотация

Документ описывает обновленный метод инкрементального расчёта стандартной контрольной суммы Internet. Это обновляет метод, описанный в RFC 1141.

Оглавление

1. Введение

Инкрементальное обновление контрольной суммы полезно для ускорения некоторых типов операций, постоянно выполняемых для пакетов IP (обновление TTL, фрагментация IP, обновление source route).

На страницах 4 и 5 RFC 1071 описана процедура инкрементального обновления стандартной контрольной суммы Internet. Приведенное там обсуждение расчета оказалось неполным. Поэтому был опубликован RFC 1141 с обновлением описания инкрементального обновления (Incremental Update). В частности, в RFC 1141 более подробно описана процедура, заданная RFC 1071. Однако в некоторых случаях результат инкрементального обновления отличается от результата полного расчета (дополнение до 1[1] суммы дополнений до 1 для исходных полей).

Для полноты в этом документе кратко повторены основные моменты из RFC 1071 и RFC 1141. На основе обсуждения разработана и представлена новая процедура инкрементального расчета стандартных контрольных сумм Internet.

2. Обозначения и уравнения

На основе приведенных ниже обозначений

HC - старая контрольная сумма заголовка;

C - сумма дополнений до 1 для старого заголовка;

HC' - новая контрольная сумма заголовка;

C' - сумма дополнений до 1 для нового заголовка;

m - старое значение 16-битового поля;

m' - новое значение 16-битового поля

в RFC 1071 приведено уравнение для C'

```
C' = C + (-m) + m'        [1]
   = C + (m' - m)
```

Как отмечено в RFC 1141, приведенное выше уравнение бесполезно для прямого использования при расчете инкрементального обновления, поскольку C и C' не относятся к фактической контрольной сумме в заголовке. Кроме того, следует отметить, что в RFC 1071 не указана необходимость использования арифметики с дополнением до 1.

Дополнение приведенного уравнения для получения фактической контрольной суммы представлено в RFC 1141 как

```
HC' = ~(C + (-m) + m')
    = HC + (m - m')
    = HC + m + ~m'        [2]
```

[1] В литературе на русском языке часто применяется термин «обратный код». *Прим. перев.*

3. Обсуждение

Хотя это уравнение представляется работающим, имеются граничные условия, при которых оно дает результат, отличающийся от полного расчета контрольной суммы. Это связано с обработкой 0 в арифметике с дополнением до 1.

В обратном коде существует два представления нуля - нули во всех битах или единицы во всех битах, часто обозначаемые как +0 и -0. Сложение отличных от нуля значений в этой арифметике может давать -0, но никогда не дает +0. Поскольку в заголовке IP гарантировано наличие хотя бы одного поля, отличного от 0, а поле контрольной суммы в заголовке является дополнением суммы, поле контрольной суммы не может иметь значения ~(+0), которое является -0 (0xFFFF). Однако оно может содержать ~(-0), т. е. +0 (0x0000).

В RFC 1141 представлено обновление для контрольной суммы заголовка -0, когда ей следует иметь значение +0. Это связано с допущением о том, что дополнение до 1 обладает дистрибутивностью, но это допущение неверно для нулевого результата (см. вывод уравнения [2]).

Проблемы можно избежать, отказавшись от этого допущения. Корректное уравнение приведено ниже.

```
HC' = ~(C + (-m) + m')          [3]
    = ~(~HC + ~m + m')
```

4. Примеры

Рассмотрим заголовок пакета IP, в котором 16-битовое поле m = 0x5555 меняется на m' = 0x3285. Сумма дополнений до 1 для остальных октетов заголовка составляет 0xCD7A.

Контрольная сумма исходного заголовка будет иметь значение

```
HC = ~(0xCD7A + 0x5555)
   = ~0x22D0
   =  0xDD2F
```

Новая контрольная сумма будет иметь значение

```
HC' = ~(0xCD7A + 0x3285)
    = ~0xFFFF
    =  0x0000
```

Используя уравнение [2], как указано в RFC 1141, новая контрольная сумма рассчитывается как

```
HC' = HC + m + ~m'
    =  0xDD2F + 0x5555 + ~0x3285
    =  0xFFFF
```

Что отличается от результата полного расчета и никогда не может быть получено для заголовка IP.

Использование уравнения [3] дает корректный результат, как показано ниже.

```
HC' = ~(C + (-m) + m')
    = ~(0x22D0 + ~0x5555 + 0x3285)
    = ~0xFFFF
    =  0x0000
```

5. Проверка контрольных сумм конечными системами

Если конечная система проверяет контрольную сумму, включая само поле контрольной суммы в сумму дополнений до 1, а затем сравнивает результат с -0, как рекомендует RFC 1071, не имеет значения указание промежуточной системой значения -0 вместо +0, благодаря описанному здесь свойству из RFC 1141. Для приведенного выше примера будет

```
0xCD7A + 0x3285 + 0xFFFF = 0xFFFF
0xCD7A + 0x3285 + 0x0000 = 0xFFFF
```

Однако имеются реализации, проверяющие контрольную сумму путем полного расчета и сравнения с полем контрольной суммы в заголовке.

Промежуточным системам рекомендуется выполнять инкрементальное обновление контрольной суммы, как описано в этом документе, а конечным системам рекомендуется выполнять проверку контрольной суммы по методу, описанному в RFC 1071.

Метод из уравнения [3] несколько «дороже» предложенного в RFC 1141. Если это имеет значение, можно исключить две дополнительные инструкции путем вычитания дополнений с заимствованием (см. раздел 7). Это дает уравнение

```
HC' = HC - ~m - m'          [4]
```

Для приведенного выше примера

```
HC' = HC - ~m - m'
    =  0xDD2F - ~0x5555 - 0x3285
    =  0x0000
```

6. Историческое замечание

Стандартная арифметика с дополнением до 1 (обратный код) может давать результат -0 и это является одним из ее основных недостатков, осложняя интерпретацию результата. В компьютерах серии CDC 6000 [4] эта проблема решена за счет использования вычитания в качестве примитива арифметики с обратным кодом (т. е. сложение заменено вычитанием дополнения).

7. Благодарности

Ниже перечислены люди, внесшие свой вклад в создание этого документа.

Manu Kaycee - Ascom Timeplex, Incorporated

Paul Koning - Digital Equipment Corporation

Tracy Mallory - 3Com Corporation

Krishna Narayanaswamy - Digital Equipment Corporation

Atul Pandya - Digital Equipment Corporation

Были обнаружены отказы при тестировании IP на продукции, реализующей алгоритм RFC 1141. Отказы были проанализированы и разработан обновленный алгоритм. Этот алгоритм также был протестирован с использованием моделирования. Было также показано, что условий отказа не возникает при проверке контрольных сумм в соответствии с RFC 1071.

8. Вопросы безопасности

Вопросы безопасности не рассматриваются в этом документе.

9. Заключение

В реализациях рекомендуется применять уравнение [3] или [4] для инкрементального обновления стандартных контрольных сумм Internet.

10. Адрес автора

Anil Rijsinghani

Digital Equipment Corporation

550 King St

Littleton, MA 01460

Phone: (508) 486-6786

EMail: anil@levers.enet.dec.com

11. Литература

[1] Postel, J., "Internet Protocol - DARPA Internet Program Protocol Specification", STD 5, RFC 791, DARPA, September 1981.

[2] Braden, R., Borman, D., and C. Partridge, "Computing the Internet Checksum", RFC 1071, ISI, Cray Research, BBN Laboratories, September 1988.

[3] Mallory, T., and A. Kullberg, "Incremental Updating of the Internet Checksum", RFC 1141, BBN Communications, January 1990.

[4] Thornton, J., "Design of a Computer -- the Control Data 6600", Scott, Foresman and Company, 1970.

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru