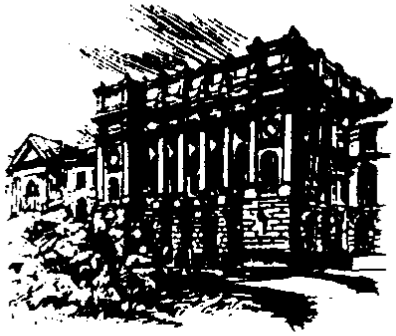
САНКТ-ПЕТЕРБУРГСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ПЕТРА ВЕЛИКОГО
ИНСТИТУТ КОМПЬЮТЕРНЫХ НАУК И ТЕХНОЛОГИЙ
Высшая школа программной инженерии

Направление: «Информатика и вычислительная техника»
Профиль: «Распределённые информационные системы»
Специальность: 010300 «Фундаментальная информатика и информационные технологии»
Группа 3530202/80202 6-й семестр (весна 2021)



ПОЛИТЕХ
Санкт-Петербургский
политехнический университет
Петра Великого

Отчёт о курсовой работе

по дисциплине «**Семейства протоколов компьютерных сетей**»
(на английском языке «***Network Protocol Families***»)
на тему
«DCCP (Datagram Congestion Control Protocol)»

Выполнил
студент группы 3530202/80202 Козлова Е.А.
.________________________

Руководитель:
к.ф.м-н. доц. Глебовский А.Ю.
.________________________

“15” мая 2021 г.

Санкт-Петербург
2021 г.

Результат проверки приложением антиплагиат.

Краткий отчет

ПОЛУЧИТЬ ПОЛНЫЙ ОТЧЕТ

ПАРАМЕТРЫ ПРОВЕРКИ | ЭКСПОРТ | ИСТОРИЯ ОТЧЕТОВ | ВЫЙТИ В КАБИНЕТ | ЕЩЁ...

3530202_80202_Козлова Елена_DCCP_Co...

ПРОВЕРЕНО: 25.05.2021 15:34:28

№	Доля в отчете	Источник	Актуальна на	Модуль поиска
[01]	3,21%	Datagram Congestion Control Protocol (DCCP) Overview - PDF	06 Янв 2021	Модуль поиска inet
[02]	3,31%	https://www.potaroo.net/cgi-bin/id2pdf?f1=draft-ietf-dccp-spec-08.txt	30 Апр 2020	Модуль поиска inet
[03]	0,67%	F2FS: A New File System for Flash Storage - PDF	22 Окт 2018	Модуль поиска inet

ЗАИМСТВОВАНИЯ
7,19%

САМОЦИТИРОВАНИЯ
0%

ЦИТИРОВАНИЯ
0%

ОРИГИНАЛЬНОСТЬ
92,81%

ИСТОЧНИКОВ: 3

Table of contents

Abstract

К курсовому проекту на тему: «FDDI Network Architecture».

Курсовой проект выполнен 25.05.2021г., студентом гр. 3530202/80202 Козлова Е.А. Руководитель - Глебовский А.Ю.
Курсовой проект выполнен на

В данной работе подробно разобран протокол транспортного уровня модели OSI.

Keywords

DCCP, protocol, internet, protocol, TCP, UDP

Introduction

DCCP provides mechanisms for monitoring network congestion, avoiding the need to create them at the application layer. This protocol does not guarantee the delivery of information in the correct order.

DCCP is very effective for applications where data that arrived at the wrong time becomes useless. For example, streaming media, online games, and Internet telephony. The main feature of these applications is that old messages become useless very quickly, so it is better to get a new message than to try to forward the old one. But at the moment, most of these applications independently implement congestion tracking, and TCP or UDP is used as the transmission protocol.

The DHCP protocol has been available in the Linux kernel since version 2.6.14 and is being improved with each release.

One of the goals of DCCP was to make it as easy as possible for UDP applications to switch to DHCP when it is implemented. To facilitate this, the DCCP was designed with minimal redundancy, both in terms of the packet header size and in terms of the CPU load of the partner machines. Minimal functionality has been included in CCCP, while retaining the ability to include new features such as FEC (Forward Error Correction), pseudo-reliability, and multiple threads that can be added on top of DCCP if required.

Content

Specifications

- Implements a datagram stream with confirmation of receipt, but without re-sending.
- Unreliable connection establishment and disconnection dialog.
- Reliable parameter matching.
- Selection of TCP-friendly congestion suppression mechanisms, including TCP-like congestion control (CCID 2-Chip Card Interface Device-USB) and TCP-friendly flow Control [RFC 3448] (CCID 3). CCID 2 uses a variation of the TCP congestion control mechanism, and is acceptable for threads that seek to take advantage of the available bandwidth, CCID 3 is suitable for threads that require a more stable transfer rate.
- Options that tell the sender with high reliability which packets have reached the receiver, whether these packets have been marked with ECN [RFC 3168 and RFC 3540], corrupted, or dropped in the receiver's input buffer.
- Overload control with built-in ECN Explicit Congestion Notification (Explicit Congestion Notification).
- Mechanisms that allow the server to avoid maintaining states of unconfirmed connection attempts.
- Detecting the path MTU [RFC 1191].

Main differences from TCP

- Packet stream. DCCP is a protocol for packet streams, not byte streams.
- Unreliability. DCCP never resends datagrams.
- Sequence numbers of packages. Sequence numbers refer to packets, not bytes. Each packet sent by DHCP is assigned a new sequence number, and this also applies to confirmation packets. This allows the recipient of DCCP packets to detect confirmation losses; see the section "Sequence Number Validity" in [DCCP].
- Extensive space for options (up to 1020 bytes).
- Coordination of parameters. This is the basic mechanism by which partners agree on parameter values or connection properties.
- Select overload control. Partners can use different congestion management mechanisms. In connection A<- >B, the information packets sent from A->B can use the CCID 2 algorithm, and the data packets from B->A can use CCID 3.

DCCP Packages

- DCCP-Request

Sent by the client to initialize the connection (the first step of the three-way procedure).

- DCCP-Response

It is sent by the server in response to a DHCP Request (the second stage of the three-step connection initiation procedure).

- DCCP-Data

Used for transmitting application data.

- DCCP-Ack

Used for sending only confirmations.

- DCCP-DataAck

Used for transmitting application data in combination with confirmations.

- DCCP-CloseReq

Sent by the server to prompt the client to close the connection.

- DCCP-Close

Used by the client or server to close the connection; to start the reset procedure (DCCP-Reset).

- DCCP-Reset

Used to close the connection, in a normal or unusual way.

- DCCP-Sync, DCCP-SyncAck

Used for resynchronizing packet numbers after a long period of loss.

DCCP and RTP

The real-time transport protocol, RTP [RFC 1889], is currently used (over UDP) by many DCCP applications. There are two potential sources of redundancy in the RTP-over-TCP combination, duplicate acknowledgment data, and duplicate sequence numbers. This redundancy source adds 4 bytes per packet with respect to

RTP-over-UDP. However, specific ccids can use the space occupied by the RTP sequence number.

Safety

The DCCP protocol does not provide cryptographic security guarantees. Applications that require serious security should use IPsec or some other security scheme. Despite everything, DCCP has the ability to resist some types of attacks. This is facilitated by the package numbering system used.

Conclusions

So we looked at the transport layer protocol and came to the conclusion that the DCCP protocol is designed for streaming applications and other tasks that can benefit from the use of control by being able to choose between the amount of delay and reliable delivery in compliance with the order. The TCP protocol is not suitable for such applications, because the mechanisms used in it to control saturation and ensure orderly delivery can lead to arbitrarily long delays. The UDP protocol gets rid of long delays, but UDP applications that support saturation control do so at their own risk. The DHCP protocol supports saturation controls, including ECN, for datagram streams without delivery guarantees, but also without the arbitrarily long delays inherent in TCP. The protocol also supports organization, parameter negotiation, and connection termination with guaranteed delivery.

References

- ***https://ru.bmstu.wiki/DCCP_(Datagram_Congestion_Control_Protocol)***
- ***http://book.itep.ru/4/44/dccp.htm***

Bibliography

- *E. Kohler, M. Handley, S. Floyd, and J. Padhye. Datagram Congestion Control Protocol, draft-ietf-dccp-spec-04.txt*
- *R. Stewart, Q. Xie, K. Morneault, C. Sharp, H. Schwarzbauer, T. Taylor, I. Rytina, M. Kalla, L. Zhang, and V. Paxson. Stream Control Transmission Protocol. RFC 2960.*