Datagram Congestion Control Protocol (DCCP)

SUBMITTED BY
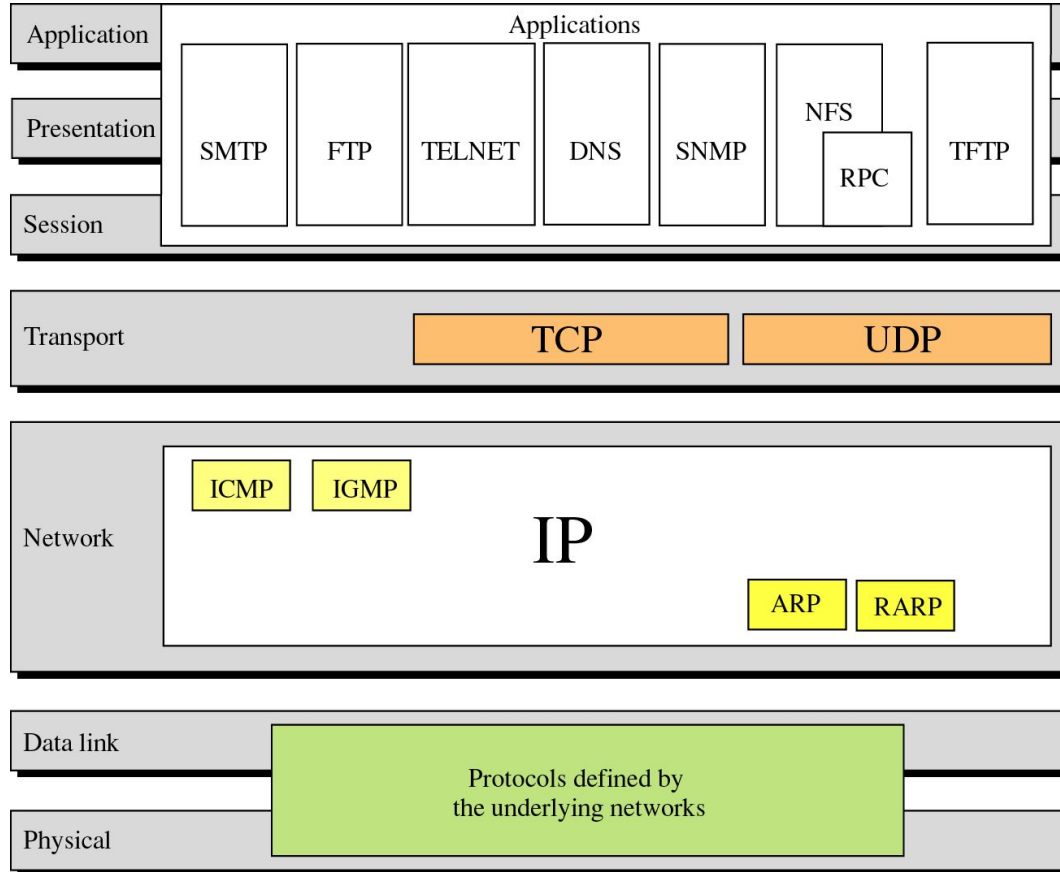**JINASH P**
S5 COMPUTER ENGINEERING

Overview

- Introduction.

- History.

- Important Differences from TCP.

- DCCP packets.

- Features negotiation.

- Choice of congestion control.

- Applications of DCCP.

- Security of DCCP.

Introduction

- DCCP is a Message-oriented , Transport layer protocol.

- DCCP implements

    - Reliable connection setup and teardown.

    - Explicit Congestion Notification (ECN).

    - Congestion control.

    - Feature negotiation.

- DCCP is suitable for applications that transfer large amounts of data.

- Benefits from control over the tradeoff between timeliness and reliability.

DCCP in Transport Layer

Application	Applications
Presentation	SMTP FTP TELNET DNS SNMP NFS/RPC TFTP
Session	

Transport	TCP UDP

Network	ICMP IGMP IP ARP RARP

Data link	Protocols defined by the underlying networks
Physical	

History of DCCP

- Initially Datagram Control Protocol (DCP)

- July 2001: First Internet Draft

- February 2002: DCCP Problem Statement

- May 2002: Changed name to DCCP

- October 2003: Latest Internet Draft

- Implementations circa 2002 and late 2003
    - FreeBSD (kernel-level)
    - Linux (kernel-level and user-level)

Important Differences from TCP

- DCCP is a packet stream protocol, not a byte stream protocol. The application is responsible for framing.

- DCCP will never retransmit a datagram. Options are retransmitted as required to make feature negotiation and ack information reliable.

- Every packet sent by a DCCP endpoint gets a new sequence number.

- Copious space for options (up to 1020 bytes).

- DCCP only included minimal functionality to minimize overhead.

Important Differences from TCP

Feature	UDP	TCP	DCCP
Packet size	8 bytes	20 bytes	12 or 16 bytes
Transport layer packet entity	Datagram	Segment	Datagram
Port numbering	Yes	Yes	Yes
Error detection	Optional	Yes	Yes
Reliability: Error recovery by ARQ	No	Yes	No
Sequence numbering and reordering	No	Yes	Yes/No
Flow control	No	Yes	Yes
Congestion Control	No	Yes	Yes
ECN support	No	Yes	Yes

DCCP Packet Types

DCCP-Request
DCCP-Response
DCCP-Ack
DCCP-Data
DCCP-DataAck
DCCP-CloseReq
DCCP-Close
DCCP-Reset
DCCP-Sync, DCCP-SyncAck

DCCP Packet Formats

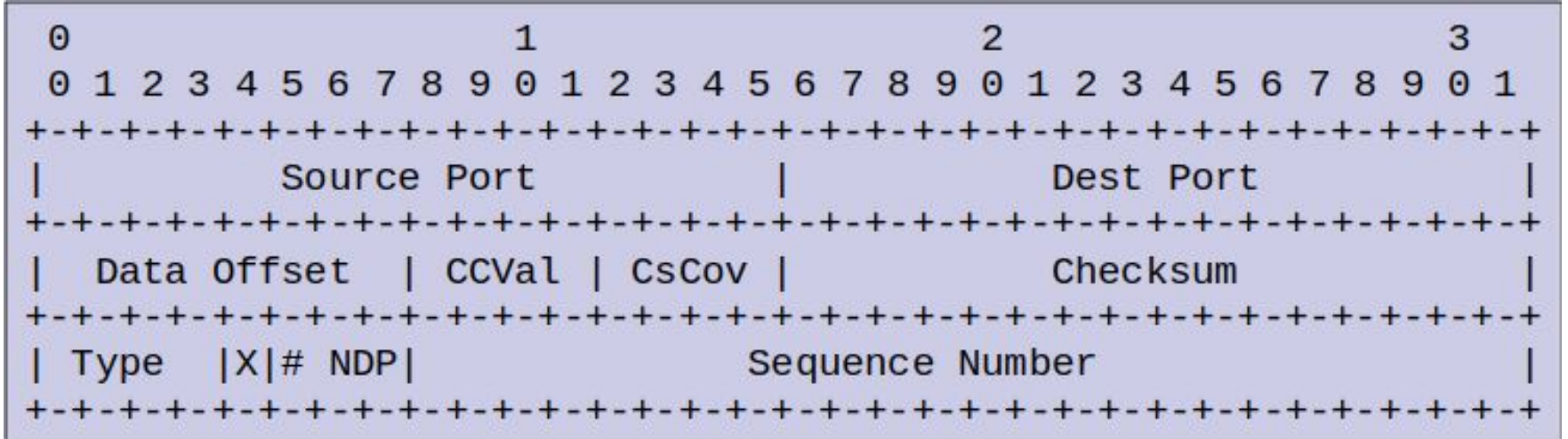| Generic Header |
| :---: |
| Additional Fields (depending on type) |
| Options (optional) |
| Application Data Area |

- DCCP header can be from 12 to 1020 bytes.

- Generic header: 12 bytes.

- Additional fields: fixed length field.

- Options: variable length field.

Packet Structure

- Basic packet similar to UDP
- Small (12 bytes)
- Extensible for additional features instead of using a fixed-length flag field

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          Source Port          |           Dest Port           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Data Offset  | CCVal | CsCov |           Checksum            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Type  |X|# NDP|            Sequence Number                   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Congestion Control in DCCP

- Each congestion control mechanism supported by DCCP is assigned a congestion control identifier, or CCID: a number from 0 to 255.
    - CCID 0 and CCID 1 are reserved
    - TCP-like congestion control – CCID 2
    - TCP friendly rate control (TFRC) – CCID 3
    - CCID 4-255 are reserved

Feature Numbers

- The first data byte of every Change, Prefer, or Confirm option is a feature number, defining the type of feature being negotiated.

- The remainder of the data gives one or more values for the feature.

Applications of DCCP

- DCCP is useful for applications with timing constraints on the delivery of data.

   - **Media Streaming.**

   - **Online Multiplayer Gaming.**
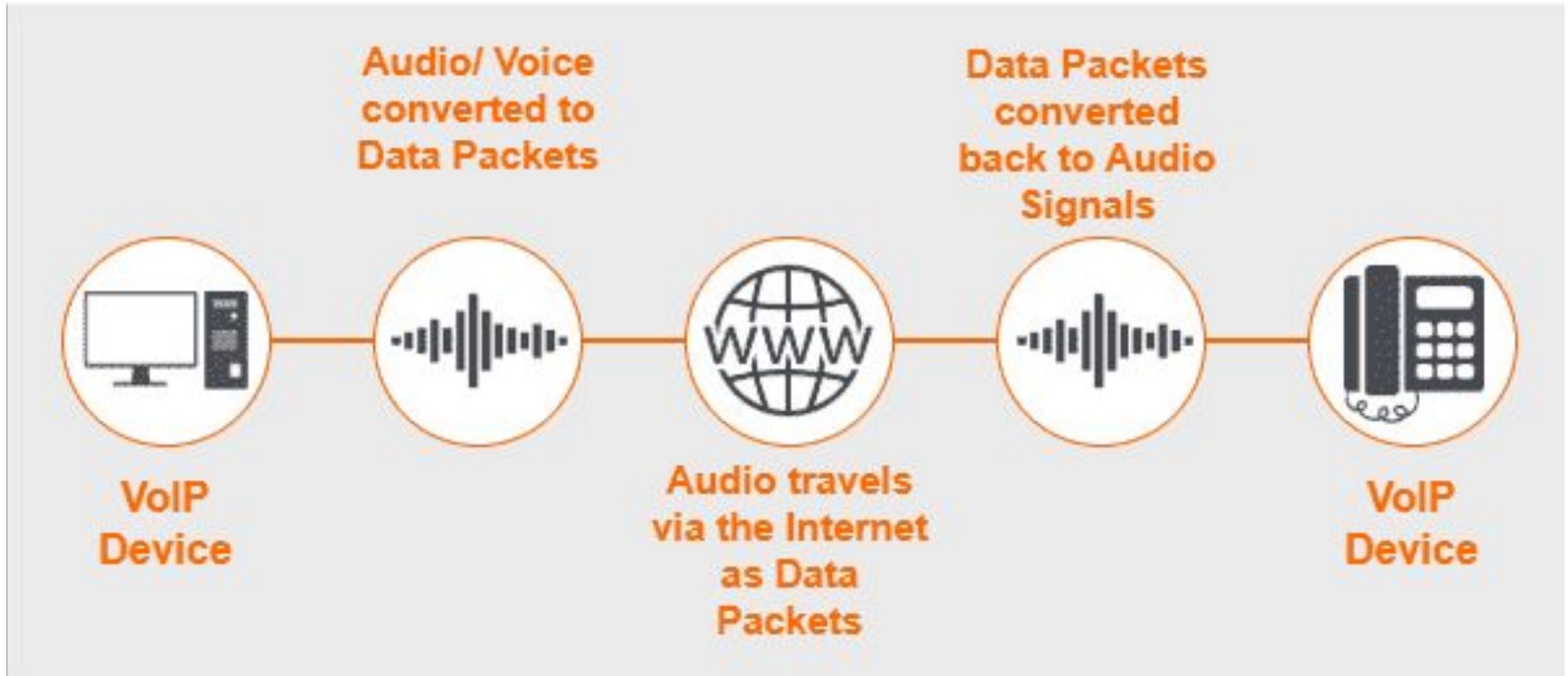
   - **Internet Voice calling**

Online Video/Audio Streaming

Online Multiplayer Video Games

Voice/Video Calls over Internet

Security Considerations

- DCCP does not provide cryptographic security guarantees.

- Applications desiring hard security should use IPsec or end-to-end security of some kind.

- Attackers cannot hijack a DCCP connection unless they can guess valid sequence numbers.

- The sequence number validity and mobility mechanisms provide security.

Security Considerations

- Prevents DDoS attacks – init cookie

- Prevents Sequence Number Attack

    - Large Sequence Number

    - Sequence and Acknowledgement Number Windows

- Data Corruption

    - CRC data Checksum Option

Conclusion

- DCCP - a relatively simple protocol that robustly manages congestion controlled connections without reliability.

- Modular congestion control mechanism - makes it possible to adapt congestion control within a fixed protocol framework.

- Robustness against attack addressed in a more thorough way.

THANK YOU