**SEANet报文设计**

（v0.73）

编 制：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

编制日期：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

审 核：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

批 准：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**国家网络新媒体工程技术研究中心**

# 目 录

[目 录 2](#_Toc135051840)

[修订记录 3](#_Toc135051841)

[1. SEAID 5](#_Toc135051842)

[2. SEANet协议栈 5](#_Toc135051843)

[3. SEANet报文结构 6](#_Toc135051844)

[4. IDP协议 7](#_Toc135051845)

[5. SEANet传输协议族 9](#_Toc135051846)

[5.1 SEANet传输层报文 9](#_Toc135051847)

[5.2 SEANet网络增强传输机制 11](#_Toc135051848)

[5.3 SEANet网络增强传输报文 11](#_Toc135051849)

[6. SEADP协议 12](#_Toc135051850)

[6.1 SEADP协议层次结构 13](#_Toc135051851)

[6.2 SEADP原理及传输机制 13](#_Toc135051852)

[6.3 SEADP报文格式 13](#_Toc135051853)

[6.4 SEADP传输流程 18](#_Toc135051854)

[7. SEAUP协议 19](#_Toc135051855)

[7.1 SEAUP协议层次结构 19](#_Toc135051856)

[7.2 SEAUP原理及传输机制 19](#_Toc135051857)

[7.3 SEAUP报文格式 20](#_Toc135051858)

[7.4 SEAUP传输流程 22](#_Toc135051859)

[8. SEASP协议 22](#_Toc135051860)

[8.1 SEASP协议层次结构 23](#_Toc135051861)

[8.2 SEASP原理及传输机制 23](#_Toc135051862)

[8.3 SEASP报文格式 26](#_Toc135051863)

[8.4 SEASP传输流程 31](#_Toc135051864)

[9. 附录 33](#_Toc135051865)

[9.1 变长整数编码 33](#_Toc135051866)

[9.2 IDP首部Flag分配和使用情况 33](#_Toc135051867)

[9.3 NeT\_defined Fields字段分配和使用情况 34](#_Toc135051868)

[9.4 数据报文设计框架 35](#_Toc135051869)

# 修订记录

|  |  |  |  |
| --- | --- | --- | --- |
| 版本 | 日期 | 作者 | 修改内容 |
| V0.1 | 2022-7-5 | 韩锐、李杨 | 创建文档 |
| V0.11 | 2022-7-15 | 韩锐、李杨 | 修改网内服务的划分，在idp字段增加网内服务类型，细化偏好字段的设计 |
| V0.2 | 2022-9-2 | 韩锐、李杨 | 调整整体设计思路，增加ID传输层，提供基于ID数据包层面传输，包含IDP机制 |
| V0.3 | 2022-9-5 | 李杨 | 基于讨论结论，更新文档 |
| V0.4 | 2022-10-30 | 李杨 | 1）第1章，更新SEAID描述  2）第2，3章，添加SEASP描述  3）第4章，补充IDP Preference字段定义  4）增加第6章：SEASP设计  5）补充第7章：SEADP设计  6）修改第8章：SEAUP设计 |
| V0.5 | 2022-11-4 | 李杨 | 1）补充了IDP首部IrA Flag和IrA para中关于缓存的定义  2）修改IDP首部Dest SEAID-s、Source SEAID-s字段的长度和定义，将其修改为四个应用定义字段（长度为16bytes），修改Flag为4bits，Reserved为4bits。增加附录9.2用以描述Flag取值分配和使用情况  3）修改SEADP中偏好字段的定义，去掉协同存储，变为预留字段  4）根据SEADP实现需求：   * SEADP数据分片报文（FDAT,DAT）偏好中，补充了存储可靠性字段的详细定义 * SEADP无数据块分片响应报文（NACK）中，补充了“表示无数据块”详细定义和说明 * SEADP传输结束报文（FIN）中，补充了结束原因的详细定义和说明 * REQ，NACK,FIN报文中，type字段后添加4bits预留字段，用于字节对齐 |
| V0.6 | 2023-3-6 | 李杨 | 1）对SEANet传输层协议整体进行了规划，分为面向数据块、面向字节流和面向数据报三种模式，并基于此对文档中相关内容进行更新  2）更新SEAUP部分  3）更新SEASP部分 |
| V0.61 | 2023-3-15 | 李杨 | 1) 修改SEAGP的英文全拼  2）将公共偏好部分放到了SEAGP层，将高可靠增强传输相关的消息报文使用SEAGP承载  3）SEAUP/SEADP/SEASP上偏好统一设置为32bits，留出了预留字段为将来的存储/算力等使用  4）对全文的报文格式表格进行了梳理和修改 |
| V0.7 | 2023-3-22 | 李杨 | 1）协议层次中去掉SEAGP，SEAGP部分字段更改为公共报文头  2）报文中增加version版本字段  3）对SEAUP/SEADP/SEASP进行梳理和更新  4）此版本中SEAUP设计时，数据报的长度限制在1个MTU内 |
| V0.71 | 2023-3-27 | 李杨 | 根据大家反馈意见修改文稿  1）version字段放到type字段之前  2）建议一个NACK可以带多个（一段）数据包，而不是每个NACK只带一个包  3）需讨论多路径使用Option A和B后，无法与INT的BCD字段一起使用  4）源SEAID、目的SEAID传输组合表需要修改，匹配后面SEAID的类型 |
| V0.72 | 2023-4-14 | 李杨 | 1）增加宋磊反馈意见，把RSIP拿到IDP层之后，可在传输层原RSIP位置放一个“高可靠传输的流标识”，占用2或者4个字节，方便传输层流表在自己的层次上做匹配（待讨论）  2）把NeT\_defined Fields字段放到了preference字段后面，使得三种传输协议下字段偏移量相同便于处理 |
| V0.73 | 2023-5-15 | 李杨 | 1）将包序号PN放到了公共报文首部  2）增加附录9.4数据报文设计框架  3）修改5.3节中NACK和NACK\_reply格式 |

# SEAID

SEAID：**ID**entifier in **SEA**Net，海计算网标识，SEAID按类型分为：设备、数据、用户和服务四种。SEAID包括名称标识（SEAID-n）和安全标识（SEAID-s）两部分，即：SEAID = [SEAID-n: SEAID-s]。

SEAID-n：名称标识，160bits，用于标识SEANet网络实体的名称。

SEAID-s：安全标识，256bits，作为SEANet网络实体的安全指纹。

解析系统维护SEAID-n、SEAID-s和NA（网络地址）的映射关系。

SEANet报文中的源ID和目的ID字段中携带的是SEAID-n，目前使用固定长度20 bytes（160 bits）,可支持多种长度类型，包括：1byte，2bytes，4bytes，8bytes，…，32bytes等。SEAID-s可以在SEANet报文的可选字段中携带。

源SEAID和目的SEAID传输组合情况包括：

|  |  |  |
| --- | --- | --- |
| **源SEAID** | **目的SEAID** | **场景示例** |
| 数据标识 | 传输服务标识 | NDC（Named Data Chunk）传输-发送数据 |
| 传输服务标识 | 数据标识 | NDC传输-请求数据 |
| 传输服务标识 | 传输服务标识 | 端到端传输 |
| 传输服务标识 | 组播服务标识 | 组播 |

# SEANet协议栈



图 1 SEANet协议栈

SEANet协议栈的示意如图1所示。

* IDP（ID Protocol）：位于网络层，是一个处理机制，负责基于SEAID的地址变换。
* SEADP（SEANet Data chunk Protocol）: 位于传输层，是一种面向数据块的网络增强的传输层协议；支持“推”和“拉”两种传输模式，支持数据块网内缓存，支持流量控制和拥塞控制、支持可靠传输，支持利用网络的能力对传输过程进行增强。
* SEAUP（SEANet User datagram Protocol）: 位于传输层，是一种面向数据报的网络增强的传输层协议，支持利用网络的能力对传输过程进行增强。
* SEASP（SEANet Service connection Protocol）: 位于传输层，是一种面向字节流的网络增强的传输层协议；支持流量控制和拥塞控制、支持可靠传输，支持利用网络的能力对传输过程进行增强。
* 安全协议：待设计。

备注：后续补充SCMP（SEANet Control Message Protocol）相关内容

# SEANet报文结构

SEANet报文的层次结构如下图2所示：



图 2 SEANet报文层次结构

1. 当网络层协议使用IPv6时，以太网帧中的类型字段填IPv6协议所对应字段。
2. IPv6中的Next header填写的是已注册的互联网协议号（Assigned Internet Protocol Numbers），需要在国际标准化组织IANA中申请和注册，协议号按顺序进行申请和分配，当前阶段，145~252为可用的未被定义序号[[[1]](#footnote-1)]。需要向IANA申请和注册IDP协议和SEANet传输层协议的协议号，用于IPv6中的Next Header字段的填写。**开发过程中，暂时约定IDP为146（0x92），****SEANet传输层协议为147（0x93）。**
3. 使用SEANet传输层协议的公共首部Public Header的Type字段标明SEANet传输层协议的报文类型。**Type字段的高3位取值为000时，表示是公共消息报文；取值为001时，表示SEADP协议相关报文；取值为010时，表示SEAUP协议相关报文；取值为011时，表示SEASP协议相关报文。**

# IDP协议

IDP协议位于网络层，是一个处理机制，负责基于SEAID的地址变换。IDP首部位于IPv6首部和SEANet传输协议公共首部之间，其格式如图3所示。



图 3 IDP首部格式

* **Next Header：**8 bits，指明下一个IPV6扩展首部的类型。
* **Header Length：**8 bits，首部长度，单位是bytes。
* **D.SEAID type**：4bits，指明目的SEAID的类型。
* **S.SEAID type**：4bits，指明源SEAID的类型。

|  |  |
| --- | --- |
| **S.SEAID type和D.SEAID type字段** | |
| **值** | **含义** |
| 0x0 | 数据标识 |
| 0x1 | 传输服务标识 |
| 0x2 | 组播服务标识 |
| 0x3-0xF | 预留 |

* **D.SEAID-n Length**：4bits，指明目的SEAID-n的长度。
* **S.SEAID-n Length**：4bits，指明源SEAID-n的长度。

|  |  |
| --- | --- |
| **D.SEAID-n Length和S.SEAID-n Length字段** | |
| **值** | **含义** |
| 0x0 | 不包含对应的SEAID-n字段（支持不包含源SEAID-n） |
| 0x1 | 对应的SEAID-n字段长度1Bytes |
| 0x2 | 对应的SEAID-n字段长度2Bytes |
| 0x3 | 对应的SEAID-n字段长度4Bytes |
| 0x4 | 对应的SEAID-n字段长度8Bytes |
| 0x5 | 对应的SEAID-n字段长度16Bytes |
| 0x6 | 对应的SEAID-n字段长度20Bytes |
| 0x7 | 对应的SEAID-n字段长度32Bytes |
| 0x8-0xF | 预留 |

* **Preference**： 56bits，表示IDP处理偏好值，具体格式如下。



图 4 IDP首部Preference字段格式

**1）业务标识（srvType）**：6bits，最多可支持64种业务定义，包括：默认、通用业务类型和定制化业务。每种业务对应一个逻辑拓扑，其中：0表示默认拓扑。

**2）路由策略（RoST）**：2bits，支持4种路由策略，例如：DHT策略（IPFS路由）、最短路径策略等。其中：0表示默认策略。

**3）队列优先级（QP）：**8bits，用于标识数据包在队列中的处理优先级，最多支持256个优先级，每个优先级可以映射到一个或多个队列。

**4）即刻重寻址标识（****IrA Flag）**：8bits，每个bit标识一种即刻重寻址类型，包括：隐匿传输、多路径传输等。支持多个bit同时置1情况。

IrA Flag字段表示成如下形式：



|  |  |  |
| --- | --- | --- |
| **IrA Flag定义** | | |
| **位数** | **值** | **含义** |
| Bit7 | 1 | 隐匿传输 |
| Bit6 | 1 | 多路径传输 |
| Bit5 | 1 | 缓存 |
| Bit4~Bit0 |  | 预留（未来可用于确定性传输、算力路由等） |

示例：当只有隐匿传输一种重寻址偏好时，IrA Flag=10000000=0x80。

**5）即刻重寻址参数（****IrA Para）**：4bytes，每种即刻重寻址类型对应一个参数，其中：

即刻重寻址参数1：4bits，为隐匿传输参数；

即刻重寻址参数2：4bits，为多路径传输参数;

即刻重寻址参数3：4bits，为缓存参数;

即刻重寻址参数4~8待定义。

* **Reserved**：4bits，预留。
* **Flag**：4bits，用于标识是否存在可选字段，取值范围是0x0~0xF，采用申请和分配的方式，每个Flag取值对应一种应用组合情况，应用组合决定可选字段的使用情况。具体Flag取值的分配情况见**附录9.2**所示。
* **Dest SEAID-n**：目的SEAID-n，变长，根据D.SEAID-n Length取值确定长度。
* **Source SEAID-n**：源SEAID-n，变长，根据S.SEAID-n Length取值确定长度。
* **Extended Address**：可选字段，扩展地址，128bits。
* **APP-defined Field A：**可选字段，128bits，网络应用自定义。
* **APP-defined Field B：**可选字段，128bits，网络应用自定义。
* **APP-defined Field C：**可选字段，128bits，网络应用自定义。
* **APP-defined Field D：**可选字段，128bits，网络应用自定义。

# SEANet传输协议族

SEANet传输协议族包括：SEADP协议、SEAUP协议和SEASP协议，使用公共的报文首部Public Header，需要向IANA申请SEANet传输协议的协议号，用于在IPv6中的Next Header字段的填写。开发过程中，暂时约定为147（0x93）。

SEANet传输协议的特点在于能够提供以数据包为基本处理单元的网络增强能力，提升数据包在网络中的传输质量，例如：降低丢包率等。通过在SEANet传输协议偏好字段中携带传输需求、传输标识、传输参数等字段辅助网络增强传输相关机制的生效，网络节点可以填写、读取和修改相关字段。因此，SEANet数据包（添加传输层、网络层和链路层报文首部后）不能超过一个MTU，以保证在网络层（IP层）不会被分段。

### SEANet传输层报文



图 5 SEANet传输层报文格式

* **Public Header：**10bytes，为SEANet传输层协议的公共报文头，使用Type字段标明SEANet传输层协议报文类型。
* **Type-defined Fields**：变长,根据Type类型，进行单独定义。

#### SEANet传输层公共首部格式

SEANet传输层协议使用公共首部（Public Header），其格式如下：



图 6 SEANet传输层公共首部（Public Header）格式

* **Version：**8bits，标明SEANet协议报文的版本号，取值及含义如下表所示。

|  |  |
| --- | --- |
| **Version字段** | |
| **值** | **含义** |
| 0x1 | 版本xx |
| 0x0,0x2~0xFF | 预留 |

* **Type：**8bits，SEANet传输层协议报文类型，高位的3bits用于标明协议类型，低位5bits用于标明每个类型下面的报文分类，具体取值及含义如下表所示。

|  |  |  |
| --- | --- | --- |
| **bit7~bit5** | **bit4~bit0** | **含义** |
| 000  **公共消息**  **报文** | 00001 | 否定性确认报文（NeT\_Reliable\_NACK） |
| 00010 | 否定性确认回复报文（NeT\_Reliable\_NACKReply） |
| 00000,00011~11111 | 预留 |
| 001  **SEADP协议**  **相关报文** | 00000 | SEADP数据报文（DP\_DAT） |
| 00001 | 数据块分片请求（DP\_PULL\_REQ） |
| 00010 | 无数据块分片响应（DP\_PULL\_NACK） |
| 00011 | 数据块分片接收选择性确认（DP\_PUSH\_ACK） |
| 00100 | 数据块分片接收否定性确认（DP\_PUSH\_NACK） |
| 00101 | 传输结束（DP\_FIN） |
| 00110~11111 | 预留 |
| 010  **SEAUP协议**  **相关报文** | 00000 | SEAUP数据报文（UP\_DAT） |
| 00001~11111 | 预留 |
| 011  **SEASP协议**  **相关报文** | 00000 | SEASP数据报文（SP\_DAT） |
| 00001 | 选择性确认报文（SP\_SACK） |
| 00010 | 否定性确认报文（SP\_NACK） |
| 00011 | 协商报文（SP\_NEO） |
| 00100 | 连接关闭报文（SP\_Connection\_CLOSE） |
| 00101~11111 | 预留 |
| 100~111 | 预留，用于SEANet安全协议中握手协议、报警协议等相关报文定义 | |

* **Length：**16 bits，Public Header 和Type-defined Fields的总长度，单位bytes。
* **Checksum：**16 bits，校验和，校验内容包括：公共首部的Version、Type、Length字段，以及IDP首部的Next Header、Header Length、D.SEAID Type、S.SEAID Type、D.SEAID Length、S.SEAID Length、Dest SEAID-n、Source SEAID-n字段。
* 包单调递增，循环使用，发送端发送的第一个包的序号是1，随后的数据包序号的都大于前一个包的序号。

### SEANet网络增强传输机制

网络增强传输机制以数据包为基本处理单元，使用网络节点的能力，提升数据包在网络中的传输质量，例如：降低丢包率等。网络增强传输机制在SEADP、SEAUP、SEASP协议中均可使用。若要使用相关机制需要在SEADP/SEAUP/SEASP数据报文的偏好字段中将相关标志位置位。

#### 高可靠增强传输机制

针对SEANet网络节点间不可靠的传输链路，设计以数据包为单位的，网络节点之间的丢包检测和重传机制，改善网络节点之间丢包问题，达到对网络节点之间传输链路可靠性增强的目的。使用高可靠增强传输机制下，网络节点之间传输链路的丢包率会下降。

**参见《SEANet高可靠增强传输机制设计方案》。**

### SEANet网络增强传输报文

#### 高可靠增强传输报文

##### 5.3.1.1 否定性确认报文（NeT\_Reliable\_NACK）

当Public Header中Type字段取值为0x1(00000001)时，标明为否定性确认报文（NeT\_Reliable\_NACK），NeT\_Reliable\_NACK用于高可靠增强传输机制中接收方通知发送方没有收到某个数据包，格式如下：



图 7 NeT\_Reliable\_NACK报文格式

* **未确认序号数量（NPN\_Num）:** 8bits，用于标识报文中包括的连续未确认序号数量。
* **起始未确认序号（Intial\_NPN）：** 32bits，标识报文中包括的连续未确认序号中未被确认的最小数据序号RPN。

备注：

##### 5.3.1.2 否定性确认回复报文（NeT\_Reliable\_NACKReply）

当Public Header中Type字段取值为0x2(00000010)时，标明为否定性确认回复报文（NeT\_Reliable\_NACKReply），NeT\_Reliable\_NACKReply用于高可靠增强传输机制中发送方通知接收方已经收到了某个数据包的NACK，格式如下：



图 8 NeT\_Reliable\_NACKReply报文格式

* **回复NACK数量（rNPN\_Num）:** 8bits，用于标识报文中包括回复连续NACK的数量。
* **回复起始NACK序号（Intial\_rNPN）：** 32bits，标识报文中包括的要回复的连续NACK中最小数据序号RPN。

# SEADP协议

SEADP是一种面向数据块的网络增强的传输层协议，支持“推”和“拉”两种传输模式，支持数据块网内缓存，支持流量控制和拥塞控制、支持可靠传输，支持利用网络节点的能力对传输过程进行增强。设计时需要遵循下述原则和约定：

* SEADP协议的源SEAID和目的SEAID，一个为数据SEAID，一个为服务SEAID；
* SEADP的基本传输单元是数据块（chunk），具备数据块切分和重组的能力，数据块切分后的基本单元成为数据块分片（piece）；
* SEADP支持网络中间节点在传输过程中对数据块进行缓存，支持从缓存数据块的网络节点获取数据块；支持网内缓存需要在IDP首部的IrA Flag字段中标出;
* SEADP支持接收者驱动（“拉”）和发送者驱动（“推”）两种传输模式，支持的流量控制和拥塞控制、支持数据块级别的可靠传输;
* SEADP数据报文大小在添加公共报文首部、网络层和链路层报文首部后，不超过一个MTU，保证在网络层（IP层）不会被分段。

备注：基于网络MTU值，SEAUP会对数据分片(piece)的长度提出限制，要求其小于：MTU-26B(MAC头)-40B(IPv6头)-132B(IDP头)-10B(公共头)-47B(DP\_DAT头)=1245B。

### SEADP协议层次结构



图 9 SEADP层次结构

### SEADP原理及传输机制

备注：下阶段补充，重点要说明“拉”模式和“推”模式兼容问题，以及对于网络增强机制使用问题。

### SEADP报文格式

当公共首部Public Header 的Type字段的高位取值为001时，表示是SEADP协议相关报文，使用Type字段的低5位标识SEADP报文类型，其中：

* Type为0x20（001 00000）时，报文类型：SEADP数据报文（DP\_DAT）
* Type为0x21（001 00001）时，报文类型：数据块分片请求（DP\_PULL\_REQ）
* Type为0x22（001 00010）时，报文类型：无数据块分片响应（DP\_PULL\_NACK）
* Type为0x23（001 00011）时，报文类型：数据块分片接收选择性确认（DP\_PUSH\_ACK）
* Type为0x24（001 00100）时，报文类型：数据块分片接收否定性确认（DP\_PUSH\_NACK）
* Type为0x25（001 00101）时，报文类型：传输结束（DP\_FIN）

备注：DP\_PUSH\_ACK和DP\_PUSH\_NACK报文后续用于“推”模式下对数据分片的接收确认，目前仅列出、未详细设计。

#### SEADP数据报文（DP\_DAT）

SEADP数据报文（DP\_DAT）报文用于“拉”模式下回复接收端向发送端请求的数据块分片，或“推”模式下发送端向接收端发送数据分片；DP\_DAT报文为SEADP数据报文，可使用网络增强传输和IDP的即刻重寻址相关机制，格式如下：



图 10 DP\_FDAT报文格式

* **Flags**：8bits,标志位，如下所示，左边为高位，右边为低位。



|  |  |
| --- | --- |
| **位数** | **含义** |
| bit7,bit6 | 标识Preference的长度，未来可用于Preference长度扩展，其中：  00：8bytes（默认长度） |
| bit5 | 用于标识是否存在NeT\_defined Fields字段  0：不存在；1：存在 |
| bit4 | 用于标识是否存在Chunk size字段  0：不存在；1：存在 |
| bit3 | 用于标识是否存在Chunk checksum字段  0：不存在；1：存在 |
| bit2~bit0 | 预留，现阶段置0，未来可用于扩展可选字段 |

* **Preference：**Flags的(bit7,bit6)=(0,0)时，长度为8bytes，未来可通过设置Flags，扩展Preference长度；数据块的传输偏好，用于标识对传输、存储、算力等需求、资源选择意向、使用增强机制和参数等，用于指导数据块在传输过程中的网内处理操作。



图 11 DP\_DAT报文中Preference字段格式

* **传输优先级（Transport Priority, TP）:** 8bits，用于标识应用对网络提出的传输优先级需求，可在应用识别后根据应用的类型填写。网络服务商可以将优先级需求映射为可满足上述需求的一个/组业务逻辑拓扑（业务标识）、及每个拓扑下对应路由策略和队列转发优先级（优先级标识）。

备注：由端节点（SEANet协议起点）填写，网络中间节点可以查看、不能修改。



* **网络增强传输标志（Network Enhanced Transport Flag, NeT Flag）：**8bits，用于标识当前生效的网络传输增强机制，每个bit标识一种增强机制，支持多个bit同时置1情况。NeT Flag字段表示成如下形式：

备注：端节点（SEANet协议起点）填写，网络中间节点可以查看、不能修改。



|  |  |  |
| --- | --- | --- |
| **位数** | **值** | **含义** |
| bit7 (RFlag) | 1 | 高可靠增强传输机制 |
| bit6~bit0 | 预留 | 用于冗余传输等 |

示例：当只有高可靠增强传输一种机制生效时，NeT Flag=10000000=0x80。

* **网络增强传输参数（NeT Para）：**16bits

备注：网络中间节点可以查看、修改此字段。



**NeT Para 1（RPara）**：4bits，携带高可靠增强传输参数；

**NeT Para 2~8**：待定义。

* **存储意向（Storage Intent, SI）：**8bits，标识缓存/存储时对资源选择时的意向需求，包括：存储可靠性、存储位置等。通过此字段可以确定存储/缓存时可用的网络节点范围。

备注：由端节点（SEANet协议起点）填写，网络中间节点可以查看、不能修改。



|  |  |  |
| --- | --- | --- |
| **位数** | **含义** | **取值** |
| bit7-bit4（4bits） | 存储可靠性, Reliability | 用于标识数据存储的可靠性需求  0x0：不存储  0x1：冷门缓存  0x2：热门缓存  0x3：一般存储  0x4：可靠存储  0x5：高可靠存储  0x6：读写一致存储  0x7-0xF：预留 |
| bit3-bit2（2bits） | 存储位置, Location | 用于标识数据存储的位置需求  0：默认  1：数据源附近  2：网络中心  3：网络边缘 |
| bit1-bit0（2bits） | 预留，Reserved | 现阶段置零 |

* **预留：**24bits，可用于支持存储、传输、算力服务等偏好设置，现阶段置0。
* **网络增强传输定义字段（NeT\_defined Fields）:** 可选字段，变长，用于携带网络增强传输所需要的相关字段，不同机制生效时，携带字段的长度和含义不同。当Flags字段的bit5=1时，存在该字段；每个**NeT Flag**取值对应一种增强传输机制的组合，组合情况决定**NeT\_defined Fields**字段的长度和含义。具体取值和分配情况见**附录9.3**所示。
* **Offset：**32bits，表示数据分片在数据块的开始位置。
* **Length：**32bits，表示数据块分片的长度。

* **Chunk size（CS）：**32bits，可选字段，当Flags的bit4=1时存在该字段，表示数据块大小，单位是bytes。最大支持4GB的数据块。
* **Chunk Checksum：**32 bits，可选字段，当Flags的bit3=1时存在该字段，整个chunk的校验和。

备注：一般在发送第一个数据块分片时，会携带Chunk size和Chunk Checksum字段。

* **Payload**：载荷，用于承载数据块分片（piece），需要根据MTU的取值确定Payload中允许承载数据块分片的长度范围。

备注：假定MTU=1500B，要求payload长度小于：1500B-26B(MAC头)-40B(IPv6头)-132B(IDP头)-10B(公共头)-47B(DP\_DAT头)=1245B。

#### 数据块分片请求（DP\_PULL\_REQ）

数据块分片请求（DP\_PULL\_REQ）报文用于“拉”模式下，数据请求端（接收端）通知发送端要请求的数据块分片，支持同时请求多个分片；DP\_REQ 报文为SEADP消息报文，不使用网络增强传输和即刻重寻址相关机制，格式如下：



图 12 DP\_PULL\_REQ报文格式

* **请求分片数量：**8bits，用于标识报文中包括的请求数据块分片的数量。

备注：分片数量的取值范围需要根据MTU值确定，需要保障DP\_PULL\_REQ报文在1个MTU范围内。

报文中包括多个分片offset和分片length字段；字段的数量由请求分片数量决定。

* **分片Offset：**32bits，表示数据分片在数据块的开始位置。
* **分片Length：**32bits，表示数据块分片的长度。

**备注：**第一个数据块分片请求报文，请求分片数量字段置为1，分片offset=0，分片length为经验值，取值时需保障数据块分片响应报文小于1个MTU。

#### 无数据块分片响应（DP\_PULL\_NACK）

无数据块分片响应（DP\_PULL\_NACK）报文用于发送端通知数据请求端（接收端）本地无请求的数据块分片，支持同时通知多个分片；DP\_NACK报文为SEADP消息报文，不使用网络增强传输和即刻重寻址相关机制，格式如下：



图 13 DP\_PULL\_NACK 报文格式

* **无数据分片数量：**8bits，用于标识报文中包括NACK数据块分片数量，最多支持256个。

备注：1）当NACK分片数量=0x0时，表示没有整个数据块。

2）分片数量的取值范围需要根据MTU值确定，需要保障DP\_PULL\_NACK报文在1个MTU范围内。

报文中包括多个分片offset和分片length字段；字段的数量由NACK分片数量决定。

* **分片Offset：**32bits，表示数据分片在数据块的开始位置。
* **分片Length：**32bits，表示数据块分片的长度。

#### 数据块分片接收选择性确认（DP\_PUSH\_ACK）

待补充

#### 数据块分片接收否定性确认（DP\_PUSH\_NACK）

待补充

#### 传输结束（DP\_FIN）

传输结束（DP\_FIN）报文用于通知对端当前连接正在被关闭；DP\_FIN报文为SEADP消息报文，不使用网络增强传输机制和即刻重寻址相关机制，格式如下：



图 14 DP\_FIN格式

* **Reason Phrase Length**：变长整数，关闭连接的原因短语长度。
* **Reason Phrase**：关闭连接的原因，是一个UTF-8编码的字符串。

|  |  |
| --- | --- |
| **Reason Phrase值** | **含义** |
| Finish | 传输完成 |
| Error | 传输异常中断 |

### SEADP传输流程



图 15 SEADP传输流程（拉模式）

备注：下阶段补充 “推”模式传输流程

# SEAUP协议

SEAUP是一种面向数据报的网络增强的传输层协议，支持利用网络节点的能力对传输过程进行增强，设计时需要遵循下述原则和约定：

* SEAUP一种ID-to-ID的传输层协议，源SEAID和目的SAEID均为服务SEAID；
* SEAUP面向数据报传输，不会对应用层待传输的数据报做任何地拆分和拼接操作；
* SEAUP数据报文大小在添加公共报文首部、网络层和链路层报文首部后，不超过一个MTU，保证在网络层（IP层）不会被分段;

备注：基于网络MTU值，SEAUP会对应用层待传输数据报的长度提出限制，要求其小于：MTU-26B(MAC头)-40B(IPv6头)-132B(IDP头)-10B(公共头)-31B(UP\_DAT头)= 1261B。

* SEAUP数据包支持使用IDP层的“一包一路由”机制，针对每个SEAUP数据包,网络节点可以根据传输需求和网络状态自主路由；
* SEAUP数据包可以选择启用高可靠增强传输机制，降低在网络传输中的丢包率，使用时需将偏好字段中的RFlag置为1。

### SEAUP协议层次结构



图 16 SEAUP协议层次结构

### SEAUP原理及传输机制

SEAUP是一种面向数据报的、网络增强的传输层协议。参与SEAUP传输过程的实体包括：发送端、网络节点和接收端，发送端与接收端之间传输数据时，网络节点根据数据包中携带的应用需求对传输进行增强，网络节点可以填写、读取和修改SEAUP报文中的相关字段。

数据传输的具体流程如下：

1）发送端将应用待发送的数据报封装成SEAUP数据包并发送，SEAUP数据包中携带应用对网络提出的传输优先级、资源意向需求、使用的增强传输机制和参数等；

2）网络节点使用相关机制对SEAUP数据包的传输进行增强；

3）接收端接收到数据包后直接将其返回给应用。

备注：后期可能会补充乱序重排机制

### SEAUP报文格式

当公共首部Public Header 的Type字段的高位取值为010时，表示是SEAUP协议相关报文：

* Type为0x40（010 00000）时，报文类型：SEAUP数据报文（UP\_DAT）

#### SEAUP数据报文（UP\_DAT）

SEAUP数据报文UP\_DAT支持使用IDP层的即刻重寻址等相关机制，格式如下：



图 17 UP\_DAT报文格式

* **Flags**：8bits,标志位，如下所示，左边为高位，右边为低位。



|  |  |
| --- | --- |
| **位数** | **含义** |
| bit7, bit6 | 标识Preference的长度，未来可用于Preference长度扩展，其中：  00：8bytes（默认长度） |
| bit5 | 用于标识是否存在NeT\_defined Fields字段  0：不存在；1：存在 |
| bit4~bit0 | 预留，现阶段置0，未来可用于扩展可选字段 |

**备注：**Flags=00100000时，表示存在NeT\_defined Fields，preference长度为8bytes。

* **Preference：**Flags的(bit7,bit6)=(0,0)时，长度为8bytes，未来可通过设置Flags，扩展Preference长度；数据报的传输偏好，用于标识对传输、算力等需求、资源选择意向、使用的增强机制、相关参数等，用于指导数据报在传输过程中的网内处理操作。



图 18 UP\_DAT报文中preference字段格式

* **传输优先级（Transport Priority, TP）:** 8bits，用于标识应用对网络提出的传输优先级需求，可在应用识别后根据应用的类型填写。网络服务商可以将优先级需求映射为可满足上述需求的一个/组业务逻辑拓扑（业务标识）、及每个拓扑下对应路由策略和队列转发优先级（优先级标识）。

备注：由端节点（SEANet协议起点）填写，网络中间节点可以查看、不能修改。

* **网络增强传输标志（Network Enhanced Transport Flag, NeT Flag）：**8bits，用于标识当前生效的网络传输增强机制，每个bit标识一种增强机制，支持多个bit同时置1情况。NeT Flag字段表示成如下形式：

备注：端节点（SEANet协议起点）填写，网络中间节点可以查看、不能修改。



|  |  |  |
| --- | --- | --- |
| **位数** | **值** | **含义** |
| bit7 (RFlag) | 1 | 高可靠增强传输机制 |
| bit6~bit0 | 预留 | 用于冗余传输等 |

示例：当只有高可靠增强传输一种机制生效时，NeT Flag=10000000=0x80。

* **网络增强传输参数（NeT Para）：**16bits

备注：网络中间节点可以查看、修改此字段。



**NeT Para 1（RPara）**：4bits，携带高可靠增强传输参数；

**NeT Para 2~8**：待定义。

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

* **预留：**24bits，后续用于支持算力服务等偏好设置，现阶段置0。
* **网络增强传输定义字段（****NeT\_defined Fields）:** 可选字段，变长，用于携带网络增强传输所需要的相关字段，不同机制生效时，携带字段的长度和含义不同。当Flags字段的bit5=1时，存在该字段；每个**NeT Flag**取值对应一种增强传输机制的组合，组合情况决定**NeT\_defined Fields**字段的长度和含义。具体取值和分配情况见**附录9.3**所示。
* **Payload：**载荷，用于承载数据报，需要根据MTU的取值确定Payload中允许承载数据报的长度范围。

备注：假定MTU=1500B，要求payload长度小于：1500B-26B(MAC头)-40B(IPv6头)-132B(IDP头)-10B(公共头)-31B(UP\_DAT头)=1261B。

### SEAUP传输流程

SEAUP数据传输过程中，可以选择启用高可靠增强传输机制，降低传输丢包率。SEAUP启用高可靠机制和不启用高可靠机制的传输流程如下图所示。



图 19 SEAUP传输流程（启用高可靠增强传输机制）



图 20 SEAUP传输流程（不启用高可靠增强传输机制）

# SEASP协议

SEASP是一种面向字节流的网络增强的传输层协议，支持流量控制和拥塞控制、支持可靠传输，支持利用网络节点的能力对传输过程进行增强。设计时需要遵循下述原则和约定：

* SEASP一种ID-to-ID的传输层协议，源ID和目的ID均为服务ID；
* SEASP协议中的发送端和接收端是指SEASP协议的起点和终点，可以为终端设备UE、CPE、PE等；网络节点参与SEASP传输过程，包括：端网协同的参数协商、基于网络节点的传输可靠性增强等；
* SEASP是一种面向连接的协议，使用 [发端ID, 收端ID] 唯一地标识一个连接，通过握手协商方式建立连接，协商的参与方包括：发送端、接收端和网络（网络节点），通过收发端的传输需求和网络的资源状态共同完成传输参数的协商；
* SEASP协议不希望出现IP层分片，构建SEASP包时，在添加公共报文首部、网络层和链路层报文首部后要小于1个MTU；

备注：基于网络MTU值，SEASP会对字节流分段（segment）长度提出限制，要求其小于：MTU-26B(MAC头)-40B(IPv6头)-132B(IDP头)-10B(公共头)-47B(SP\_DAT头)=1245B。

* SEASP连接不绑定到某条网络路径上，SEASP数据包支持使用IDP层的“一包一路由”机制，针对每个SEASP数据包,网络节点可以根据传输需求和网络状态自主路由，最终实现SEASP连接中数据包的多路径传输；
* SEAUP数据包可以选择启用高可靠增强传输机制，降低在网络传输中的丢包率，使用时需将偏好字段中的RFlag置为1；
* SEASP采用端网协同的拥塞控制机制，网络节点可根据感知的网络状态在数据包转发过程，通过缓冲、复制、变路径、变队列等方式实现拥塞控制，同时会协助端侧节点感知网络拥塞状态。

### SEASP协议层次结构



图 21 SEASP层次结构

### SEASP原理及传输机制

SEASP是一种网络增强的传输层协议，参与SEASP传输过程的实体包括：发送端、网络节点和接收端，网络节点可以填写、读取和修改SEASP传输层协议报文中的相关字段，包括：携带的传输优先级需求、传输资源选择意向需求等。



图 22 SEASP协议工作原理示意图

整个传输过程包括：连接建立、数据传输和连接关闭三个阶段。

（1）连接建立阶段

由发送端发起，网络节点、接收端共同协商完成，目标是协商出合适的传输参数（包括传输速率等），用于后面的数据传输阶段；传输过程中基于这个传输速率传输数据、传输过程中尽量不调整速率；本阶段涉及到端网协同的协商机制。具体的流程如下：

1）发送端提出传输需求参数，包括：传输速率、数据包尺寸等；

2）网络节点根据网络整体服务状态、剩余资源状态等，给出合适的传输参数；

3）接收端根据发送端需求参数和网络给出参数确定合适参数，返回给客户端进行确认。

备注：现阶段只做端到端协商，网络节点暂不参与。

（2）数据传输阶段

发送端与接收端之间传输数据，网络节点根据数据包中携带的应用需求，选择多路径、高可靠等机制对传输进行增强。在保证整个传输过程传输数据的完整性、有序性的同时，使用网络能力增强传输过程，更充分地利用网络带宽、降低丢包率，实现“高吞吐、抗丢包”的高效网络增强传输。具体流程如下：

1）发送端发送数据包，数据包中携带应用对网络提出的传输需求；

2）网络节点根据需求，选择合适的网络传输增强机制并映射成相关参数；

3）网络节点使用相关机制对数据包的传输进行增强，包括：高可靠性传输增强、多路径传输等；

4）接收端进行丢包检测和差错重传，对接收数据进行排序、重组和恢复，当某一段数据拼装完整后，通知应用读取数据。

5）当网络感知到资源不足即拥塞时，会通知发送端调节发送速率。（本阶段暂不实现）

本阶段涉及到端侧可靠传输机制、端网协同拥塞控制机制、以及网络提供的高可靠传输增强机制等，数据报文中需要携带应用需求及使用增强机制时所需参数。

（3）连接关闭阶段

由发送端/接收端发起关闭请求，发送端、接收端、网络节点收到请求后释放相关资源。关闭连接后，不能在此连接内传输数据。

#### 端网协商的连接机制

适用于面向字节流的可靠传输，分为连接建立和连接关闭两个阶段。

**A. 连接建立**

设计目标：在连接建立阶段，基于发送端和接收端提出的传输速率目标，网络节点根据网络整体服务状态、剩余资源状态等，给出一个合适的传输速率，后续发送端和接收端之间基于这个传输速率传输数据、传输过程中尽量不调整速率。

具体机制：

1）发送端发送**协商请求报文**给接收端，携带发送端期望发送速率Vs及其他传输参数，包括：MSS，WindowSize，缓冲区大小等；

2）接收端根据Vs及自身期望接收速率Vr，确定最终的发送速率V和其他传输参数，发送**协商回复报文**给发送端；

3）发送端收到报文后，回复**协商确认报文**给接收端，协商完成。

备注：1）现阶段假设网络能力足够，只在端侧协商即可；

2）端网协商的方法后续设计添加。

B. **连接关闭**

设计目标：用户可以主动关闭连接，并能通知对方，释放资源；同时系统支持超时关闭等异常连接关闭机制。

1）显示关闭机制：

* 终端可以发送CLOSE给另一端，表示要关闭连接；
* 终端可以在任何时候发送RST来表示连接的异常终止；
* 终端也可以在发送CLOSE之前，发送GOAWAY给另一端，用来表示连接将要被关闭。GOAWAY意味着正在活动的流将会继续处理，但是GOAWAY的发送端不会再发起或者接收任何新的流。

系统维护两个关闭状态closing、draining

* closing 状态：端主动关闭连接即向对端发送CLOSE时进入该状态，此时收到所有的应用层数据都将只会回复 CONNECTION\_CLOSE。
* draining 状态：端收到 CLOSE 时进入状态，该状态下终端不再回复任何数据。

2）隐式关闭机制：

* 发送某个数据包后，时间T内仍未收到ACK报文，关闭连接，默认T取值为15分钟，可在连接建立阶段协商该参数；
* 当没有任何数据传输的时间超过了空闲时间阈值ICSL，关闭连接，默认ICSL为30秒，最大取值为10分钟，可在连接建立阶段协商该参数；
* 默认情况下当一端关闭连接后，会发送CLOSE，通知对端关闭连接；当显式关闭代价较高时，可以选择激活静默式关闭，即不通知对端，可在连接建立时协商。

#### 端网协同拥塞控制机制

设计目标：当网络感知到拥塞必须调整发送端速率时，网络节点能够对拥塞状态进行精确的感知，并通知发送端调整到一个合适的发送速率。通过网络节点的参与，使得传输速率的设置和调整更加精准，避免调节过程带来的效率损耗。

具体机制：待设计。

备注：

1）现阶段假设网络能力足够，使用初始协商速率传输，传输过程中不进行拥塞控制、调节速率。

2）后续设计时可考虑：通过网络感知、评估拥塞状态，决策对不同优先级/SLA的数据包的速率调整比例，在报文中携带速率调整指令信息；端侧根据网络给出的调整指令，调整发送速率。

#### 端侧可靠传输机制

设计目标：能够解决数据在发送方和接收方之间准确、精确传输问题，需要保证传输数据的完整性（数据包收齐）和有序性（可按序组装），提供传输可靠性保障。

设计需求：

（1）由于网络节点间使用高可靠增强机制，所以网络中丢包率较低，应将丢包看成是“小概率”事件

（2）使用高可靠增强机制和多路径机制后，数据包乱序会增加，应将乱序看成是“大概率”事件

（3）丢包检测和确认过程也应保证数据的发送速率

具体机制：拟采用基于ACK的丢包检测和重传机制， 发送端根据收到的确认应答ACK/SACK消息，对“已发包缓冲区”中的数据包进行丢包检测，检测到丢包以后，重新发送该数据包。大致思路如下：

（1）确认应答机制：

* 接收端对收到的数据包，向发送端发送ACK响应（可采用SACK方式）；
* 若某个数据包序号后已经收到N个数据包，且时间超过一定阈值T，则发送NACK响应；
* 支持数据包乱序确认。

（2）丢包检测机制：

* 超时机制：设置重传超时阈值RTO，对于“已发包缓冲区”中的数据包，若已经超过了RTO，还没有收到这个包的ACK，则认为发生丢包。

暂定RTO计算方式为：RTO = smoothed\_rtt + max(4\*rttvar, 1ms) + max\_ack\_delay

备注：smoothed\_rtt、rttvar探测计算方法需将多路径调度、高可靠增强的影响考虑进去。

* NACK机制：若收到NACK，则认为发生丢包。

（3）重传机制：

* 当通过丢包检测判定数据包丢失时，重新发送该数据包，并将重传数据包设置成高优先级。

备注：

1）后续优化方向为优化由于数据包未确认带来的发送窗口滑动速率减慢问题

2）ACK和NACK联合使用机制

### SEASP报文格式

当公共首部Public Header 的Type字段的高位取值为011时，表示是SEASP协议相关报文，使用Type字段的低5位标识SEASP报文类型，其中：

* Type为0x60（011 00000）时，报文类型：SEASP数据报文（SP\_DAT）
* Type为0x61（011 00001）时，报文类型：选择性确认报文（SP\_SACK）
* Type为0x62（011 00010）时，报文类型：否定性确认报文（SP\_NACK）
* Type为0x63（011 00011）时，报文类型：协商报文（SP\_NEO）
* Type为0x64（011 00100）时，报文类型：连接关闭报文（SP\_Connection\_CLOSE）

#### SEASP数据报文（SP\_DAT）

数据报文（SP\_DAT）用于采用字节流模式发送数据包，可使用IDP的即刻重寻址相关机制，格式如下：



图 23 SP\_DAT报文格式

* **Flags**：8bits,标志位，如下所示，左边为高位，右边为低位。



|  |  |
| --- | --- |
| **位数** | **含义** |
| bit7, bit6 | 标识Preference的长度，未来可用于Preference长度扩展，其中：  00：8bytes（默认长度） |
| bit5 | 用于标识是否存在NeT\_defined Fields字段  0：不存在；1：存在 |
| bit4~bit0 | 预留，现阶段置0，未来可用于扩展可选字段 |

* **Preference：**Flags的(bit7,bit6)=(0,0)时，长度为8bytes，未来可通过设置Flags，扩展Preference长度；字节流的传输偏好，用于标识对传输、算力等需求、资源选择意向、使用的增强机制、相关参数等，用于指导字节流在传输过程中的网内处理操作。



图 24 SP\_DAT报文中Preference字段格式

* **传输优先级（Transport Priority, TP）:** 8bits，用于标识应用对网络提出的传输优先级需求，可在应用识别后根据应用的类型填写。网络服务商可以将优先级需求映射为可满足上述需求的一个/组业务逻辑拓扑（业务标识）、及每个拓扑下对应路由策略和队列转发优先级（优先级标识）。

备注：由端节点（SEANet协议起点）填写，网络中间节点可以查看、不能修改。

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

* **网络增强传输标志（Network Enhanced Transport Flag, NeT Flag）：**8bits，用于标识当前生效的网络传输增强机制，每个bit标识一种增强机制，支持多个bit同时置1情况。NeT Flag字段表示成如下形式：

备注：端节点（SEANet协议起点）填写，网络中间节点可以查看、不能修改。



|  |  |  |
| --- | --- | --- |
| **位数** | **值** | **含义** |
| bit7 (RFlag) | 1 | 高可靠增强传输机制 |
| bit6~bit0 | 预留 | 用于冗余传输等 |

示例：当只有高可靠增强传输一种机制生效时，NeT Flag=10000000=0x80。

* **网络增强传输参数（NeT Para）：**16bits

备注：网络中间节点可以查看、修改此字段。



**NeT Para 1（RPara）**：4bits，携带高可靠增强传输参数；

**NeT Para 2~8**：待定义。

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

* **预留：**24bits，可用于支持端网协同拥塞控制、算力服务等偏好设置，现阶段置0。
* **网络增强传输定义字段（NeT\_defined Fields）:** 可选字段，变长，用于携带网络增强传输所需要的相关字段，不同机制生效时，携带字段的长度和含义不同。当Flags字段的bit5=1时，存在该字段；每个**NeT Flag**取值对应一种增强传输机制的组合，组合情况决定**NeT\_defined Fields**字段的长度和含义。具体取值和分配情况见**附录9.3**所示。
* **Offset**：变长整数编码（见附录9.1），指明字节流中，数据段的字节偏移量。
* **Length**：变长整数编码（见附录9.1），指明字节流中，数据段的长度。
* **Payload**：载荷，用于承载字节流中要传送的字节，需要根据MTU的取值确定Payload中允许承载字节的长度范围。

备注：假定MTU=1500B，要求payload长度小于：1500B-26B(MAC头)-40B(IPv6头)-132B(IDP头)-10B(公共头)-47B(SP\_DAT头)=1245B。

#### 选择性确认报文（SP\_SACK）

选择性确认报文（SP\_SACK）用于端侧可靠传输中发送端和接收端之间进行数据包确认；SP\_SACK报文为SEASP消息报文，不使用网络增强传输和即刻重寻址相关机制。格式如下：



图 25 SP\_SACK报文格式

* **SFlags**：4bits,标志位，高2位用于标识最大确认号的长度，其中，00：长度为1bytes；01：长度为2bytes；10：长度为4bytes；11：长度为6bytes。低2位预留，置零。
* **ACK范围计数**：4bits，表示携带ACK范围字段的个数，最多支持携带15个ACK范围。
* **最大确认号**：变长，长度由Flags字段决定，表示接收端已经确认的最大数据包序号PN；等于接收端生成ACK时已收到的最大数据包序号。
* **第一ACK范围**：2bytes，最大确认包号之前收到的连续数据包的个数。
* **ACK范围**：2bytes，它包含了在交替被ack的包的间隙（GAP）和长度（Range）。
* GAP：上一个ACK范围的最小数据包号前面，不需要被ack的连续数据包号的数量
* Range：该范围内需要ack的连续数据包号的数量

示例1：接收端收到包序号分别为：{1~3}, {8~10}, {13~15}, {17~20}；SACK如下

最大确认号：20

第一ACK范围：4

第二ACK范围GAP：1；Range：3

第三ACK范围GAP：2；Range：3

第四ACK范围GAP：4；Range：3

示例2：发生序号循环使用时，接收端收到包序号分别为：{232-8~232-1}, {3~5}, {7~9}；SACK如下

最大确认号：9

第一ACK范围：3

第二ACK范围GAP：1；Range：3

第三ACK范围GAP：2；Range：8

#### 否定性确认报文（SP\_NACK）

否定性确认报文（SP\_NACK）用于接收方通知发送方没有收到某个数据包，用于端侧可靠传输机制中的无数据包确认；SP\_SACK报文为SEASP消息报文，不使用网络增强传输和即刻重寻址相关机制，格式如下：



图 26 SP\_NACK报文格式

* **SFlags**：4bits,标志位，高2位用于标识最大未确认号的长度，其中，00：长度为1bytes；01：长度为2bytes；10：长度为4bytes；11：长度为6bytes。低2位预留，置零。
* **NACK范围计数**：4bits，表示携带NACK范围字段个数，最多支持携带15个NACK范围。
* **最大未确认号（NPN）**：变长，长度由Flags字段决定，表示接收端未被确认的数据序号的最大值NPN。
* **第一NACK范围**：2bytes，最大未确认包号之前未被确认的连续数据包的个数
* **NACK范围**：2bytes，它包含了在交替被nack的包的间隙（GAP）和长度（Range）。
* GAP：上一个NACK范围的最小数据包号前面，不需要被nack连续数据包号的数量
* Range：该范围内需要nack的连续数据包号的数量

#### 协商报文（SP\_NEO）

协商报文（SP\_NEO）用于发送方、接收方和网络之间进行传输参数协商。包括：协商请求、协商回复和协商确认报文，通过SFlag字段来区分；SP\_NEO报文为SEASP消息报文，不使用网络增强传输机制和即刻重寻址相关机制。格式如下：



图 27 SP\_NEO报文格式

* **SFlags：**8bits，高3位用于标识协商报文类型，其中：000，协商请求报文ClientHello；001，协商回复报文ServerHello；010，协商确认报文ClientFinish；低5位预留，现阶段置零。
* **协商确认号：**8bits，用于同一连接中存在多次协商请求情况下，协商请求、协商回复和协商确认报文之间的相互确认。
* **传输参数个数**：8bits，指出报文中携带的传输参数的个数。
* **参数**：变长，采用TLV编码形式。

Tag：8bits，标识参数类型

Length：8bits，标识参数长度，单位是bytes

Value：参数取值，长度由Length决定。

|  |  |  |  |
| --- | --- | --- | --- |
| 参数名称 | Tag | Length | Value |
| 发送速率  Sending-Rate, SR | 0x1 | 6 | 取值范围是：0~248-1，单位是bps  最多支持256Tbps的速率 |
| 接收速率  Receiving-Rate, RR | 0x2 | 6 | 取值范围是：0~248-1，单位是bps  最多支持256Tbps的速率 |
| 最大报文段长度  MSS | 0x3 | 2 | 取值范围是：0~216-1，单位是Bytes  实际中MSSmax=1500-40(IP)-132(IDP)-10(PHeader)-45 (SEASP)=1273Bytes |
| 窗口大小  Window-SIZE | 0x4 | 4 | 取值范围是：0~232-1，单位是Bytes  最多支持4GB的缓存 |

#### 连接关闭报文（SP\_Connection\_CLOSE）

连接关闭报文（SP\_Connection\_CLOSE）用于通知对端当前连接正在被关闭；SP\_Connection\_CLOSE报文为SEASP消息报文，不使用网络增强传输和即刻重寻址相关机制，格式如下：



图 28 SP\_Connection\_CLOSE报文格式

* **SFlag：**8bits，高3位用于标识连接关闭报文类型，其中：000，连接关闭报文CLOSE；001，连接即将关闭通知报文GOAWAY；010，连接重置报文RST；低5位预留，现阶段置零。
* **RP Length**：，变长整数，关闭连接的原因短语长度。
* **Reason Phrase**：关闭连接的原因，是一个UTF-8编码的字符串。

|  |  |
| --- | --- |
| **Reason Phrase值** | **含义** |
| Finish | 传输完成 |
| Error | 传输异常中断 |

### SEASP传输流程

SEASP连接建立和关闭流程如下：



图 29 SEASP连接建立和关闭

SEASP数据包传输过程中，可以选择启用高可靠增强传输机制，降低传输丢包率。SEASP启用高可靠机制和不启用高可靠机制的传输流程如下图所示。



图 30 SEASP传输流程（启用高可靠增强传输机制）



图 31 SEASP传输流程（不启用高可靠增强传输机制）

# 附录

### 变长整数编码

SEASP对非负整数值使用变长编码方式，这种编码确保较小的整数可以使用更少的字节来编码。SEASP变长整数编码使用第一个字节的最高两位（2MSB）标识整数的长度，当2MSB为n时，表示编码整数的长度为2n字节，整数值在剩余的位上编码。因此，整数可以编码为1,2,4,8字节，整数值所占位数分别不超过6bits, 14bits, 30bits, 62 bits。

|  |  |  |  |
| --- | --- | --- | --- |
| 2MSB | 长度 | 可用位数 | 取值范围 |
| 00 | 1 | 6 | 0-63 |
| 01 | 2 | 14 | 0-16383 |
| 10 | 4 | 30 | 0-1073741823 |
| 11 | 8 | 62 | 0-4611686018427387903 |

### IDP首部Flag分配和使用情况

IDP首部Flag字段的分配和使用情况如下：

|  |  |  |  |
| --- | --- | --- | --- |
| Flag | 应用组合 | 可选字段使用情况 | 详细用法 |
| 0x0 | 默认 | 无 |  |
| 0x1 | 多路径（流） | Extended Address  APP-defined Field A | 参见  《SEANet多路径传输设计方案》 |
| 0x2 | 缓存 | Extended Address  APP-defined Field A | 参见  《缓存技术方案v0.2【审定】》 |
| 0x3~0xF | 预留 |  |  |

备注：现阶段实现时Reserved字段的bit3置1，表示使用带内遥测（INT），具体如下：

|  |  |  |  |
| --- | --- | --- | --- |
| Reserved | 应用组合 | 可选字段使用情况 | 详细用法 |
| 1000 | INT | APP-defined Field B  APP-defined Field C  APP-defined Field D | 具体定义参见  《SEANet带内网络遥测方案  （V0.31）》 |

### NeT\_defined Fields字段分配和使用情况

|  |  |  |  |
| --- | --- | --- | --- |
| **NeT Flag** | **增强机制组合** | **字段长度** | **NeT\_defined Fields** |
| 00000000 | 无 | 0 | 无 |
| 10000000 | 高可靠增强传输 | 20bytes | * **高可靠传输流标识（RFID）**：2bytes，用于携带高可靠增强增强传输的流标识，现阶段由发送方IP和接收方IP哈希得到。 * **高可靠传输发送方地址（RSIP）：**16bytes，用于携带高可靠增强传输的发送方网络节点的IP。 * **高可靠增强传输包序号（RPN）：**4bytes，用于携带高可靠增强传输机制数据包的序号，取值范围是：0~232-1。   备注：网络节点填写、查看和修改。 |
| - | - | - | - |

### 数据报文设计框架

数据报文采用统一的格式定义，如下所示：





* Flags：标志位，用于标识字段长度和是否存在可选字段
* Preference：偏好字段，中间节点查看、修改
* NeT\_defined Fields：网络增强传输定义字段（可选字段），中间节点查看、修改
* Reliable Related Fields：辅助可靠传输相关字段，若为非可靠传输不存在此字段
* Optional Fields：可选字段

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | SEADP  (Public Header. Type=001 00000) | SEAUP  (Public Header. Type=010 00000) | SEASP  (Public Header. Type=011 00000) |
| Flags  （1byte） | bit7~bit6 | Preference的长度，未来可用于Preference长度扩展，00：长度为8bytes（默认长度） | | |
| bit5 | 是否存在NeT\_defined Fields，0：不存在；1：存在 | | |
| bit4 | 是否存在Chunk size | 预留 | 预留 |
| bit3 | 是否存在Chunk checksum |
| Bit2~Bit0 | 预留 |
| Preference  （8bytes） | Byte7 | 传输优先级（TP），可映射为满足上述需求的一个/组业务逻辑拓扑（业务标识）、及每个拓扑下路由策略和队列优先级（优先级标识） | | |
| Byte6 | 网络增强传输标志（NeT Flag），用于标识当前生效的网络传输增强机制 | | |
| Byte5~4 | 网络增强传输参数（NeT Para），用于携带高可靠增强传输相关参数 | | |
| Byte3 | 存储意向（SI） | 传输意向（TI） | 传输意向（TI） |
| Byte2~0 | 预留，用于支持存储、传输、算力服务等偏好设置，现阶段置0 | | |
| NeT\_defined Fields  （可选，22bytes） | | 网络增强传输定义字段，可选字段，变长，现阶段定义如下：   * 高可靠传输流标识（RFID）：4bytes，用于携带高可靠增强传输的流标识，现阶段由发送方IP和接收方IP哈希得到【待讨论】 * 高可靠传输发送方地址（RSIP）：16bytes，用于携带高可靠增强传输的发送方网络节点的IP。 * 高可靠增强传输包序号（RPN）：4bytes，用于携带高可靠增强传输机制数据包的序号，取值范围是：0~232-1 | | |
| Reliable Related Fields | | Offset（4bytes）  Length（4bytes） | 无 | Offset（变长，1/2/4/8bytes）  Length（变长，1/2/4/8bytes） |
| Optional Fields | | Chunk Size（4bytes）  Chunk Checksum（4bytes） | 无 | 无 |
| **首部总长度** | | 27bytes/49bytes/57bytes | 19bytes/41bytes | 21bytes/23bytes/27bytes/35bytes  43bytes/45bytes/49bytes/57bytes |

传输层偏好定义



SEASP/SEAUP使用**传输意向（TI）**，具体定义如下：

|  |  |  |
| --- | --- | --- |
| **传输意向** | **含义** | **取值** |
| bit7-bit5（3bits） | 位置  Location | 标识传输过程中选择中间节点的位置偏好  0：默认；1：发端附近；2：收端附近 |
| bit4-bit2（3bits） | 范围  Range | 标识传输过程中选择中间节点集的范围偏好  0：全局解析域；1：C1解析域；2：C2解析域；3：C3解析域 |
| bit1-bit0（2bits） | 预留 | 现阶段置零 |

SEADP使用**存储意向（SI）**，具体定义如下：

|  |  |  |
| --- | --- | --- |
| **位数** | **含义** | **取值** |
| bit7-bit4（4bits） | 存储可靠性  Reliability | 用于标识数据存储的可靠性需求  0：不存储；1：冷门缓存；2：热门缓存；3：一般存储；4：可靠存储；5：高可靠存储；6：读写一致存储 |
| bit3-bit2（2bits） | 存储位置  Location | 用于标识数据存储的位置需求  0：默认；1：数据源附近；2：网络中心；3：网络边缘 |
| bit1-bit0（2bits） | 预留 | 现阶段置零 |

1. [] <https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml> [↑](#footnote-ref-1)