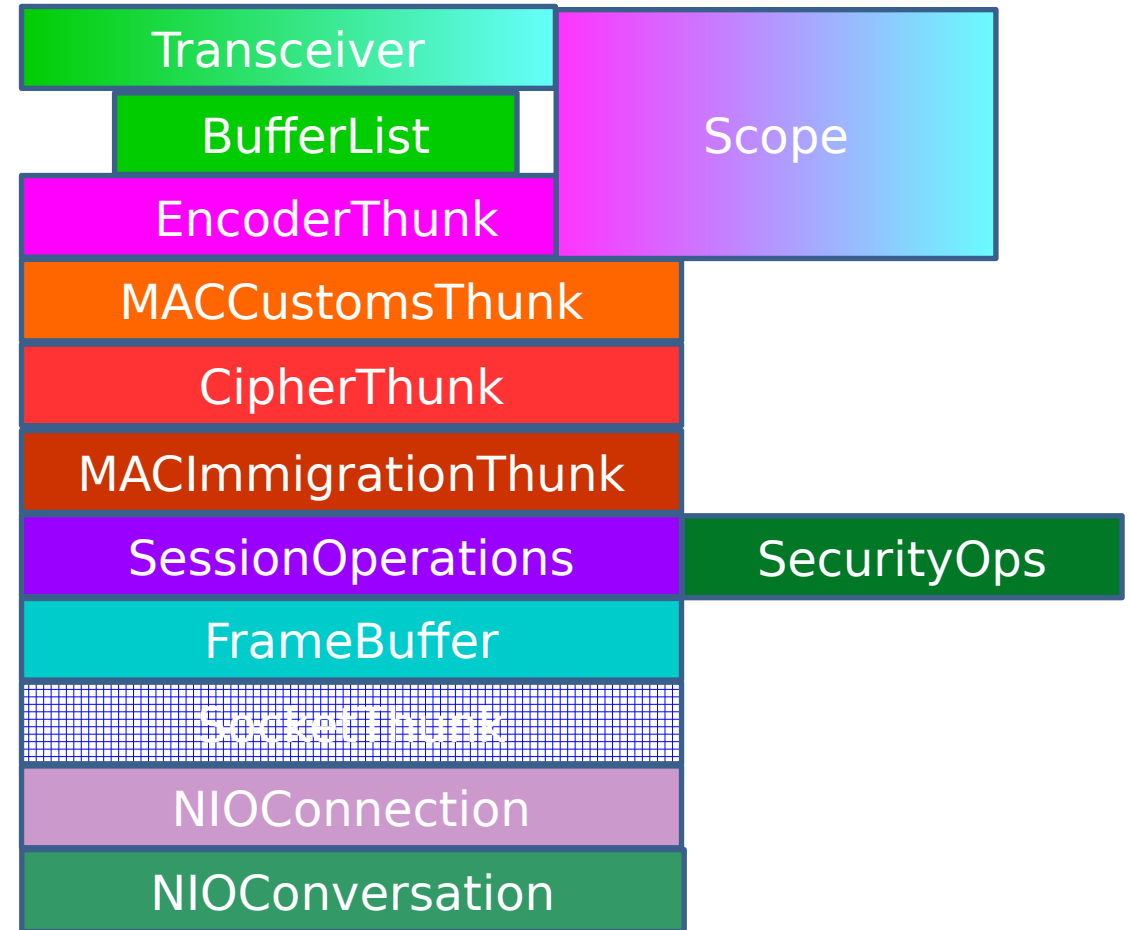
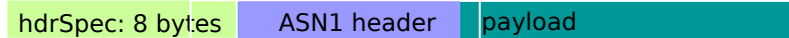


ParrotTalk Frame Design

version 3.5

Homeless Council
Callisto House Limited
Callisto Enterprises

Frame



ParrotTalk Frame Design

- Frames are used in message pipeline, consisting of
 - an 8 byte message specification,
 - a msgType ASN1Choice Encoded header
 - a possible data payload.
- Frames are exchanged between layers, up & down the stack.
- Each protocol frame transforms session state through the SessionOperations layer.
- Each data layer transforms each frame by established session protocol.
- As payload is transformed, header is transformed and re-encoded ASN1Der.
- MsgSpec knows header & frame encoding specification.
- Natural nested wrapping of data msgs, where an inner frame's messageSize removes down stack padding.
- Protocol stack is established during session rendezvous with these data wrapping specifications:
 - Encoded – Primary payload
 - Encrypted – AES-256/CBC/PKCS7Padding with 128-bit blockSize & IV and a 256-bit key
 - MAC – 160-bit hmac hash

ParrotTalk Protocol

- 3-way rendezvous handshake protocol with Protocol pre-exchange
- Protocol pre-exchange (ProtocolOffered/ProtocolAccepted)
- VatId/Domain agreement (IWant/IAM)
- 2048-bit RSA PublicKey exchange (Iam/GiveInfo)
- CryptoProtocol negotiation (ReplyInfo/Go/GoToo)
- DataEncoder negotiation (ReplyInfo/Go/GoToo)
- 2048-bit prime/secret Diffie-Hellman parameter exchange (Go/GoToo)
- Prior protocol traffic 2048-bit RSA Signature authentication (Go/GoToo)
- DoubleBakedKeyExchangeProtocol: low route; high session.
- QuadScopeInfrastructure 4,5,6, , ,9:
 - 4: Goose - routing
 - 5: Raven - session
 - 6: Parrot - presentation
 - 7: Pidgeon - App DSL
 - 8: Vulture - Container DSL
 - 9: Eagle - meta
- Diffie-Hellman prime is the 2048-bit <https://tools.ietf.org/html/rfc3526#page-3>
- Diffie-Hellman generator is 2 from the same source

ParrotTalk Protocol Headers

- Layer 5: Raven – session
 - <5> Encoded
 - <6> Encrypted
 - <7> MAC
 - <8> IWant
 - <9> IAm
 - <10> GiveInfo
 - <11> ReplyInfo
 - <12> GO
 - <13> GOToo
 - <14> DuplicateConn
 - <15> NotMe
- Layer 4: Goose – routing
 - <1> ProtocolOffered
 - <3> ProtocolAccepted
- Layer 6: Parrot – presentation
 - <16> DeliverOnly
 - <17> Deliver
 - <18> GCAnswer
 - <19> GCExport
 - <20> Shutdown

Generic Structure

8-byte MessageSpecification

- messageSpecification: 8 byte frame header, bit encoded
 - 1st word, 4 bytes
 - 4 bits : tags
 - 10 bits : multicast
 - 10 bits : hash
 - 1 bits : frameVersion = 1
 - 2 bits : priority
 - 5 bits : headerType {headerTypes unspecified: 0, 2, 4, 21-31}
 - 2nd word, 4 bytes
 - 32 bits : messageSize <payload bytes = (messageSize - headerSize - 8 bytes)>
- messageHeader: headerType::size byte ASN1.Der encoded
- payload: (Z bytes)

ProtocolOffered Message

- messageSpecification: 8 bytes frame header, bit encoded
 - headerType = <1>
- ProtocolOffered Header: ASN1.Der encoded explicitTag: 1
 - offered - ASN1UTF8StringType
 - preferred - ASN1UTF8StringType
- payload - zero bytes

ProtocolAccepted Message

- messageSpecification: 8 bytes frame header, bit encoded
 - headerType = <3>
- ProtocolAccepted Header: ASN1.Der encoded explicitTag: 3
 - accepted – ASN1UTF8StringType
- payload – zero bytes

Encoded Message

- messageSpecification: 8 bytes frame header, bit encoded
 - HeaderType = <5>
- Encoded Header: ASN1.Der encoded explicitTag: 5
- payload – data bytes

Encrypted Message

- messageSpecification: 8 bytes frame header, bit encoded
 - headerType = <6>
- Encrypted Header: ASN1.Der encoded explicitTag: 6
 - ivSequence - ASN1ByteArrayType
- payload – data bytes

MAC Message

- messageSpecification: 8 bytes frame header, bit encoded
 - headerType = <7>
- MAC Header: ASN1.Der encoded explicitTag: 7
 - MAC: ASN1ByteArrayType
- payload: Data bytes

IWant Message

- messageSpecification: 8 bytes frame header, bit encoded
 - headerType = <8>
- IWant Header: ASN1.Der encoded explicitTag: 8
 - vatID - ASN1UTF8StringType
 - domain - ASN1UTF8StringType
- payload - zero bytes

IAm Message

- messageSpecification: 8 bytes frame header, bit encoded
 - headerType = <9>
- IAm Header: ASN1.Der encoded explicitTag: 9
 - vatID – ASN1UTF8StringType
 - domain – ASN1UTF8StringType
 - publicKey – RSAPublicKey
- payload – zero bytes

GiveInfo Message

- messageSpecification: 8 bytes frame header, bit encoded
 - headerType = <10>
- GiveInfo Header: ASN1.Der encoded explicitTag: 10
 - vatID – ASN1UTF8StringType
 - domain – ASN1UTF8StringType
 - publicKey – RSAPublicKey
- payload – zero bytes

ReplyInfo Message

- messageSpecification: 8 bytes frame header, bit encoded
 - headerType = <11>
- ReplyInfo Header: ASN1.Der encoded explicitTag: 11
 - cryptoProtocols - ASN1SequenceOfType(ASN1UTF8StringType)
 - dataEncoders - ASN1SequenceOfType(ASN1UTF8StringType)
- payload – zero bytes

GO Message

- messageSpecification: 8 bytes frame header, bit encoded
 - headerType = <12>
- GO Header: ASN1.Der encoded explicitTag: 12
 - cryptoProtocol – ASN1UTF8StringType
 - dataEncoder – ASN1UTF8StringType
 - diffieHellmanParam – ASN1ByteArrayType
 - signature – ASN1ByteArrayType
- payload – zero bytes

GOToo Message

- messageSpecification: 8 bytes frame header, bit encoded
 - headerType = <13>
- GOToo Header: ASN1.Der encoded explicitTag: 13
 - cryptoProtocol – ASN1UTF8StringType
 - dataEncoder – ASN1UTF8StringType
 - diffieHellmanParam – ASN1ByteArrayType
 - signature – ASN1ByteArrayType
- payload – zero bytes

DuplicateConn Message

- messageSpecification: 8 bytes frame header, bit encoded
 - headerType = <14>
- DuplicateConn Header: ASN1.Der encoded explicitTag: 14
- payload – zero bytes

NotMe Message

- messageSpecification: 8 bytes frame header, bit encoded
 - headerType = <15>
- NotMe Header: ASN1.Der encoded explicitTag: 15
- payload – zero bytes

DeliverOnly Message

- messageSpecification: 8 bytes frame header, bit encoded
 - headerType = <16>
- DeliverOnly Header: ASN1.Der encoded explicitTag: 16
 - receiver – IncomingType
 - selector – ASN1UTF8StringType
 - arguments – ASN1SequenceType
- payload – zero bytes

Deliver Message

- messageSpecification: 8 bytes frame header, bit encoded
 - headerType = <17>
- Deliver Header: ASN1.Der encoded explicitTag: 17
 - receiver – IncomingType
 - selector – ASN1UTF8StringType
 - arguments – ASN1SequenceType
 - answer – ImportType
 - redirector – IncomingType
- payload – zero bytes

GCAnswer Message

- messageSpecification: 8 bytes frame header, bit encoded
 - headerType = <18>
- GCAnswer Header: ASN1.Der encoded explicitTag: 18
 - wirePosition – AnswerType
- payload – zero bytes

GCEXport Message

- messageSpecification: 8 bytes frame header, bit encoded
 - headerType = <19>
- GCEXport Header: ASN1.Der encoded explicitTag: 19
 - wirePosition – AnswerType
 - wireCount – ASN1IntegerType
- payload – zero bytes

Shutdown Message

- messageSpecification: 8 bytes frame header, bit encoded
 - headerType = <20>
- Shutdown Header: ASN1.Der encoded explicitTag: 20
- payload – zero bytes