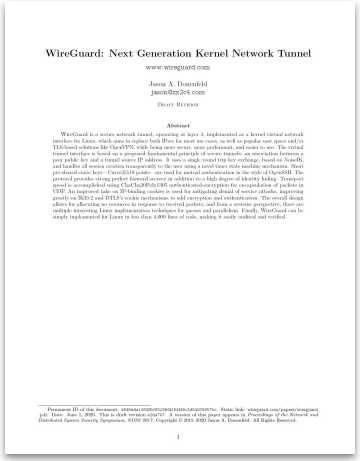
Architectural Overview
Kick-off Meeting
10/17/2024

Outline

- Wireguard Protocol
- Target Platform & Requirements
- HW/SW Partitioning
- HW Architecture
- SW Architecture
- Data Flow Example

Wireguard Protocol

- Stateless UDP-based Protocol + Timestamping
- Simple Two-Step Handshake
  - Curve25519 ECDH - Exchange Static Public Keys
  - BLAKE2s MAC-HMAC - DoS Mitigation
- ChaCha20-Poly1305 Encryption
- Cryptokey Routing



WireGuard: Next Generation Kernel Network Tunnel

www.wireguard.com

Jason A. Donenfeld
Jason@zx2c4.com

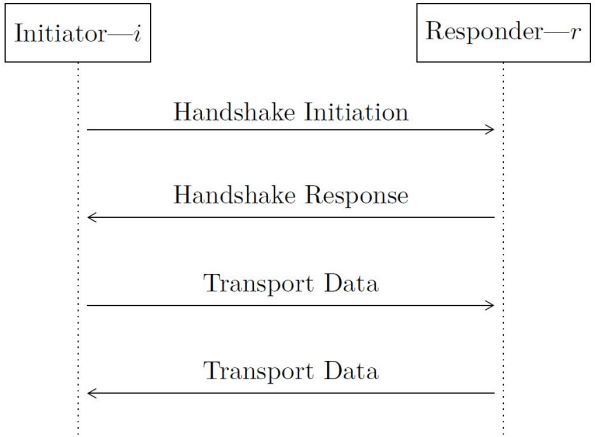
Draft Revision

Abstract

Jason Donenfeld, "WireGuard: Next Generation Kernel Network Tunnel," in *Proceedings of the Network and Distributed System Security Symposium*, NDSS 2017.

type := 0x1 (1 byte)	reserved := 0^3 (3 bytes)
sender := I_i (4 bytes)	
ephemeral (32 bytes)	
static ($\widehat{32}$ bytes)	
timestamp ($\widehat{12}$ bytes)	
mac1 (16 bytes)	mac2 (16 bytes)

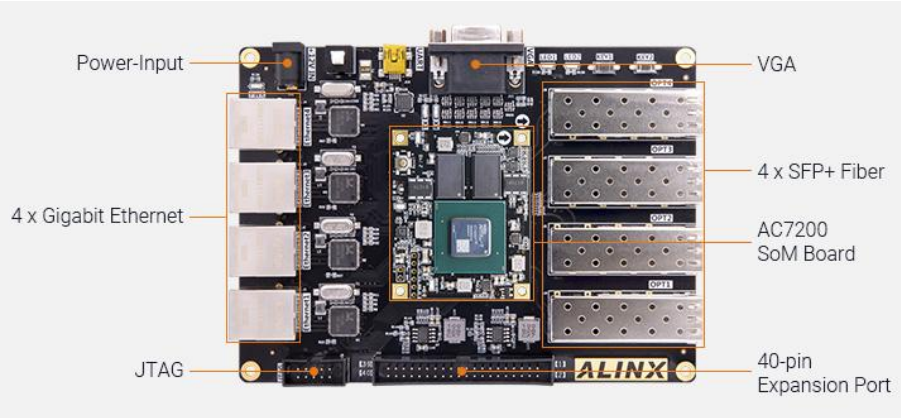
type := 0x4 (1 byte)	reserved := 0^3 (3 bytes)
receiver := $I_{m'}$ (4 bytes)	
counter (8 bytes)	
packet ($\widehat{\|P\|}$ bytes)	



type := 0x2 (1 byte)	reserved := 0^3 (3 bytes)
sender := I_r (4 bytes)	receiver := I_i (4 bytes)
ephemeral (32 bytes)	
empty ($\widehat{0}$ bytes)	
mac1 (16 bytes)	mac2 (16 bytes)

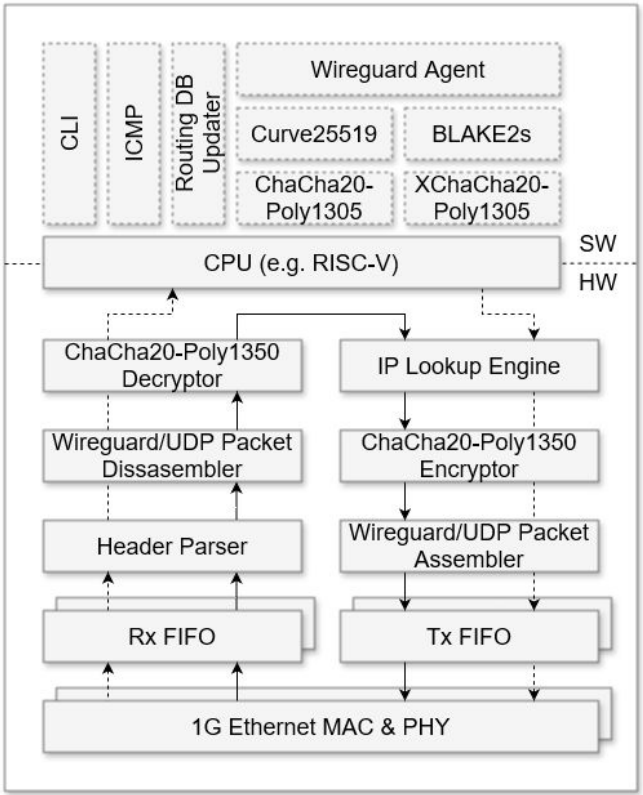
Target Platform & Requirements

- ALINX AMD Artix 7 XC7A200T FPGA Development Board
- 4 x Gigabit Ethernet (Realtek RTL8211EG PHY)
- 4 Gbps Encryption/Decryption

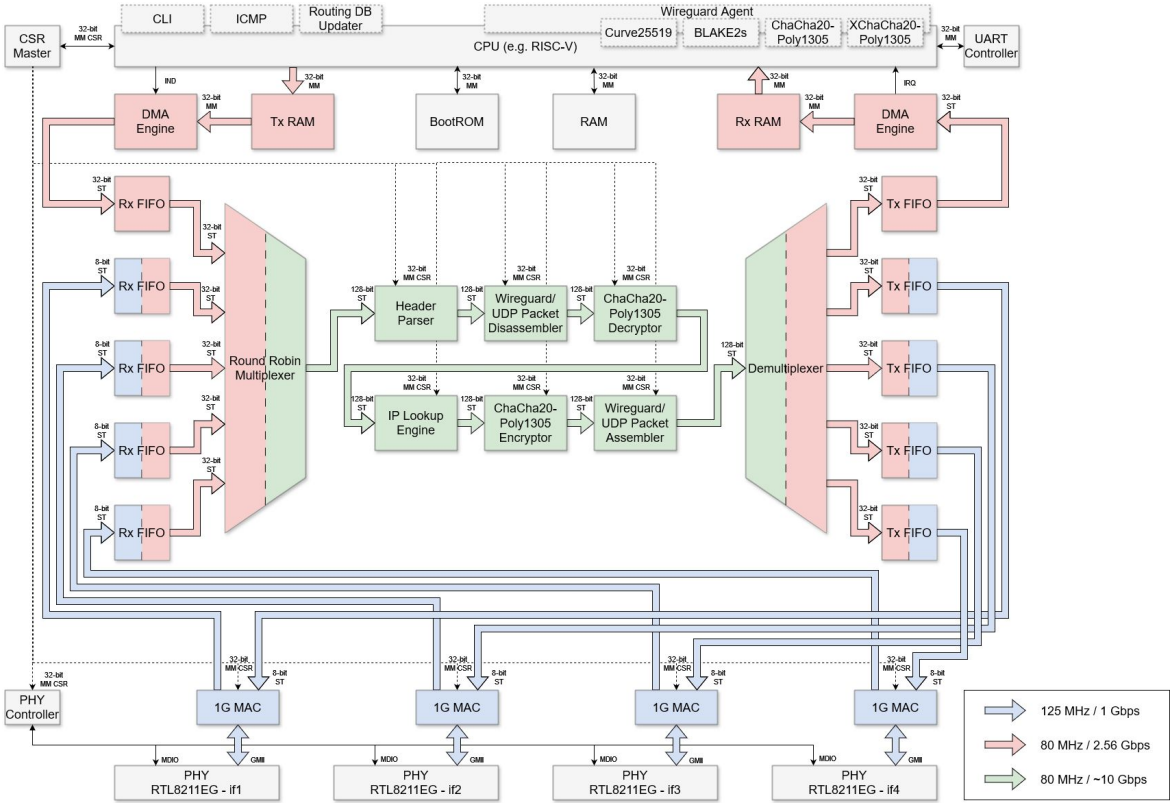


	Part Number	XC7A200T
Logic Resources	Logic Cells	215,360
	Slices	33,650
	CLB Flip-Flops	269,200
Memory Resources	Maximum Distributed RAM (Kb)	2,888
	Block RAM/FIFO w/ ECC (36 Kb each)	365
	Total Block RAM (Kb)	13,140
Clock Resources	CMTs (1 MMCM + 1 PLL)	10
I/O Resources	Maximum Single-Ended I/O	500
	Maximum Differential I/O Pairs	240
Embedded Hard IP Resources	DSP Slices	740
	PCIe® Gen2[1]	1
	Analog Mixed Signal (AMS) / XADC	1
	Configuration AES / HMAC Blocks	1
	GTP Transceivers (6.6 Gb/s Max Rate)[2]	16

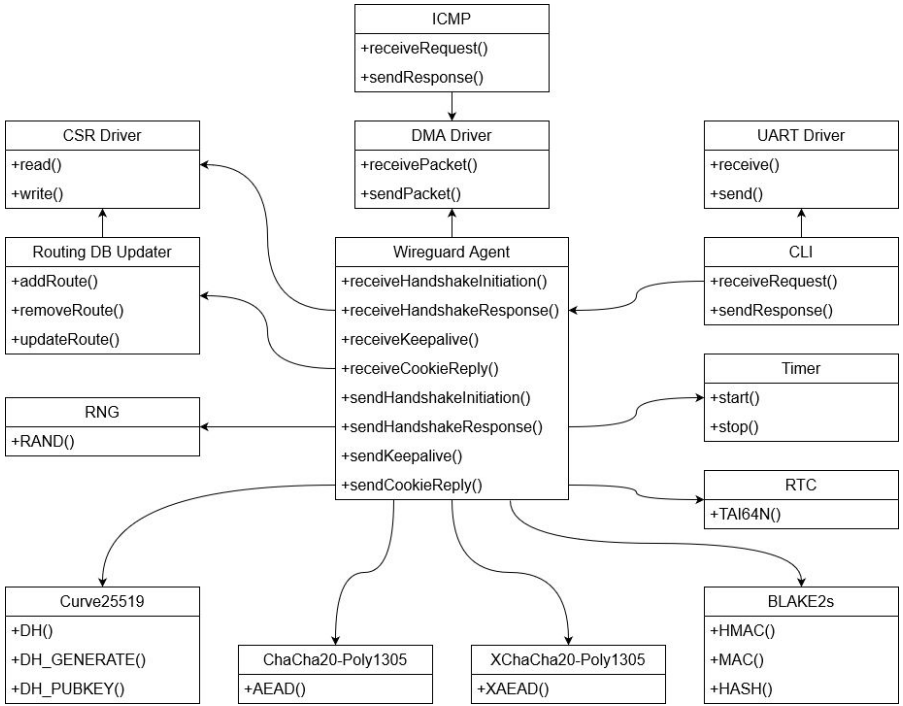
HW/SW Partitioning



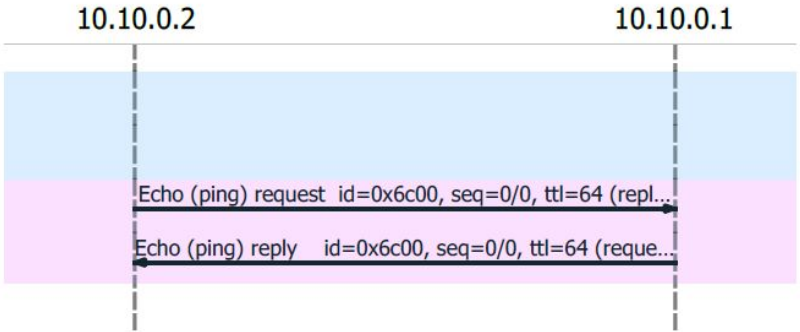
HW Architecture

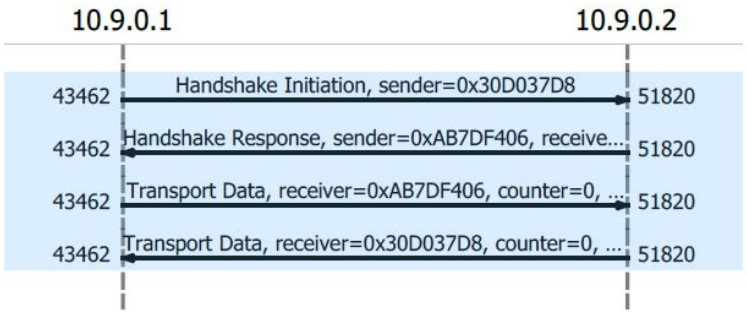


SW Architecture

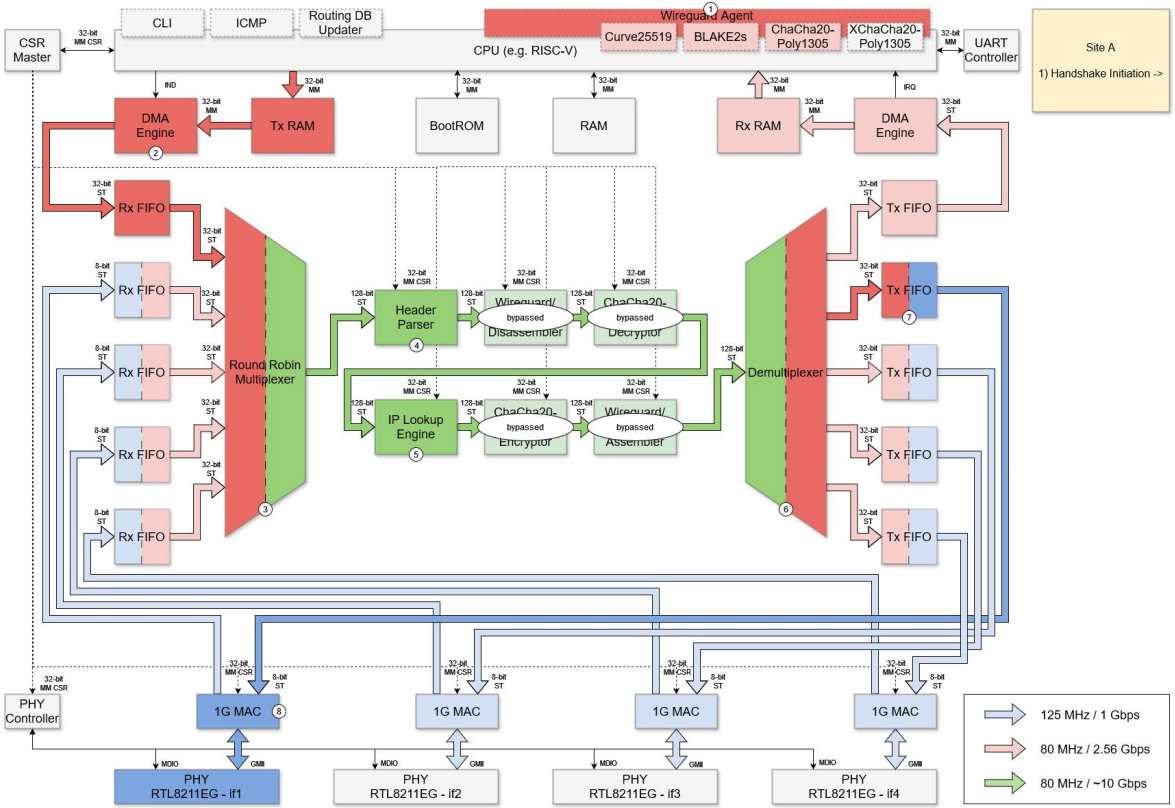


Data Flow Example





Data Flow Example (1 - 8)



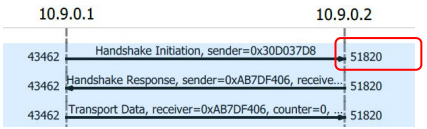

```
> Ethernet II, Src: 3a:36:e5:bf:5a:f8 (3a:36:e5:bf:5a:f8), Dst: a2:e6:34:94:b5:83
> Internet Protocol Version 4, Src: 10.9.0.1, Dst: 10.9.0.2
v User Datagram Protocol, Src Port: 43462, Dst Port: 51820
    Source Port: 43462
    Destination Port: 51820
    Length: 156
    Checksum: 0x14c2 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  > [Timestamps]
v WireGuard Protocol
    Type: Handshake Initiation (1)
    Reserved: 000000
    Sender: 0x30d037d8
  > Ephemeral: X87HyOXI4uP3mJ7vYMIo2CMp1gK2seK7nQaPic+dTUU=
    Encrypted Static
  > Static Public Key: Igge9KzRytKNwrgkzDE/8hrLu6Ly0OqVdvOPWhA5KR4=
    Encrypted Timestamp
  > Timestamp: Jul 20, 2018 22:38:51.356537872 UTC
    mac1: 533b01dd965e7ec76976e28f683d6712
  > [Receiver Static Public Key: YDCttCs9e1J52/g9vEnwJJa+2x6RqaayAYMpSVQfGEY=]
    mac2: 00000000000000000000000000000000
    [Stream index: 0]
    [Response in Frame: 2]
```

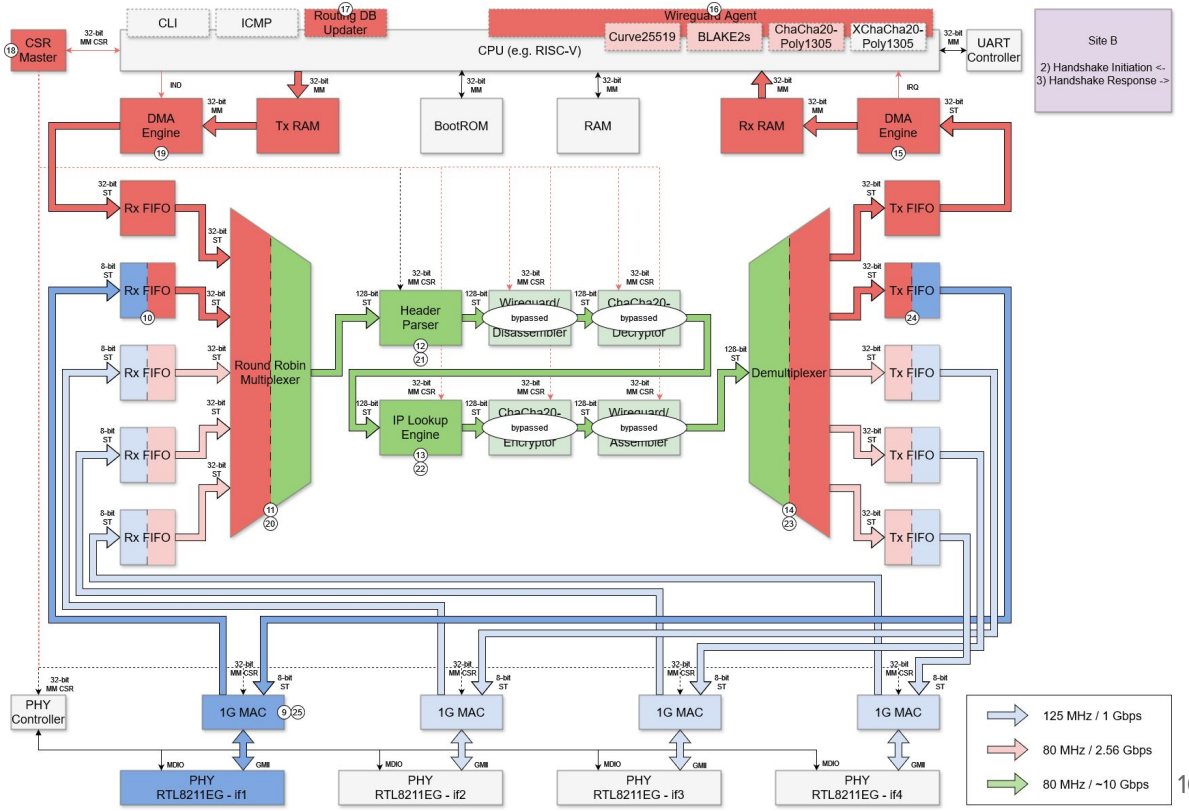
```
0000  a2 e6 34 94 b5 83 3a 36  e5 bf 5a f8 08 00 45 88   ··4···:6 ··Z···E·
0010  00 b0 02 4b 00 00 40 11  63 56 0a 09 00 01 0a 09   ···K··@· cV······
0020  00 02 a9 c6 ca 6c 00 9c  14 c2 01 00 00 00 d8 37   ·····l·· ·······7
0030  d0 30 5f ce c7 c8 e5 c8  e2 e3 f7 98 9e ef 60 c2   ·0_····· ······`·
0040  28 d8 23 29 d6 02 b6 b1  e2 bb 9d 06 8f 89 cf 9d   (·#)···· ········
0050  4d 45 32 78 0f 6d 27 26  4f 7b 98 70 1f dc 27 a4   ME2x·m'& O{·p··'·
0060  ec 00 ae b6 be cd be f2  33 2f 1b 40 84 ca db 93   ········ 3/·@····
0070  82 39 35 c0 12 ae 25 5e  7b 25 ef f1 39 40 c3 21   ·95···%^ {%··9@·!
0080  fa 6b d6 6a 2a 87 b0 61  db 14 30 17 3e 93 7f 56   ·k·j*··a ··0·>··V
0090  93 49 de 28 56 dc 5f 26  16 76 3e ee af c0 53 3b   ·I·(V·_& ·v>···S;
00a0  01 dd 96 5e 7e c7 69 76  e2 8f 68 3d 67 12 00 00   ···^~·iv ··h=g···
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
```

Data Flow Example (9 - 18)

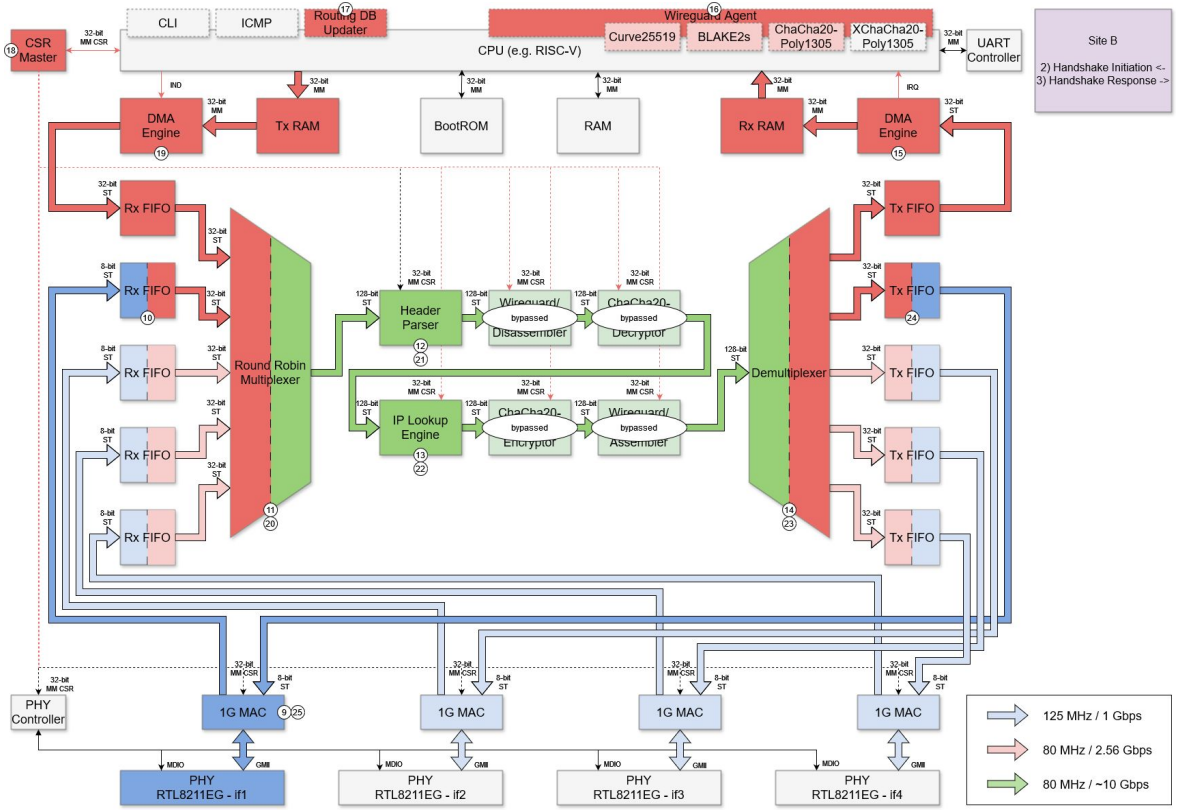
```
> Ethernet II, Src: 3a:36:e5:bf:5a:f8 (3a:36:e5:bf:5a:f8), Dst: a2:e6:34:94:b5:83
> Internet Protocol Version 4, Src: 10.9.0.1, Dst: 10.9.0.2
v User Datagram Protocol, Src Port: 43462, Dst Port: 51820
    Source Port: 43462
    Destination Port: 51820
    Length: 156
    Checksum: 0x14c2 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  > [Timestamps]
v WireGuard Protocol
    Type: Handshake Initiation (1)
    Reserved: 000000
    Sender: 0x30d037d8
  > Ephemeral: X87HyOXI4uP3mJ7vYMIo2CMp1gK2seK7nQaPic+dTUU=
    Encrypted Static
  > Static Public Key: Igge9KzRytKNwrgkzDE/8hrLu6Ly0OqVdvOPWhA5KR4=
    Encrypted Timestamp
  > Timestamp: Jul 20, 2018 22:38:51.356537872 UTC
    mac1: 533b01dd965e7ec76976e28f683d6712
  > [Receiver Static Public Key: YDCttCs9e1J52/g9vEnwJJa+2x6RqaayAYMpSVQfGEY=]
    mac2: 00000000000000000000000000000000
    [Stream index: 0]
    [Response in Frame: 2]
```

```
0000  a2 e6 34 94 b5 83 3a 36  e5 bf 5a f8 08 00 45 88   ··4···:6 ··Z···E·
0010  00 b0 02 4b 00 00 40 11  63 56 0a 09 00 01 0a 09   ···K··@· cV······
0020  00 02 a9 c6 ca 6c 00 9c  14 c2 01 00 00 00 d8 37   ·····l·· ·······7
0030  d0 30 5f ce c7 c8 e5 c8  e2 e3 f7 98 9e ef 60 c2   ·0_····· ····`·
0040  28 d8 23 29 d6 02 b6 b1  e2 bb 9d 06 8f 89 cf 9d   (·#)···· ········
0050  4d 45 32 78 0f 6d 27 26  4f 7b 98 70 1f dc 27 a4   ME2x·m'& O{·p··'·
0060  ec 00 ae b6 be cd be f2  33 2f 1b 40 84 ca db 93   ········ 3/·@····
0070  82 39 35 c0 12 ae 25 5e  7b 25 ef f1 39 40 c3 21   ·95···%^ {%··9@·!
0080  fa 6b d6 6a 2a 87 b0 61  db 14 30 17 3e 93 7f 56   ·k·j*··a ··0·>··V
0090  93 49 de 28 56 dc 5f 26  16 76 3e ee af c0 53 3b   ·I·(V·_& ·v>···S;
00a0  01 dd 96 5e 7e c7 69 76  e2 8f 68 3d 67 12 00 00   ···^~·iv ··h=g···
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00        ········ ······
```



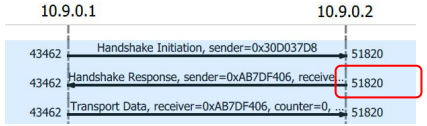


Data Flow Example (19 - 25)




```
> Ethernet II, Src: a2:e6:34:94:b5:83 (a2:e6:34:94:b5:83), Dst: 3a:36:e5:bf:5a:f8
> Internet Protocol Version 4, Src: 10.9.0.2, Dst: 10.9.0.1
v User Datagram Protocol, Src Port: 51820, Dst Port: 43462
    Source Port: 51820
    Destination Port: 43462
    Length: 100
    Checksum: 0x148a [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  > [Timestamps]
v WireGuard Protocol
    Type: Handshake Response (2)
    Reserved: 000000
    Sender: 0xab7df406
    Receiver: 0x30d037d8
  > Ephemeral: sY1VUL1AQqN6RoI6wI2x7GaDm8DKLWS8Fc2AIytmIy8=
    Encrypted Empty
    [Handshake decryption successful: True]
    mac1: f272214c5260110dc4c61e32cdd85421
  > [Receiver Static Public Key: Igge9KzRytKNwrgkzDE/8hrLu6Ly0OqVdvOPWhA5KR4=]
    mac2: 00000000000000000000000000000000
    [Stream index: 0]
    [Response to Frame: 1]
```

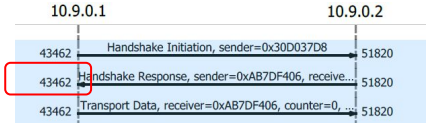
```
0000  3a 36 e5 bf 5a f8 a2 e6  34 94 b5 83 08 00 45 88   :6··Z··· 4·····E·
0010  00 78 2a 39 00 00 40 11  3b a0 0a 09 00 02 0a 09   ·x*9··@· ;·······
0020  00 01 ca 6c a9 c6 00 64  14 8a 02 00 00 00 06 f4   ···l···d ········
0030  7d ab d8 37 d0 30 b1 8d  55 50 bd 40 42 a3 7a 46   }··7·0·· UP·@B·zF
0040  82 3a c0 8d b1 ec 66 83  9b c0 ca 2d 64 bc 15 cd   ·:····f· ···-d···
0050  80 23 2b 66 23 2f ae c2  4a f8 91 8d e1 06 0f f5   ·#+f#/·· J·······
0060  c9 8e 86 5d 5f 35 f2 72  21 4c 52 60 11 0d c4 c6   ···]_5·r !LR`····
0070  1e 32 cd d8 54 21 00 00  00 00 00 00 00 00 00 00   ·2··T!·· ········
0080  00 00 00 00 00 00                                 ·····
```

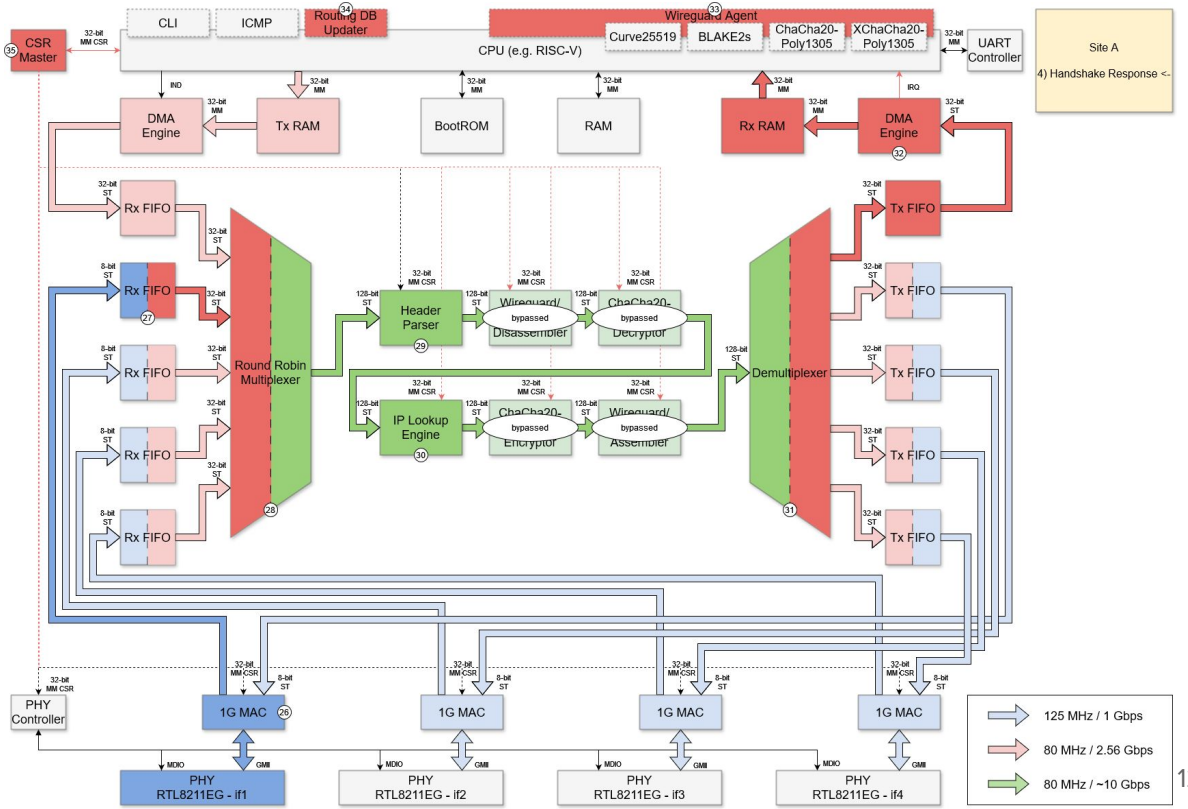


Data Flow Example (26 - 35)

```
> Ethernet II, Src: a2:e6:34:94:b5:83 (a2:e6:34:94:b5:83), Dst: 3a:36:e5:bf:5a:f8
> Internet Protocol Version 4, Src: 10.9.0.2, Dst: 10.9.0.1
v User Datagram Protocol, Src Port: 51820, Dst Port: 43462
    Source Port: 51820
    Destination Port: 43462
    Length: 100
    Checksum: 0x148a [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  > [Timestamps]
v WireGuard Protocol
    Type: Handshake Response (2)
    Reserved: 000000
    Sender: 0xab7df406
    Receiver: 0x30d037d8
  > Ephemeral: sY1VUL1AQqN6RoI6wI2x7GaDm8DKLWS8Fc2AIytmIy8=
    Encrypted Empty
    [Handshake decryption successful: True]
    mac1: f272214c5260110dc4c61e32cdd85421
  > [Receiver Static Public Key: Igge9KzRytKNwrgkzDE/8hrLu6Ly0OqVdvOPWhA5KR4=]
    mac2: 00000000000000000000000000000000
    [Stream index: 0]
    [Response to Frame: 1]
```

```
0000  3a 36 e5 bf 5a f8 a2 e6  34 94 b5 83 08 00 45 88   :6··Z··· 4·····E·
0010  00 78 2a 39 00 00 40 11  3b a0 0a 09 00 02 0a 09   ·x*9··@· ;·······
0020  00 01 ca 6c a9 c6 00 64  14 8a 02 00 00 00 06 f4   ···l···d ········
0030  7d ab d8 37 d0 30 b1 8d  55 50 bd 40 42 a3 7a 46   }··7·0·· UP·@B·zF
0040  82 3a c0 8d b1 ec 66 83  9b c0 ca 2d 64 bc 15 cd   ·:····f· ···-d···
0050  80 23 2b 66 23 2f ae c2  4a f8 91 8d e1 06 0f f5   ·#+f#/·· J·······
0060  c9 8e 86 5d 5f 35 f2 72  21 4c 52 60 11 0d c4 c6   ···]_5·r !LR`····
0070  1e 32 cd d8 54 21 00 00  00 00 00 00 00 00 00 00   ·2··T!·· ········
0080  00 00 00 00 00 00                                 ·····
```

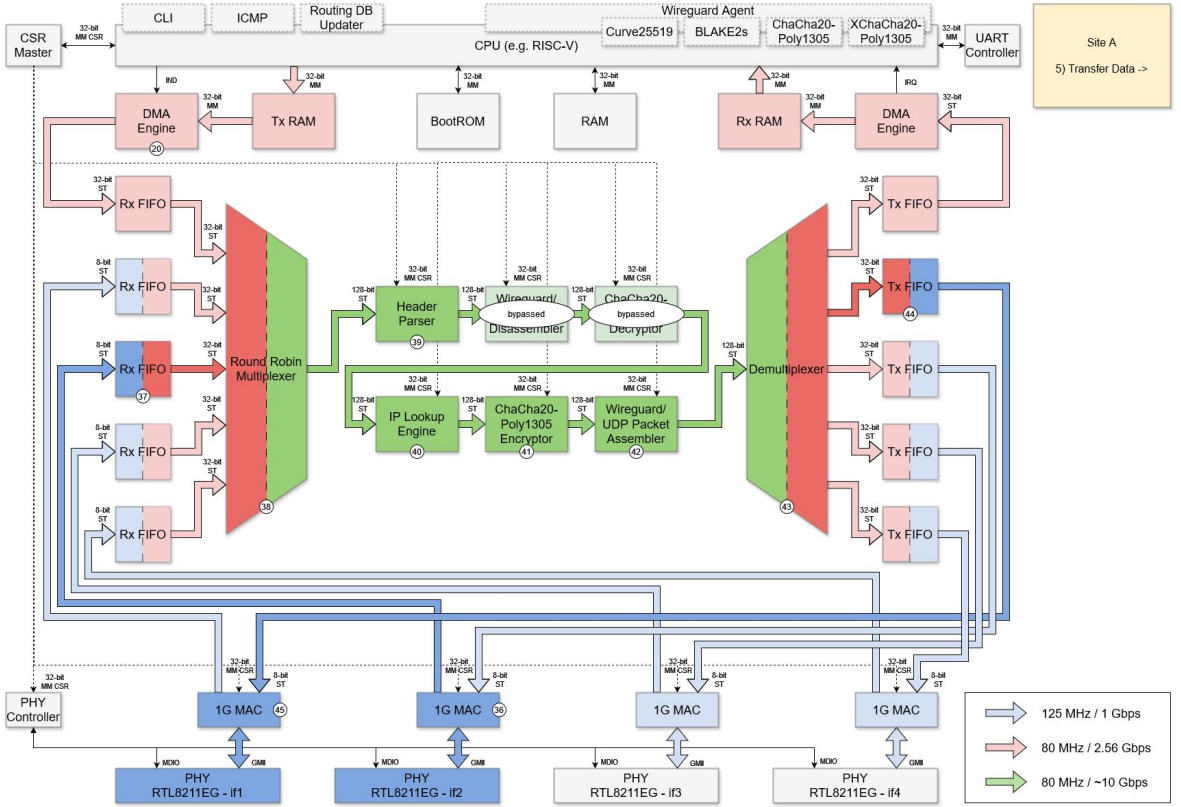




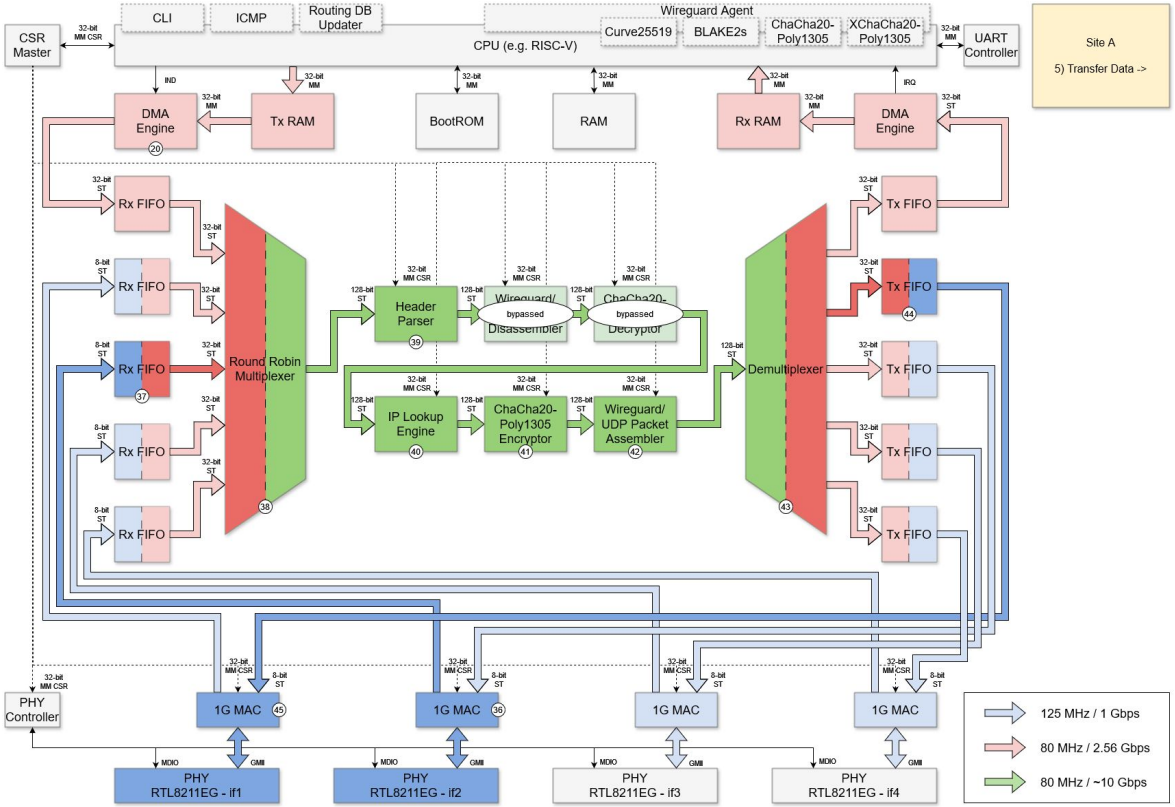
Data Flow Example (36 - 40)

```
Internet Protocol Version 4, Src: 10.10.0.2, Dst: 10.10.0.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0xe546 (58694)
  > Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 64
    Protocol: ICMP (1)
    Header checksum: 0x414c [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.10.0.2
    Destination: 10.10.0.1
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xf95c [correct]
    [Checksum Status: Good]
    Identifier (BE): 27648 (0x6c00)
    Identifier (LE): 108 (0x006c)
    Sequence number (BE): 0 (0x0000)
    Sequence number (LE): 0 (0x0000)
    [Response frame: 4]
  > Data (56 bytes)
```

```
0000  45 00 00 54 e5 46 40 00  40 01 41 4c 0a 0a 00 02   E··T·F@· @·AL····
0010  0a 0a 00 01 08 00 f9 5c  6c 00 00 00 6f ad 22 f5   ·····\ l···o·"·
0020  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ···· ···· ····
0030  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ···· ···· ····
0040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ···· ···· ····
0050  00 00 00 00                                       ····
```



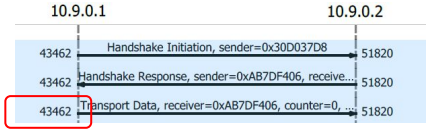
Data Flow Example (41 - 45)




```
> Ethernet II, Src: 3a:36:e5:bf:5a:f8 (3a:36:e5:bf:5a:f8), Dst: a2:e6:34:94:b5:83
> Internet Protocol Version 4, Src: 10.9.0.1, Dst: 10.9.0.2
v User Datagram Protocol, Src Port: 43462, Dst Port: 51820
    Source Port: 43462
    Destination Port: 51820
    Length: 136
    Checksum: 0x14ae [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  > [Timestamps]
v WireGuard Protocol
    Type: Transport Data (4)
    Reserved: 000000
    Receiver: 0xab7df406
    Counter: 0
    Encrypted Packet
    [Stream index: 0]
```

```
0000  a2 e6 34 94 b5 83 3a 36  e5 bf 5a f8 08 00 45 00   ··4···:6 ··Z···E·
0010  00 9c 02 4c 00 00 40 11  63 f1 0a 09 00 01 0a 09   ···L··@· c·······
0020  00 02 a9 c6 ca 6c 00 88  14 ae 04 00 00 00 06 f4   ·····l·· ········
0030  7d ab 00 00 00 00 00 00  00 00 a4 eb c1 2e e3 f9   }·······  ····.···
0040  90 da 18 03 3a 07 89 c0  4e 27 00 f6 f5 c2 71 d4   ····:··· N'····q·
0050  2a c4 b4 d6 26 2e 66 65  49 b4 45 a7 43 6e 82 9b   *···&.fe I·E·Cn··
0060  ff b6 ac 65 f0 56 48 bc  0c 39 1f e7 c5 88 48 74   ···e·VH· ·9····Ht
0070  37 61 27 16 49 40 18 8f  03 db a6 7a f8 38 8e aa   7a'·I@·· ···z·8··
0080  b7 6c 59 36 28 bf 9d c7  be 03 34 6d 91 2e 91 6d   ·lY6(··· ··4m···m
0090  ad 86 25 45 45 47 01 36  4f 2d 24 86 d7 ce d4 c8   ··%EEG·6 O-$·····
00a0  64 2c e5 47 dd b2 6e f6  a4 6b                     d,·G··n· ·k
```

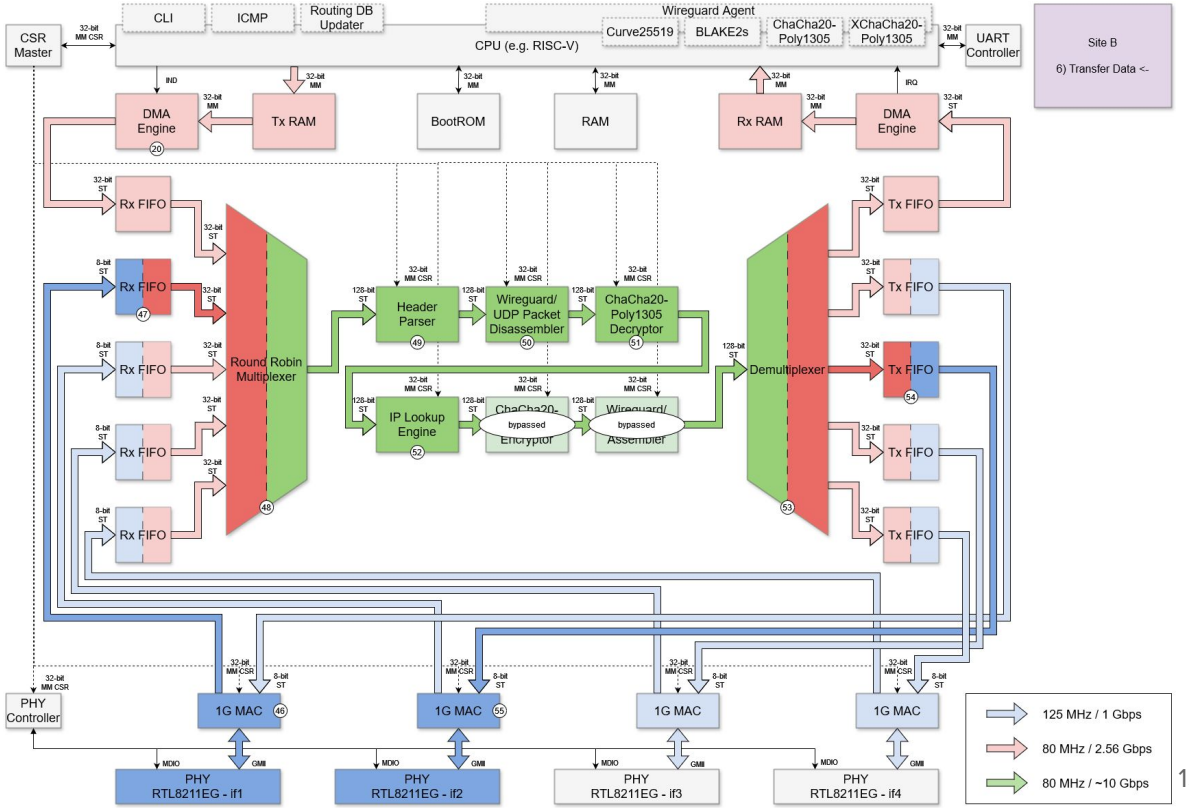
Plain-text Packet = 84B + 12B (16B alignment) = 96B
Encrypted Packet = 96B + 16B Auth. Tag = 112B



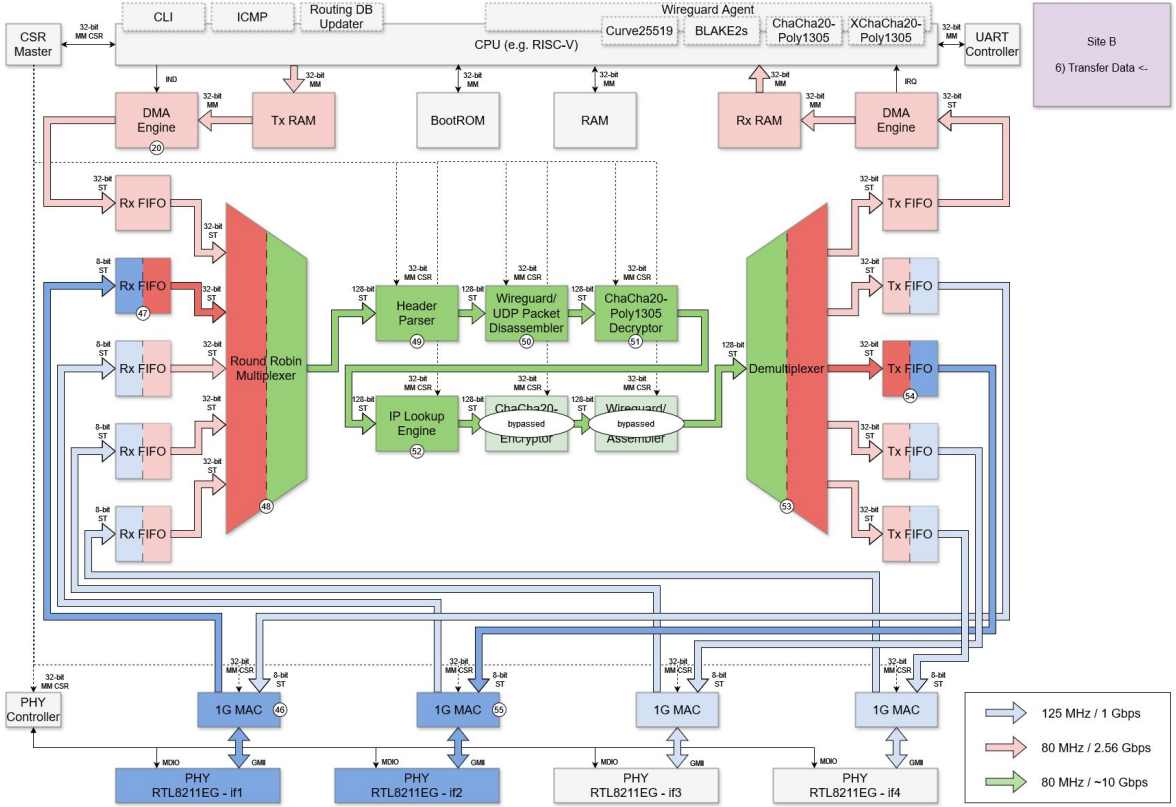
Data Flow Example (46 - 51)

```
> Ethernet II, Src: 3a:36:e5:bf:5a:f8 (3a:36:e5:bf:5a:f8), Dst: a2:e6:34:94:b5:83
> Internet Protocol Version 4, Src: 10.9.0.1, Dst: 10.9.0.2
v User Datagram Protocol, Src Port: 43462, Dst Port: 51820
    Source Port: 43462
    Destination Port: 51820
    Length: 136
    Checksum: 0x14ae [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  > [Timestamps]
v WireGuard Protocol
    Type: Transport Data (4)
    Reserved: 000000
    Receiver: 0xab7df406
    Counter: 0
    Encrypted Packet
    [Stream index: 0]
```

```
0000  a2 e6 34 94 b5 83 3a 36  e5 bf 5a f8 08 00 45 00   ··4···:6 ··Z···E·
0010  00 9c 02 4c 00 00 40 11  63 f1 0a 09 00 01 0a 09   ···L··@· c·······
0020  00 02 a9 c6 ca 6c 00 88  14 ae 04 00 00 00 06 f4   ·····l·· ········
0030  7d ab 00 00 00 00 00 00  00 00 b4 eb c1 2e e3 f9   }·······  ····.···
0040  90 da 18 03 3a 07 89 c0  4e 27 00 f6 f5 c2 71 d4   ····:··· N'····q·
0050  2a c4 b4 d6 26 2e 66 65  49 b4 45 a7 43 6e 82 9b   *···&.fe I·E·Cn··
0060  ff b6 ac 65 f0 56 48 bc  0c 39 1f e7 c5 88 48 74   ···e·VH· ·9····Ht
0070  37 61 27 16 49 40 18 8f  03 db a6 7a f8 38 8e aa   7a'·I@·· ···z·8··
0080  b7 6c 59 36 28 bf 9d c7  be 03 34 6d 91 2e 91 6d   ·lY6(··· ··4m···m
0090  ad 86 25 45 45 47 01 36  4f 2d 24 86 d7 ce d4 c8   ··%EEG·6 O-$·····
00a0  64 2c e5 47 dd b2 6e f6  a4 6b                     d,·G··n· ·k
```

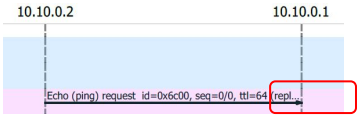


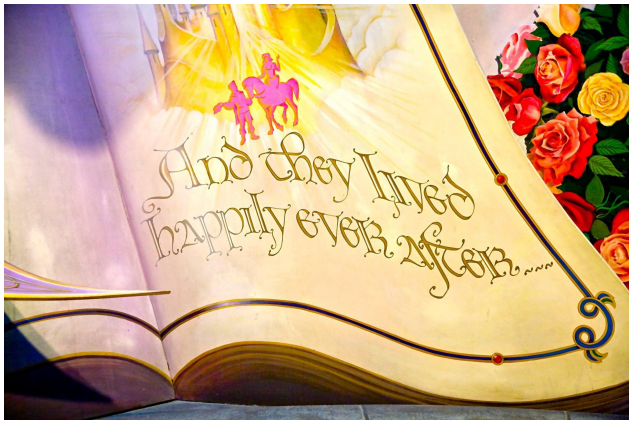
Data Flow Example (52 - 55)




```
▾ Internet Protocol Version 4, Src: 10.10.0.2, Dst: 10.10.0.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  › Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0xe546 (58694)
  › Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 64
    Protocol: ICMP (1)
    Header checksum: 0x414c [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.10.0.2
    Destination: 10.10.0.1
▾ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xf95c [correct]
    [Checksum Status: Good]
    Identifier (BE): 27648 (0x6c00)
    Identifier (LE): 108 (0x006c)
    Sequence number (BE): 0 (0x0000)
    Sequence number (LE): 0 (0x0000)
    [Response frame: 4]
  › Data (56 bytes)
```

```
0000  45 00 00 54 e5 46 40 00  40 01 41 4c 0a 0a 00 02   E··T·F@· @·AL····
0010  0a 0a 00 01 08 00 f9 5c  6c 00 00 00 6f ad 22 f5   ·······\ l···o·"·
0020  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ···· ···· ····
0030  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ···· ···· ····
0040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ···· ···· ····
0050  00 00 00 00                                       ····
```





Thank you!