Mobile Computing Architecture

UW Bothell, WA

Lecture 6: Mobile Network Protocols Stack – 5G User Plane

TCP Example

```
    15 10.015520     2607:fb90:b2e1:1a44… 2607:7700:0:12::113… TLSv1.2  1201 Application Data
    16 10.019482     2607:7700:0:12::113… 2607:fb90:b2e1:1a44… TLSv1.2   129 Application Data
    17 10.019484     2607:7700:0:12::113… 2607:fb90:b2e1:1a44… TLSv1.2   145 Application Data
    18 10.019486     2607:7700:0:12::113… 2607:fb90:b2e1:1a44… TCP        76 5223 → 55768 [ACK] Seq=176 Ack=5419 Win=1452 Len=0 TSval=1241803181 TSecr=1140758802
    19 10.019604     2607:fb90:b2e1:1a44… 2607:7700:0:12::113… TCP        76 55768 → 5223 [ACK] Seq=6544 Ack=107 Win=1023 Len=0 TSval=1140758950 TSecr=1241803179
    20 10.019611     2607:fb90:b2e1:1a44… 2607:7700:0:12::113… TCP        76 55768 → 5223 [ACK] Seq=6544 Ack=176 Win=1023 Len=0 TSval=1140758950 TSecr=1241803179
    21 10.035317     fd00:976a::9         2607:fb90:b2e1:1a44… DNS       273 Standard query response 0x8bbf AAAA init-p01md.apple.com CNAME init-p01md-lb.push-appl
    22 10.039662     2607:fb90:b2e1:1a44… 2607:7700:0:12::173… TCP        88 56201 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1400 WS=128 TSval=1140782720 TSecr=0 SACK_P
    23 10.043288     fd00:976a::9         2607:fb90:b2e1:1a44… DNS       220 Standard query response 0xef47 AAAA init.ess.apple.com CNAME init.ess.apple.com.edgesu
    24 10.045614     2607:fb90:b2e1:1a44… 2607:7700:0:12::173… TCP        88 56202 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1400 WS=128 TSval=1140782726 TSecr=0 SACK_P
    25 10.075344     2607:7700:0:12::113… 2607:fb90:b2e1:1a44… TCP      1444 5223 → 55768 [ACK] Seq=176 Ack=5419 Win=1452 Len=1368 TSval=1241803225 TSecr=114075880
    26 10.075350     2607:7700:0:12::113… 2607:fb90:b2e1:1a44… TLSv1.2  1193 Application Data
    27 10.075353     2607:7700:0:12::113… 2607:fb90:b2e1:1a44… TLSv1.2   145 Application Data
    28 10.075591     2607:fb90:b2e1:1a44… 2607:7700:0:12::113… TCP        76 55768 → 5223 [ACK] Seq=6544 Ack=2661 Win=1004 Len=0 TSval=1140759005 TSecr=1241803225
```

```
> Null/Loopback
> Internet Protocol Version 6, Src: 2607:7700:0:12::1139:90b5, Dst: 2607:fb90:b2e1:1a44:6cf7:8d36:edd:f590
v Transmission Control Protocol, Src Port: 5223, Dst Port: 55768, Seq: 176, Ack: 5419, Len: 0
    Source Port: 5223
    Destination Port: 55768
    <Source or Destination Port: 5223>
    <Source or Destination Port: 55768>
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 176    (relative sequence number)
    Sequence number (raw): 3168717983
    [Next sequence number: 176    (relative sequence number)]
    Acknowledgment number: 5419    (relative ack number)
    Acknowledgment number (raw): 2418351078
    1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x010 (ACK)
    Window size value: 1452
    [Calculated window size: 1452]
    [Window size scaling factor: -1 (unknown)]
    Checksum: 0x9023 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  > Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  > [SEQ/ACK analysis]
  > [Timestamps]
```

trace.pcap

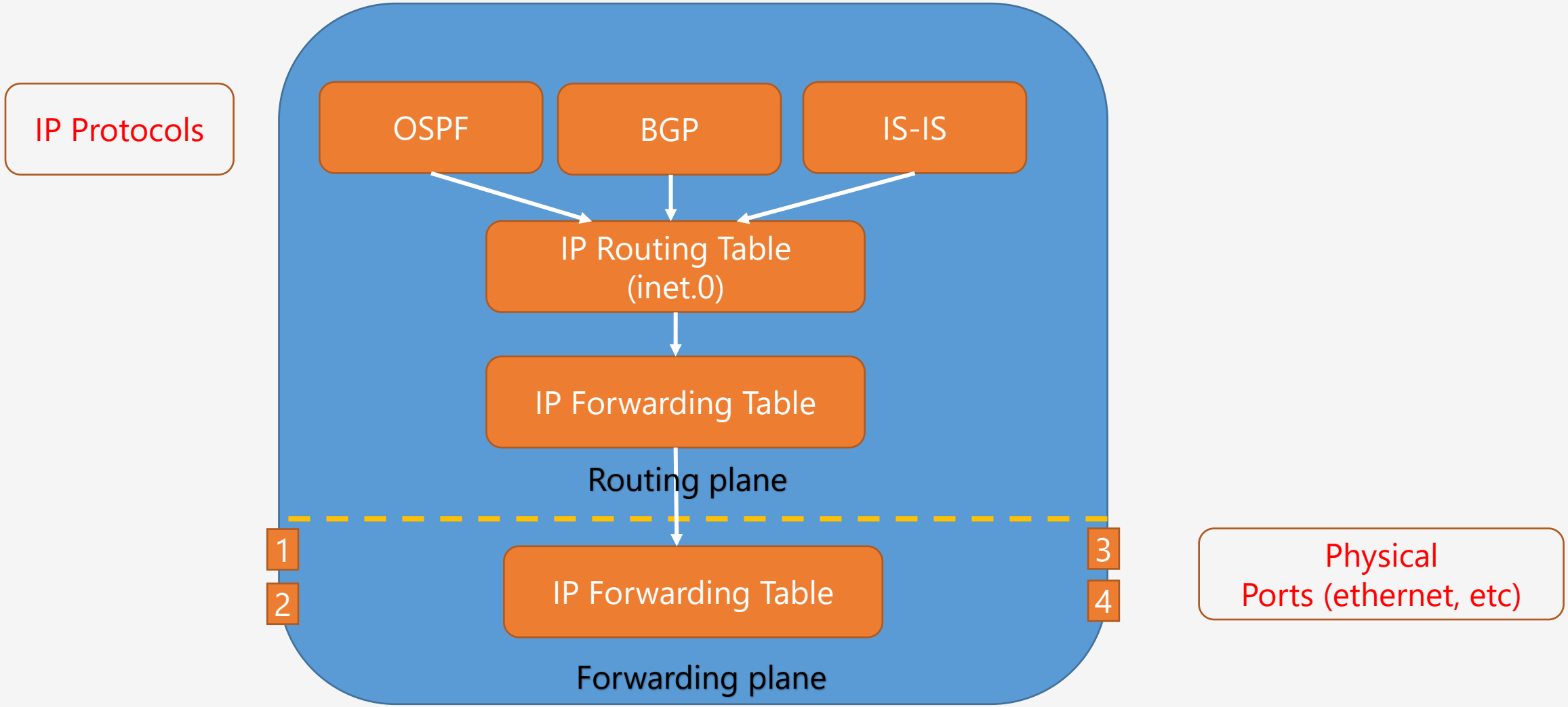
UDP Example

72	10.271237	fd00:976a::9	2607:fb90:b2e1:1a44…	DNS	161 Standard query response 0x1e84 AAAA kt-prod.apple.com
172	14.445952	0.0.0.0	255.255.255.255	DHCP	342 DHCP Discover - Transaction ID 0x9caffa05
178	19.635833	2607:fb90:b2e1:1a44…	fd00:976a::9	DNS	92 Standard query 0xaffc A mqtt.c10r.facebook.com
179	19.636397	2607:fb90:b2e1:1a44…	fd00:976a::9	DNS	92 Standard query 0xd1cc AAAA mqtt.c10r.facebook.com
180	19.645263	2607:fb90:b2e1:1a44…	fd00:976a::9	DNS	97 Standard query 0xd89e A instagram.c10r.facebook.com
181	19.645264	2607:fb90:b2e1:1a44…	2a03:2880:f201:c4:f…	QUIC	1284 Initial, DCID=80fb2e43e4d45234, PKN: 1, CRYPTO, PADDIN
183	19.647726	2607:fb90:b2e1:1a44…	fd00:976a::9	DNS	97 Standard query 0x1667 AAAA instagram.c10r.facebook.com
188	19.683312	fd00:976a::9	2607:fb90:b2e1:1a44…	DNS	108 Standard query response 0xaffc A mqtt.c10r.facebook.cor
189	19.683317	fd00:976a::9	2607:fb90:b2e1:1a44…	DNS	120 Standard query response 0xd1cc AAAA mqtt.c10r.facebook.
190	19.683319	fd00:976a::9	2607:fb90:b2e1:1a44…	DNS	125 Standard query response 0x1667 AAAA instagram.c10r.face
193	19.691420	fd00:976a::9	2607:fb90:b2e1:1a44…	DNS	113 Standard query response 0xd89e A instagram.c10r.faceboo
210	19.703217	2a03:2880:f201:c4:f…	2607:fb90:b2e1:1a44…	QUIC	1284 Initial, SCID=5b40884dc41de977, PKN: 1, ACK, PADDING
211	19.707361	2a03:2880:f201:c4:f…	2607:fb90:b2e1:1a44…	QUIC	1284 Initial, SCID=5b40884dc41de977, PKN: 3, CRYPTO, PADDIN
212	19.707365	2a03:2880:f201:c4:f…	2607:fb90:b2e1:1a44…	QUIC	245 Handshake, SCID=5b40884dc41de977
213	19.707367	2a03:2880:f201:c4:f…	2607:fb90:b2e1:1a44…	QUIC	105 Protected Payload (KP0)
221	19.727384	2607:fb90:b2e1:1a44…	2a03:2880:f201:c4:f…	QUIC	1284 Initial, DCID=5b40884dc41de977, PKN: 3, ACK, PADDING
222	19.727660	2607:fb90:b2e1:1a44…	2a03:2880:f201:c4:f…	QUIC	129 Handshake, DCID=5b40884dc41de977
223	19.727718	2607:fb90:b2e1:1a44…	2a03:2880:f201:c4:f…	QUIC	113 Protected Payload (KP0), DCID=5b40884dc41de977
248	19.760108	2607:fb90:b2e1:1a44…	2a03:2880:f201:c4:f…	QUIC	84 Protected Payload (KP0), DCID=5b40884dc41de977
249	19.761745	2607:fb90:b2e1:1a44…	fd00:976a::9	DNS	105 Standard query 0x91a4 AAAA p15-buy.itunes-apple.com.aka

```
Frame 72: 161 bytes on wire (1288 bits), 161 bytes captured (1288 bits) on interface pdp_ip0, id 0 (inbound)
Null/Loopback
    Family: IPv6 (30)
Internet Protocol Version 6, Src: fd00:976a::9, Dst: 2607:fb90:b2e1:1a44:6cf7:8d36:edd:f590
User Datagram Protocol, Src Port: 53, Dst Port: 59791
    Source Port: 53
    Destination Port: 59791
    <Source or Destination Port: 53>
    <Source or Destination Port: 59791>
    Length: 117
    Checksum: 0x2813 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 3]
  > [Timestamps]
Domain Name System (response)
    Transaction ID: 0x1e84
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
```

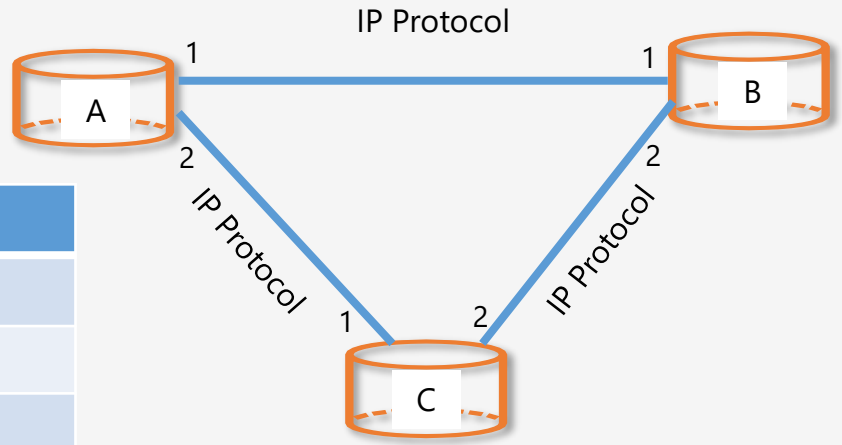
trace.pcap

Router- IP Routing and Forwarding Overview



IP Routing Basics

Path Calculation Algorithm: Shortest Path First (SPF)

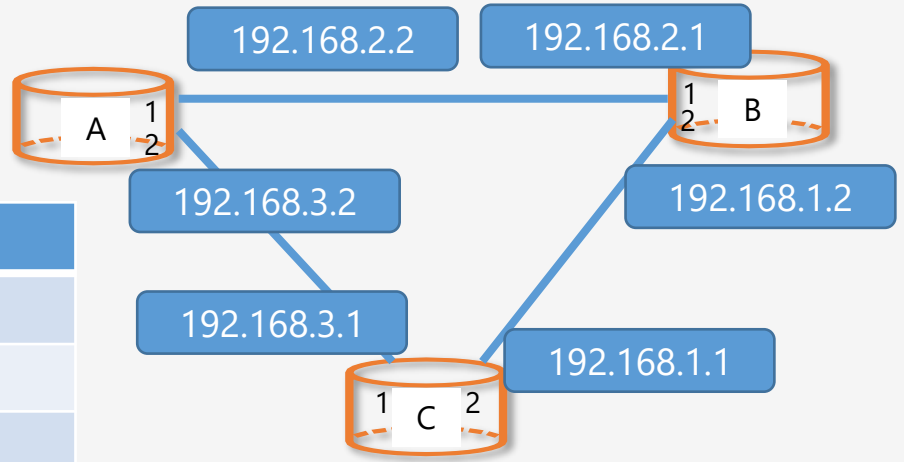


Router A: Routing Table		
Destination	Port	Hops
B	1	1
B	2	2
C	2	1
C	1	2

Router A: Forwarding Table		
Destination	Port	Hops
B	1	1
C	2	1

IP Routing Basics

Path Calculation Algorithm: Shortest Path First (SPF)



Router A: Routing Table		
Destination	Port	Hops
192.168.2.1	1	1
192.168.2.1	2	2
192.168.3.1	2	1
192.168.3.1	1	2

Router A: Forwarding Table		
Destination	Port	Hops
192.168.2.1	1	1
192.168.3.1	2	1

IPv4 Addressing Basics

Byte 1	Byte 2	Byte 3	Byte 4
192	168	10	1

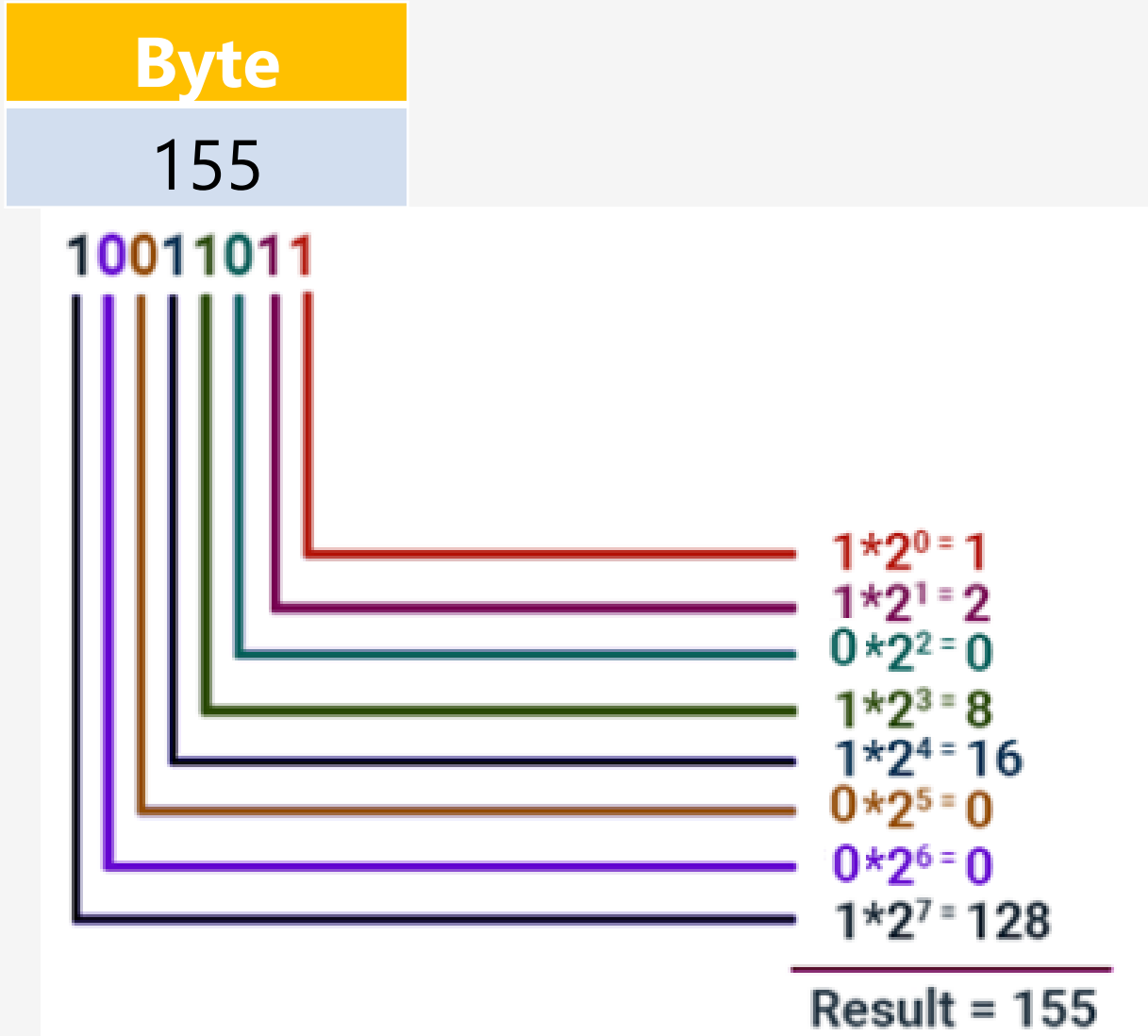
	Octet - 1	Octet - 2	Octet - 3	Octet - 4
In Binary	11000000	10101000	00001010	00000001
	8 bits	8 bits	8 bits	8 bits
In Decimal	192	168	10	1
	Total 32 bits			

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0		
128	64	32	16	8	4	2	1	=	192
1	1	0	0	0	0	0	0		

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0		
128	64	32	16	8	4	2	1	=	168
1	0	1	0	1	0	0	0		

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0		
128	64	32	16	8	4	2	1	=	10
0	0	0	0	1	0	1	0		

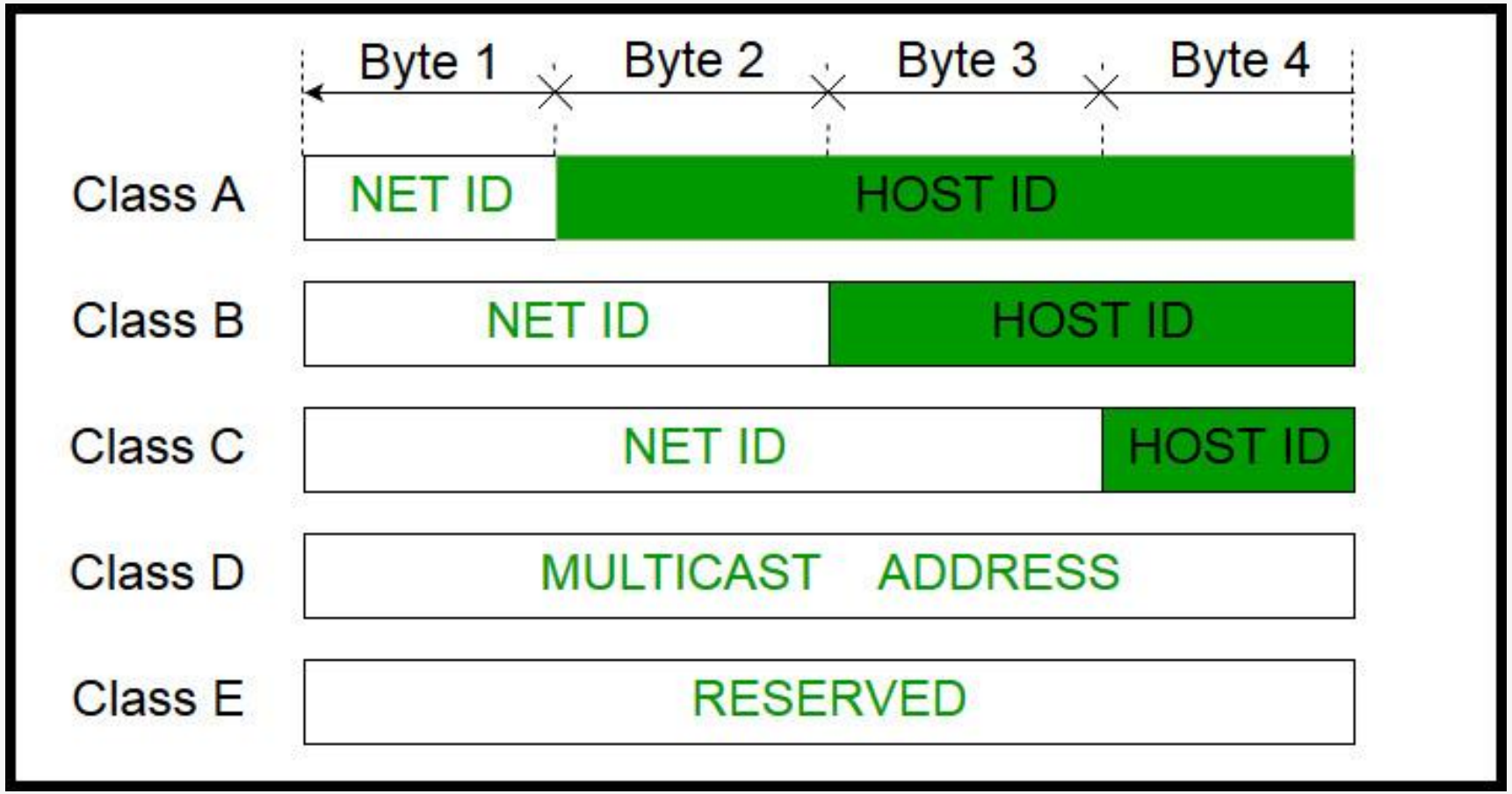
Binary Conversion



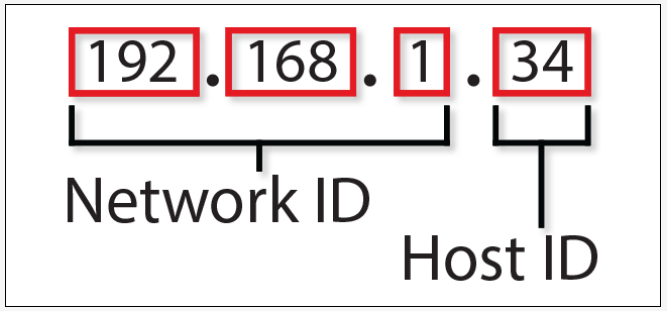
Binary Math

	1	0	0	1	1	0	1	1			
	128	0	0	16	8	0	2	1		155	
Position	8	7	6	5	4	3	2	1			

IPv4 Addressing Basics



IP Addressing Basics



Note subtract 2 addresses:

- First address in the subnet is not used
- Last address in the subnet is not used

Requirement	6 hosts			
$2^h - 2$	>= requirement			
$2^3 - 2$	6			
8 -2	6 valid hosts			
Default Subnet	11111111	11111111	11111111	00000000
With using only 3 host bits	11111111	11111111	11111111	**11111**000
/ 29	8	8	8	5
Subnet Mask	255	255	255	248

IP Addressing Basics - Examples

= 32 -7

= 32 -6

Departments	Start Range		End Range
Accounts: $2^h = 2^7 = 128$	192.168.1.0 /25	---	192.168.1.127 /25
	(+128)		
Marketing: $2^h = 2^6 = 64$	192.168.1.128 /26	---	192.168.1.191 /26
	(+64)		
Sales : $2^h = 2^5 = 32$	192.168.1.192 /27	---	192.168.1.223 /27
	(+32)		
HR : $2^h = 2^3 = 8$	192.168.1.224 /29	---	192.168.1.231 /29
	(+8)		
Still Available in Range	192.168.1.232		192.168.1.255

Exercise

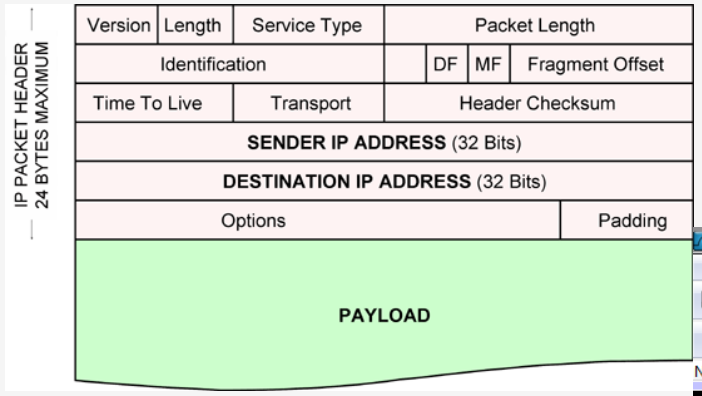
Class C subnet for 24 computers

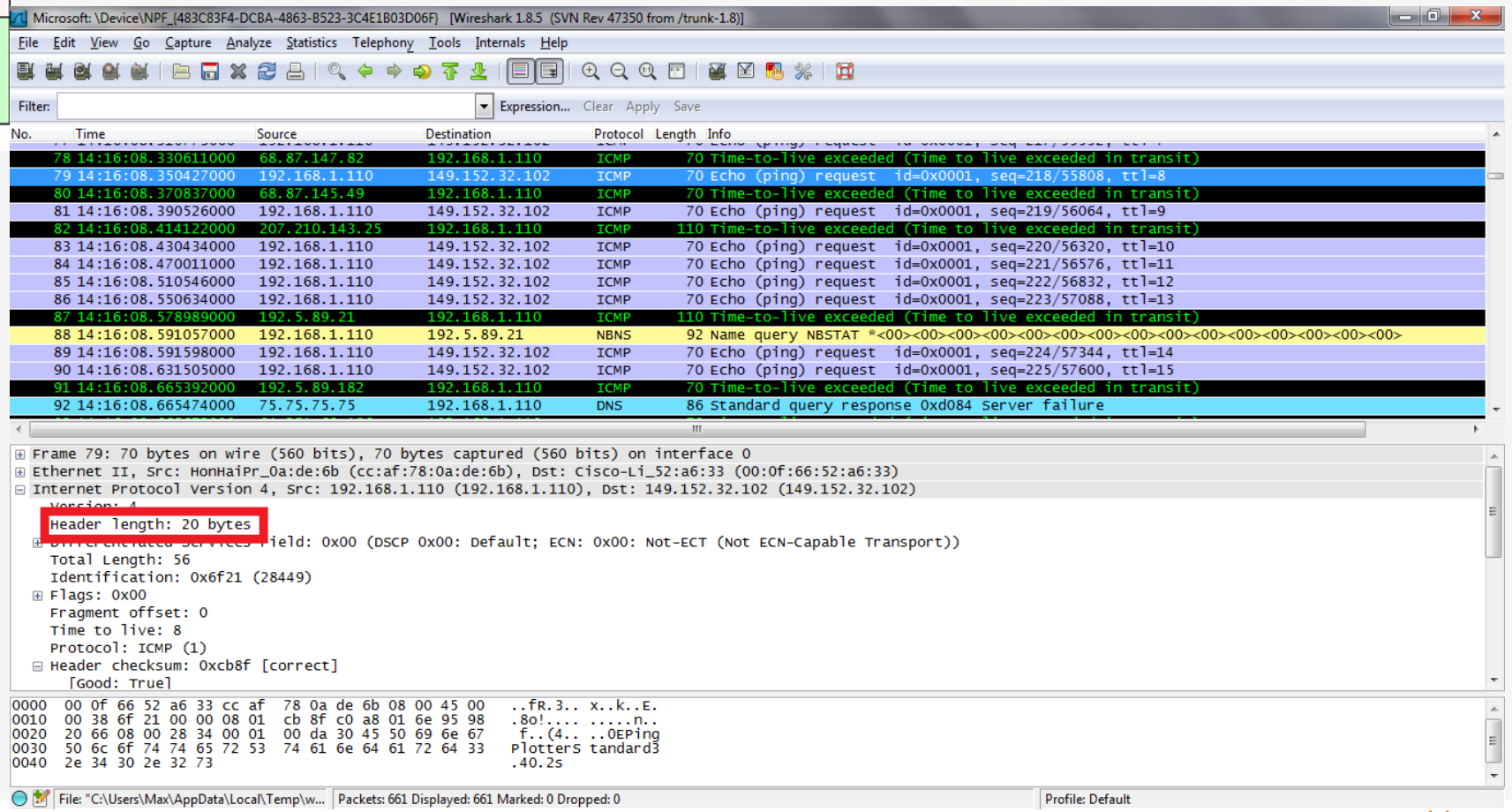
192.168.1.x / y

For 24 devices (computers)

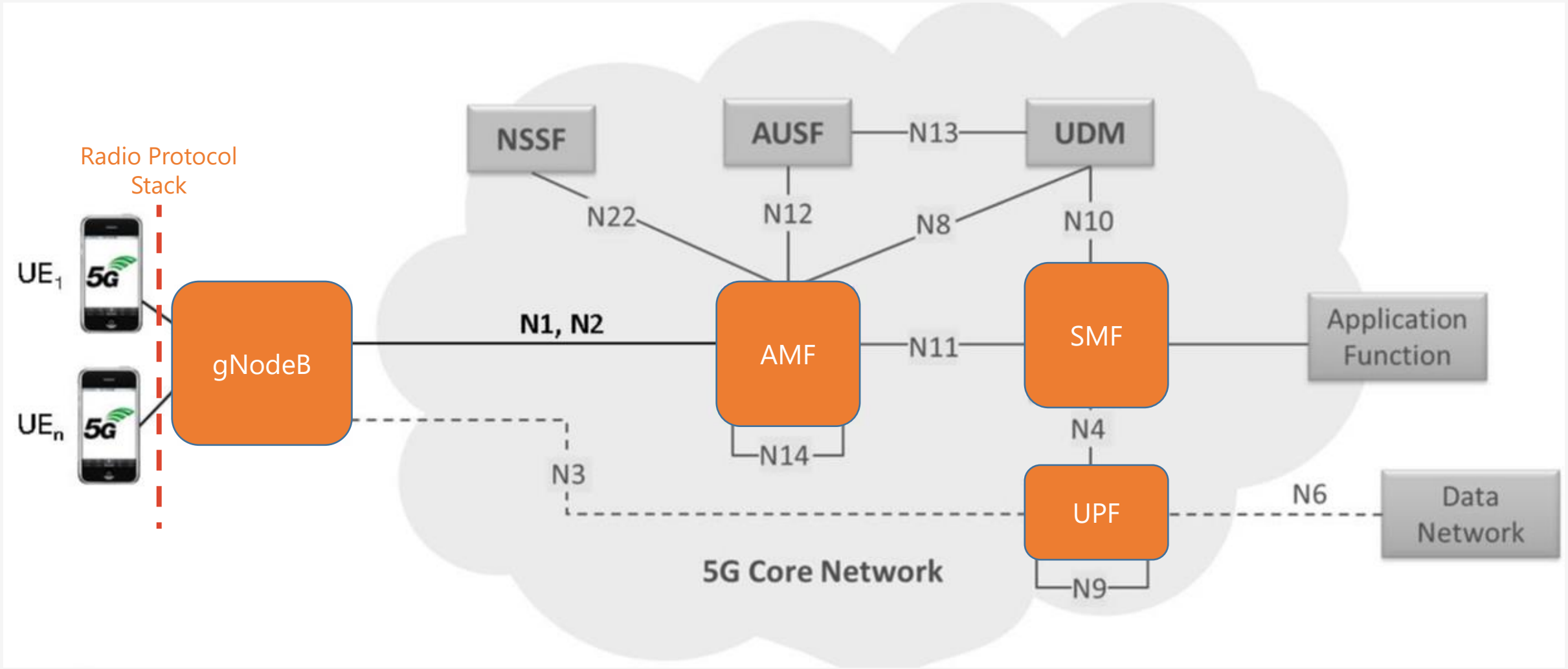
What is x?
What is y?

IP Packet



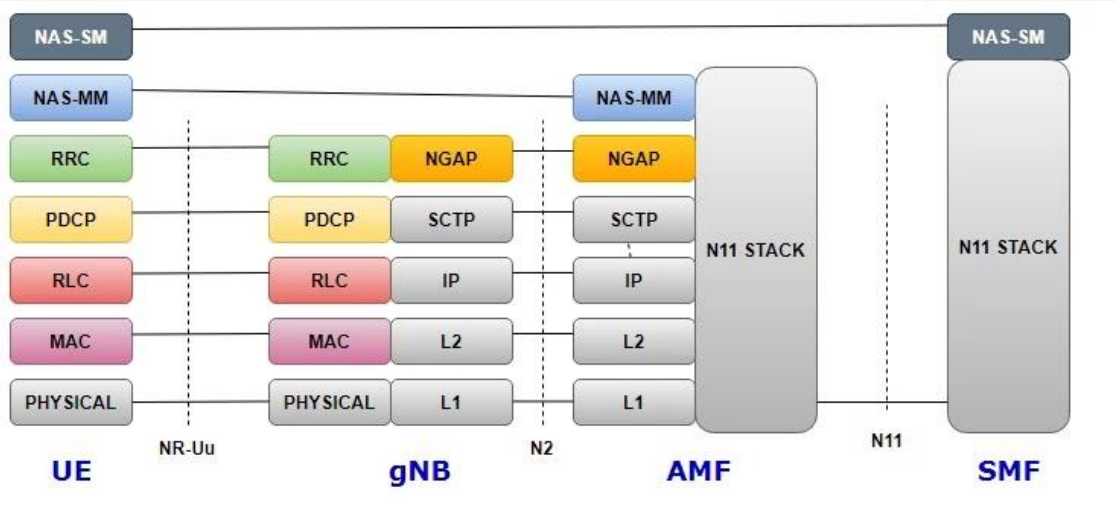


5G Network Architecture

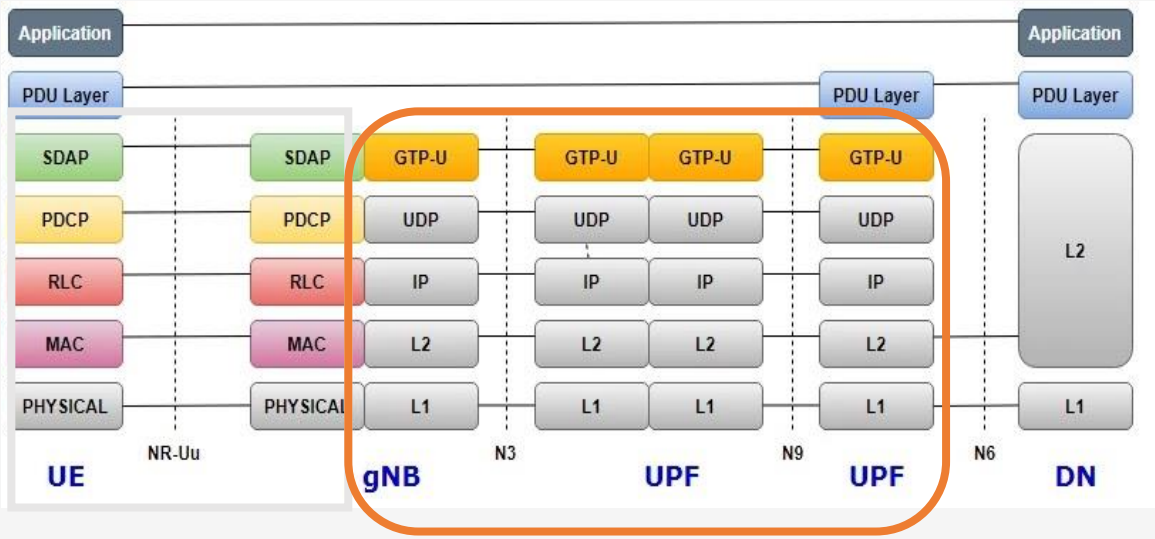


5G RAN- Core Protocol Stack

Control Plane Protocol Stack



User Plane Protocol Stack

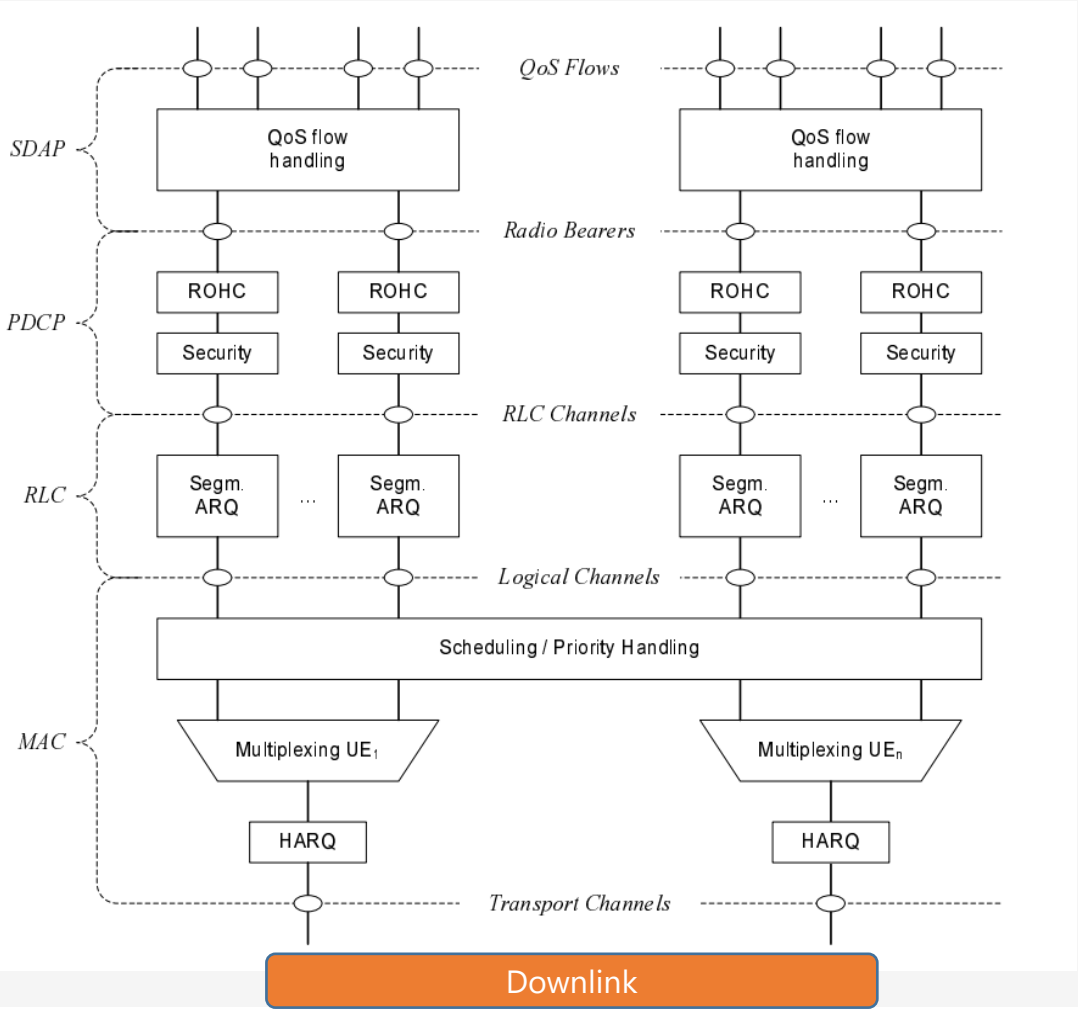


https://www.6g5g4g.com/2020/02/5g-protocol-stack.html

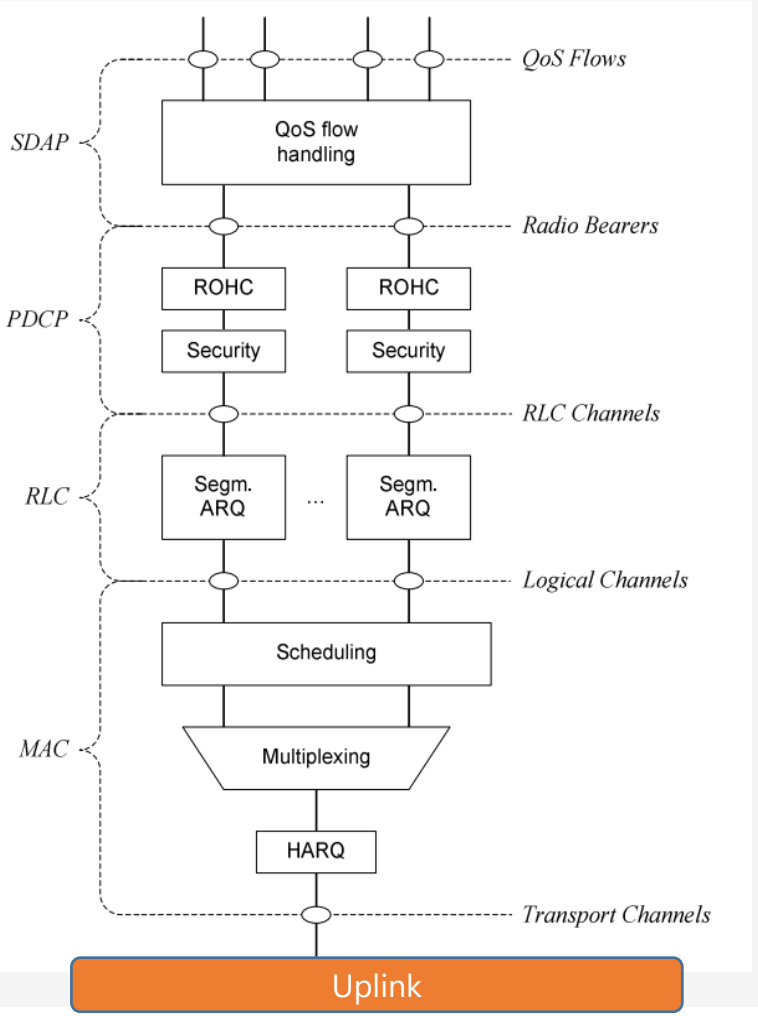
RAN Protocol Stack - Layer 2

The layer 2 is split into the following sublayers: Medium Access Control (MAC), Radio Link Control (RLC), Packet Data Convergence Protocol (PDCP) and Service Data Adaptation Protocol (SDAP). The two figures below depict the Layer 2 architecture for downlink and uplink

- The physical layer offers to the MAC sublayer transport channels
- The MAC sublayer offers to the RLC sublayer logical channels
- The RLC sublayer offers to the PDCP sublayer RLC channels
- The PDCP sublayer offers to the SDAP sublayer radio bearers
- The SDAP sublayer offers to 5GC QoS flows



Downlink



Uplink

ETSI TS 138 300 V15.3.1

GTP Primer

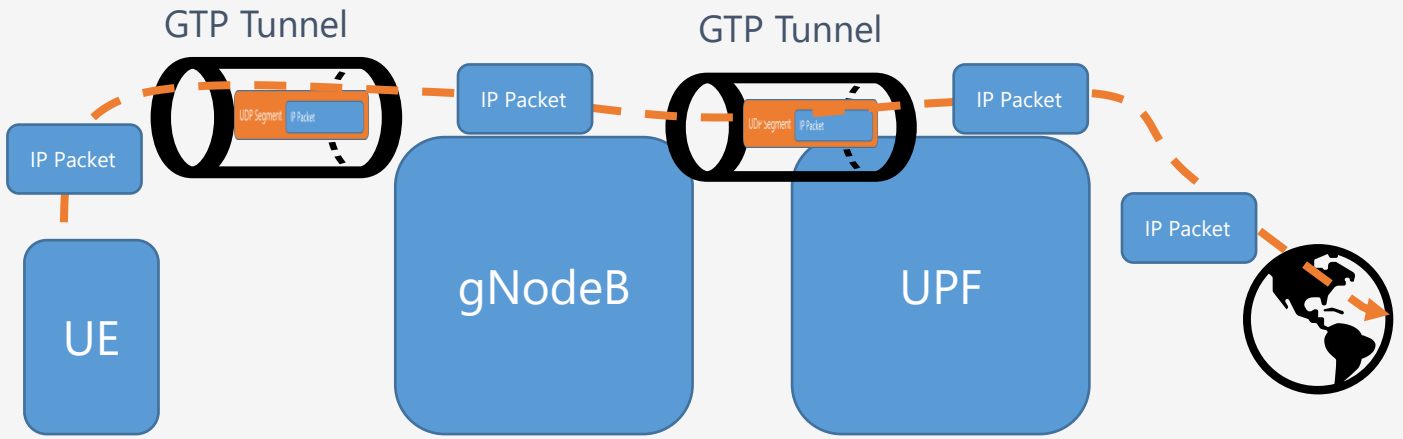
GTP	GPRS Tunnelling Protocol
GTP-PDU	GTP-C PDU or GTP-PDU
GTPv2-C	GTP version 2, **control plane**
GTPv2-U	GTP version 2, **user plane**

What is IP Tunnelling?

Putting an IP Packet within an IP Packet

What is GTP Tunneling?

Putting an IP Packet within a UDP Packet



Tunneling hides the traffic, and also allows the session to go over IP network without Shortest Path First algorithms for IP protocols.

GTPv1 - Header

+	0-2	3	4	5	6	7	8-15	16-23	24-31
0	Version	Protocol type	Reserved	Extension Header Flag	Sequence Number Flag	N-PDU Number Flag	Message Type	Message length	
32	TEID								
64	Sequence number							N-PDU number	Next extension header type

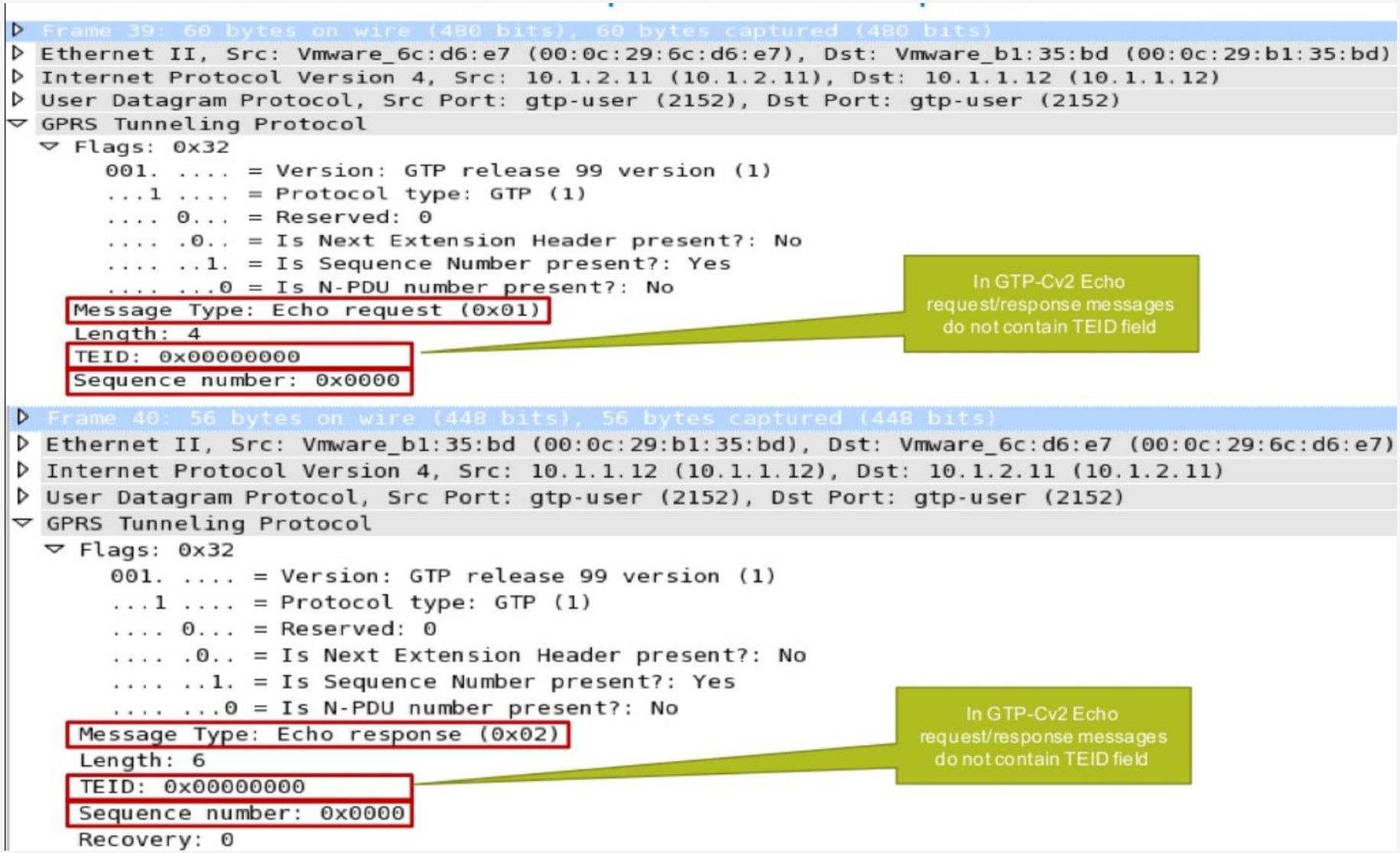
Version
It is a 3-bit field. For GTPv1, this has a value of 1.
Protocol Type (PT)
a 1-bit value that differentiates GTP (value 1) from GTP' (value 0).
Reserved
a 1-bit reserved field (must be 0).
Extension header flag(E)
a 1-bit value that states whether there is an extension header optional field.
Sequence number flag(S)
a 1-bit value that states whether there is a Sequence Number optional field.
N-PDU number flag(PN)
a 1-bit value that states whether there is a N-PDU number optional field.
Message Type
an 8-bit field that indicates the type of GTP message. Different types of messages are defined in 3GPP TS 29.060 section 7.1
Message Length
a 16-bit field that indicates the length of the payload in bytes (rest of the packet following the mandatory 8-byte GTP header). Includes the optional fields.
Tunnel endpoint identifier (TEID)
A 32-bit(4-octet) field used to multiplex different connections in the same GTP tunnel.
Sequence number
an (optional) 16-bit field. This field exists if any of the E, S, or PN bits are on. The field must be interpreted only if the S bit is on.
N-PDU number
an (optional) 8-bit field. This field exists if any of the E, S, or PN bits are on. The field must be interpreted only if the PN bit is on.
Next extension header type
an (optional) 8-bit field. This field exists if any of the E, S, or PN bits are on. The field must be interpreted only if the E bit is on.

GTP can be used with UDP or TCP. UDP is either recommended or mandatory

GTPv1 Message Types

GTP	MESSAGE VALUE	MESSAGE TYPE
GTPv1	1	Echo Request
	2	Echo Response
	3	Version Not Supported
	4	Node Alive Request
	5	Node Alive Response
	6	Redirection Request
	7	Create PDP Context Request
	16	Create PDP Context Response
	17	Update PDP Context Request
	18	Update PDP Context Response
	19	Delete PDP Context Request
	20	Delete PDP Context Response
	22	Initiate PDP Context Activation Request
	23	Initiate PDP Context Activation Response
	26	Error Indication
	27	PDU Notification Request
	28	PDU Notification Response
	29	PDU Notification Reject Request
	30	PDU Notification Reject Response
	31	Supported Extensions Header Notification
	32	Send Routing for GPRS Request
	33	Send Routing for GPRS Response
	34	Failure Report Request
	35	Failure Report Response
	36	Note MS Present Request
	36	Note MS Present Request
	37	Note MS Present Response
	38	Identification Request
	39	Identification Response
	50	SGSN Context Request
	51	SGSN Context Response
	52	SGSN Context Acknowledge
	53	Forward Relocation Request
	54	Forward Relocation Response
	55	Forward Relocation Complete
	56	Relocation Cancel Request
	57	Relocation Cancel Response
	58	Forward SRNS Context
	59	Forward Relocation Complete Acknowledge
	60	Forward SRNS Context Acknowledge
	61	UE Registration Request
	62	UE Registration Response
	70	RAN Information Relay
	96	MBMS Notification Request
	97	MBMS Notification Response
	98	MBMS Notification Reject Request

GTP Example: Echo Request and Response



GTP Standards

GTPv1-C is defined in 3GPP TS 29.060. It is used in th3 4G/5G Networks

GTPv1-C carries various types of control plane signaling messages. The registered port number for GTPv1-C is 2123.

GTPv2-C is defined in 3GPP TS 29.274. It is used on various Mobile Packet Core signaling interfaces.

GTPv2-C carries various types of control plane signaling messages. The registered port number for GTPv2-C is 2123.

GTP-U is defined in 3GPP TS 29.281. It encapsulates and routes user plane traffic across multiple signaling interfaces such as S1, S3, S5, and S8. GTP-U messages are either user plane or signaling messages. The registered port number for GTP-U is 2152.

Reading Material

SDN and Security.pdf