Chair of Distributed Systems and Security
School of Computation, Information and Technology
Technical University of Munich

Ethernet / IEEE 802.3 header and EtherTypes

	0–31	
0 B	Destination Address	
4 B		Source Address
8 B	Source Address	
12 B	Ethertype	

IEEE 802.3 header

Ethertype	Keyword	Protocol
`0x0800`	IPv4	Internet Protocol, version 4
`0x0806`	ARP	Address Resolution Protocol
`0x0842`	WoL	Wake-on-LAN magic packet
`0x8035`	RARP	Reverse Address Resolution Protocol
`0x814c`	SNMP	Simple Network Management Protocol
`0x86dd`	IPv6	Internet Protocol, version 6

IPv4/6 Header and IP Protocol Numbers / Next Header

	0–31						
0 B	Version	IHL	TOS	Total Length			
4 B	Identification	RES	DF	MF	Fragment Offset		
8 B	TTL	Protocol	Header Checksum				
12 B	Source Address						
16 B	Destination Address						
20 B	Options / Padding (optional)						

IPv4 header

	0–31		
0 B	Version	Traffic Class	Flow Label
4 B	Payload Length	Next Header	Hop Limit
8 B	Source Address		
24 B	Destination Address		
40 B	Extension Headers (optional)		

IPv6 header

	0–31				
0 B	Next Header	Reserved	Fragment Offset	Reserved	M F
4 B	Identification				
8 B	additional Extension Headers (optional)				

IPv6 fragmentation header

No / NH	protocol	No / NH	protocol
`0x01`	ICMPv4 (Internet Control Management)	`0x2f`	GRE (General Routing Encapsulation)
`0x06`	TCP (Transmission Control Protocol)	`0x3a`	ICMPv6 (ICMP for IPv6)
`0x11`	UDP (User Datagram Protocol)	`0x3b`	no next header
`0x2c`	fragment header	`0x84`	SCTP (Stream Control Transmission)

TCP/UDP Header and Selected Well-Known Ports

	0–31								
0 B	Source Port	Destination Port							
4 B	Sequence Number								
8 B	Acknowledgement Number								
12 B	Offset	Reserved	URG	ACK	PSH	RST	SYN	FIN	Window
16 B	Checksum	Urgent Pointer							
20 B	Options (0 or more multiples of 4 B)								

TCP header

	0–31	
0 B	Source Port	Destination Port
4 B	Length	Checksum

UDP header

port	service name	port	service name
20/21	ftp	68	bootpc
22	ssh	80	http
23	telnet	110	pop3
25	smtp	443	https
53	domain (dns)	546	dhcpv6-client
67	bootps	547	dhcpv6-server

ARP

	0–31		
0 B	Hardware Type: `0x0001` (Ethernet)	Protocol Type: `0x0800` (IPv4)	
4 B	Hardware Addr. Length	Protocol Addr. Length	Operation: `0x0001` (Request) or `0x0002` (Reply)
8 B	Sender Hardware Address		
12 B		Sender Protocol Address	
16 B	Sender Protocol Address (contintued)		
20 B	Target Hardware Address		
24 B	Target Protocol Address		

ARP packet format

ICMPv4

	0–31		
0 B	Type	Code	Checksum
4 B	Identifier	Sequence Number	
8 B	Data (≥ 0 B)		

ICMPv4 echo request/reply

	0–31		
0 B	Type	Code	Checksum
4 B	unused		
8 B	IP Header + first 8 B of original datagram's data		

ICMPv4 time exceeded

	0–31		
0 B	Type	Code	Checksum
4 B	unused		
8 B	IP Header + first 8 B of original datagram's data		

ICMPv4 destination unreachable

Type	Code	Description
0 – echo reply	0	echo reply
1 and 2		*reserved*
3 – Destination Unreachable	0	destination network unreachable
	1	destination host unreachable
	2	destination protocol unreachable
	3	destination port unreachable
4 – source quench	0	source quench (congestion control)
5 – redirect message	0	redirect datagram for the network
	1	redirect datagram for the host
8 – echo request	0	echo request
11 – time exceeded	0	TTL expired in transit
	1	fragment reassembly time exceeded

selected ICMPv4 types/codes

ICMPv6

Hint: The following ICMPv6 messages are identical to their ICMPv4 counterparts:

- echo request / reply
- destination unreachable
- time exceeded

However, for ICMPv6 types / codes (see below) the restrictions regarding the minimum length or alignment apply (padding).

	0–31		
0 B	Type	Code	Checksum
4 B	Reserved (set to zero)		
8 B	Target Address		
24 B	Option Type = `0x01`	Option Length = `0x01`	Source Link Address
28 B			
32 B	Additional Options		

neighbor solicitation

	0–31			
0 B	Type	Code	Checksum	
4 B	R	S	O	Reserved (set to zero)
8 B	Target Address			
24 B	Option Type = `0x02`	Option Length = `0x01`	Target Link Address	
28 B				
32 B	Additional Options			

Flags: R = Router, S = Solicited, O = Override

neighbor advertisement

type	code	description
0		*reserved*
1 – destination unreachable	0	no route to destination
	3	address unreachable
	4	port unreachable
2 – packet too big	0	packet too big
3 – time exceeded	0	hop limit exceeded in transit
	1	fragment reassembly time exceeded
128 – echo request	0	echo request
129 – echo reply	0	echo reply
133 – router solicitation	0	*Neighbor Discovery Protocol (NDP)*
134 – router advertisement	0	*Neighbor Discovery Protocol (NDP)*
135 – neighbor solicitation	0	*Neighbor Discovery Protocol (NDP)*
136 – neighbor advertisement	0	*Neighbor Discovery Protocol (NDP)*
137 – redirect message	0	*Neighbor Discovery Protocol (NDP)*

selected ICMPv6 types/codes

Number Systems 1/2

dec	hex	binary	ascii	dec	hex	binary	ascii	dec	hex	binary	ascii	dec	hex	binary	ascii
0	00	00000000	NUL	32	20	00100000	SPACE	64	40	01000000	@	96	60	01100000	‘
1	01	00000001	SOH	33	21	00100001	!	65	41	01000001	A	97	61	01100001	a
2	02	00000010	STX	34	22	00100010	"	66	42	01000010	B	98	62	01100010	b
3	03	00000011	ETX	35	23	00100011	#	67	43	01000011	C	99	63	01100011	c
4	04	00000100	EOT	36	24	00100100	$	68	44	01000100	D	100	64	01100100	d
5	05	00000101	ENQ	37	25	00100101	%	69	45	01000101	E	101	65	01100101	e
6	06	00000110	ACK	38	26	00100110	&	70	46	01000110	F	102	66	01100110	f
7	07	00000111	BEL	39	27	00100111	’	71	47	01000111	G	103	67	01100111	g
8	08	00001000	BS	40	28	00101000	(	72	48	01001000	H	104	68	01101000	h
9	09	00001001	HT	41	29	00101001	)	73	49	01001001	I	105	69	01101001	i
10	0a	00001010	LF	42	2a	00101010	*	74	4a	01001010	J	106	6a	01101010	j
11	0b	00001011	VT	43	2b	00101011	+	75	4b	01001011	K	107	6b	01101011	k
12	0c	00001100	FF	44	2c	00101100	,	76	4c	01001100	L	108	6c	01101100	l
13	0d	00001101	CR	45	2d	00101101	-	77	4d	01001101	M	109	6d	01101101	m
14	0e	00001110	SO	46	2e	00101110	.	78	4e	01001110	N	110	6e	01101110	n
15	0f	00001111	SI	47	2f	00101111	/	79	4f	01001111	O	111	6f	01101111	o
16	10	00010000	DLE	48	30	00110000	0	80	50	01010000	P	112	70	01110000	p
17	11	00010001	DC1	49	31	00110001	1	81	51	01010001	Q	113	71	01110001	q
18	12	00010010	DC2	50	32	00110010	2	82	52	01010010	R	114	72	01110010	r
19	13	00010011	DC3	51	33	00110011	3	83	53	01010011	S	115	73	01110011	s
20	14	00010100	DC4	52	34	00110100	4	84	54	01010100	T	116	74	01110100	t
21	15	00010101	NAK	53	35	00110101	5	85	55	01010101	U	117	75	01110101	u
22	16	00010110	SYN	54	36	00110110	6	86	56	01010110	V	118	76	01110110	v
23	17	00010111	ETB	55	37	00110111	7	87	57	01010111	W	119	77	01110111	w
24	18	00011000	CAN	56	38	00111000	8	88	58	01011000	X	120	78	01111000	x
25	19	00011001	EM	57	39	00111001	9	89	59	01011001	Y	121	79	01111001	y
26	1a	00011010	SUB	58	3a	00111010	:	90	5a	01011010	Z	122	7a	01111010	z
27	1b	00011011	ESC	59	3b	00111011	;	91	5b	01011011	[	123	7b	01111011	{
28	1c	00011100	FS	60	3c	00111100	<	92	5c	01011100	\	124	7c	01111100	|
29	1d	00011101	GS	61	3d	00111101	=	93	5d	01011101	]	125	7d	01111101	}
30	1e	00011110	RS	62	3e	00111110	>	94	5e	01011110	^	126	7e	01111110	~
31	1f	00011111	US	63	3f	00111111	?	95	5f	01011111	_	127	7f	01111111	DEL

Number Systems 2/2

dec	hex	binary	dec	hex	binary	dec	hex	binary	dec	hex	binary
128	80	10000000	160	a0	10100000	192	c0	11000000	224	e0	11100000
129	81	10000001	161	a1	10100001	193	c1	11000001	225	e1	11100001
130	82	10000010	162	a2	10100010	194	c2	11000010	226	e2	11100010
131	83	10000011	163	a3	10100011	195	c3	11000011	227	e3	11100011
132	84	10000100	164	a4	10100100	196	c4	11000100	228	e4	11100100
133	85	10000101	165	a5	10100101	197	c5	11000101	229	e5	11100101
134	86	10000110	166	a6	10100110	198	c6	11000110	230	e6	11100110
135	87	10000111	167	a7	10100111	199	c7	11000111	231	e7	11100111
136	88	10001000	168	a8	10101000	200	c8	11001000	232	e8	11101000
137	89	10001001	169	a9	10101001	201	c9	11001001	233	e9	11101001
138	8a	10001010	170	aa	10101010	202	ca	11001010	234	ea	11101010
139	8b	10001011	171	ab	10101011	203	cb	11001011	235	eb	11101011
140	8c	10001100	172	ac	10101100	204	cc	11001100	236	ec	11101100
141	8d	10001101	173	ad	10101101	205	cd	11001101	237	ed	11101101
142	8e	10001110	174	ae	10101110	206	ce	11001110	238	ee	11101110
143	8f	10001111	175	af	10101111	207	cf	11001111	239	ef	11101111
144	90	10010000	176	b0	10110000	208	d0	11010000	240	f0	11110000
145	91	10010001	177	b1	10110001	209	d1	11010001	241	f1	11110001
146	92	10010010	178	b2	10110010	210	d2	11010010	242	f2	11110010
147	93	10010011	179	b3	10110011	211	d3	11010011	243	f3	11110011
148	94	10010100	180	b4	10110100	212	d4	11010100	244	f4	11110100
149	95	10010101	181	b5	10110101	213	d5	11010101	245	f5	11110101
150	96	10010110	182	b6	10110110	214	d6	11010110	246	f6	11110110
151	97	10010111	183	b7	10110111	215	d7	11010111	247	f7	11110111
152	98	10011000	184	b8	10111000	216	d8	11011000	248	f8	11111000
153	99	10011001	185	b9	10111001	217	d9	11011001	249	f9	11111001
154	9a	10011010	186	ba	10111010	218	da	11011010	250	fa	11111010
155	9b	10011011	187	bb	10111011	219	db	11011011	251	fb	11111011
156	9c	10011100	188	bc	10111100	220	dc	11011100	252	fc	11111100
157	9d	10011101	189	bd	10111101	221	dd	11011101	253	fd	11111101
158	9e	10011110	190	be	10111110	222	de	11011110	254	fe	11111110
159	9f	10011111	191	bf	10111111	223	df	11011111	255	ff	11111111

Chair of Distributed Systems and Security
School of Computation, Information and Technology
Technical University of Munich

Physical Layer

constants:

speed of light:	$c_0 \approx 3 \cdot 10^8\,\mathrm{m/s}$
relative velocity of propagation in copper / glass:	$\nu \approx 2/3$
relative velocity of propagation in vacuum / air:	$\nu \approx 1$
wavelength in the medium:	$\lambda = c/f$

information content and entropy: Memoryless source emits characters $x \in \mathcal{X}$, expressed by X:

information content of $x \in \mathcal{X}$: $I(x) = -\log_2(\Pr[X = x])$

entropy of the source: $H(X) = -\sum_{x\in\mathcal{X}} \Pr[X = x] \log_2(\Pr[X = x])$

fourier series: angular frequency $\omega = 2\pi/T$

$$s(t) = \frac{a_0}{2} + \sum_{k=1}^{\infty} a_k \cos(k\omega t) + b_k \sin(k\omega t) \text{ mit } a_k = \frac{2}{T}\int_{-T/2}^{T/2} s(t)\cos(k\omega t)\,\mathrm{d}t,\ b_k = \frac{2}{T}\int_{-T/2}^{T/2} s(t)\sin(k\omega t)\,\mathrm{d}t\,.$$

fourier transform: $s(t) \circ\!\!-\!\!\bullet\, S(f)$

$$S(f) = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\infty} s(t)e^{-j2\pi ft}\,\mathrm{d}t = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\infty} s(t)\left(\cos(2\pi ft) - j\sin(2\pi ft)\right)\mathrm{d}t \quad (j \text{ refers to the imaginary unit})$$

sampling, quantisation and reconstruction:

sampling theorem (Nyquist): $f_N = 2B$ (B is the one-sided cut-off frequency in the baseband)

sampled signal: $\hat{s}(t) = s(t)\sum_{n=-\infty}^{\infty}\delta[t - nT_a]$, mit $\delta[t - nT_a] = \begin{cases}1 & \text{for } t = nT_a\\ 0 & \text{otherwise}\end{cases}$

sampled values: $\hat{s}[n] = s(nT_a)$

step width: $\Delta = \frac{b-a}{M}$, mit $M = 2^N$ steps at N bit accuracy

quantization levels: $Q = \{a + \Delta/2, a + \Delta(1 + 1/2), \ldots, a + \Delta(M - 1 + 1/2)\}$
$\mathbb{R} \to Q,\ \hat{s}[n] \mapsto \bar{s}[n]$ (rounded)

quantized signal: $\bar{s}(t) = \sum_{n=-\infty}^{\infty} \hat{s}[n] \cdot \mathrm{rect}(t - nT_a)$, $\mathrm{rect}(t) = \begin{cases}1 & \text{for } -T_a/2 \le t \le T_a/2\\ 0 & \text{otherwise}\end{cases}$

quantization error: $q_e(t) = s(t) - \bar{s}(t) \le \Delta/2$, wenn $a \le s(t) \le b$

reconstruction: $s(t) \approx \sum_{n=-\infty}^{\infty} \hat{s}[n] \cdot \mathrm{sinc}\left(\frac{t - nT_a}{T_a}\right)$, $\mathrm{sinc}(t) = \frac{\sin(\pi t)}{\pi t}$

channel bandwidth: $C_{\max}$ is an upper upper bound for the achievable net data rate in bit/s, i.e. transmission of redundancy-free data. For this purpose it may be necessary to add redundancy (channel coding), but this does not change the information content of the message.

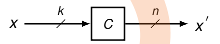
Hartley: $C_H = 2B\log_2(M)$ bit

Shannon/Hartley: $C_S = B\log_2(1 + \mathrm{SNR})$ bit

signal-to-noise ratio: $\mathrm{SNR} = \frac{P_S}{P_N} = \frac{\text{signal power}}{\text{noise power}} = 10\log_{10}(\mathrm{SNR})$ dB

upper bound: $C_{\max} \le \min\{C_H, C_S\}$

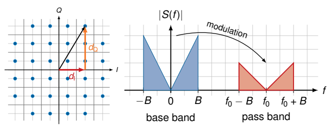
channel coding: Example block codes: a block of the line k bit is mapped to n bit long channel words are mapped ($n > k$). For each channel word $m < n - k$ bit can be corrected (depending on the code).



code rate: $R = k/n$

modulation:

$$s(t) = \left(\sum_{n=0}^{\infty} d_I[n]g_T(t - nT)\right)\cos(2\pi f_0 t) - \left(\sum_{n=0}^{\infty} d_Q[n]g_T(t - nT)\right)\sin(2\pi f_0 t)$$



Data Link Layer

serialisation time, propagation delay, transmission time, bandwidth delay product:

serialisation time:	$t_s = L/r$
propagation time:	$t_p = d/(\nu c_0)$
transmission time:	$t_d = t_s + t_p$
bandwidth delay product:	$C = t_p r$

cyclic redundancy check (CRC): addition = XOR

checksum: $c(x) = m(x)x^n \bmod r(x)$, mit $n = \mathrm{grad}\, r(x)$

sent message: $s(x) = m(x)x^n + c(x)$

check: $c'(x) = (s(x) + e(x)) \bmod r(x)$, with error pattern $e(x)$

adjacency and distance matrix:

adjacency matrix: $\boldsymbol{A} = (a)_{ij} = \begin{cases}1 & \exists(i,j) \in \mathcal{A}\\ 0 & \text{sonst}\end{cases}$ distance matrix: $\boldsymbol{D} = (d)_{ij} = \begin{cases}c_{ij} & \exists(i,j) \in \mathcal{A}\\ 0 & \text{if } i = j\\ \infty & \text{otherwise}\end{cases}$

min-plus-product: $\boldsymbol{D}^n = \boldsymbol{D}^{n-1} \otimes \boldsymbol{D}$, mit $d^n_{ij} = \min_{k\in\mathcal{N}}\left\{d^{n-1}_{ik} + d_{kj}\right\}$, $n \ge 1$

Network Layer

kinds of transmission: Transmission time of a message of length L over n intermediate stations, each with an identical data rate r over the total distance d:

circuit switching: $T_{\mathrm{LS}} = t_s + 4t_p = \frac{L}{r} + \frac{4d}{\nu c_0}$

message forwarding: $T_{\mathrm{NF}} = (n+1)t_s + t_p = (n+1)\frac{L_H + L}{r} + \frac{d}{\nu c_0}$, L_H = length of the message header

packet switching: $T_{\mathrm{PS}} = \frac{1}{r}\left(\left\lceil\frac{L}{p_{\max}}\right\rceil L_h + L + n(L_h + p_{\max})\right) + \frac{d}{\nu c_0}$, L_h = length of the packet header

round trip time (RTT): RTT between the nodes $s, t \in \mathcal{N}$ over the path $\mathcal{P} = \{(s,1),(1,2),\ldots,(n,t)\}$ and the (in general) non-symmetric return path $\mathcal{P}'$:

RTT (general): $\mathrm{RTT}(s,t) = \sum_{(i,j)\in\mathcal{P}}(t_s(i,j) + t_p(i,j)) + \sum_{(i,j)\in\mathcal{P}'}(t_s(i,j) + t_p(i,j))$

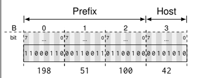
RTT (symmetric paths): $\mathrm{RTT}(s,t) = 2\sum_{(i,j)\in\mathcal{P}}(t_s(i,j) + t_p(i,j))$

special IP addresses and ranges:

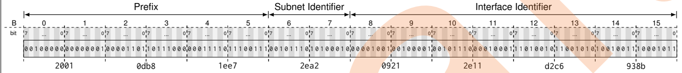
address range	use
`0.0.0.0/8`	hosts in this network
`127.0.0.0/8`	loopback, especially 127.0.0.1
`10.0.0.0/8`	private addresses
`172.16.0.0/12`	private addresses
`192.168.0.0/16`	private addresses
`169.254.0.0/16`	automatic private IP addressing
`255.255.255.255/32`	global broadcast

address range	use
`::/128`	unspecified address
`::1/128`	loopback
`fe80::/10`	link-local addresses
`fc00::/7`	unique-local unicast addresses
`ff00::/8`	multicast addresses
`ff02::1/128`	all nodes
`ff02::1:ff00:0/104`	solicited node addresses

IPv4/6 address format: (examples)



With IPv4, no distinction is made between prefix and subnet (the defines the respective subnet). With IPv6, one additionally speaks of a *subnet identifier*, which, together with the prefix, identifies the respective subnet. The notation `<address>/N` always specifies the length of the network part.



Transport Layer

sliding window protocols

Cardinality of Sequence Numbers: N. Maximum size of the transmission window w_s to avoid collisions:

go-back-n: $w_s \le N - 1$

selective repeat: $w_s \le \left\lfloor\frac{N}{2}\right\rfloor$

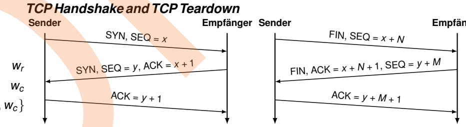
windows related to TCP

receive window: w_r

congestion window: w_c

transmit window: $w_s = \min\{w_r, w_c\}$

TCP Handshake and TCP Teardown



TCP throughput in the congestion avoidance phase. Assumption: segment loss in the network as soon as $w_s \ge x \cdot \mathrm{MSS}$.

time between segment losses: $T = \left(\frac{x}{2} + 1\right)\cdot \mathrm{RTT}$

number of sent segments in T: $n = \frac{3}{8}x^2 + \frac{3}{4}x$

loss-rate: $\theta = \frac{1}{n}$

throughput: $r_{TCP} = \frac{n \cdot \mathrm{MSS}}{T}\cdot(1 - \theta)$

Application Layer

prefix-free codes

Valid code words of a prefix-free code are never a prefix of another code word of the same code. An *optimal* prefix-free code minimizes average code word length

$$\sum_{i\in\mathcal{A}} p(i)\cdot|c(i)|,$$

where $p(i)$ denotes the probability of occurrence of $i \in \mathcal{A}$ and $c(i)$ denotes the mapping to a corresponding code word.

dns resource records

record type	use
`SOA`	(Start of Authority) marks the root of a zone
`NS`	specify the FQDNs of the authoritative NS of this zone
`A`	associate a FQDN with an IPv4 address
`AAAA`	associate a FQDN with an IPv6 address
`CNAME`	alias, references a canonical name, which itself is an FQDN
`MX`	associates a FQDN with a mail server
`TXT`	associates a FQDN with a string.
`PTR`	associates an IPv4 / IPv6 address with a FQDN (reverse DNS)

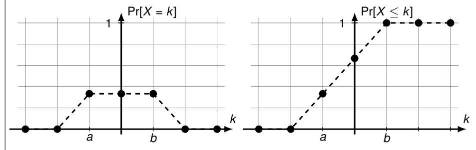
reverse DNS zones

IPv4: `in-addr.arpa.`, IPv6: `ip6.arpa.`

Probability Distributions

discrete uniform distribution: $X \sim \mathrm{U}(a,b)$:

Expresses the probability of the occurrence of a certain event out of several equally probable events, e.g. fair dice.



$\Pr[X = k] = \frac{1}{b - a + 1}$

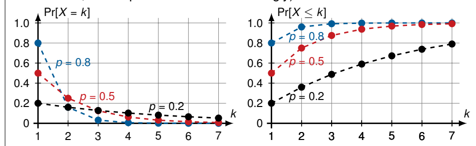
$\Pr[X \le k] = \frac{k - a + 1}{b - a + 1}$

$\mathrm{E}[X] = \frac{a + b}{2}$

$\mathrm{Var}[X] = \frac{(b - a + 1)^2 - 1}{12}$

geometric distribution: $X \sim \mathrm{Geo}(p)$:

Expresses a discrete-time waiting problem, e.g. the number of attempts until success (or the number of unsuccessful attempts until success, if the exponent is shifted accordingly).



$\Pr[X = k] = (1 - p)^{k-1}p$

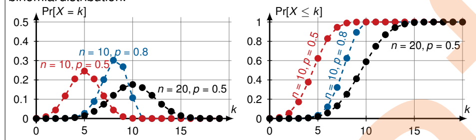
$\Pr[X \le k] = 1 - (1 - p)^k$

$\mathrm{E}[X] = \frac{1}{p}$

$\mathrm{Var}[X] = \frac{1 - p}{p^2}$

binomial distribution: $X \sim \mathrm{Bin}(n,p)$:

expresses the probability of $0 \le k \le n$ successes at constant probability of success p, e.g. lottery. For $n \to \infty$ and $p \to 0$ the Poisson distribution is obtained. For $n \ge 10$ and $p < 0.5$, the Poisson distribution can be used as a approximation for the binomial distribution.



$\Pr[X = k] = \binom{n}{k}p^k(1 - p)^{n-k}$

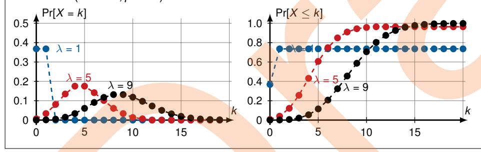
$\Pr[X \le k]$ *no short hand*

$\mathrm{E}[X] = np$

$\mathrm{Var}[X] = np(1 - p)$

Poisson Distribution: $X \sim \mathrm{Po}(\lambda)$:

Counts the occurrence of independent and equally distributed events with rate λ. Represents for $\lambda = np$ the limit of the binomial distribution ($n \to \infty, p \to 0$).



$\Pr[X = k] = \frac{\lambda^k}{k!}e^{-\lambda}$

$\Pr[X \le k]$ *no short hand*

$\mathrm{E}[X] = \lambda$

$\mathrm{Var}[X] = \lambda$