

Zabezpieczanie i Analiza Danych z Urządzeń Mobilnych

Wykład #2 – Technologie i protokoły komunikacyjne urządzeń mobilnych



Plan wykładu

- Dane a metadane
- Kodowanie, format, protokół
- Enkapsulacja, model warstwowy
- Protokoły sieciowe
 - Wi-Fi
 - Bluetooth
 - Protokoły warstwy aplikacji
- GSM i pochodne
- Protokoły peryferyjne

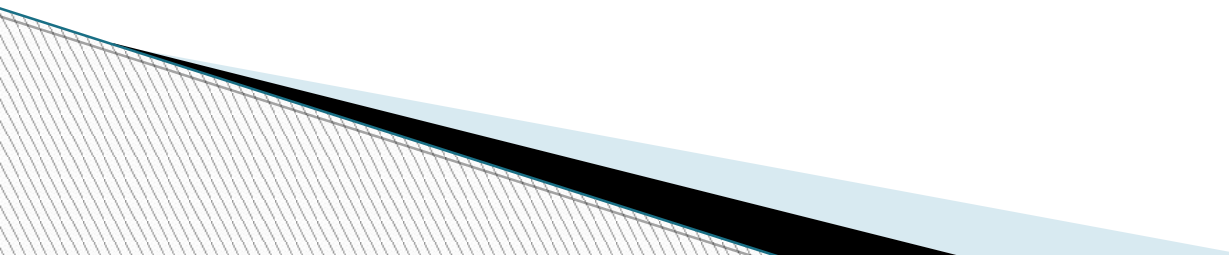
Dane a metadane

Z technicznego punktu widzenia

Do danych zaliczamy właściwą zawartość, której świadom jest każdy użytkownik, np:

- Tekst pliku tekstowego
- Wizja i fonia pliku multimedialnego
- Wizja pliku graficznego
- Wszystkie powyższe na np. stronie www
- Itd.

Do metadanych zaliczamy resztę; dane opisujące/odnoszące się do danych właściwych, np.:

- Informacje o rozmiarze, dacie modyfikacji, autorze
 - Nazwy, tytuły
 - Logi (zapis aktywności poszczególnych usług)
 - Billingi połączeń
 - Parametry uruchomieniowe
 - Itd..
- 

Dane a metadane

Z punktu widzenia informatyki śledczej

Jedne i drugie dane są równie cenne; bardzo często same metadane przenoszą wystarczającą ilość informacji, np.:

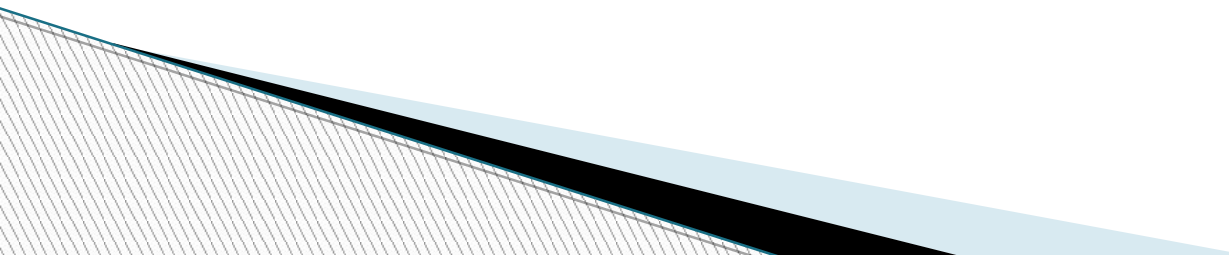
- „W aptece widać, że kupuję lek na astmę, choć diagnoza jest objęta tajemnicą lekarską”
- „Wziąłem urlop na żądanie, ale nikt nie wie, co robiłem wczoraj wieczorem”
- „Dzwoniłem na linię pomocy dla alkoholików, ale tajemnicą pozostaje, czego dotyczyła rozmowa”
- „Poszedłem na strzelnicę, ale nie wiadomo, co tam robiłem”
- Itd..

Kodowanie

Kodowanie można rozumieć jako funkcję:

- deterministyczną (dla tych samych danych wejściowych zawsze zwróci takie same dane wyjściowe)
- dwukierunkową (istnieje tryb kodujący i dekodujący)
- o niepustej dziedzinie i zbiorze wartości (zawsze istnieją dane wejściowe i wyjściowe)

Przykłady

- Kodowanie transmisji (CER, BER, DER)
 - Base64
 - Kompresja (np. kodowanie Huffmana)
 - Szyfrowanie
 - Kodowanie znaków (tzw. strona kodowa, charset)
 - Reprezentacja (np. zapis binarny, szesnastkowy)
 - Optymalizacja (np. format U2)
 - Reverse byte nibbling (GSM)
- 

Kodowanie - ASCII

Podstawowe ASCII (7 bitów)

Dec	Hx	Oct	Char	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr
0	0	000	NUL (null)	32	20	040	 	Space	64	40	100	@	@	96	60	140	`	`
1	1	001	SOH (start of heading)	33	21	041	!	!	65	41	101	A	A	97	61	141	a	a
2	2	002	STX (start of text)	34	22	042	"	"	66	42	102	B	B	98	62	142	b	b
3	3	003	ETX (end of text)	35	23	043	#	#	67	43	103	C	C	99	63	143	c	c
4	4	004	EOT (end of transmission)	36	24	044	$	\$	68	44	104	D	D	100	64	144	d	d
5	5	005	ENQ (enquiry)	37	25	045	%	%	69	45	105	E	E	101	65	145	e	e
6	6	006	ACK (acknowledge)	38	26	046	&	&	70	46	106	F	F	102	66	146	f	f
7	7	007	BEL (bell)	39	27	047	'	'	71	47	107	G	G	103	67	147	g	g
8	8	010	BS (backspace)	40	28	050	((72	48	110	H	H	104	68	150	h	h
9	9	011	TAB (horizontal tab)	41	29	051))	73	49	111	I	I	105	69	151	i	i
10	A	012	LF (NL line feed, new line)	42	2A	052	*	*	74	4A	112	J	J	106	6A	152	j	j
11	B	013	VT (vertical tab)	43	2B	053	+	+	75	4B	113	K	K	107	6B	153	k	k
12	C	014	FF (NP form feed, new page)	44	2C	054	,	,	76	4C	114	L	L	108	6C	154	l	l
13	D	015	CR (carriage return)	45	2D	055	-	-	77	4D	115	M	M	109	6D	155	m	m
14	E	016	SO (shift out)	46	2E	056	.	.	78	4E	116	N	N	110	6E	156	n	n
15	F	017	SI (shift in)	47	2F	057	/	/	79	4F	117	O	O	111	6F	157	o	o
16	10	020	DLE (data link escape)	48	30	060	0	0	80	50	120	P	P	112	70	160	p	p
17	11	021	DC1 (device control 1)	49	31	061	1	1	81	51	121	Q	Q	113	71	161	q	q
18	12	022	DC2 (device control 2)	50	32	062	2	2	82	52	122	R	R	114	72	162	r	r
19	13	023	DC3 (device control 3)	51	33	063	3	3	83	53	123	S	S	115	73	163	s	s
20	14	024	DC4 (device control 4)	52	34	064	4	4	84	54	124	T	T	116	74	164	t	t
21	15	025	NAK (negative acknowledge)	53	35	065	5	5	85	55	125	U	U	117	75	165	u	u
22	16	026	SYN (synchronous idle)	54	36	066	6	6	86	56	126	V	V	118	76	166	v	v
23	17	027	ETB (end of trans. block)	55	37	067	7	7	87	57	127	W	W	119	77	167	w	w
24	18	030	CAN (cancel)	56	38	070	8	8	88	58	130	X	X	120	78	170	x	x
25	19	031	EM (end of medium)	57	39	071	9	9	89	59	131	Y	Y	121	79	171	y	y
26	1A	032	SUB (substitute)	58	3A	072	:	:	90	5A	132	Z	Z	122	7A	172	z	z
27	1B	033	ESC (escape)	59	3B	073	;	;	91	5B	133	[[123	7B	173	{	{
28	1C	034	FS (file separator)	60	3C	074	<	<	92	5C	134	\	\	124	7C	174	|	
29	1D	035	GS (group separator)	61	3D	075	=	=	93	5D	135]]	125	7D	175	}	}
30	1E	036	RS (record separator)	62	3E	076	>	>	94	5E	136	^	^	126	7E	176	~	~
31	1F	037	US (unit separator)	63	3F	077	?	?	95	5F	137	_	_	127	7F	177		DEL

Source: www.LookupTables.com

Kodowanie - ASCII

Rozszerzone ASCII (do 8 bitów)

128	Ç	144	É	160	á	176	ð	192	Ł	208	Š	224	α	240	≡
129	ü	145	æ	161	í	177	ë	193	ł	209	ŧ	225	β	241	±
130	é	146	Æ	162	ó	178	ü	194	ŧ	210	ŧ	226	Γ	242	≥
131	â	147	ô	163	ú	179		195	ı	211	š	227	π	243	≤
132	ä	148	ö	164	ñ	180	†	196	—	212	š	228	Σ	244	∫
133	à	149	ò	165	Ñ	181	‡	197	+	213	ŕ	229	σ	245	∫
134	å	150	û	166	²	182	‡	198	†	214	ŕ	230	μ	246	÷
135	ç	151	ù	167	°	183	¶	199	‡	215	‡	231	τ	247	≈
136	ê	152	ÿ	168	¿	184	¶	200	¶	216	‡	232	Φ	248	°
137	ë	153	Ö	169	ƒ	185	¶	201	ŕ	217	∫	233	⊙	249	.
138	è	154	Û	170	ŕ	186	¶	202	š	218	ŕ	234	Ω	250	.
139	ï	155	©	171	½	187	¶	203	ŧ	219	■	235	δ	251	√
140	î	156	£	172	¼	188	¶	204	‡	220	■	236	∞	252	π
141	ì	157	¥	173	¡	189	¶	205	=	221	■	237	φ	253	²
142	Ä	158	£	174	«	190	¶	206	‡	222	■	238	ε	254	■
143	Å	159	ƒ	175	»	191	¶	207	±	223	■	239	∧	255	

Source: www.LookupTables.com

Kodowanie - base64

Kodowanie pozwalające na przedstawienie dowolnej wartości oktetu (bajtu) w formie znaków drukowanych (alfanumerycznych).

- Ze względu na fakt, że wszystkie oktety mają przestrzeń 256 wartości (2^8 ; od 0 do 255), a znaków alfanumerycznych jest 62 (zmieszczą się na 6 bitach), niemożliwe jest stworzenie mapowania 1:1
- Aby reprezentować 8-bitowe wartości 6-bitowymi sekwencjami, ciąg 8 bitowych wartości dzieli się na 6-bitowe elementy i wyraża ich wartości jako kolejne znaki alfanumeryczne
- Powoduje to, że ciąg wynikowy jest o 1/3 dłuższy niż ciąg oryginalny
- Ciąg bajtów, którego suma bitów nie jest podzielny przez 6, jest po przekodowaniu uzupełniany znakami „=”

Text content	M								a								n															
ASCII	77 (0x4d)								97 (0x61)								110 (0x6e)															
Bit pattern	0	1	0	0	1	1	0	1	0	1	1	0	0	0	0	1	0	1	1	0	1	1	1	0								
Index	19								22								5								46							
Base64-encoded	T								W								F								u							

[BASE64]

Kodowanie - base64

Tabela wartości dziesiętnych powstałych w wyniku interpretacji danych oryginalnych jako komórek sześciobitowych wraz z odpowiadającymi im znakami z zakresu alfanumerycznego uzupełnionego o „/” i „+”.

Value	Char	Value	Char	Value	Char	Value	Char
0	A	16	Q	32	g	48	w
1	B	17	R	33	h	49	x
2	C	18	S	34	i	50	y
3	D	19	T	35	j	51	z
4	E	20	U	36	k	52	0
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	J	25	Z	41	p	57	5
10	K	26	a	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	s	60	8
13	N	29	d	45	t	61	9
14	O	30	e	46	u	62	+
15	P	31	f	47	v	63	/

[BASE64]

Kodowanie - UTF-8

- Najpowszechniej stosowany schemat kodowania znaków tekstowych
- Pozwala na stosowanie znaków z dowolnego alfabetu
- Jeden znak reprezentowany jest przez 1-4 bajty
- Informacja o ilości bajtów należących do obecnie definiowanego znaku znajduje się w pierwszym bajcie
- Kompatybilny z ASCII
- Częściej występujące znaki mają przypisane niższe wartości (co optymalizuje objętość tekstów zapisanych w UTF-8)

Bits of code point	First code point	Last code point	Bytes in sequence	Byte 1	Byte 2	Byte 3	Byte 4	Byte 5	Byte 6
7	U+0000	U+007F	1	0xxxxxxx					
11	U+0080	U+07FF	2	110xxxxx	10xxxxxx				
16	U+0800	U+FFFF	3	1110xxxx	10xxxxxx	10xxxxxx			
21	U+10000	U+1FFFFF	4	11110xxx	10xxxxxx	10xxxxxx	10xxxxxx		

Kodowanie - SMS-y (7 bit GSM, UTF-16)

	0	1	2	3	4	5	6	7
0	@	Δ	SP	0	i	P	z	p
1	£	_	!	1	A	Q	a	q
2	\$	Φ	"	2	B	R	b	r
3	¥	Γ	#	3	C	S	c	s
4	è	Λ	α	4	D	T	d	t
5	é	Ω	%	5	E	U	e	u
6	ù	Π	&	6	F	V	f	v
7	ì	Ψ	'	7	G	W	g	w
8	ò	Σ	(8	H	X	h	x
9	ç	Θ)	9	I	Y	i	y
A	LF	Ξ	*	:	J	Z	j	z
B	Ø	Note 1	+	;	K	Ä	k	ä
C	ø	Æ	,	<	L	Ö	l	ö
D	CR	æ	-	=	M	Ñ	m	ñ
E	Å	ß	.	>	N	Û	n	ü
F	å	É	/	?	O	Š	o	à

- Zgodnie ze standardem GSM 03.38 SMS-y tekst SMS-ów jest kodowany zgodnie z alfabetem mieszczącym się na 7 bitach
- Nie jest on w pełni kompatybilny z ASCII, ale litery alfabetu łacińskiego mają w obydwóch alfabetach te same wartości
- Większość klasycznych telefonów w tej samej formie przechowuje wiadomości w swojej pamięci (to samo dotyczy karty SIM)

Np.:

t = 74 = 7*16+4 = 116 (ASCII i GSM)

z = 7A = 7*16+10 = 122 (ASCII i GSM)

Ale już:

` (ASCII) = 60 = 96, w GSM jest to odwrócony znak zapytania ?

Najstarszy, nieużywany bit jest zazwyczaj wypełniany jedynką.

W przypadku wprowadzenia do wiadomości znaku spoza tego zakresu, telefon automatycznie przechodzi na kodowanie UTF-16 (dawniej UCS-2), w którym każdy znak zajmuje 2 bajty - ogranicza to automatycznie długość SMS-a ze 140 do 70 znaków.

Kodowanie - GSM reverse byte nibbling

Dane w GSM zapisane i transmitowane są w kolejności określonej terminem **reverse byte nibbling**. Oznacza to, że każde dwa kolejne sąsiadujące bajty (a czasami półbajty) zapisane są w kolejności odwrotnej.

Dla przykładu następujący numer ICCID:

8948031452966687483

w pamięci telefonu (jak i karty SIM) zapisany jest jako

988430412569667884F3

Szczególnie polecane źródło: [GSM SMS]



GSM - format przechowywania dat

TP-SCTS (Service Centre Time Stamp) [7 BIT FORENSICS]

Przykład:

Oryginalna postać rekordu: 9001425100704A

Po odwróceniu (reverse byte nibbling): 09 10 24 15 00 70
A4

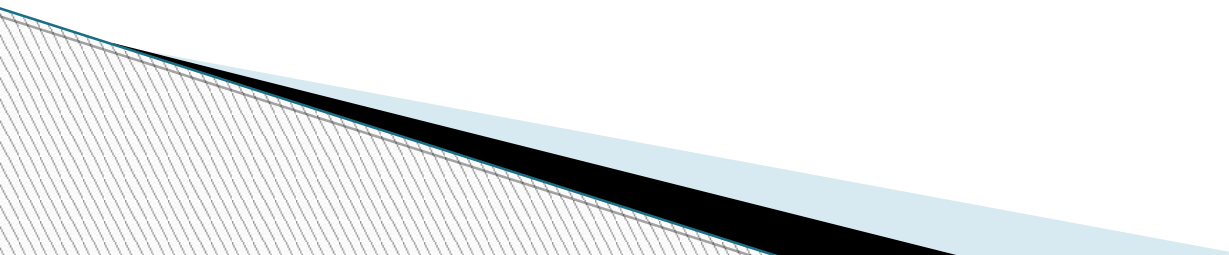
Oznacza: 2009-10-24 15:00:07

- Ostatni bajt oznacza offset w stosunku do UTC/GMT (dla przypomnienia, dla Polski ten offset wynosi 2):
- Oryginalnie: 4A
- Po odwróceniu: A4
- Binarnie: 10100100
- Jeśli najstarszy bit (najbardziej w lewo)=1, oznacza to minus; -010 0100 = -24
- Offset wyrażony jest w KWADRANSACH, co dla powyższego przykładu daje -6 (wschodnie wybrzeże USA)

Format danych

- Zestaw reguł definiujących
 - poprawną gramatykę (składnię)
 - Interpretację (semantykę, logikę) danych zgodnych z ową składnią

Typy formatów danych

- Kodowania
 - Metaformaty (np. ASN.1)
 - Systemy plików (przechowywanie)
 - Formaty plików (przechowywanie, transport)
 - Protokoły (transport)
- 

Protokół komunikacyjny

Zestaw reguł określających język komunikacji, w tym:

- transport (przekaz danych)
- koordynację (synchronizację)
- semantykę (znaczenie), format danych (w tym kodowanie)

Podział na warstwy i enkapsulacja



[MATRIOSZKA]

Analogia enkapsulacji: list pocztowy

1. Tekst (dane właściwe) zapisany długopisem na papierze (nośnik)
2. Koperta (podstawowe opakowanie nośnika)
3. Worek/skrzynia (opakowanie do transportu między urzędami pocztowymi)
4. Samochód/pociąg/samolot (transport pomiędzy urzędami pocztowymi)

Warto zwrócić uwagę na fakt, że koperta przed otwarciem przez adresata może zostać wielokrotnie przepakowana między skrzyniami, a skrzynie między pojazdami.

Podział na warstwy; enkapsulacja

- To samo zjawisko ma zastosowanie dla danych elektronicznych
- Poziomy opakowania określa się mianem warstw
- Każda warstwa ma swoje przeznaczenie
- Opakowanie danej warstwy = protokół danej warstwy
- Następuje zjawisko narzutu (na każdej warstwie doklejane są metadane odpowiedniego protokołu)
- Pełen rozmiar przenoszonych danych = oryginalne dane + nagłówki protokołów
- Analogicznie towar/przesyłka waży więcej z opakowaniem
- W praktyce większość faz enkapsulacji polega po prostu na doklejeniu kolejnej porcji danych (nagłówki/metadane protokołu), bez dodatkowej transformacji danych z warstw wyższych (np. zaszyfrowania, zakodowania – transformacji, która utrudnia przeszukanie danych przez zignorowanie warstw niższych)

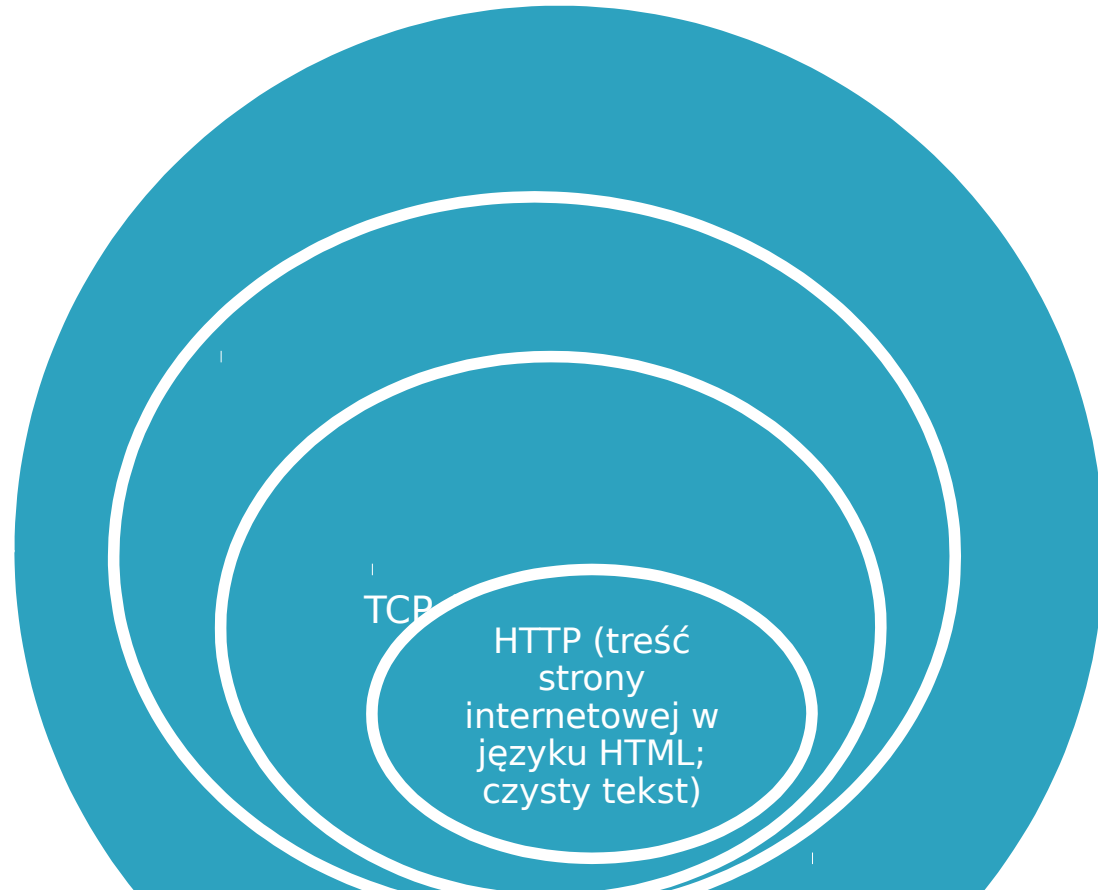


Model OSI/ISO oraz TCP

Warstwa		Jednostka danych	Pełniona rola
Model TCP	Model OSI/ISO		
Aplikacji	Aplikacji	Bajt	Protokół indywidualny dla programu + właściwe dane
	Prezentacji	Bajt	Szyfrowanie, kodowanie, kompresja
	Sesji	Bajt	Sesje między aplikacjami
Transportu	Transportu	Segment	Integralny transport danych
Warstwa sieciowa	Sieci	Pakiet	Routing, adresacja
Warstwa dostępu do sieci	Łącza danych	Ramka	Transport danych typu punkt<->punkt
	Fizyczna	Bit	Transport danych typu punkt <-> punkt, fizyczna reprezentacja danych

Przykład enkapsulacji

Narzut do warstwy aplikacji = 467
- 413 = 54 bajty
Narzut HTTP=413-19
(/dynaform/custom.js)=393 bajty



```
< Frame 1074: 467 bytes on wire (3736 bits), 467 bytes captured (3736 bits) on interface 0
+ Ethernet II, Src: IntelCor_34:15:6e (84:3a:4b:34:15:6e), Dst: Tp-LinkT_a1:94:e0 (64:70:02:a1:94:e0) adresy MAC
+ Internet Protocol Version 4, Src: 192.168.0.104 (192.168.0.104), Dst: 192.168.0.1 (192.168.0.1) adresy IP
+ Transmission Control Protocol, Src Port: 51221 (51221), Dst Port: postgresql (5432), Seq: 1, Ack: 1, Len: 413
```

```
0000 64 70 02 a1 94 e0 84 3a 4b 34 15 6e 08 00 45 00
0010 01 c5 65 1a 40 00 80 06 12 5f c0 a8 00 68 c0 a8
0020 00 01 c8 15 15 38 26 89 56 af 5d 94 89 76 50 18
0030 11 1c cd 4d 00 00 47 45 54 20 2f 64 79 6e 61 66
0040 6f 72 6d 2f 63 75 73 74 6f 6d 2e 6a 73 20 48 54
0050 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 31 39
0060 32 2e 31 36 38 2e 30 2e 31 3a 35 34 33 32 0d 0a
0070 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70
0080 2d 61 6c 69 76 65 0d 0a 41 75 74 68 6f 72 69 7a
0090 61 74 69 6f 6e 3a 20 42 61 73 69 63 20 59 57 52
00a0 74 61 57 34 36 63 6e 70 35 5a 32 46 74 61 33 4a
00b0 33 61 57 45 3d 0d 0a 41 63 63 65 70 74 3a 20 2a
00c0 2f 2a 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20
00d0 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e
00e0 64 6f 77 73 20 4e 54 20 36 2e 31 3b 20 57 4f 57
00f0 36 34 29 20 41 70 70 6c 65 57 65 62 4b 69 74 2f
0100 35 33 37 2e 33 36 20 28 4b 48 54 4d 4c 2c 20 6c
0110 69 6b 65 20 47 65 63 6b 6f 29 20 43 68 72 6f 6d
```

```
dp.....: K4.n..E.
..e.@... ..h..
.....8& V.]..vP.
...M..GE T /dynaf
orm/cust om.js HT
TP/1.1.. Host: 19
2.168.0. 1:5432..
Connecti on: keep
-alive.. Authoriz
ation: B asic YwB
3awE=..A ccept: *
/*..User -Agent:
Mozilla/ 5.0 (win
dows NT 6.1; wow
64) Appl ewebKit/
537.36 ( KHTML, l
ike Geck o) chrom
```



HTTP (żądanie
/dynaform.custom.js,
z przeglądarki
Chrome)

Protokoły sieciowe

warstwa dostępu do sieci

Ethernet (IEEE 802.3)

- medium przewodowe
- najpopularniejszy (nie tylko sieci lokalne)
- pierwszy protokół używający adresów MAC (Media Access Control), 48 bitów
- MTU 1500 bajtów



[1]

Ethernet_II

Preamble 8 bytes	DA 6 bytes	SA 6 bytes	Type 2 bytes	Data	FCS 4 bytes
---------------------	---------------	---------------	-----------------	------	----------------

802.3_Ethernet

Preamble 8 bytes	DA 6 bytes	SA 6 bytes	Length 2 bytes	Data	FCS
---------------------	---------------	---------------	-------------------	------	-----

802.3 and Ethernet frame formats

[2]

Protokoły sieciowe

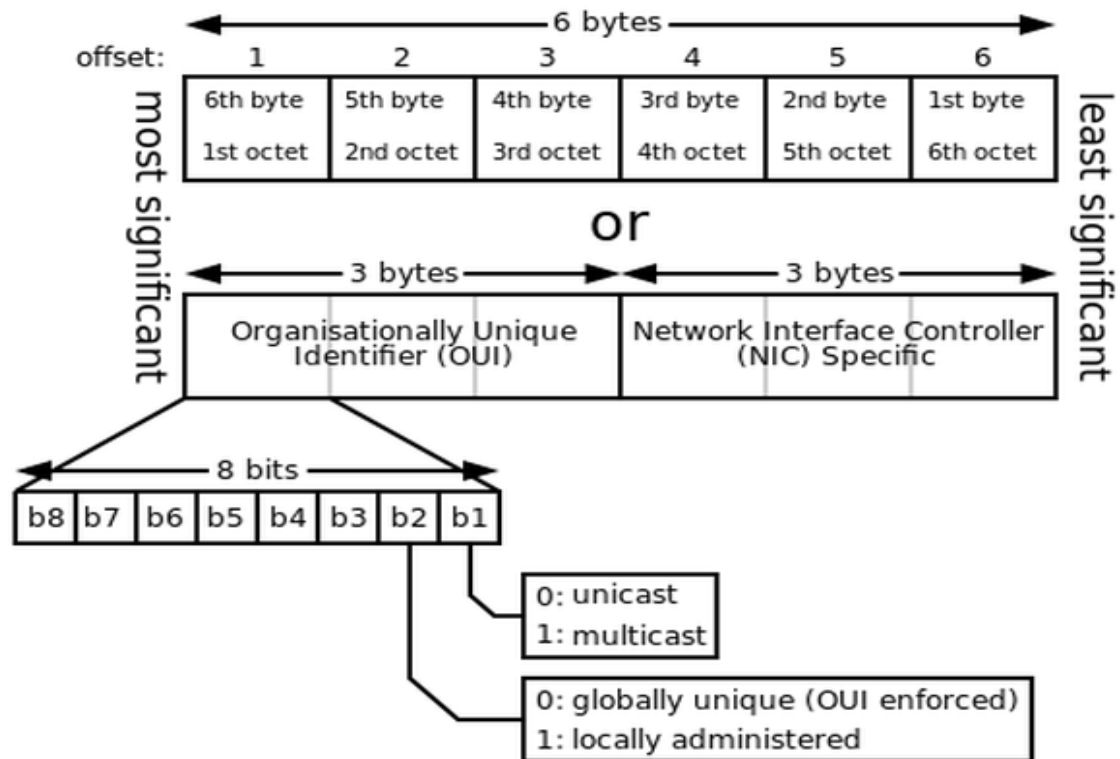
warstwa dostępu do sieci - adres MAC (Media Access Control)

- 6 bajtów
- Unikalny dla każdego urządzenia (karty sieciowej)
- Stały dla każdego urządzenia (zaprogramowany w ROM, BIA – Burned In Address)
- Zawiera informację o producencie karty sieciowej (pozwala wstępnie zidentyfikować sprzęt)
- Używany również w innych protokołach warstwy łącza danych/dostępu do sieci (np. Wi-Fi, Bluetooth, Token Ring)
- Uniwersalny adres rozgłoszeniowy FF:FF:FF:FF:FF
- Bez przeszkód można „nadpisać” go programowo (tzn. wysyłać ramki z takim adresem źródłowym, jaki chcemy)
- Istnieje również standard EUI-64 (64 bitowe adresy MAC, standardowe mają 48)
- Adresy MAC przemieszczają się jedynie w obrębie tzw. domeny kolizji (w obszarze połączonych switchy/access pointów), nie wykraczają poza tę samą sieć IP

Protokoły sieciowe

warstwa dostępu do sieci - adres MAC (Media Access Control)

Sekcje w adresie MAC



Protokoły sieciowe

warstwa dostępu do sieci - Wi-Fi

Łączność radiowa

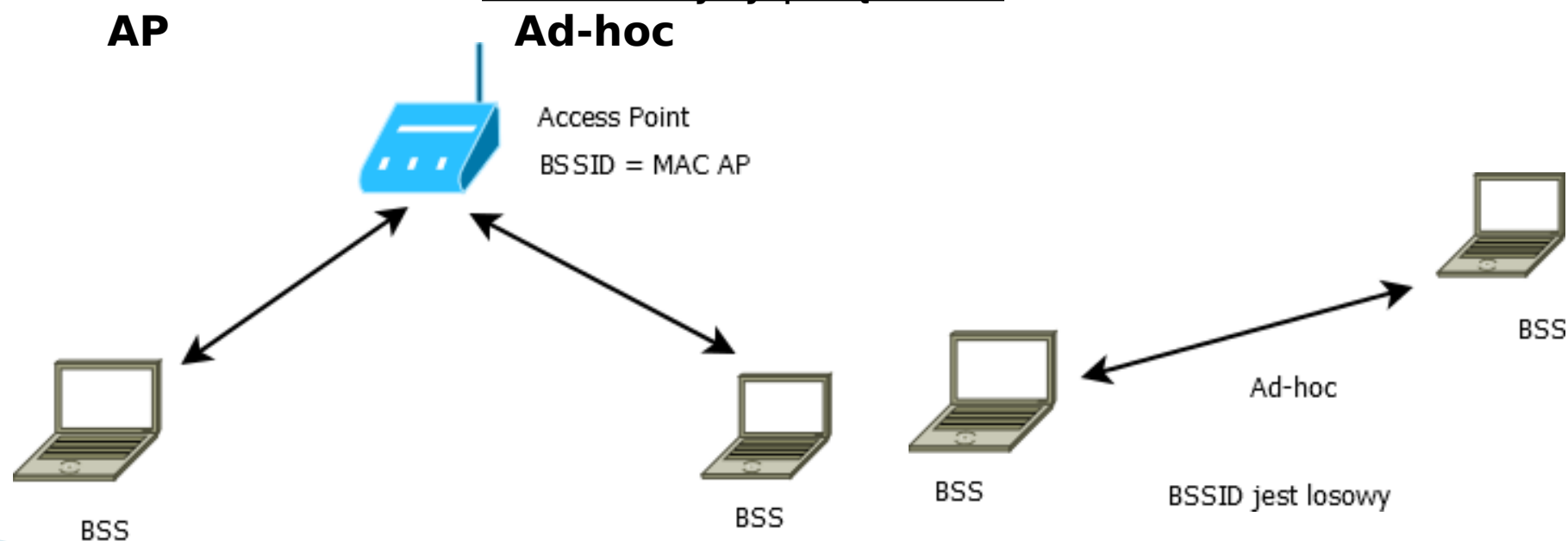
BSS – adres MAC klienta

SSID/ESSID – nazwa sieci WLAN (max. 32 znaki)

BSSID – adres MAC punktu dostępowego



Możliwe tryby połączenia



Protokoły sieciow

warstwa dostępu do sieci - Wi-Fi



Standardy, częstotliwości, przepustowość

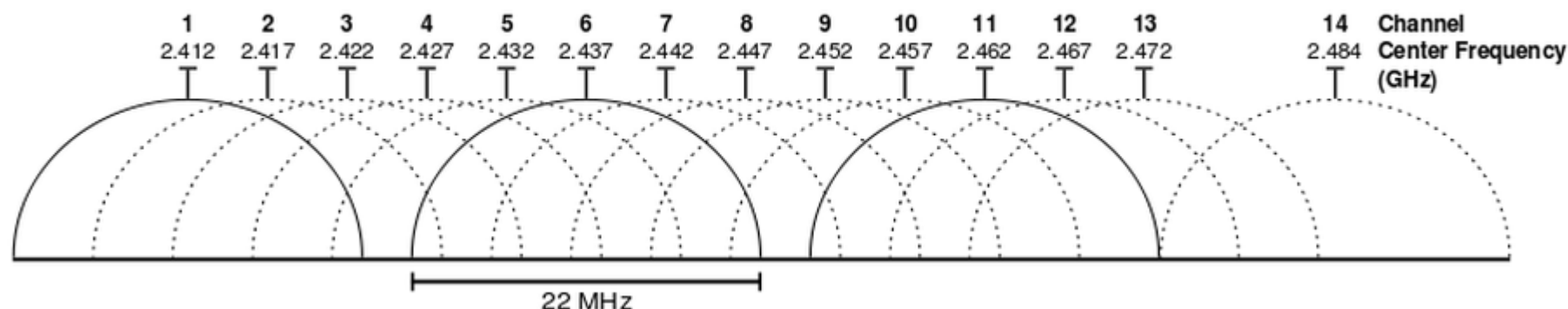
Standard	Pasmo	Max przepustowość
802.11a	5-6GHz, 13 nienachodzących kanałów (mało zatłoczone pasmo), kanał o szer. 20-25 Mhz	54 Mbps
802.11b	2.4-2.45 GHz, kanał o szer. 20-25 Mhz	11 Mbps
802.11g	2.4-2.45 GHz (wstecznie kompatybilny z b), kanał o szer. 20-25 Mhz	54 Mbps
802.11n	2.4-2.45 & 5 GHz, kanał o szerokości 40MHz	54-600 Mbps, MIMO

Protokoły sieciow

warstwa dostępu do sieci - Wi-Fi



Kanały 802.11b/g (w U.S. 1, 6, 11 z szerokością 25 MHz, w Europie (1, 5, 9, 13) o szerokości 20 MHz



[4]

Pasmo wi-fi jest bardzo zatłoczone, co powoduje liczne zakłócenia (telefony komórkowe, mikrofalówki, bluetooth itd.)

Protokoły sieciowe

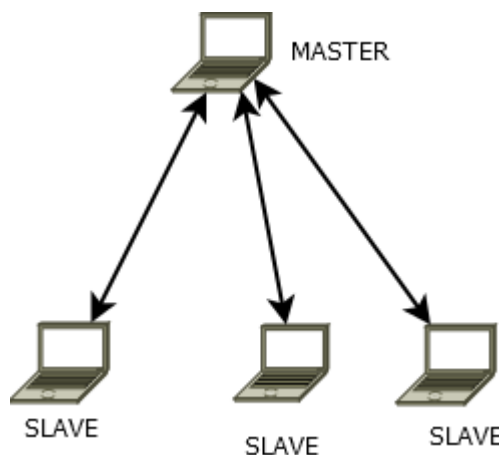
warstwa dostępu do sieci - Bluetooth



Bluetooth

Pasmo 2.4-2485 GHz
Krótki zasięg (kilka metrów)

Architektura master-slave (tzw. „piconet”, 1 master i do 7 slave (3 bitowa przestrzeń adresowa))



Zastosowania:

- Transfer plików
- Transfer multimediów (np. słuchawki, audio streaming)
- Sterowanie telefonem (handsfree calling)
- Urządzenia peryferyjne (np. klawiatury/myszki)
- Wraz z bluetooth 4.0 pojawił się BLE (Bluetooth Low Energy) wykorzystywany obecnie w beaconach

IP - Internet Protocol

(warstwa sieciowa)



- Głównym zadaniem protokołu IP jest dostarczenie skalowalnego systemu adresacji
- Powszechna w użyciu jest wersja 4 z 32 bitowymi adresami (4 bajty, nazywane często zamiennie oktetami)
- W czytelnym zapisie poprawny adres IP (w wersji 4) to 4 liczby od 0 do 255 oddzielone kropkami
- Adresy 10.0.0.0–10.255.255.255, 172.16.0.0–172.31.255.255, 192.168.0.0–192.168.255.255 używane są jako tzw. adresy prywatne/lokalne
- Inne specjalne adresy to m. in.
 - 127.0.0.0-127.255.255.255 localhost
 - 169.254.0.0/16 link-local
- Pozostałe to adresy globalne, teoretycznie unikalne dla każdego komputera

Protokoły sieciowe - warstwa transportowa

TCP - Transmission Control Protocol

- Zapewnia dotarcie danych w odpowiedniej kolejności
- Posiada mechanizm kontroli przepływu danych (szybkości transferu)
- Posiada mechanizm weryfikowania, czy segment został dostarczony (potwierdzenia, utrzymywanie sesji)
- Stosunkowo duży narzut nagłowa

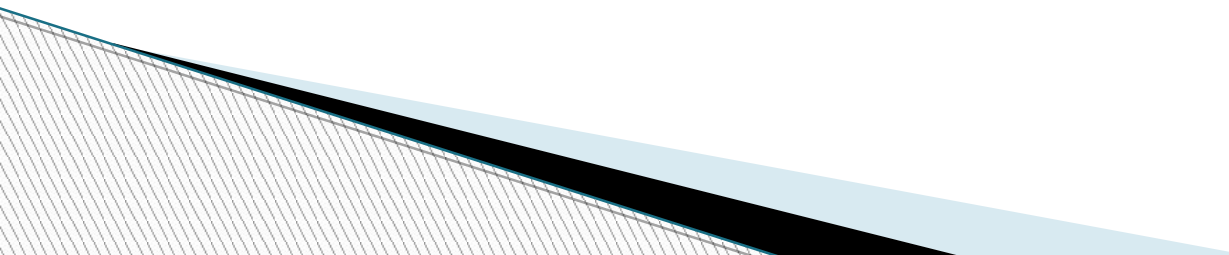
UDP - Universal Datagram Protocol

- Prosty, bezpołączeniowy (bez sesji)
- Nie zapewnia dotarcia danych w odpowiedniej kolejności
- Nie posiada mechanizmu weryfikacji, czy segment został dostarczony
- Szybszy od TCP ze względu na brak konieczności otrzymywania potwierdzeń

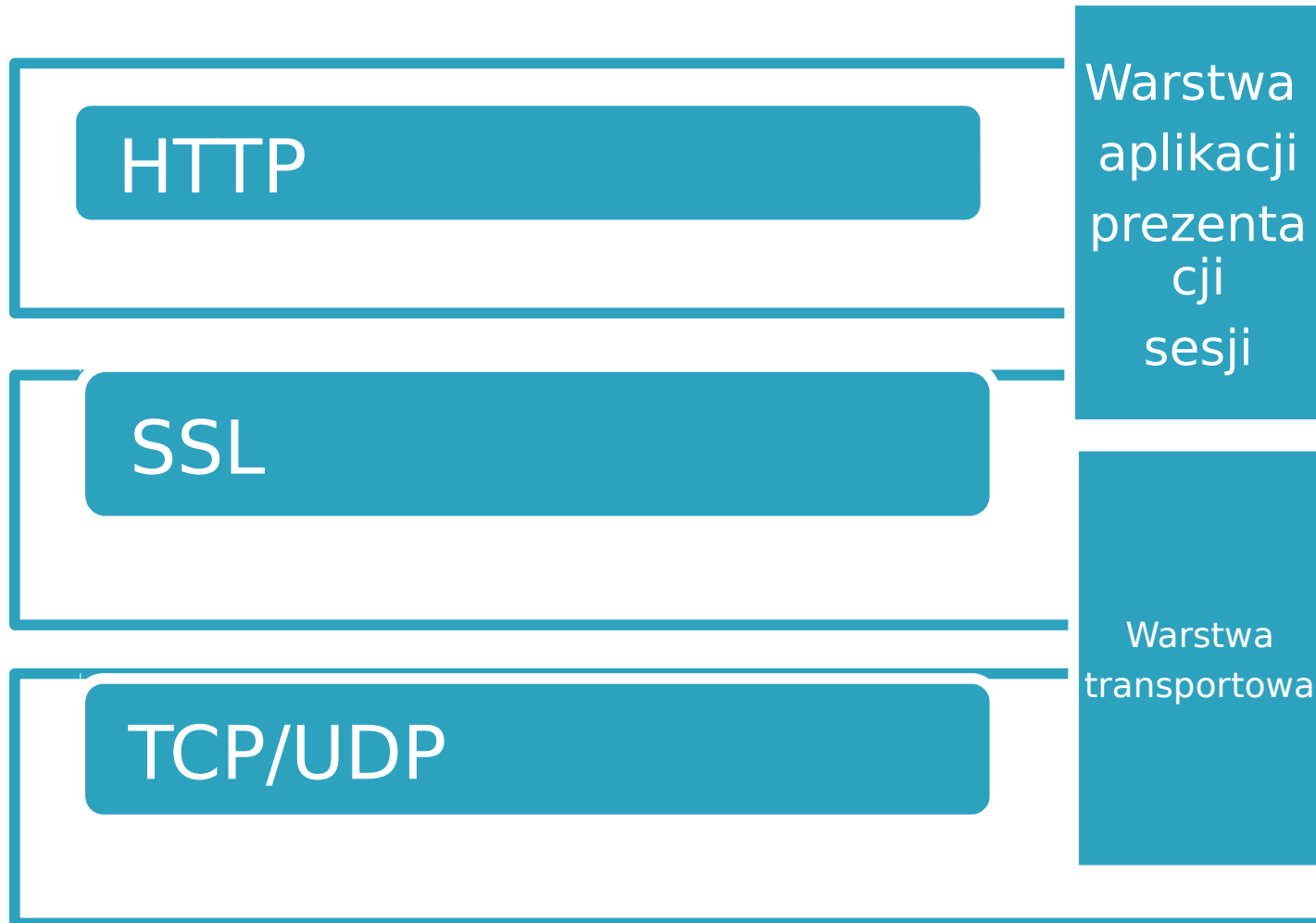
SCTP - Stream Control Transmission Protocol

- rzadko spotykany protokół warstwy transportowej, hybryda TCP i UDP

Protokoły sieciowe - warstwa aplikacji - przykłady

- HTTP
 - SMTP
 - POP3
 - IMAP
 - FTP
 - CIFS
 - TOR
 - Torrent
 - RDP
 - SIP
 - RTP
 - Skype
- 

Protokoły sieciowe - warstwa aplikacji - SSL



Protokoły sieciowe - warstwa aplikacji - VoIP

- Zestaw protokołów łączących komputery z telekomunikacją
- Dostarcza nowych możliwości interakcji między komputerami (w tym komputerami mobilnymi) a telefonią komórkową i telefonią PSTN

Najpopularniejszy zestaw protokołów (warstwa aplikacji):

- SIP + RTP
- Skype

SIP - Session Initiation Protocol

- Składnią oparty o HTTP
- Jego zadaniem jest nawiązywanie i kontrola połączeń
- Zazwyczaj transportowany przez UDP

RTP - Realtime Protocol

- Jego zadaniem jest transport strumienia głosowego
 - Zazwyczaj transportowany przez UDP
- 

GSM (Global System for Mobile Communications)

GSM odnosi się przede wszystkim do całego zestawu protokołów zapewniających komunikację **głosową**, ale także do rozwiniętych wokół niego technologii służących do transmisji danych

Generacje

1G – historyczny, analogowy standard komunikacji mobilnej

2G – cyfrowe połączenia telefoniczne, wiadomości SMS (GSM oraz CDMA*)

2.5G – GPRS (General Packet Radio Service), cyfrowa transmisja danych

3G – zestaw technologii dostarczający lepszej jakości usług transmisji zarówno głosu jak i danych (UMTS, EGPRS, EDGE, HSPA, HSPA+)

4G – LTE (Long Term Evolution), wykorzystuje oddzielną architekturę sprzętową

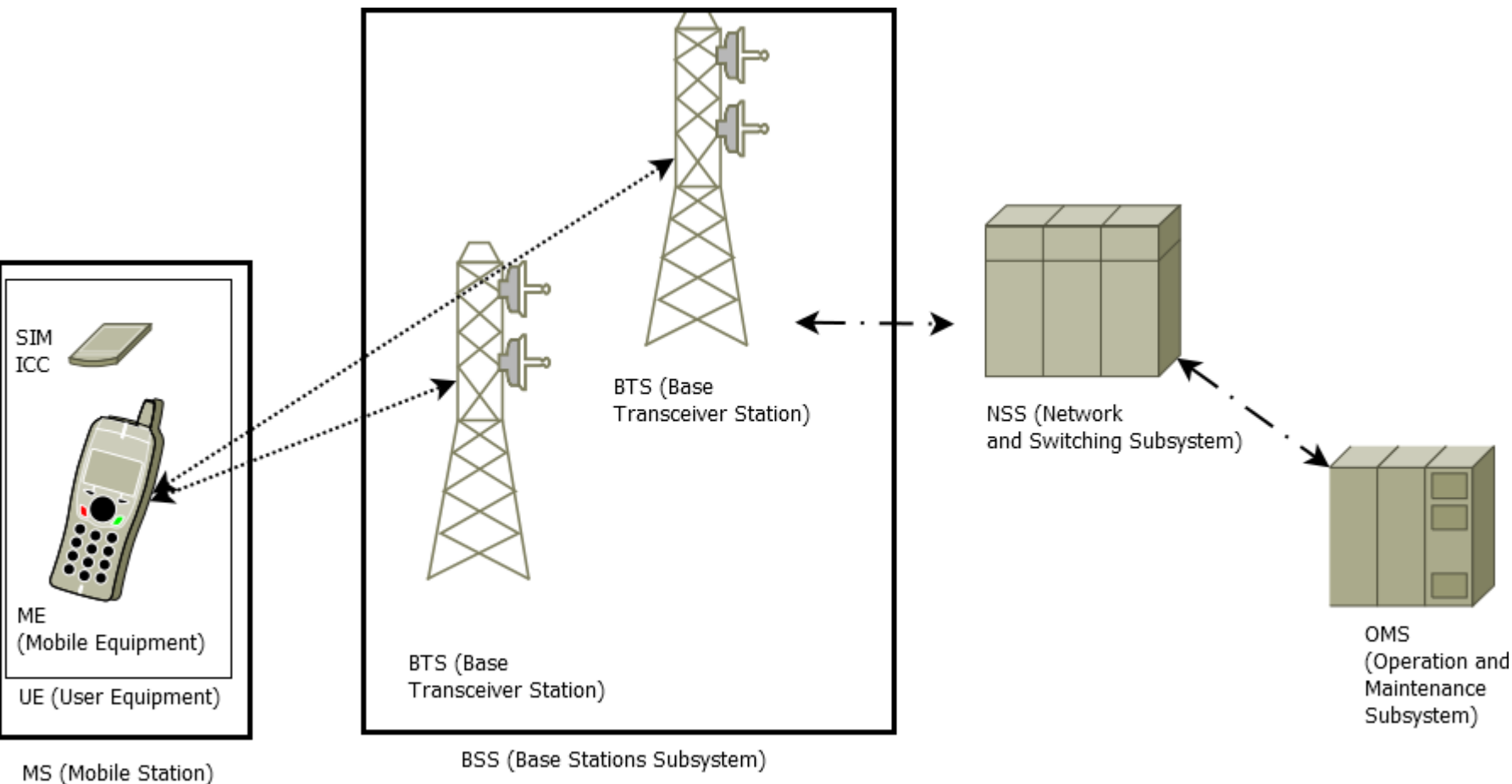
Z punktu widzenia protokołów, kodowania itd. GSM 2G różni się od GSM 3G tylko i wyłącznie radiem.

* CDMA jest popularne wyłącznie w USA

GSM – telefonia komórkowa

Uproszczony schemat sieci komórkowej

BTS – odpowiada za łączność między sprzętem mobilnym i resztą sieci
NSS – odpowiada za łączność sieciową abonenta między BTS-ami a OMS, odpowiada za przełączanie lokalizacji podczas przemieszczania się zalogowanego abonenta
OMS – odpowiada za identyfikację, uwierzytelnianie i autoryzację abonentów



[GSM ARCH]

GSM – najważniejsze skróty

MSISDN – numer telefonu

PLMN – Public Land Mobile Network (operator)

LND – ostatnio wybrany numer

SMS – Short Message Service

ADN – Abbreviated Dialing Numbers (lista numerów popularnych usług (np. połączenia alarmowe) oraz lista kontaktów)

LOCI – zbiorcze informacje o lokalizacji (zawiera TMSI, LAI oraz TMSI TIME)

TMSI (Temporary Mobile Subscriber Identity), generowany losowo jednorazowy klucz uwierzytelnionej sesji GSM

LAI – Location Area Information/Location Area Identifier- informacje o lokalizacji punktu dostępowego (BTS)

GSM - najważniejsze pojęcia

ICCID - Integrated Circuit Card ID

- Identyfikuje kartę SIM
- ICCID - 19 cyfr, można odczytać bez znajomości PIN/PUK
- 2 cyfry - urządzenie mobilne (89)
- 2 cyfry - kod kraju (48 dla PL)
- 2 cyfry - kod operatora
- 2 cyfry - rok wydania karty
- 10 cyfr - unikalny numer karty (znajduje się również w IMSI)

- Ostatnia cyfra - suma kontrolna
- Zazwyczaj nadrukowany i widoczny na karcie

IMSI - International Mobile Subscriber Identity

- Identyfikuje konkretnego abonenta (wraz z numerem IMEI jest wykorzystywany przy logowaniu do sieci GSM)
- Możliwy do odczytania z karty SIM po podaniu PIN/PUK
- 3 cyfry - kod kraju (MCC/MSC, 260 dla Polski)
- 2 cyfry - kod operatora (MNC), np.:
 - 01 Plus
 - 02 T-Mobile
 - 03 Orange
 - 06 Play
- 2 cyfry - HLR (Home Location Register, wewnętrzna jednostka organizacyjna operatora)
- 9 cyfr - kod abonenta (MSIN)

GSM – ICCID a IMSI

ICCID – Integrated Circuit Card ID

89 48 03 14 52966687483

89 – mobile telecom
48 – Polska
03 – Orange
14 – rok wydania karty (2014)
52**96668748** – kod abonenta
3 – suma kontrolna

IMSI – International Mobile Subscriber Identity

260 03 2996668748

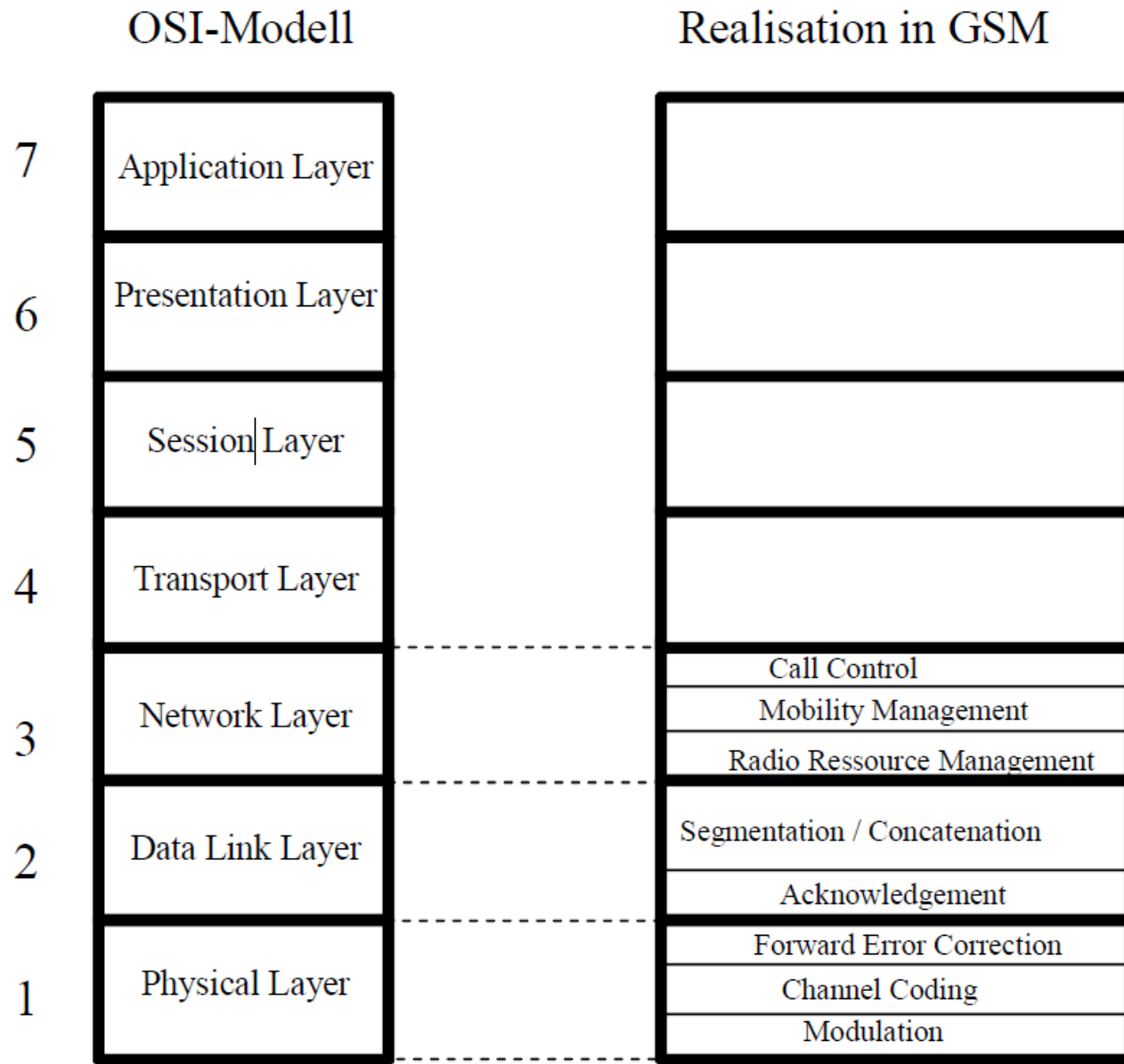
260 – Polska
03 – Orange
29 – HLR
96668748 – kod abonenta

Kolorem zaznaczono elementy wspólne (okazuje się, że przy znajomości ICCID zakres możliwych numerów IMSI ogranicza się do 99 możliwości – trafienie w numer HLR (Home Location Register))

GSM – SMS

- Protokół SMS zdefiniowany jest w standardach GSM 03.40 i 03.41
- Class 0 SMS (pierwotnie SMS służył jedynie operatorom do przekazywania informacji abonentom; później rozszerzono usługę)
- Tzw. binarne SMS-y (nieczytelne bezpośrednio jako tekst), zastosowanie:
 - OTA/OTASL (Over The Air/Over The Air Software Loading)
 - MMS (Multimedia Message Service) – MMS to specjalne SMS-y zawierające odnośniki do treści multimedialnej, która umieszczona jest na serwerach HTTP operatora i odczytywana za pośrednictwem WAP w momencie otwarcia MMS-a przez użytkownika
 - Inne [BINARY SMS]

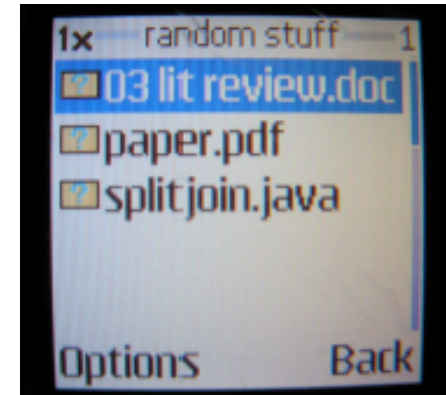
GSM w odniesieniu do modelu OSI



[GSM PROTOCOL STACK]

Protokoły peryferyjne

- Fizyczne
 - USB
 - RS-232
 - SD
 - ATA
 - SCSI
- Najczęściej stosowane w urządzeniach mobilnych
 - SyncML
 - OBEX
 - F-BUS
 - AT
 - Inne



OBEX
[AUSTRALIAN, p 20]

Odnośniki

Lista odnośników dostępna pod adresem:
https://github.com/ewilded/mobile/W2_URLs.txt