

Мрежова сигурност

Datalink and Network
layer security #1

Боян Кроснов

boyan@krosnov.org

<http://boyan.krosnov.org/>

Кой съм аз

- Свободен консултант, асоцииран с
 - Делян Делчев, Михаил Михайлов и компания
 - Индустрия
 - други
- За свободен софтуер, свобода на словото, достъпа до информация и т.н, както и Хуманизъм, Neurodiversity, etc.
- CCIE #8701 (Януари 2002)

Увод

- Какво е сигурност ?
 - надеждност/безотказност
 - предсказуемост/повторимост
 - дискретност
 - достоверност
 - права
- Защо сигурност ?
- Защо основни познания ?

Лекцията

- Мрежови модели
- Често срещани протоколи
- Стандартни организации
- Инструменти и примери

- Ethernet
 - рамка
 - принципи на работа
 - уязвимости

Слоести ...



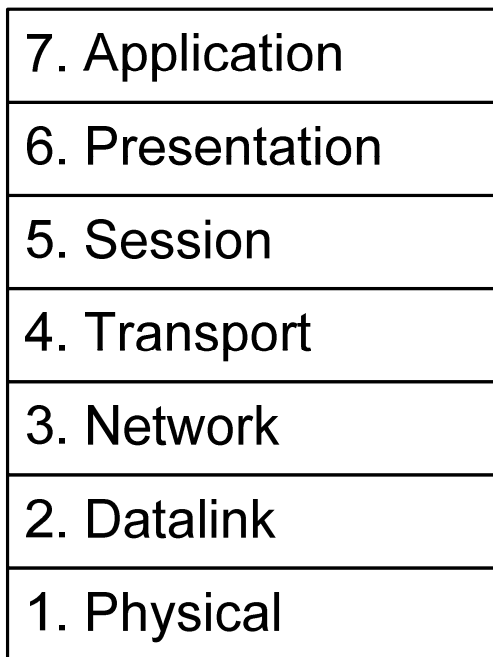
Слоести мрежови модели

OSI

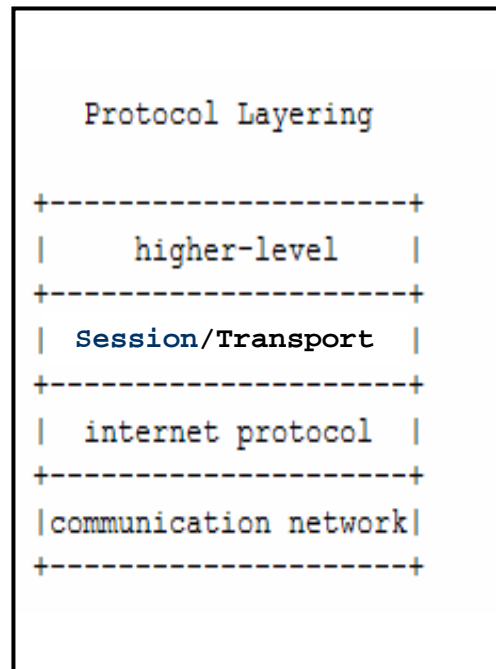
7. Application
6. Presentation
5. Session
4. Transport
3. Network
2. Datalink
1. Physical

Моделите

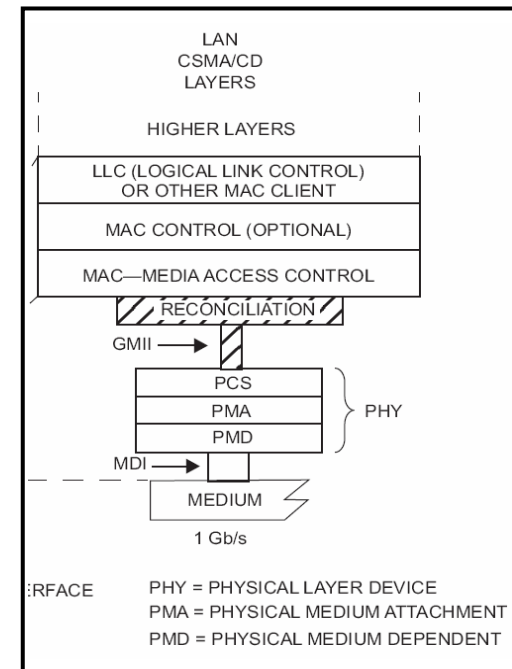
OSI

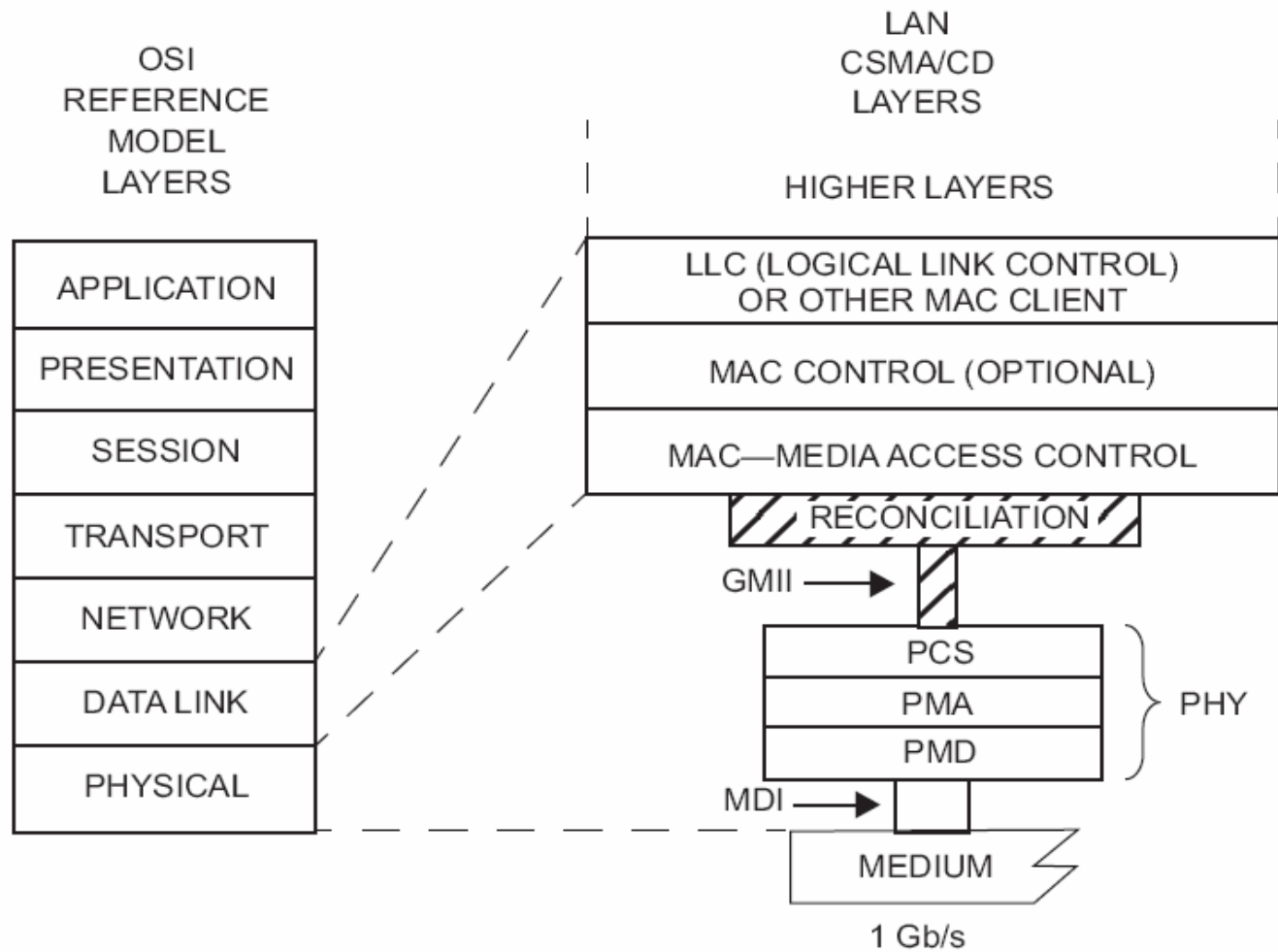


IETF



IEEE





GMII = GIGABIT MEDIA INDEPENDENT INTERFACE
 MDI = MEDIUM DEPENDENT INTERFACE
 PCS = PHYSICAL CODING SUBLAYER

PHY = PHYSICAL LAYER DEVICE
 PMA = PHYSICAL MEDIUM ATTACHMENT
 PMD = PHYSICAL MEDIUM DEPENDENT

Протоколи

7. HTTP, FTP, SMTP, POP3, IMAP4, SIP, XMPP, IRC, SNMP, SSH, TELNET, DNS, NTP, DHCP

4 and 5. TCP, UDP, RTP

3. IP/IPv6

2. Ethernet (802.3) , 802.11, 802.15, 802.16, PPP

1. baseband, *PSK, QAM-*, OFDM, CDMA, etc. over Cat5, Fiber, HFC, phone line, RF etc.

Протоколи

7. HTTP, FTP, SMTP, POP3, IMAP4, SIP, XMPP, IRC, SNMP, SSH, TELNET, DNS, NTP, DHCP		6? SSL / TLS	
4 and 5. TCP, UDP, RTP		3.5? – IGMP, MLD	
3. IP/IPv6	3? – ICMP	2.5? – ARP	
2. Ethernet (802.3), 802.11, 802.15, 802.16, 802.17, 802.18, 802.19, 802.20, 802.21, 802.22, 802.23, 802.24, 802.25, 802.26, 802.27, 802.28, 802.29, 802.30, 802.31, 802.32, 802.33, 802.34, 802.35, 802.36, 802.37, 802.38, 802.39, 802.40, 802.41, 802.42, 802.43, 802.44, 802.45, 802.46, 802.47, 802.48, 802.49, 802.50, 802.51, 802.52, 802.53, 802.54, 802.55, 802.56, 802.57, 802.58, 802.59, 802.60, 802.61, 802.62, 802.63, 802.64, 802.65, 802.66, 802.67, 802.68, 802.69, 802.70, 802.71, 802.72, 802.73, 802.74, 802.75, 802.76, 802.77, 802.78, 802.79, 802.80, 802.81, 802.82, 802.83, 802.84, 802.85, 802.86, 802.87, 802.88, 802.89, 802.90, 802.91, 802.92, 802.93, 802.94, 802.95, 802.96, 802.97, 802.98, 802.99, 803.00			
1. baseband, *PSK, QAM-*, OFDM, CDMA, etc. over Cat5, Fiber, HFC, phone line, RF etc.			

Стандартни организации

7. IETF, W3C, 3GPP, ...	IETF	W3C	3GPP	...
4. IETF, ...	IETF	...	IETF	...
3. IETF, 3?, IETF	IETF	3?	IETF	3.5? IETF MLD
2. IEEE, ITU, IETF, ...	IEEE	ITU	IETF	...
1. IEEE, ITU, ...	IEEE	ITU	...	FDMA, CDMA, etc. over Cat5, Fiber, HFC, phone line, RF etc.

Стандартни организации

- IETF (www.ietf.org)
- IEEE (www.ieee.org)
- ITU (www.itu.int)
- 3GPP (www.3gpp.org)
- x Forum, y Alliance, z Foundation (WiMax Forum, WiMedia Alliance, XMPP Standards Foundation, и т.н.)
- Повечето широко-използвани протоколи в мрежите са свободни

Инструменти



Инструменти

- Wireshark, демонстрация

```
⊕ Frame 1 (508 bytes on wire, 508 bytes captured)
⊕ Ethernet II, Src: 00:12:3f:ed:ff:0d (00:12:3f:ed:ff:0d), Dst: 00:30:48:83:93:e9 (00:30:48:83:93:e9)
⊕ Internet Protocol, Src: 172.19.55.203 (172.19.55.203), Dst: 145.97.39.155 (145.97.39.155)
⊕ Transmission Control Protocol, Src Port: 1856 (1856), Dst Port: http (80), Seq: 0, Ack: 0, Len: 454
⊕ Hypertext Transfer Protocol
```

- tcpdump

Рамки, пакети, сегменти



Рамки, Пакети, Сегменти

7. Application

6. Presentation

5. Session

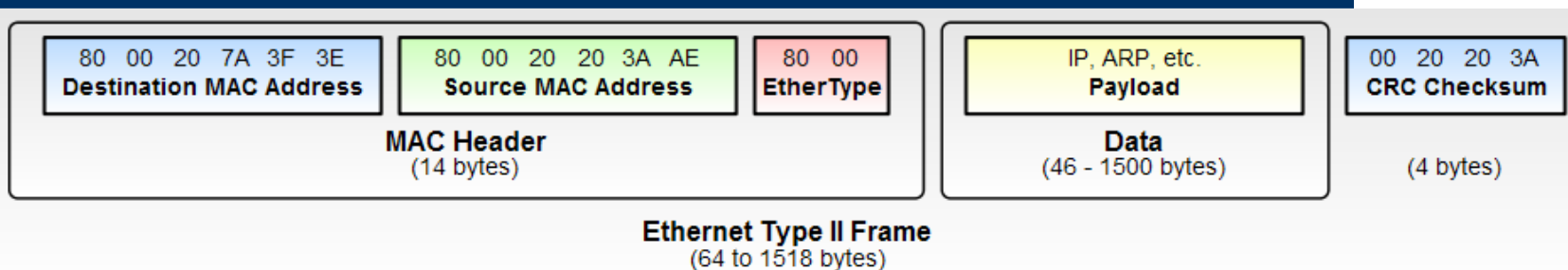
4. Transport

3. Network

2. Datalink

1. Physical

Ethernet рамка



- Network order / Machine order ...
- битове 6 и 7 от MAC адреса ...
- MAC address spoofing
- Wire tapping

- max 150 Kpps @ 100Mbps

Hub, Switch, Router

7. HTTP, FTP, SMTP, POP3, IMAP4, SIP, XMPP, IRC, SNMP, SSH, TELNET, DNS, NTP, DHCP

4 and 5. TCP, UDP, RTP

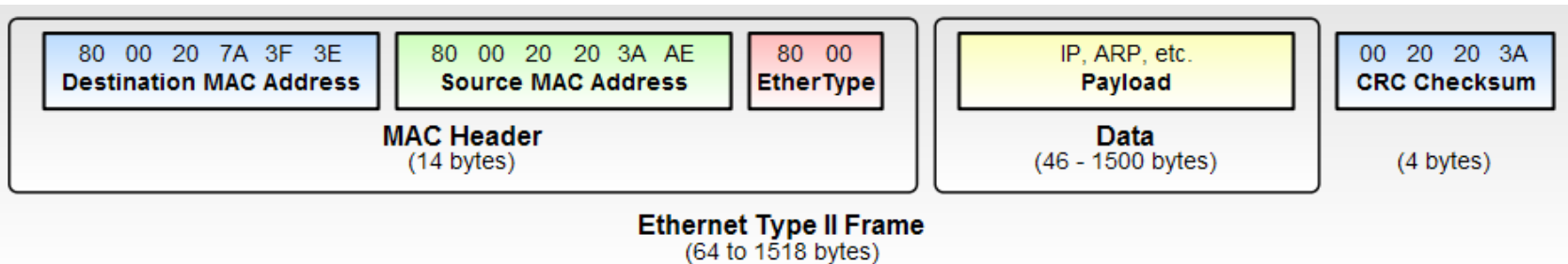
3. IP/IPv6

2. Ethernet (802.3) , 802.11, 802.15, 802.16, PPP

1. baseband, *PSK, QAM-*, OFDM, CDMA, etc. over Cat5, Fiber, HFC, phone line, RF etc.

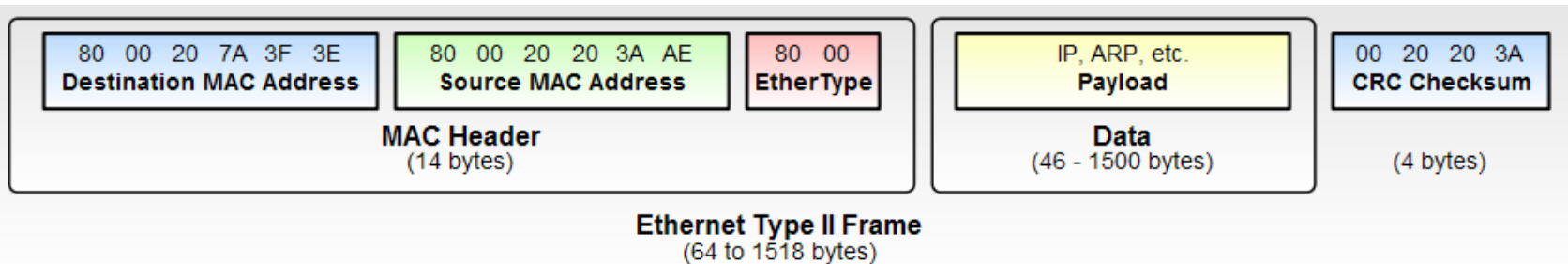
Switch

- Принцип на работа
- Физически достъп и конфигурация
- Интерфейс за менажиране



Switch

- Broadcast/Multicast/Unicast
- MAC address table size
- MAC address learning rate
- MAC address spoofing



Flow control

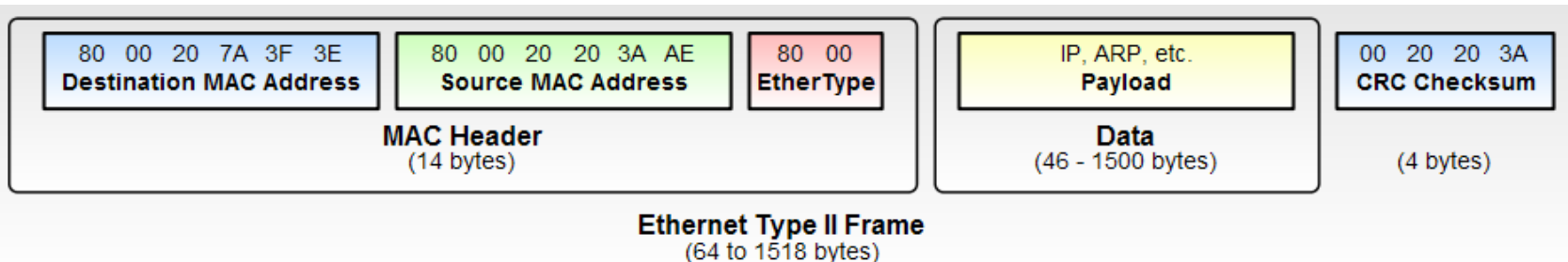
- Принцип на работа
- Pause frames
- $x \cdot 512$ bit times. $x = 0 - 0xFFFF$

- Буфери на свичовете
- 3pps ...

Preamble (7-bytes)	Start Frame Delimiter (1-byte)	Dest. MAC Address (6-bytes) = (01-80-C2- 00-00-01) or unique DA	Source MAC Address (6-bytes)	Length/Type (2-bytes) = 802.3 MAC Control (88-08)	MAC Control Opcode (2-bytes) = PAUSE (00-01)	MAC Control Parameters (2-bytes) = (00-00 to FF-FF)	Reserved (42-bytes) = all zeros	Frame Check Sequence (4-bytes)
-----------------------	---	--	---------------------------------------	---	--	---	--	---

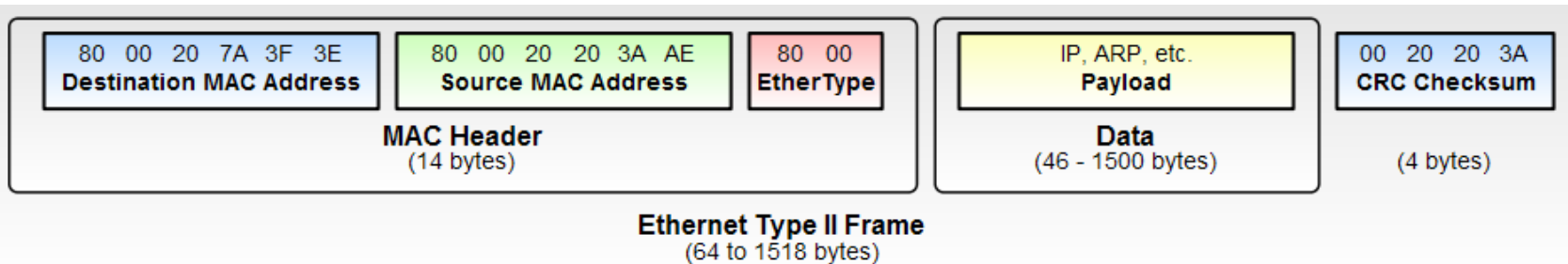
Spanning tree protocol

- Принцип на работа
- Root bridge election
- Designated bridge election



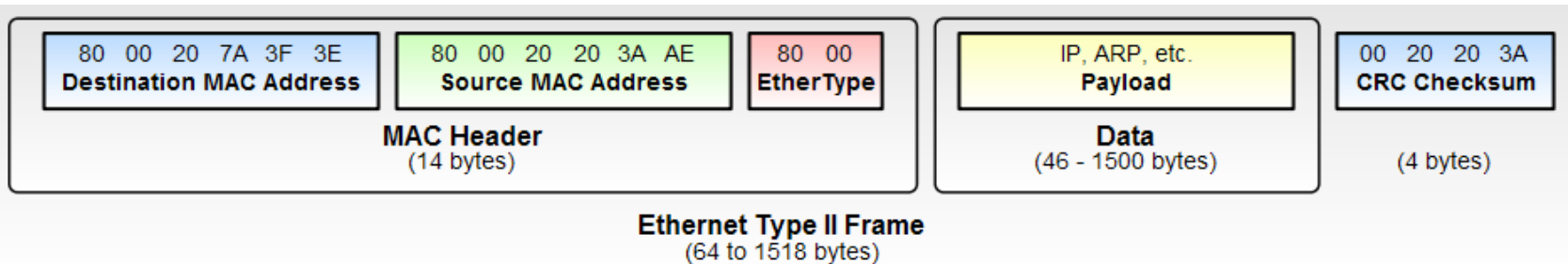
VLANs and Trunking

- Принцип на работа
- Native VLAN
- VLAN tag insertion
- VLAN filtering



Протоколи по подразбиране

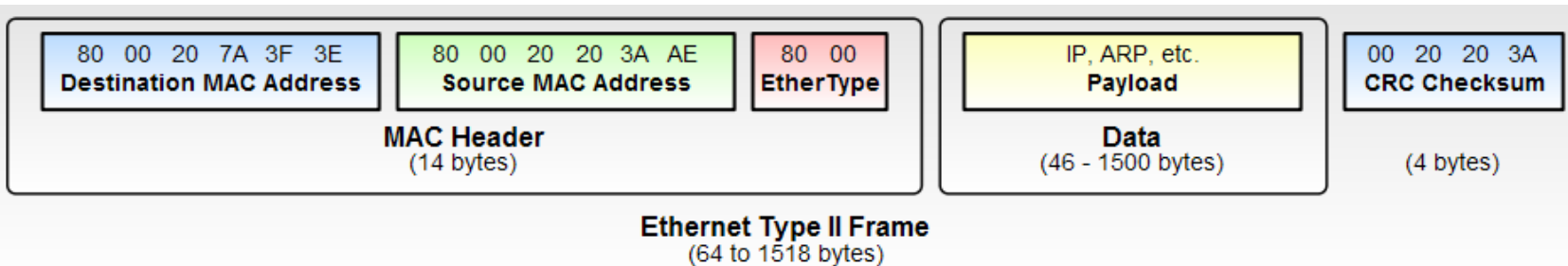
- STP
- LLDP, CDP, EDP
- DTP
- GVRP, VTP
- LACP
- Flow control negotiation



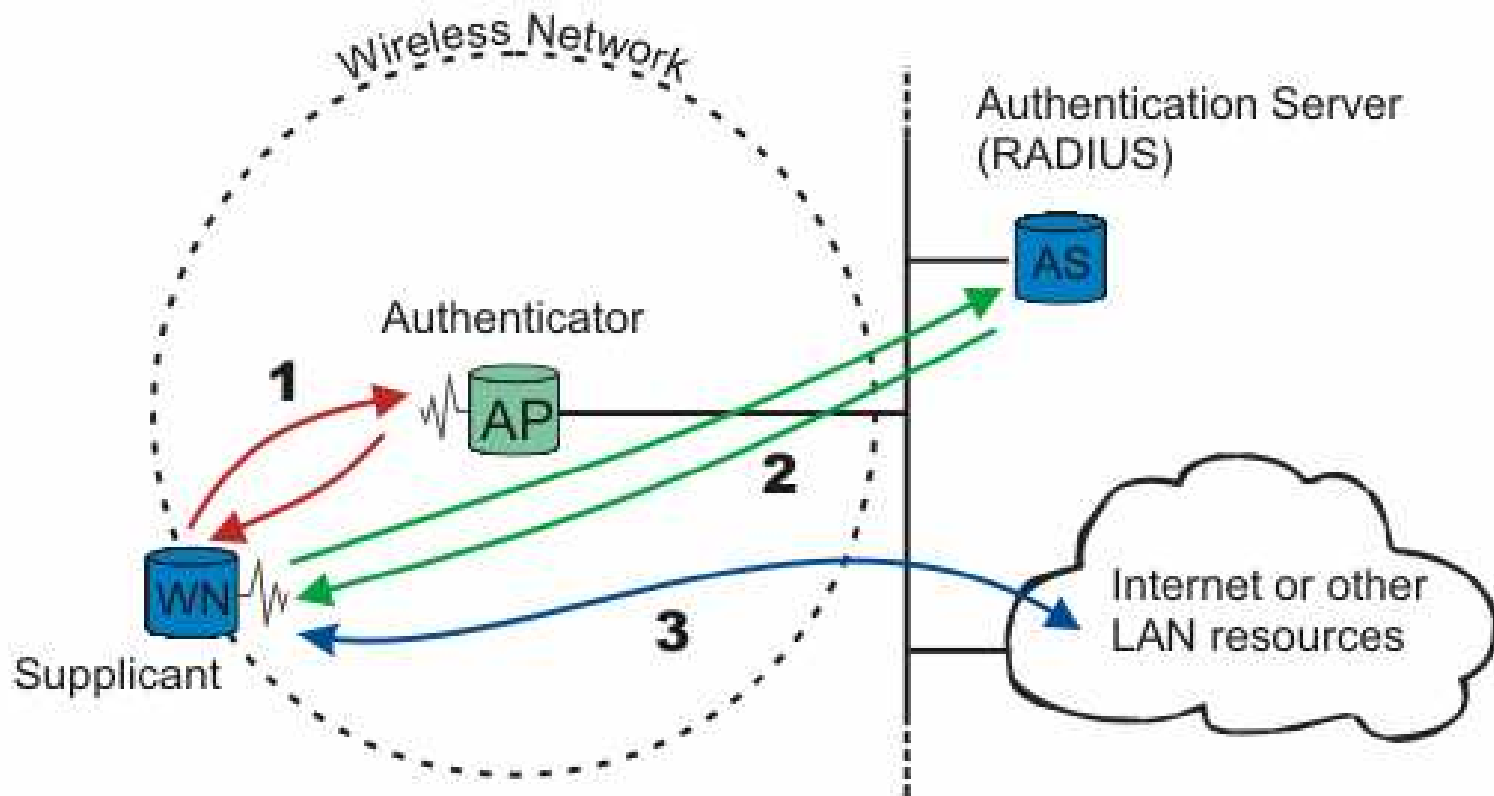
Техники за сигурност

- Мрежов дизайн
- Ограничения по MAC адрес
- Ограничения на STP и други протоколи
- Ограничения на VLANs
- Authentication (802.1x)

- Контрол върху хостовете



802.1x



wikipedia 802.1X

google 802.1X HOWTO

7. HTTP, FTP, SMTP, POP3, IMAP4, SIP, XMPP, IRC, SNMP, SSH, TELNET, DNS, NTP, DHCP

4 and 5. TCP, UDP, RTP

3. IP/IPv6

2. Ethernet (802.3) , 802.11, 802.15, 802.16, PPP

1. baseband, *PSK, QAM-*, OFDM, CDMA, etc. over Cat5, Fiber, HFC, phone line, RF etc.