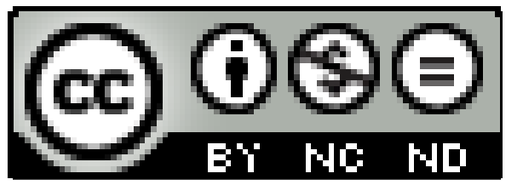
Мрежова сигурност I

http://training.iseca.org/

Ethernet 2/3



Boyan Krosnov

Acknowledgements

Some materials are based on work by

- Wikipedia users
  - Mikm, Bruceadler, GhosT, Arr2036, HammondJr

План

- Преговор
- Как работят суичовете
  - MAC address learning, timers
  - VLANs
  - carrier features & tweaks
- Spanning tree
- Link aggregation
- VLAN automation
- Multicasting
- Authentication

Преговор

- Стандарт
- Топология
- Физическа среда
  - Физически атаки
- Формат на Ethernet фрейма

80 00 20 7A 3F 3E **Destination MAC Address**	80 00 20 20 3A AE **Source MAC Address**	08 00 **EtherType**	IP, ARP, etc. **Payload**	00 20 20 3A **CRC Checksum**
MAC Header (14 bytes)			**Payload and Padding** (46 – 1500 bytes)	(4 bytes)

Ethernet Type II Frame (64 to 1518 bytes)

Как работи суича

- IEEE 802.1D-2004 Clause 7 - Principles of Bridge operation

- Store and forward, буфери
- Flooding
  - Broadcast
  - Multicast
  - Unknown Unicast - Фреймовете адресирани до неизвестни MAC адреси се пращат на всички
- MAC learning
- MAC ageing

Как работи суича (pseudocode)

```
function receive(frame, port)
    checkCRC(frame)
    learn(frame.src, port)
    forward(frame)
```

```
function forward(frame)
    if frame.dst.igBit == 1:
        send(frame, BROADCAST)                    <- Broadcast
    else if macTable[frame.dst] exists:
        send(frame, macTable[frame.dst])          <- Unicast
    else:                                         <- Unknown Unicast
        send(frame, BROADCAST)
```

Как работи суича (pseudocode)

```
function learn(mac, port)
    if mac.igBit == 0
        macTable[frame.src] = port
```

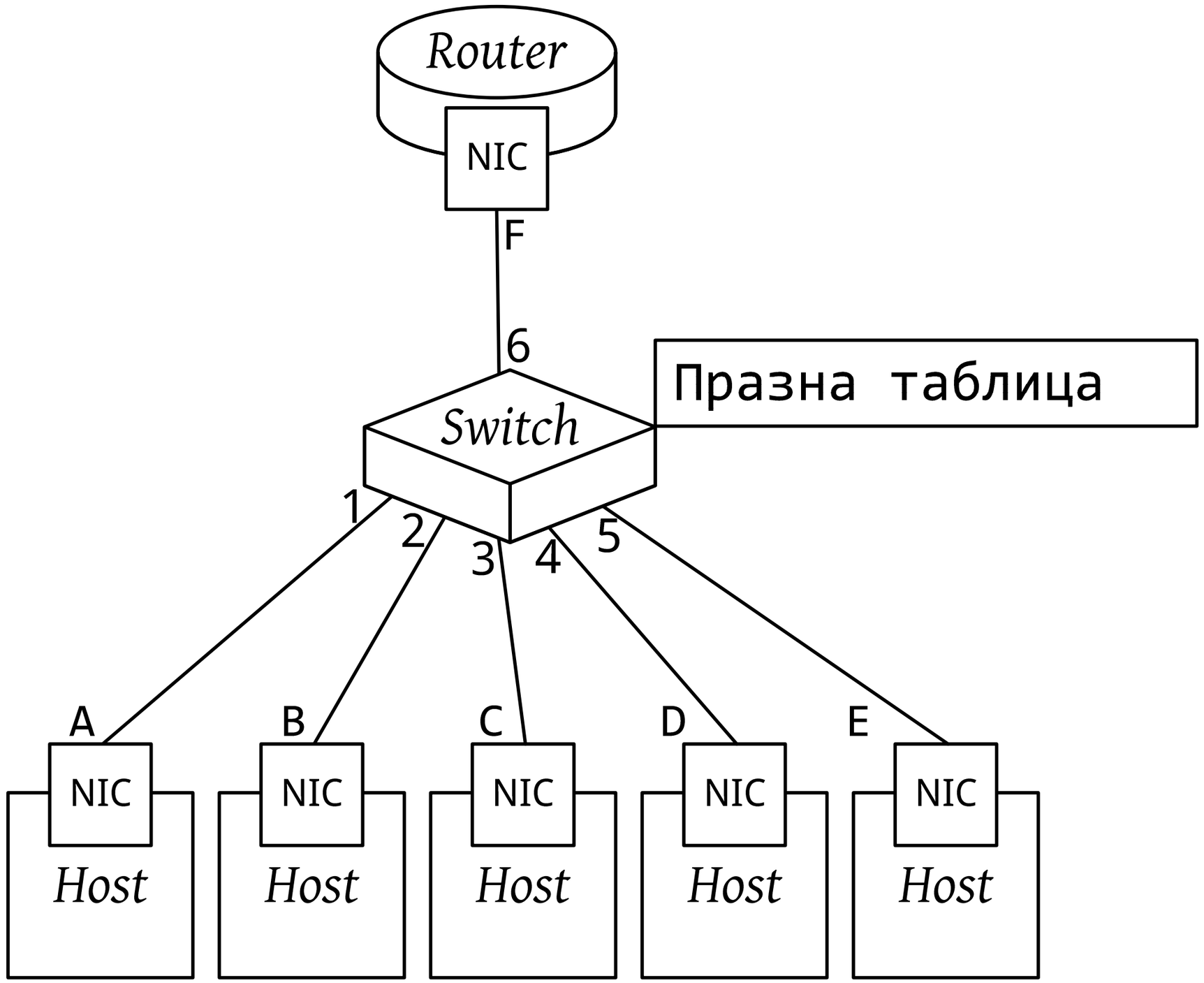
- macTable е таблица с ограничена големина
- Таблицата се почиства от стари записи

Switch vs. Router

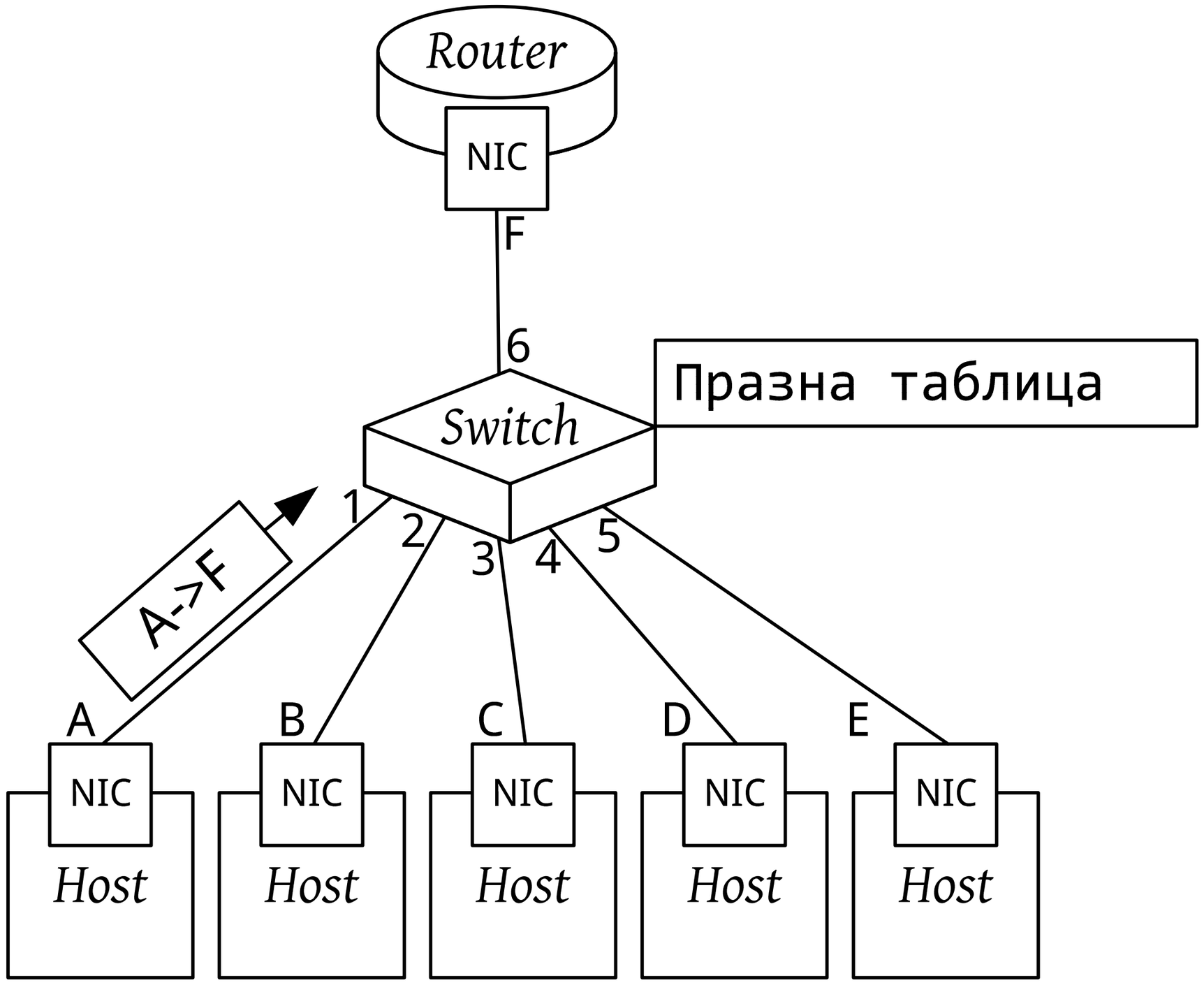
- Bridge и Switch – Layer 2 – Ethernet
  - lookup destination MAC in table
  - forward
- Router – Layer 3 – IP
  - lookup destination IP in table
  - forward

- Какво е Layer 3 Switch ?
- Какво е Layer 7 Switch ?

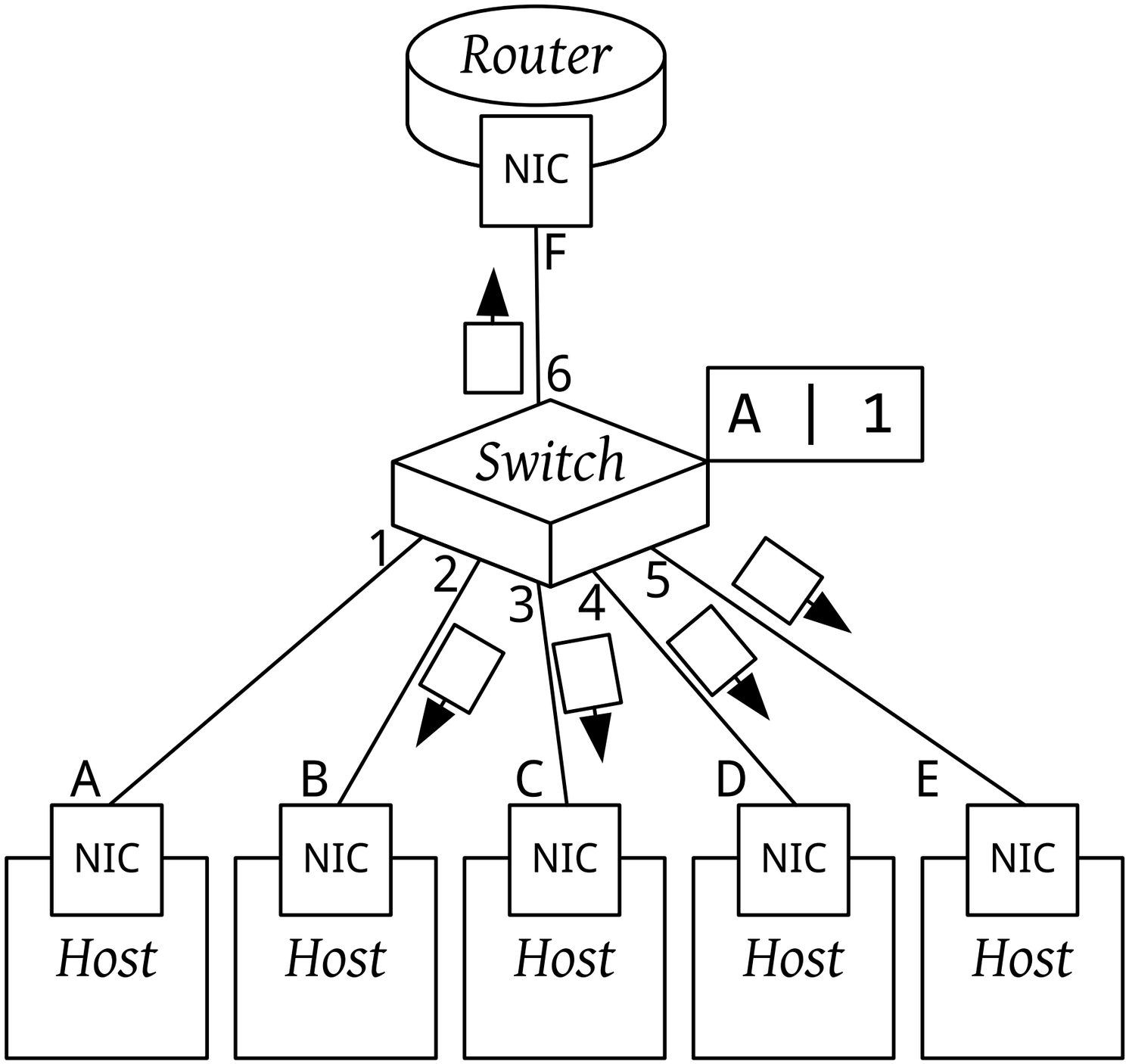
Пример


Router
NIC
F
6
Switch
Празна таблица
1
2
3
4
5
A
B
C
D
E
NIC
NIC
NIC
NIC
NIC
Host
Host
Host
Host
Host

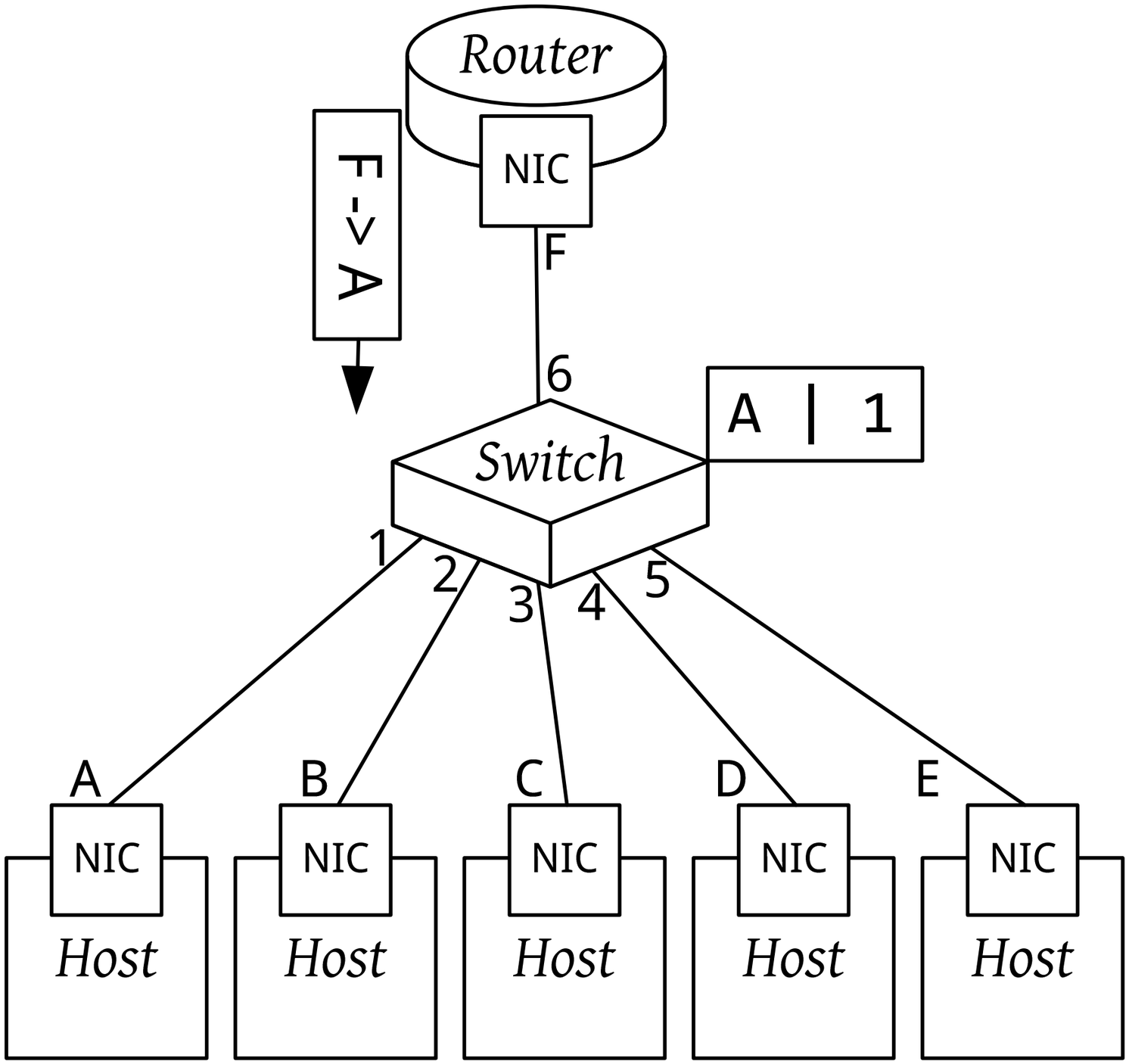
Пример


Router
NIC
F
6
Switch
Празна таблица
A->F
1
2
3
4
5
A
B
C
D
E
NIC
NIC
NIC
NIC
NIC
Host
Host
Host
Host
Host

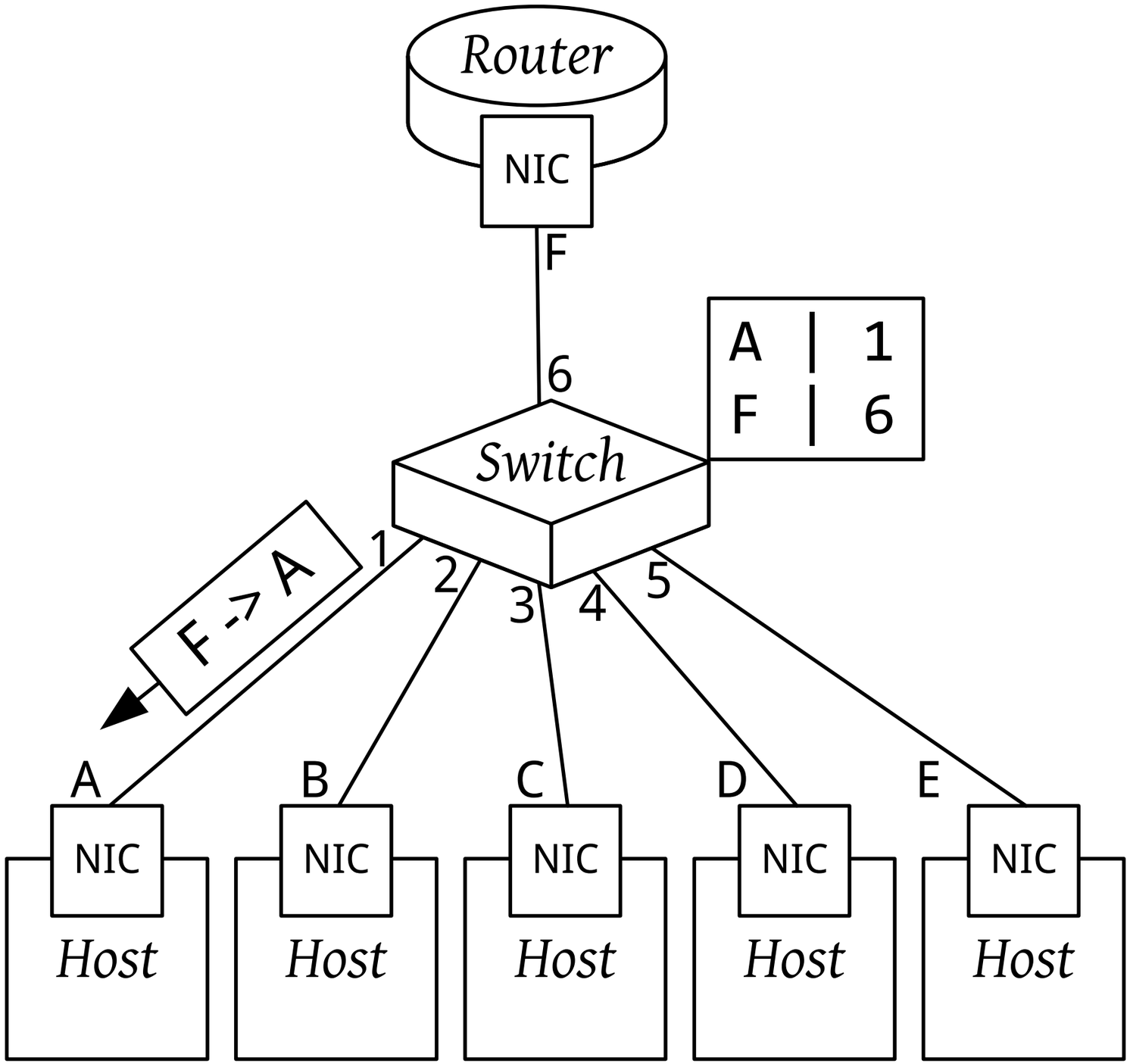
Пример


Router
NIC
F
6
A | 1
Switch
1
2
3
4
5
A
B
C
D
E
NIC
NIC
NIC
NIC
NIC
Host
Host
Host
Host
Host

Пример


Router
NIC
F
F - V A
6
A | 1
Switch
1
2
3
4
5
A
B
C
D
E
NIC
NIC
NIC
NIC
NIC
Host
Host
Host
Host
Host

Пример


Router
NIC
F
6
Switch
A | 1
F | 6
F -> A
1
2
3
4
5
A
B
C
D
E
NIC
NIC
NIC
NIC
NIC
Host
Host
Host
Host
Host

Други специални MAC адреси

- 00-80-C2-00-00-00 до 00-80-C2-FF-FF-FF – Unicast адреси за стандартни протоколи

- 01-80-C2-00-00-00 до 01-80-C2-FF-FF-FF – Multicast адреси за стандартни протоколи
  - 01-80-C2-00-00-00 to 01-80-C2-00-00-0F – don’t relay
  - 01-80-C2-00-00-10 to 01-80-C2-00-00-FF – ok to relay

`http://standards.ieee.org/regauth/groupmac/tutorial.html`

VLANs

- 802.1Q - Virtual Bridged Local Area Networks
- Виртуални суичове
- VLAN/priority tag

80 00 20 7A 3F 3E **Destination MAC Address**	80 00 20 20 3A AE **Source MAC Address**	81 00 **EtherType**	04 D2 **VLAN tag**	08 00 **EtherType**	IP, ARP, etc. **Payload**	00 20 20 3A **CRC Checksum**
MAC Header (14 bytes)			**VLAN Header** (4 bytes)		**Payload and Padding** (46 – 1500 bytes)	(4 bytes)

Ethernet Type II Frame with 1 VLAN tag (64 to 1522 bytes)

80 00 20 7A 3F 3E **Destination MAC Address**	80 00 20 20 3A AE **Source MAC Address**	08 00 **EtherType**	IP, ARP, etc. **Payload**	00 20 20 3A **CRC Checksum**
MAC Header (14 bytes)			**Payload and Padding** (46 – 1500 bytes)	(4 bytes)

Ethernet Type II Frame (64 to 1518 bytes)

VLANs

- VLAN ID 0-4095 (12 bits)
- 0 – no VLAN tag
- 1 – default VLAN
- 4095 за бъдещи разширения

- Приоритет (802.1p) - 3 bits под-поле в Q/P полето

80 00 20 7A 3F 3E **Destination MAC Address**	80 00 20 20 3A AE **Source MAC Address**	81 00 **EtherType**	04 D2 **VLAN tag**	08 00 **EtherType**	IP, ARP, etc. **Payload**	00 20 20 3A **CRC Checksum**
MAC Header (14 bytes)			**VLAN Header** (4 bytes)		**Payload and Padding** (46 – 1500 bytes)	(4 bytes)

Ethernet Type II Frame with 1 VLAN tag (64 to 1522 bytes)

Въпроси

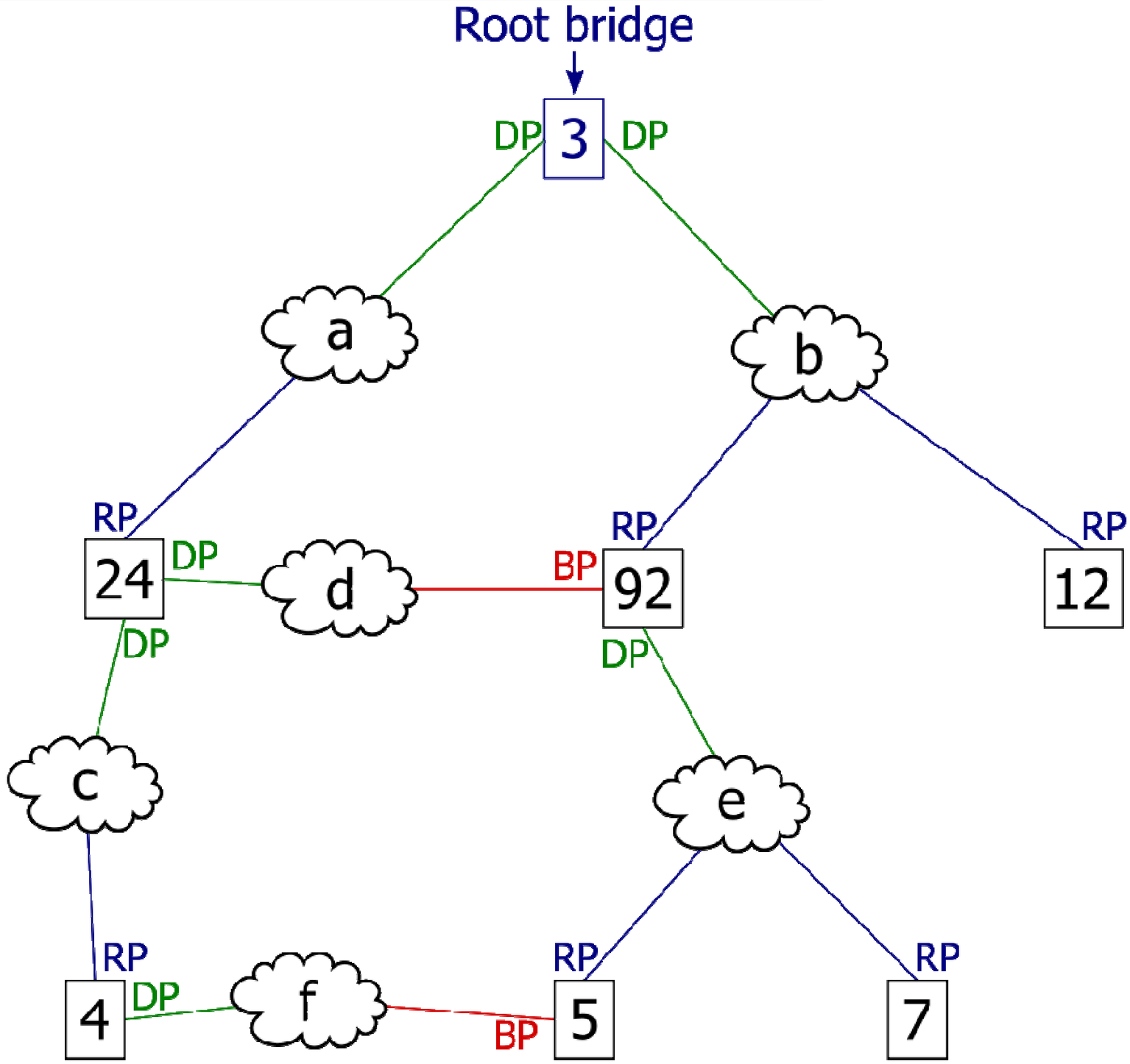
Carrier features and tweaks

- MAC-Forced forwarding (RFC 4562)
- Private VLANs
- VLAN in VLAN (QinQ, Provider Bridges)
- Ethernet over Ethernet (MACinMAC, PBB)
- Traffic Engineering (PBB-TE)

- Access – Ethernet in the First mile (802.3ah)
- Metro - MEF

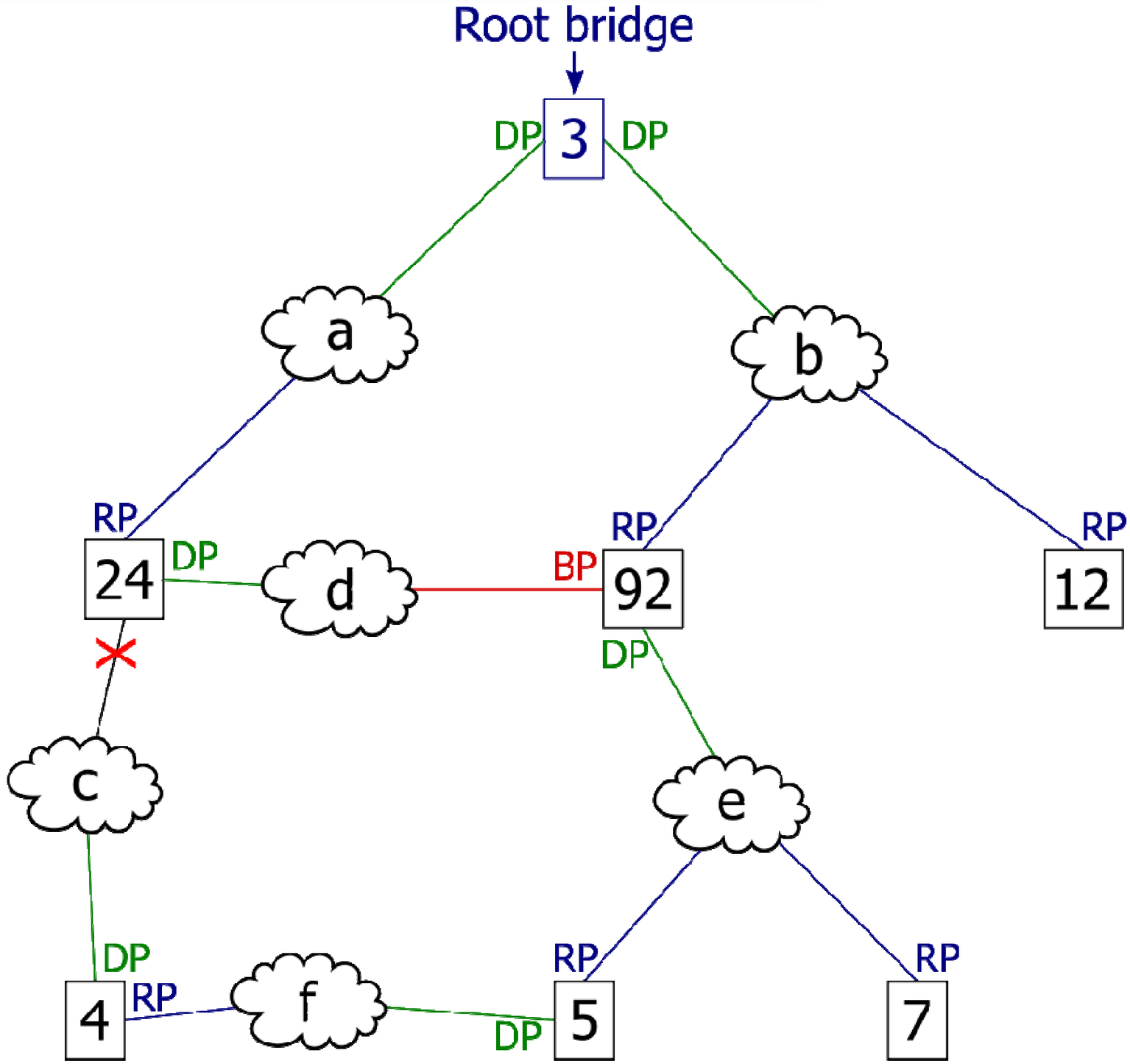
Spanning tree protocol

- STP
- RSTP
- MSTP



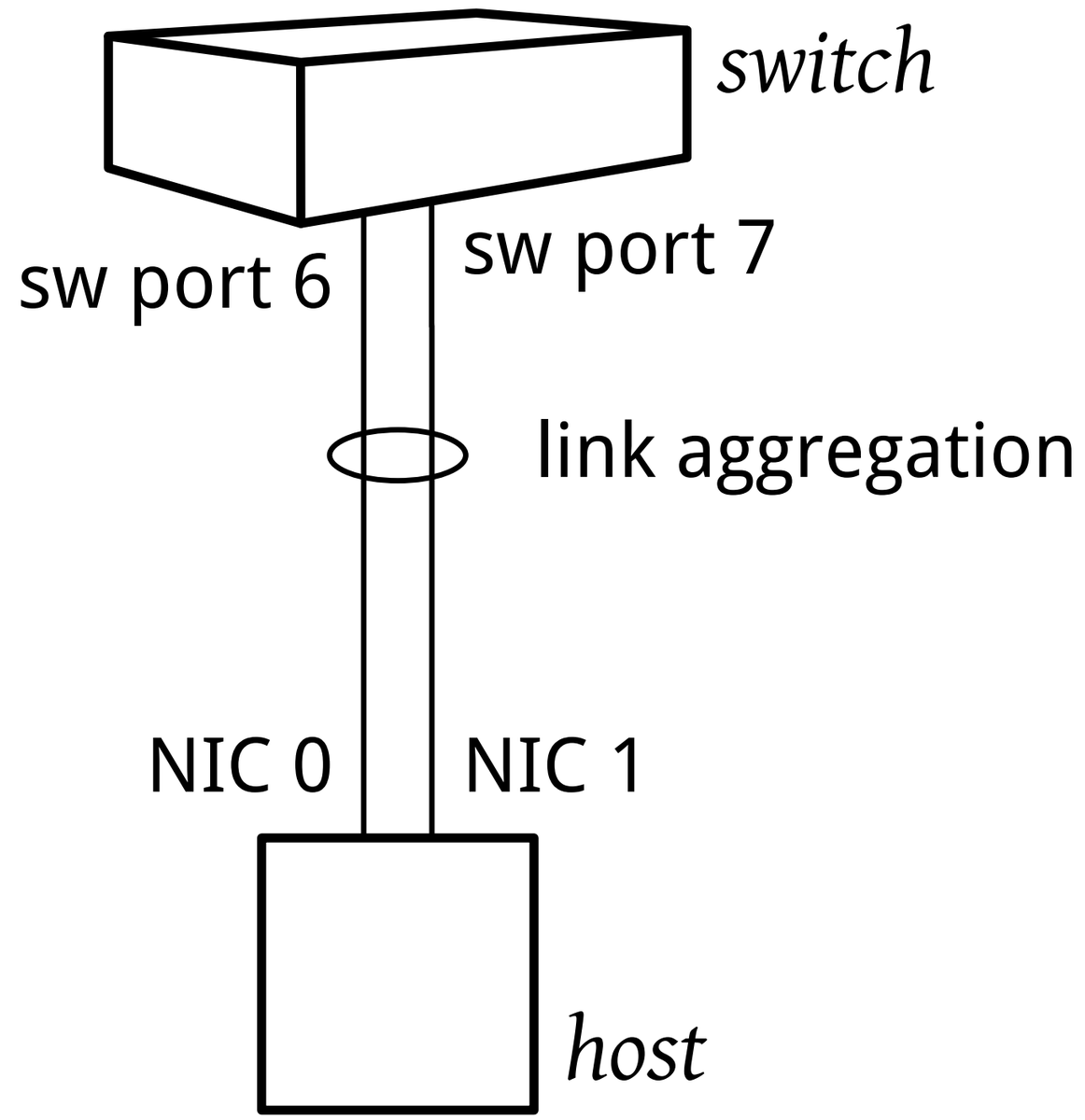
Spanning tree protocol

- STP
- RSTP
- MSTP



Link aggregation

- Терминология
  - link aggregation (IEEE, neutral)
  - bonding (*nix)
  - port channel (Cisco)
  - trunking (HP, Nortel)
- Балансиране
- Ръчна настройка
- LACP, PAGP



VLAN automation & more

- Автоматично конфигуриране на трънкове
  - Dynamic Trunking Protocol (DTP)

- VLAN база
  - GARP/GVRP, MRP/MVRP
  - VLAN Trunking Protocol (VTP)

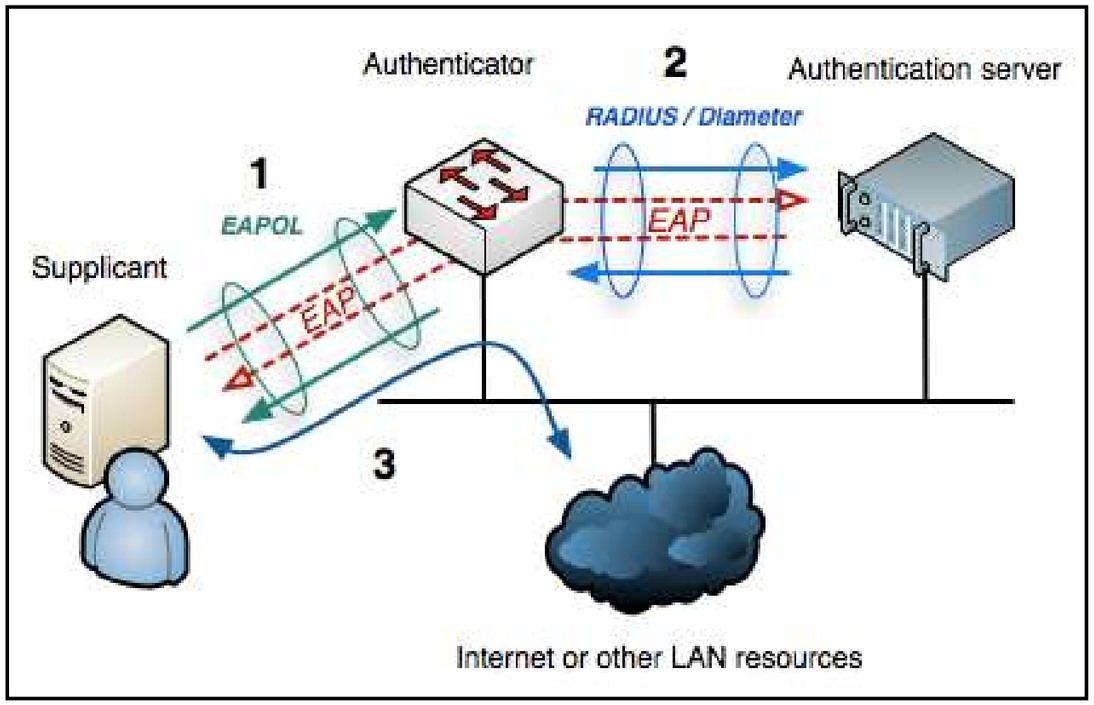
- Откриване на съседни устройства
  - Link-layer Discovery Protocol (LLDP)
  - CDP, EDP, etc.

Multicasting

- IGMP snooping
- CGMP
- GMRP/MMRP

Authentication & Encryption

- Autentication - 802.1X



- Encryption
  - MACsec (802.1AE)
  - LinkSec

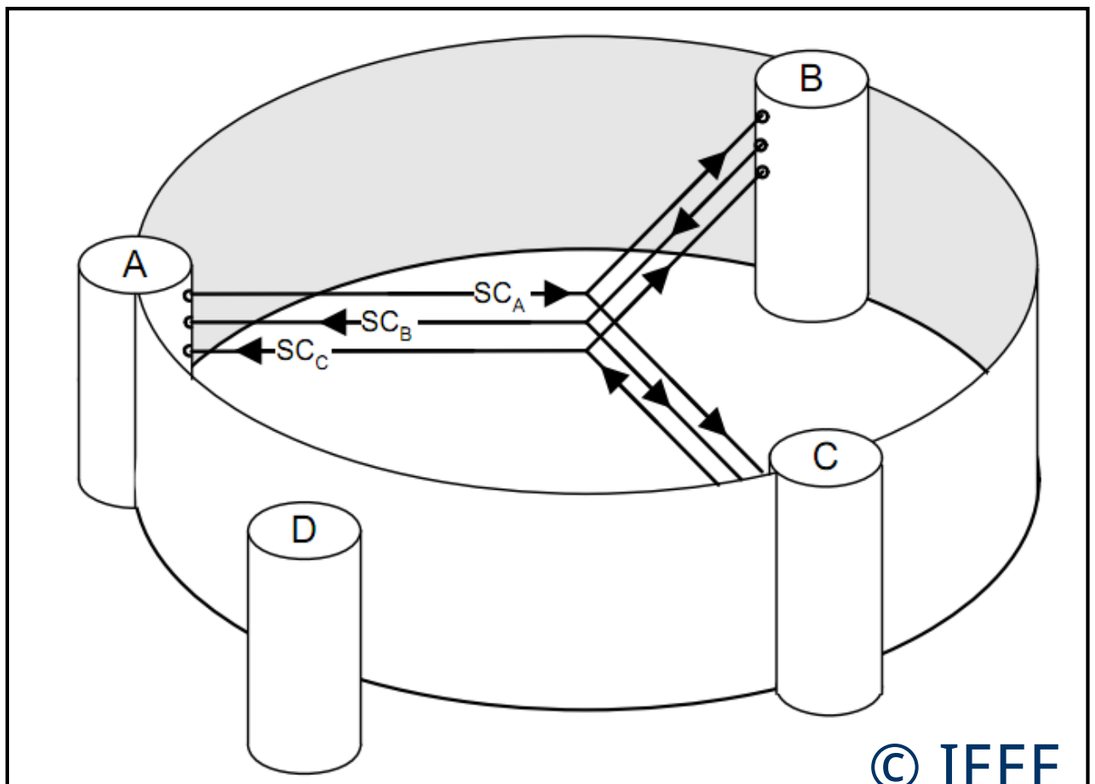


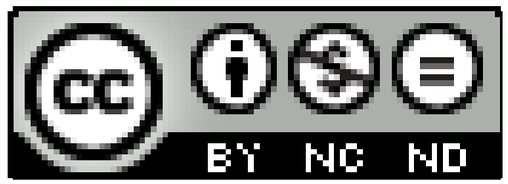
Figure 7-6—Secure communication between three stations

Въпроси

Мрежова сигурност I

http://training.iseca.org/

Ethernet 3/3



Boyan Krosnov

Атаки

- Resource exhaustion
- Bottlenecks
- Софтуерни експлойти на суичове
- Flow control атака
- MAC spoofing
- VLAN automation атаки
- VLAN hopping атаки
- STP атаки

Resource exhaustion

- Таблици в суичовете
  - MAC flooding
- Буфери в суичовете
  - Bursts

Bottlenecks

- Бавни връзки
  - Портове за менажиране на 10/100Mbps
- Бавни карти
  - Типичен сървър – 300 kpps @ GigE
- Бавни хостове
  - IP телефон с 100 MHz DSP
- Бавни процесори на суичовете
  - Суич за $10k с PowerPC405 на 250 Mhz

Софтуерни експлойти на суичове

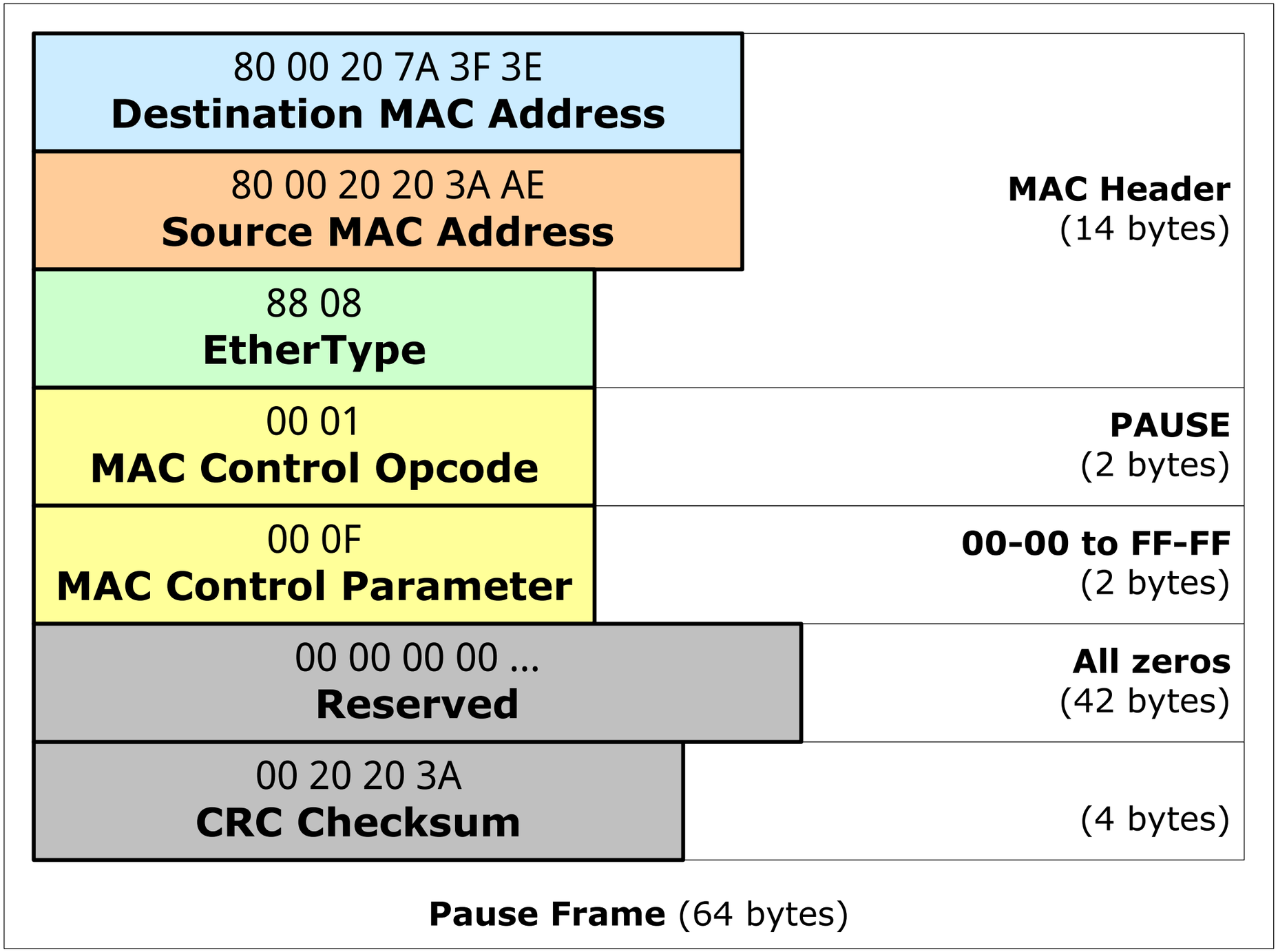
- Софтуер на типичен менажируем суич
  - STP, RSTP, MSTP
  - CDP, LLDP
  - LACP
  - DTP, VTP, GARP/GVRP

Софтуерни експлойти на суичове

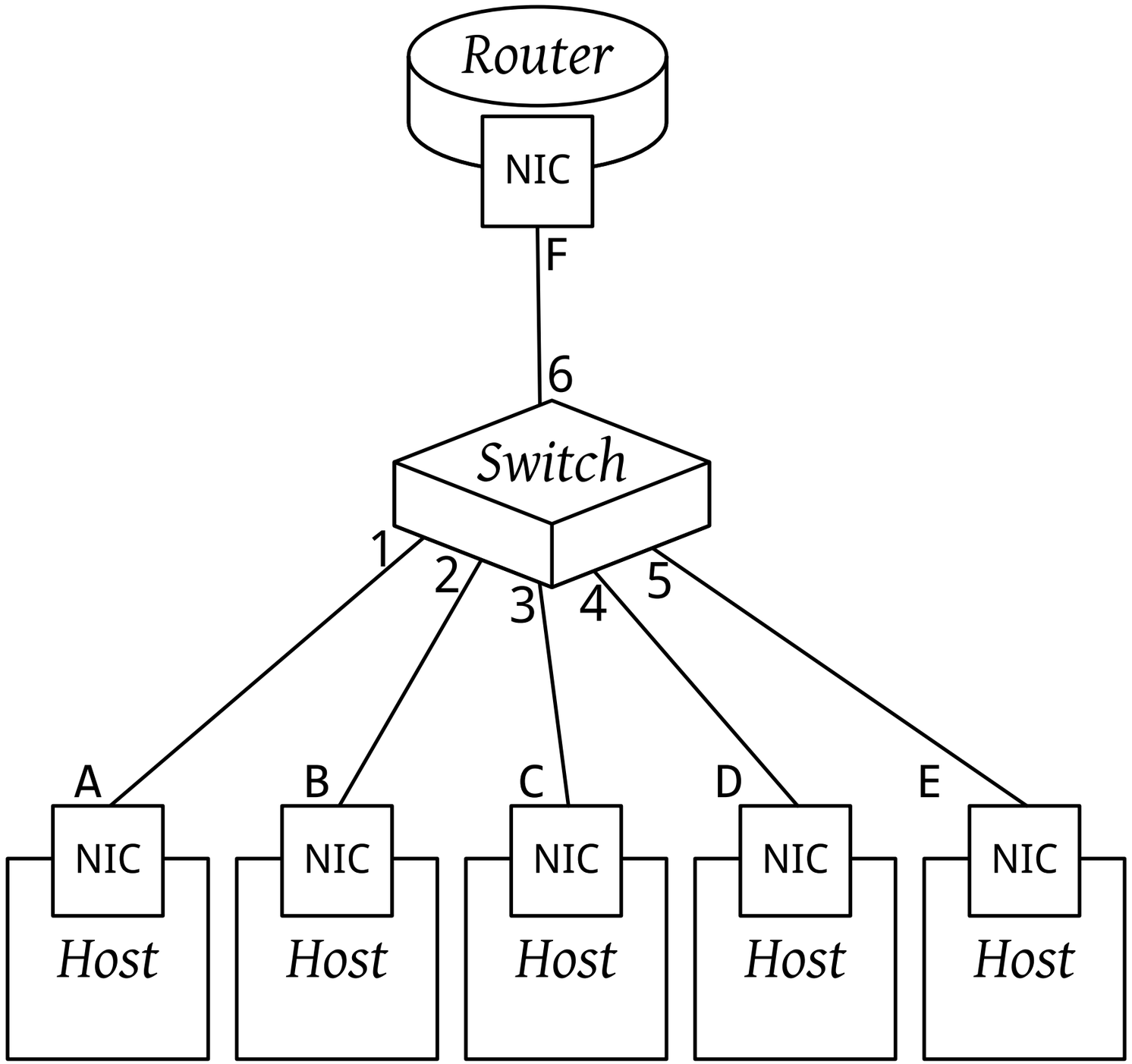
- И ....
  - IGMP snooper, DHCP snooper, ARP snooper
  - TCP/IP host stack - IP, TCP, UDP, ICMP, DNS, etc.
  - SSH, Telnet
  - SNMP
  - HTTP/HTTPs server
  - RADIUS client
  - DHCP server, DHCP client
  - и боклук от типа на echo, chargen, finger, etc.

Flow control атака

- Принцип на работа на flow control
- 30 pps



MAC spoofing



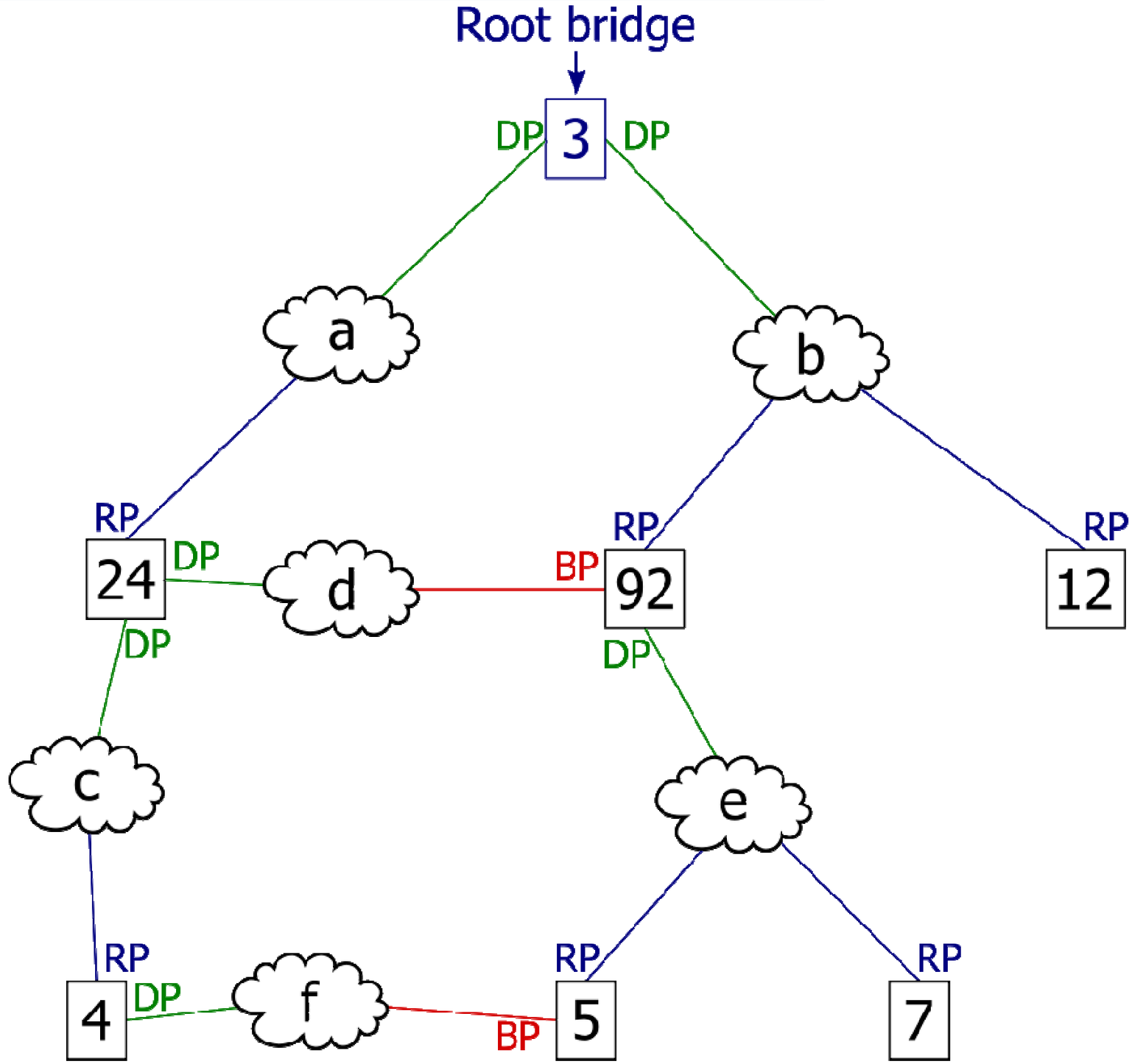
VLAN automation атаки

- DTP
  - access -> trunk
- VTP, GARP/GVRP

VLAN hopping атаки

- Access порт който приема VLAN тагнати пакети
- Trunk портове, които приемат всички VLAN-и
- Грешно конфигуриран native vlan на trunk порт

STP атаки


Root bridge
DP
3
DP
a
b
RP
RP
RP
24
DP
d
BP
92
12
DP
DP
c
e
RP
RP
RP
4
DP
f
BP
5
7