

VYSOKÉ UČENÍ FAKULTA
TECHNICKÉ INFORMAČNÍCH
V BRNĚ TECHNOLOGIÍ

8

Linková vrstva

Počítačové komunikace a sítě

Obsah

ÚVODNÍ INFORMACE

- Motivace
- Detekce a oprava chyb

MEDIA ACCESS CONTROL

- Řízení přístupu k sdílenému médiu

ETHERNET

- Adresování
- ARP
- Aktivní síťové prvky

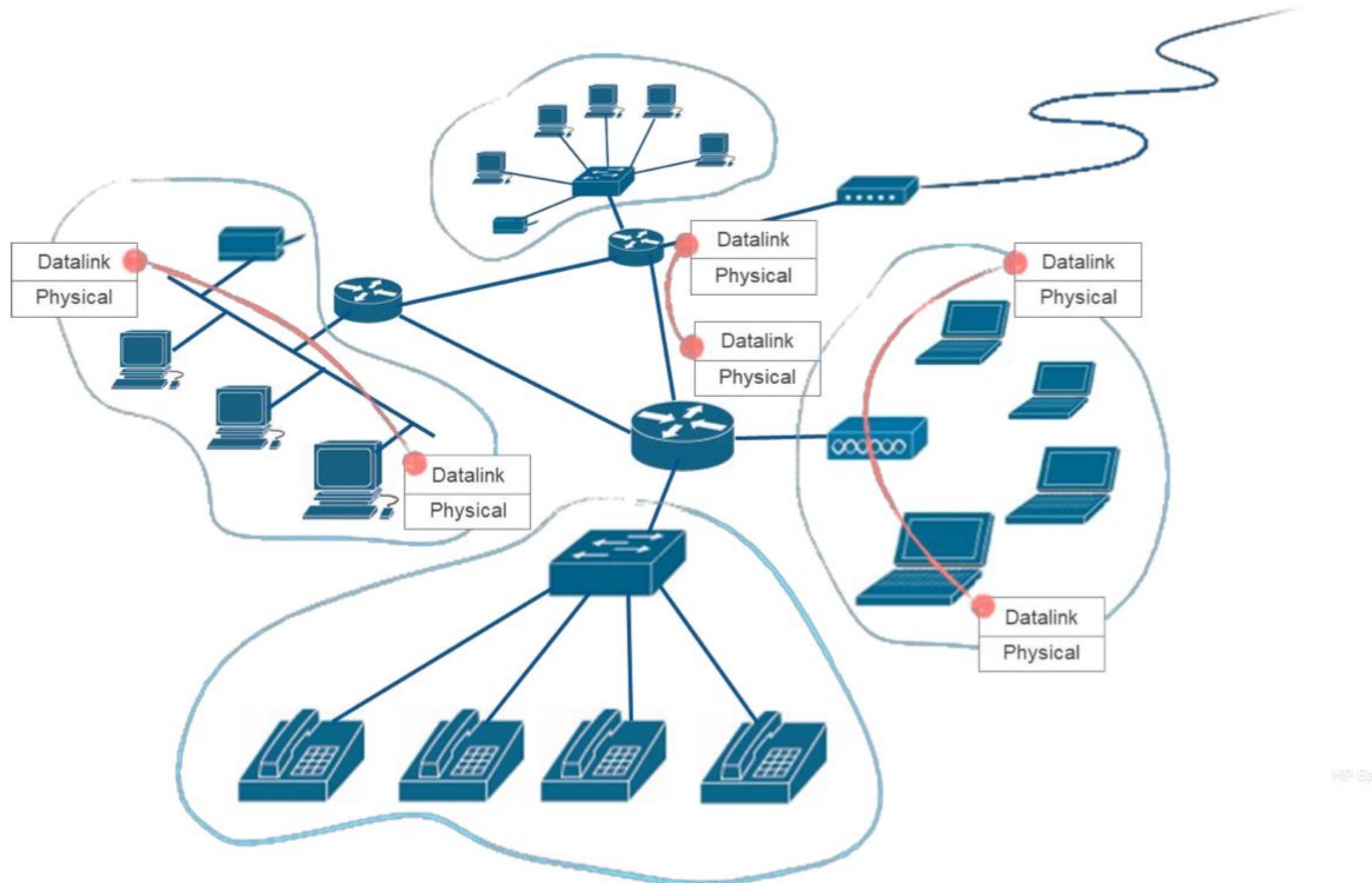
VIRTUÁLNÍ LAN SÍTĚ

STP

Bezdrátové sítě

Úvod

Komunikace na linkové vrstvě



Přehled

- Linková vrstva doručuje rámce linkové vrstvy mezi sousedními počítači v lokální síti – na jedné lince
 - Rámec linkové vrstvy zapouzdřuje pakety datagram síťové vrstvy
 - Adresování na linkové vrstvě
- Různé technologie LAN sítí
 - podle řízení vícenásobného přístupu
 - přenosové médium může být řízené (koaxiální kabel, dvoulinka, optika) nebo neřízené (vzduch)
 - polo-duplexní (half-duplex) nebo plně-duplexní (full-duplex) přenos
- Umožňuje detekci chyby při přenosu
- Technologie řízení linkové vrstvy často implementována v síťovém adaptéru (NIC – Network Interface Card)

Služby linkové vrstvy

Přístup k médiu

- Zabalení dat do rámců
- Přístup ke sdílenému médiu

Adresování

- Spolehlivé doručení mezi sousedními uzly a řízení toku
- Záleží na technologii (FrameRelay ano, Ethernet ne)
- Proměnná rychlosť přenosu

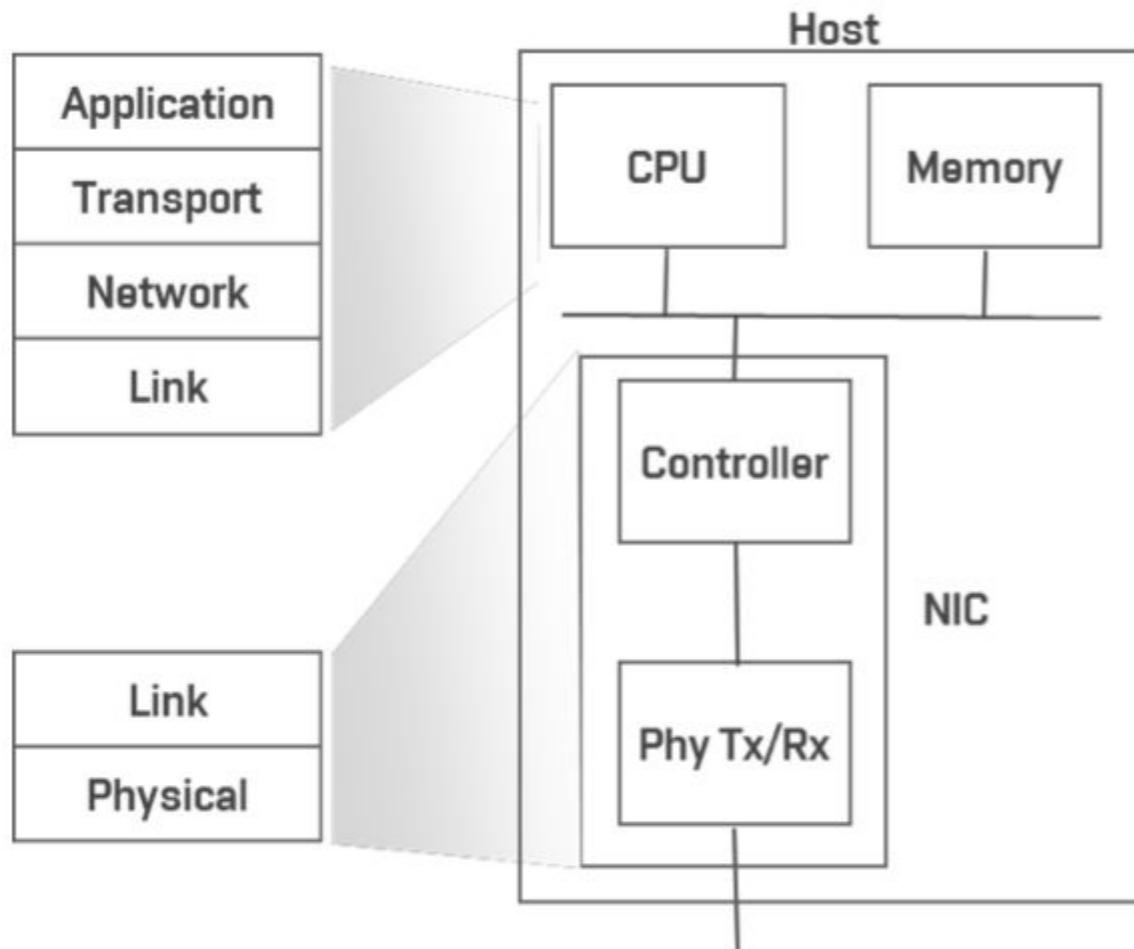
Detekce chyb

- Chyby způsobeny útlumem, rušením

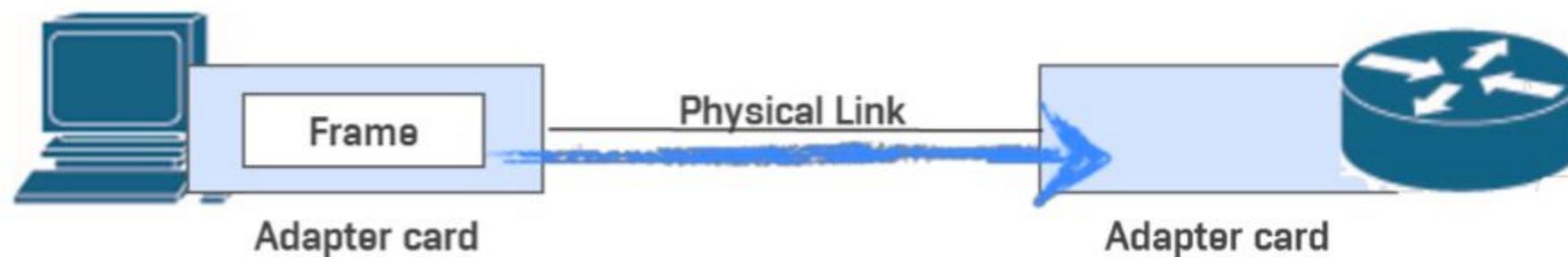
Oprava chyb

- Není nutné znova přenášet poškozený rámec

Síťový adaptér



- většina funkcí implementována v HW
- v SW je realizováno vytváření rámců, adresování, komunikace s NIC kontrolérem
- optimalizace - více funkcí do HW (porušení vrstvení)



Detekce a oprava chyb

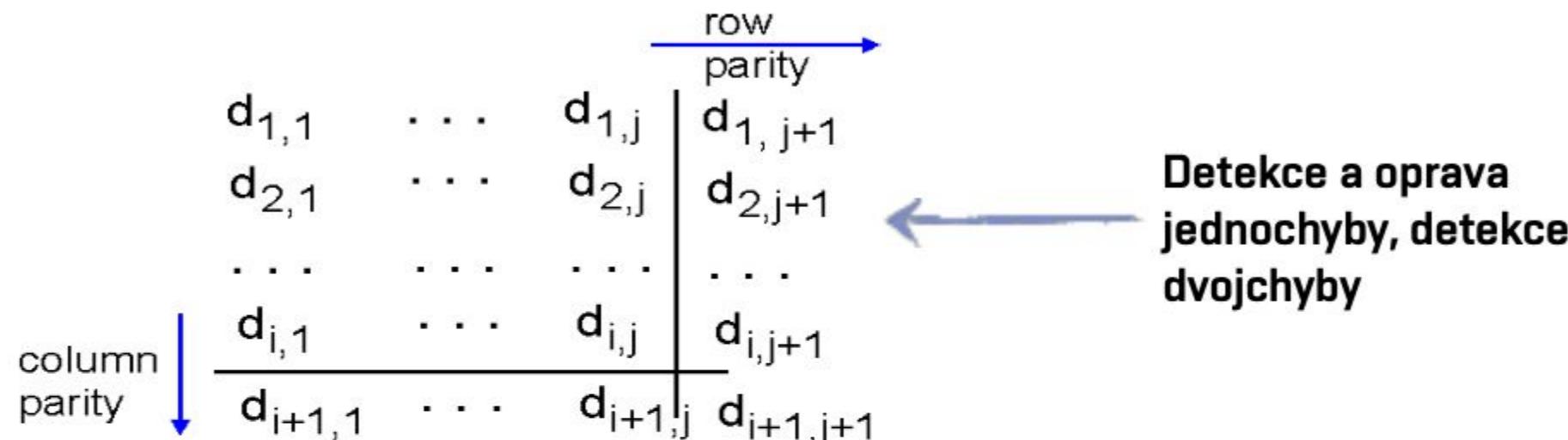
Při přenosu může dojít k chybě (útlum signálu, šum, interference, odraz)

Detekce chyby - možnost oznámit chybu a data odesílatel odešle znovu nebo se pouze chybný rámec zahodí

Oprava chyby - použitý kód umožňuje opravu obsahu bez nutnosti vyslat chybný rámec znovu



Jednoduchá parita



101011	101011
111100	101100
011101	011101
<hr/>	<hr/>
001010	001010
<i>no errors</i>	

*correctable
single bit error*

Forward error correction (FEC)

Hammingova vzdálenost je nejmenší počet pozic, na kterých se řetězce stejně délky daného kódu liší, neboli počet záměn, které je potřeba provést pro změnu jednoho z řetězců na druhý.

https://en.wikipedia.org/wiki/Hamming_distance

1010101010
1100110010



IPv4 kontrolní součet

- 1) Datové oktety jsou sdruženy do 16-ti bitových slov, a jejich suma v jedničkovém doplňku je vypočtena.
- 2) Jedničkový doplněk tohoto součtu je uložen do checksum políčka paketu.
- 3) Při kontrole je vypočtena suma jedničkového doplňku pro všechny pole, je-li výsledek Oxffff, pak je v pořádku.

- Obvykle se používá dvojkový doplněk pro reprezentaci čísel
- Pro součet v jedničkové doplňku je nutné zahrnout přenos z MSB do LSB

	Byte-by-byte	"Normal" Order	Swapped Order
Byte 0/1:	00 01	0001	0100
Byte 2/3:	f2 03	f203	03f2
Byte 4/5:	f4 f5	f4f5	f5f4
Byte 6/7:	f6 f7	f6f7	f7f6
	---	----	----
Sum1:	2dc 1f0	2ddf0	1f2dc
Carrys:	dc f0	ddf0	f2dc
	1 2	2	1
	-- --	----	----
Sum2:	dd f2	ddf2	f2dd
Final Swap:	dd f2	ddf2	ddf2

HP Easy Scan
ddf2

Příklad

4	5	0	28					
1			0	0				
4	17	0			↑			
10.12.14.5								
12.6.7.9								

4, 5, and 0	→	4	5	0	0
28	→	0	0	1	C
1	→	0	0	0	1
0 and 0	→	0	0	0	0
4 and 17	→	0	4	1	1
0	→	0	0	0	0
10.12	→	0	A	0	C
14.5	→	0	E	0	5
12.6	→	0	C	0	6
7.9	→	0	7	0	9
Sum	→	7	4	4	E
Checksum	→	8	B	B	1

CRC

Teorie polynomiálních kódů:

- Generátor $G(x)$ (polynom) stupně $n + 1$
- Zpráva $D(x)$ stupně d , délka zprávy d bitů
- Zbytek po dělení $R(x)$ stupně n

Snadná realizace pomocí posuvu a XOR

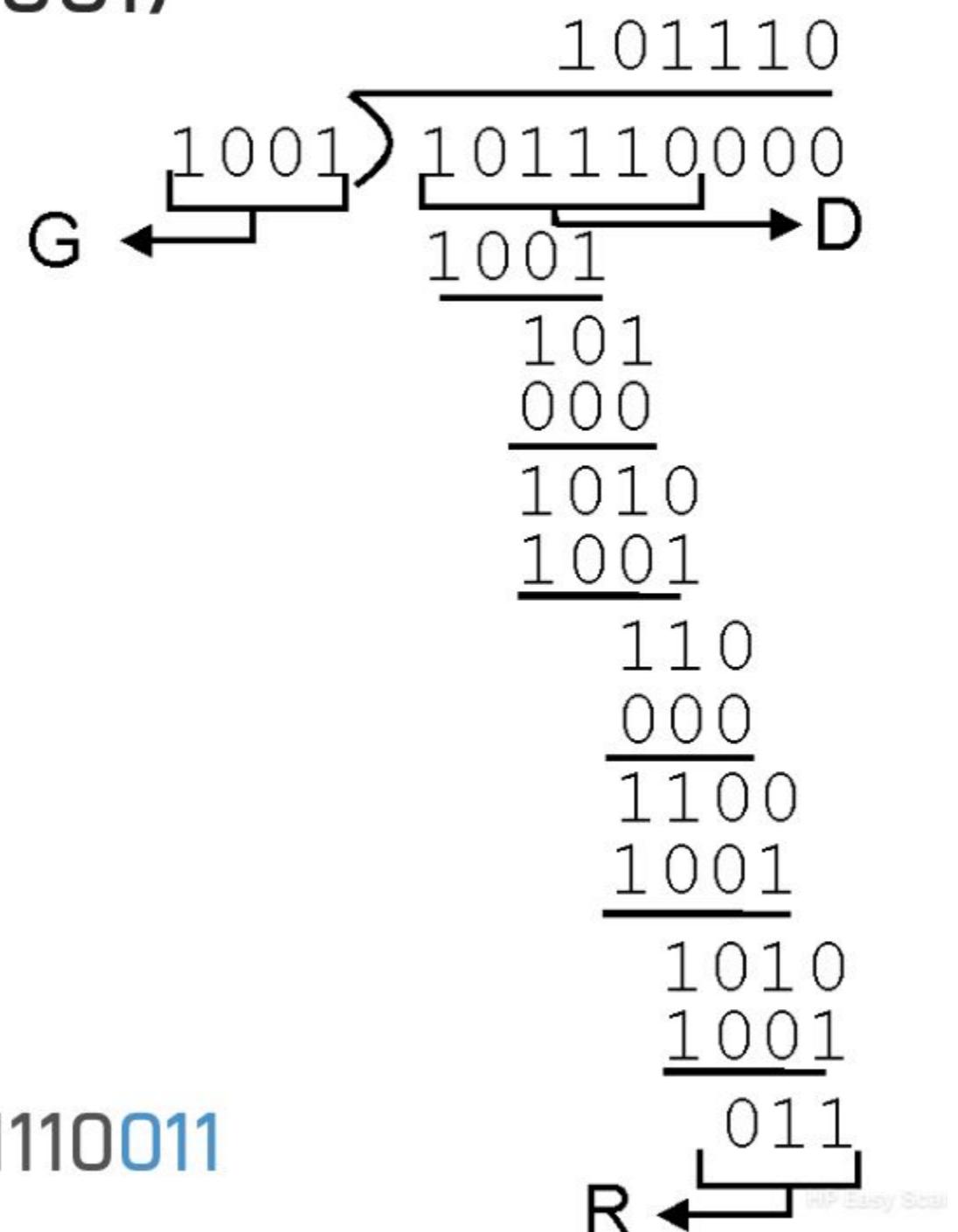
Detekce všech shlukových chyb do délky r

Použité u Ethernetu, HDLC, ATM, ISDN ...

Standardizované generující polynomy pro CRC-8,12,16,32

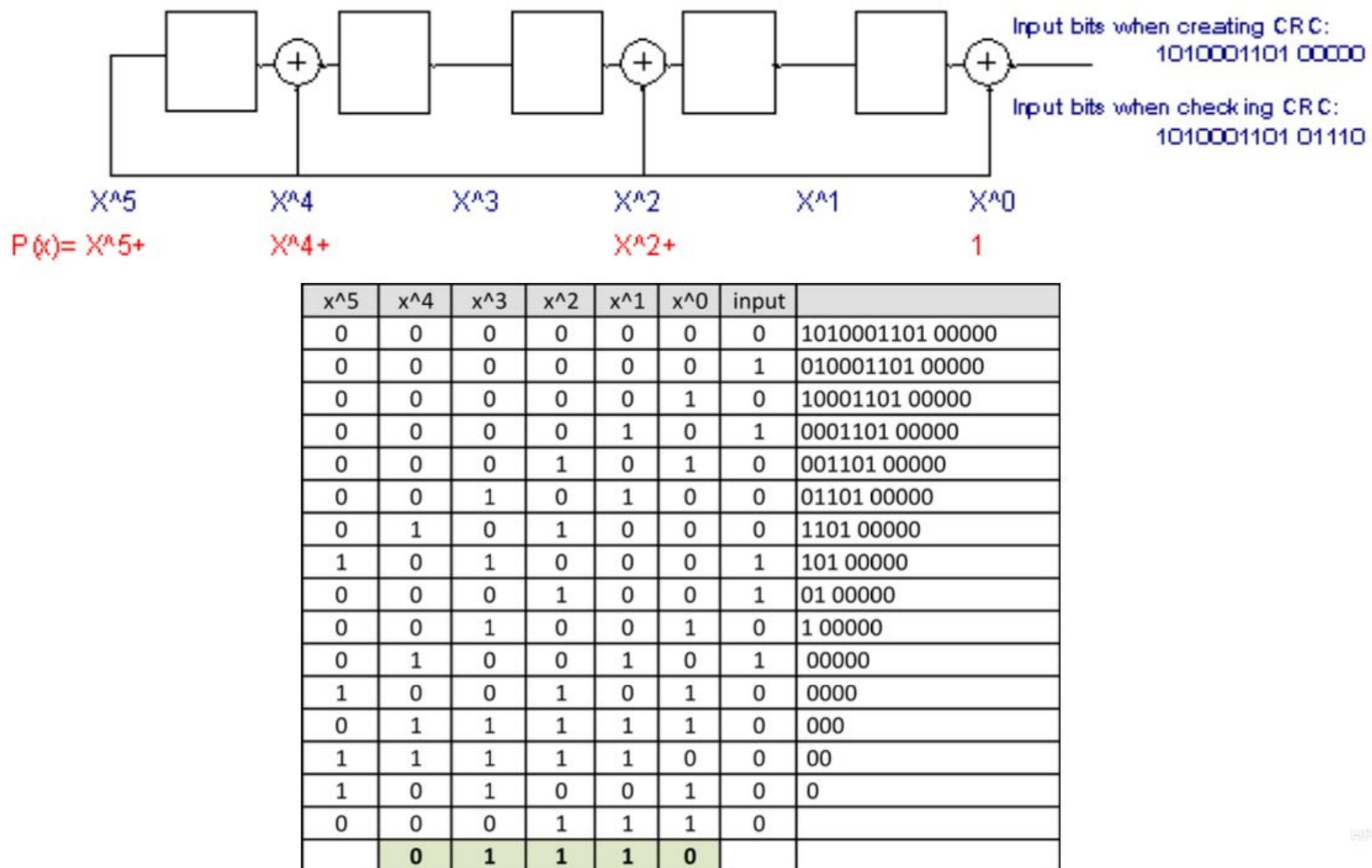
CRC příklad

- Generující polynom x^3+1 ($G = 1001$)
- Data: 101110



Přenášená zpráva: 101110011

CRC HW Implementace



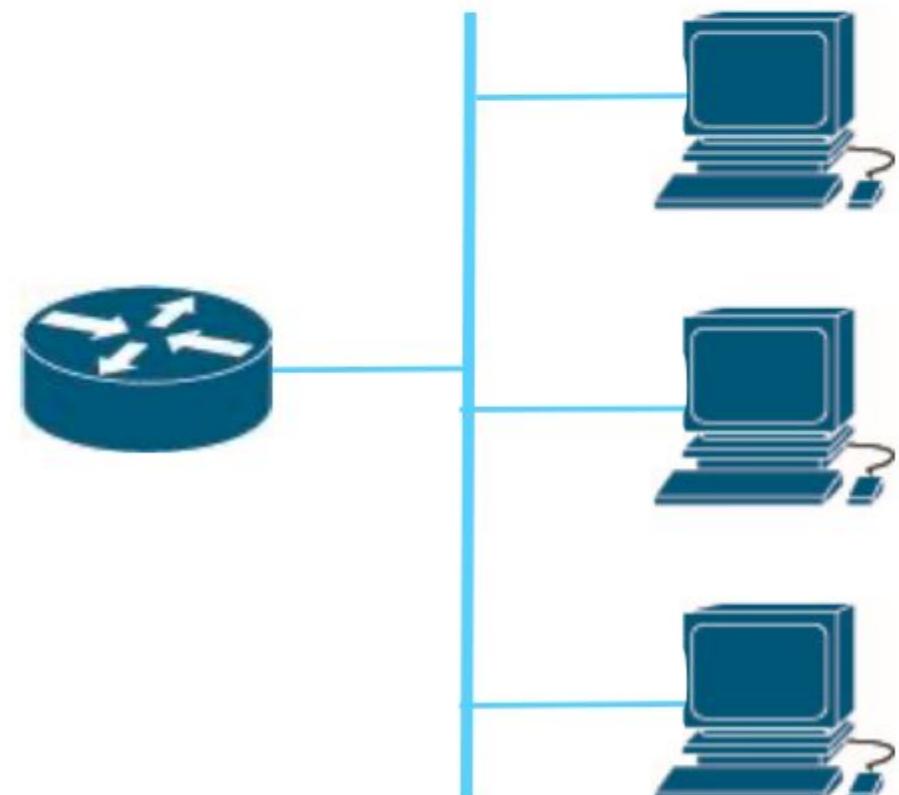
Řízení přístupu k sdílenému médiu

Typy linek

- **Bod-bod (point-to-point)**
 - PPP protokol pro vytáčenou telefonní linku
 - přepínaný Ethernet mezi hostem s přepínačem



- **Multi-access**
 - funguje broadcast
 - tradiční (historický) Ethernet
 - 802.11 bezdrátové sítě
 - odchozí datový tok HFC (Hybrid Fiber-Coax)



Řízení přístupu

Máme

- Jeden sdílený přenosový kanál (médium)
- Dva a více uzlů vysílající data ve stejném čase: interference

Chceme

- Férově rozdělit dostupnou kapacitu pro přenos

Protokoly pro řízení přístupu

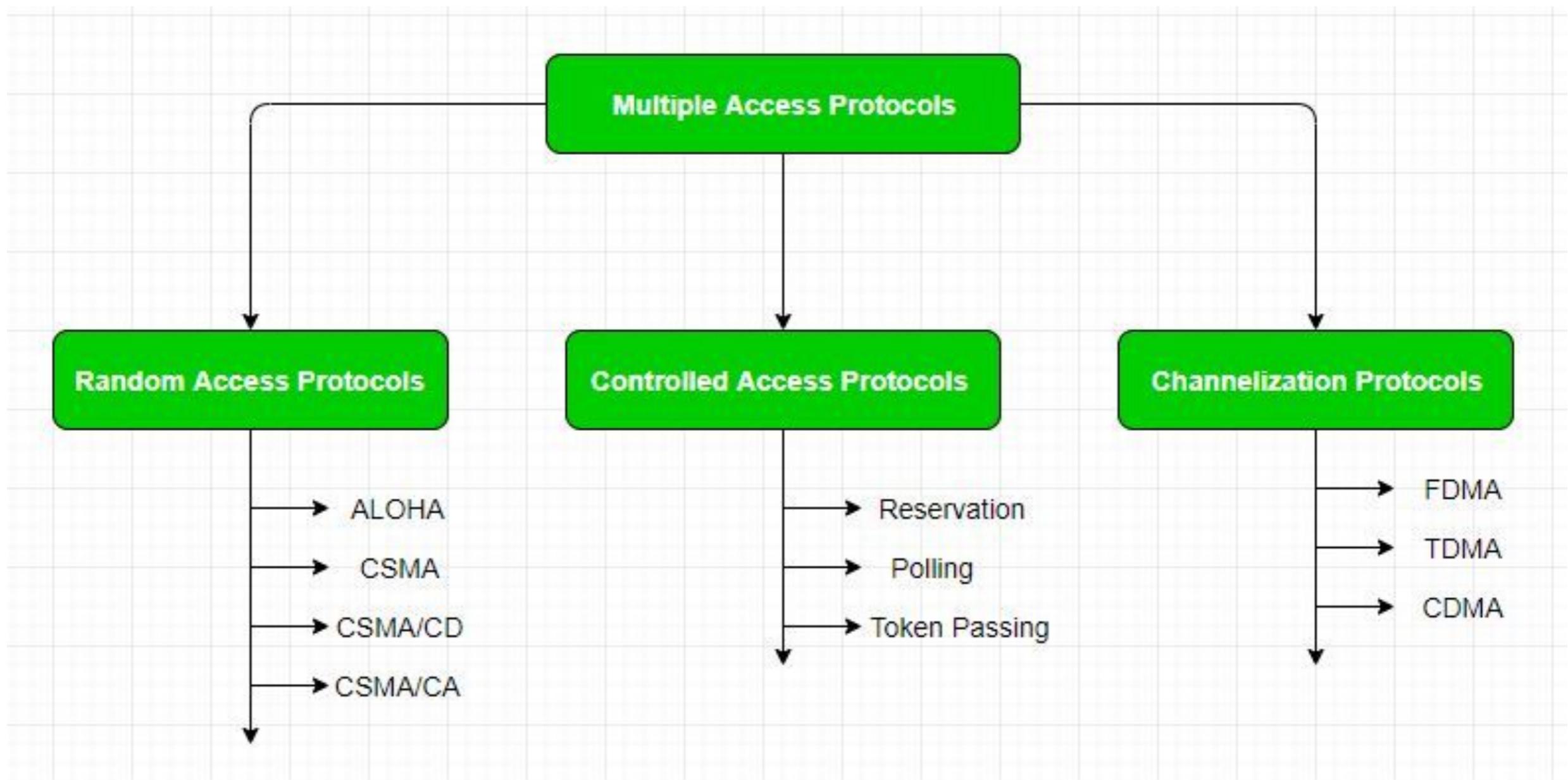
Distribuovaný algoritmus určující jak uzly budou sdílet společný přenosový kanál, určit kdy uzel může vysílat data.

Informace o řízení přístupu musí použít tento přenosový kanál.

Ideální protokol pro kanál s propustností R:

- a) Když má pouze jeden uzel data k odeslání, propustnost R.
- b) Když M uzlů má data k odeslání, každý z těchto uzlů má spravedlivý podíl na šířce pásma kanálu.
- c) Protokol je decentralizován, tj. neexistuje žádný hlavní uzel představuje jeden bod selhání.
- d) Protokol je jednoduchý a snadno realizovatelný.

Protokoly

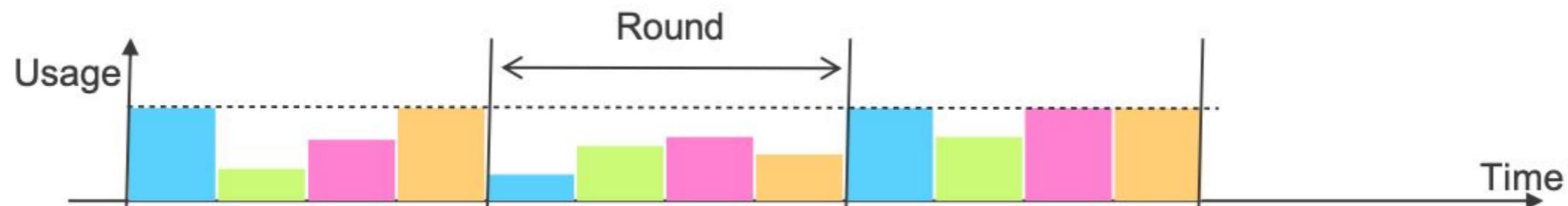


TDMA

Time Division Multiple Access

Jsou definovány intervaly (sloty), kdy může stanice přistupovat k médiu:

- Intervaly se střídají v rámci kola
- Nevyužité časové sloty jsou prázdné
- Využití je nízké - počet obsazených/počet slotů celkem
- Vyšší zpoždění v případě dlouhého kola

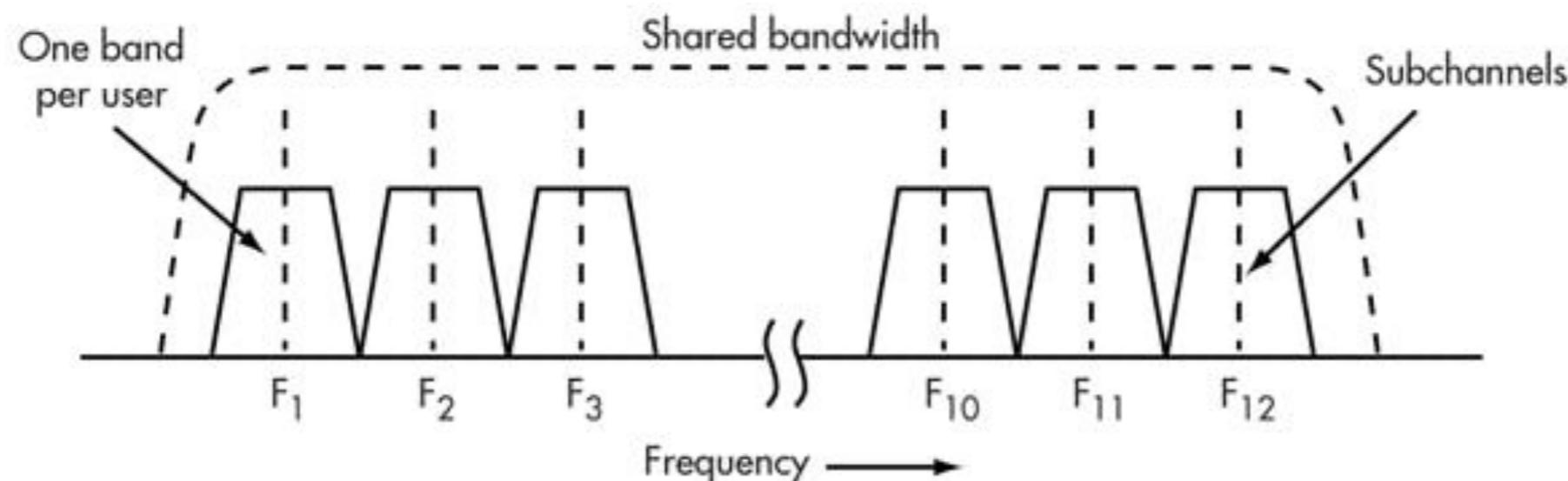


FDMA

Frequency division multiple access

Dostupné přenosové pásma je rozděleno do několika oblastí dle frekvencí:

- Uzly mohou přenášet data v jeden čas
- Každá stanice má přiděleno určité frekvenční pásma
- Nevyužité frekvenční pásma

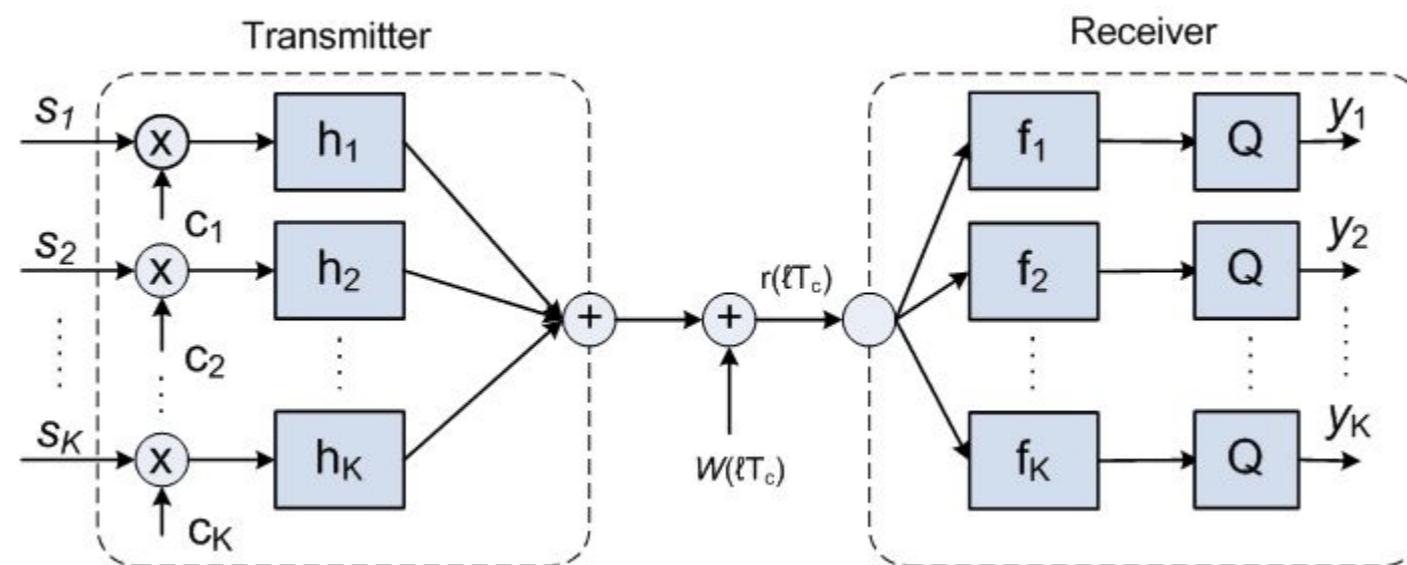


CDMA

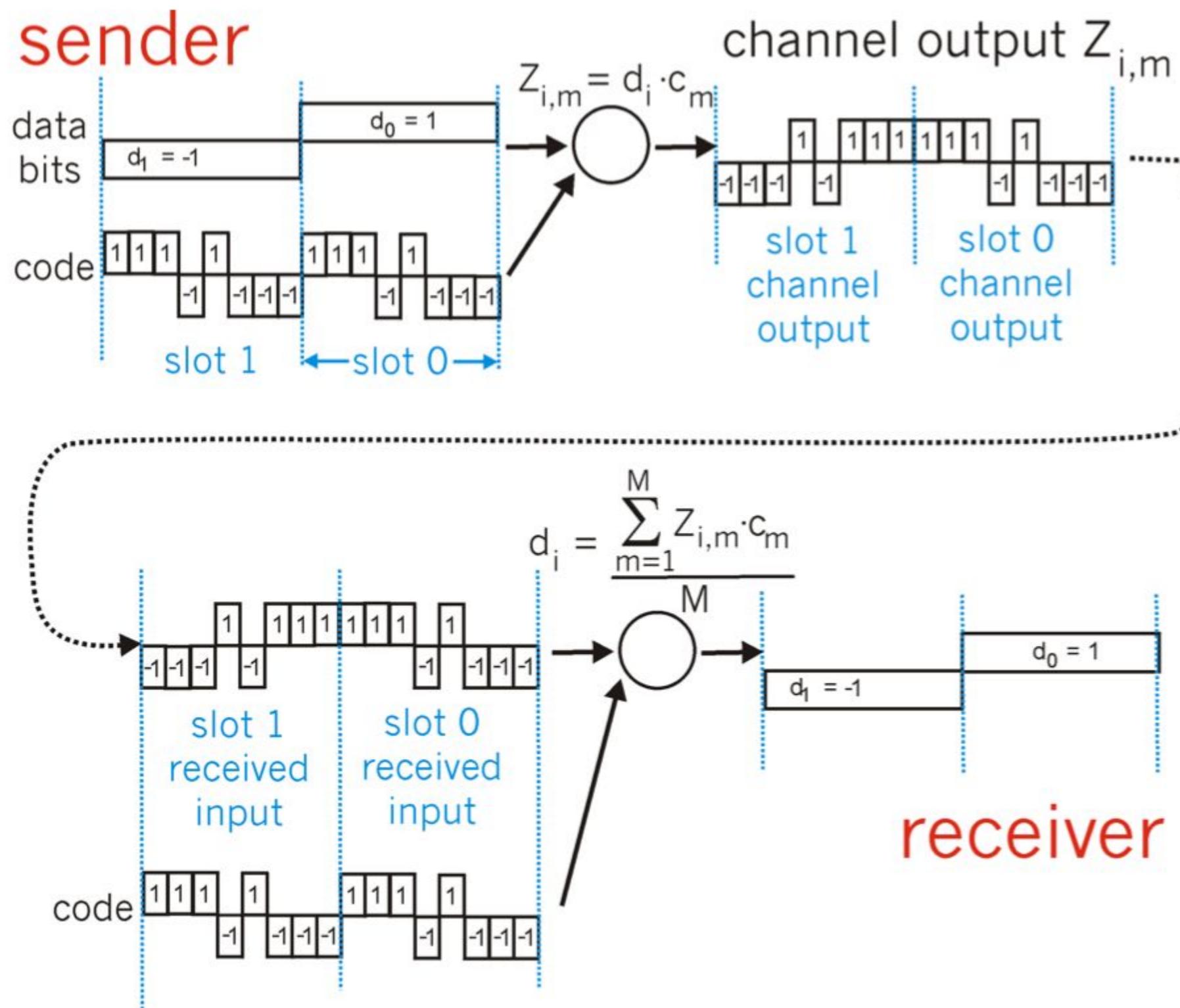
Code Division Multiple Access

Jedinečný identifikátor (code) je přiřazen každému uživateli:

- Kódy jsou ortogonální
- Všichni uživatelé sdílejí stejnou frekvenci
- Každý uživatel zakóduje zprávu pomocí svého kódu
- Umožňuje sdílení média více uživateli současně
- Používá se v bezdrátových sítích

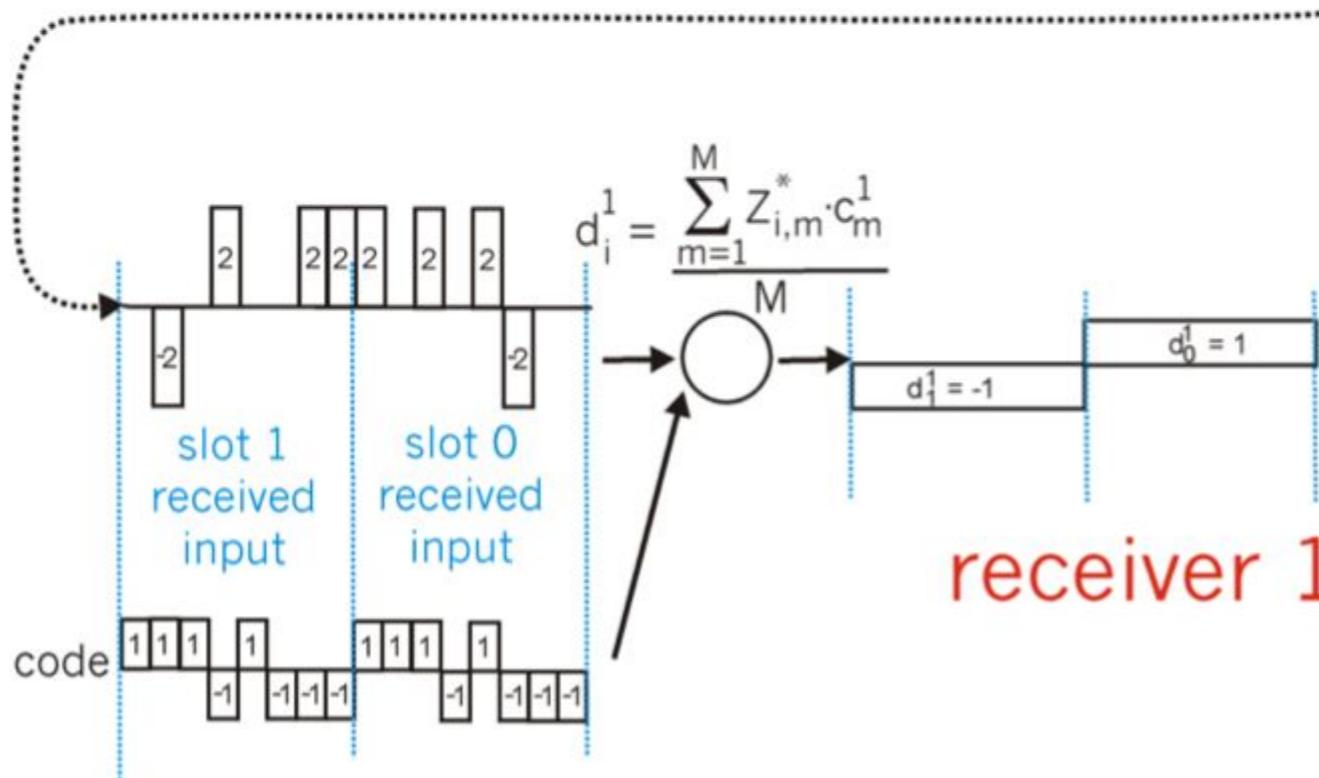
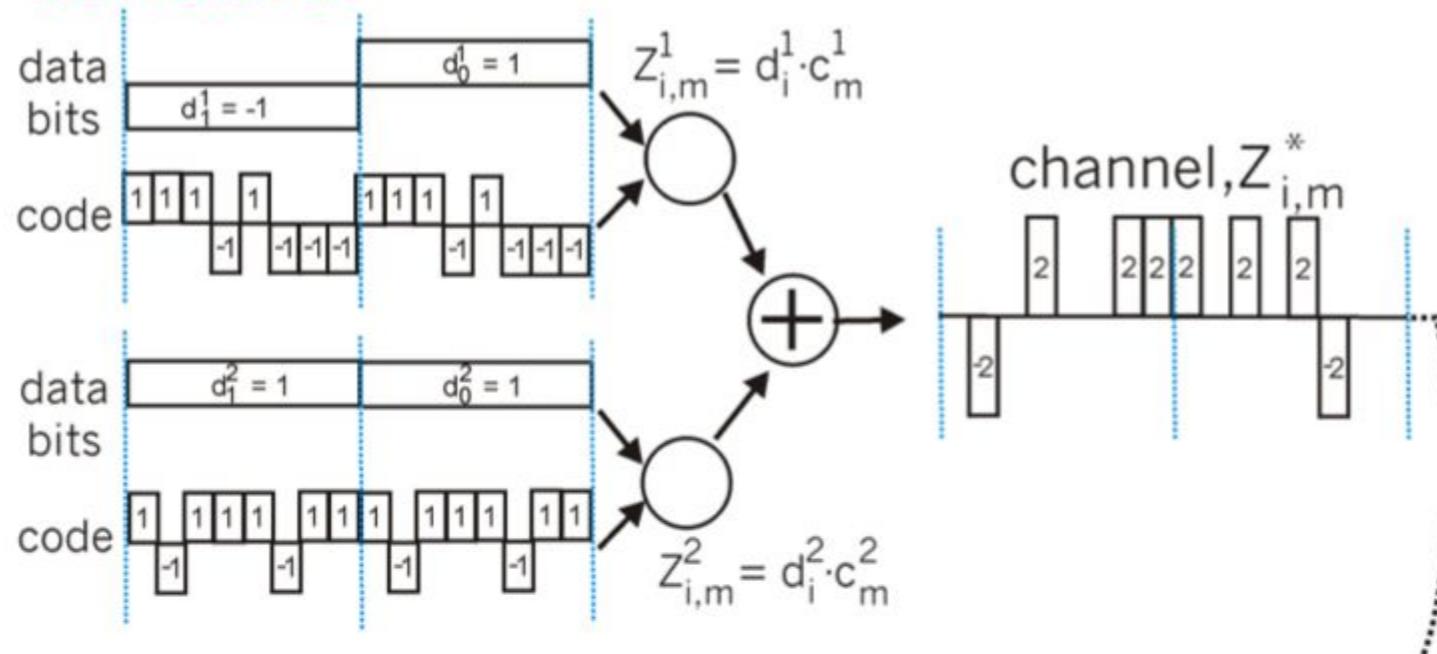


CDMA princip



CDMA příklad

senders



Podmínka ortogonality

$$\sum_{m=1}^M c_m^2 \times c_m^1 = 0$$

$$1 \cdot 1 + 1 \cdot (-1) + 1 \cdot 1 + (-1) \cdot 1 + \\ 1 \cdot 1 + (-1) \cdot (-1) + (-1) \cdot 1 + (-1) \cdot 1 = 0$$

$$\begin{aligned} \sum_{m=1}^M z_{i,m}^* \times c_m^1 &= \sum_{m=1}^M z_{i,m}^1 \times c_m^1 + \sum_{m=1}^M z_{i,m}^2 \times c_m^1 \\ &= \sum_{m=1}^M d_i^1 \times c_m^1 \times c_m^1 + \sum_{m=1}^M d_i^2 \times c_m^2 \times c_m^1 \\ &= d_i^1 \sum_{m=1}^M c_m^1 \times c_m^1 + d_i^2 \sum_{m=1}^M c_m^2 \times c_m^1 \\ &= d_i^1 + 0 \end{aligned}$$

Protokoly s náhodným přístupem

Zabrání celé kapacity média v případě, že chce stanice vyslat data.

Kolize v případě, že více stanic chce vysílat současně.

Protokol specifikuje:

- Detekci kolizí
- Zotavení se z kolize

Protokoly:

- Slotted ALOHA
- ALOHA
- CSMA, CSMA/CD, CSMA/CA

Slotted ALOHA

PRINCIP:

Všechny rámce mají stejnou fixní velikost

Čas je rozdělen do stejných časových slotů (1 rámec)

Uzly začínají vysílat pouze na začátku slotu

Uzly jsou synchronizované

V případě současného vysílání, všechny uzly detekují kolizi

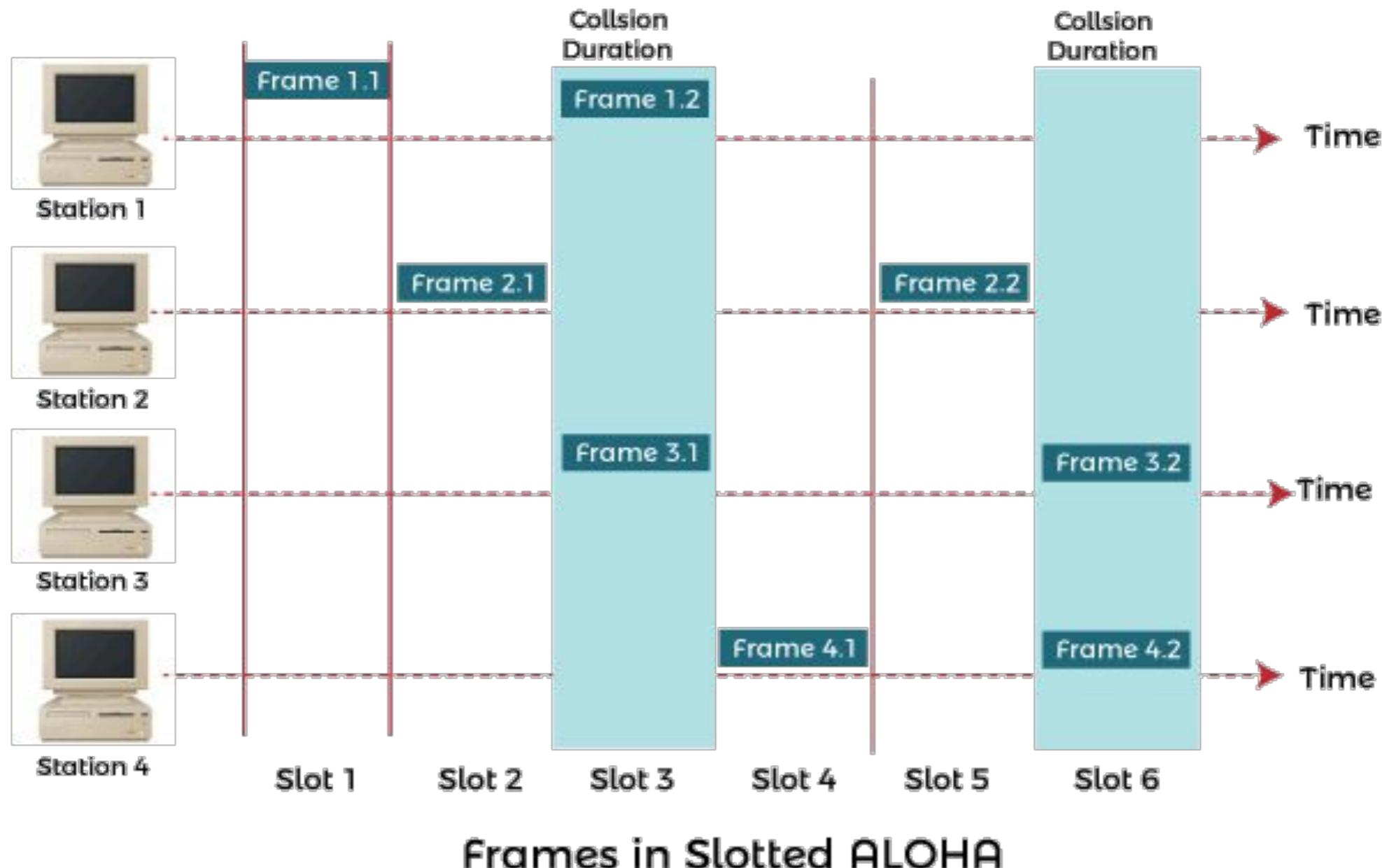
POSTUP:

Uzel čeká na začátek časového slotu pro zaslání nového rámce

Není-li kolize uzel pokračuje v posílaní i dalším slotu

V případě kolize je snaha o znovu zaslání rámce v dalším slotu

SLOTTED ALOHA

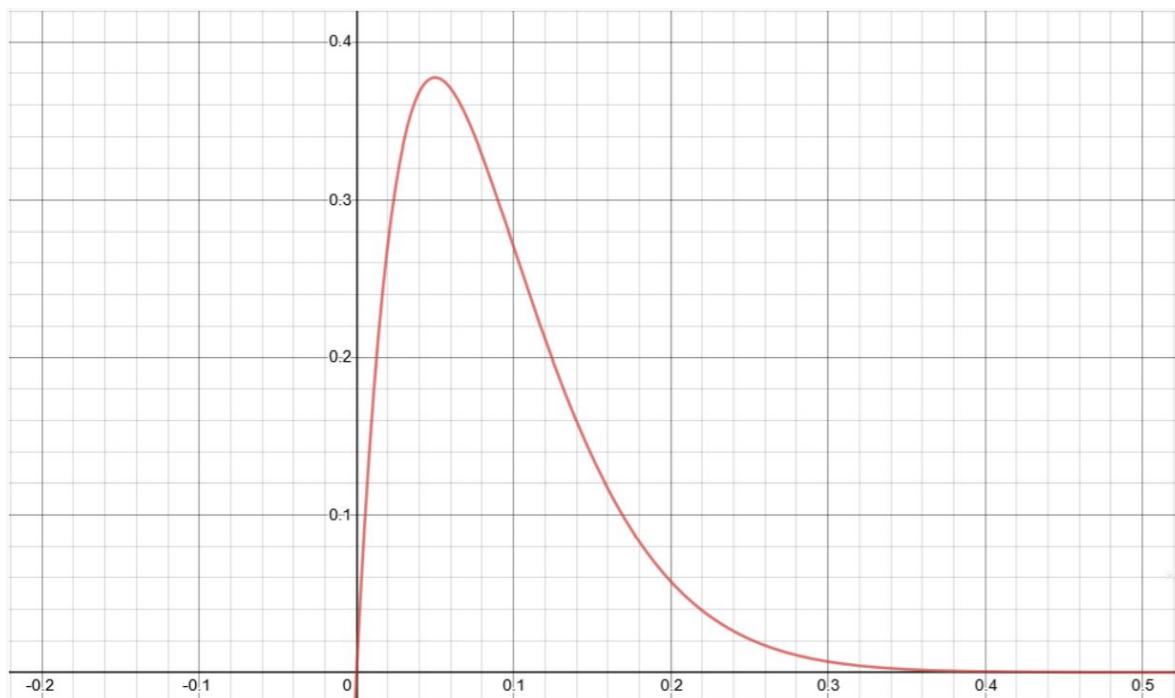


Slotted ALOHA efektivnost

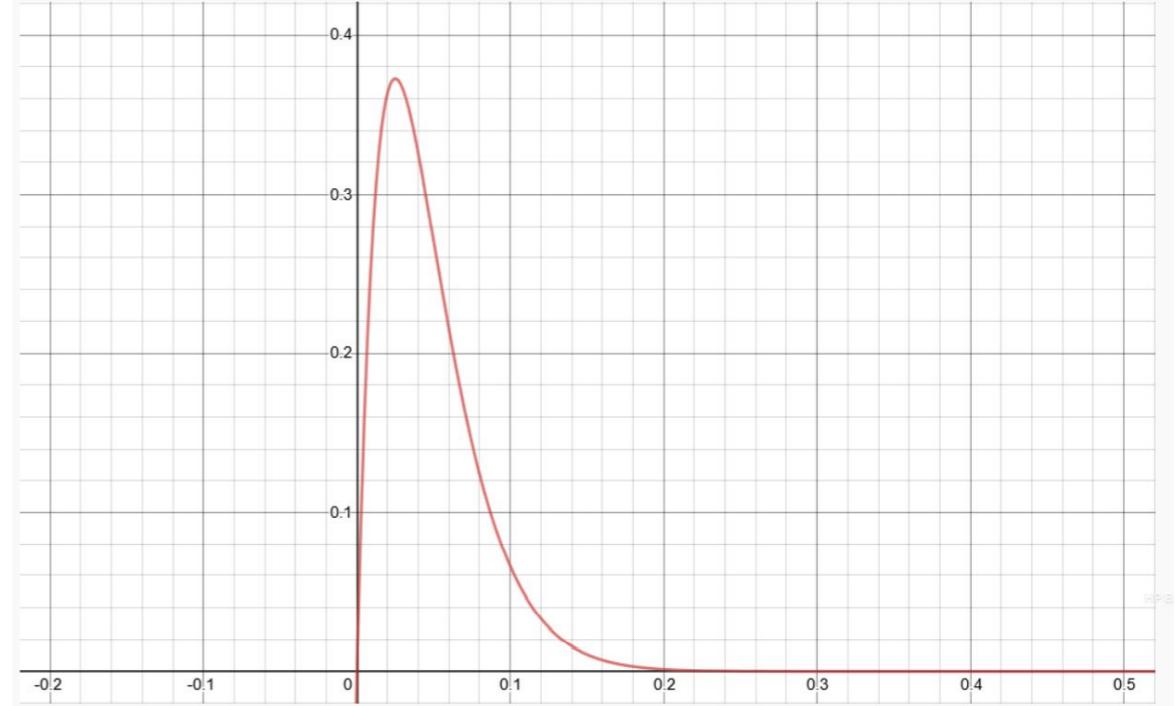
Pravděpodobnost přenosu dat..... p

Průměrná propustnost pro jeden uzel..... $p.(1-p)^{N-1}$

Propustnost pro N uzelů..... $Np.(1-p)^{N-1}$



$N=20$

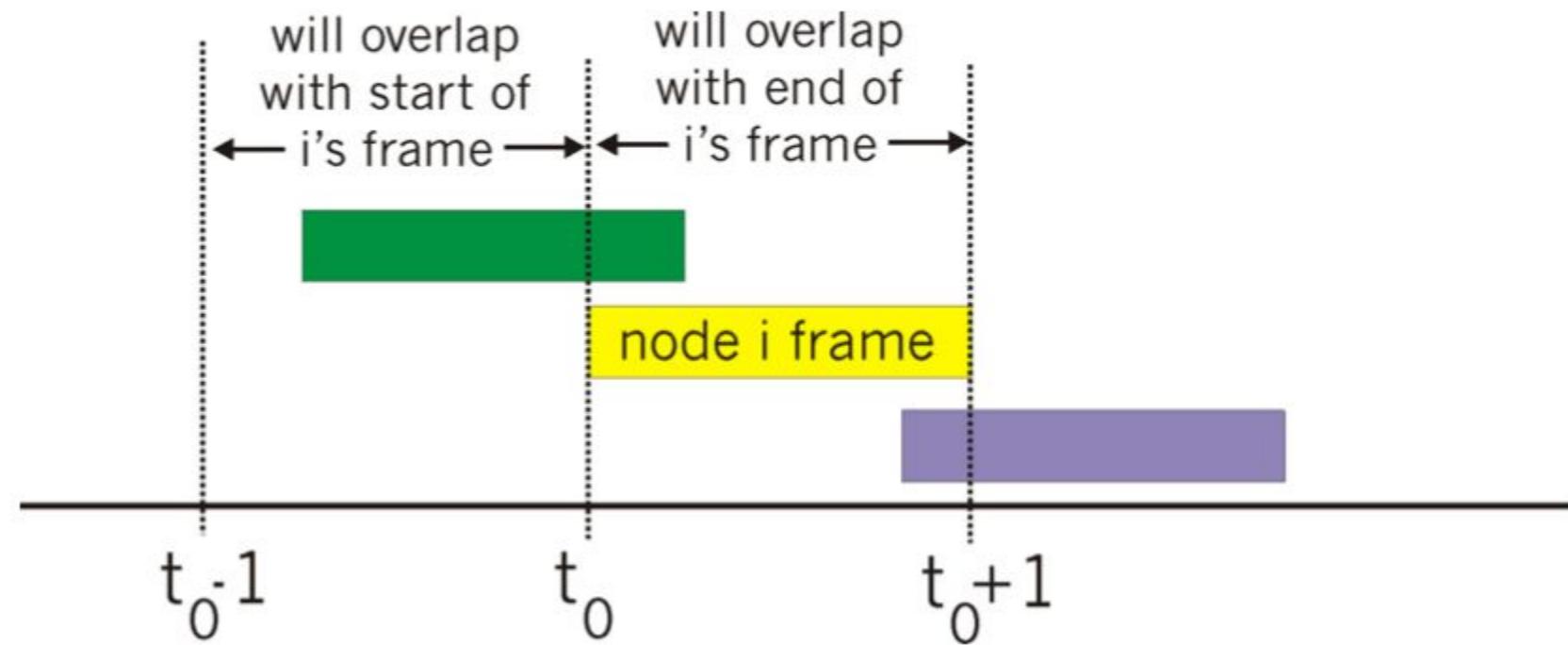


$N=40$

Pure ALOHA

Jednodušší, žádná synchronizace

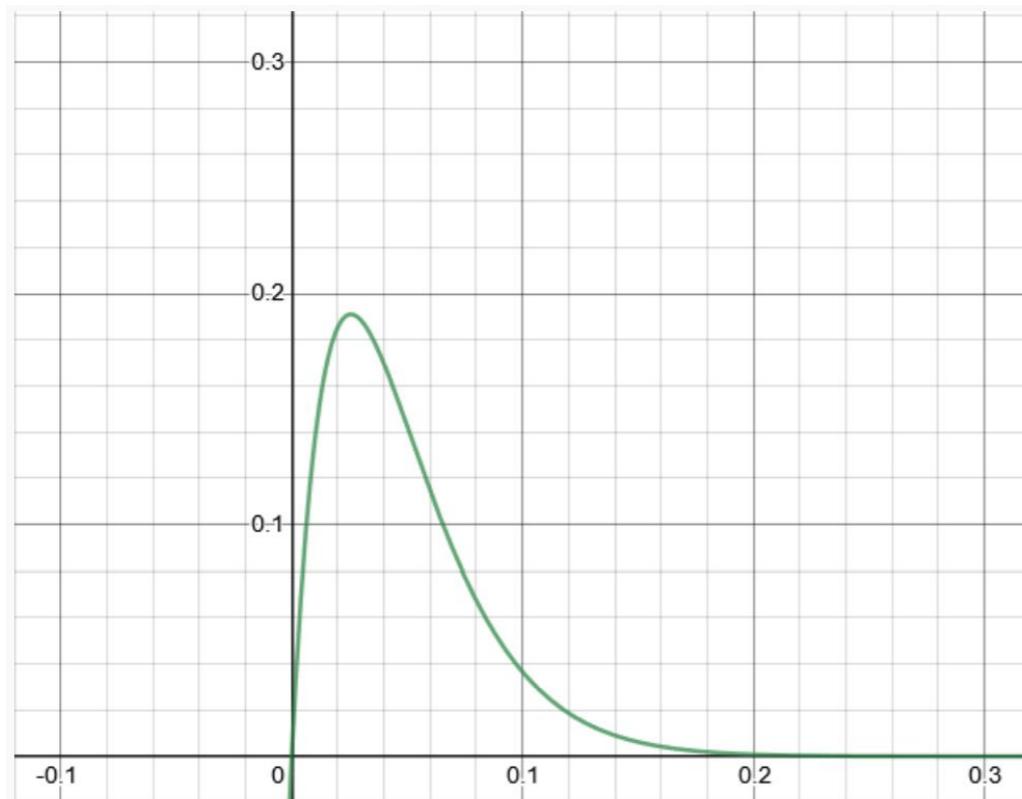
- Odesílání okamžitě, bez čekání na začátek slotu
- Pravděpodobnost kolize vzrůstá



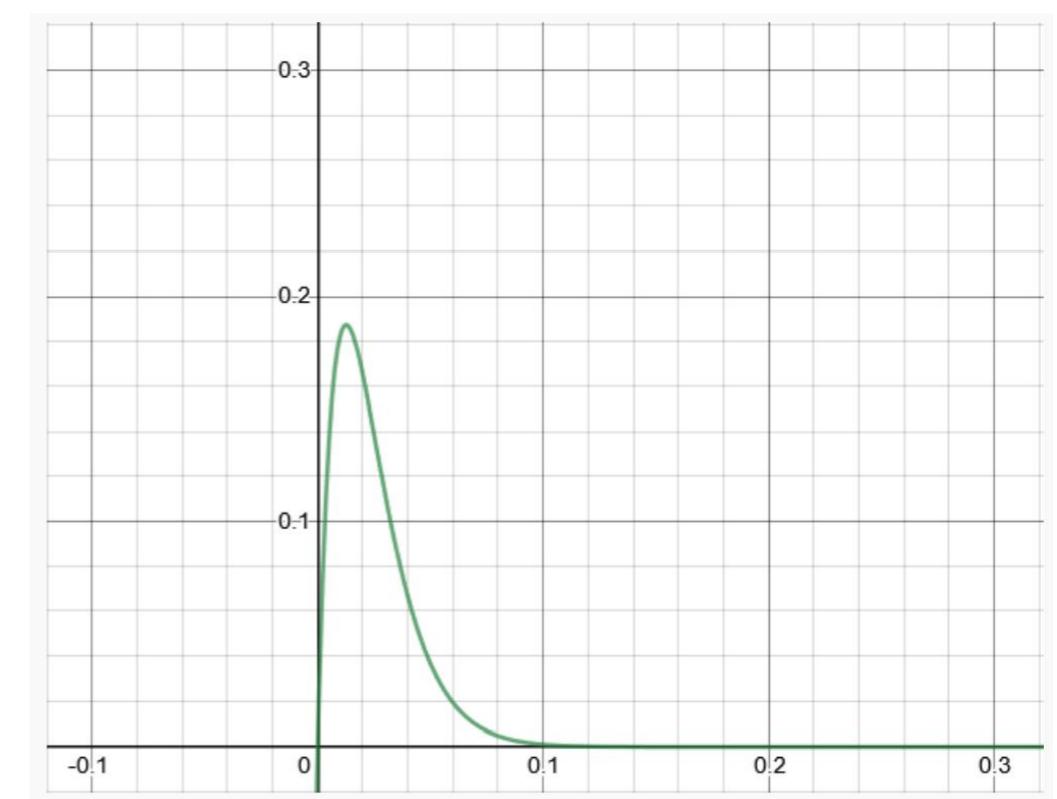
Pure ALOHA

Rámeč může kolidovat s rámci v „jiném slotu“..... $N \cdot p(1-p) \cdot p(1-p)$

Pro N uzlů..... $N \cdot p \cdot (1-p)^{2(N-1)}$



$N=20$



$N=40$

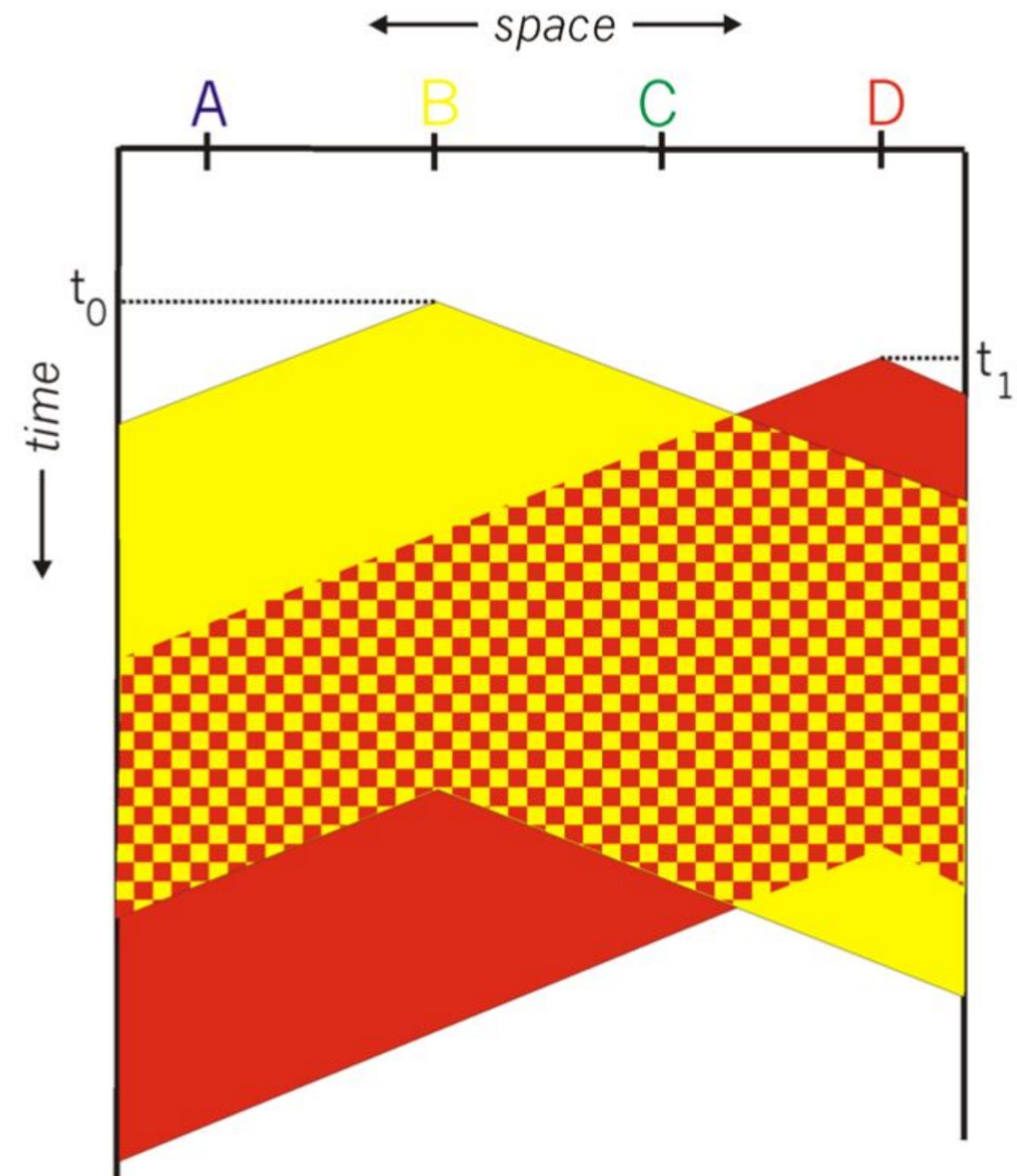
CSMA

Carrier Sense Multiple Access

- Je-li médium volné odešli rámec
- Je-li médium obsazené pak čekej

Kolize

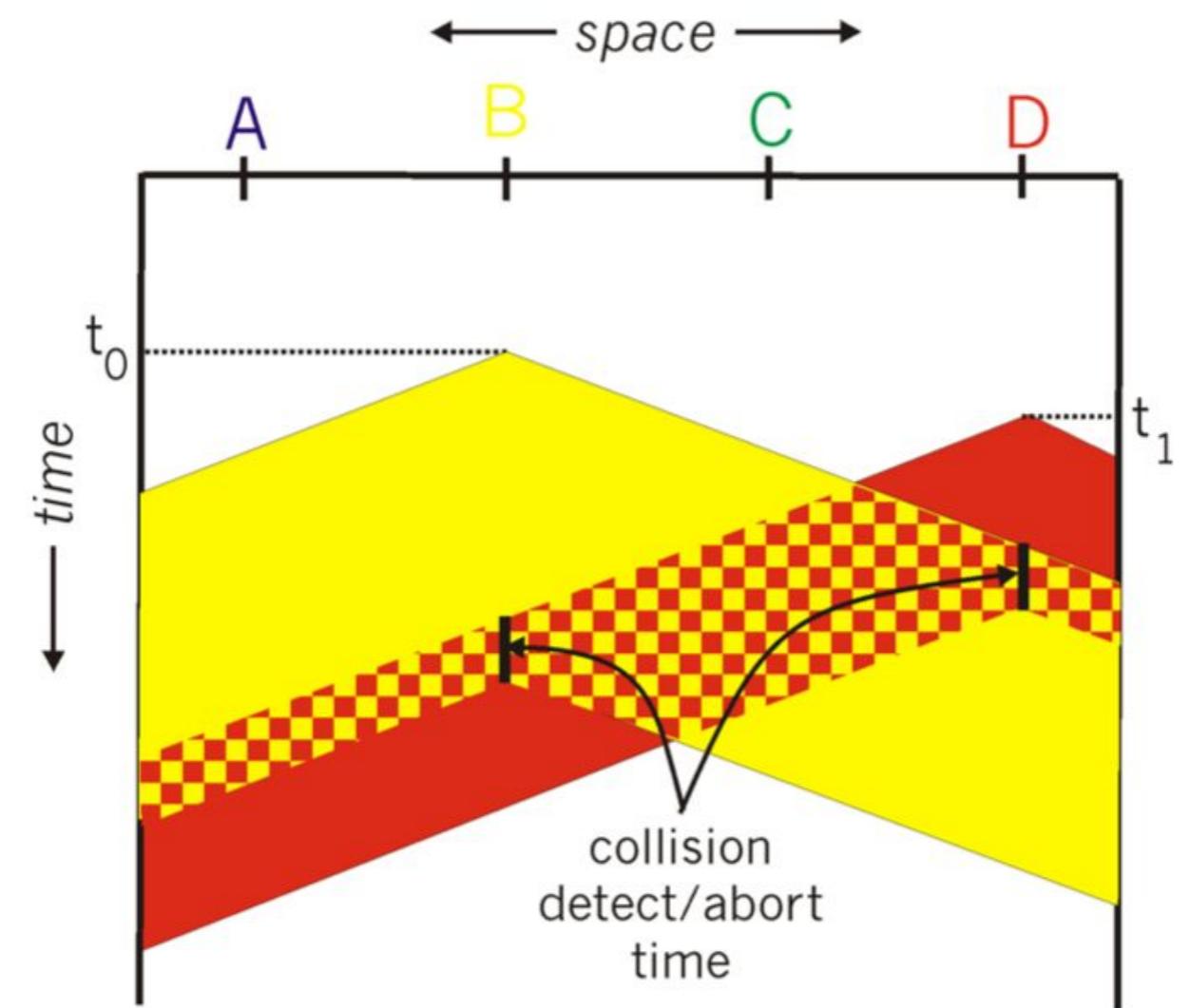
- Doba šíření signálu
- Celý kolizní rámec je nepoužitelný



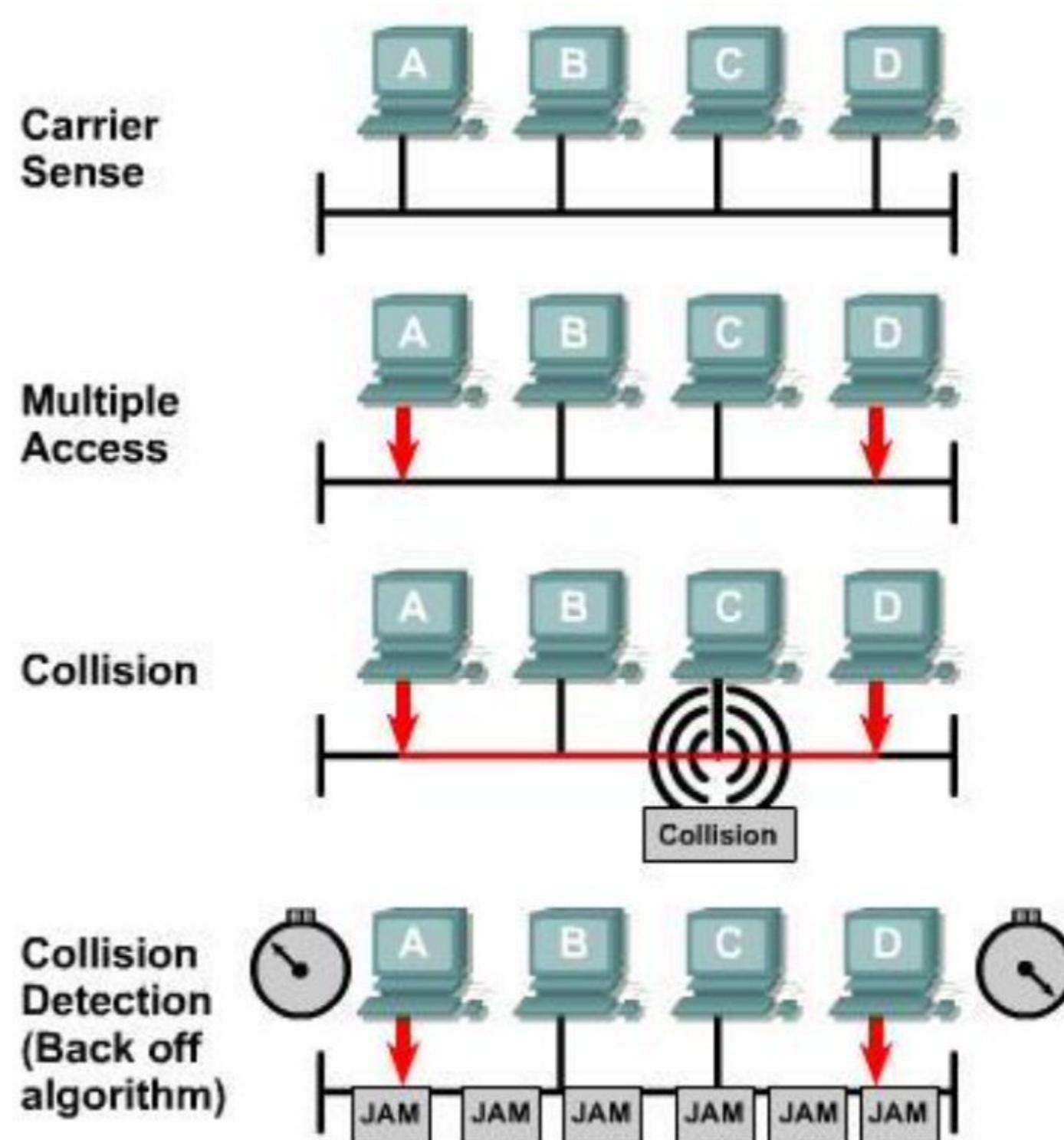
CSMA/CD

Collision Detection

- po detekci kolize je přenos okamžitě ukončen
- Šetření přenosovým pásmem
- jednoduché v drátových sítích
- těžké pro bezdrátové spoje, přijímač je při vysílání vypnuto



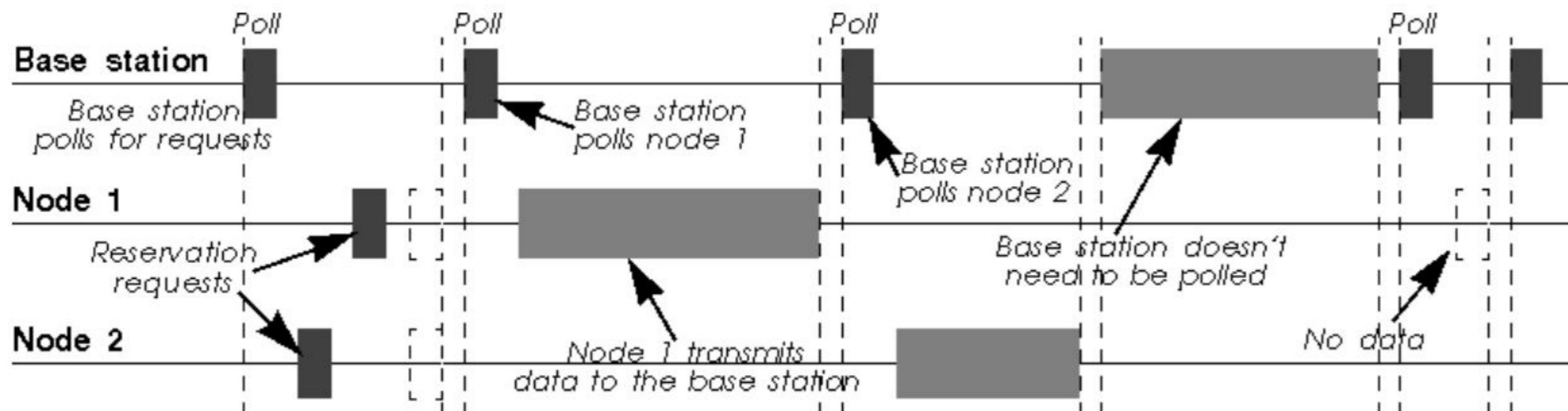
CSMA/CD na sdíleném médiu



Polling protocol

Master uzel vyzývá uzly k odesílání dat:

- Režie vyzývání
- Zpoždění při čekání na dotaz
- Selhání master uzlu



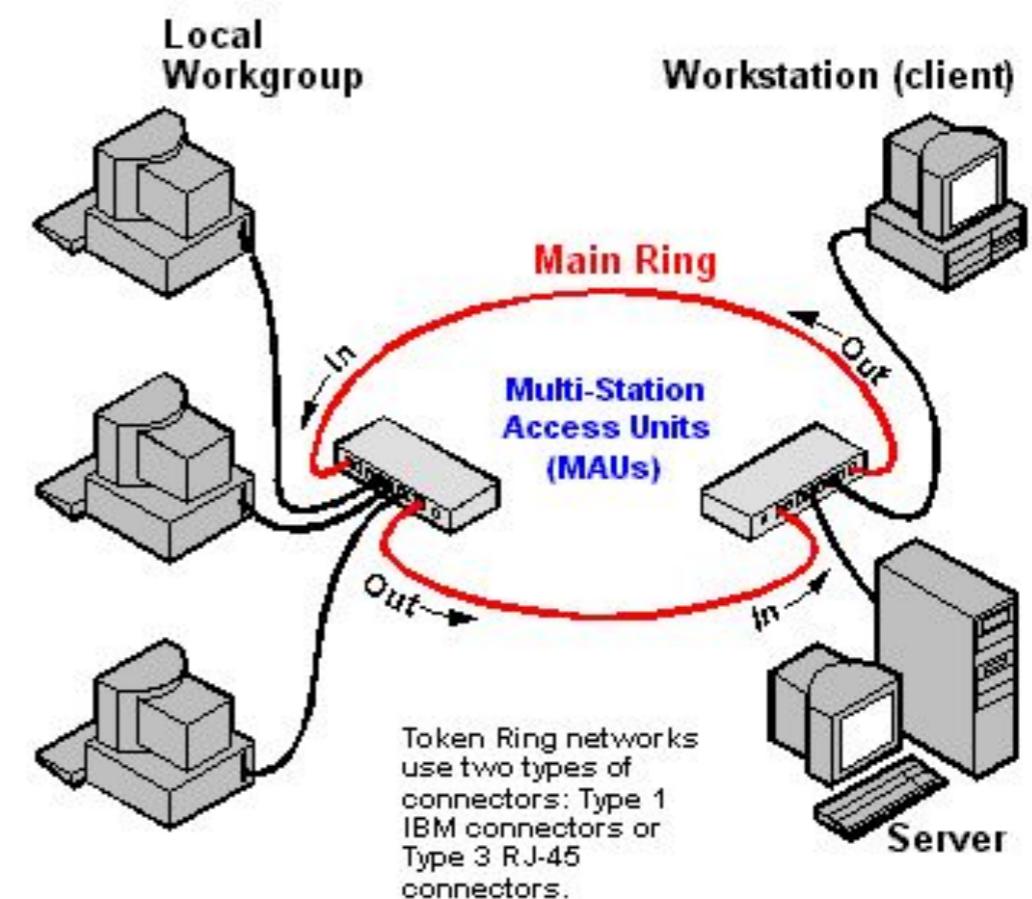
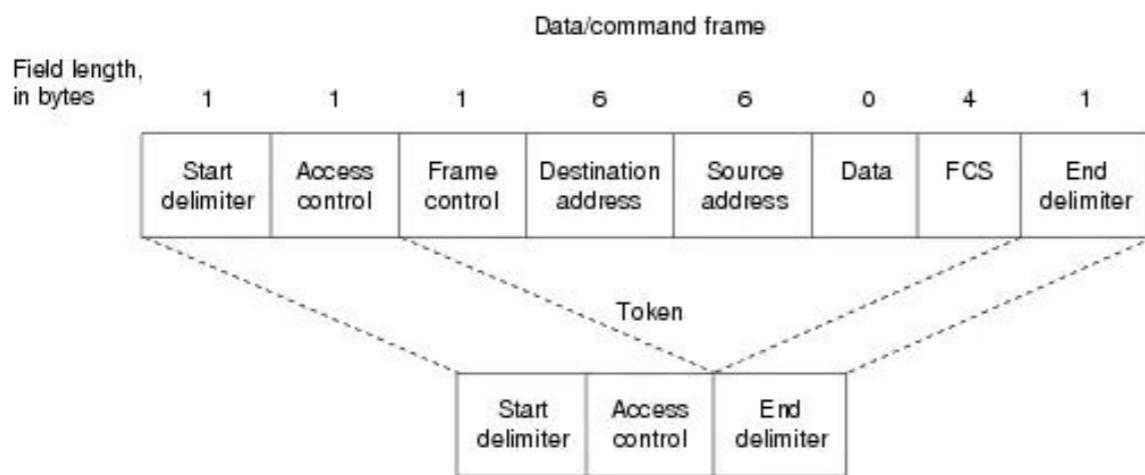
Token-ring

PRINCIPY

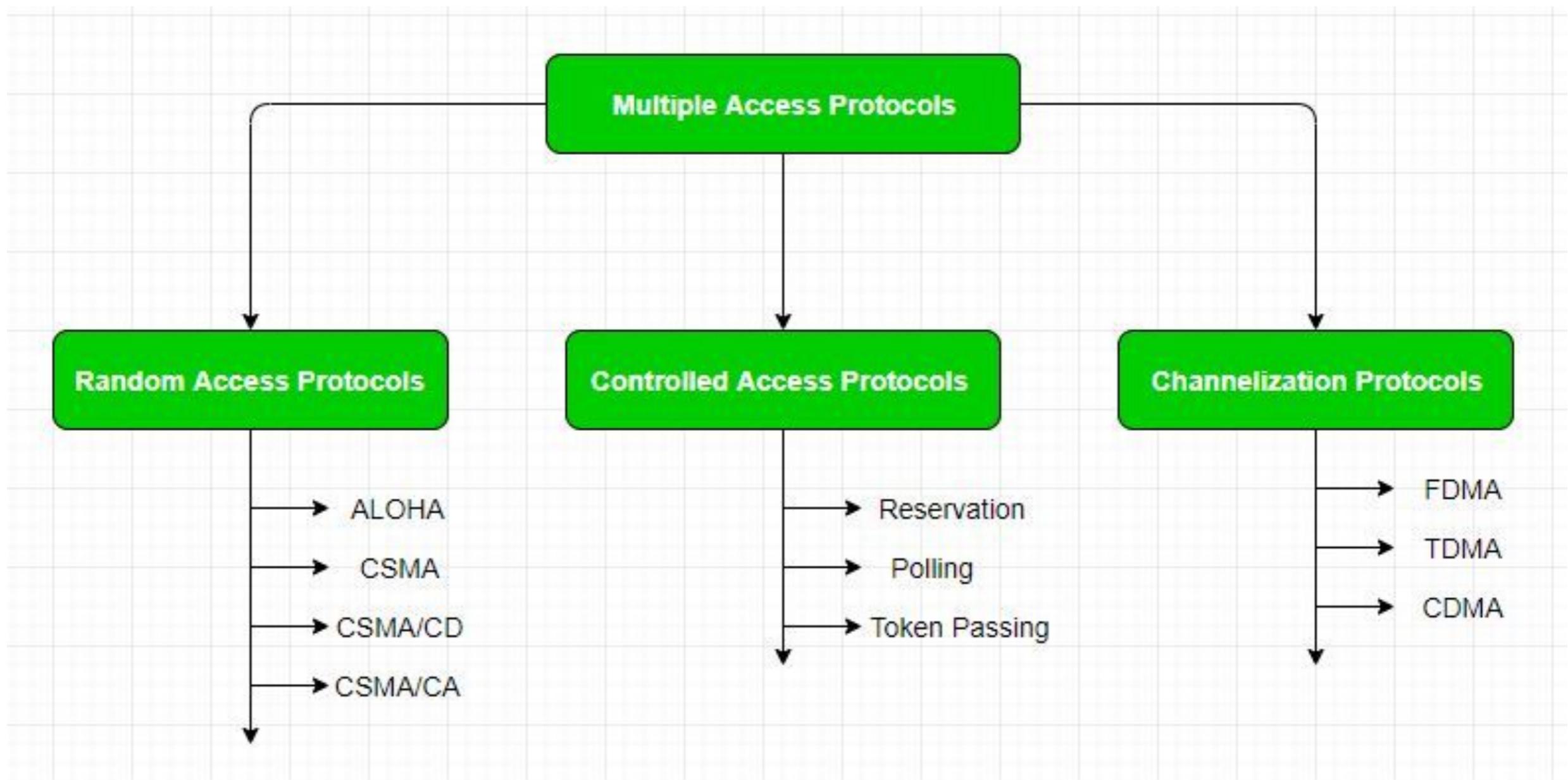
- Řídící žeton je zasílán sekvenčně mezi uzly ve zvláštní zprávě
- Režie předávání žetonu
- Zpoždění při čekání na žeton
- Ztráta žetonu

TECHNOLOGIE:

- IEEE 802.5 Token RING



Protokoly přístupu



ETHERNET

Ethernet

IEEE Standard 802.3

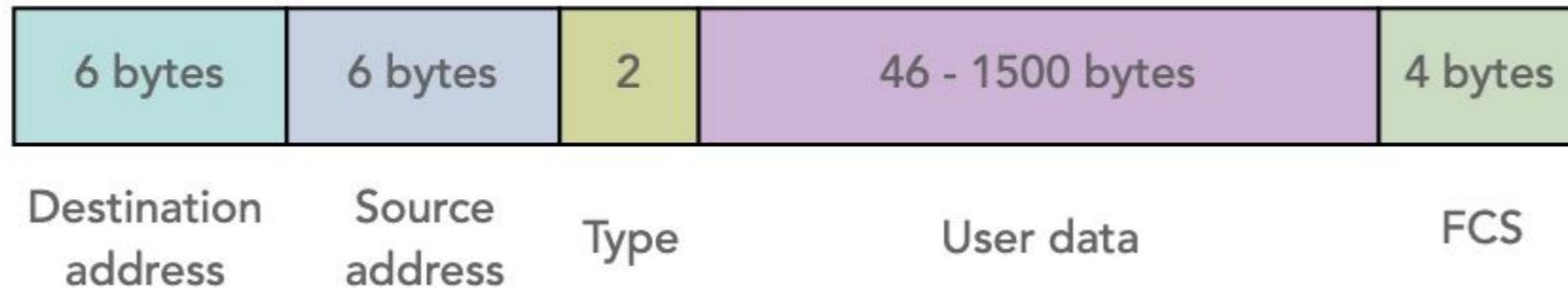
Levná technologie

- Nejpoužívanější LAN technologie současnosti
- Snadná instalace a správa
- Spolehlivost

Různé rychlosti od 10Mb/s do 400Gb/s

- Sdílené médium
- Přepínaný Ethernet
- Half-duplex / Full-duplex

Struktura rámce



```
> Frame 25: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
└╼ Ethernet II, Src: b0:7f:b9:ff:70:aa, Dst: 1c:87:2c:72:86:bc
    > Destination: 1c:87:2c:72:86:bc
    > Source: b0:7f:b9:ff:70:aa
    Type: ARP (0x0806)
    Padding: 0000000000000000000000000000000000000000000000000000000000000000
    > Address Resolution Protocol (reply)
```

0000	1c 87 2c 72 86 bc b0 7f b9 ff 70 aa 08 06 00 01	.,r..... .p....
0010	08 00 06 04 00 02 b0 7f b9 ff 70 aa 0a 00 00 01p....
0020	1c 87 2c 72 86 bc 0a 00 00 16 00 00 00 00 00 00	.,r..... ..p....
0030	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Vlastnosti

Posílání rámců:

- žádná synchronizace stavu
- nespolehlivá komunikace
- kontrolní součet pro detekci chybných rámců

Media Access Control

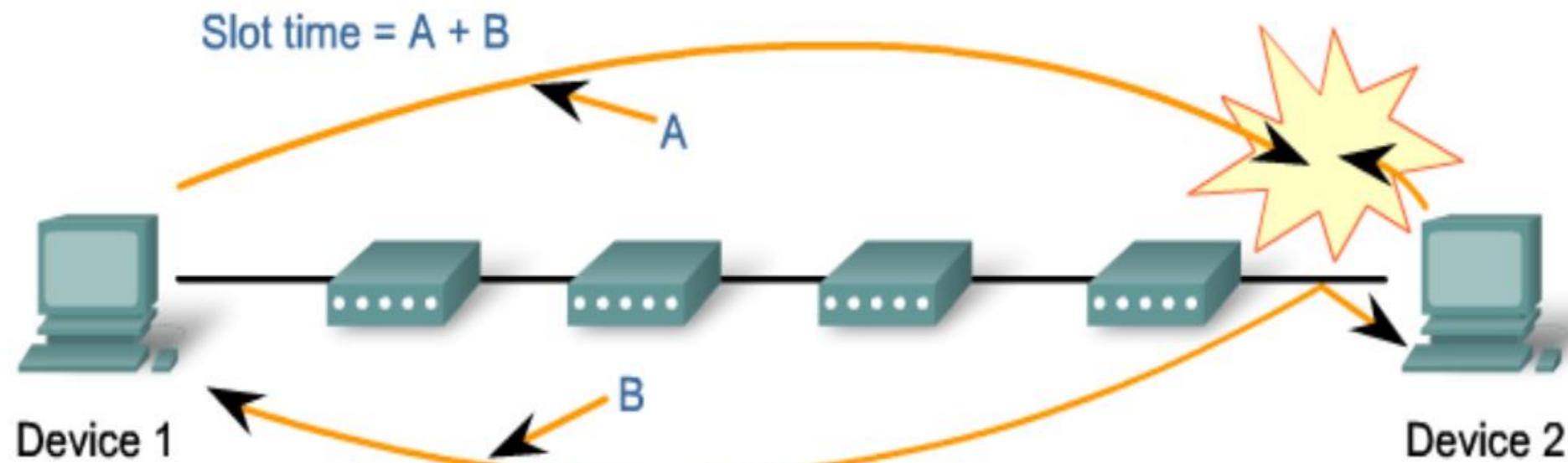
- Bezkolizní pro full-duplex (přepínaný ethernet)
- Používá CSMA/CD pro half-duplex (sdílené médium)

Praktické CSMA/CD

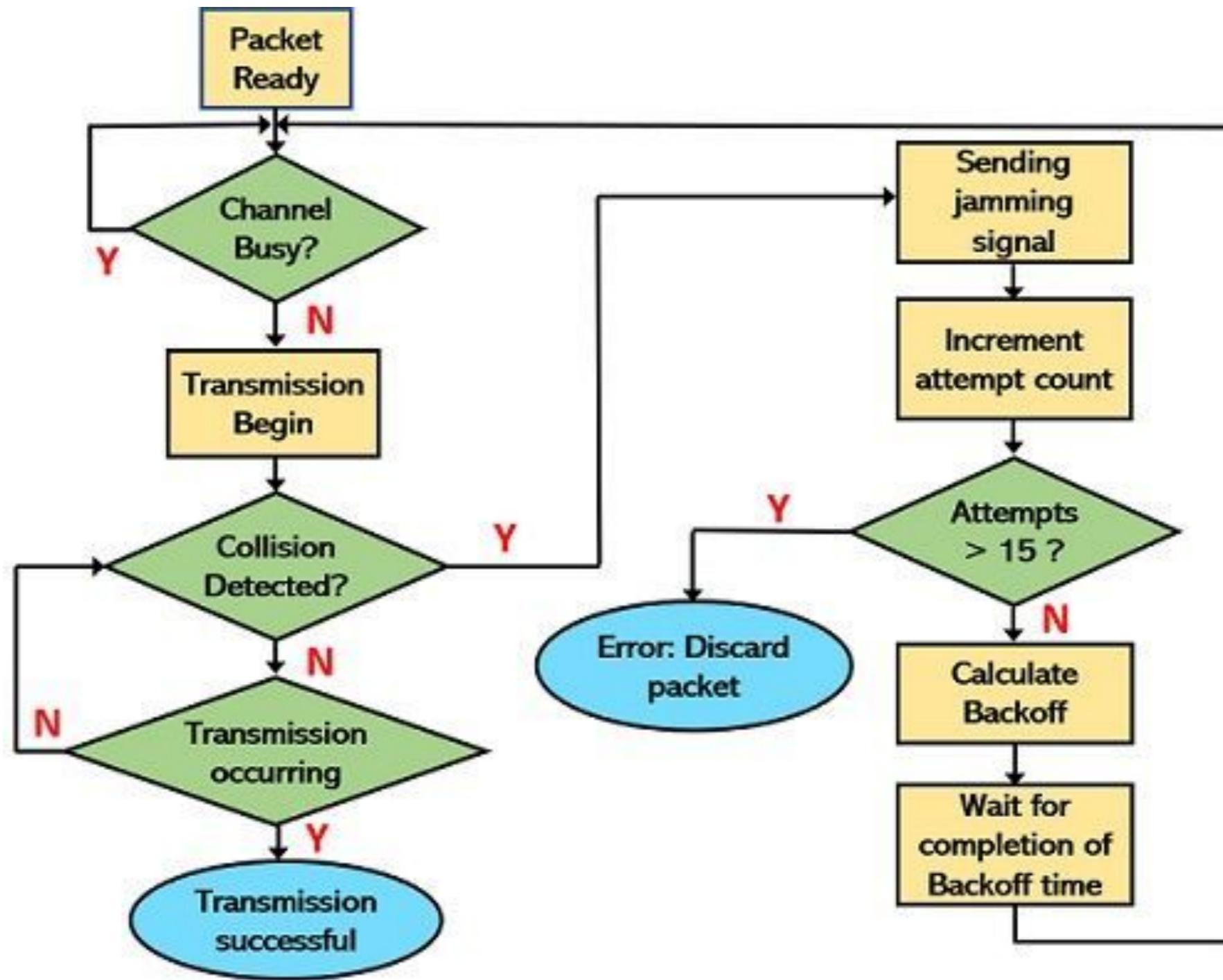
V případě kolize vysílající strany posílají 32-bitů dlouhou JAM posloupnost:

- stanice musí detekovat kolizi před dokončením přenosu
- rámce musí mít minimální velikost (64 bajtů)
- délka kabeláže musí být omezena (100m)

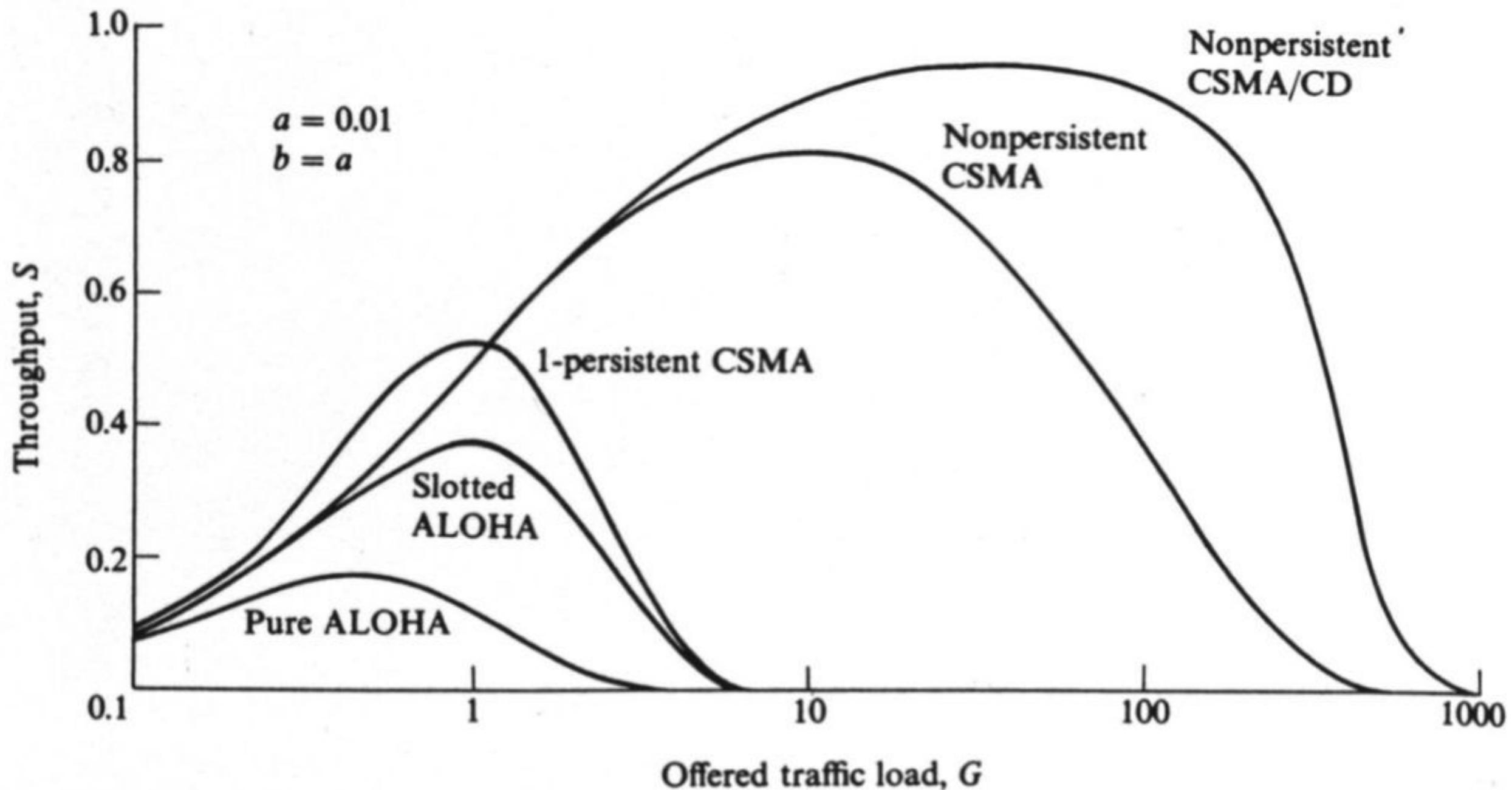
Co se stane, když nebude splněno?



CSMA/CD Backoff Timer



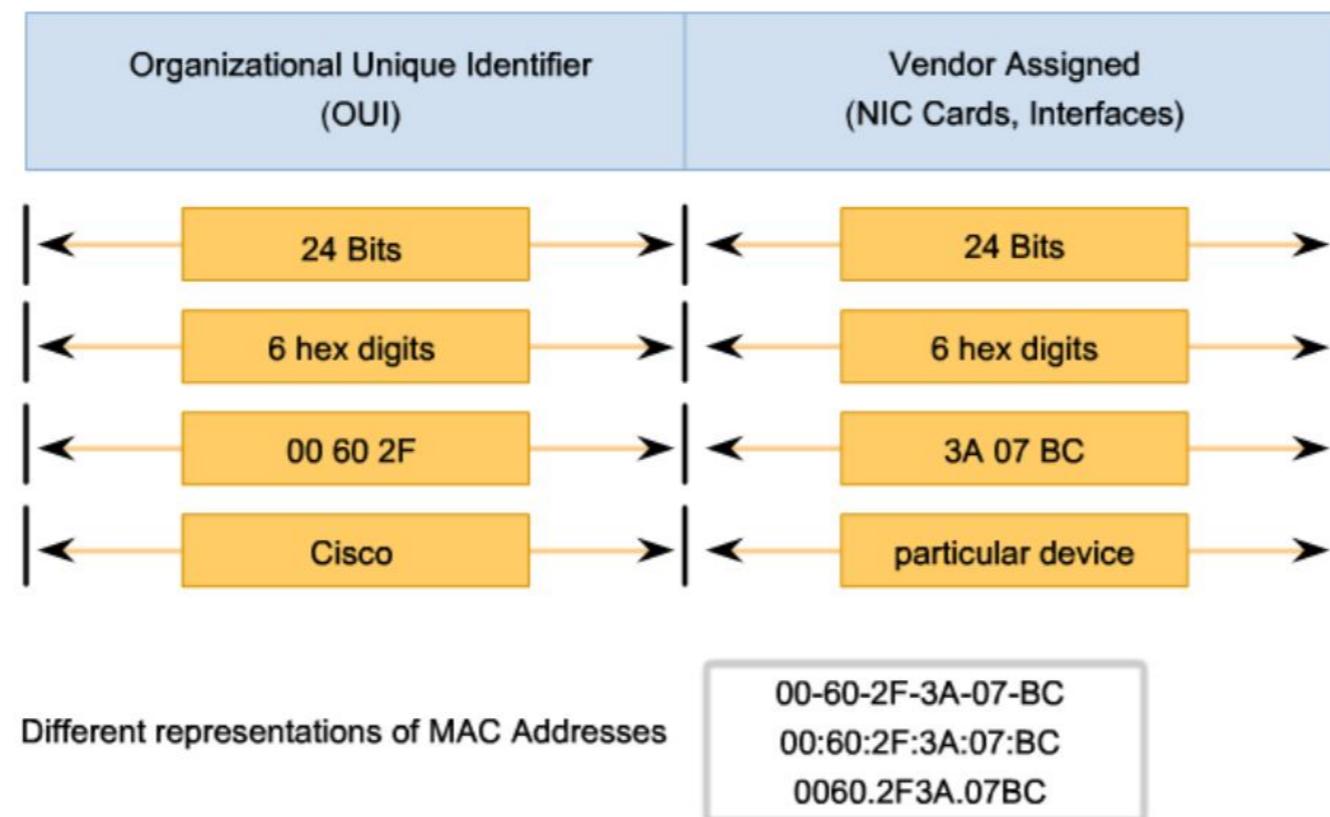
Efektivnost



Adresování

Medium Access Control adresa:

- 48-bitů, vypálena v ROM paměti síťového adaptéru
- Každý adaptér v lokální síti musí mít unikátní adresu
- Čísla MAC adres přidělovány tvůrcem standardu, tedy IEEE
- MAC adresy jsou ploché, snadné přenositelnost mezi LAN



Jaká je moje MAC adresa?

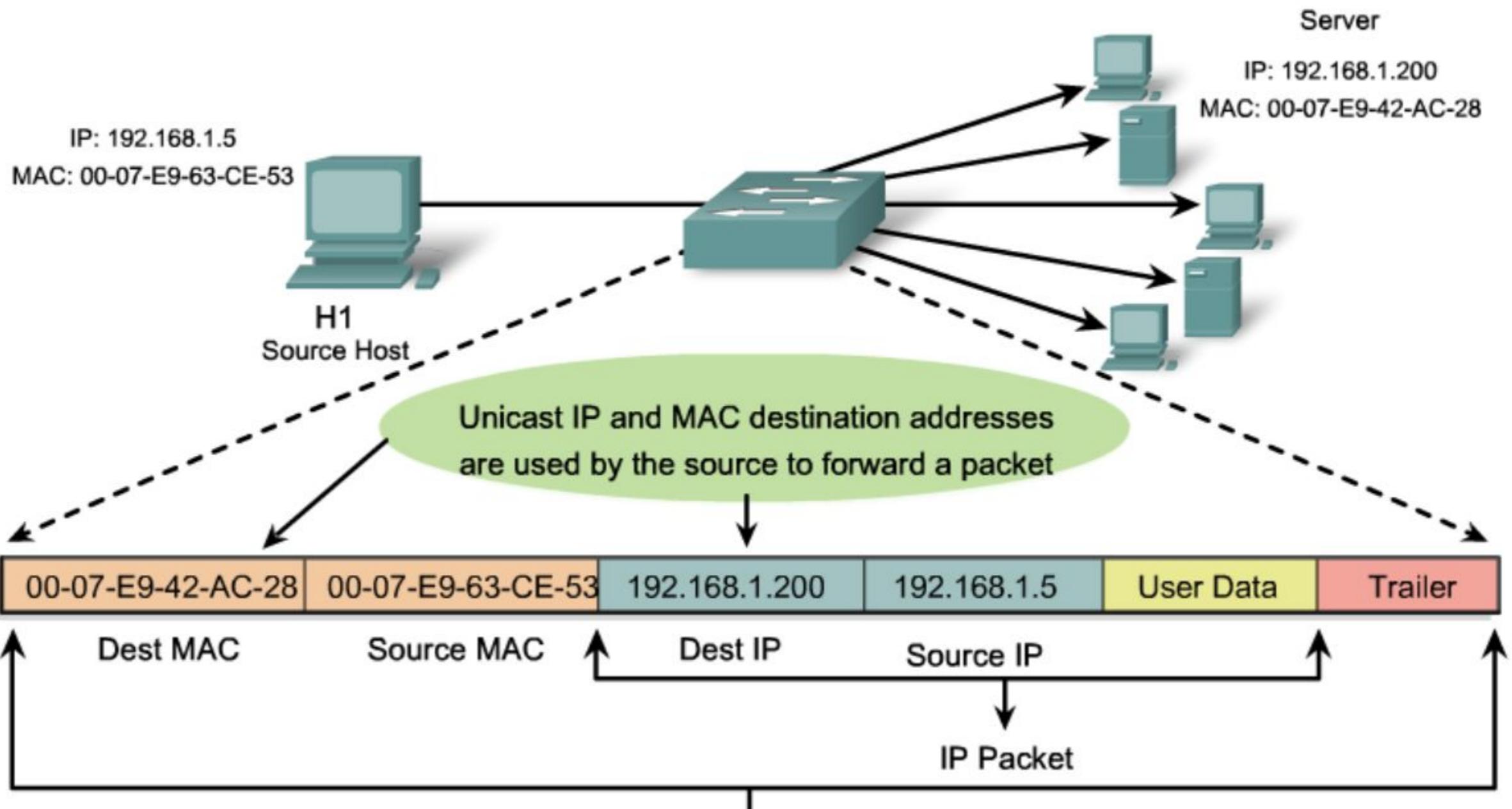
- Win: ipconfig /all
- Unix: ifconfig, ip addr



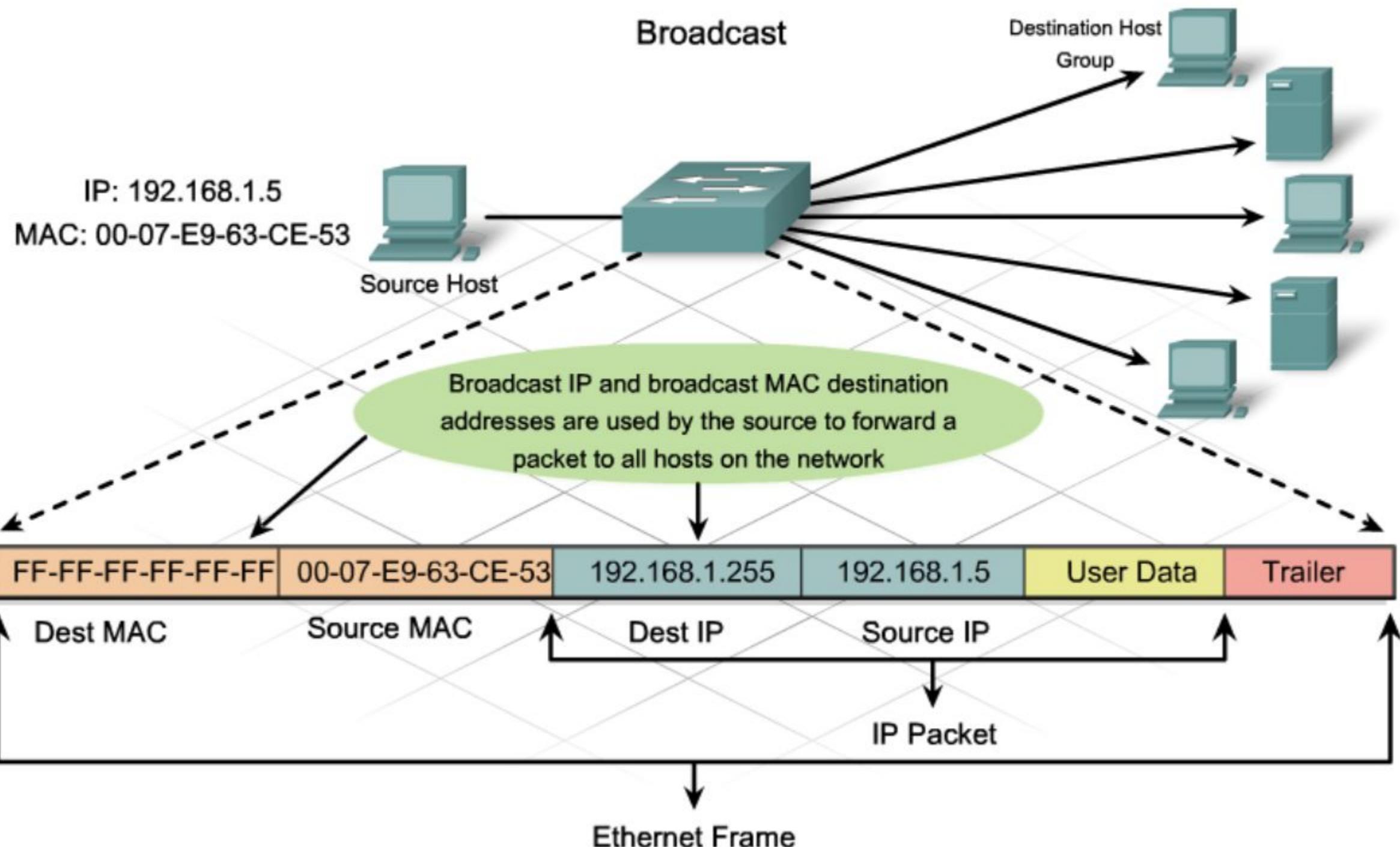
```
root@ciscoLab:~# ifconfig pnet0
pnet0      Link encap:Ethernet HWaddr 00:0c:29:c9:11:06
           inet addr:147.229.9.78 Bcast:147.229.9.255 Mask:255.255.255.0
             inet6 addr: fe80::20c:29ff:fec9:1106/64 Scope:Link
               inet6 addr: 2001:67c:1220:809::93e5:94e/64 Scope:Global
                 UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
                 RX packets:332165854 errors:0 dropped:3105 overruns:0 frame:0
                 TX packets:6598957 errors:0 dropped:0 overruns:0 carrier:0
                   collisions:0 txqueuelen:0
                     RX bytes:18092627024 (18.0 GB)  TX bytes:6992759417 (6.9 GB)

root@ciscoLab:~# ip addr show dev pnet0
4: pnet0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 00:0c:29:c9:11:06 brd ff:ff:ff:ff:ff:ff
      inet 147.229.9.78/24 brd 147.229.9.255 scope global pnet0
        valid_lft forever preferred_lft forever
      inet6 2001:67c:1220:809::93e5:94e/64 scope global
        valid_lft forever preferred_lft forever
      inet6 fe80::20c:29ff:fec9:1106/64 scope link
        valid_lft forever preferred_lft forever
root@ciscoLab:~#
```

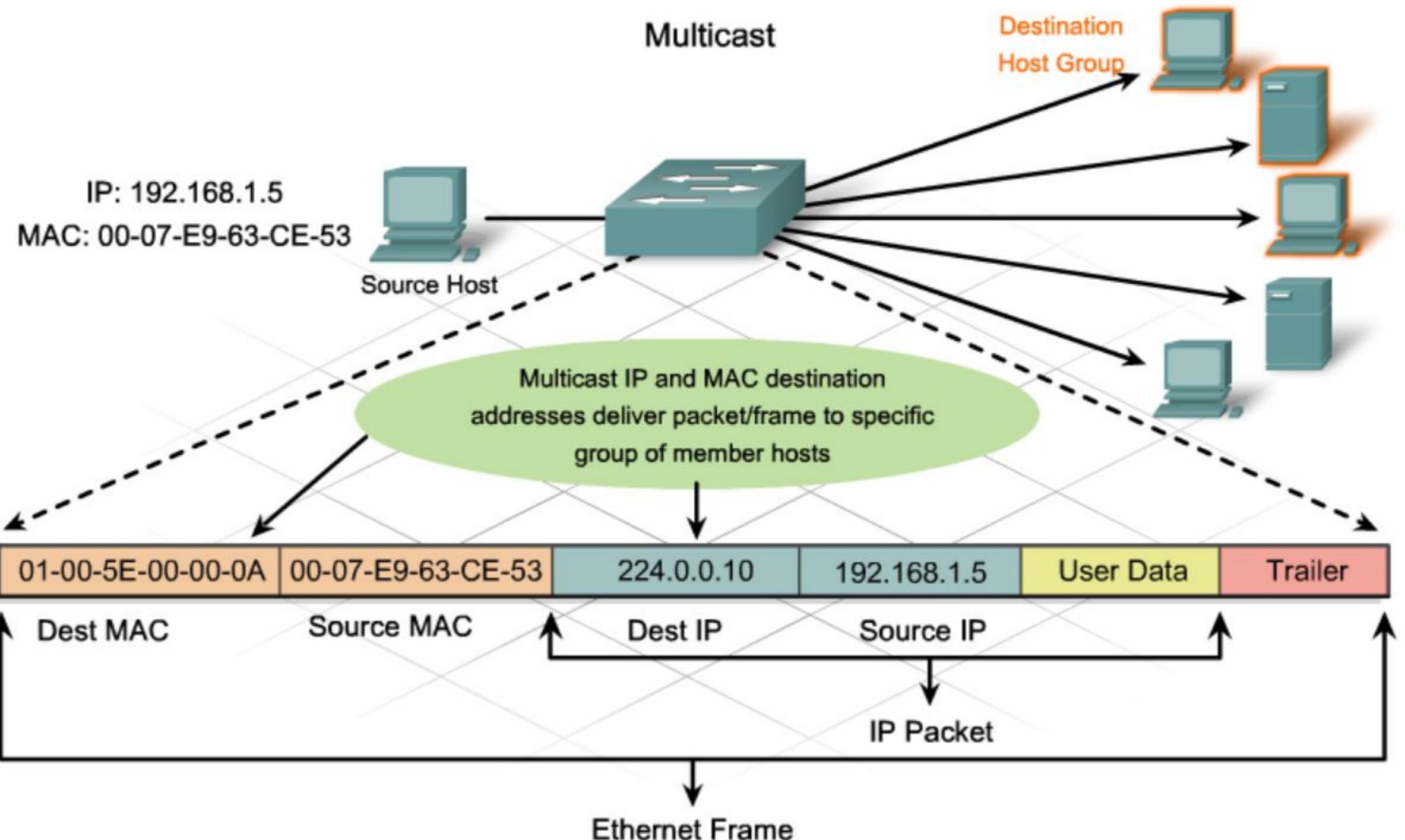
Ethernet Unicast



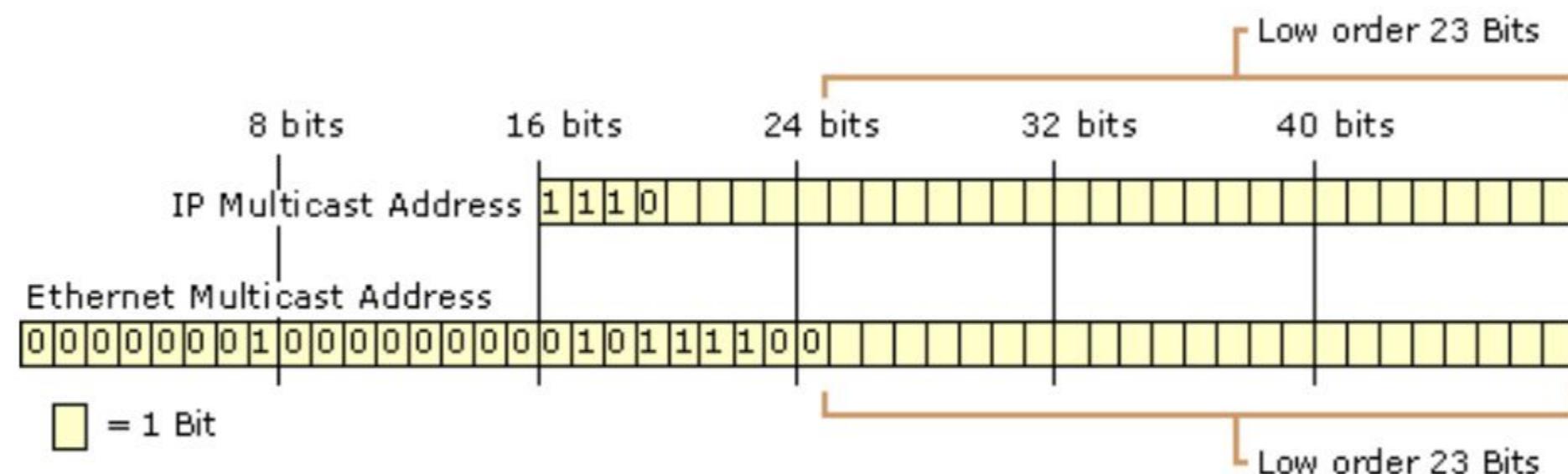
Ethernet Broadcast



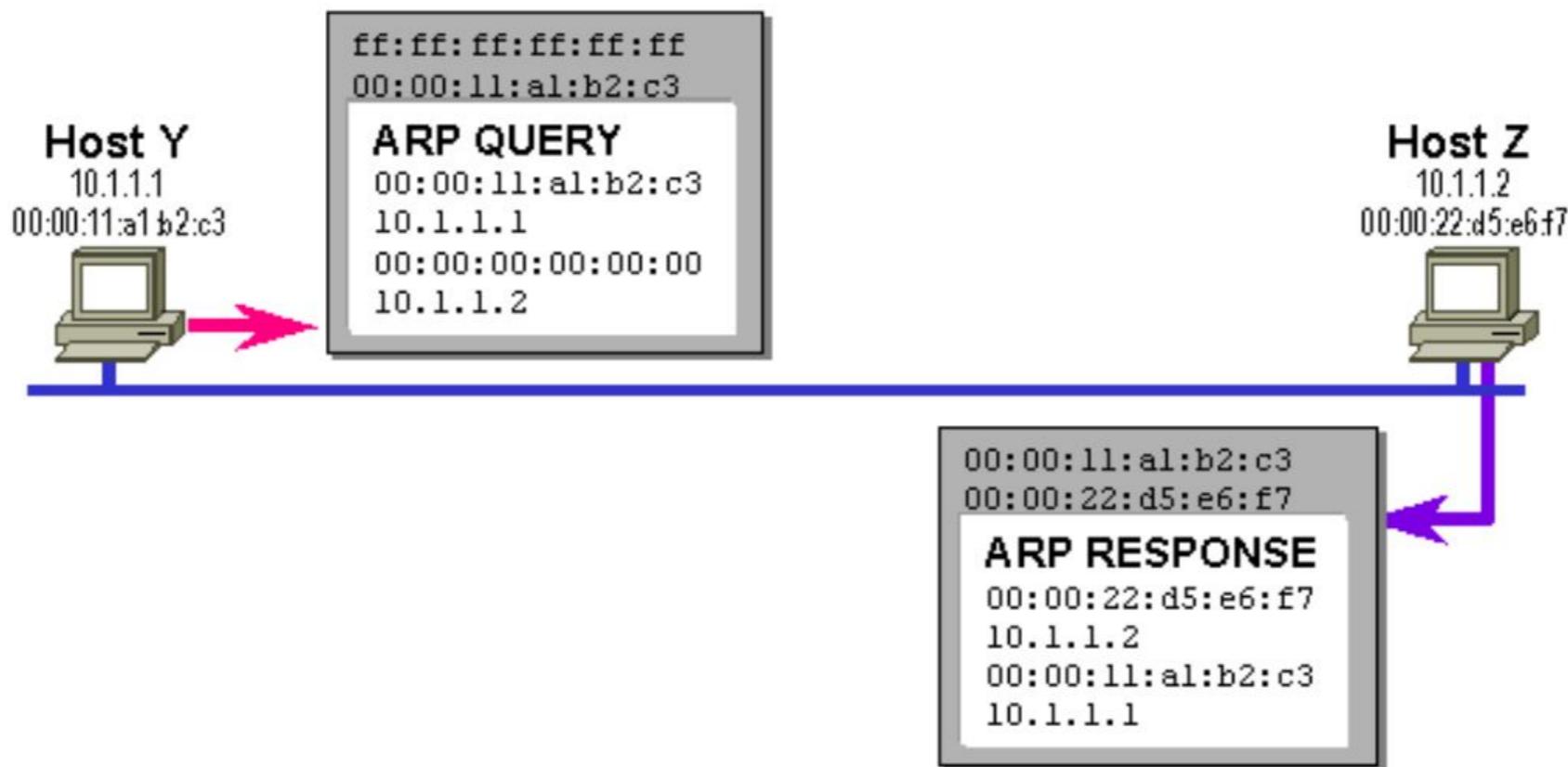
Ethernet Multicast



Mapování multicastu



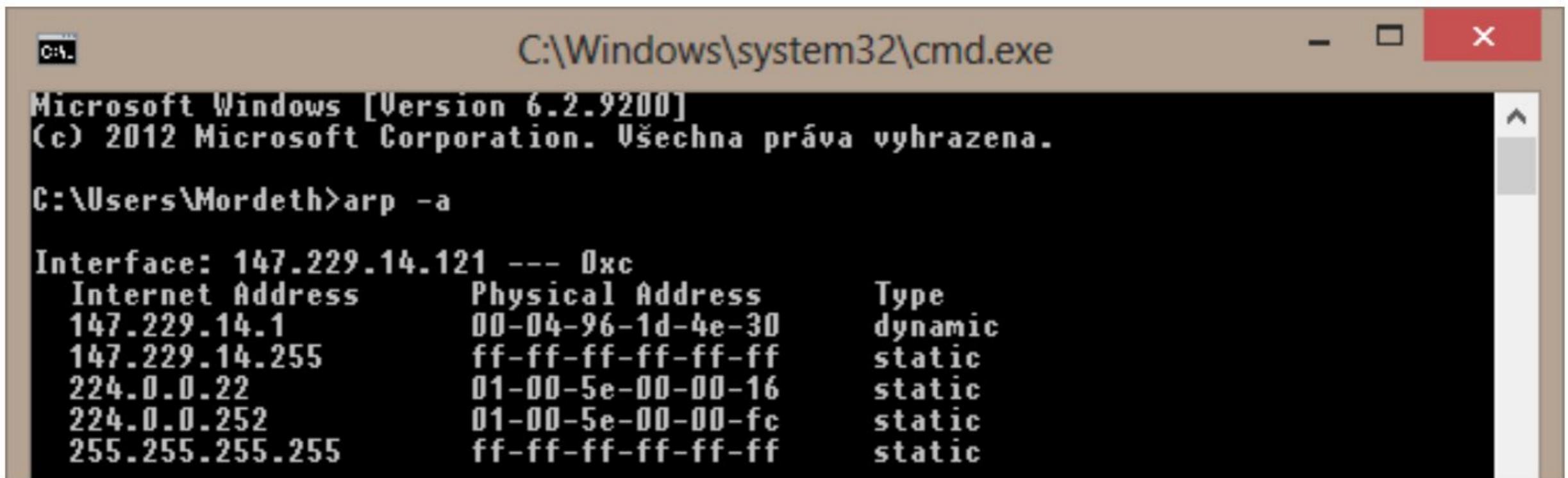
Address Resolution Protocol



8 bits	8 bits	8 bits	8 bits
Hardware Type (2bytes)		Protocol Type (2bytes)	
Hardware Add Length (1byte)	Protocol Add Length (1byte)	Operation (2bytes)	
Sender Hardware Address (6bytes)		Sender IP Address (4bytes)	
		Target Hardware Address (6bytes)	
Target IP Address (4bytes)			

ARP Cache

- Windows/Linux: arp -a
- Linux: ip neighbor



A screenshot of a Windows Command Prompt window titled "C:\Windows\system32\cmd.exe". The window shows the output of the "arp -a" command. The output is as follows:

```
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. Všechna práva vyhrazena.

C:\Users\Mordeth>arp -a

Interface: 147.229.14.121 --- 0xc
 Internet Address      Physical Address          Type
 147.229.14.1           00-04-96-1d-4e-30        dynamic
 147.229.14.255         ff-ff-ff-ff-ff-ff        static
 224.0.0.22              01-00-5e-00-00-16        static
 224.0.0.252             01-00-5e-00-00-fc        static
 255.255.255.255        ff-ff-ff-ff-ff-ff        static
```

ARP Paket

*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

arp Expression... +

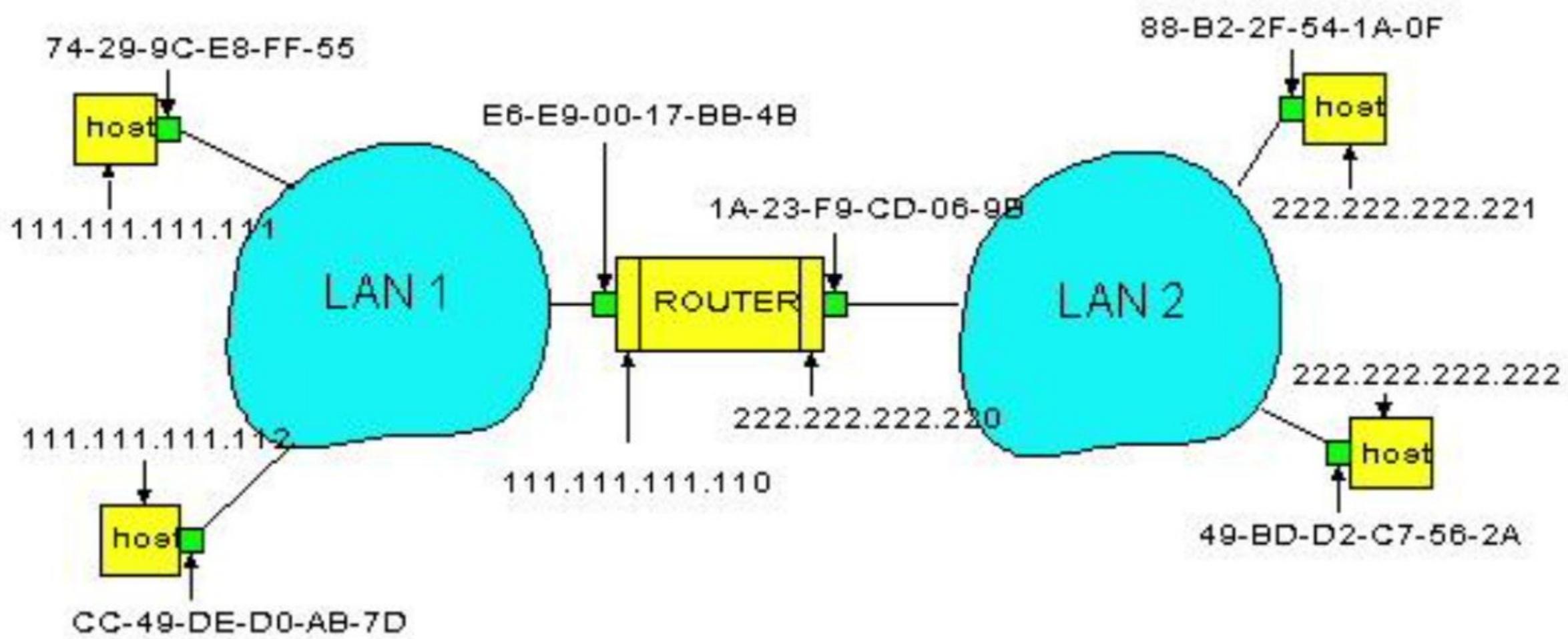
No.	Time	Source	Destination	Protocol	Length	Info
376	2017-03-16 09:36:42.244520	AsustekC_8a:95:6e	Broadcast	ARP	42	Who has 10.20.40.1? Tell 10.20.40.10
377	2017-03-16 09:36:42.244648	SuperMic_0e:a4:0d	AsustekC_8a:95:6e	ARP	60	10.20.40.1 is at 00:25:90:0e:a4:0d

> Frame 376: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
> Ethernet II, Src: AsustekC_8a:95:6e (78:24:af:8a:95:6e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▼ Address Resolution Protocol (request)
 Hardware type: Ethernet (1)
 Protocol type: IPv4 (0x0800)
 Hardware size: 6
 Protocol size: 4
 Opcode: request (1)
 Sender MAC address: AsustekC_8a:95:6e (78:24:af:8a:95:6e)
 Sender IP address: 10.20.40.10
 Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
 Target IP address: 10.20.40.1

0000	ff ff ff ff ff ff 78 24 af 8a 95 6e 08 06 00 01x\$...n....
0010	08 00 06 04 00 01 78 24 af 8a 95 6e 0a 14 28 0ax\$...n...(.
0020	00 00 00 00 00 00 0a 14 28 01 (.

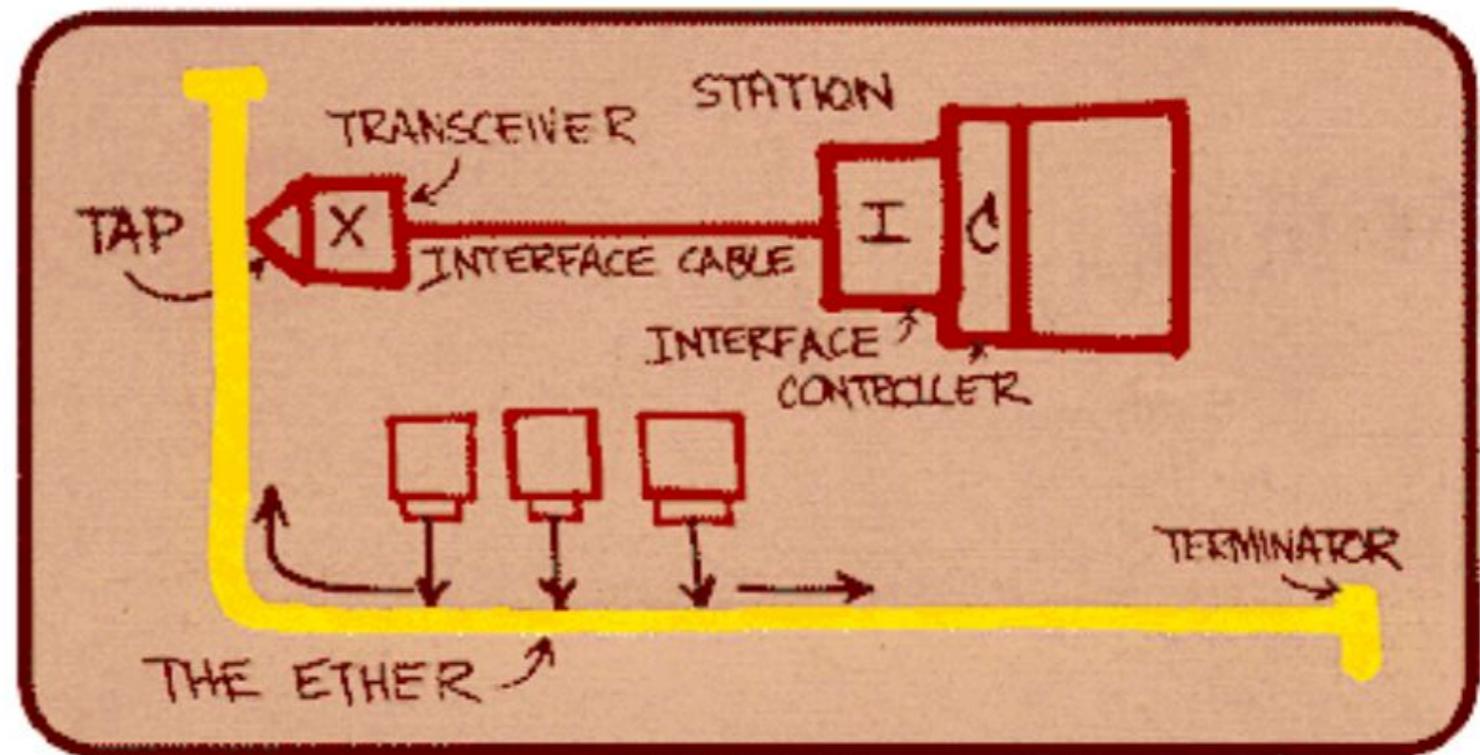
Address Resolution Protocol (arp), 28 bytes || Packets: 674 · Displayed: 2 (0.3%) || Profile: Default

LAN/WAN komunikace



10Base2 a 10Base5

- 10Base2
 - Maximální vzdálenost 200m
 - Tenký koaxiální kabel
- 10Base5
 - Maximální vzdálenost 500m
 - Tlustý koaxiální kabel

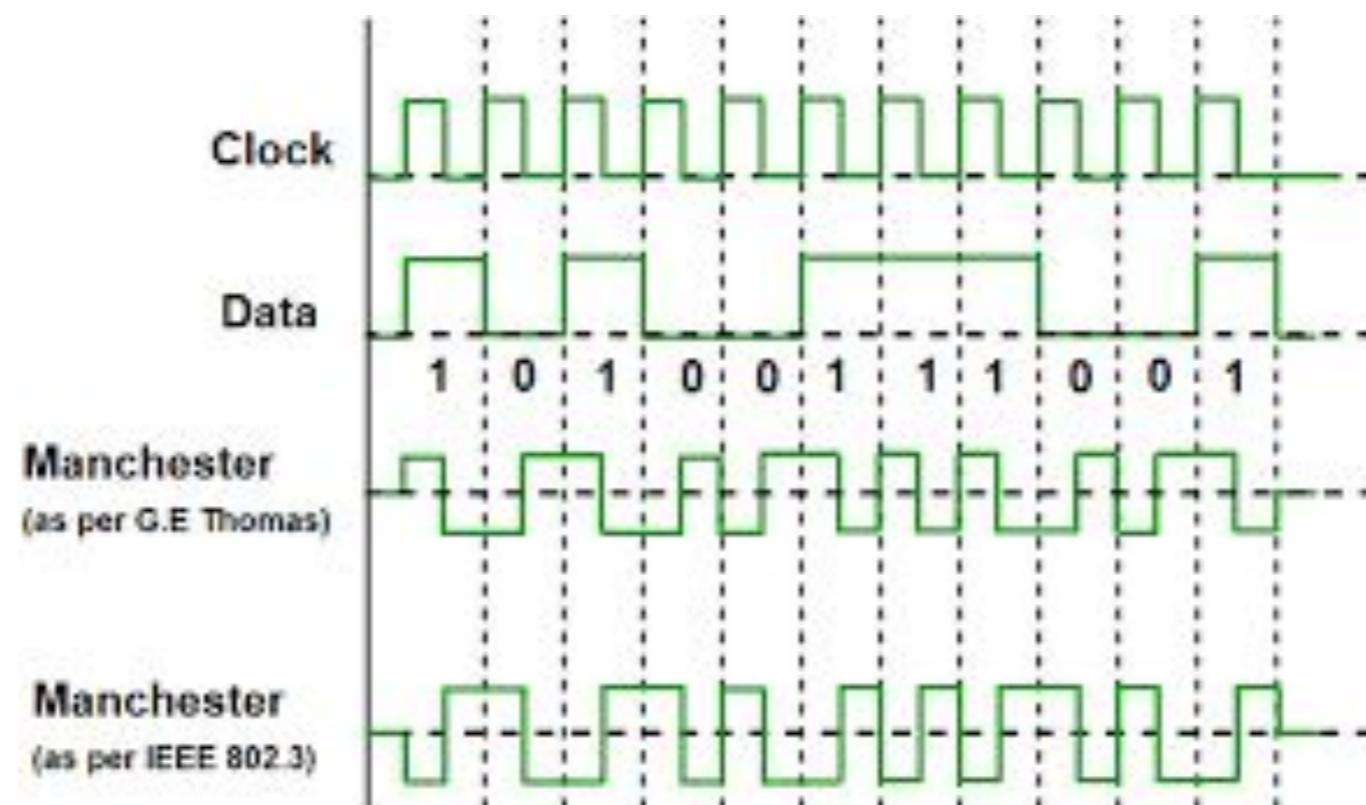


- Rychlosť 10Mbit/s
- Half-duplex
- Baseband



10Base kódování a signalizace

Kódování a signalizace: Manchester a 0/+5V



100BaseT (Fast Ethernet)

Twisted Pair

Lepší odolnost vůči stínění a přeslechům

Star topologie

Maximální vzdálenost 100m mezi uzly

RJ45 konektory

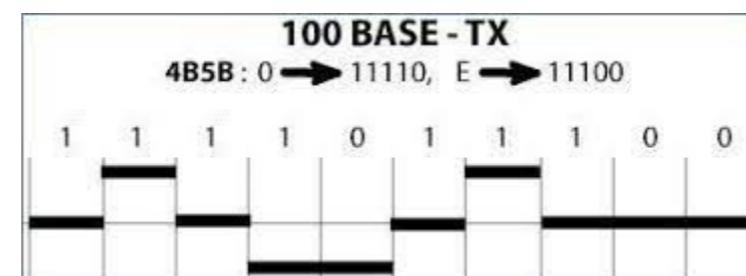
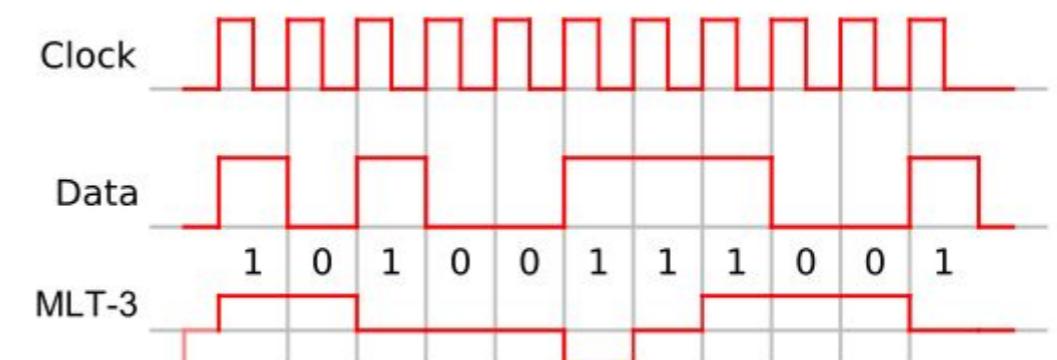


100BaseT kódování a signalizace

Kódování: 4B/5B

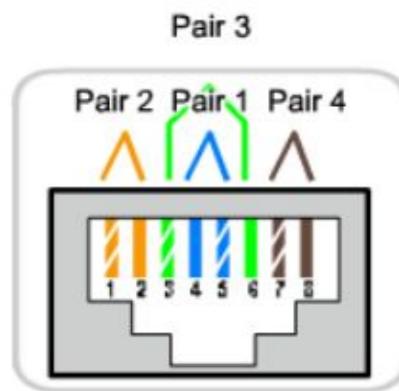
Signalizace: MLT-3

4 bit value nibble	5 bit value symbol	4 bit value nibble	5 bit value symbol
0000	11110	1000	10010
0001	01001	1001	10011
0010	10100	1010	10110
0011	10101	1011	10111
0100	01010	1100	11010
0101	01011	1101	11011
0110	01110	1110	11100
0111	01111	1111	11101



UTP a RJ45

10Base-T Ethernet RJ-45 Pinouts



RJ-45 Connectors



Pin Number	Signal
1	TD+ (Transmit Data, positive-going differential signal)
2	TD- (Transmit Data, negative-going differential signal)
3	RD+ (Receive Data, positive-going differential signal)
4	Unused
5	Unused
6	RD- (Receive Data, negative-going differential signal)
7	Unused
8	Unused

TIA/EIA 568A Wiring

1	White and Green
2	Green
3	White and Orange
4	Blue
5	White and Blue
6	Orange
7	White and Brown
8	Brown

TIA/EIA 568B Wiring

1	White and Orange
2	Orange
3	White and Green
4	Blue
5	White and Blue
6	Green
7	White and Brown
8	Brown

Figure A

Shows the Pin Out of Straight through Cables

TIA/EIA 568A Crossed Wiring

1	White and Green	1
2	Green	2
3	White and Orange	3
4	Blue	4
5	White and Blue	5
6	Orange	6
7	White and Brown	7
8	Brown	8

Figure B

Shows the Pin Out of Crossover Cables

Ethernet Standards

The Evolution of Ethernet Standards to Meet Higher Speeds				
Date	IEEE Std.	Name	Data Rate	Type of Cabling
1990	802.3i	10BASE-T	10 Mb/s	Category 3 cabling
1995	802.3u	100BASE-TX	100 Mb/s*	Category 5 cabling
1998	802.3z	1000BASE-SX	1 Gb/s	Multimode fiber
	802.3z	1000BASE-LX/EX		Single mode fiber
1999	802.3ab	1000BASE-T	1 Gb/s*	Category 5e or higher Category
2003	802.3ae	10GBASE-SR	10 Gb/s	Laser-Optimized MMF
	802.3ae	10GBASE-LR/ER		Single mode fiber
2006	802.3an	10GBASE-T	10 Gb/s*	Category 6A cabling
2015	802.3bq	40GBASE-T	40 Gb/s*	Category 8 (Class I & II) Cabling
2010	802.3ba	40GBASE-SR4/LR4	40 Gb/s	Laser-Optimized MMF or SMF
	802.3ba	100GBASE-SR10/LR4/ER4	100 Gb/s	Laser-Optimized MMF or SMF
2015	802.3bm	100GBASE-SR4	100 Gb/s	Laser-Optimized MMF
2016	SG	Under development	400 Gb/s	Laser-Optimized MMF or SMF

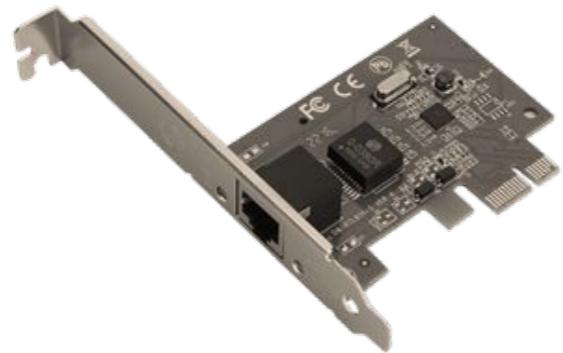
Note: *with auto negotiation

LAN Zařízení

Síťová karta
klient



Modem



NIC



Repeater



Hub



Switch



Router

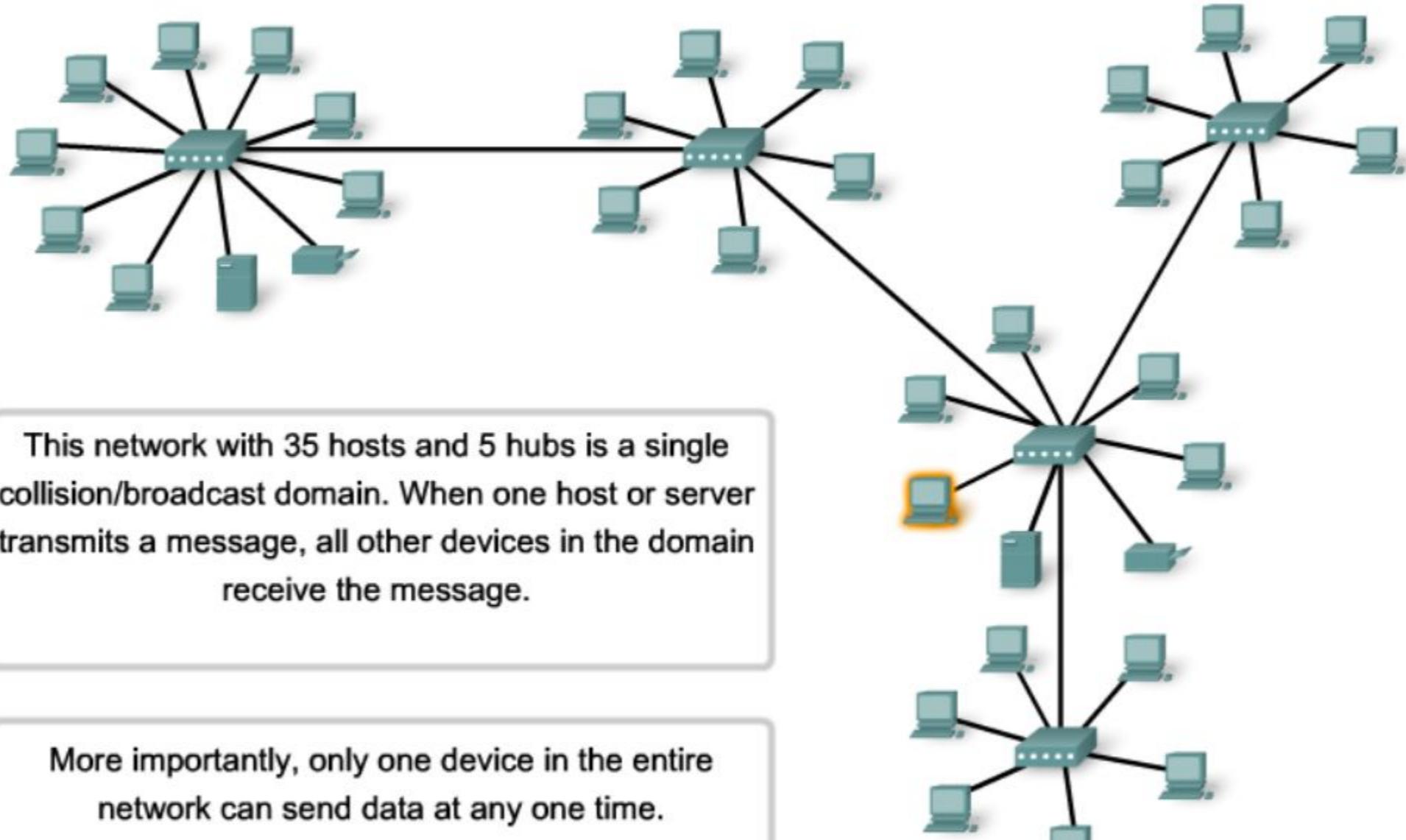


Bridge



Gateway

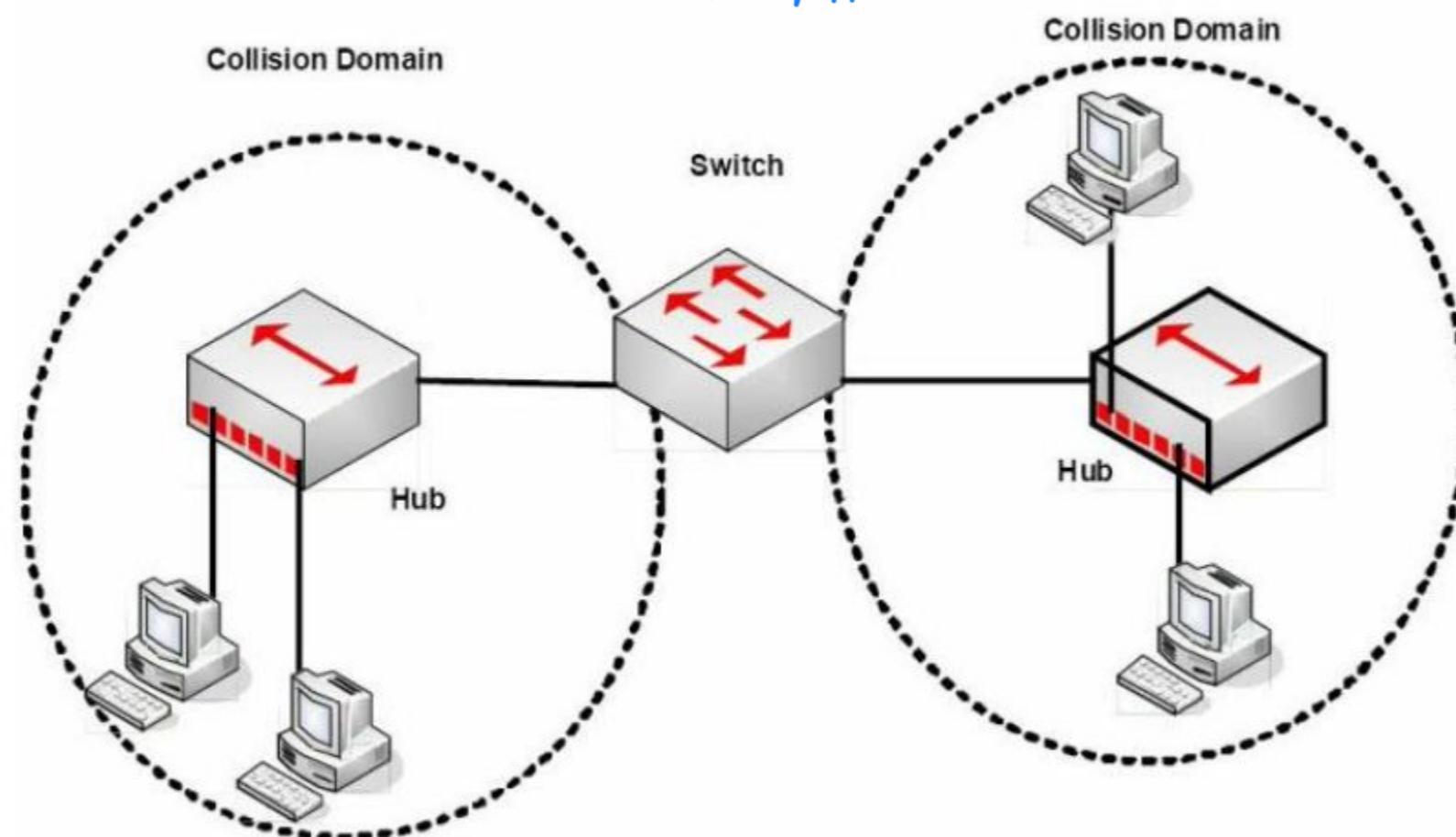
Hub/repeater (opakovač)



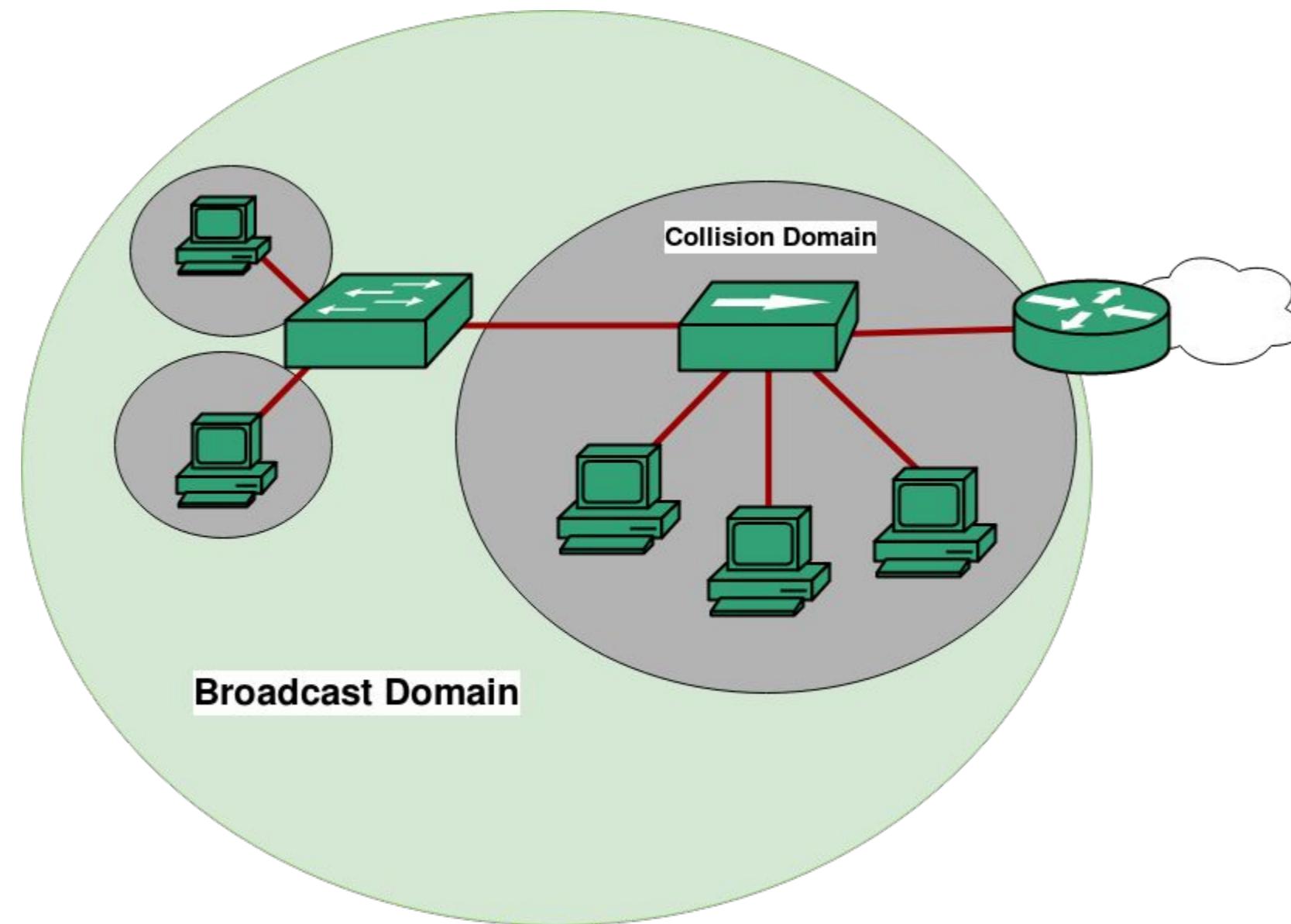
Switch (přepínač)

L2 zařízení, podporuje full-duplex komunikaci, ukládá a posílá rámce, zkoumá hlavičky rámciů a selektivně přeposíla rámce dle Content Address Memory (CAM) na základě cílové MAC, rozděluje kolizní doménu

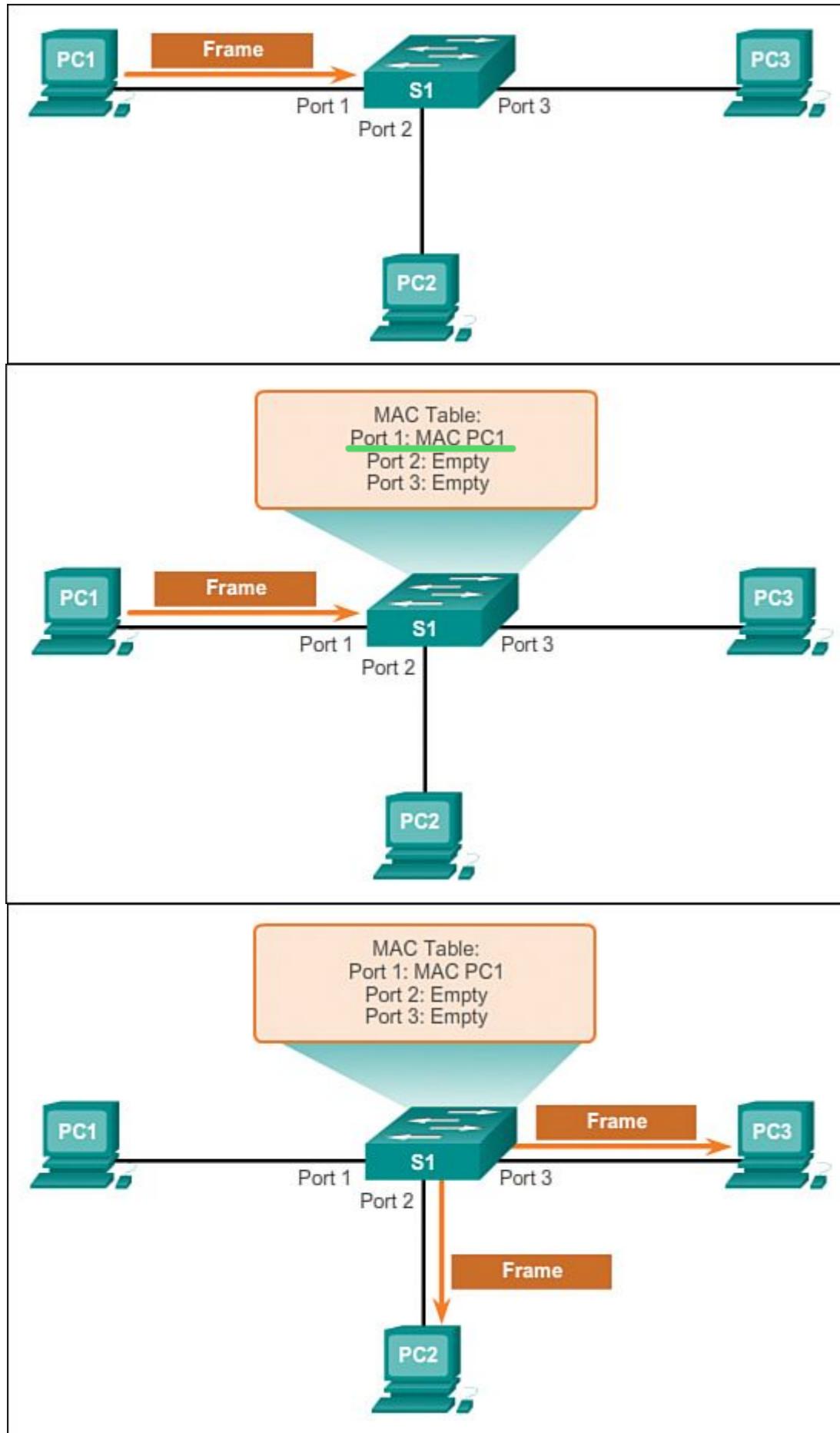
kolizní doména
v rámci portov



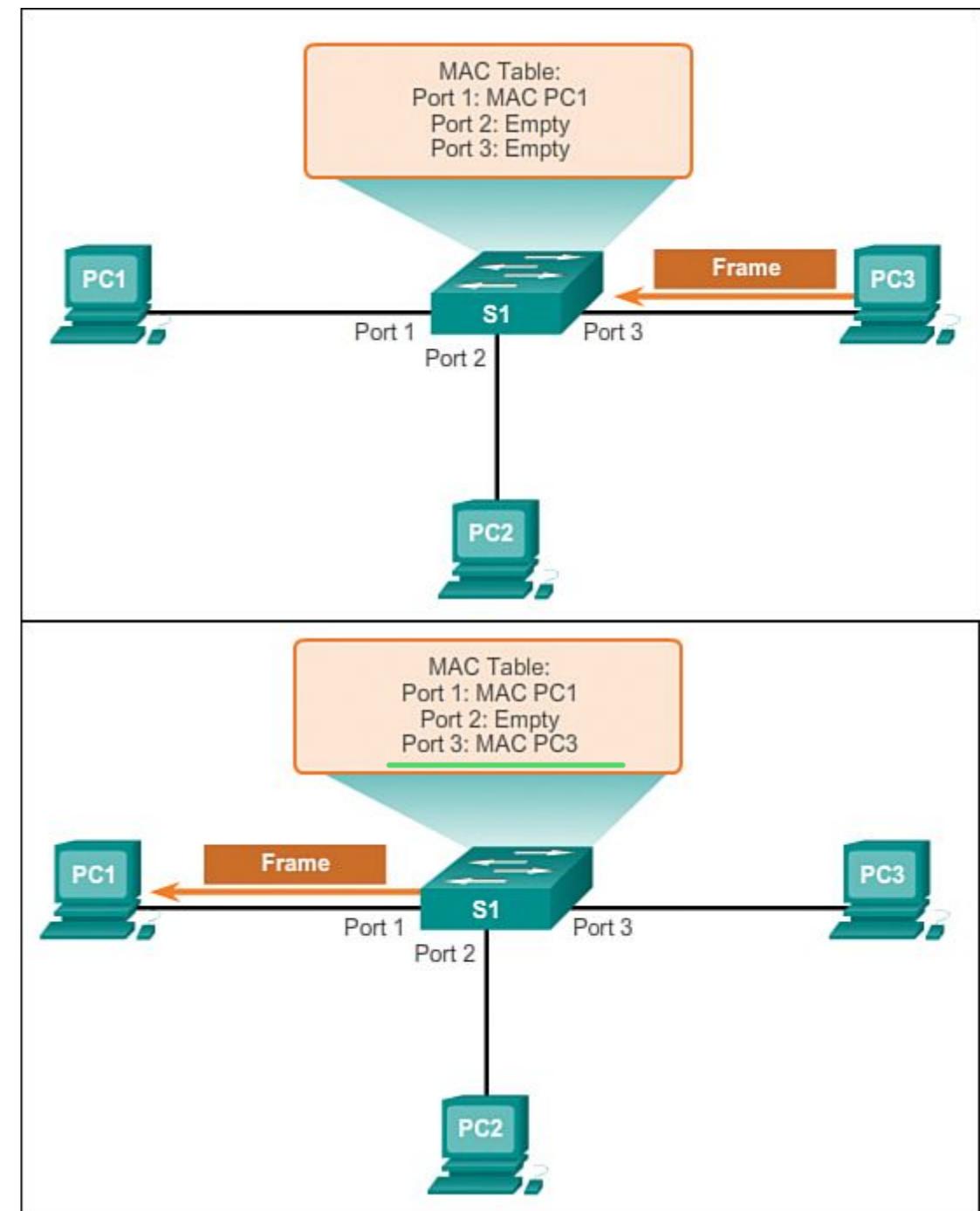
Broadcast/Collision domain



Unicast



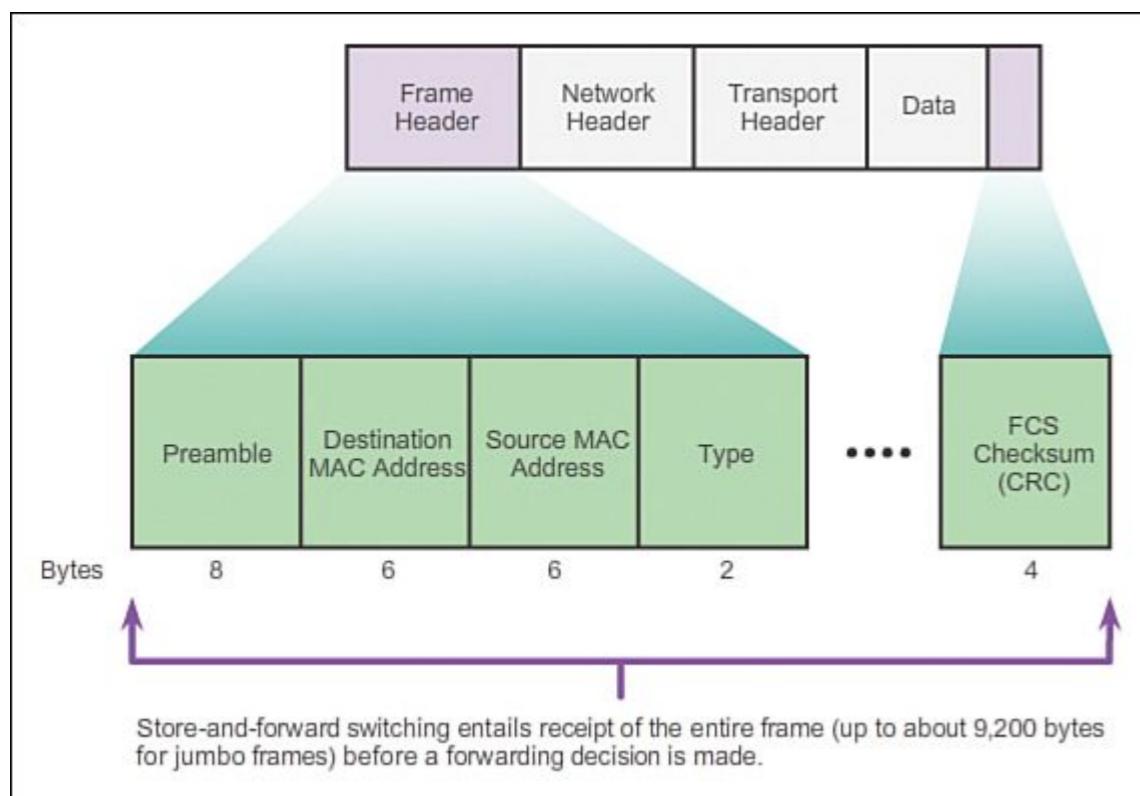
Tabulka MAC



Metody přepínání

Store-and-forward

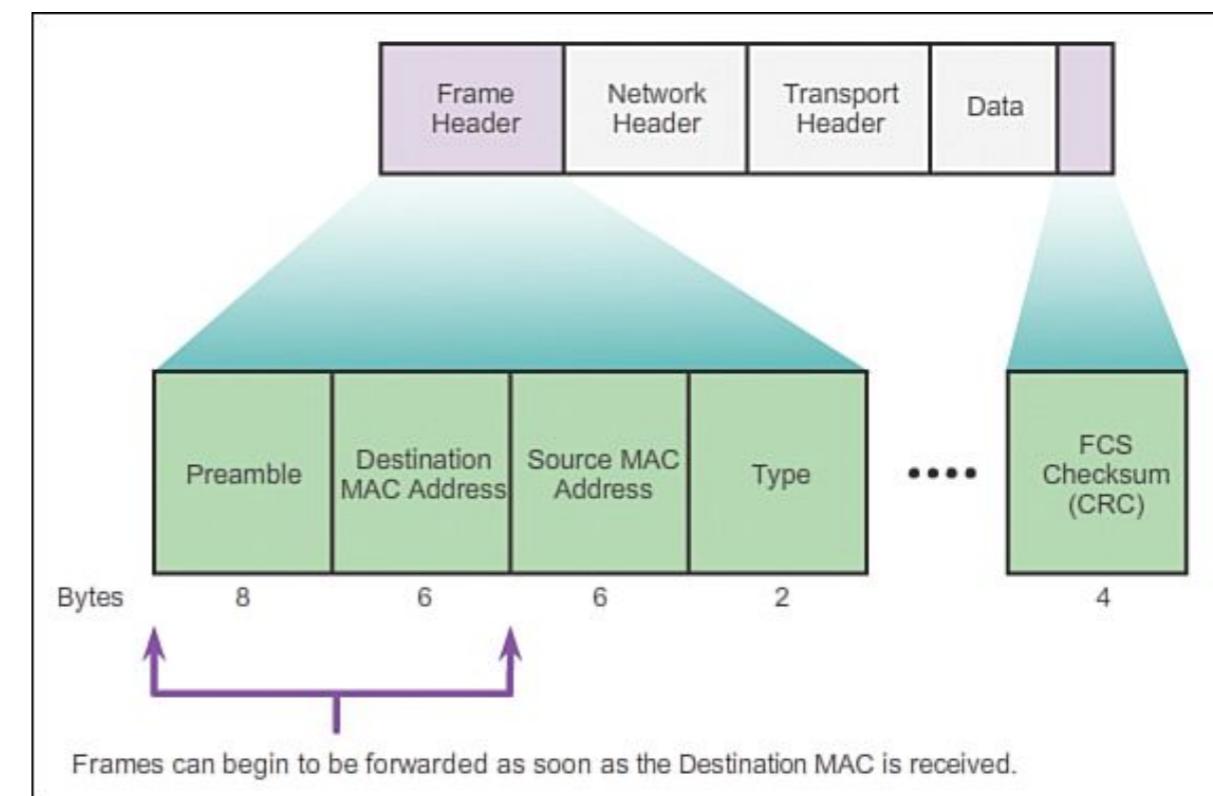
- umožňuje kontrolovat chyby
- nutné pro přepínání mezi rozhraními různých rychlostí



Cut-Through

- rychlejší přepnutí rámce
- nevhodné v případě vyšší chybovosti linek

Maci třamp na bastou (Po náhradu odosielat římkou)
a třímkou přeslať

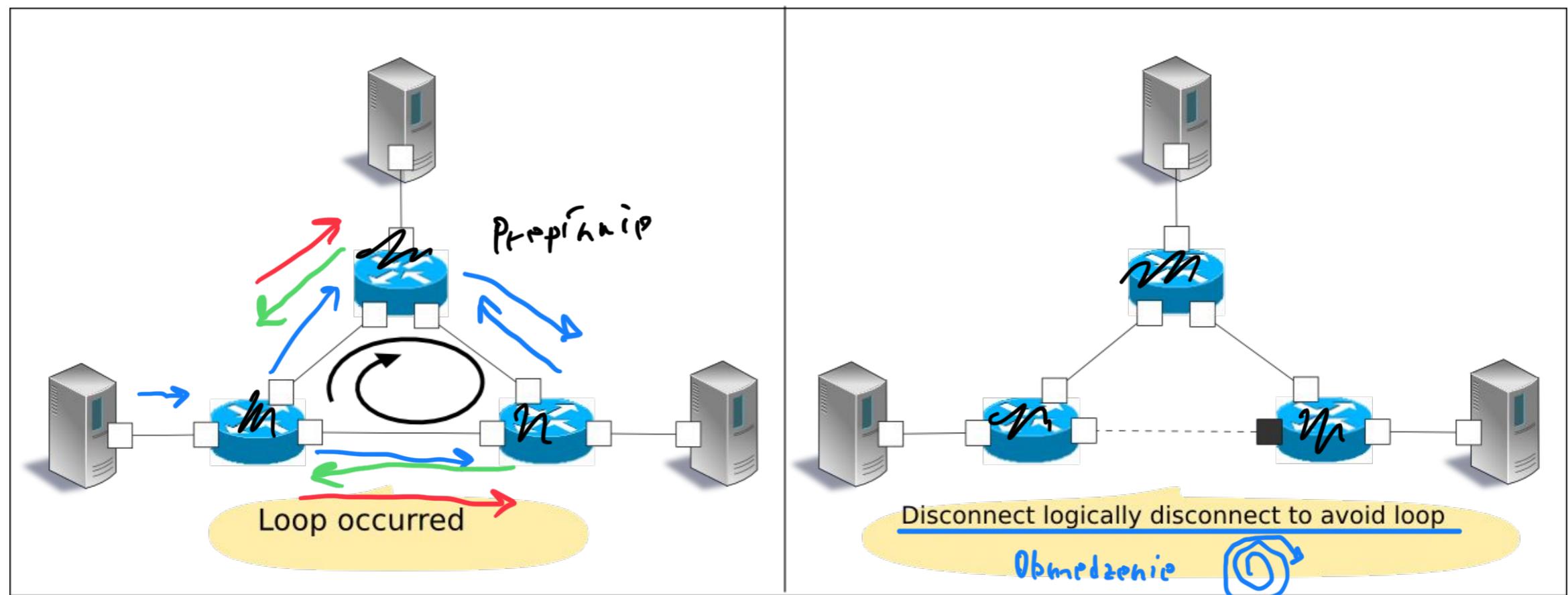


Spanning Tree

Motivace

Redundance (více možných cest) pro zajištění spolehlivosti přináší problémy na L2:

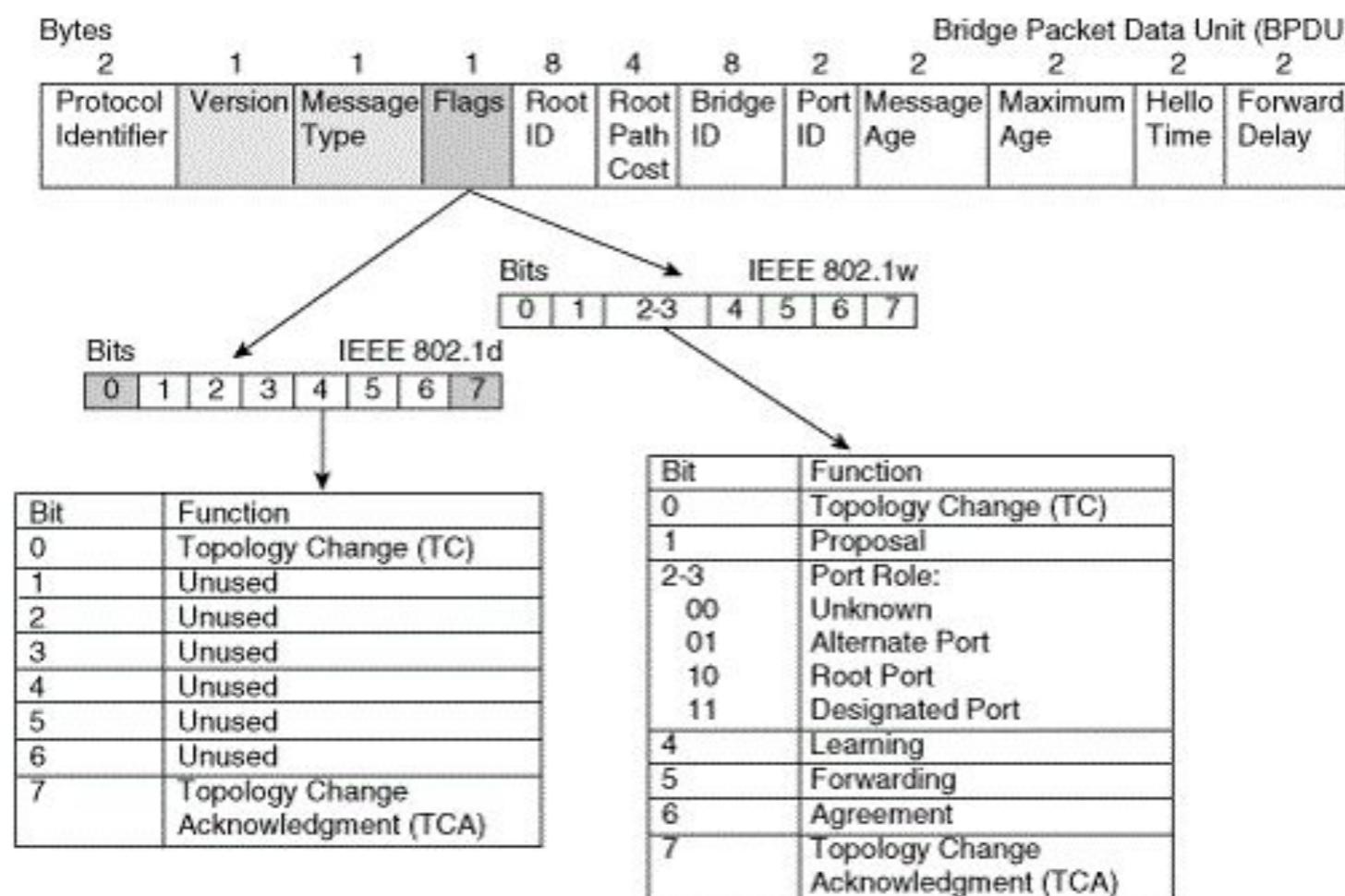
- broadcast storm
- nestabilní MAC tabulky
- duplicita rámců



Spanning Tree Protocol

Bridge Protocol Data Unit (BPDU) jsou zprávy, které přepínač odesílá na broadcastovou MAC adresu a slouží k:

- Volbě root-bridge
- Určení typu každého z portů v segmentu



STP operace

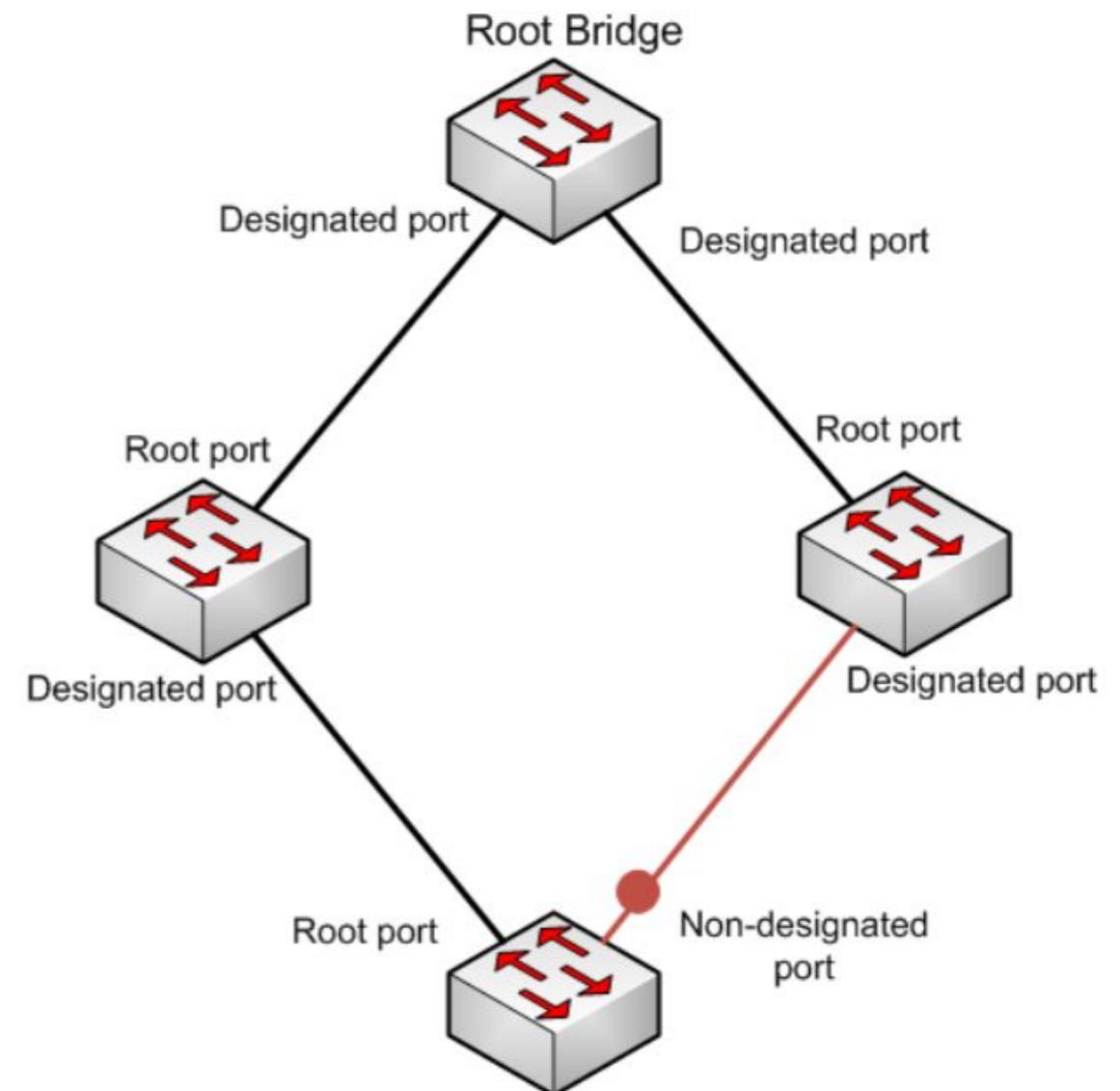
POSTUP:

1. Volba Root Bridge
2. Určení typů portů:
 - a. Root
 - b. Designated
 - c. Non-designated

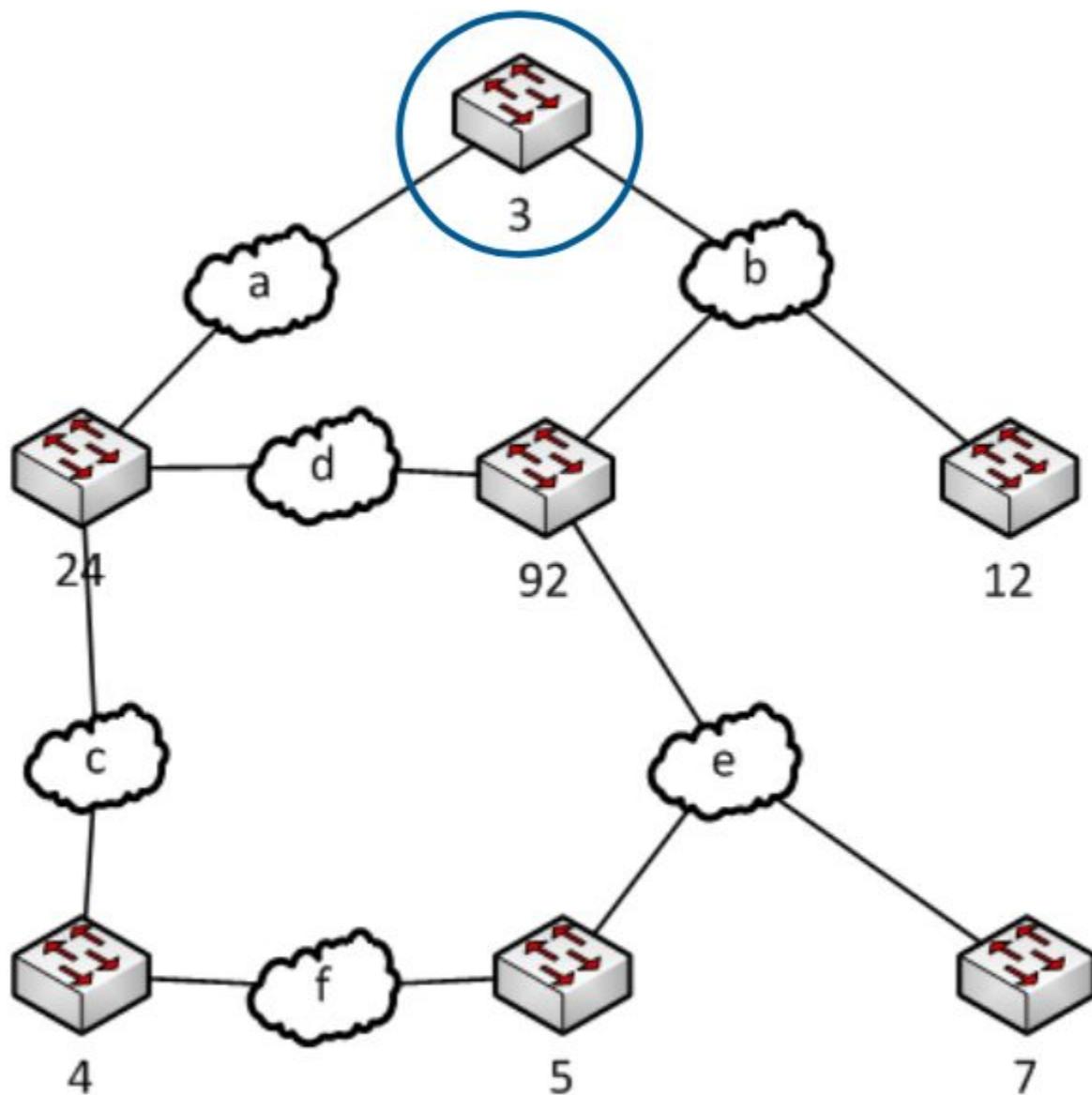
Root port - port s nejnižší cenou, bud' linka přímo spojená s Root Bridge nebo s nejkratší cestou k němu.

Designated port - port, který je členem STP topologie a připojuje segment.

Non-designated port - blokovaný port, redundantní cesta.



1. Volba Root Bridge

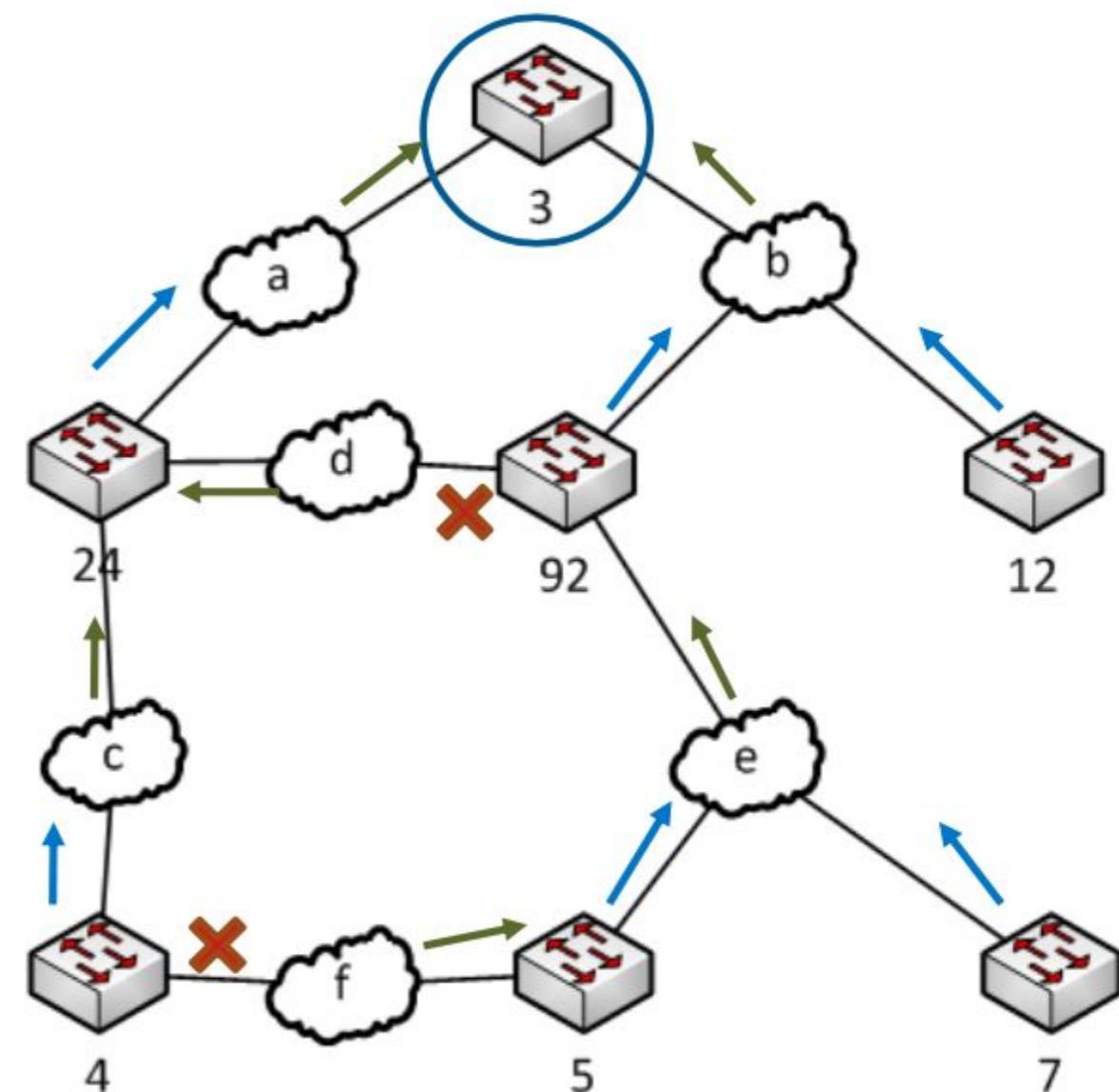


Bridge s nejmenším Bridge ID

- explicitně nastavena (Bridge priority)
- odvozena z nekonfigurovatelné MAC a konfigurovatelného parametru priority

2. Tyty portů

- Podle ceny linky/segmentu
- Porty vedoucí k root s nejnižší cenou jsou označeny jako **root**
- Porty které slouží segmentům jako cesta k root jsou označeny jako **designated**
- Ostatní porty jsou zakázány a označeny jako **blocked**



Stavy portů

Blocking

- Zahazuje rámce
- Přijímá BPDU
- Nezpracovává BPDU
- Neodesílá BPDU

Listening

- Zahazuje rámce
- Přijímá BPDU
- Zpracovává BPDU
- Neodesílá BPDU

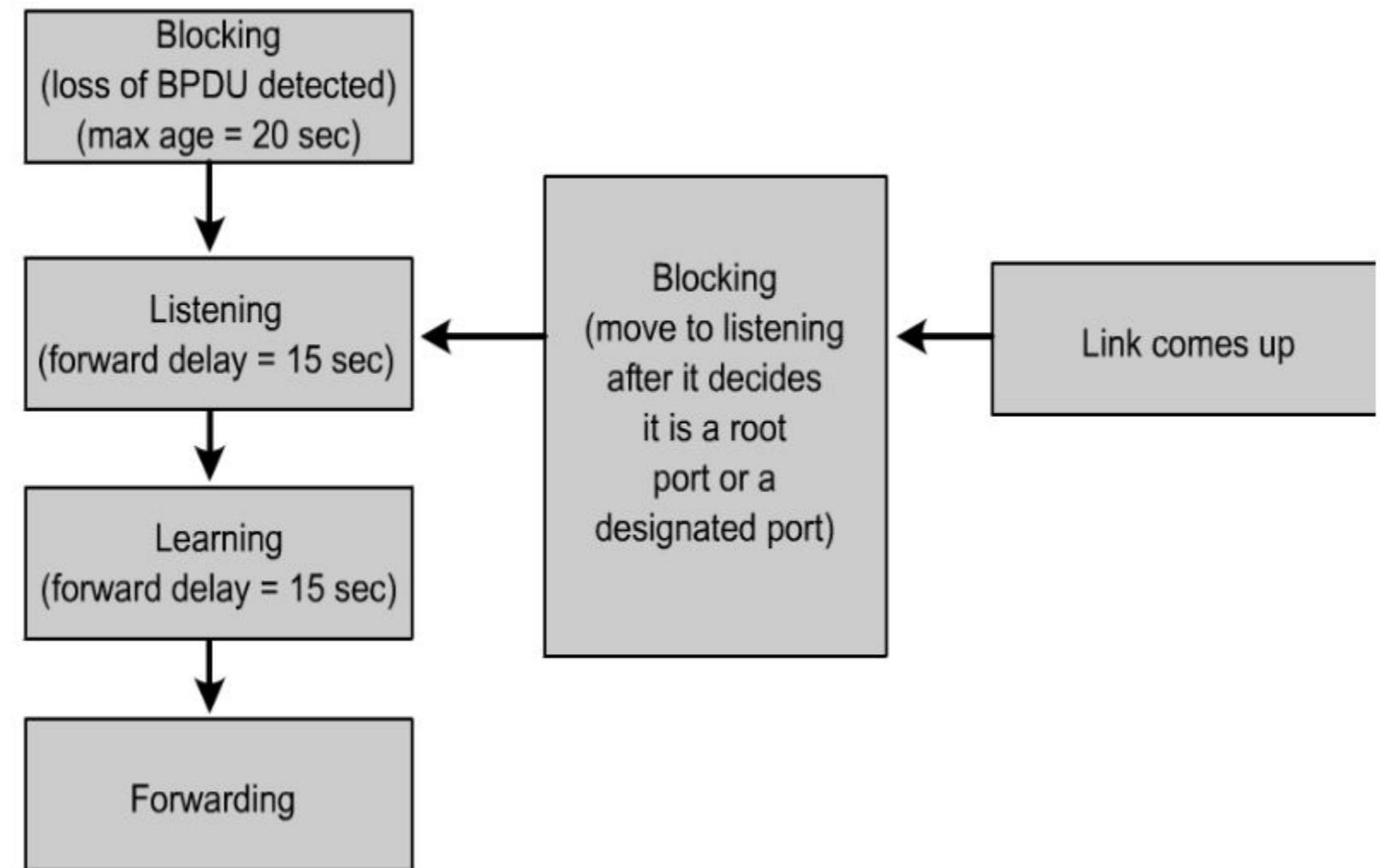
Learning

- Zahazuje rámce
- Přijímá BPDU
- Zpracovává BPDU
- Odesílá BPDU

Forwarding

- Posílá rámce
- Přijímá BPDU
- Zpracovává BPDU
- Odesílá BPDU

Bridge Protocol Data Unit



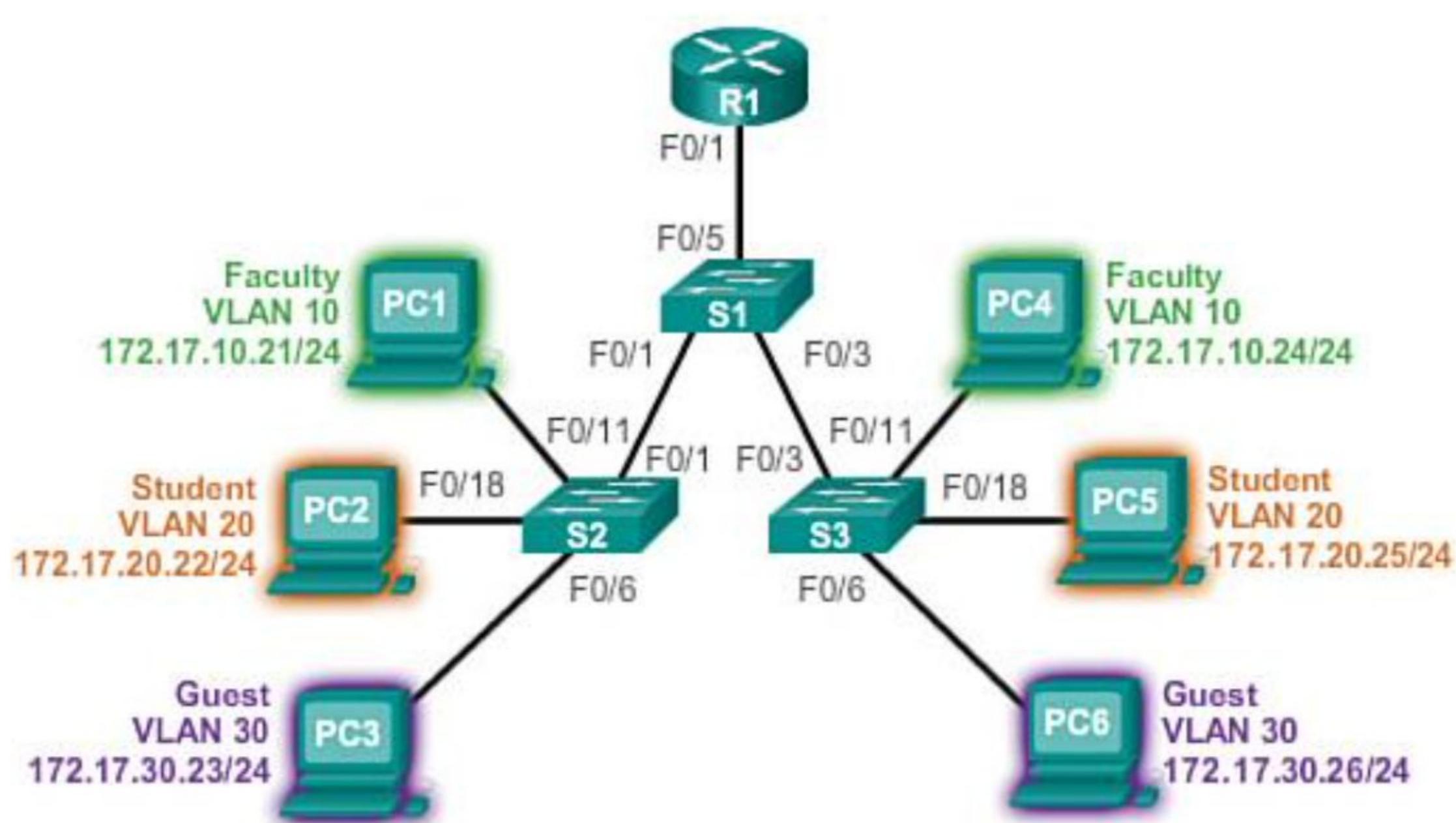
STP verze

Spanning tree protocol

Standard	Name	Features
Cisco proprietary	PVST (per-VLAN STP)	<ul style="list-style-type: none">• Uses the Cisco proprietary ISL trunking protocol• Each VLAN has an instance of spanning tree• Ability to load balance traffic at layer-2• Includes extensions BackboneFast, UplinkFast, and PortFast
	PVST+	<ul style="list-style-type: none">• Supports ISL and IEEE 802.1Q trunking• Supports Cisco proprietary STP extensions• Adds BPDU guard and Root guard enhancements
	Rapid PVST+	<ul style="list-style-type: none">• rapid-PVST+• Based on IEEE802.1w standard• Has faster convergence than 802.1D
IEEE standard	RSTP	<ul style="list-style-type: none">• Introduced in 1982 provides faster convergence than 802.1D• Implements generic versions of the Cisco proprietary STP extensions• IEEE has incorporated RSTP into 802.1D, identifying the specification as IEEE 802.1D-2004
	MSTP	<ul style="list-style-type: none">• Multiple VLANs can be mapped to the same spanning-tree instance• Inspired by the Cisco Multiple Instances Spanning Tree Protocol (MISTP)• IEEE 802.1Q-2003 now includes MSTP

Virtuální síť

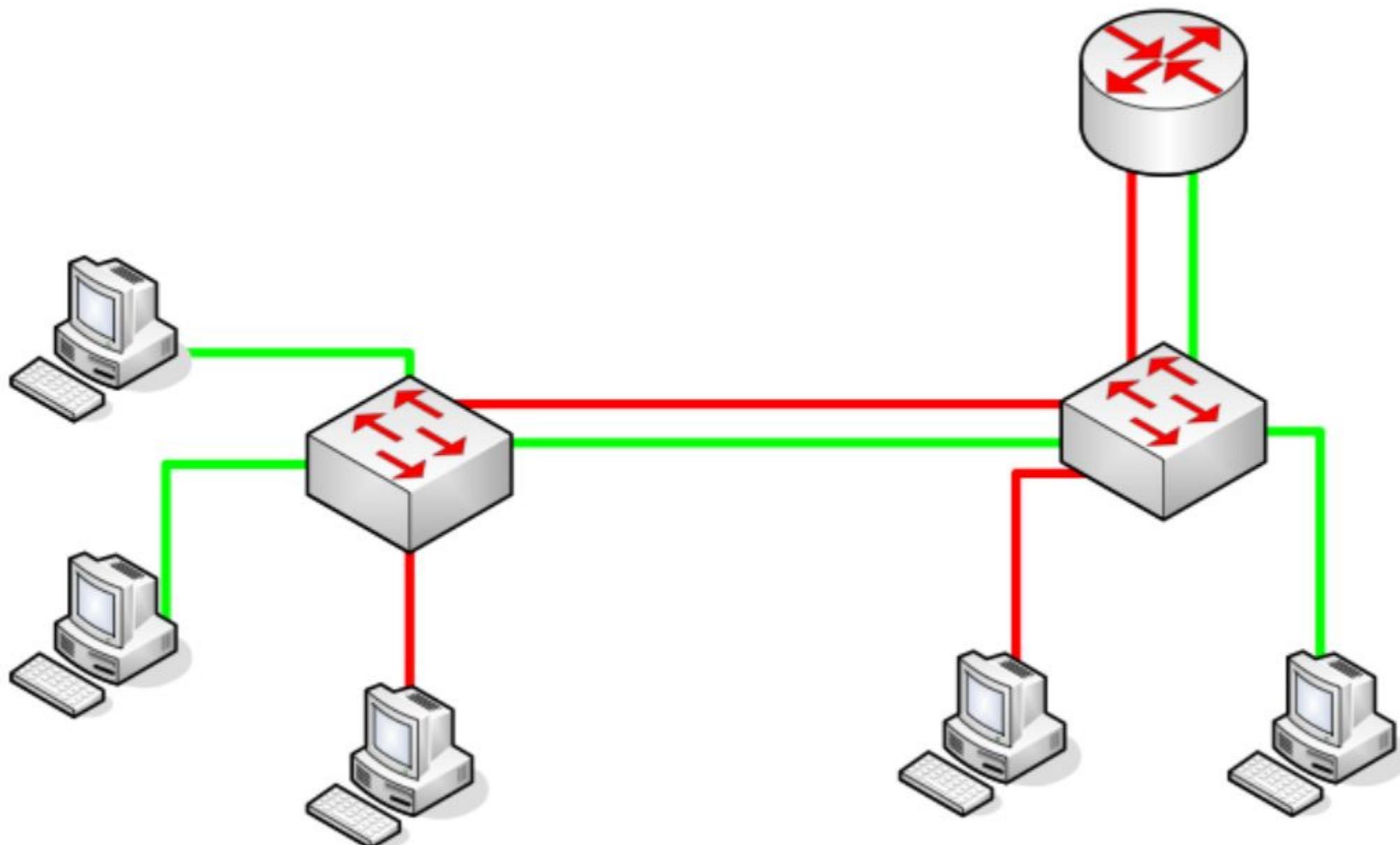
Proč VLAN?



VLAN vlastnosti

- Část síťové infrastruktury (typicky ethernetové), která se chová jako samostatná LAN.
- Softwarově konfigurovatelná, může zasahovat do několika budov.
- Počítače komunikují přímo, distribuuje se broadcast, apod.
- Propojení jednotlivých VLAN sítí pouze na směrovači.
- Není nutné pořizovat samostatný přepínač pro jednotlivé LAN sítě.
- Propojení více přepínačů bez nutnosti připojit samostatně každou VLAN (plýtvání porty) – trunking 802.1Q (Cisco proprietární ISL)

VLAN na zařízení



IEEE802.1Q

Trunking

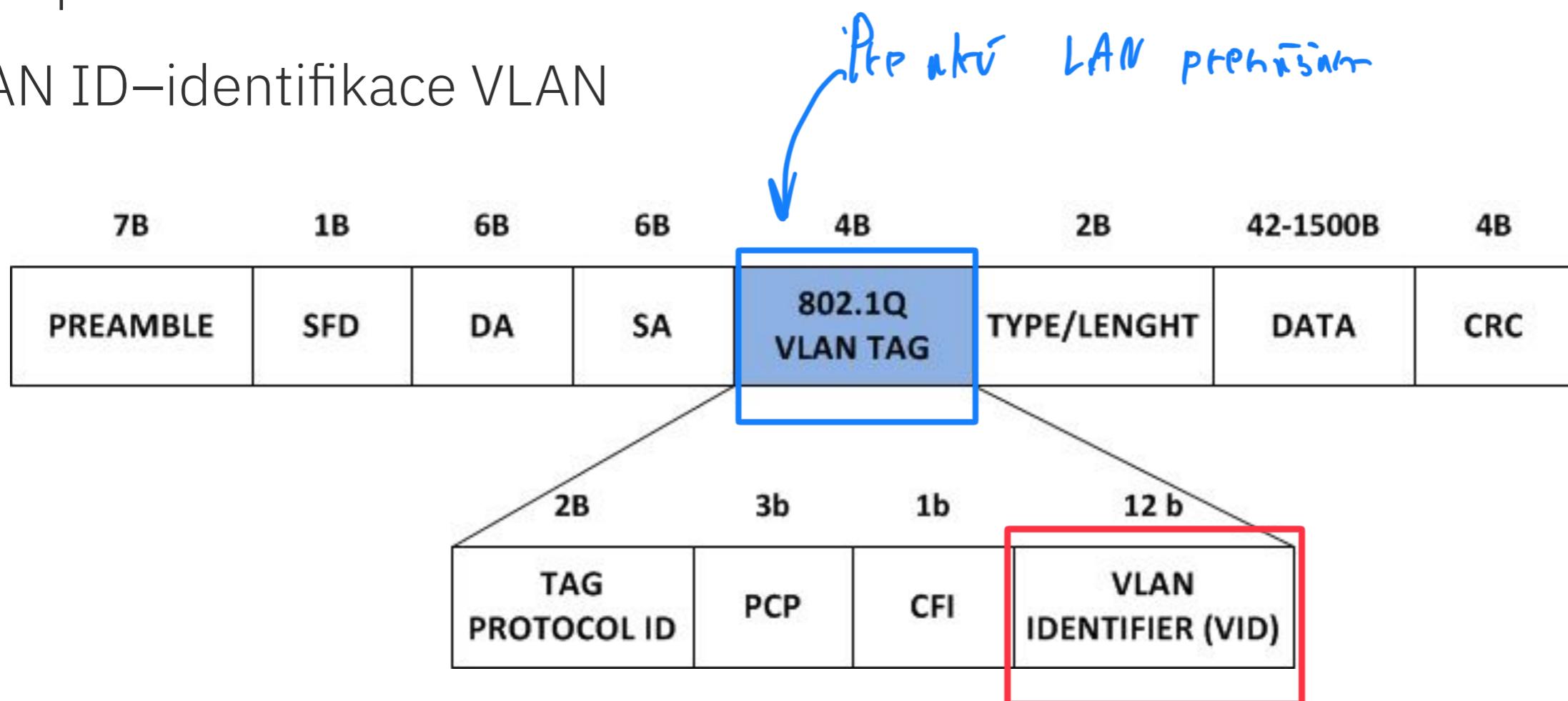
Přidány 4B pro identifikaci virtuální sítě:

TPID—Tag Protocol Identifier (16 bitů): 0x8100 pro Ethernet

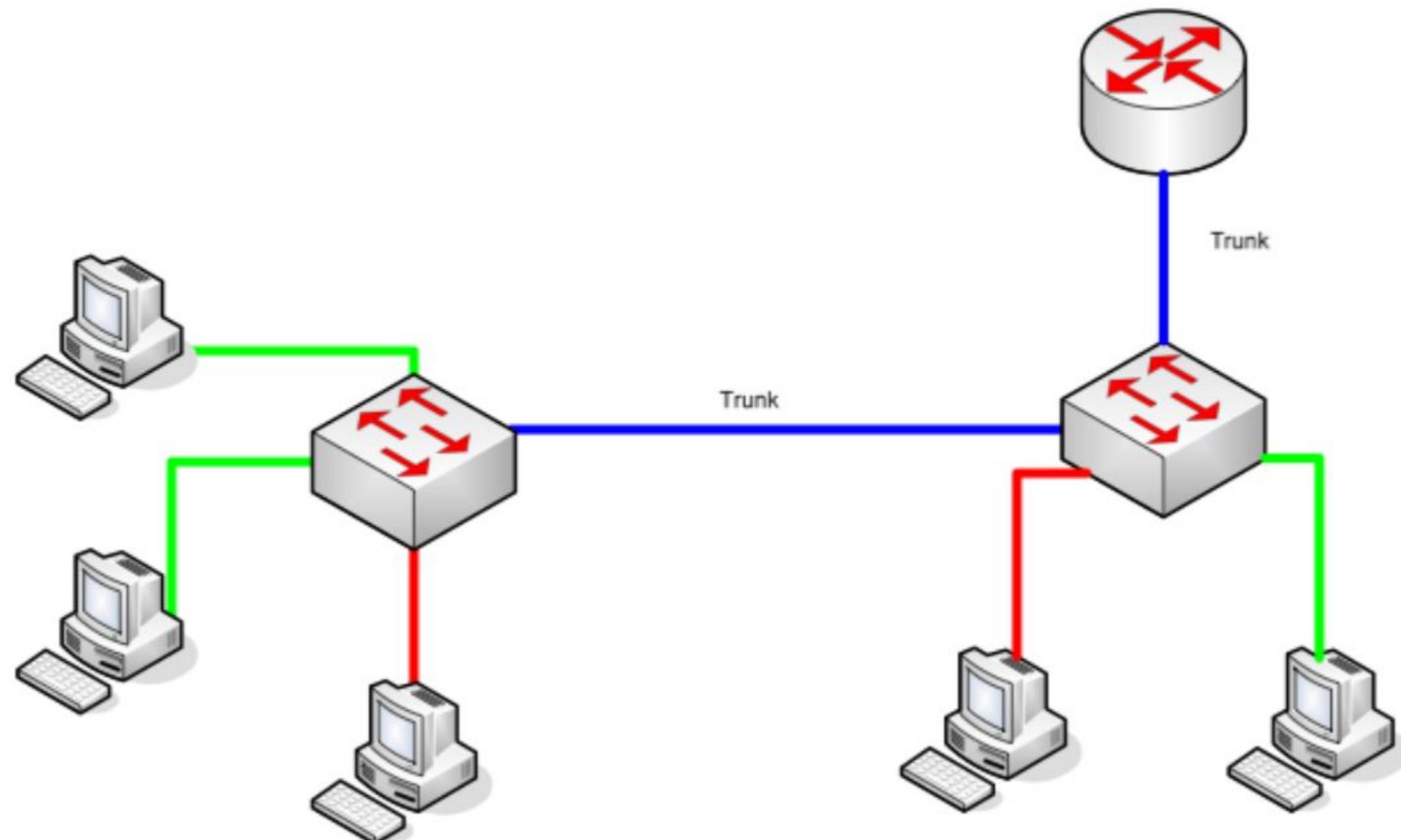
TCI—Tag Control Information (16 bitů):

PCP—priorita rámce

VLAN ID—identifikace VLAN



Použití 802.1Q



Bezdrátové sítě

Bezdrátová komunikace

Využití elektromagnetického vlnění pro vysokorychlostní přenos dat:

- Rádiové vlny
- Světlo

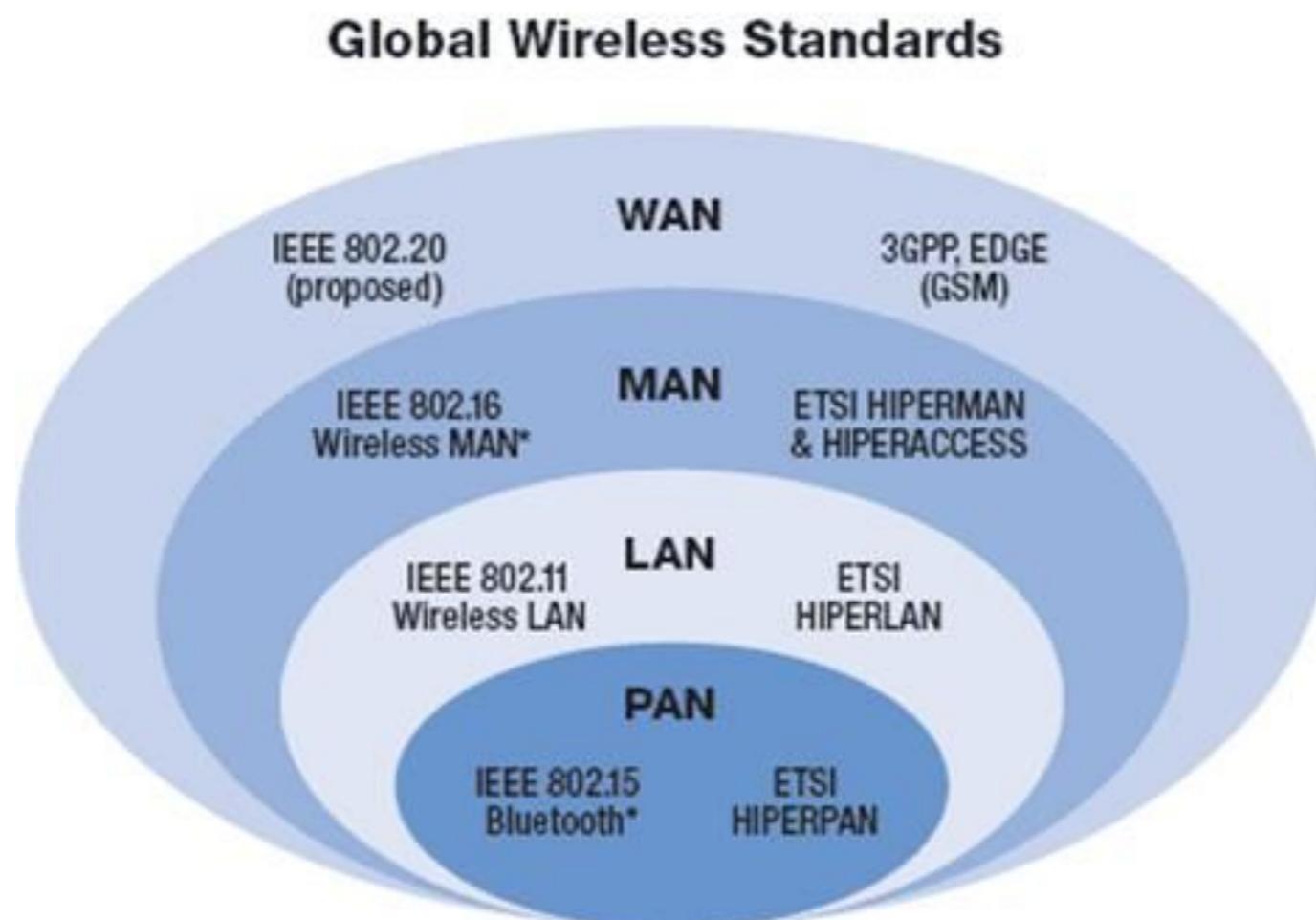
Výhody:

- Plošné pokrytí
- Mobilita
- Operativnost
- Možnost překonat poměrně velké vzdálenosti a relativně náročný terén

Wireless LAN

Wireless LAN (WLAN) technologie je ta část bezdrátových technologií, která poskytuje službu jako tradiční LAN sítě

V současnosti jsou v oblasti WLAN nejpoužívanější standardy IEEE 802.11



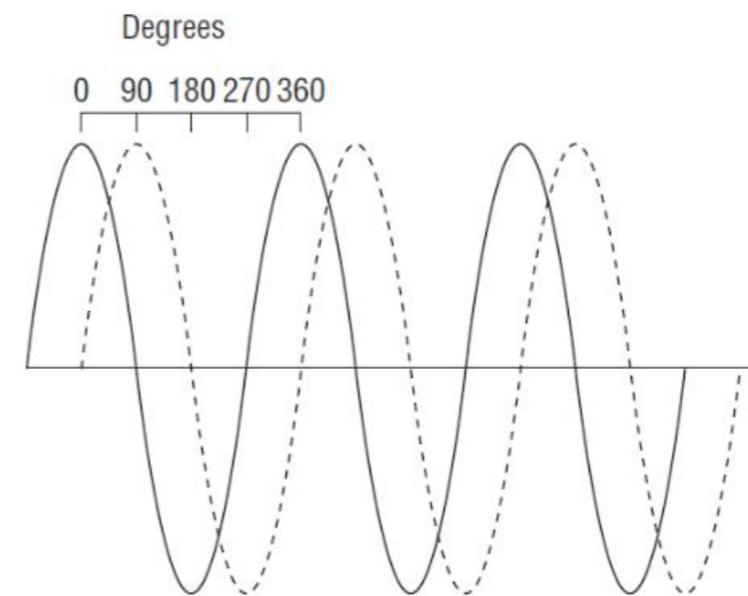
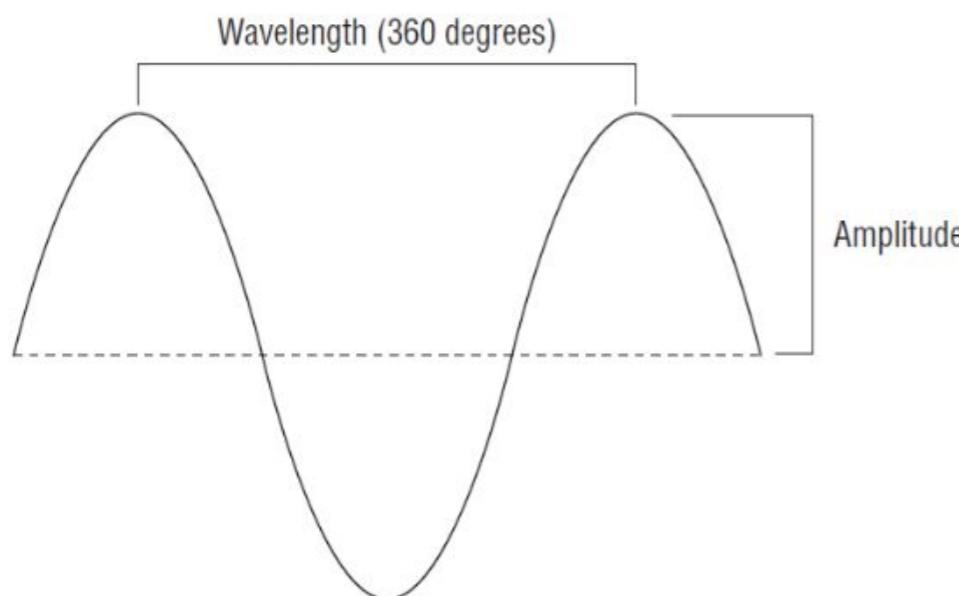
Bezdrátový signál

Elektrický signál (sinusový), který sám o sobě nenese žádnou informaci

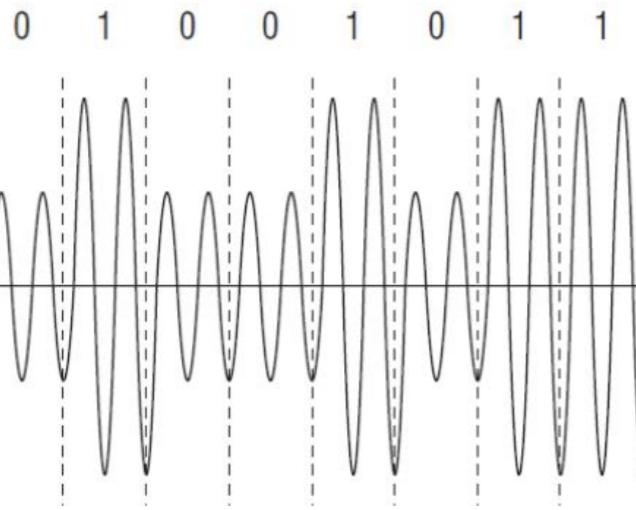
Může být modifikován (modulován), aby přenášel informaci (například binární)

Charakteristiky signálu, které lze změnit :

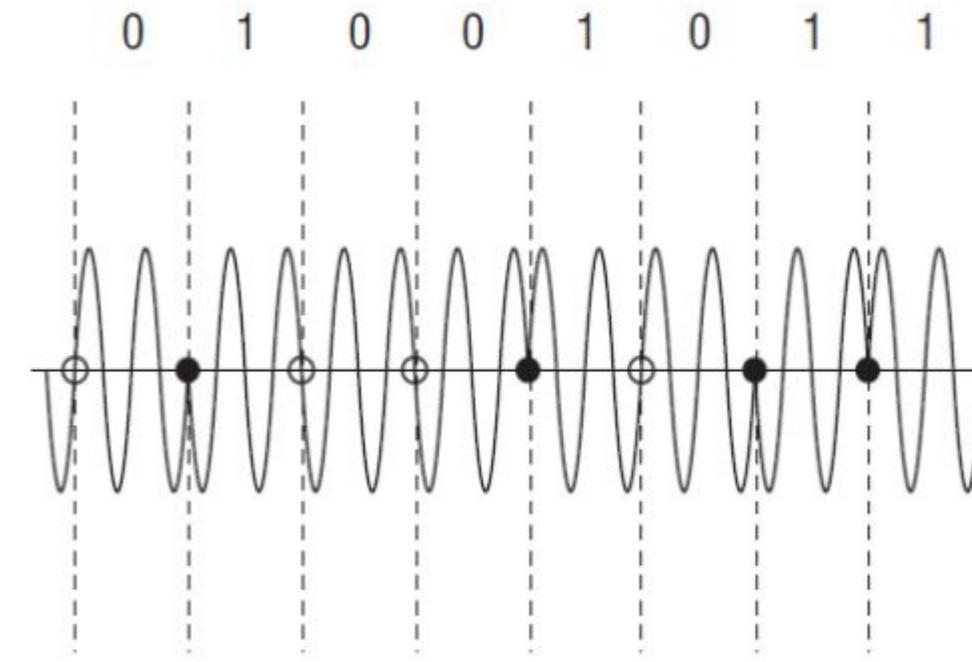
- Síla signálu (amplituda)
- Frekvence signálu
- Fáze



Modulace

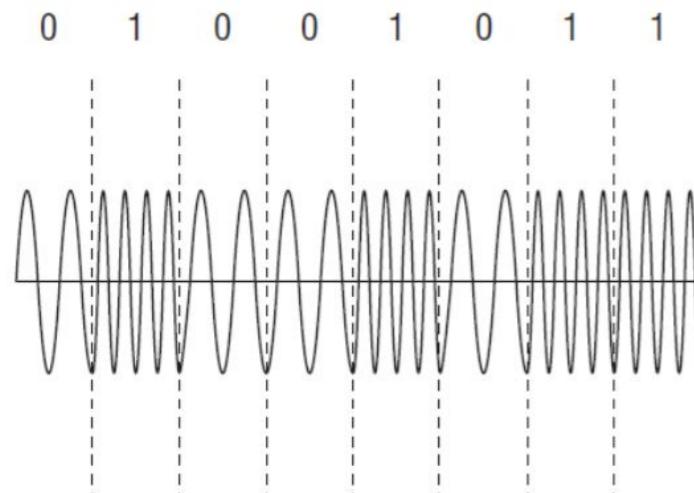


Amplitude-shift keying (ASK)



- No phase change occurred
- Phase change occurred

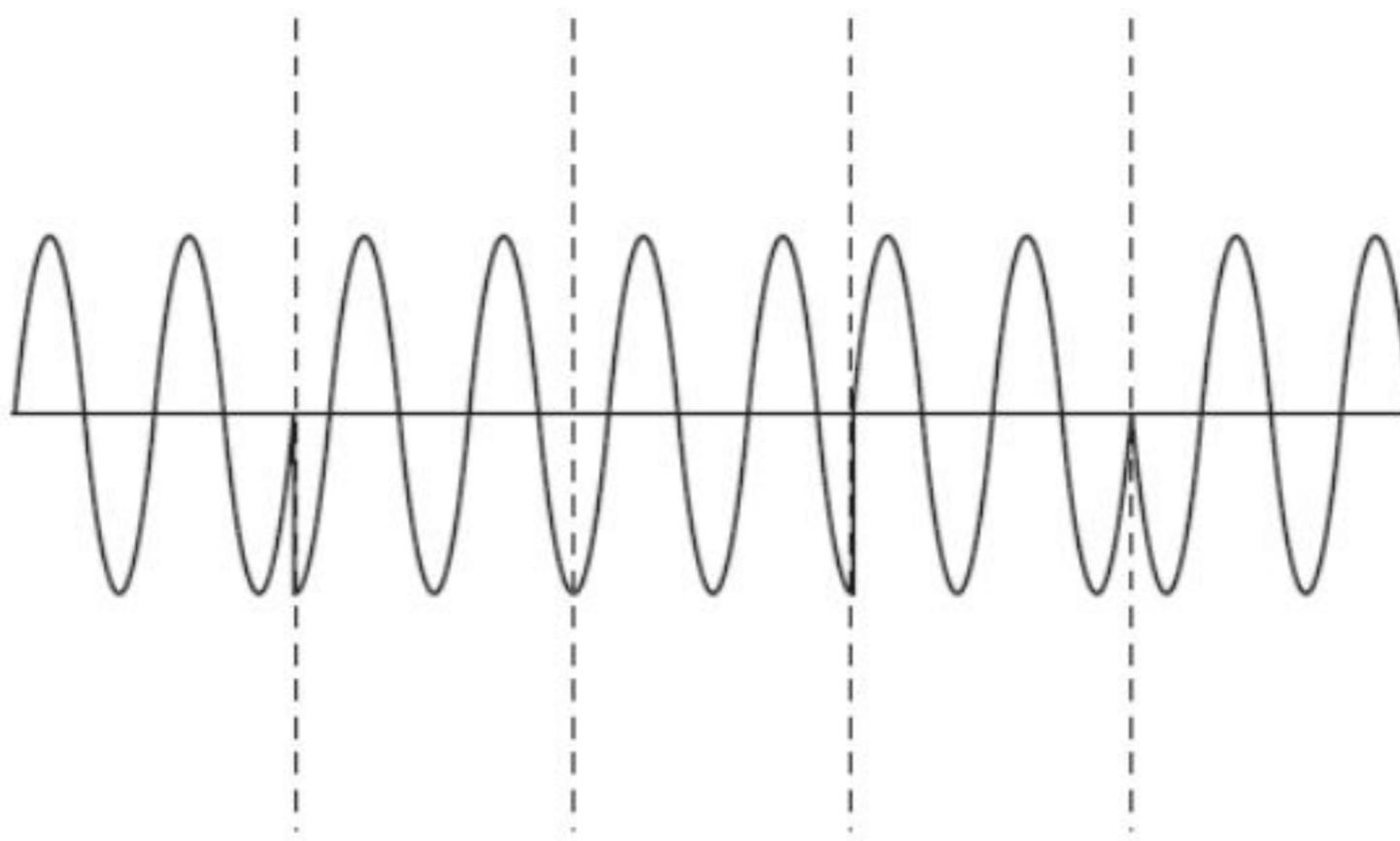
Phase-shift keying (PSK)



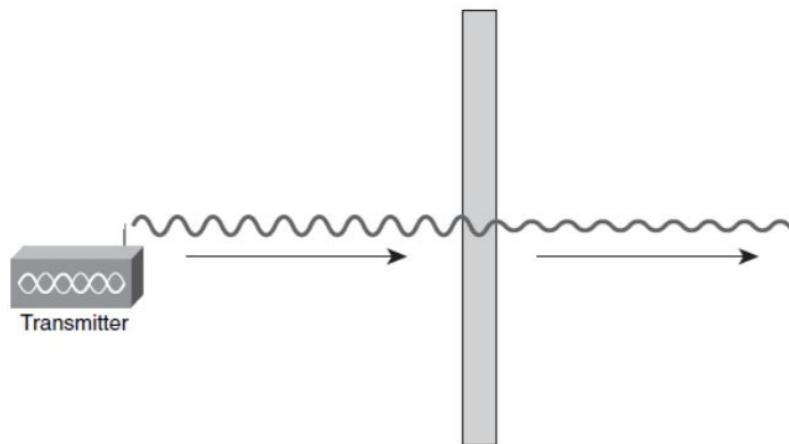
Frequency-shift keying (FSK)

Phase-Shift Keying

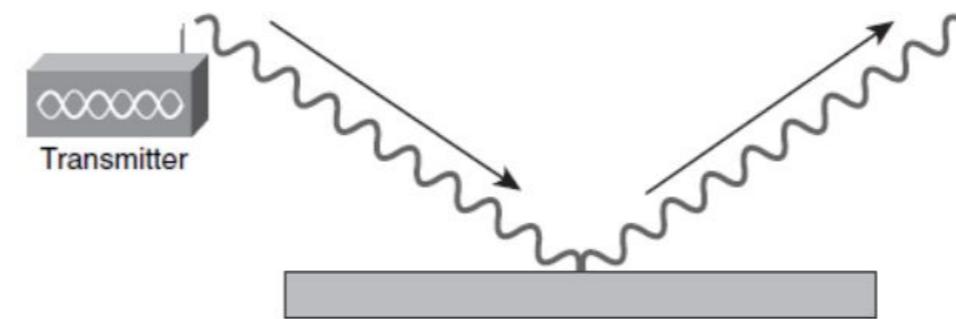
Previous symbol	+90° change 01	No change 00	+270° change 10	+180° change 11
-----------------	-------------------	-----------------	--------------------	--------------------



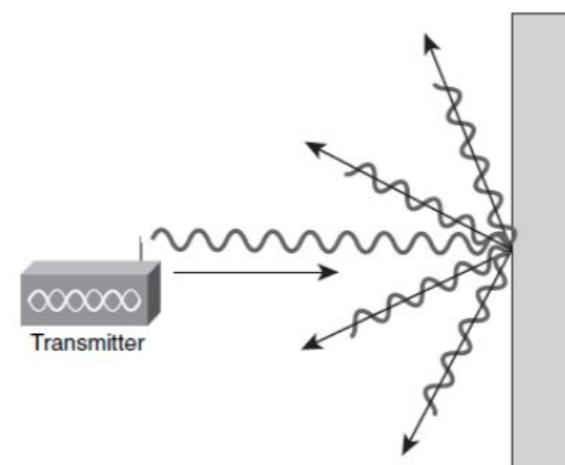
Šíření signálu v prostředí



Absorbce

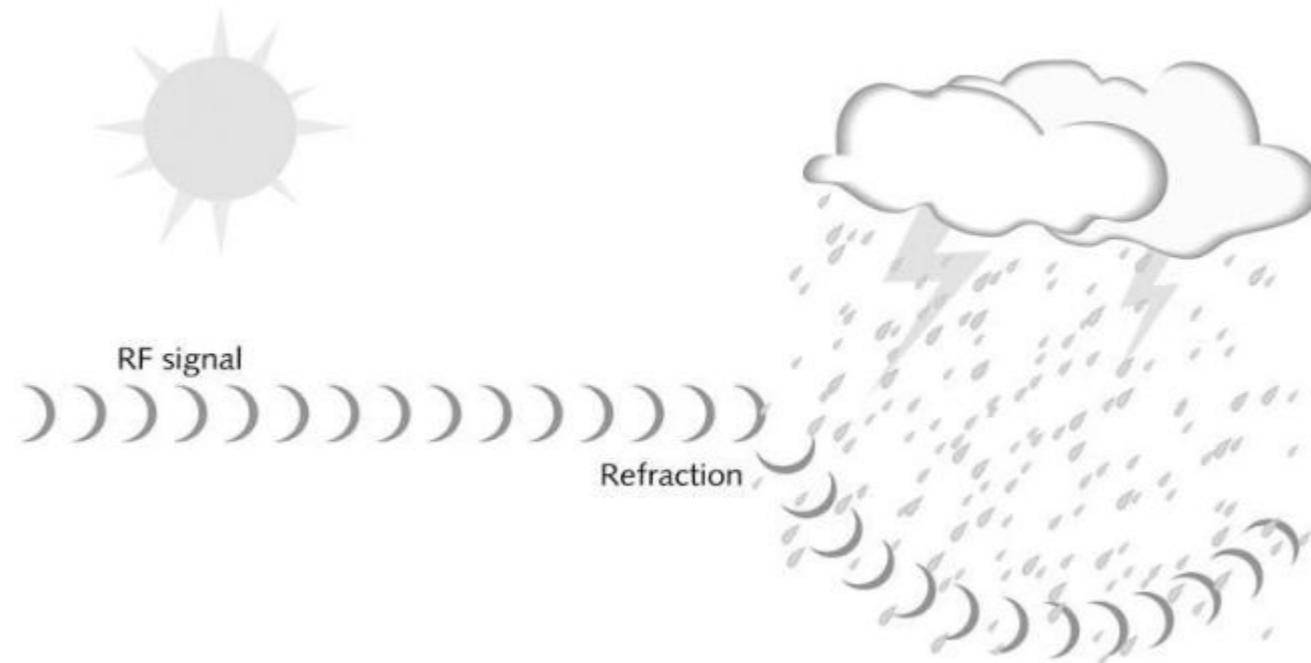


Odrاز

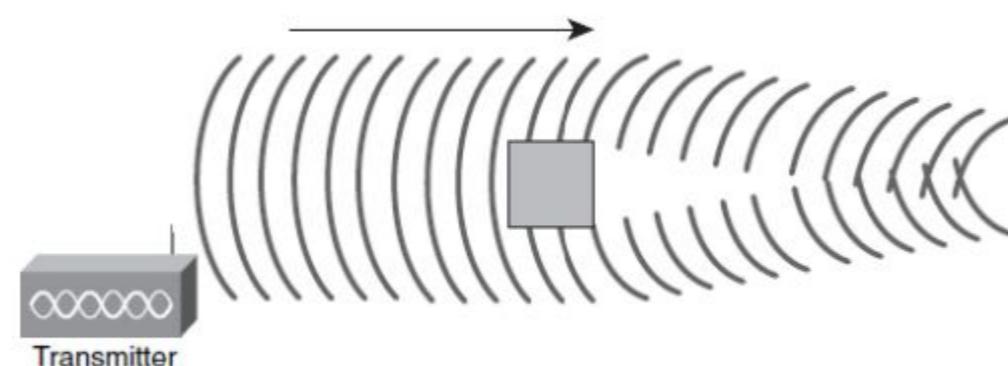


Rozptyl

“Ohnutí” signálu



Refraction



Diffraction

Útlum signálu

- Útlum signálu se vzdáleností
- Ztráta signálu je logaritmická a ne lineární
 - A 2.4 GHz signal will change in power by about 80 dB after 100 meters but will lessen only another 6 dB in the next 100 meters

$$FSPL = 32.44 + (20 \log_{10} f + 20 \log_{10} D)$$

- FSPL - útlum v dB
- F - frekvence v MHz
- D - vzdálenost mezi anténami

Wifi standardy

Organizace

IEEE

Wifi standard 802.11 – více jak 30 protokolů

WiFi Alliance

Certifikuje kompatibilitu komunikace mezi bezdrátovými zařízeními

IETF

Vytváří standardy protokolů vyšších vrstev (Internet)

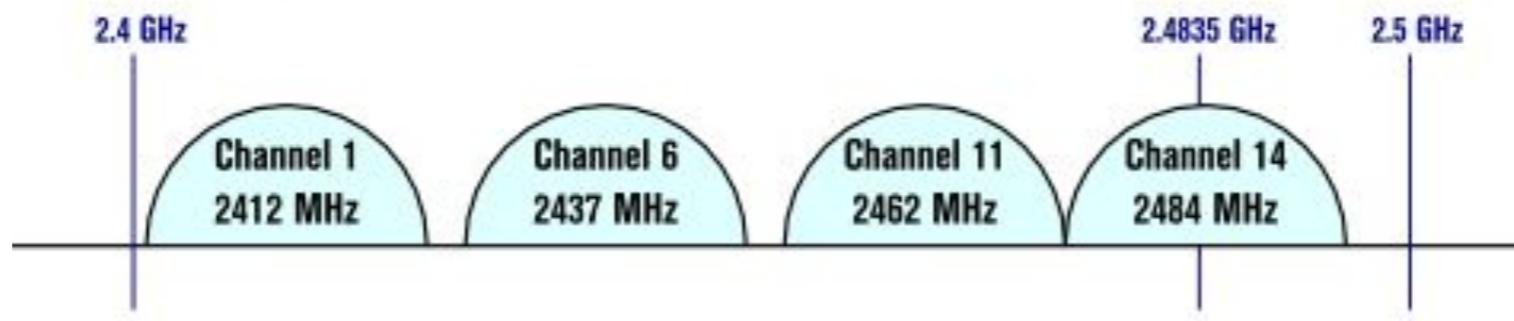
TABLE 1: IEEE 802.11 COMMON WIFI STANDARDS BREAKDOWN

Standard	Frequency Band	Bandwidth	Modulation Scheme	Channel Arch.	Maximum Data Rate	Range	Max Transmit Power
802.11	2.4 GHz	20 MHz	BPSK to 256-QAM	DSSS, FHSS	2 Mbps	20 m	100 mW
b	2.4 GHz	21 MHz	BPSK to 256-QAM	CCK, DSSS	11 Mbps	35 m	100 mW
a	5 GHz	22 MHz	BPSK to 256-QAM	OFDM	54 Mbps	35 m	100 mW
g	2.4 GHz	23 MHz	BPSK to 256-QAM	DSSS, OFDM	54 Mbps	70 m	100 mW
n	2.4 GHz, 5 GHz	24 MHz and 40 MHz	BPSK to 256-QAM	OFDM	600 Mbps	70 m	100 mW
ac	5 GHz	20, 40, 80, 80+80=160 MHz	BPSK to 256-QAM	OFDM	6.93 Gbps	35 m	160 mW
ad	60 GHz	2.16 GHz	BPSK to 64-QAM	SC, OFDM	6.76 Gbps	10 m	10 mW
af	54-790 MHz	6, 7, and 8 MHz	BPSK to 256-QAM	SC, OFDM	26.7 Mbps	>1km ?	100 mW
ah	900 MHz	1, 2, 4, 8, and 16 MHz	BPSK to 256-QAM	SC, OFDM	40 Mbps	1 km	100 mW

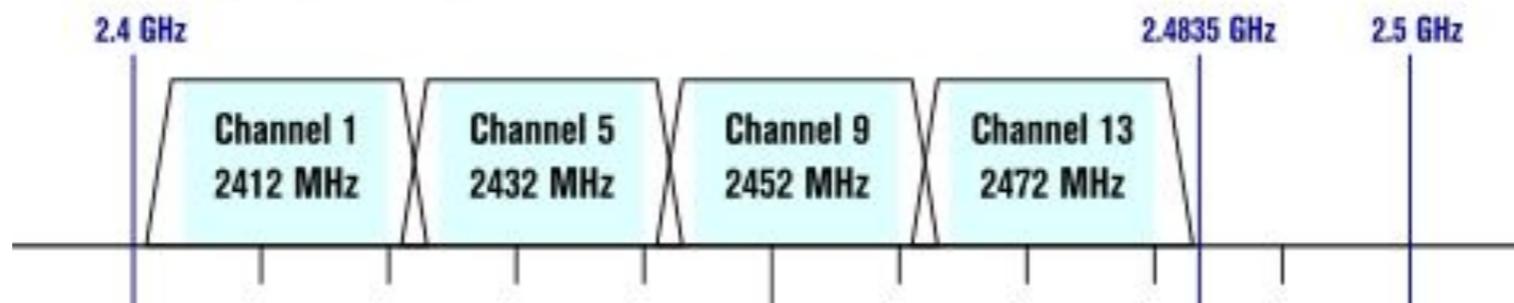
Kanály 2.4 GHz

Non-Overlapping Channels for 2.4 GHz WLAN

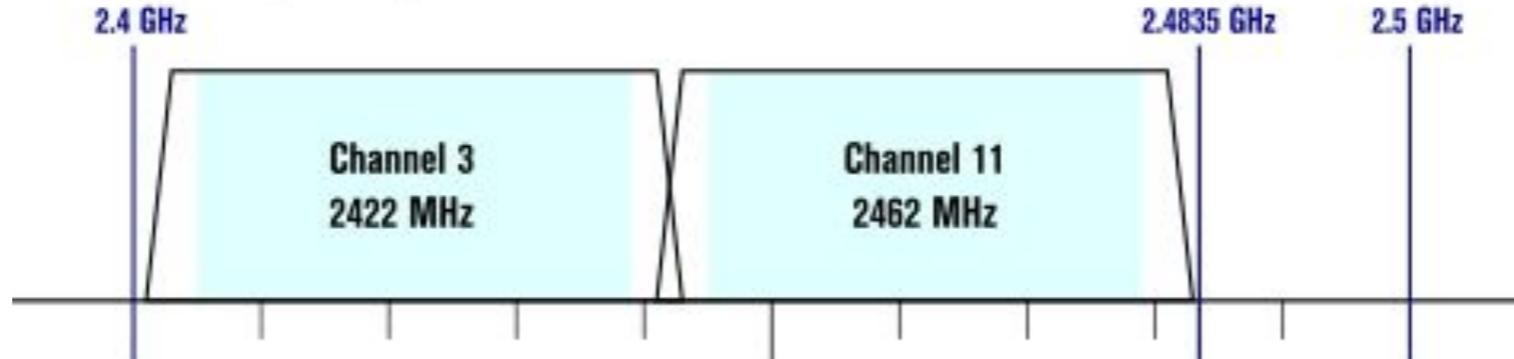
802.11b (DSSS) channel width 22 MHz



802.11g/n (OFDM) 20 MHz ch. width - 16.25 MHz used by sub-carriers



802.11n (OFDM) 40 MHz ch. width - 33.75 MHz used by sub-carriers



Kanály 5GHz

802.11AC kanály mohou být široké 20 MHz, 40 MHz, 80 MHz nebo 160 MHz.

Channel 5180/20-Ceee/ac/P(20dBm)																									
5 GHz Channel Allocations																									
Frequency (GHz)	5.150	5.250	5.470	5.600	5.640	5.725	5.850																		
802.11 Allocations	UNII-1			UNII-2a			UNII-2c (Extended)			UNII-3															
Center Frequency	5180	5200	5220	5240	5260	5280	5300	5320	5500	5520	5540	5560	5580	5600	5620	5640	5660	5680	5700	5720	5745	5765	5785	5805	5825
20 MHz	36	40	44	48	52	56	60	64	100	104	108	112	116	120	124	128	132	136	140	144	149	153	157	161	165
40 MHz	38	46			54	62			102	110			118	126			134	142			151	159			
80 MHz		42				58			106				122				138			155					
160 MHz		50					114																		
FCC	1,000 mW Tx Power Indoor & Outdoor No DFS needed	250 mw w/6dBi Indoor & Outdoor DFS Required	250mw w/6dBi Indoor & Outdoor DFS Required 144 Now Allowed	120, 124, 128 Devices Now Allowed													1,000 mW EIRP Indoor & Outdoor No DFS needed 165 was ISM, now UNII-3								
DFS Channels					DFS Channels																				

Komponenty Wifi sítí

Bezdrátový klient

Koncová stanice WLAN sítě

Specializovaná bezdrátová síťová karta

Různé karty, různé rozhraní



40

Přístupový bod

Zabezpečuje vzájemnou komunikaci WLAN klientů a spojení WLAN s LAN

Může být integrovaný s dalšími zařízeními – typicky směrovač a DSL/kabelový modem

Různá zařízení pro venkovní/vnitřní použití



Další komponenty

Opakovač – repeater

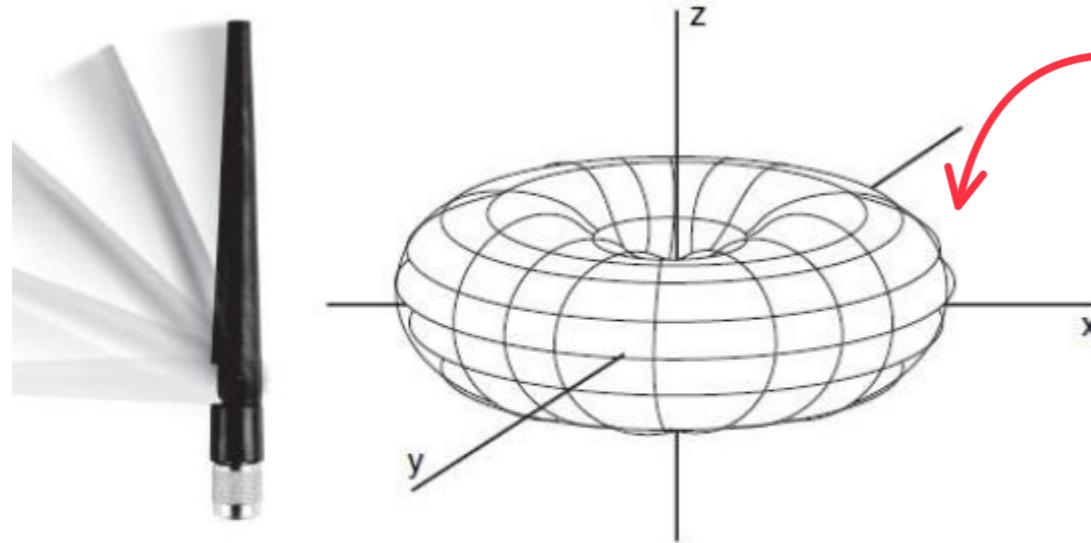
- Zabezpečuje zvýšení plochy pokryté signálem
- Jeho použití snižuje efektivní přenosovou rychlosť
- Potřebné 50% překrytí tzv. catchment area

Antény

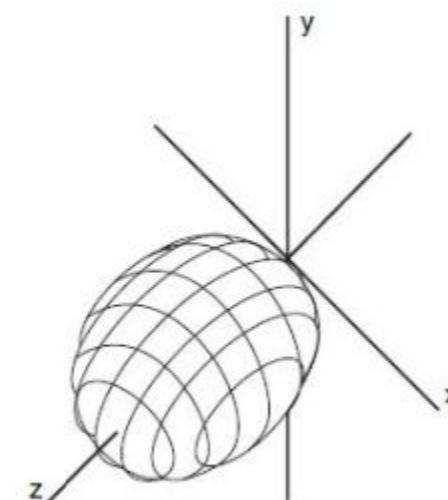
- Různé druhy – vše směrové, sektorové, směrové
- Liší se použitým druhem konektoru, kabelem, ziskovostí, směrovostí...



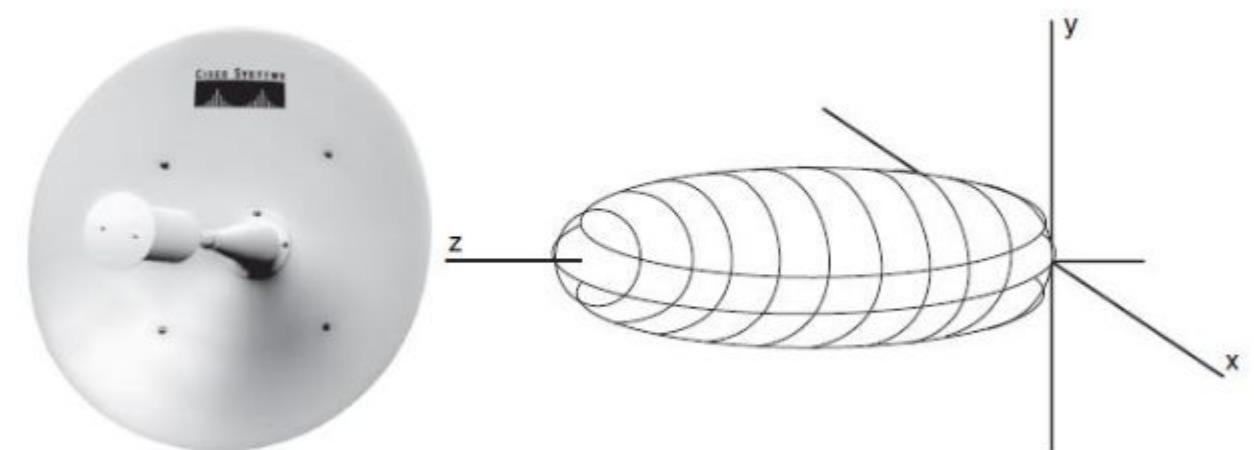
Antény



Všeobecná – zisk 2dBi



Sektorová – zisk 6-8dBi



Směrová – zisk 22dBi

Základní formy WLAN sítí

Independent Basic Service Set (IBSS):

- Síť tvořená výlučně WLAN klienty bez centrálního prvku
- Mode Ad-Hoc

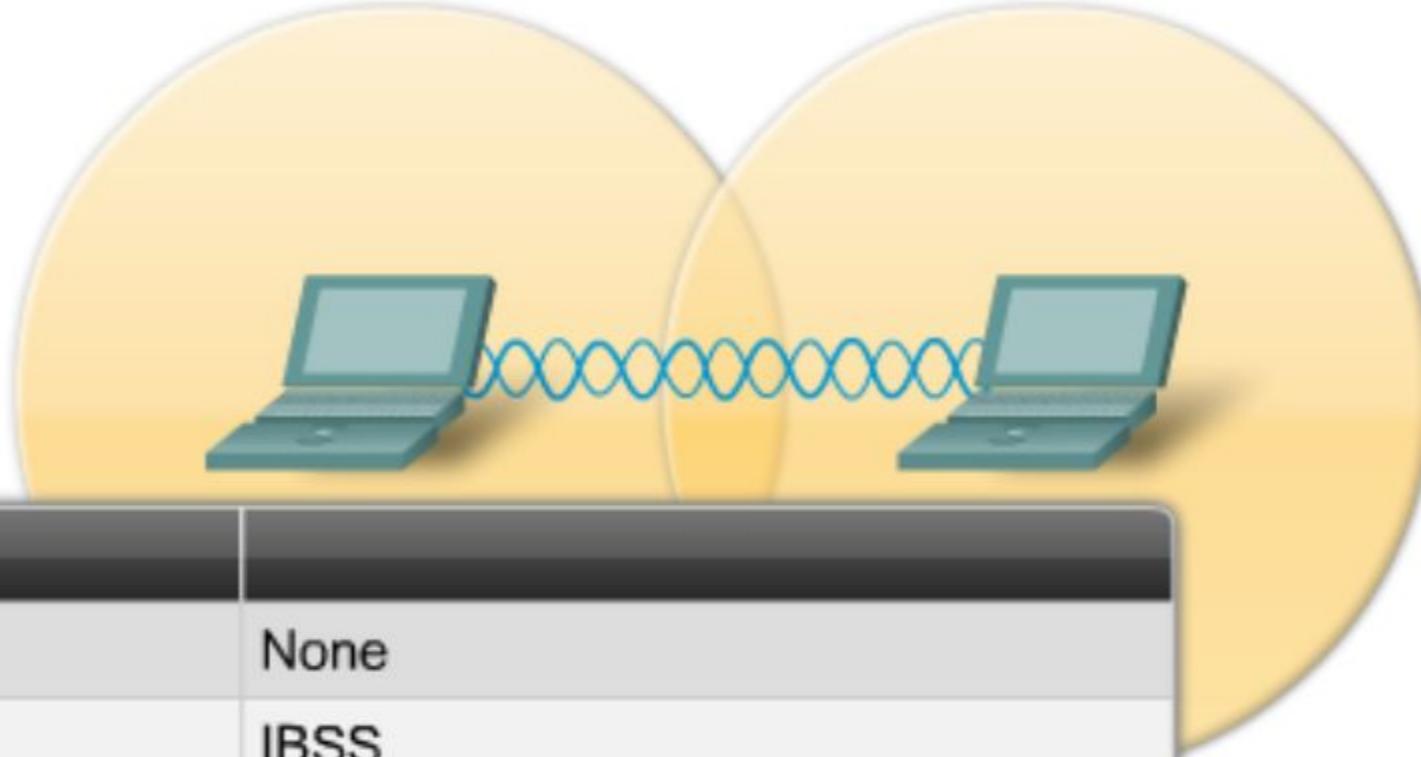
Basic Service Set (BSS):

- WLAN síť tvořená přístupovým bodem a klienty
- Mode Infrastructure

Extended Service Set (ESS):

- WLAN síť se skládá z několika BSS sítí propojených tzv. distribučním systémem
- Mode Infrastructure

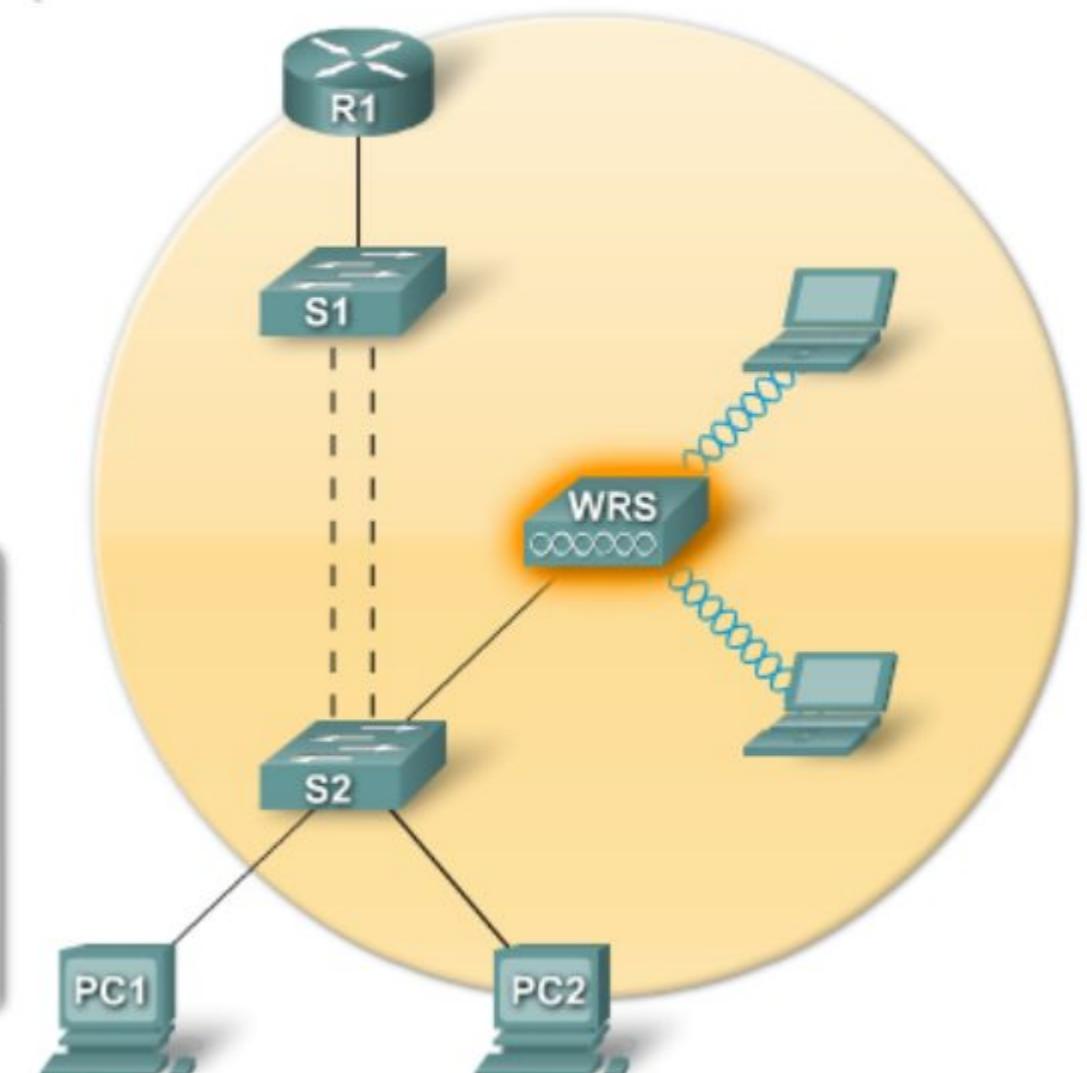
Ad-hoc - IBSS



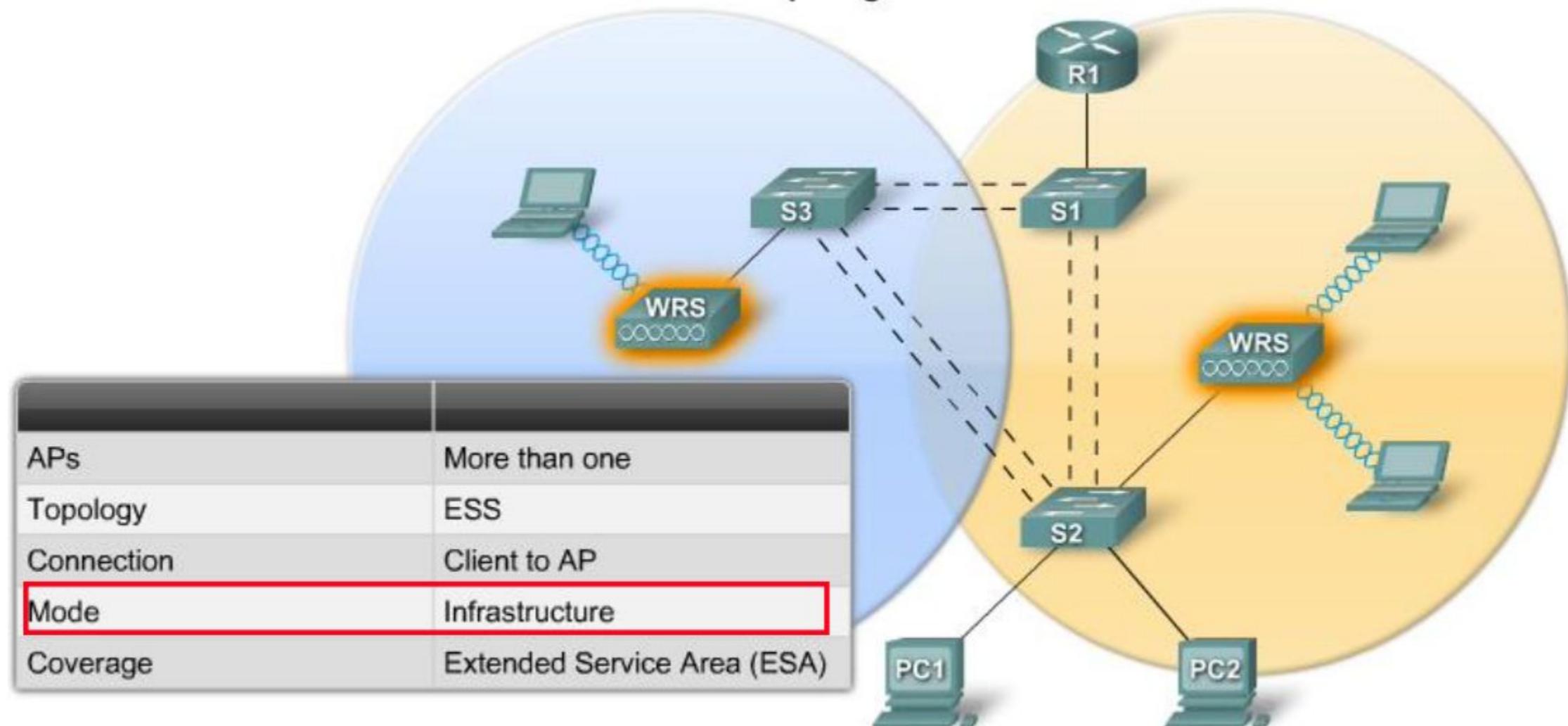
APs	None
Topology	IBSS
Connection	Peer-to-Peer
Mode	Ad hoc
Coverage	Basic Service Area (BSA)

Infrastructure BSS

APs	One
Topology	BSS
Connection	Client to AP
Mode	Infrastructure
Coverage	Basic Service Area (BSA)



Infrastructure ESS



Identifikátor bezdrátové sítě – SSID

- SSID (Service Set ID) je slovní název sítě
- AP může SSID vysílat ve svých tzv. beacon rámcích
- SSID může být i skryté
- Klient musí znát SSID při přihlašování se do sítě
- Jeden AP může rozesílat několik SSID
- Každý SSID má samostatnou VLAN
- AP využívá trunking a 802.1Q na roztrídění rámců mezi SSID/VLAN

WLAN Client Access

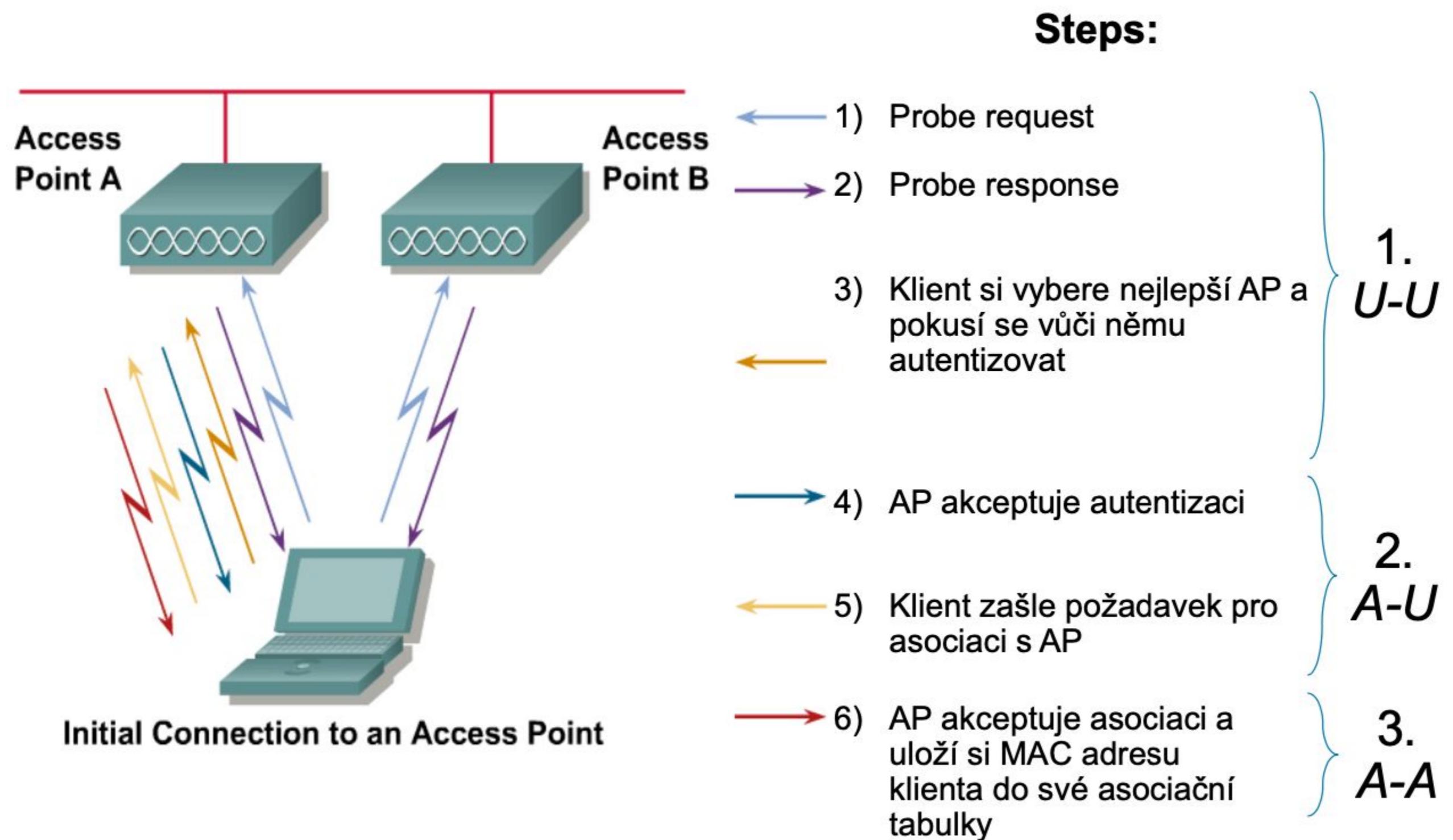
Pro připojení WLAN klient potřebuje:

- SSID
- Kompatibilní komunikaci (a,g,n,ac,...)
- Autentizaci

Připojení k AP prochází třemi stavy:

1. Unauthenticated, Unassociated
Počáteční stav
2. Authenticated, Unassociated
Klient se autentizuje vůči AP správnými údaji
3. Authenticated, Associated
Klient se může po autentizaci asociovat s daným AP a získat tak plnou konektivitu

WLAN Client Access



Komunikace ve WLAN sítích

Způsob komunikace

- Half duplex
- Sdílené přenosové médium
Stejný kanál pro všechna zařízení v síti
- Závislost mezi přenosovou rychlostí a vzdáleností od AP
Vzdálenost a vzájemné rušení sousedních kanálů ovlivňuje rychlosť
- Různé přenosové rychlosti na jednom kanále
Zařízení s nižší rychlostí snižuje celkovou propustnost
- Potvrzování zpráv
Zařízení nedokáže současně vysílat a přijímat, proto musí přijímací zařízení potvrdit každý přenesený rámec aby chom věděli, že nedošlo ke kolizi a poškození rámce.

Komunikace ve WLAN síti

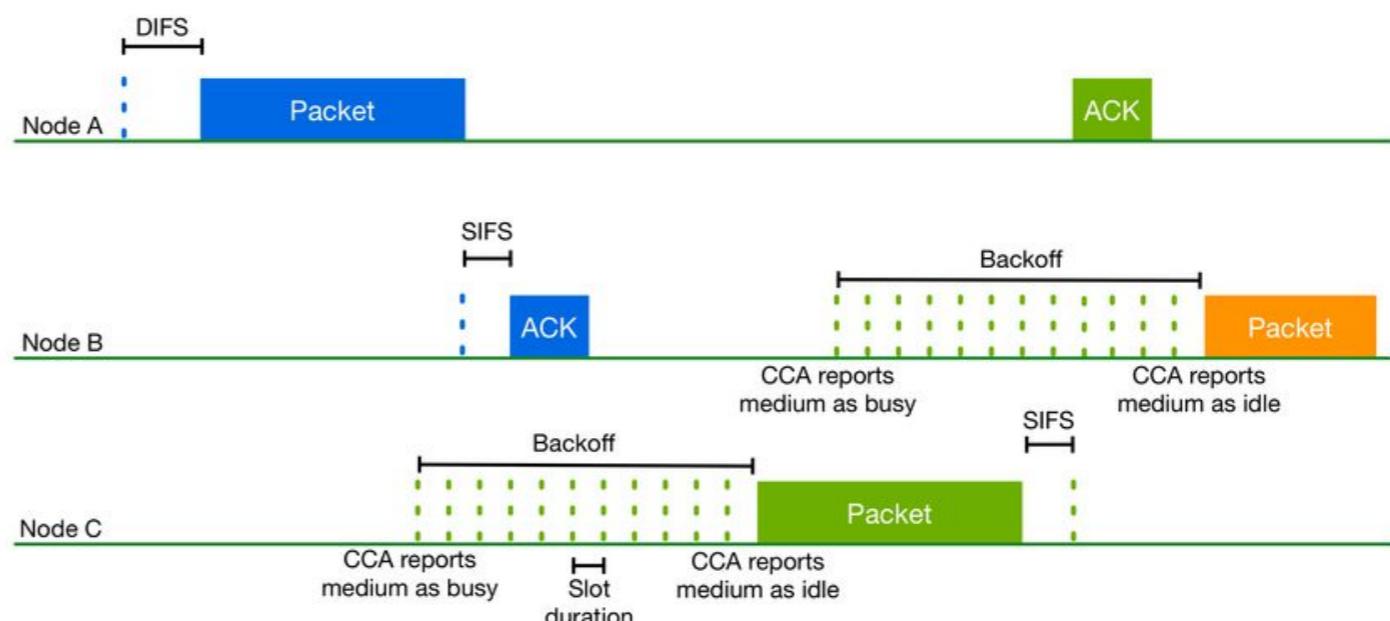
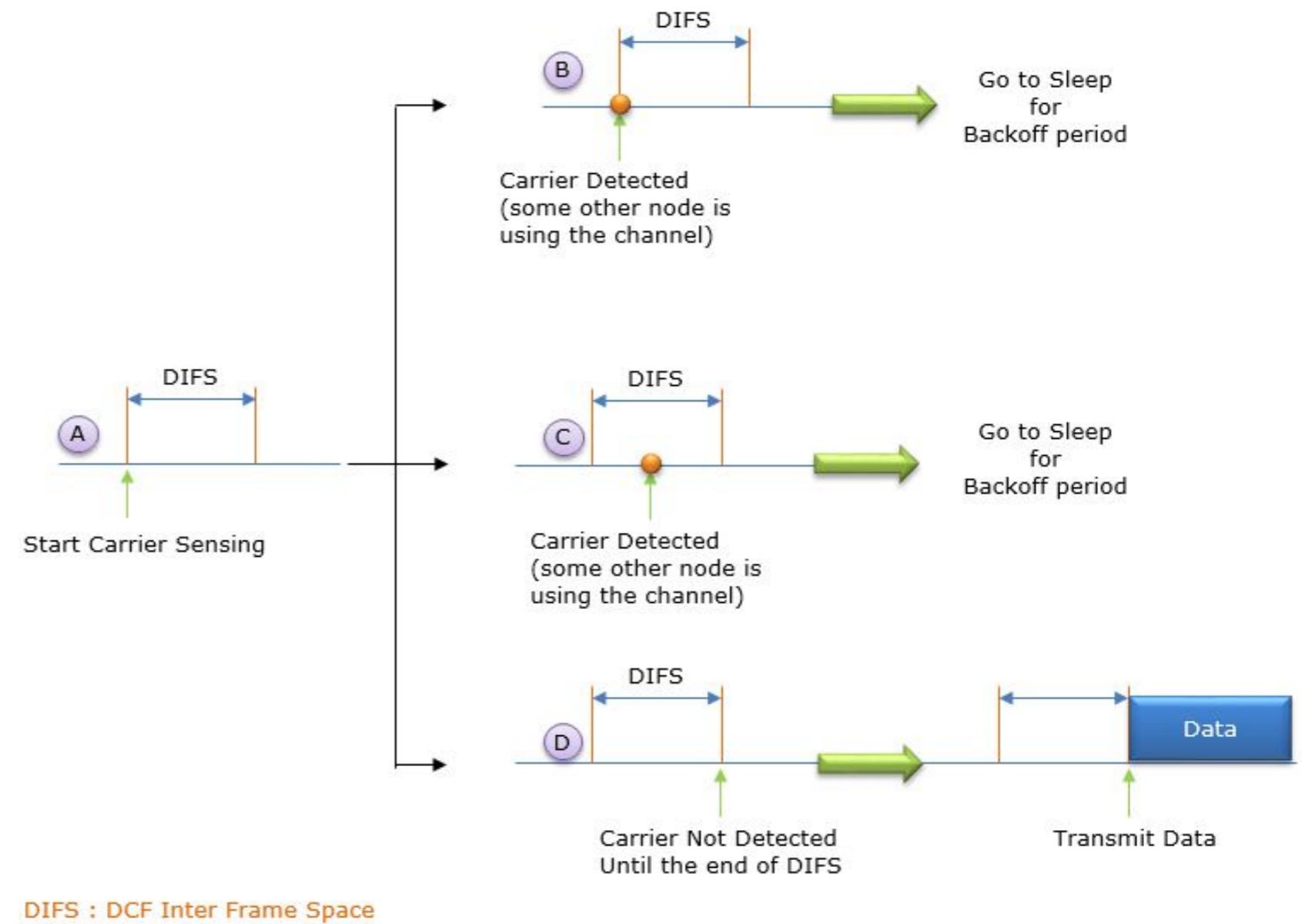
WLAN klienti se vzájemně musí slyšet, ale data se přenášejí výhradně pomocí AP

Metoda přístupu k sdílenému médiu:

- CSMA/CA: Carrier Sense Multiple Access with Collision Avoidance
- RTS/CTS: Request to Send and Clear to Send

Hidden node problem

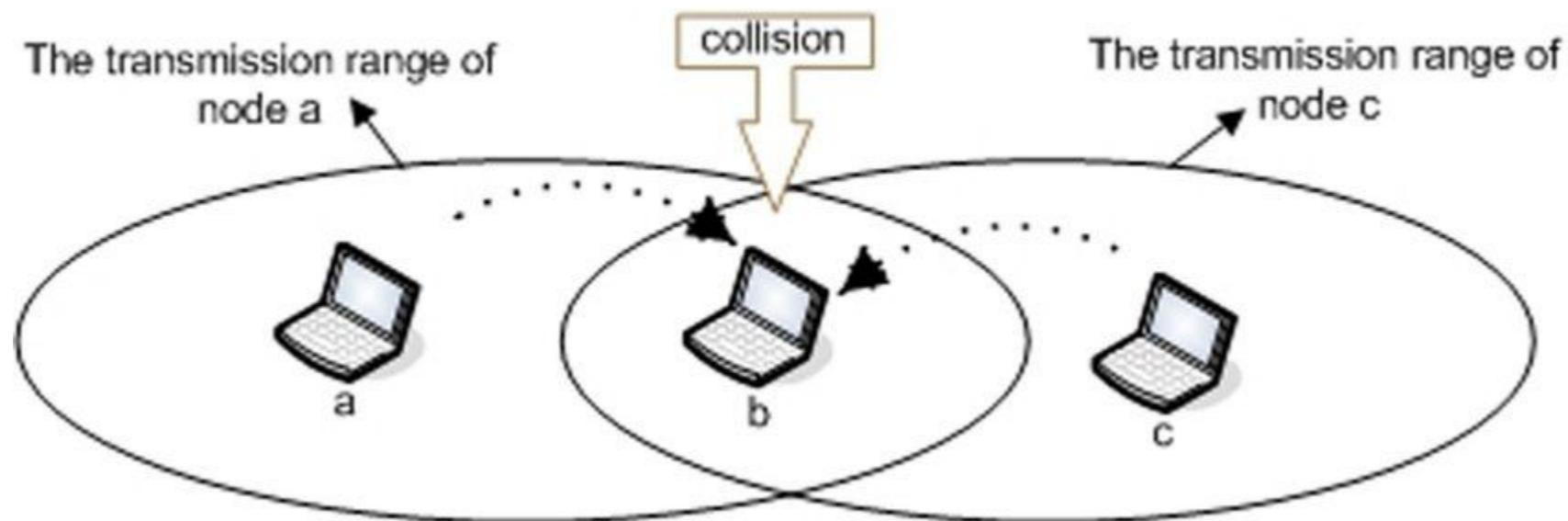
CSMA/CA



Hidden Node Problem

CSMA/CA není v této situaci funkční mechanismus

V případě, že b je AP, lze řešit pomocí RTS/CTS



IEEE 802.11 RTS/CTS

Request To Send (RTS)

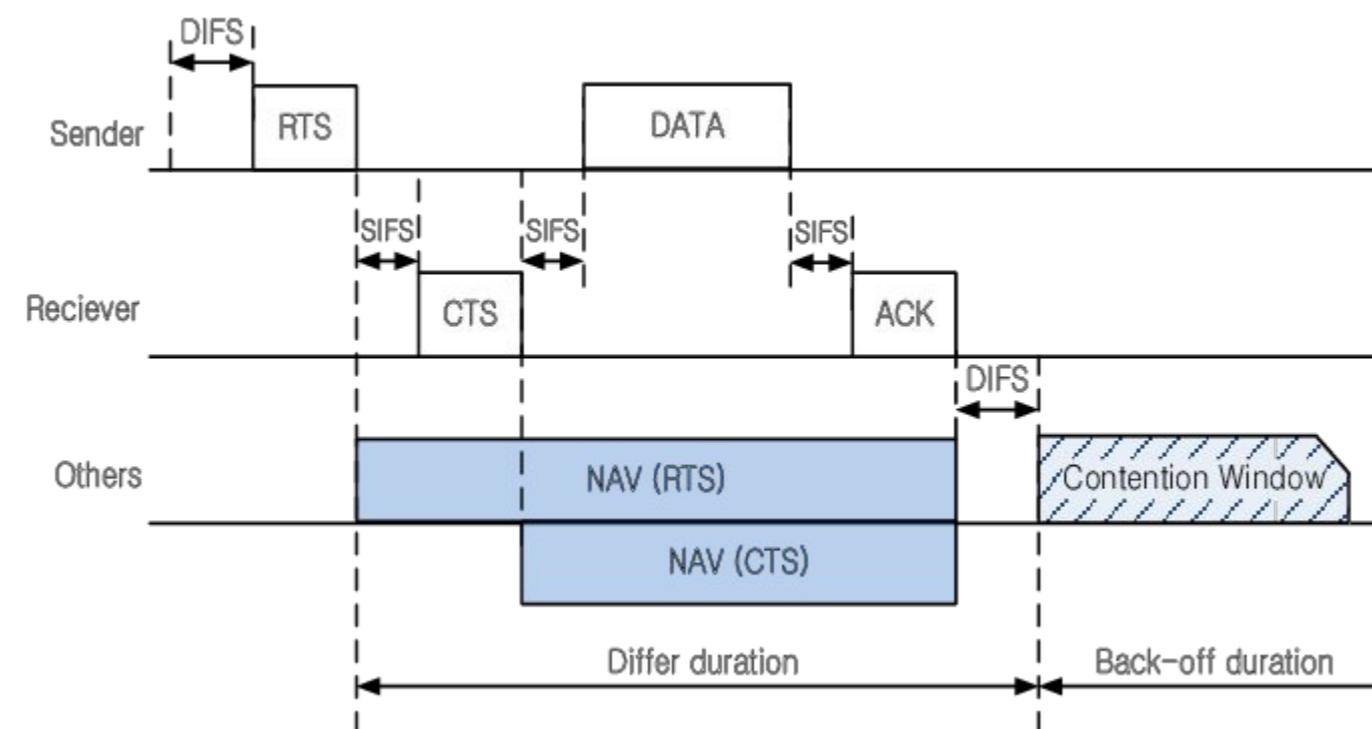
Stanice informuje příjemce, že mu chce poslat data a informuje o potřebném čase pro tento přenos

Clear To Send (CTS)

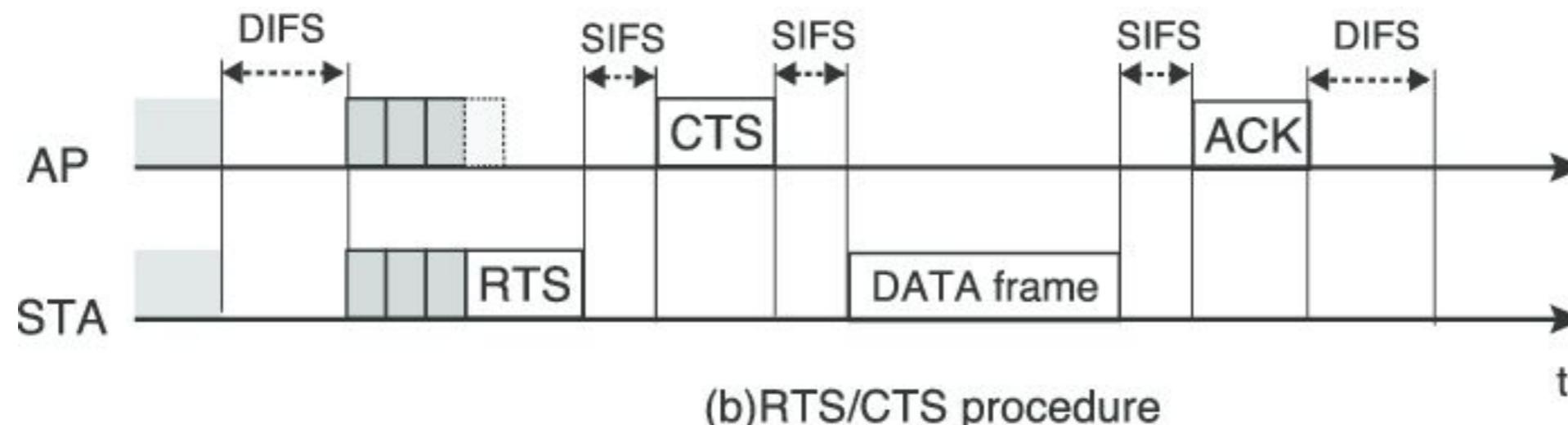
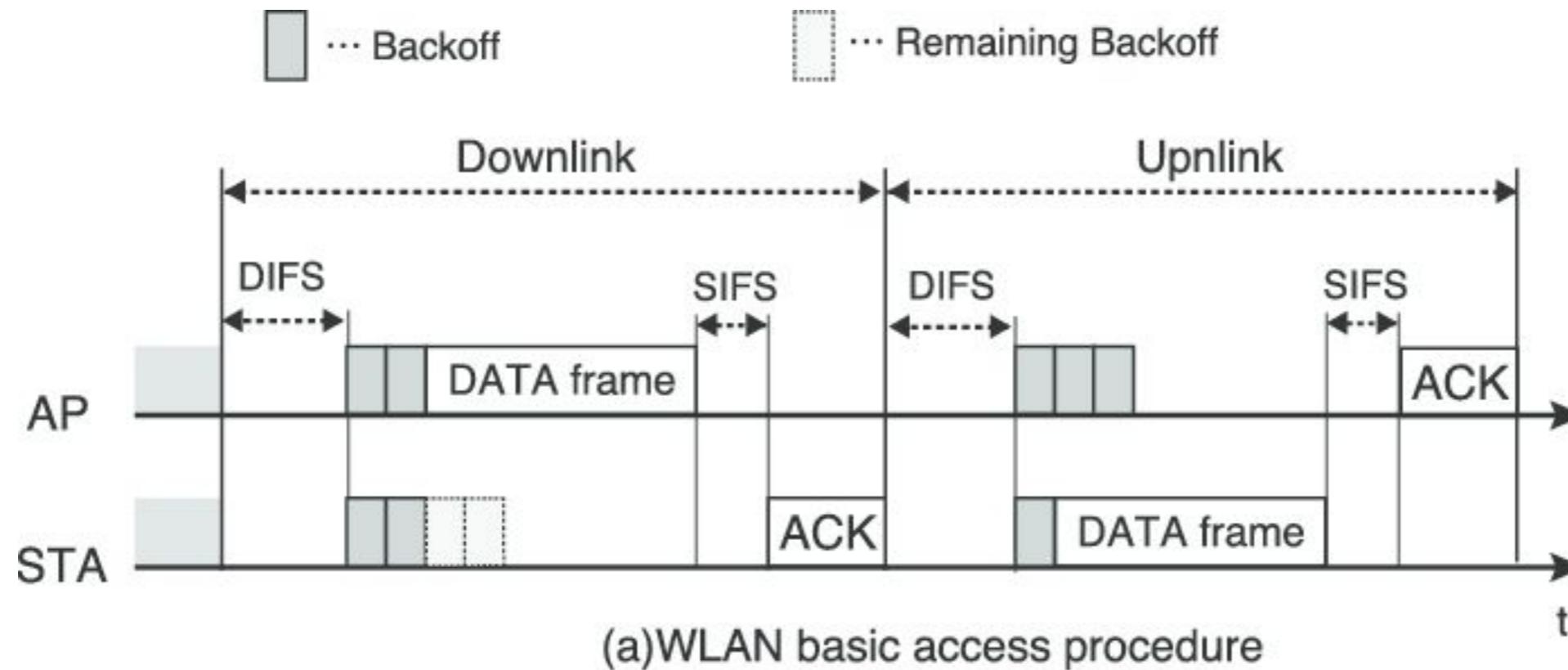
Stanice potvrzuje příjem žádosti RTS a informuje o potřebném čase pro přenos

Network Allocation Vector (NAV)

Slouží pro určení okamžiku, kdy bude médium volné



Rozdíl CSMA/CA a RTS/CTS



Bezpečnost WLAN

Bezpečnost WLAN

Třeba si uvědomit že:

- Pasivní odposlouchávání není možné detektovat
- Rádiový signál není možné ohraňčit

U WLAN je potřebné akceptovat, že provoz bude odposloucháván a zaměřit se na to, aby jeho zachycením útočník nic nezískal

Vhodné řešení: šifrování přenášených dat

Původní standard: Wired Equivalent Privacy (WEP)

Novější standardy: WPA/WPA2 a nejnověji WPA3

Bezpečnost WLAN - Autentizace

Původní standard 802.11b obsahuje jednoduchou podporu pro autentizaci:

Open System - bez ověření

Shared Key

- AP posílá klientovi výzvu (challenge), klient ji pomocí hesla zašifruje a posílá zpět na AP. Pokud je AP schopen pomocí stejného hesla odpověď dešifrovat a dostat původní challenge, klienta autentizuje
- Používá Static WEP key
- Problémy s kryptografickou bezpečností, nedoporučuje se používat

Heslo používané v režimu Shared Key se používá i pro šifrování přenášených dat

WPA2

WiFi Protected Access 2 (WPA2)

- Standardizovaná v 802.11i
- Využívá šifrovací algoritmus AES (Rijndael)
- Advanced Encryption Standard
- V současnosti nejsou proti WPA2 známé efektivní způsoby útoku
- Zpravidla si žádá výměnu prvků (AES je třeba dělat v HW), která často není možná

WPA verze

WPA-PSK (TKIP)

- Temporal Key Integrity Protocol využívá k šifrování proudovou šifru RC4 a k autentizaci zpráv keyed-hash algoritmus Michael.

WPA2-PSK (AES)

- PSK AES šifruje data pomocí šifry AES a k ověření autentizace využívá CBC-MAC.

WPA2-Enterprise

- používá autentizační server (RADIUS)
- unikátní uživatelská jména a hesla

Bezpečnost WLAN - Autentizace

EAP – Extensible Authentication Protocol, RFC 3748

- Generický protokol (framework) pro přenos různých druhů autentizačních dialogů mezi klientem (tzv. supplicant) a bodem vyžadujícím autentizaci (tzv. authenticator)
- Poskytuje základní formát datových struktur, které jsou využitelné pro libovolný druh autentizace
- Výhodou je, že authenticator nemusí konkrétnímu typu autentizace rozumět, jen přenáší dialog mezi supplicantem a autentizačním serverem

RFC 4017 „Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs“

- Pokrývá EAP pro WiFi prostředí

Bezpečnost WLAN - RADIUS

Otevřený protokol standardizovaný v IETF RFC 2865

Postavený nad UDP, využívá port 1812 a 1813

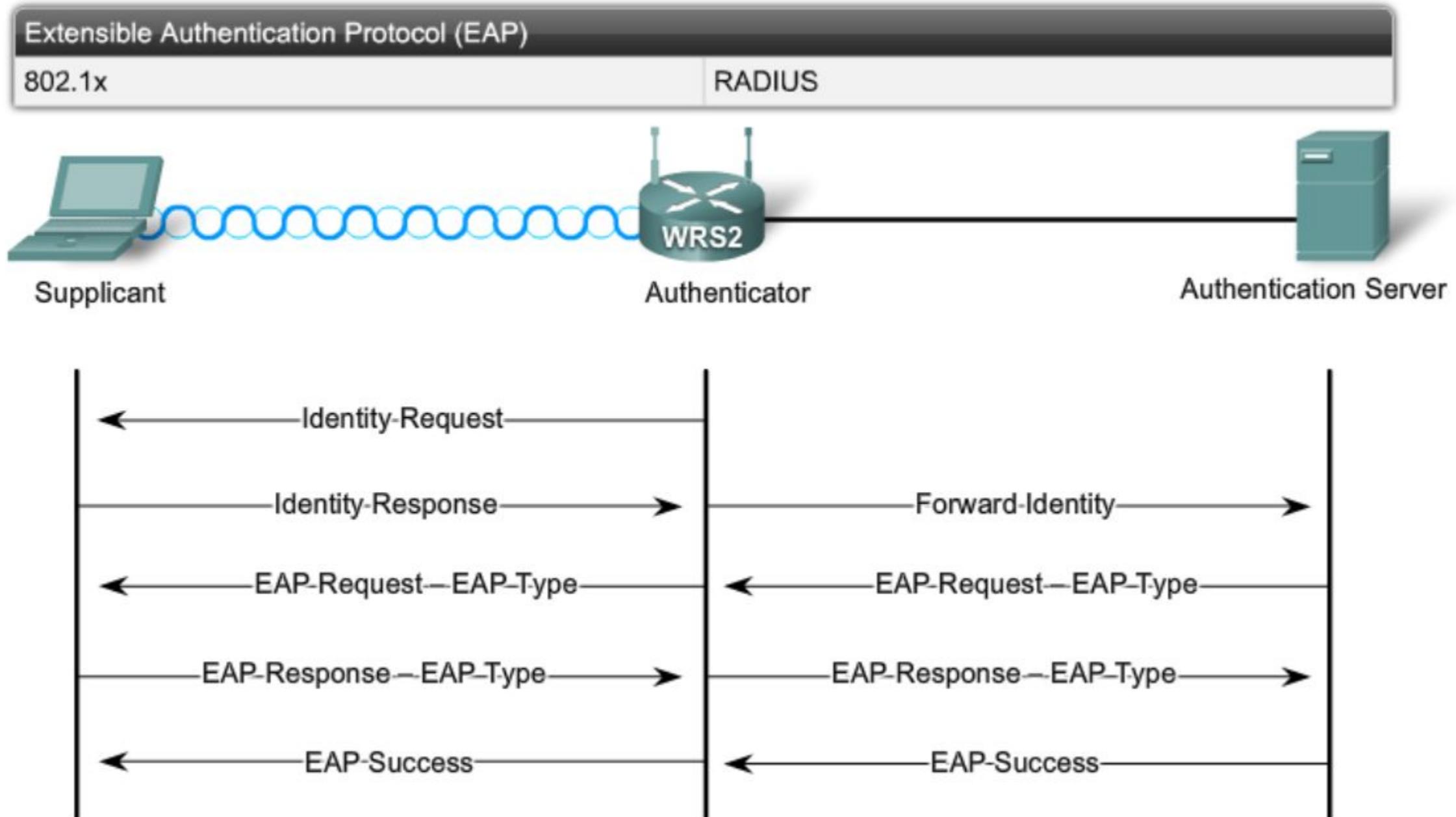
Zabezpečuje AAA funkce mezi tzv. Network Access Serverem (klient) a RADIUS serverem

Poskytuje možnosti poskytnout klientovi doplňující konfigurační informace

EAP zprávy od klienta (supplicant) se na AP (authenticator) zabalí do RADIUS zpráv a odošlou na RADIUS server

Pokud RADIUS vyžaduje doplňující informace, odešle EAP zprávu obalenou do RADIUS paketu na AP a ten ji přepošle klientovi

EAP



Závěr

Závěr

Detekce a oprava chyb

Řízení přístupu k sdílenému médiu

ETHERNET

- CSMA/CD
- Adresování
- ARP
- Aktivní síťové prvky
- VIRTUÁLNÍ LAN SÍTĚ
- STP

Bezdrátové sítě

- Principy komunikace a řízení média
- Zabezpečení