Point to Point prepoje a PPP protokol

M3, CCNA4, v5

Pavel Segeč

Katedra informačných sietí

Fakulta riadenia a informatiky, ŽU

Obsah

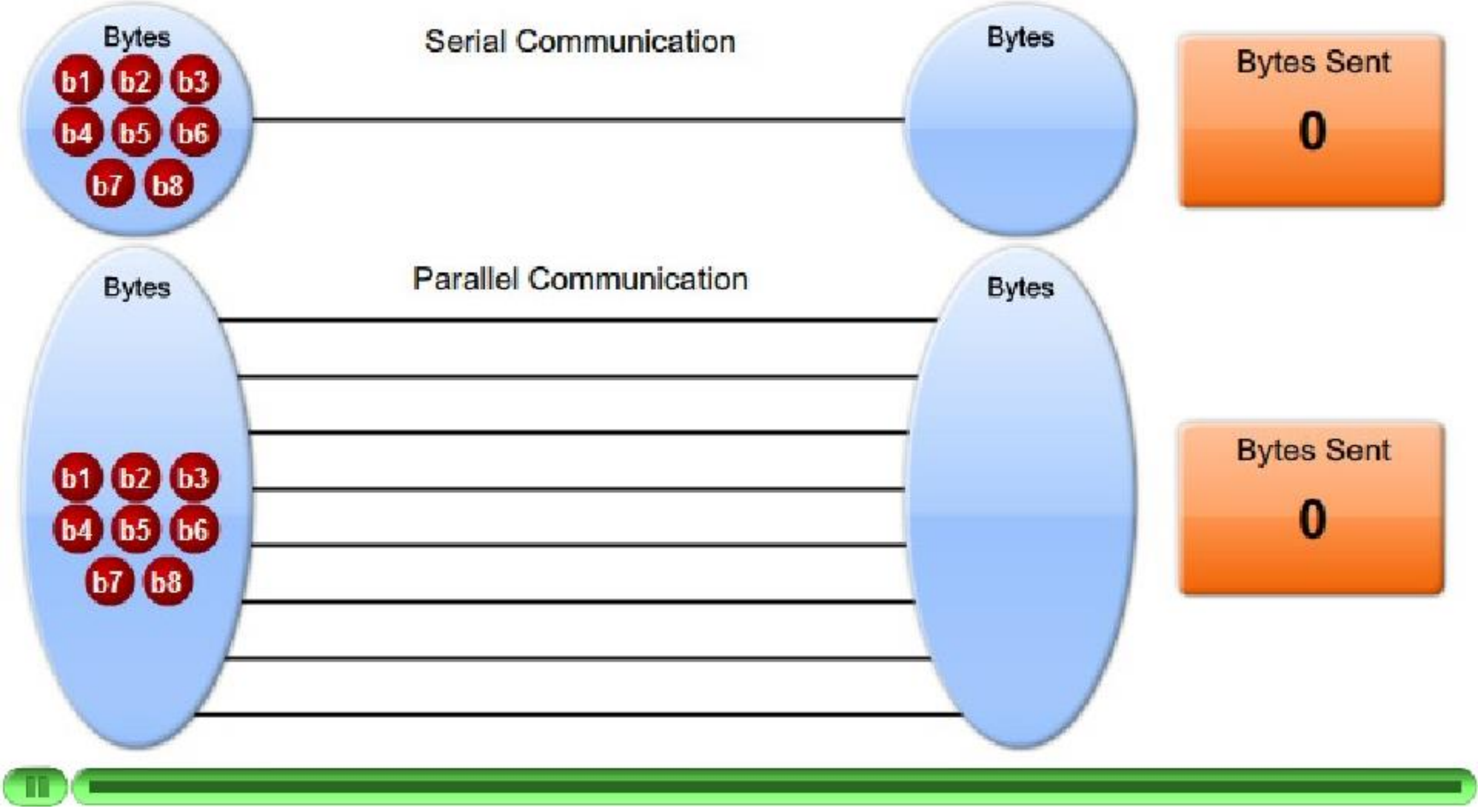
- HDLC
- Serial Point-to-Point linky
- PPP
- PPP autentifikácia
  - PAP
  - CHAP
- Konfigurácia PPP

Sériová komunikácia, HDLC a Point-to-Point protokol (PPP) - WAN

Semester 4, Modul 3

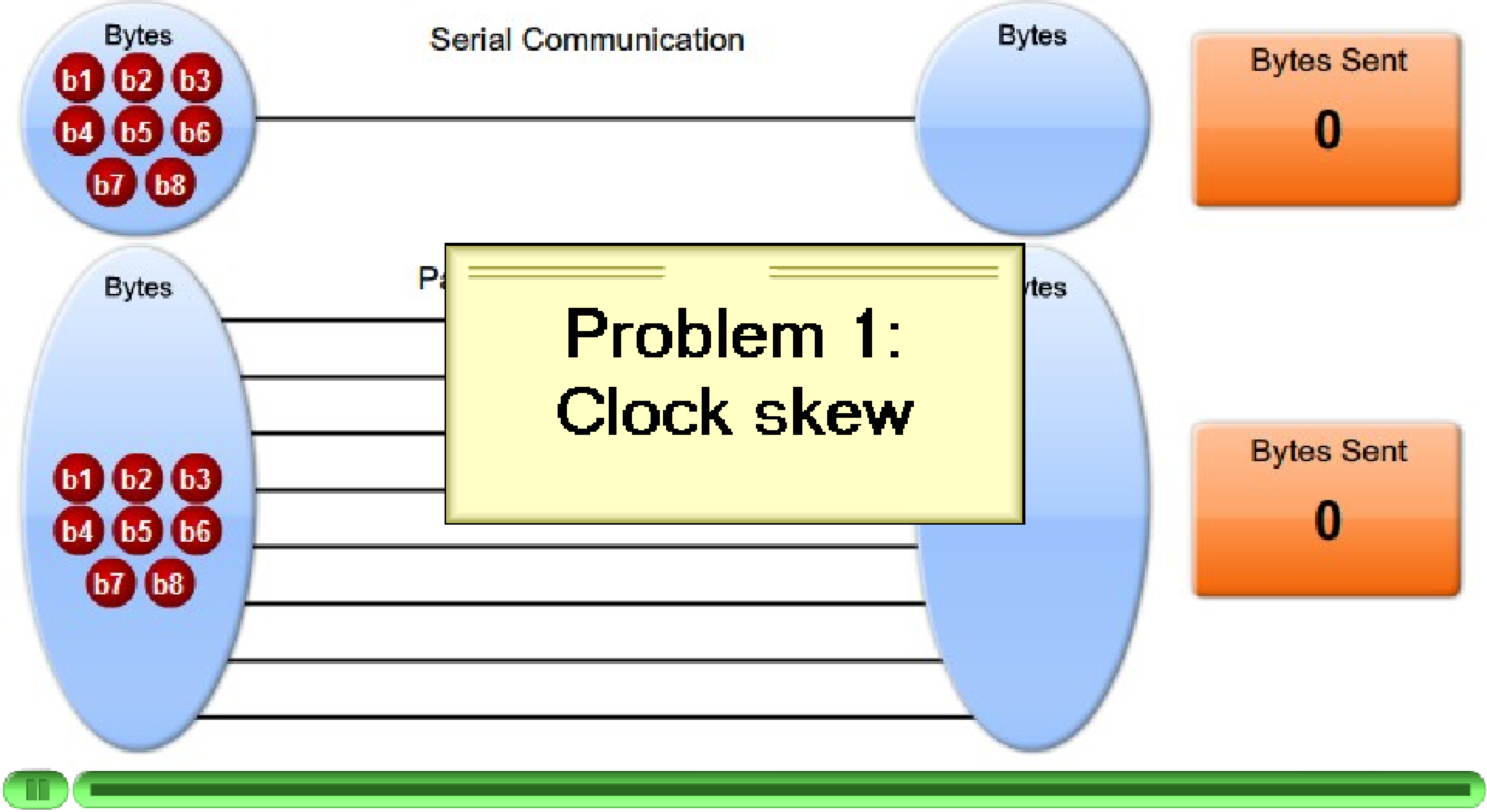
Sériová komunikácia

Sériová vs. Paralélna komunikácia



Sériová komunikácia

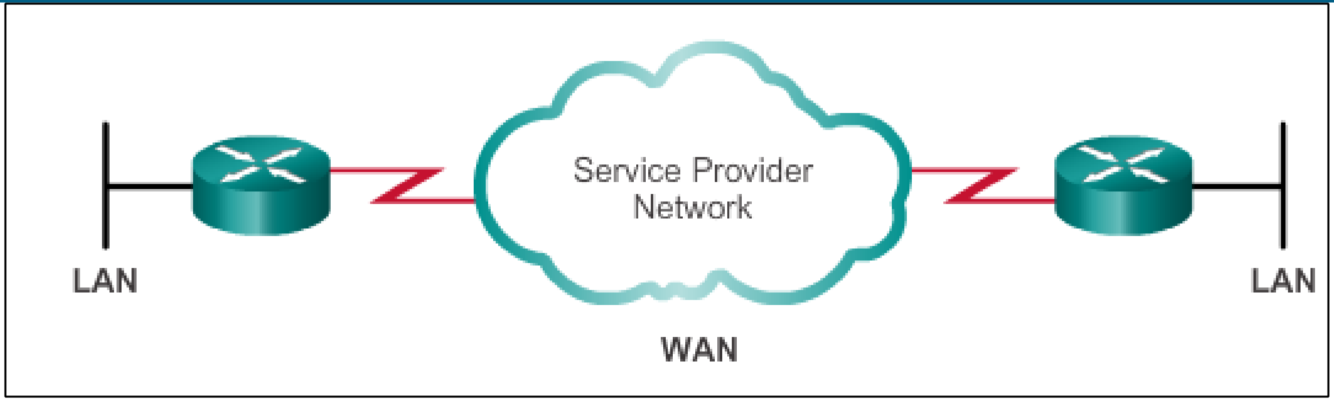
Sériová vs. Paralélna komunikácia - Problémy

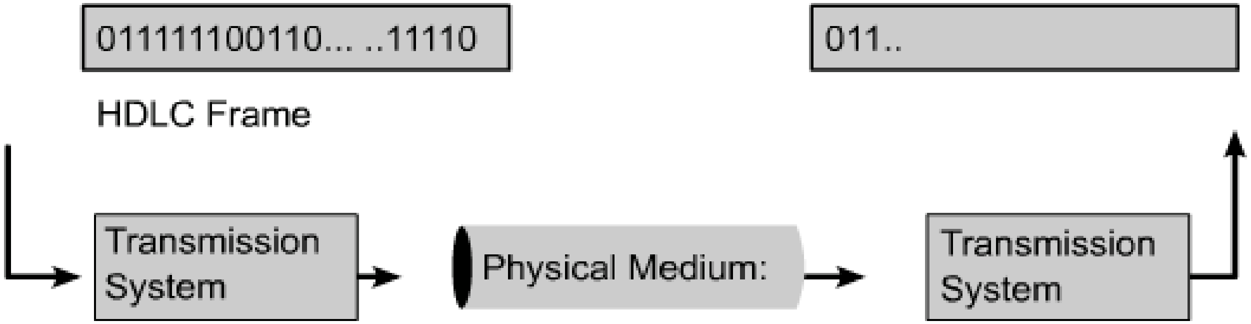


Problem 1:
Clock skew

Sériová komunikácia

WAN komunikácia



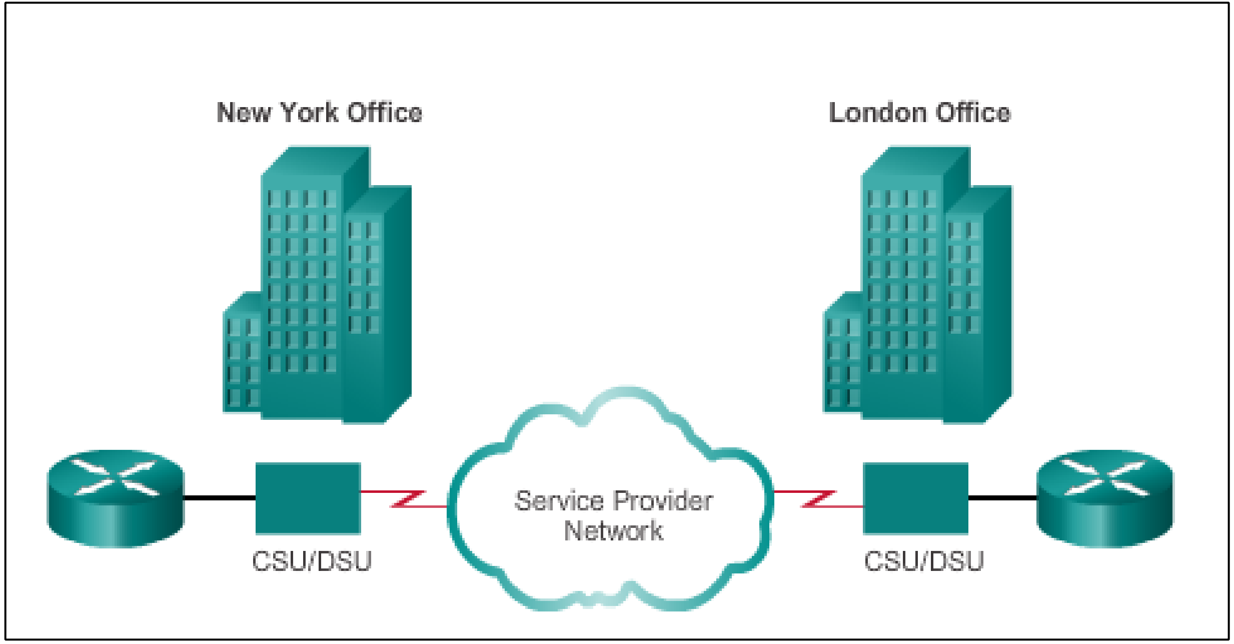


- WAN
  - Vzdialený Point-to-point prepoj medzi LAN
  - Typicky používa sériovú komunikáciu, nie paralélnu
    - Lacnejšie média, odpadá problém so synchronizáciou
    - Médium má dlhší dosah, nakoľko odpadá CrossTalk
  - Na WAN linke sú dáta zapuzdrené odosielajúcim smerovačom
    - Prijímajúci smerovač použije rovnaký Wan protokol na odpuzdrené
- Príklady
  - RS-232, RS/422/423, V.35, HSSI

Sériová komunikácia

Point-to-Point komunikačné WAN linky

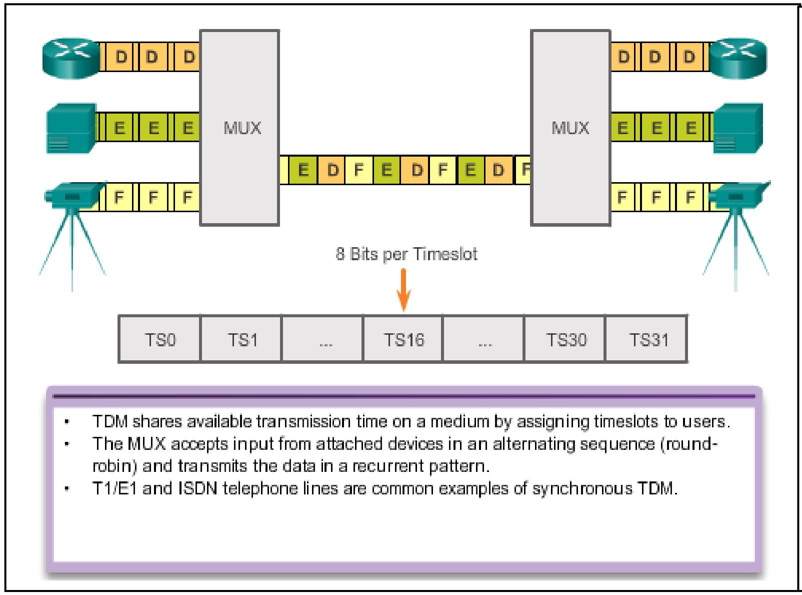
- Point-to-point linky
  - Prepájajú geograficky vzdialené oblasti
  - Typicky nie sú vlastnené danou firmou ale prenajímané
  - Používateľovi ponúkajú celú svoju kapacitu na dobu prenájmu (leased-lines)
  - Preto sú typicky o dosť drahšie ako zdieľané služby



Sériová komunikácia

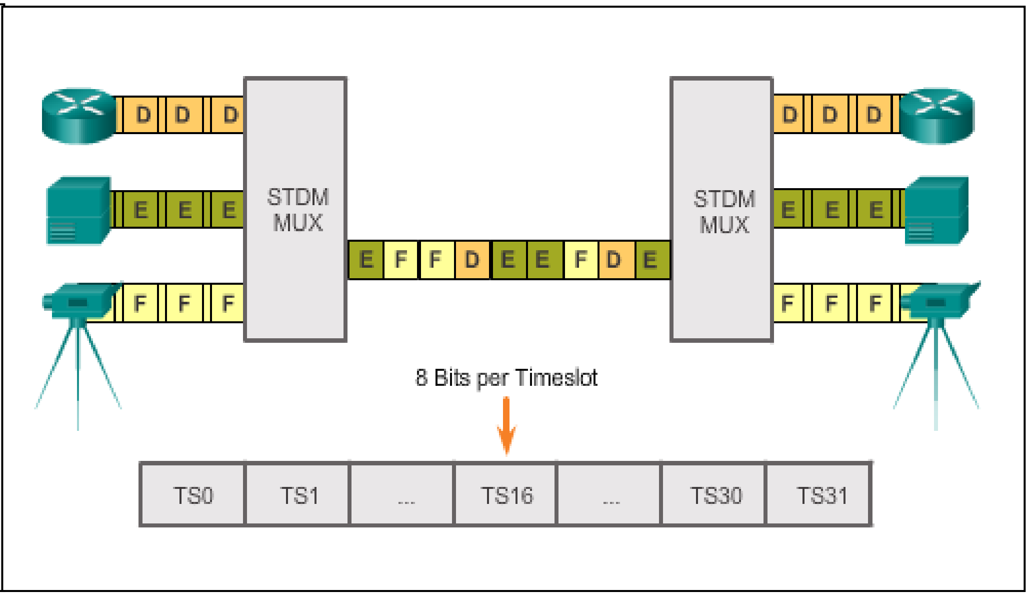
Riešenia

TDM

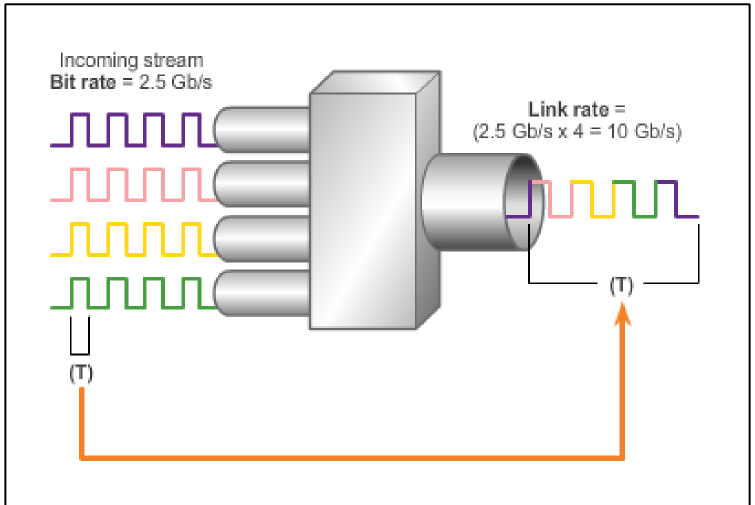


- TDM shares available transmission time on a medium by assigning timeslots to users.
- The MUX accepts input from attached devices in an alternating sequence (round-robin) and transmits the data in a recurrent pattern.
- T1/E1 and ISDN telephone lines are common examples of synchronous TDM.

Štatistický TDM

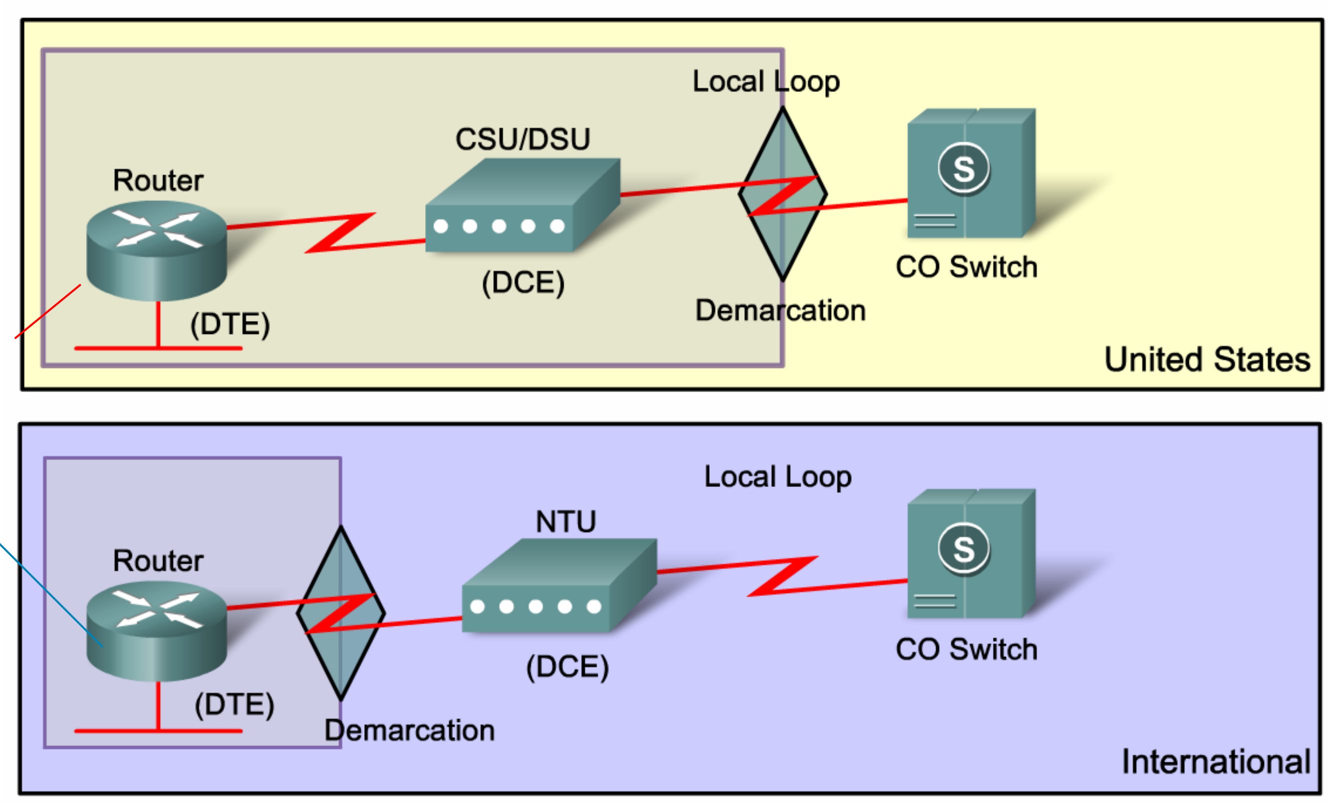


Synchronous Optical Networking (SONET) or Synchronous Digital Hierarchy (SDH)



Sériová komunikácia

Demarcation Point (Demarc)

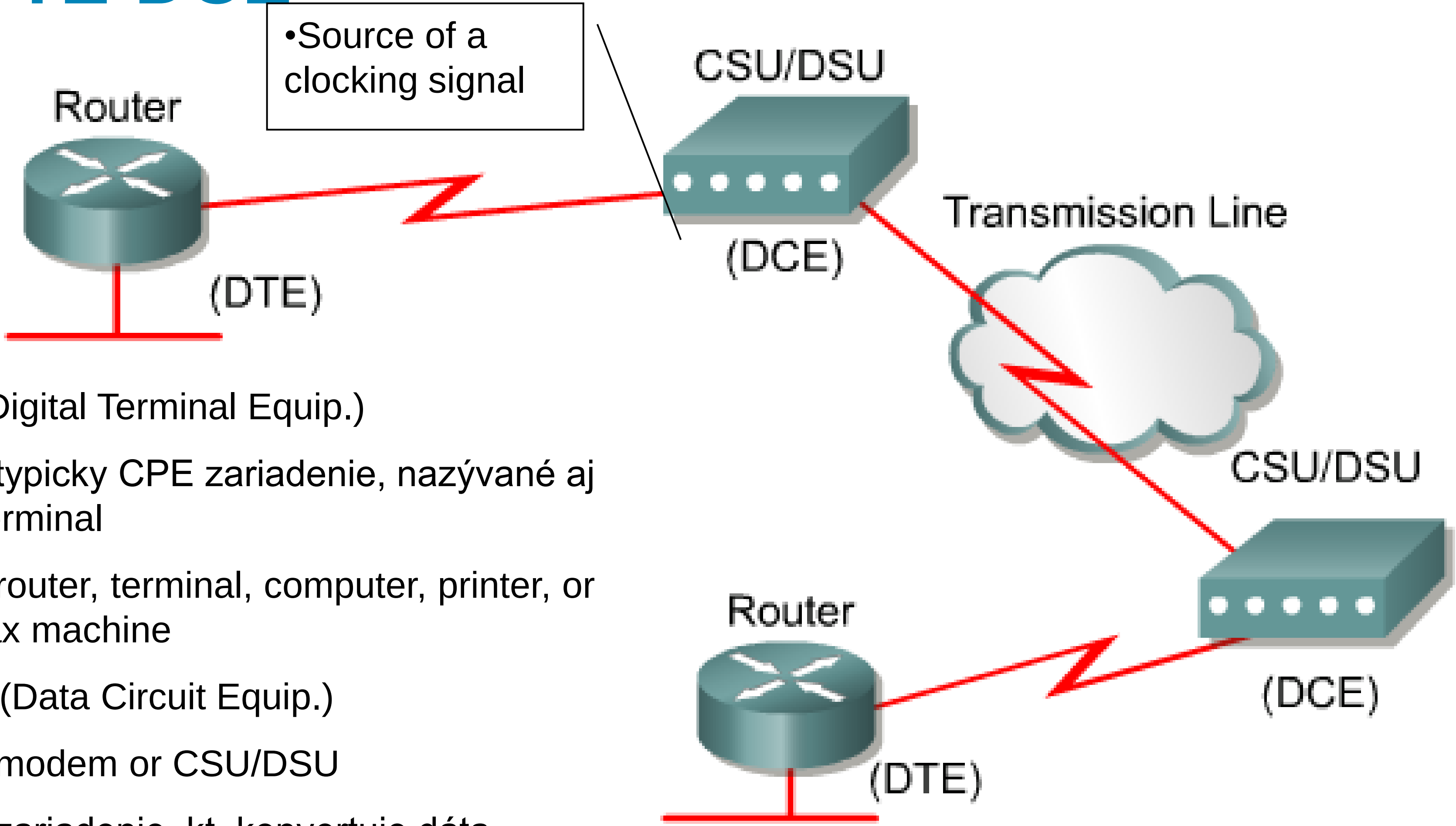


CPE (Customer Premises Equipment)

- Bod v sieti v ktorom končí zodpovednosť poskytovateľa služby.
- Určuje rozhranie medzi zariadením zákazníka (Customer Premises Equipment) a poskytovateľom

Sériová komunikácia

DTE-DCE



•Source of a clocking signal

DTE (Digital Terminal Equip.)

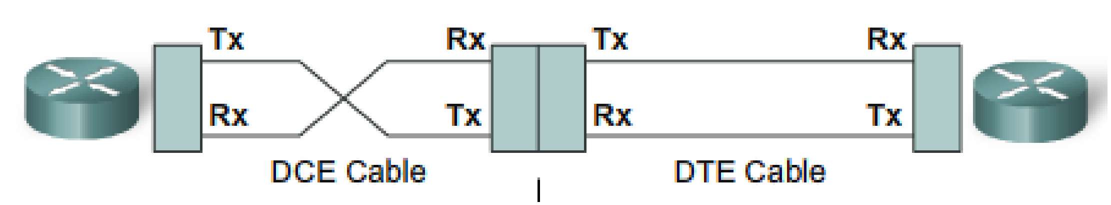
- typicky CPE zariadenie, nazývané aj terminal
- router, terminal, computer, printer, or fax machine

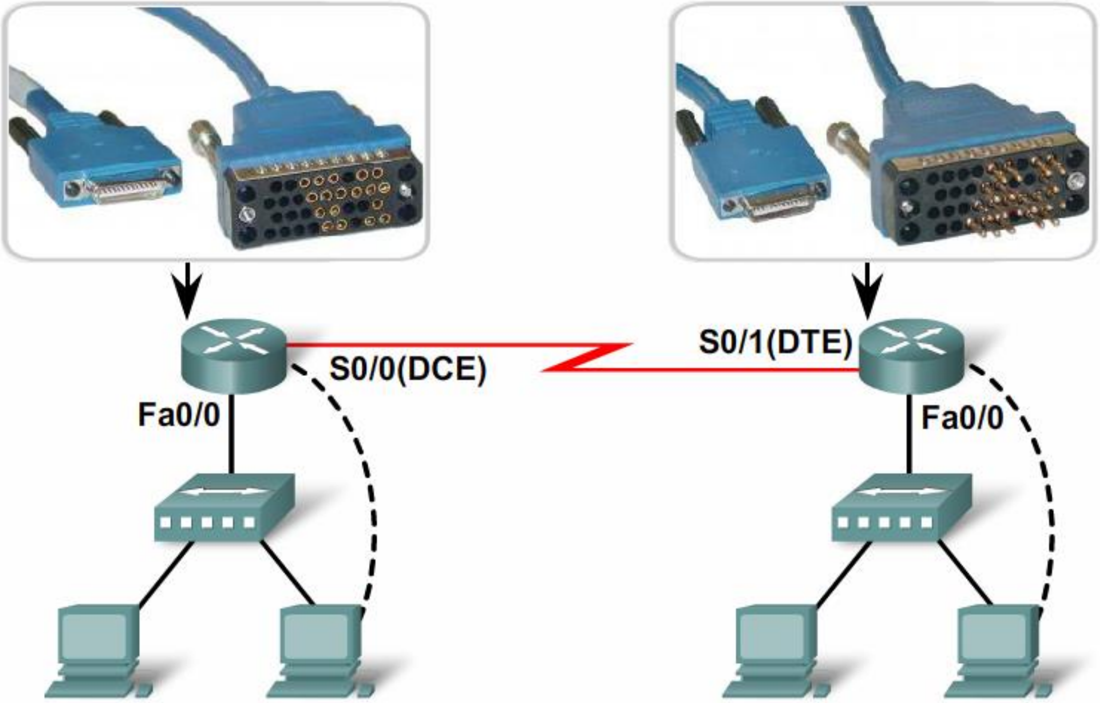
- DCE (Data Circuit Equip.)
  - modem or CSU/DSU
  - zariadenie, kt. konvertuje dáta odosielané z DTE do formy vhodnej pre prenos cez WAN prenosové prostriedky poskytovaeľa. ink.

Sériová komunikácia

DTE a DCE – zapojenie v labe (back to back)

Null modem





Sériová komunikácia

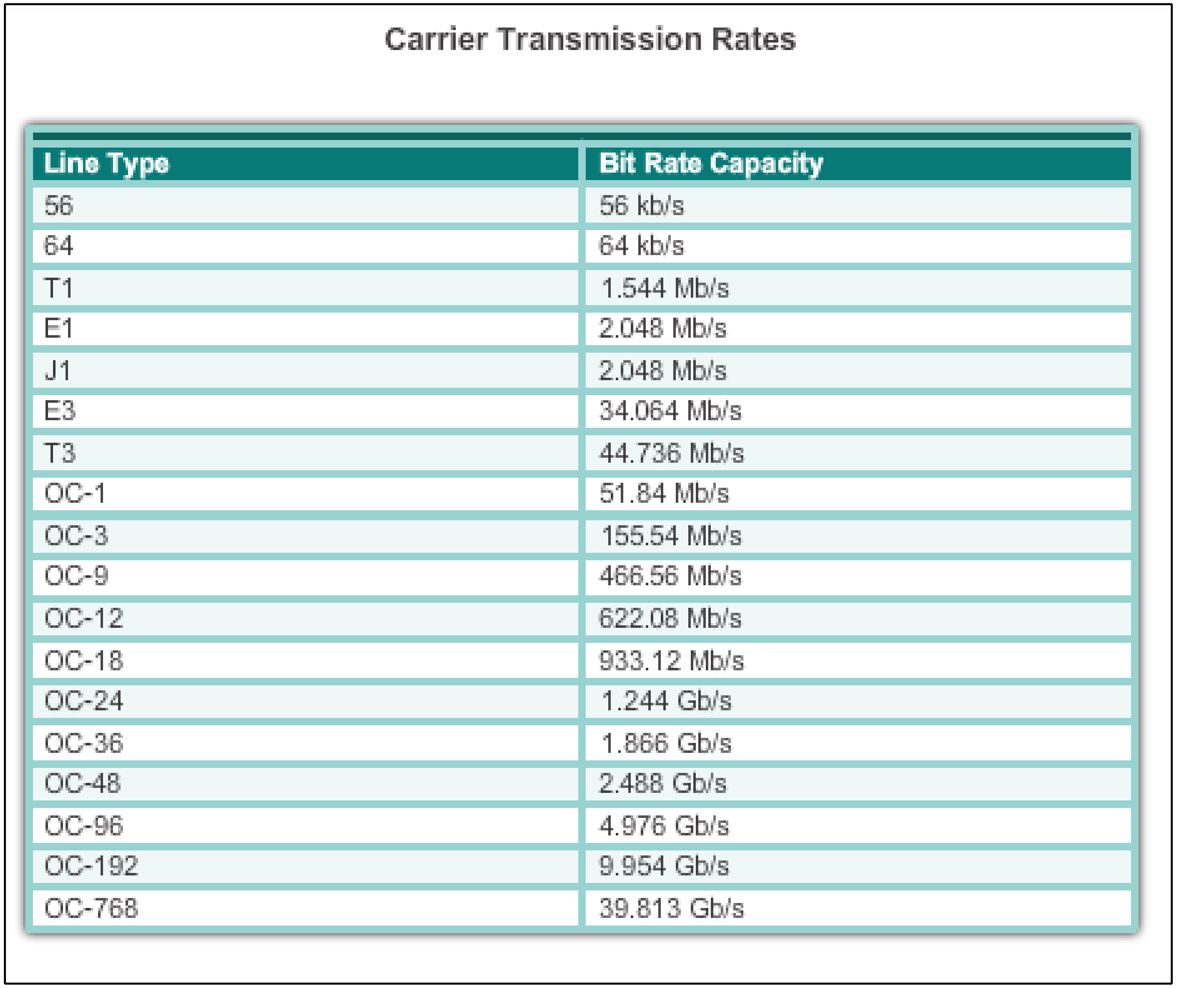
DTE-DCE

- Synchrónne sériové linky musia mať clock
  - Zvyčajne poskytuje DCE zariadenie
- Ak prepápájam dve DTE zariadenia (napr. routre v labe) cez synchrónne rozhranie
  - Jeden musí byť zdrojom hodin. taktu
  - Default je router DTE zariadenie
  - Musím zmeniť konfiguráciou na DCE
    - Podľa typu pripojeného kábla
    - `Clock-rate 64000`

Sériová komunikácia

Šírka pásma a jej značenie

Šírka pásma odkazuje na rýchlosť prenosu dát cez danú linku



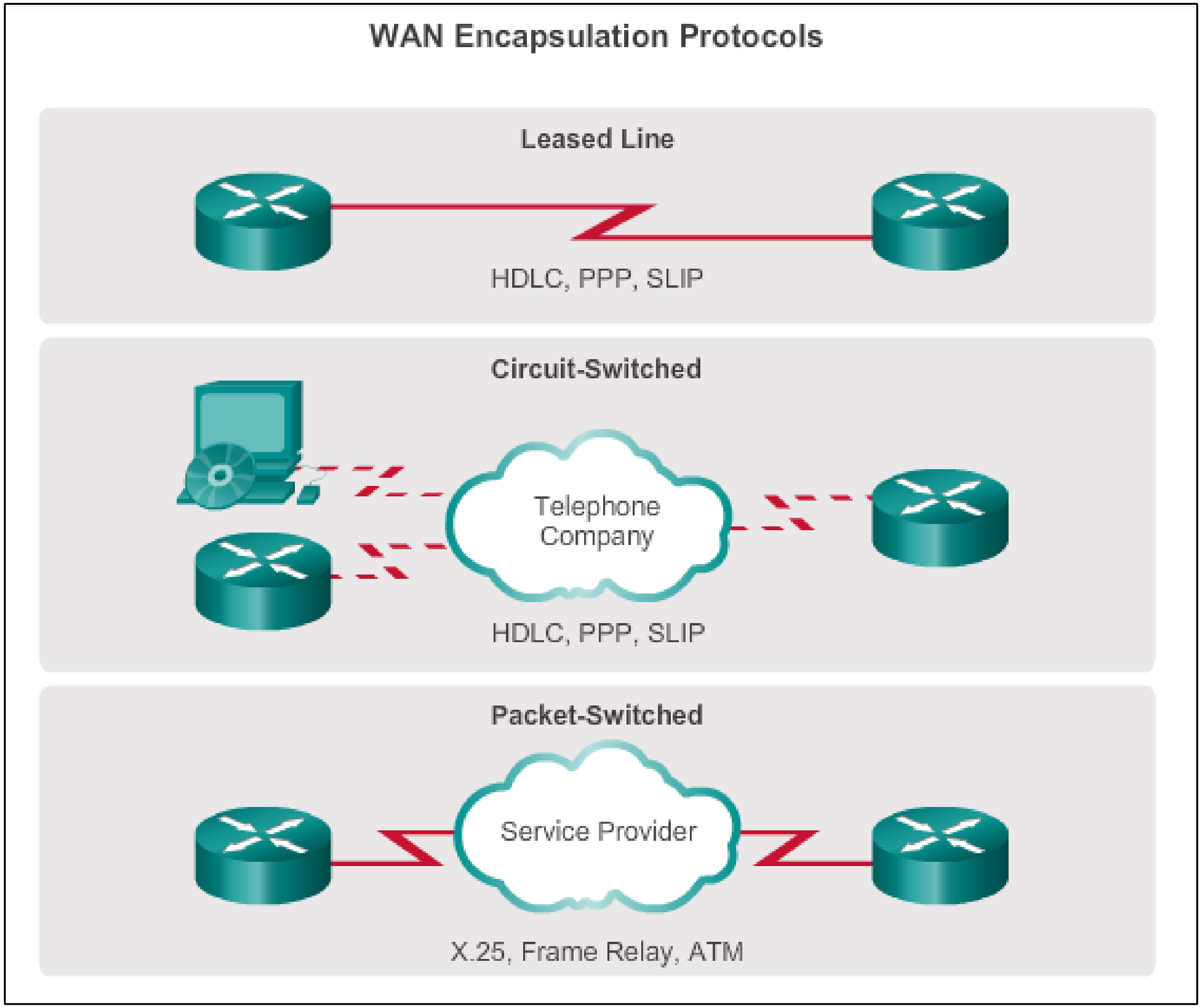
Carrier Transmission Rates

Line Type	Bit Rate Capacity
56	56 kb/s
64	64 kb/s
T1	1.544 Mb/s
E1	2.048 Mb/s
J1	2.048 Mb/s
E3	34.064 Mb/s
T3	44.736 Mb/s
OC-1	51.84 Mb/s
OC-3	155.54 Mb/s
OC-9	466.56 Mb/s
OC-12	622.08 Mb/s
OC-18	933.12 Mb/s
OC-24	1.244 Gb/s
OC-36	1.866 Gb/s
OC-48	2.488 Gb/s
OC-96	4.976 Gb/s
OC-192	9.954 Gb/s
OC-768	39.813 Gb/s

High Level Data Link (HDLC) protokol

WAN linky

L2 WAN komunikácia



WAN linky

L2 komunikácia cez sériové linky

- Bolo vyvinutých viacero protokolov
  - HDLC, PPP, SLIP, FR, apod.
- **High-level data link control** (HDLC) protokol
  - Definovaný ISO 9 (ISO3239)
  - Bitovo orientovaný data link protokol
  - Point-to-point protokol
    - Bezchybový
  - Full duplex
  - Definuje ako enkapsulovať dáta na synchrónnych seriových linkách
    - Využíva L1 Clocking
  - Umožňuje riadenie toku (flow control) cez potvrdzovanie a systém Okna

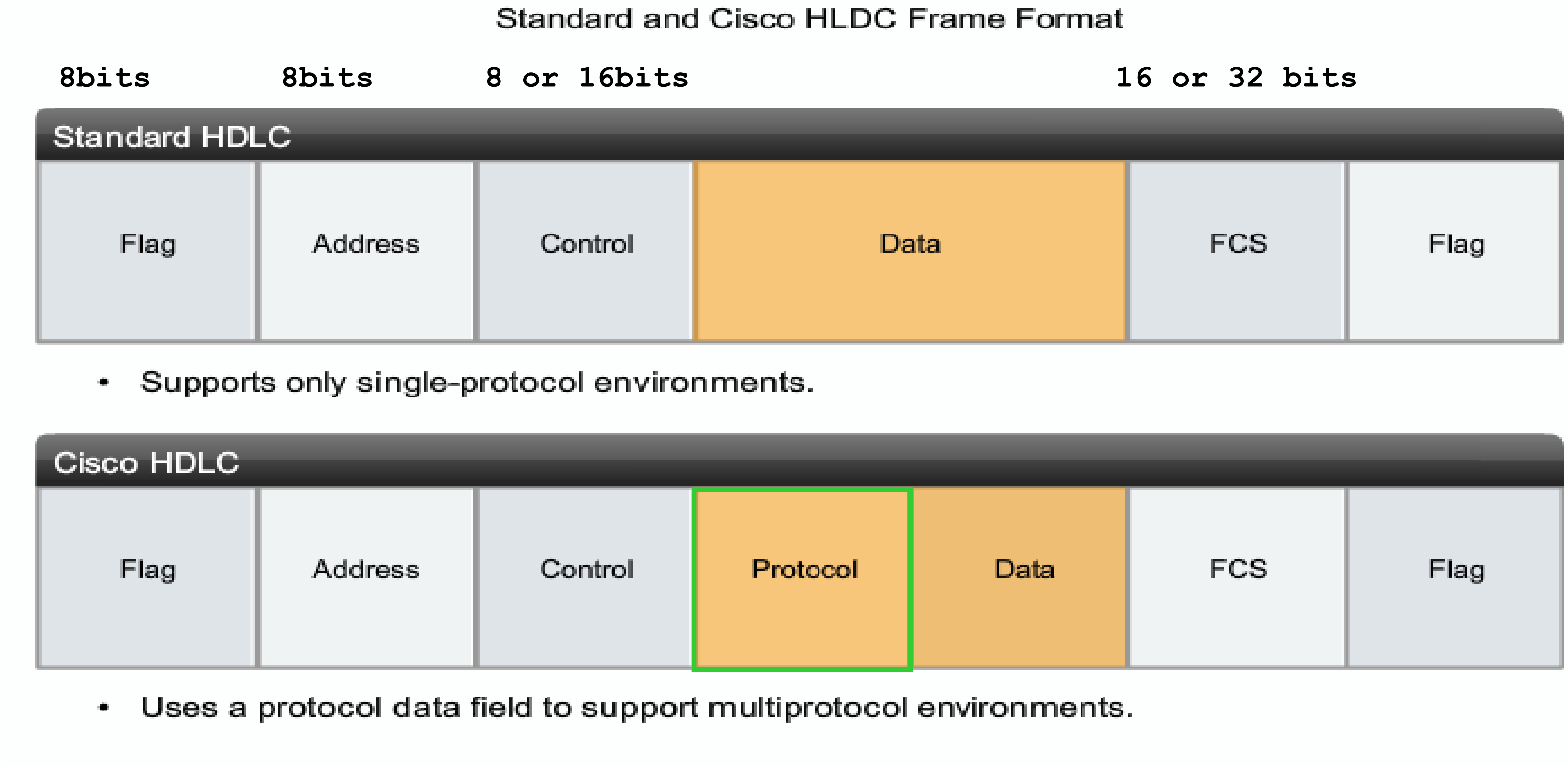
HDLC protokol

HDLC verzie

- ***Standard HDLC*** (ISO štandard)
    - Nepodporuje prenos viacerých L3 protokolov cez L2 linku
        - Nemá spôsob ako by príjemcovi naznačil, čo je nesené v HDLC rámci
- ***Cisco HDLC*** (cHDLC)
    - Proprietárna Cisco verzia HDLC.
    - Rámec nesie proprietárne pole 'type' alebo tiež tzv. protocol pole.
        - Pole umožňuje prenášať dáta viacerých L3 protokolov cez tú istp L2 linku.
    - cHDCL je spúšťaná ako default enkapsulácia na sériových rozhraniach.

HDLC protokol

HDLC verzie – formát rámca



Standard and Cisco HLDC Frame Format

8bits 8bits 8 or 16bits 16 or 32 bits

Standard HDLC

Flag	Address	Control	Data	FCS	Flag

- Supports only single-protocol environments.

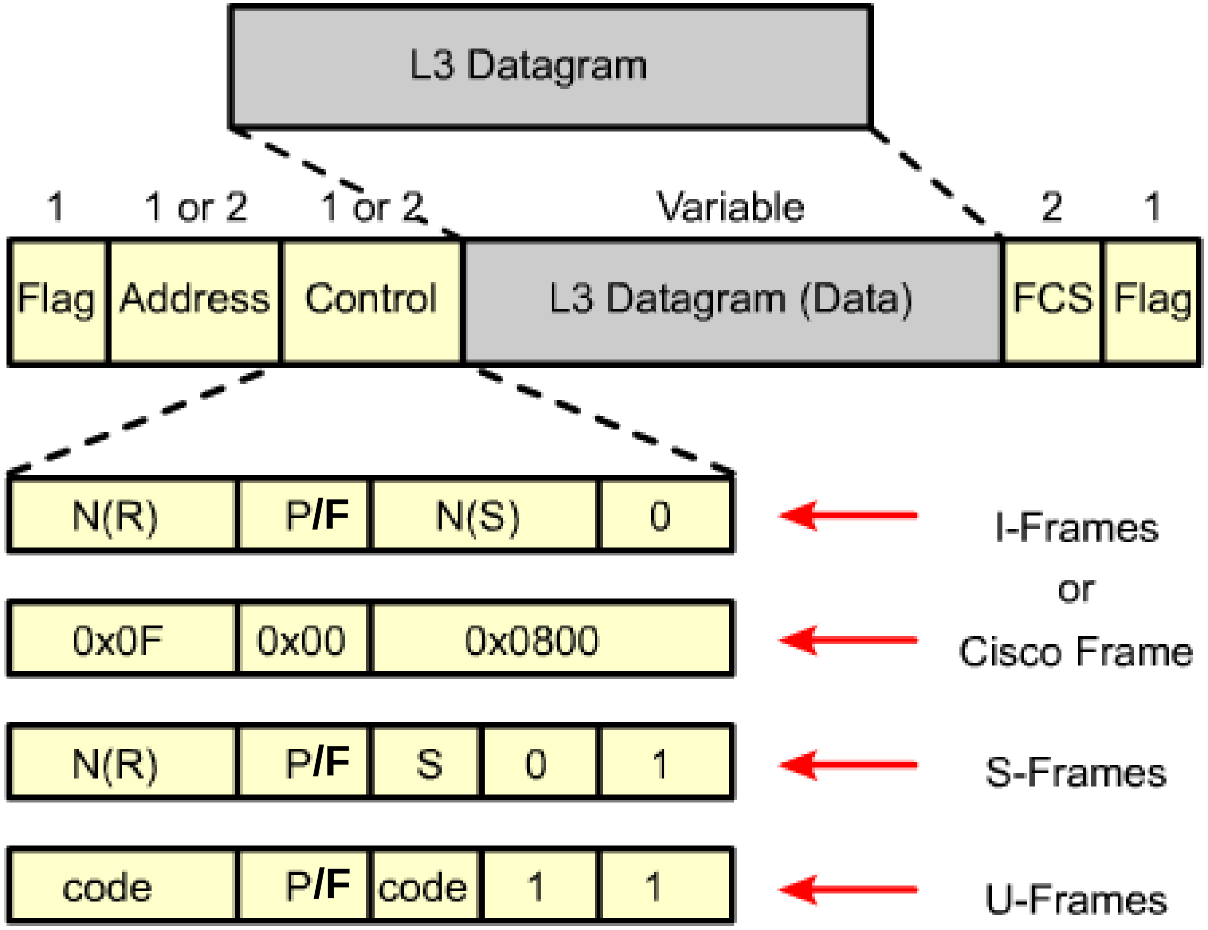
Cisco HDLC

Flag	Address	Control	Protocol	Data	FCS	Flag

- Uses a protocol data field to support multiprotocol environments.

Opening Flag, 8 bits [01111110], [7E Hex]
Address, 8 bits [môže byť viac]
Control, 8 bits, or 16 bits
Data [Payload], Variabilná dĺžka
CRC, 16 bits, or 32 bits
Closing Flag, 8 bits [01111110], [7E hex]

HDLC Typy rámcov



N(R)	P/F	N(S)		0
0x0F	0x00	0x0800		
N(R)	P/F	S	0	1
code	P/F	code	1	1

- **Information frames (I-frames)** – Carry upper layer information and some control info. Additional flow and error control data may be carried on an I-frame.

- **Supervisory frames (S-frames)** – provide error and flow control information. An S-frame can request and suspend transmission, report on status, and acknowledge receipt of I-frames (if no piggybacking).

- **Unnumbered frames (U-frames)** – Provide supplemental link control functions such as connection setup. The code field identifies the U-frame type.

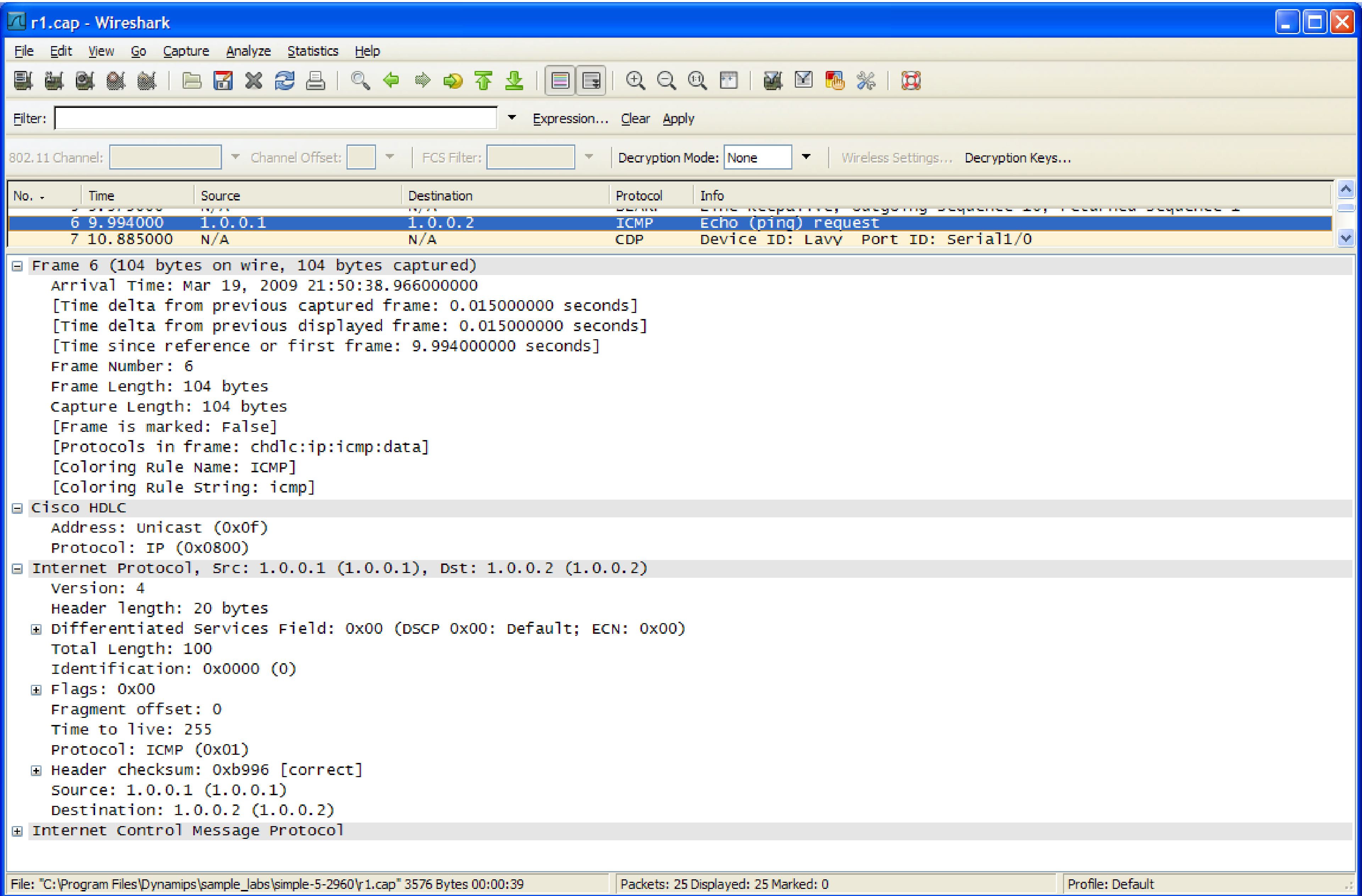
N(R) – receive seq. Numb.

N(S) – send seq. Numb.

Poll/Final

0x00 – 2 bit – indicate S messages (RR-Receive Ready, RNR-Receive Not Ready, REJ-Reject, SREJ-Selective Reject)

Wireshark sniff



Decryption Mode: None

```
No. .  Time        Source     Destination  Protocol  Info
  6 9.994000     1.0.0.1    1.0.0.2      ICMP      Echo (ping) request
  7 10.885000    N/A        N/A          CDP       Device ID: Lavy  Port ID: Serial1/0
```

```
⊟ Frame 6 (104 bytes on wire, 104 bytes captured)
    Arrival Time: Mar 19, 2009 21:50:38.966000000
    [Time delta from previous captured frame: 0.015000000 seconds]
    [Time delta from previous displayed frame: 0.015000000 seconds]
    [Time since reference or first frame: 9.994000000 seconds]
    Frame Number: 6
    Frame Length: 104 bytes
    Capture Length: 104 bytes
    [Frame is marked: False]
    [Protocols in frame: chdlc:ip:icmp:data]
    [Coloring Rule Name: ICMP]
    [Coloring Rule String: icmp]
⊟ Cisco HDLC
    Address: Unicast (0x0f)
    Protocol: IP (0x0800)
⊟ Internet Protocol, Src: 1.0.0.1 (1.0.0.1), Dst: 1.0.0.2 (1.0.0.2)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    Total Length: 100
    Identification: 0x0000 (0)
  ⊞ Flags: 0x00
    Fragment offset: 0
    Time to live: 255
    Protocol: ICMP (0x01)
  ⊞ Header checksum: 0xb996 [correct]
    Source: 1.0.0.1 (1.0.0.1)
    Destination: 1.0.0.2 (1.0.0.2)
⊞ Internet Control Message Protocol
```

File: "C:\Program Files\Dynamips\sample_labs\simple-5-2960\r1.cap" 3576 Bytes 00:00:39 | Packets: 25 Displayed: 25 Marked: 0 | Profile: Default

HDLC protokol

Konfigurácia HDLC enkapsulácie

```
Router(config-if)#encapsulation hdlc
```

- cHDLC je defaultná WAN schéma na sériových rozhraniach
- Voči zariadeniam iných výrobcov použi PPP

Diagnostika sériového rozhrania

```
Router#sh interfaces serial 0/0
Serial0/0 is up, line protocol is up
  Hardware is PowerQUICC Serial
  Internet address is 1.1.1.1/8
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
  Keepalive set (10 sec)
  Last input 00:00:01, output 00:00:01, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/1/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 1158 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     13 packets input, 1488 bytes, 0 no buffer
     Received 13 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     19 packets output, 2508 bytes, 0 underruns
     0 output errors, 0 collisions, 4 interface resets
     0 unknown protocol drops
```

Diagnostika sériového rozhrania

```
Router#sh controllers serial 0/0
Interface Serial0/0
Hardware is PowerQUICC MPC860
DCE 530, clock rate 64000
idb at 0x82561E58, driver data structure at 0x82569574
SCC Registers:
General [GSMR]=0x2:0x00000030, Protocol-specific [PSMR]=0x8
Events [SCCE]=0x0000, Mask [SCCM]=0x001F, Status [SCCS]=0x00
Transmit on Demand [TODR]=0x0, Data Sync [DSR]=0x0
Interrupt Registers:
Config [CICR]=0x00367F80, Pending [CIPR]=0x00000000
Mask   [CIMR]=0x40204000, In-srv  [CISR]=0x00000000
Command register [CR]=0x0
Port A [PADIR]=0x0000, [PAPAR]=0x0000
       [PAODR]=0x0000, [PADAT]=0x0000
Port B [PBDIR]=0x00000, [PBPAR]=0x00000
       [PBODR]=0x00000, [PBDAT]=0x28400
Port C [PCDIR]=0x000, [PCPAR]=0x000
       [PCSO]=0x000,  [PCDAT]=0x000, [PCINT]=0x000
Receive Ring
        rmd(680126B0): status 9000 length 60C address 376DCA4
        rmd(680126B8): status 9000 length 60C address 376D624
        rmd(680126C0): status 9000 length 60C address 376CFA4
        rmd(680126C8): status 9000 length 60C address 376C924
```

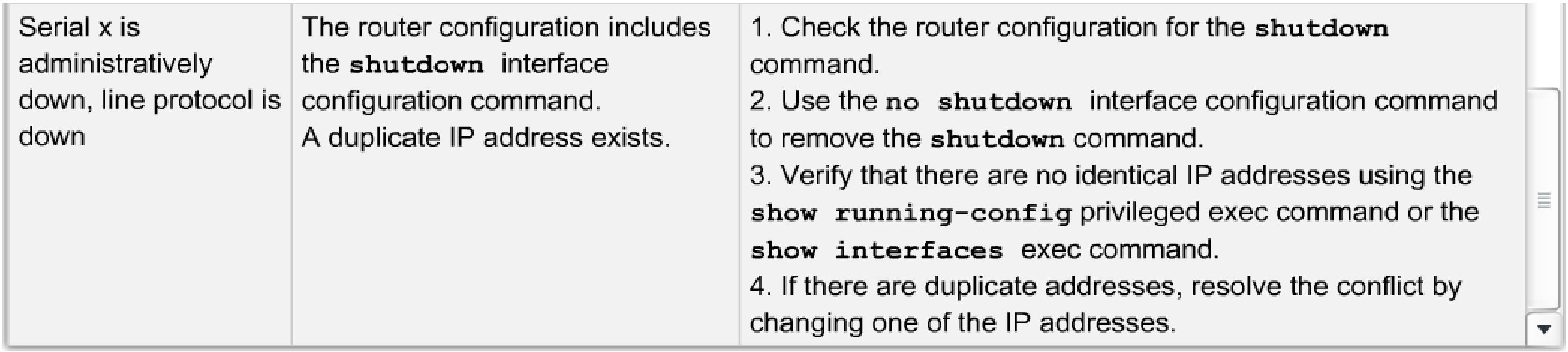
Diagnostika sériového rozhrania

```
Router#sh ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            unassigned      YES unset  administratively down down
Serial0/0                  1.1.1.1         YES manual up                    up
FastEthernet0/1            unassigned      YES unset  administratively down down
Serial0/1                  unassigned      YES unset  administratively down down
```

Diagnostika sériového rozhrania

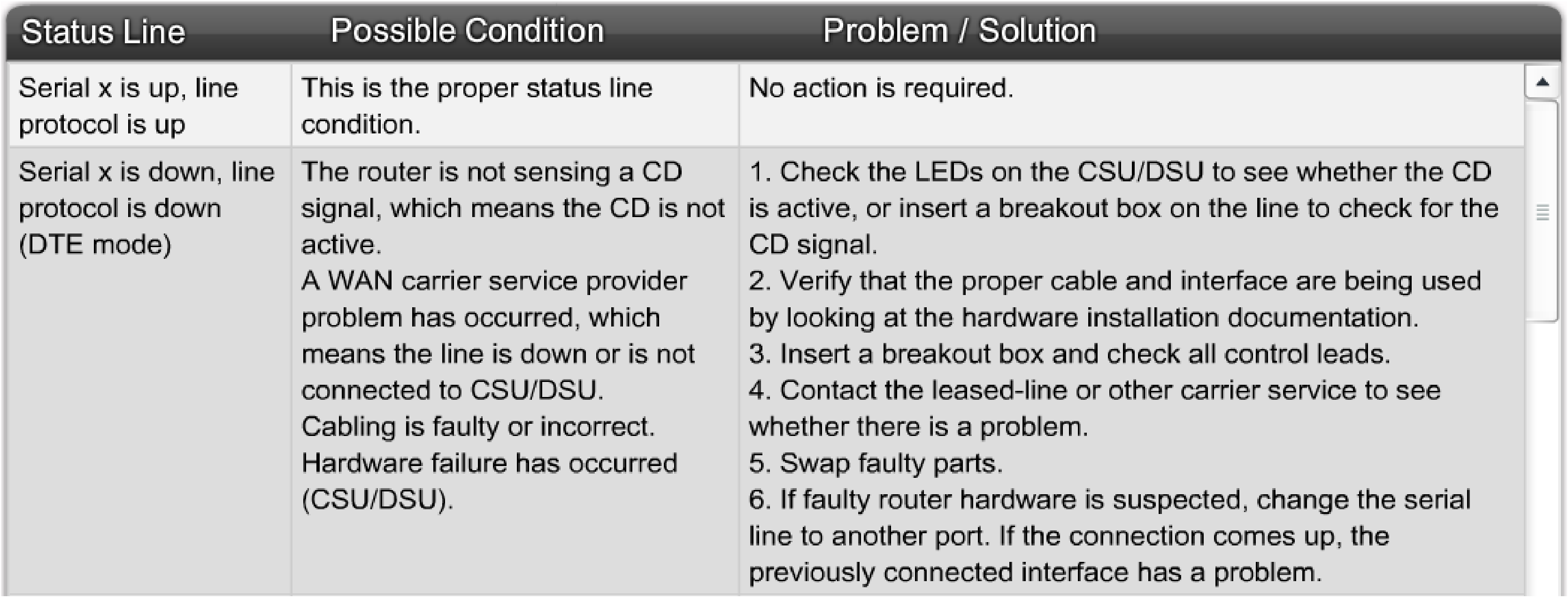
- Možné stavy rozhraní:
  - Serial *x* is down, line protocol is down.
  - Serial *x* is up, line protocol is down.
  - Serial *x* is up, line protocol is up (looped).
  - Serial *x* is up, line protocol is down (disabled).
  - Serial *x* is administratively down, line protocol is down.

show interface serial



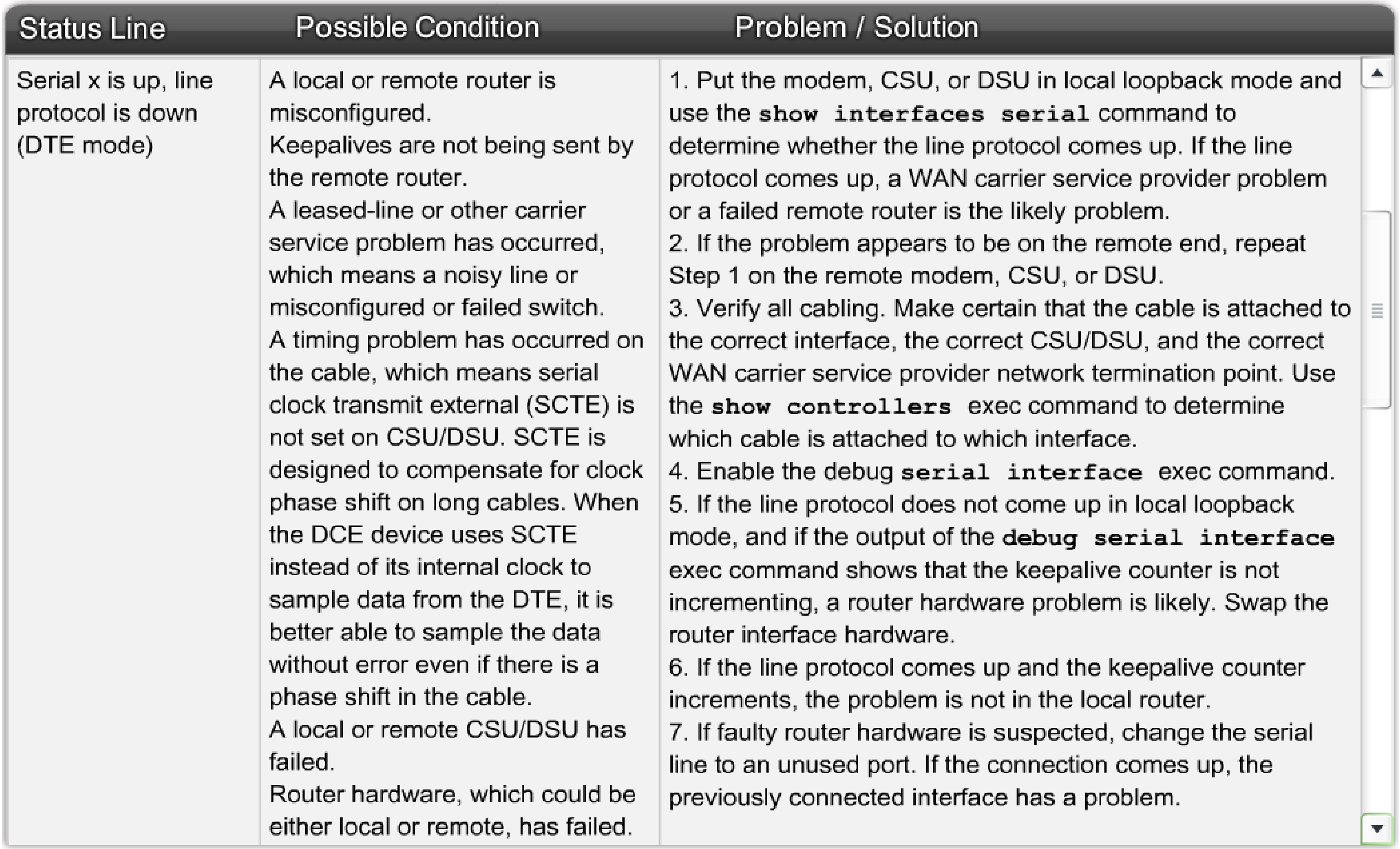
Serial x is administratively down, line protocol is down	The router configuration includes the **shutdown** interface configuration command. A duplicate IP address exists.	1. Check the router configuration for the **shutdown** command. 2. Use the **no shutdown** interface configuration command to remove the **shutdown** command. 3. Verify that there are no identical IP addresses using the **show running-config** privileged exec command or the **show interfaces** exec command. 4. If there are duplicate addresses, resolve the conflict by changing one of the IP addresses.

show interface serial



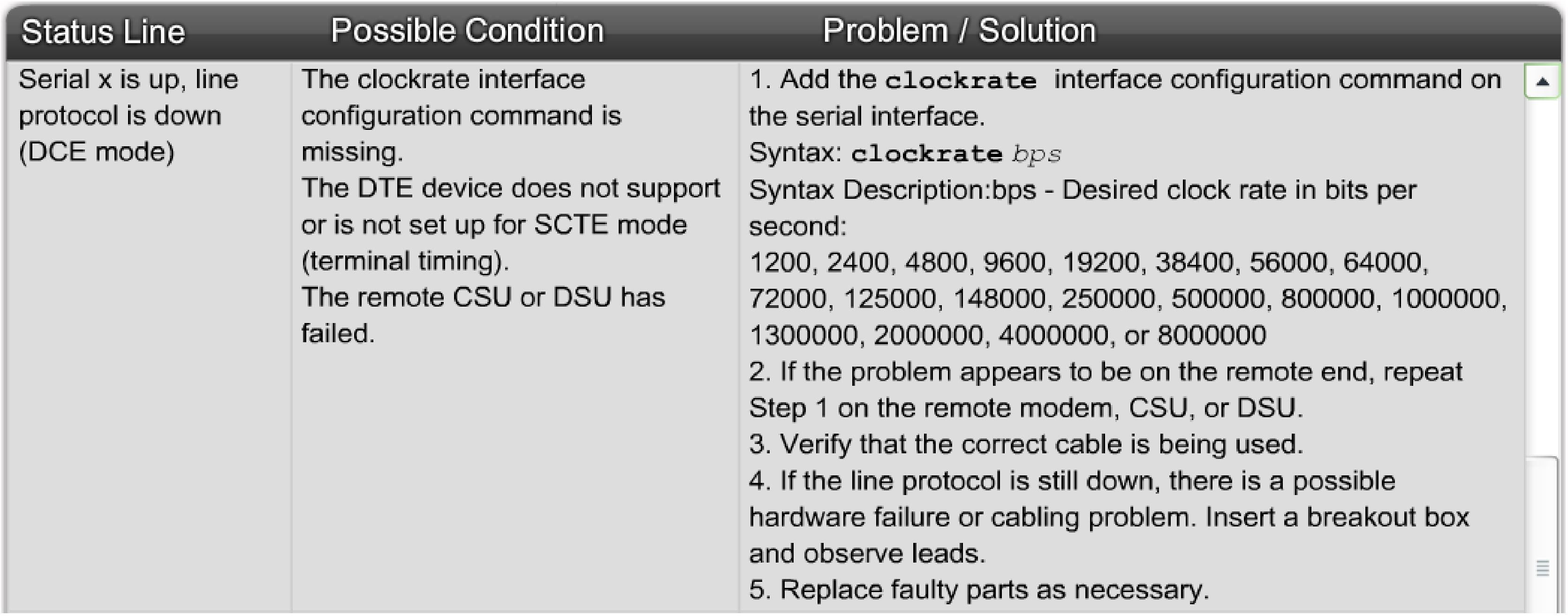
Status Line	Possible Condition	Problem / Solution
Serial x is up, line protocol is up	This is the proper status line condition.	No action is required.
Serial x is down, line protocol is down (DTE mode)	The router is not sensing a CD signal, which means the CD is not active. A WAN carrier service provider problem has occurred, which means the line is down or is not connected to CSU/DSU. Cabling is faulty or incorrect. Hardware failure has occurred (CSU/DSU).	1. Check the LEDs on the CSU/DSU to see whether the CD is active, or insert a breakout box on the line to check for the CD signal. 2. Verify that the proper cable and interface are being used by looking at the hardware installation documentation. 3. Insert a breakout box and check all control leads. 4. Contact the leased-line or other carrier service to see whether there is a problem. 5. Swap faulty parts. 6. If faulty router hardware is suspected, change the serial line to another port. If the connection comes up, the previously connected interface has a problem.

show interface serial



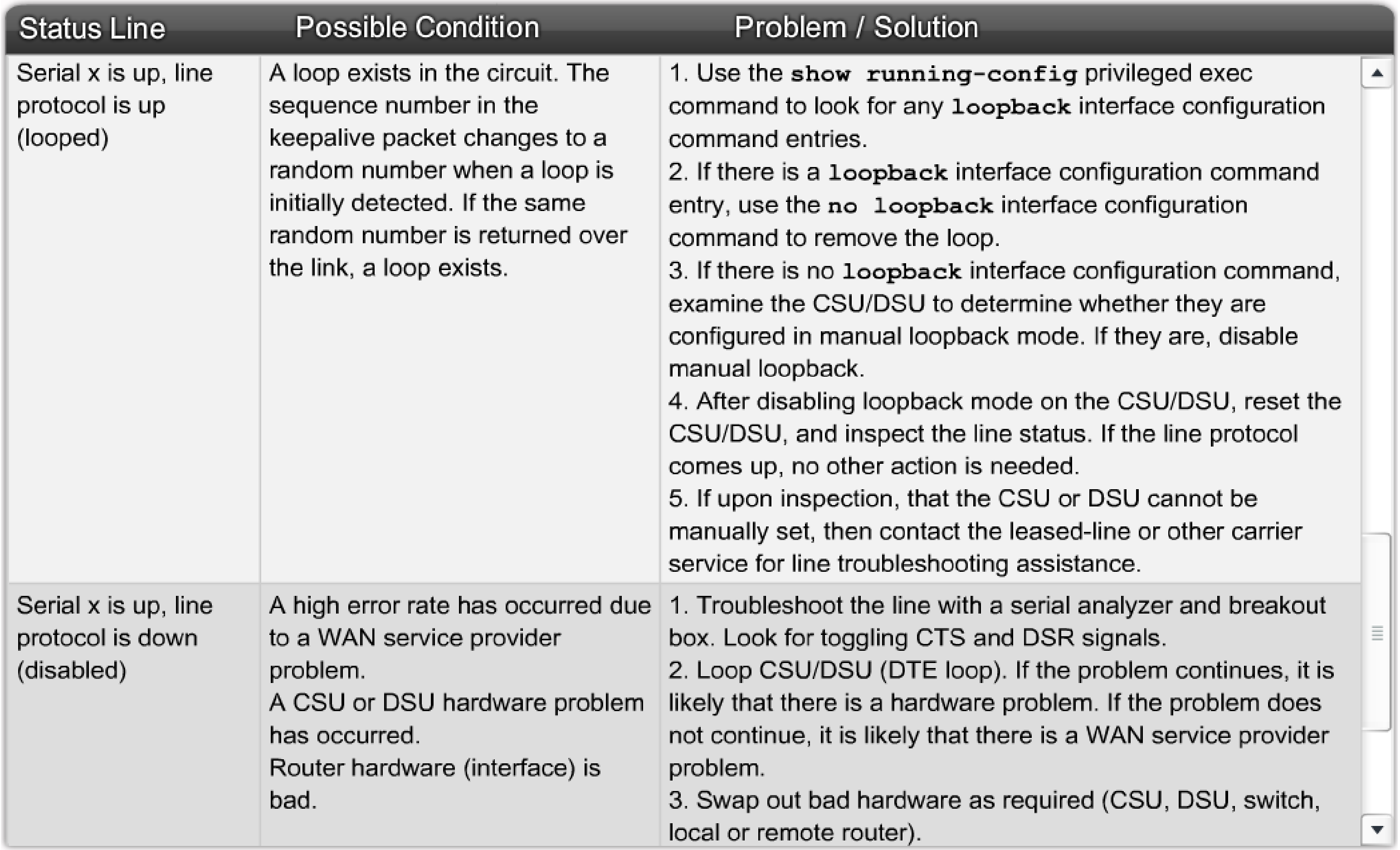
Status Line	Possible Condition	Problem / Solution
Serial x is up, line protocol is down (DTE mode)	A local or remote router is misconfigured. Keepalives are not being sent by the remote router. A leased-line or other carrier service problem has occurred, which means a noisy line or misconfigured or failed switch. A timing problem has occurred on the cable, which means serial clock transmit external (SCTE) is not set on CSU/DSU. SCTE is designed to compensate for clock phase shift on long cables. When the DCE device uses SCTE instead of its internal clock to sample data from the DTE, it is better able to sample the data without error even if there is a phase shift in the cable. A local or remote CSU/DSU has failed. Router hardware, which could be either local or remote, has failed.	1. Put the modem, CSU, or DSU in local loopback mode and use the **show interfaces serial** command to determine whether the line protocol comes up. If the line protocol comes up, a WAN carrier service provider problem or a failed remote router is the likely problem. 2. If the problem appears to be on the remote end, repeat Step 1 on the remote modem, CSU, or DSU. 3. Verify all cabling. Make certain that the cable is attached to the correct interface, the correct CSU/DSU, and the correct WAN carrier service provider network termination point. Use the **show controllers** exec command to determine which cable is attached to which interface. 4. Enable the debug **serial interface** exec command. 5. If the line protocol does not come up in local loopback mode, and if the output of the **debug serial interface** exec command shows that the keepalive counter is not incrementing, a router hardware problem is likely. Swap the router interface hardware. 6. If the line protocol comes up and the keepalive counter increments, the problem is not in the local router. 7. If faulty router hardware is suspected, change the serial line to an unused port. If the connection comes up, the previously connected interface has a problem.

show interface serial



Status Line	Possible Condition	Problem / Solution
Serial x is up, line protocol is down (DCE mode)	The clockrate interface configuration command is missing. The DTE device does not support or is not set up for SCTE mode (terminal timing). The remote CSU or DSU has failed.	1. Add the **clockrate** interface configuration command on the serial interface. Syntax: **clockrate** *bps* Syntax Description:bps - Desired clock rate in bits per second: 1200, 2400, 4800, 9600, 19200, 38400, 56000, 64000, 72000, 125000, 148000, 250000, 500000, 800000, 1000000, 1300000, 2000000, 4000000, or 8000000 2. If the problem appears to be on the remote end, repeat Step 1 on the remote modem, CSU, or DSU. 3. Verify that the correct cable is being used. 4. If the line protocol is still down, there is a possible hardware failure or cabling problem. Insert a breakout box and observe leads. 5. Replace faulty parts as necessary.

show interface serial



Status Line	Possible Condition	Problem / Solution
Serial x is up, line protocol is up (looped)	A loop exists in the circuit. The sequence number in the keepalive packet changes to a random number when a loop is initially detected. If the same random number is returned over the link, a loop exists.	1. Use the `show running-config` privileged exec command to look for any `loopback` interface configuration command entries. 2. If there is a `loopback` interface configuration command entry, use the `no loopback` interface configuration command to remove the loop. 3. If there is no `loopback` interface configuration command, examine the CSU/DSU to determine whether they are configured in manual loopback mode. If they are, disable manual loopback. 4. After disabling loopback mode on the CSU/DSU, reset the CSU/DSU, and inspect the line status. If the line protocol comes up, no other action is needed. 5. If upon inspection, that the CSU or DSU cannot be manually set, then contact the leased-line or other carrier service for line troubleshooting assistance.
Serial x is up, line protocol is down (disabled)	A high error rate has occurred due to a WAN service provider problem. A CSU or DSU hardware problem has occurred. Router hardware (interface) is bad.	1. Troubleshoot the line with a serial analyzer and breakout box. Look for toggling CTS and DSR signals. 2. Loop CSU/DSU (DTE loop). If the problem continues, it is likely that there is a hardware problem. If the problem does not continue, it is likely that there is a WAN service provider problem. 3. Swap out bad hardware as required (CSU, DSU, switch, local or remote router).

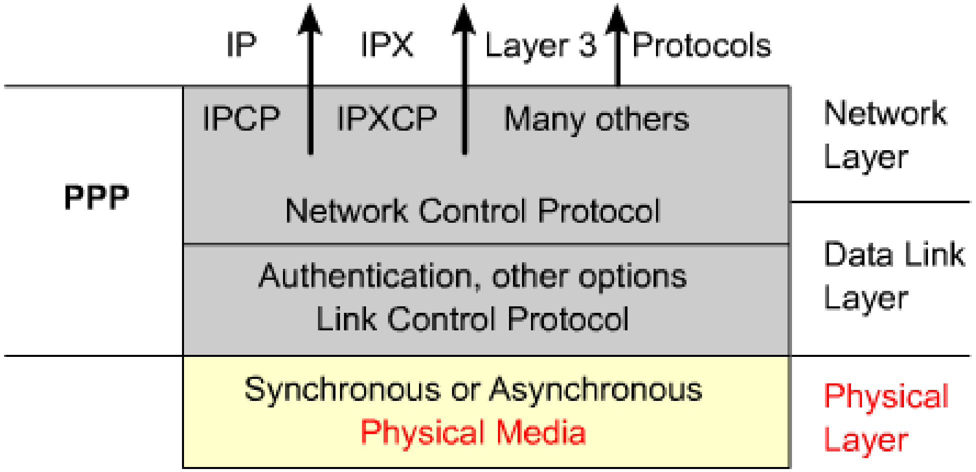
PPP protokol

Point to Point Protocol (PPP)

- Štandardizovaná schéma pre sériovu synchrónnu aj asynchrónnu komunikáciu (RFC1661, 1662)
  - Vhodné do mixovaného prostredia rôznych výrobcov
- PPP komponenty:
  - **HDLC** rámec
    - Definuje enkapsuláciu datagramov cez ppp linku – HDLC U rámec
    - PPP datagram má len tri polia – Protocol, Information, Padding, nie je úplným rámcom
    - PPP datagramy sa preto vkladajú do iného „kontajnera“, veľmi často HDLC U rámce
  - **Link Control Protocol (LCP)**
    - Založenie, konfigurácia, testovanie a ukončenie spojenia
  - **Network Control Protocols (NCPs)**
    - Založenie a konfigurácia L3 protokolov cez ppp linku
      - Internet Protocol Control Protocol, Appletalk Control Protocol, Novell IPX Control Protocol, Cisco Systems Control Protocol, SNA Control Protocol, and Compression Control Protocol.

PPP vrstvená architektúra

Fyzická vrstva



IP IPX Layer 3 Protocols

PPP

IPCP IPXCP Many others

Network Control Protocol

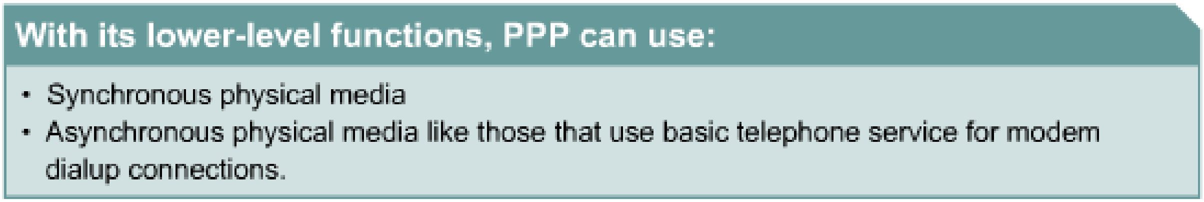
Authentication, other options
Link Control Protocol

Synchronous or Asynchronous
Physical Media

Network Layer

Data Link Layer

Physical Layer



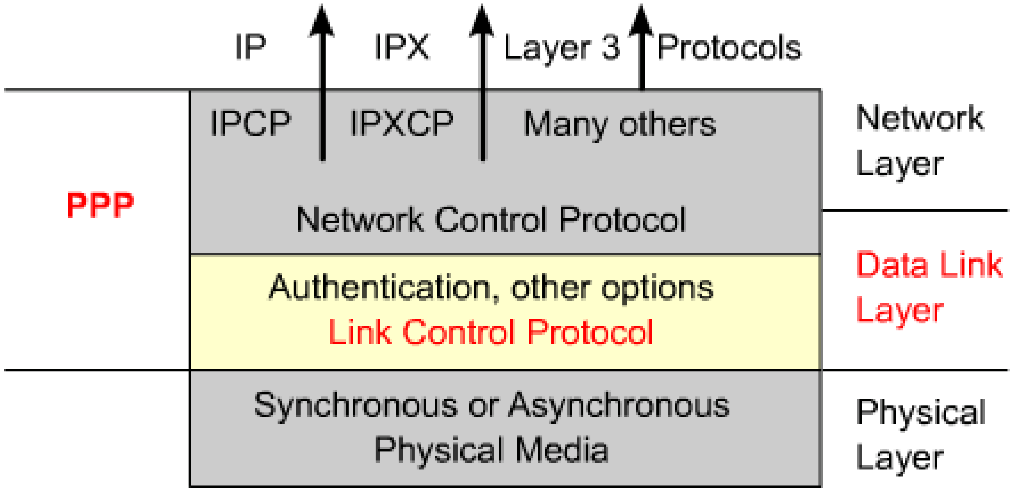
With its lower-level functions, PPP can use:

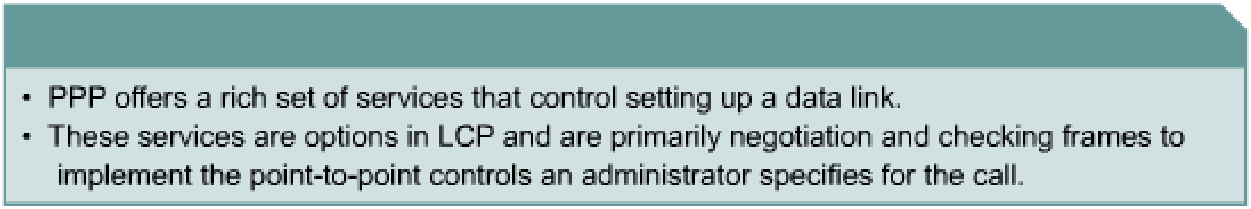
- Synchronous physical media
- Asynchronous physical media like those that use basic telephone service for modem dialup connections.

- PPP pracuje cez:
  - Asynchronous serial
    - Dialup
  - Synchronous serial
    - SONET/SDH
  - High-Speed Serial Interface (HSSI)
  - DSL
    - PPPoE, PPPoA
  - Integrated Services Digital Network (ISDN)

PPP vrstvená architektúra

L2 – Link Control Protocol





- PPP offers a rich set of services that control setting up a data link.
- These services are options in LCP and are primarily negotiation and checking frames to implement the point-to-point controls an administrator specifies for the call.

- LCP
  - Podporný protokol pre základný manažment PPP prepoja
    - Používa sa na založenie, konfiguráciu a testovanie spojenia cez linku
  - Je umiestnený v stacku nad L1 vrstvou

PPP vrstvená architektúra
LCP

- LCP functions
  - **Authentication**
    - Password Authentication Protocol (PAP)
    - Challenge Handshake Authentication Protocol (CHAP).
  - **Compression**
    - increase the effective throughput on PPP connections The protocol decompresses the frame at its destination.
    - Two compression protocols available on Cisco routers:
      - Stacker
      - Predictor.
  - **Error detection** and link quality
    - Allow to identify fault conditions. The Quality and Magic Number options help ensure a reliable, loop-free data link.
  - **Multilink**
  - **PPP Callback**
    - Cisco router can act as a callback client or as a callback server.
    - The client makes the initial call, requests that it be called back, and terminates its initial call.
    - The callback router answers the initial call and makes the return call to the client based on its configuration statements.

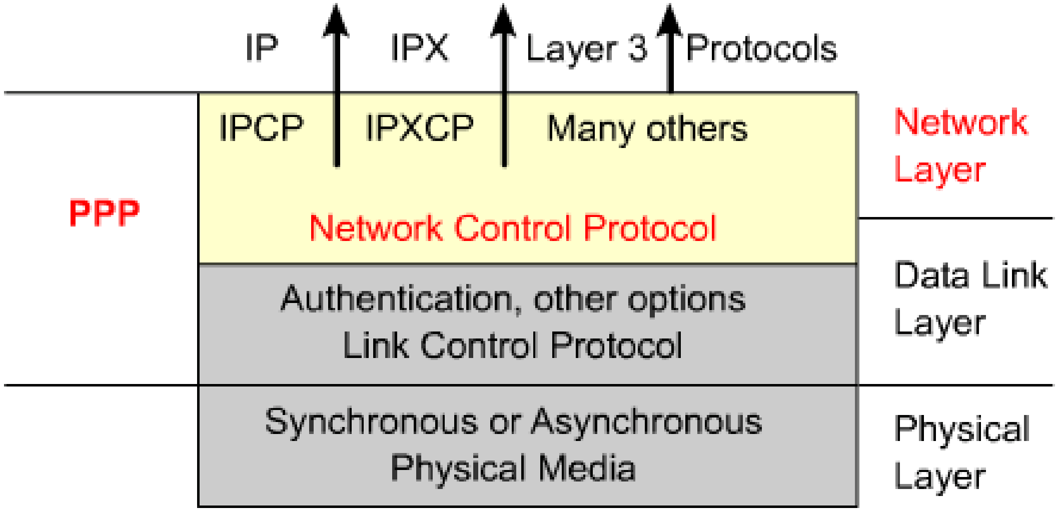
PPP vrstvená architektúra

Ďalšie funkcie LCP

- Iné funkcie LCP
  - Dohoduje veľkosť rámcov
  - Deteguje všeobecné konfiguračné chyby
  - Ukončuje linku
  - Určuje kedy linka pracuje správne a kedy s chybovosťou

PPP vrstvená architektúra

Network Control Protocol



- With its higher-level functions, PPP carries packets from several network-layer protocols in NCPs.
- These are functional fields containing standardized codes to indicate the network-layer protocol type that PPP encapsulates.

- Umožňuje prenos viacerých L3 protokolov cez L2 WAN PPP linku
  - Pre každý L3 protokol existuje samostatný NCP protokol
- Obe PPP strany sa musia pomocou príslušného NCP dohodnúť na konkrétnom L3 protokole a jeho parametroch

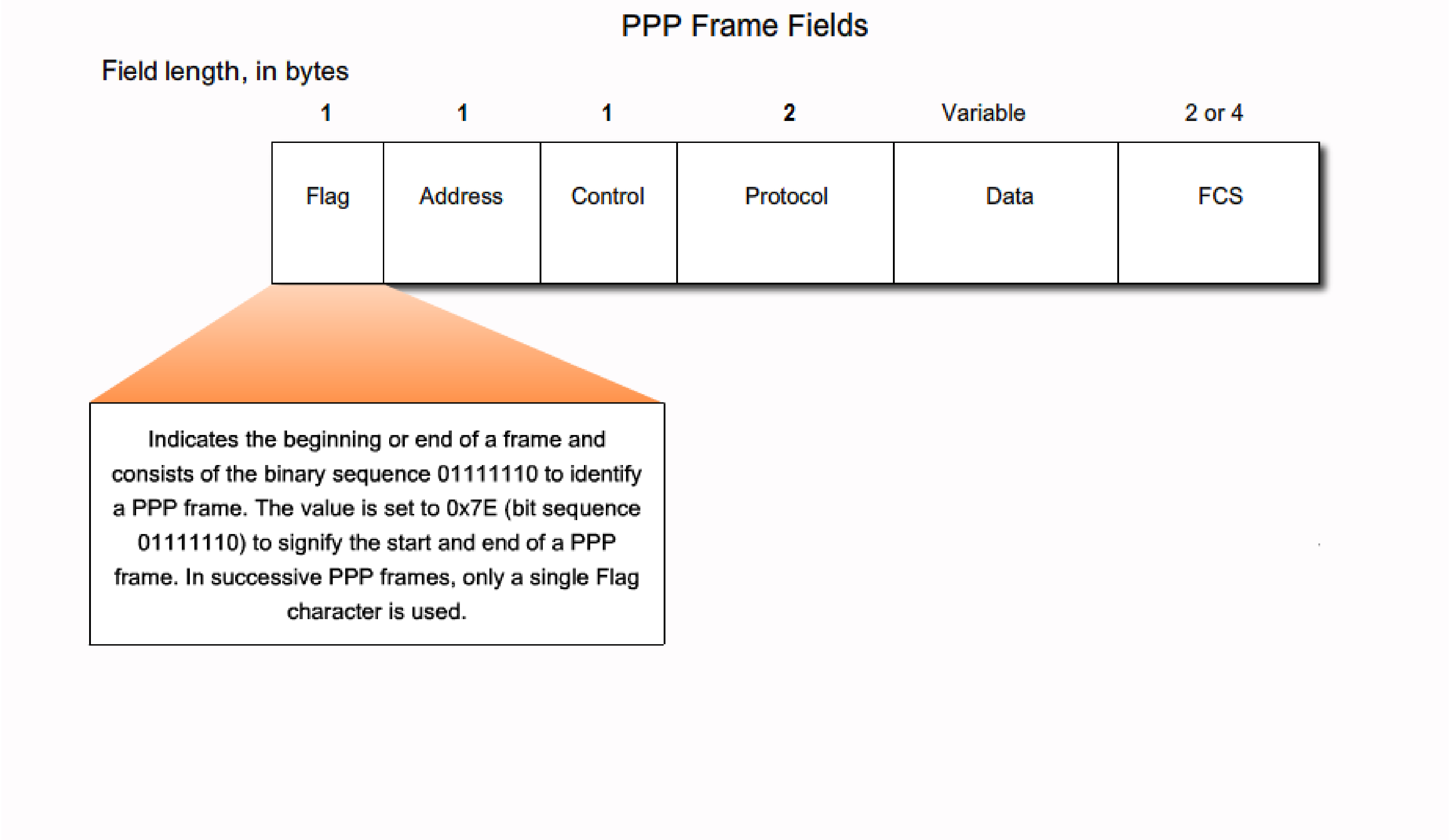
PPP vrstvená architektúra

Architektúra PPP – LCP, NCP

- LCP aj NCPs sú dodatočné správy, ktoré sa prenášajú v PPP rámcoch ako akékoľvek iné pakety
  - Nie sú to ďalšie typy rámcov
  - Hoci sa PPP zobrazuje ako vrstvovo štruktúrovaný (LCP na nižšej vrstve, NCPs na vyššej, L3 protokoly nad NCPs), neznamená to, že by sa L3 vkladali do NCPs a NCPs do LCP
  - Hierarchické vrstvenie v prípade PPP len vyjadruje, ktorý protokol je nižší, ktorý je vyšší, a kedy je možné daný protokol prenášať
    - Všetky nižšie protokoly musia úspešne dospieť do aktívneho stavu
  - Pre NCP protokoly sa zaužívalo názvoslovie <L3>CP, kde <L3> je meno konkrétneho vyššieho protokolu
    - T.j. IPCP pre IP, IP6CP pre IPv6, CDPCP pre CDP, IPXCP pre IPX, ...

PPP protokol

PPP rámec



PPP Frame Fields

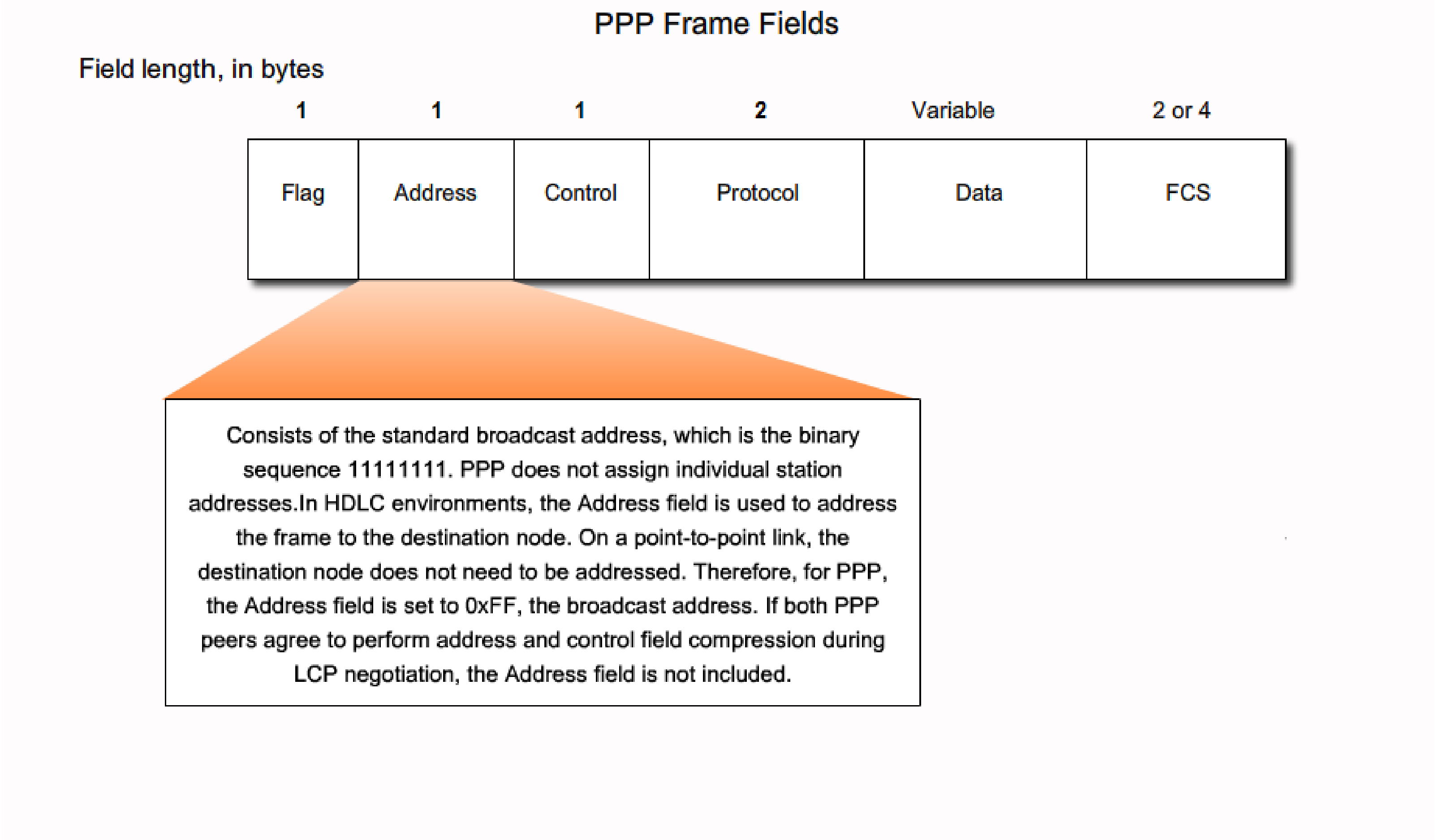
Field length, in bytes

1	1	1	2	Variable	2 or 4
Flag	Address	Control	Protocol	Data	FCS

Indicates the beginning or end of a frame and consists of the binary sequence 01111110 to identify a PPP frame. The value is set to 0x7E (bit sequence 01111110) to signify the start and end of a PPP frame. In successive PPP frames, only a single Flag character is used.

PPP protokol

PPP rámec (2)



PPP Frame Fields

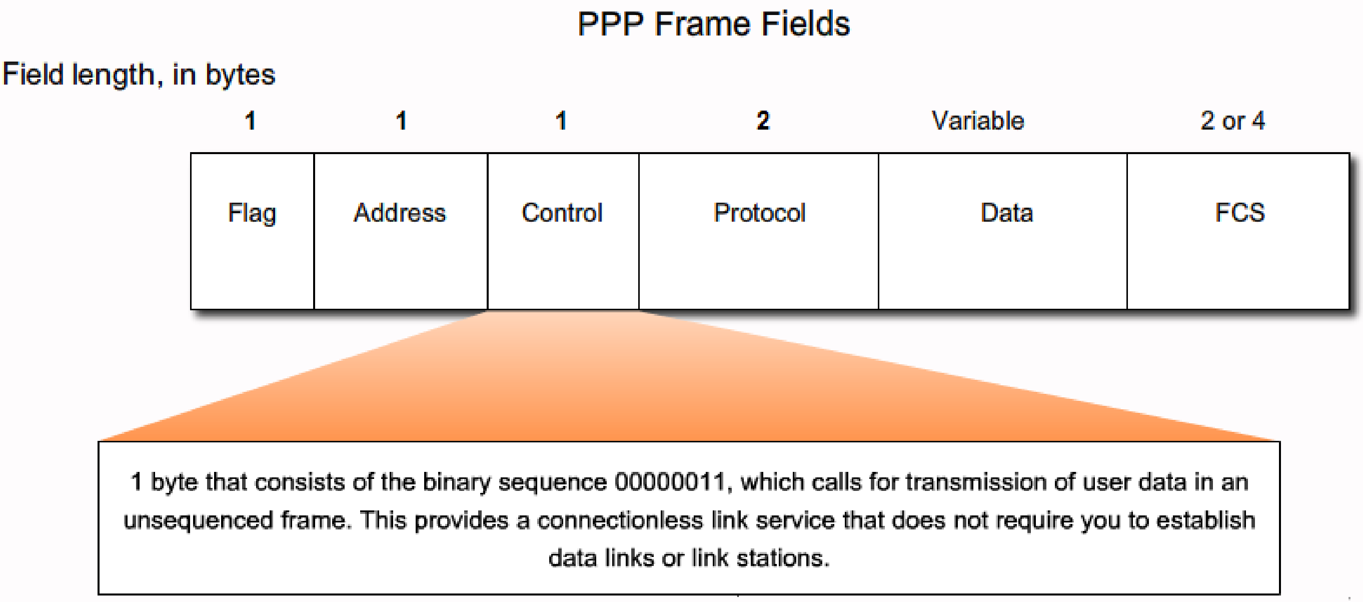
Field length, in bytes

1	1	1	2	Variable	2 or 4
Flag	Address	Control	Protocol	Data	FCS

Consists of the standard broadcast address, which is the binary sequence 11111111. PPP does not assign individual station addresses.In HDLC environments, the Address field is used to address the frame to the destination node. On a point-to-point link, the destination node does not need to be addressed. Therefore, for PPP, the Address field is set to 0xFF, the broadcast address. If both PPP peers agree to perform address and control field compression during LCP negotiation, the Address field is not included.

PPP protokol

PPP rámec (3)



PPP Frame Fields

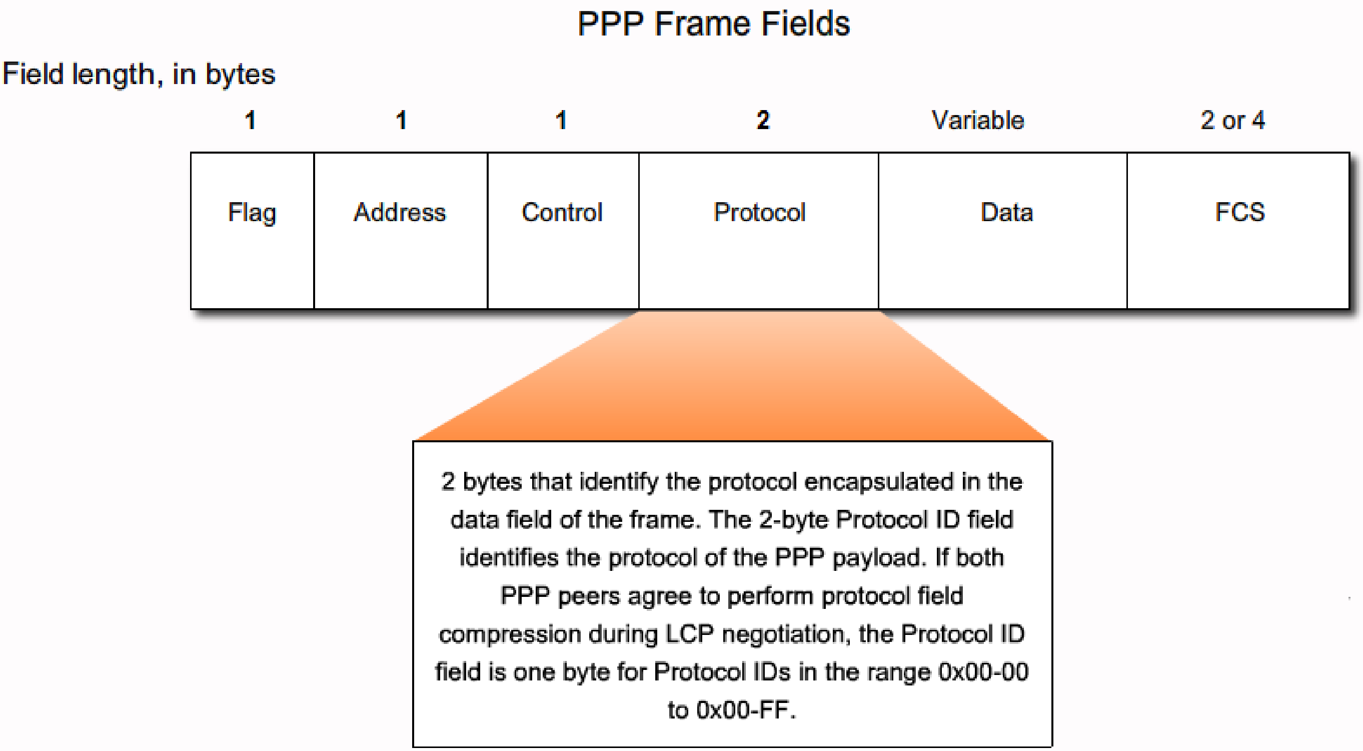
Field length, in bytes

1	1	1	2	Variable	2 or 4
Flag	Address	Control	Protocol	Data	FCS

1 byte that consists of the binary sequence 00000011, which calls for transmission of user data in an unsequenced frame. This provides a connectionless link service that does not require you to establish data links or link stations.

PPP protokol

PPP rámec (4)



PPP Frame Fields

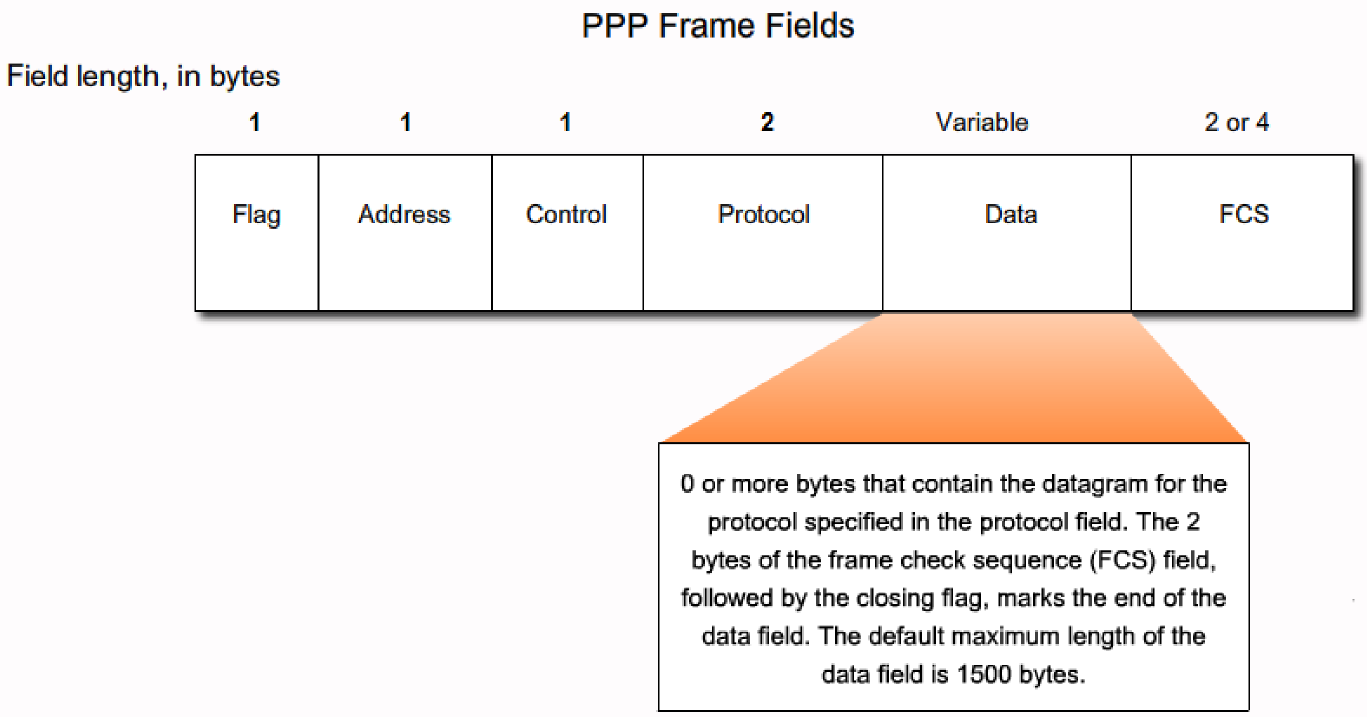
Field length, in bytes

1	1	1	2	Variable	2 or 4
Flag	Address	Control	Protocol	Data	FCS

2 bytes that identify the protocol encapsulated in the data field of the frame. The 2-byte Protocol ID field identifies the protocol of the PPP payload. If both PPP peers agree to perform protocol field compression during LCP negotiation, the Protocol ID field is one byte for Protocol IDs in the range 0x00-00 to 0x00-FF.

PPP protokol

PPP rámec (5)



PPP Frame Fields

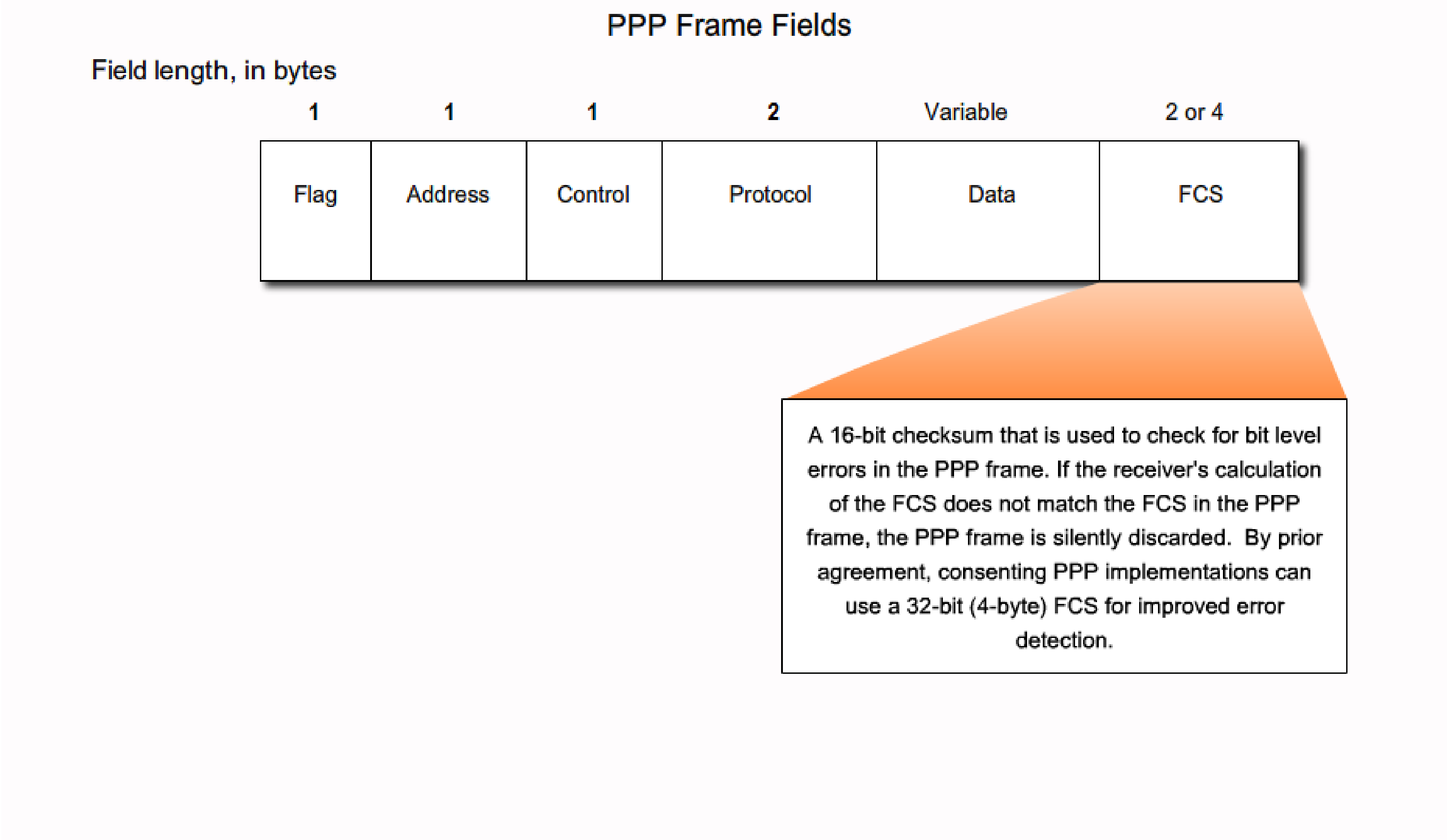
Field length, in bytes

1	1	1	2	Variable	2 or 4
Flag	Address	Control	Protocol	Data	FCS

0 or more bytes that contain the datagram for the protocol specified in the protocol field. The 2 bytes of the frame check sequence (FCS) field, followed by the closing flag, marks the end of the data field. The default maximum length of the data field is 1500 bytes.

PPP protokol

PPP rámec (6)



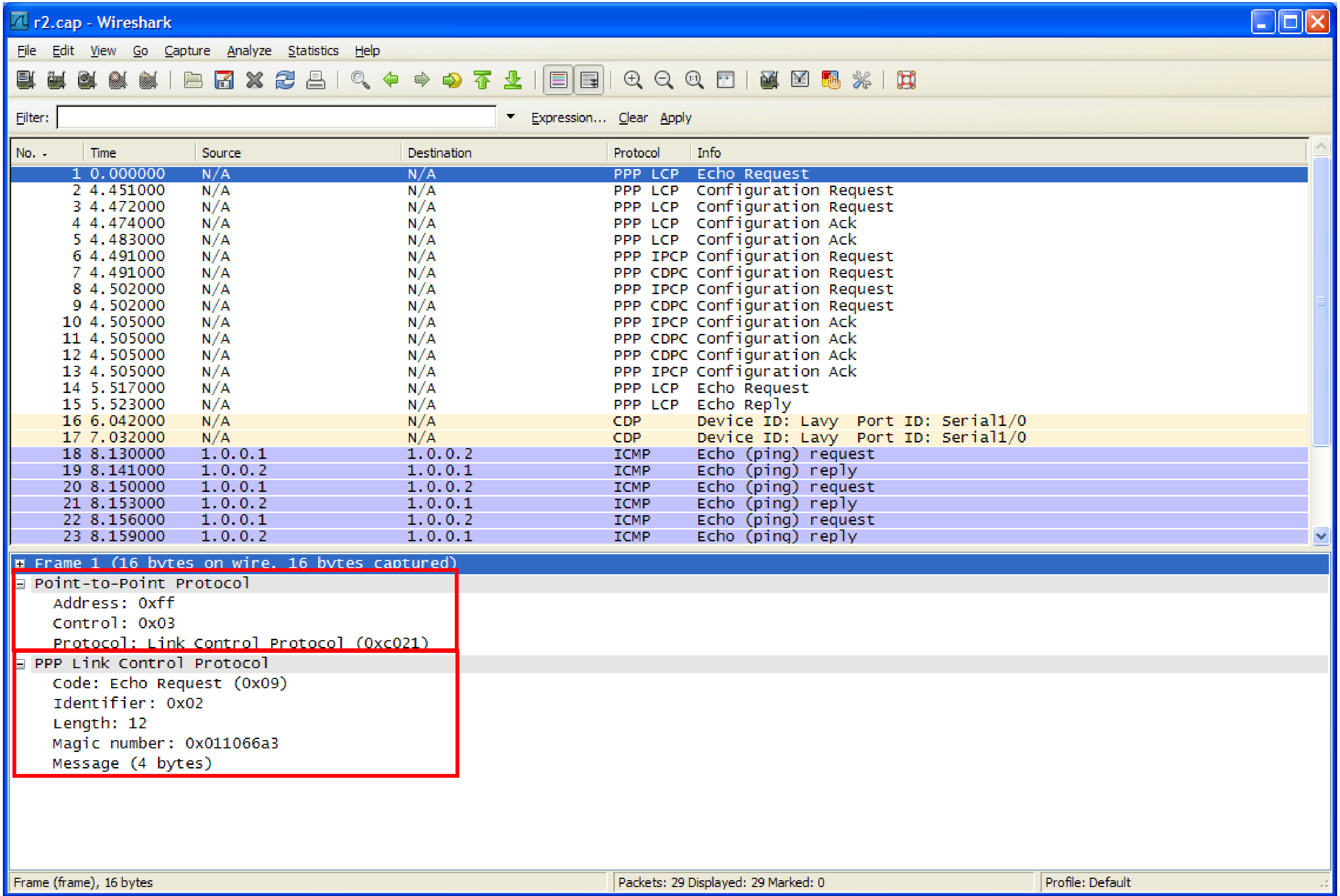
PPP Frame Fields

Field length, in bytes

1	1	1	2	Variable	2 or 4
Flag	Address	Control	Protocol	Data	FCS

A 16-bit checksum that is used to check for bit level errors in the PPP frame. If the receiver's calculation of the FCS does not match the FCS in the PPP frame, the PPP frame is silently discarded. By prior agreement, consenting PPP implementations can use a 32-bit (4-byte) FCS for improved error detection.

PPP rámec - wireshark



```
No. -  Time      Source    Destination  Protocol  Info
    1 0.000000  N/A       N/A          PPP LCP   Echo Request
    2 4.451000  N/A       N/A          PPP LCP   Configuration Request
    3 4.472000  N/A       N/A          PPP LCP   Configuration Request
    4 4.474000  N/A       N/A          PPP LCP   Configuration Ack
    5 4.483000  N/A       N/A          PPP LCP   Configuration Ack
    6 4.491000  N/A       N/A          PPP IPCP  Configuration Request
    7 4.491000  N/A       N/A          PPP CDPC  Configuration Request
    8 4.502000  N/A       N/A          PPP IPCP  Configuration Request
    9 4.502000  N/A       N/A          PPP CDPC  Configuration Request
   10 4.505000  N/A       N/A          PPP IPCP  Configuration Ack
   11 4.505000  N/A       N/A          PPP CDPC  Configuration Ack
   12 4.505000  N/A       N/A          PPP CDPC  Configuration Ack
   13 4.505000  N/A       N/A          PPP IPCP  Configuration Ack
   14 5.517000  N/A       N/A          PPP LCP   Echo Request
   15 5.523000  N/A       N/A          PPP LCP   Echo Reply
   16 6.042000  N/A       N/A          CDP       Device ID: Lavy  Port ID: Serial1/0
   17 7.032000  N/A       N/A          CDP       Device ID: Lavy  Port ID: Serial1/0
   18 8.130000  1.0.0.1   1.0.0.2      ICMP      Echo (ping) request
   19 8.141000  1.0.0.2   1.0.0.1      ICMP      Echo (ping) reply
   20 8.150000  1.0.0.1   1.0.0.2      ICMP      Echo (ping) request
   21 8.153000  1.0.0.2   1.0.0.1      ICMP      Echo (ping) reply
   22 8.156000  1.0.0.1   1.0.0.2      ICMP      Echo (ping) request
   23 8.159000  1.0.0.2   1.0.0.1      ICMP      Echo (ping) reply
```

```
⊞ Frame 1 (16 bytes on wire, 16 bytes captured)
⊟ Point-to-Point Protocol
    Address: 0xff
    Control: 0x03
    Protocol: Link Control Protocol (0xc021)
⊟ PPP Link Control Protocol
    Code: Echo Request (0x09)
    Identifier: 0x02
    Length: 12
    Magic number: 0x011066a3
    Message (4 bytes)
```

```
Frame (frame), 16 bytes    Packets: 29 Displayed: 29 Marked: 0    Profile: Default
```

PPP relácie

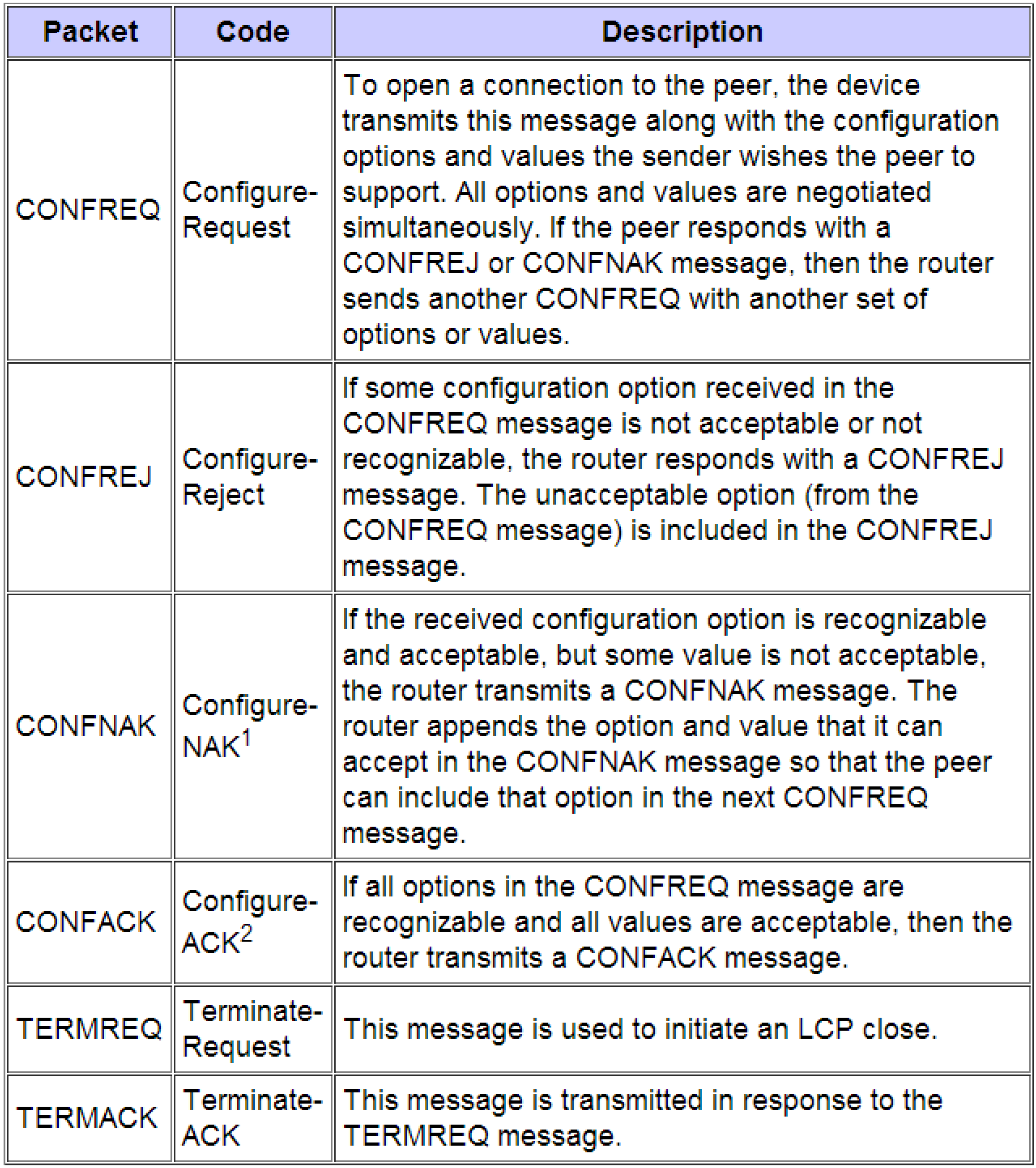
Založenie PPP spojenia - fázy

- Tri fázy aktivácie PPP spojenia
  1. Fáza vytvorenia spoja
     - LCP overí prítomnosť PPP na oboch stranách linky
     - Pomocou LCP sa dojednajú konfiguračné parametre ako maximálna podporovaná veľkosť rámcov (Maximum Receive Unit, MRU), kompresia vybraných polí PPP rámca, spôsob autentifikácie, prípadne spôsob overenia kvality linky
  2. Fáza autentifikácie a overenia kvality linky (voliteľná fáza)
     - Ak sa uzly dohodli na autentifikácii, prípadne kontrole kvality linky, táto fáza sa realizuje hneď, ako je ukončené vytvorenie spoja ešte pred tým, ako sa začnú prenášať používateľské dáta
     - Ak táto fáza skončí neúspešne, linka neprejde do fázy vyjednania konkrétnych L3 protokolov pomocou NCPs a nebude mať dovolené prenášať žiadne používateľské dáta
  3. Fáza negociácie sieťových protokolov
     - Pomocou NCP protokolov sa dohodne, aké L3 protokoly sa budú na PPP spojení prenášať a aké prevádzkové parametre tieto protokoly budú mať
  4. Fáza ukončenia spoja
- Prenos je možný až po úspešných predchádzajúcich fázach

PPP relácie

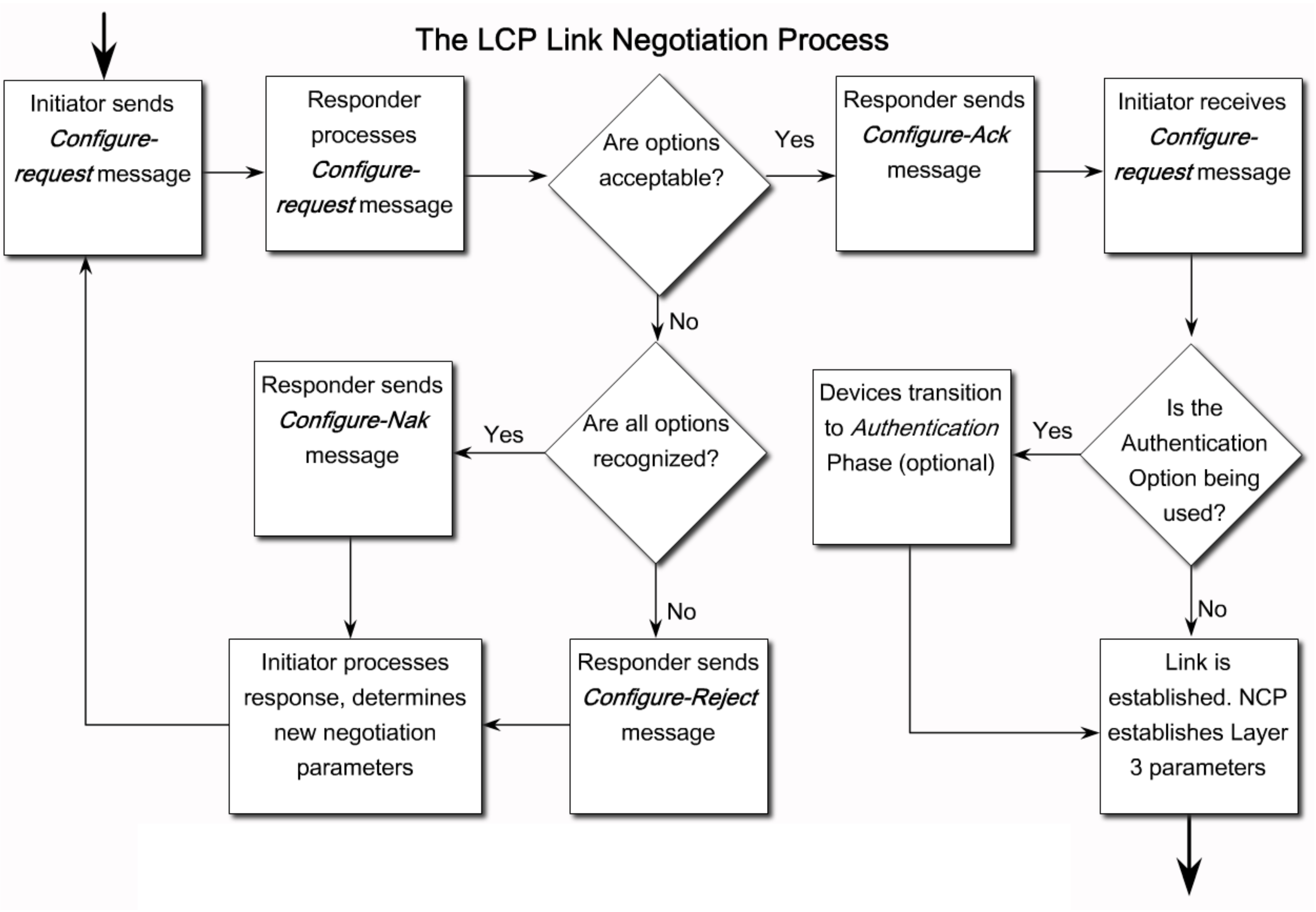
PPP správy

- Tri triedy LCP rámcov:
  - Link-establishment frames establish and configure a link.
    - Configure-Request, Configure-Ack, Configure-Nak, and Configure-Reject
  - Link-maintenance frames manage and debug a link.
    - Code-Reject, Protocol-Reject, Echo-Request, Echo-Reply, and Discard-Request
  - Link-termination frames terminate a link.
    - Terminate-Request and Terminate-Ack



Packet	Code	Description
CONFREQ	Configure-Request	To open a connection to the peer, the device transmits this message along with the configuration options and values the sender wishes the peer to support. All options and values are negotiated simultaneously. If the peer responds with a CONFREJ or CONFNAK message, then the router sends another CONFREQ with another set of options or values.
CONFREJ	Configure-Reject	If some configuration option received in the CONFREQ message is not acceptable or not recognizable, the router responds with a CONFREJ message. The unacceptable option (from the CONFREQ message) is included in the CONFREJ message.
CONFNAK	Configure-NAK[1]	If the received configuration option is recognizable and acceptable, but some value is not acceptable, the router transmits a CONFNAK message. The router appends the option and value that it can accept in the CONFNAK message so that the peer can include that option in the next CONFREQ message.
CONFACK	Configure-ACK[2]	If all options in the CONFREQ message are recognizable and all values are acceptable, then the router transmits a CONFACK message.
TERMREQ	Terminate-Request	This message is used to initiate an LCP close.
TERMACK	Terminate-ACK	This message is transmitted in response to the TERMREQ message.

Činnosť LCP



The LCP Link Negotiation Process

Initiator sends *Configure-request* message

Responder processes *Configure-request* message

Are options acceptable?

Yes

Responder sends *Configure-Ack* message

Initiator receives *Configure-request* message

No

Are all options recognized?

Yes

Responder sends *Configure-Nak* message

No

Responder sends *Configure-Reject* message

Initiator processes response, determines new negotiation parameters

Is the Authentication Option being used?

Yes

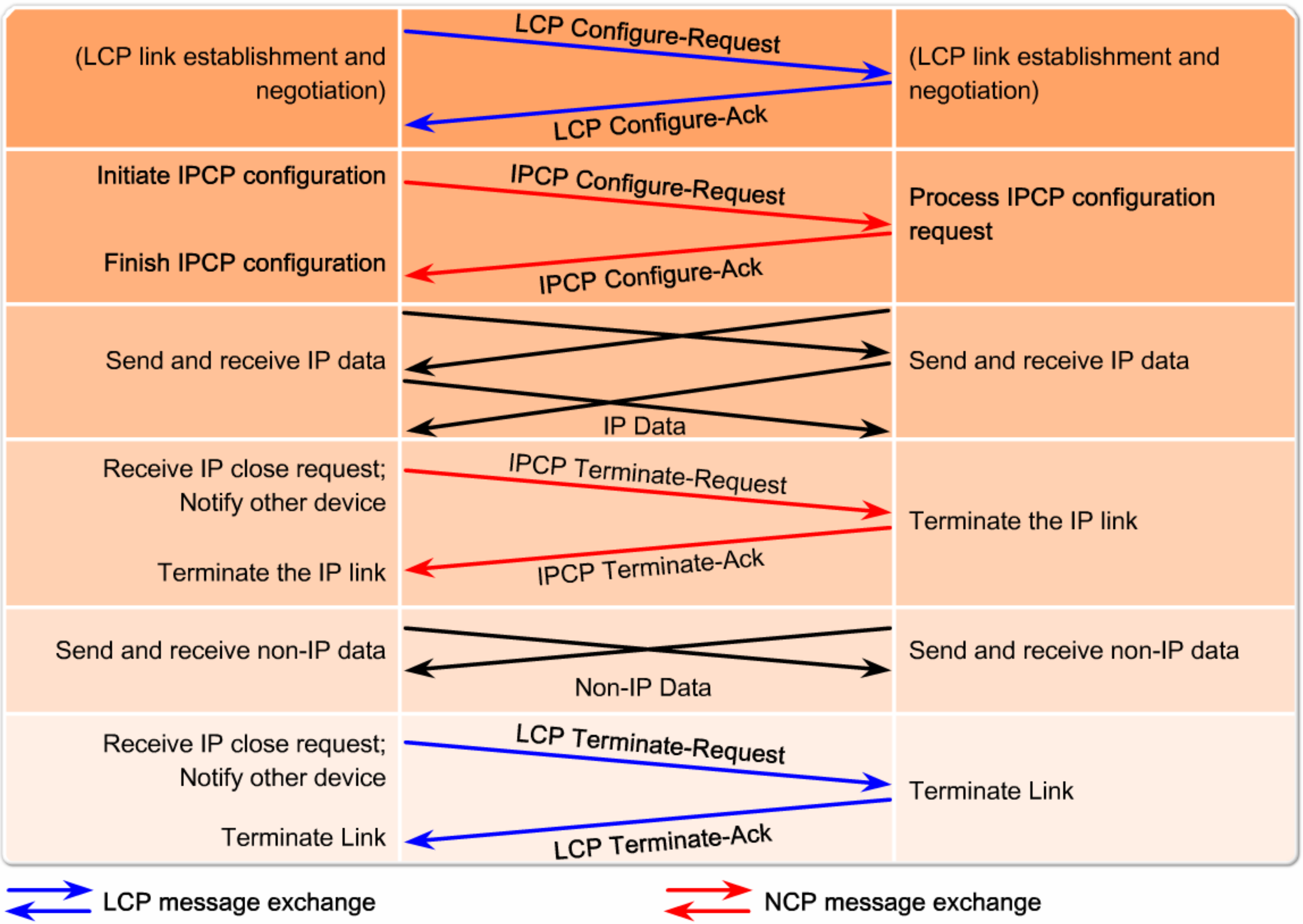
Devices transition to *Authentication* Phase (optional)

No

Link is established. NCP establishes Layer 3 parameters

Činnosť LCP a NCP pre IP (IPCP)

NCP Process

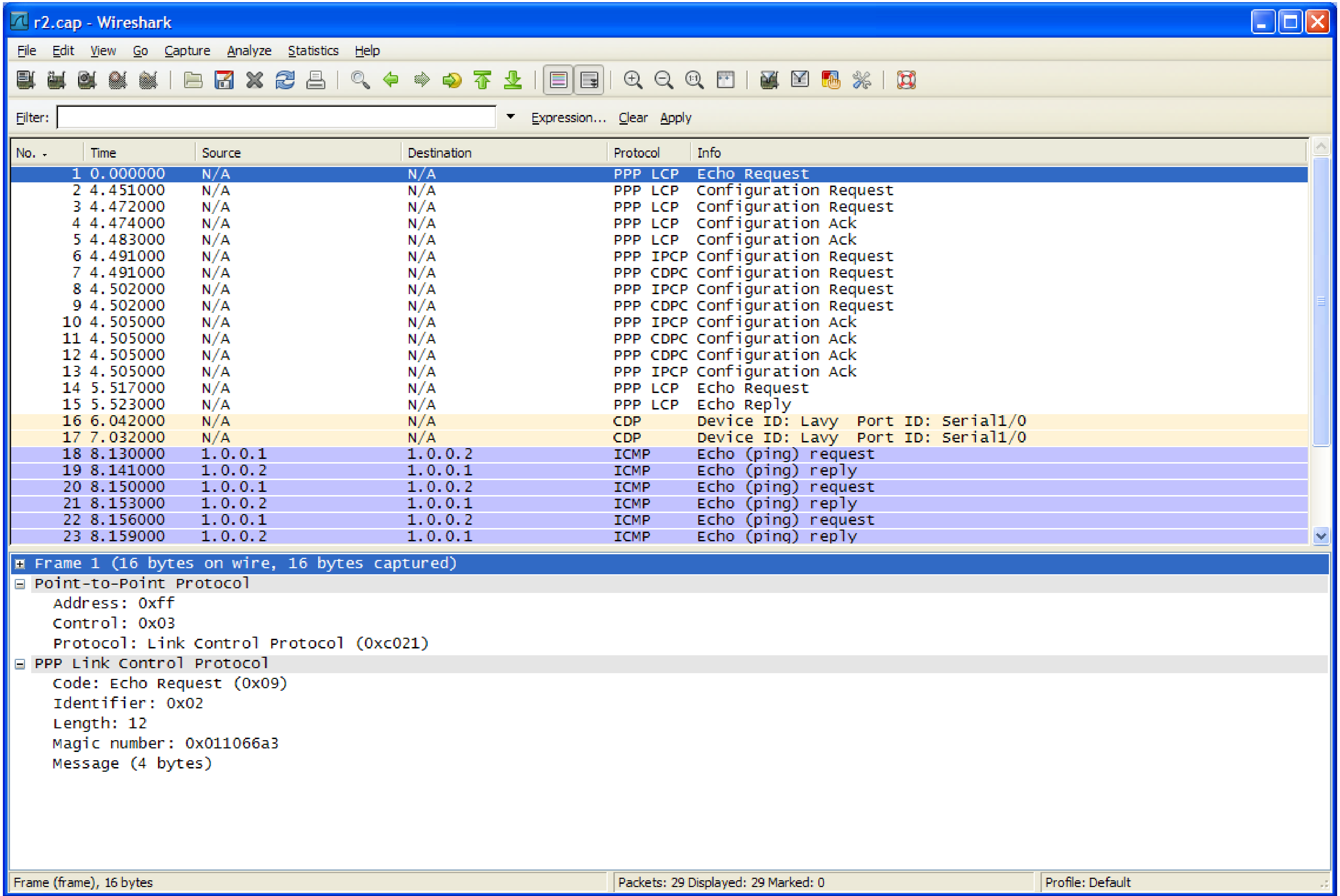


(LCP link establishment and negotiation)	LCP Configure-Request LCP Configure-Ack	(LCP link establishment and negotiation)
Initiate IPCP configuration Finish IPCP configuration	IPCP Configure-Request IPCP Configure-Ack	Process IPCP configuration request
Send and receive IP data	IP Data	Send and receive IP data
Receive IP close request; Notify other device Terminate the IP link	IPCP Terminate-Request IPCP Terminate-Ack	Terminate the IP link
Send and receive non-IP data	Non-IP Data	Send and receive non-IP data
Receive IP close request; Notify other device Terminate Link	LCP Terminate-Request LCP Terminate-Ack	Terminate Link

LCP message exchange

NCP message exchange

Wireshark – založenie spojenia


r2.cap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply

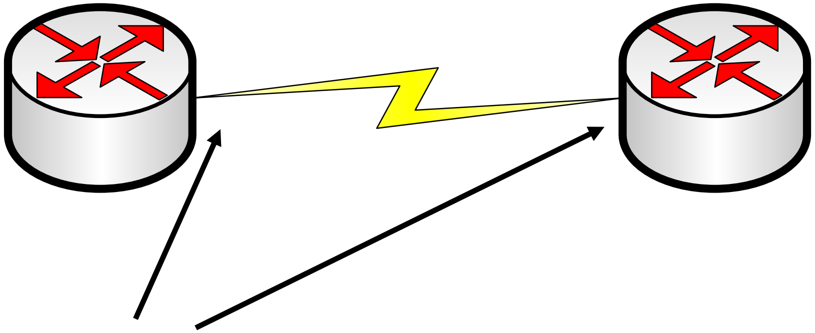
```
No. -   Time        Source     Destination  Protocol  Info
     1 0.000000    N/A        N/A          PPP LCP   Echo Request
     2 4.451000    N/A        N/A          PPP LCP   Configuration Request
     3 4.472000    N/A        N/A          PPP LCP   Configuration Request
     4 4.474000    N/A        N/A          PPP LCP   Configuration Ack
     5 4.483000    N/A        N/A          PPP LCP   Configuration Ack
     6 4.491000    N/A        N/A          PPP IPCP  Configuration Request
     7 4.491000    N/A        N/A          PPP CDPC  Configuration Request
     8 4.502000    N/A        N/A          PPP IPCP  Configuration Request
     9 4.502000    N/A        N/A          PPP CDPC  Configuration Request
    10 4.505000    N/A        N/A          PPP IPCP  Configuration Ack
    11 4.505000    N/A        N/A          PPP CDPC  Configuration Ack
    12 4.505000    N/A        N/A          PPP CDPC  Configuration Ack
    13 4.505000    N/A        N/A          PPP IPCP  Configuration Ack
    14 5.517000    N/A        N/A          PPP LCP   Echo Request
    15 5.523000    N/A        N/A          PPP LCP   Echo Reply
    16 6.042000    N/A        N/A          CDP       Device ID: Lavy  Port ID: Serial1/0
    17 7.032000    N/A        N/A          CDP       Device ID: Lavy  Port ID: Serial1/0
    18 8.130000    1.0.0.1    1.0.0.2      ICMP      Echo (ping) request
    19 8.141000    1.0.0.2    1.0.0.1      ICMP      Echo (ping) reply
    20 8.150000    1.0.0.1    1.0.0.2      ICMP      Echo (ping) request
    21 8.153000    1.0.0.2    1.0.0.1      ICMP      Echo (ping) reply
    22 8.156000    1.0.0.1    1.0.0.2      ICMP      Echo (ping) request
    23 8.159000    1.0.0.2    1.0.0.1      ICMP      Echo (ping) reply
```

```
⊞ Frame 1 (16 bytes on wire, 16 bytes captured)
⊟ Point-to-Point Protocol
    Address: 0xff
    Control: 0x03
    Protocol: Link Control Protocol (0xc021)
⊟ PPP Link Control Protocol
    Code: Echo Request (0x09)
    Identifier: 0x02
    Length: 12
    Magic number: 0x011066a3
    Message (4 bytes)
```

Frame (frame), 16 bytes | Packets: 29 Displayed: 29 Marked: 0 | Profile: Default

PPP konfigurácia

Spustenie PPP



```
Router(config-if)#encapsulation ppp
```

```
Router#sh int s 1/0
Serial1/0 is up, line protocol is up
  Hardware is M4T
  Internet address is 1.1.1.1/8
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: IPCP, CDPCP, crc 16, loopback not set
  Keepalive set (10 sec)
  Restart-Delay is 0 secs
```

```
Router#sh ip int brief
Interface                  IP-Address      OK? Method Status
   Protocol
FastEthernet0/0            unassigned      YES unset  administratively down down
FastEthernet0/1            unassigned      YES unset  administratively down down
Serial1/0                  1.1.1.1         YES manual up                    up
```

Ďalšie konfiguračné možnosti PPP

- Kompresia

```
Router(config-if)#compress ?
  lzs         lzs compression type
  mppc        MPPC compression type
  predictor   predictor compression type
  stac        stac compression algorithm
```

- Kvalita

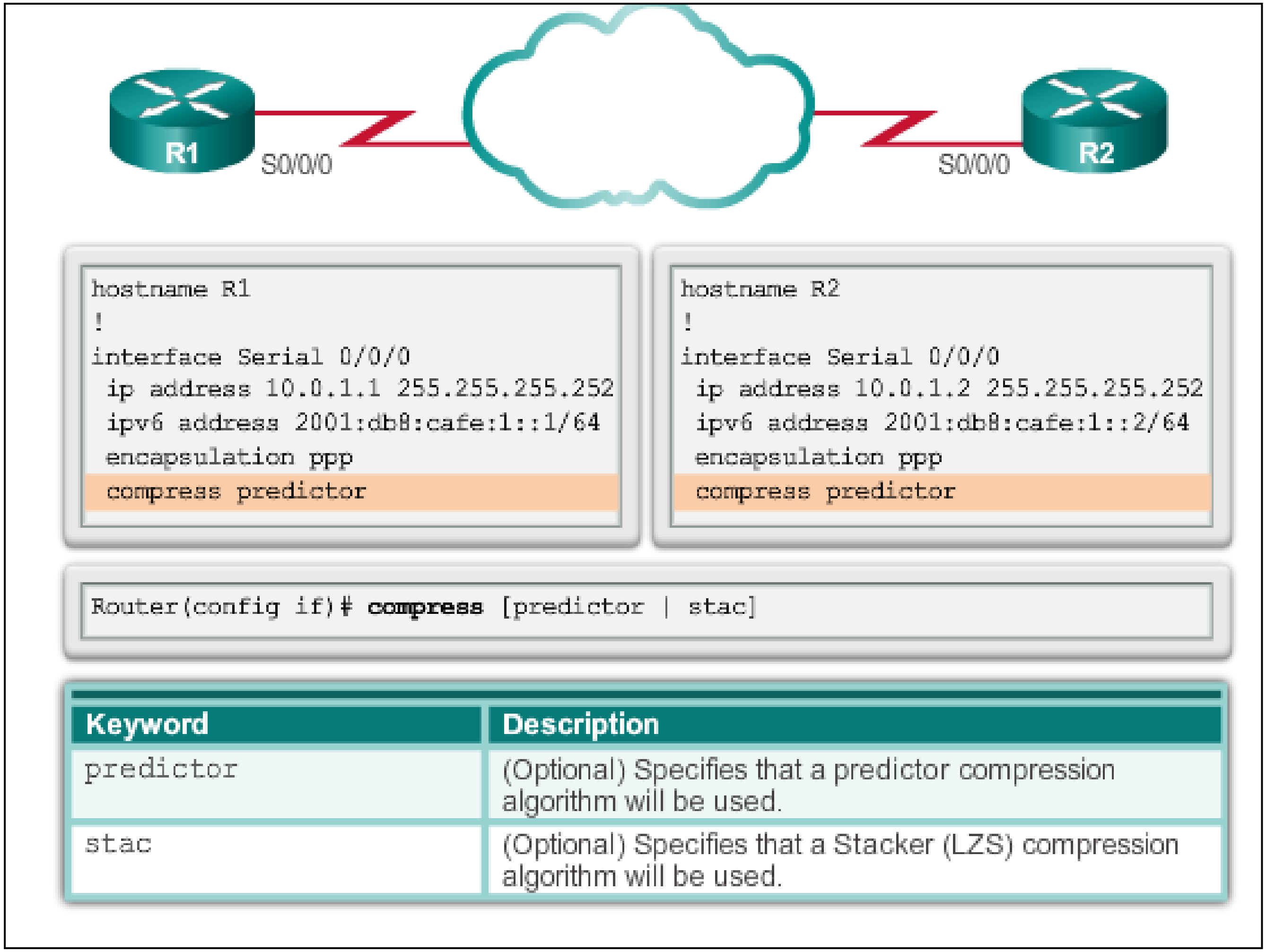
```
Router(config-if)#ppp quality ?
  <0-100>   Minimum percent of traffic successful
  reject    Reject Link Quality Monitoring negotiation
```

- Load balance

```
Router(config-if)#ppp multilink ?
  endpoint     Configure the local Endpoint Discriminator
  group        Put interface in a multilink bundle
  mrru         Configure multilink MRRU values
  multiclass   Configure support for Multiclass Multilink
  queue        Specify link queuing parameters
```

Konfigurácia PPP

PPP Kompresia



```
hostname R1
!
interface Serial 0/0/0
 ip address 10.0.1.1 255.255.255.252
 ipv6 address 2001:db8:cafe:1::1/64
 encapsulation ppp
 compress predictor
```

```
hostname R2
!
interface Serial 0/0/0
 ip address 10.0.1.2 255.255.255.252
 ipv6 address 2001:db8:cafe:1::2/64
 encapsulation ppp
 compress predictor
```

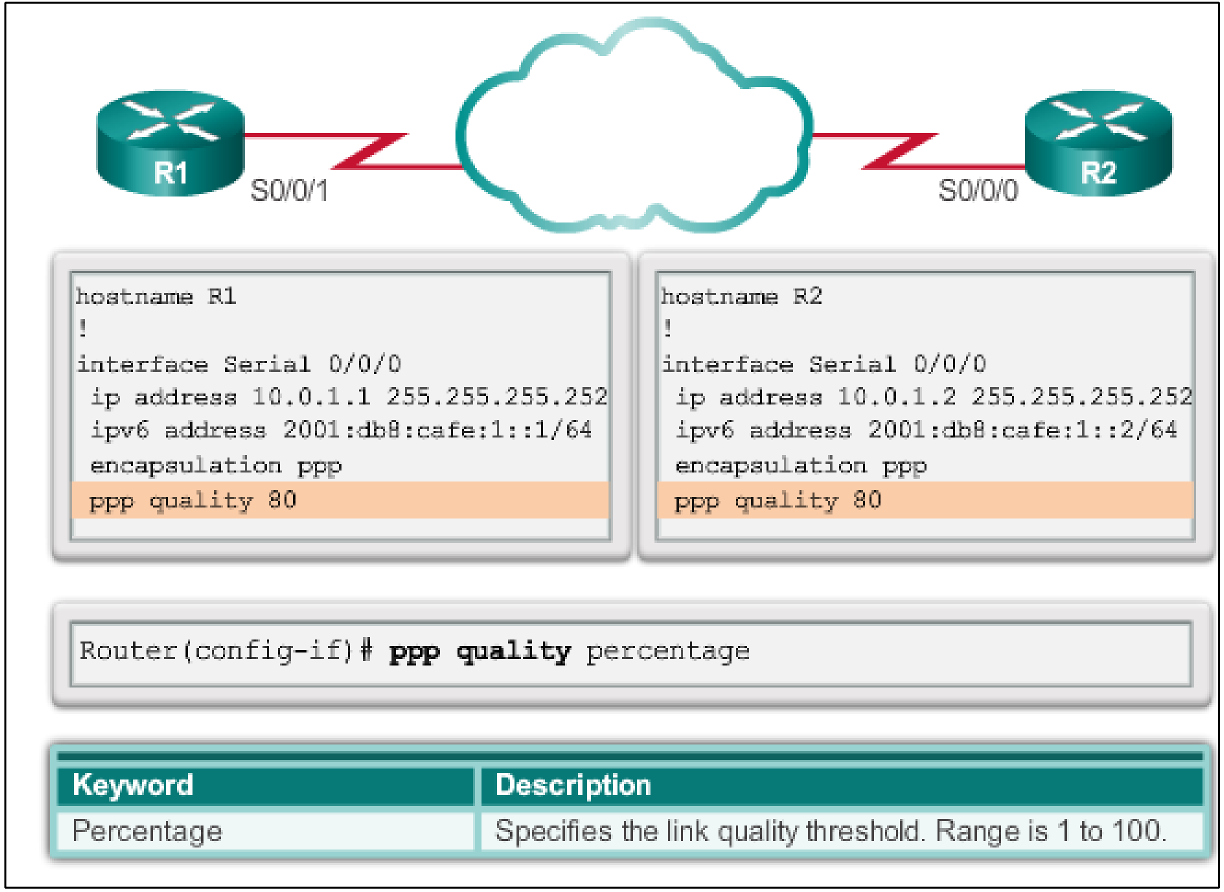
```
Router(config if)# compress [predictor | stac]
```

Keyword	Description
predictor	(Optional) Specifies that a predictor compression algorithm will be used.
stac	(Optional) Specifies that a Stacker (LZS) compression algorithm will be used.

Konfigurácia PPP

PPP monitorovanie kvality linky

The ppp quality *percentage* command ensures that the link meets the quality requirement set; otherwise, the link closes down.



```
hostname R1
!
interface Serial 0/0/0
 ip address 10.0.1.1 255.255.255.252
 ipv6 address 2001:db8:cafe:1::1/64
 encapsulation ppp
 ppp quality 80
```

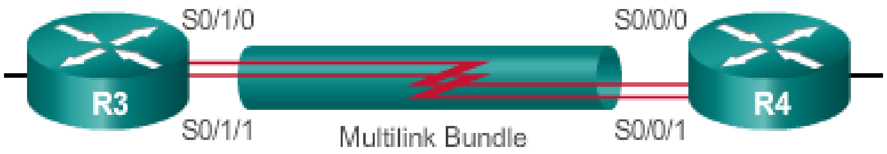
```
hostname R2
!
interface Serial 0/0/0
 ip address 10.0.1.2 255.255.255.252
 ipv6 address 2001:db8:cafe:1::2/64
 encapsulation ppp
 ppp quality 80
```

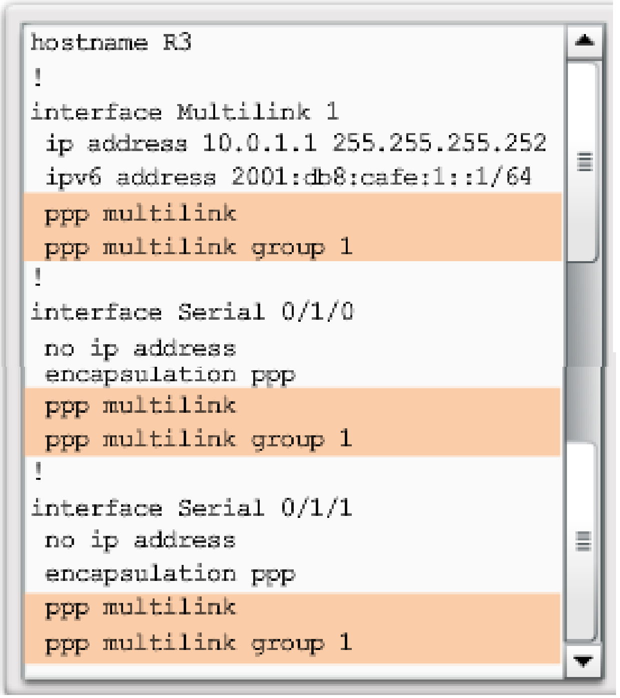
```
Router(config-if)# ppp quality percentage
```

Keyword	Description
Percentage	Specifies the link quality threshold. Range is 1 to 100.

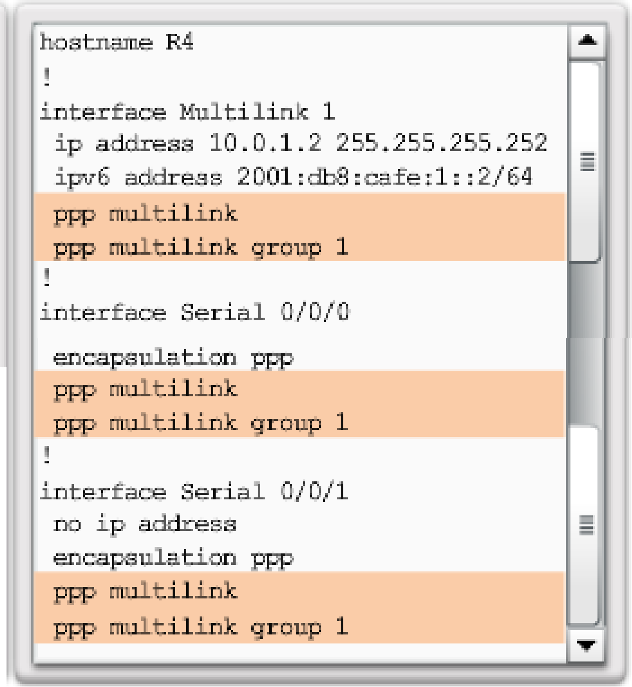
Konfigurácia PPP

PPP Multilink





```
hostname R3
!
interface Multilink 1
 ip address 10.0.1.1 255.255.255.252
 ipv6 address 2001:db8:cafe:1::1/64
 ppp multilink
 ppp multilink group 1
!
interface Serial 0/1/0
 no ip address
 encapsulation ppp
 ppp multilink
 ppp multilink group 1
!
interface Serial 0/1/1
 no ip address
 encapsulation ppp
 ppp multilink
 ppp multilink group 1
```



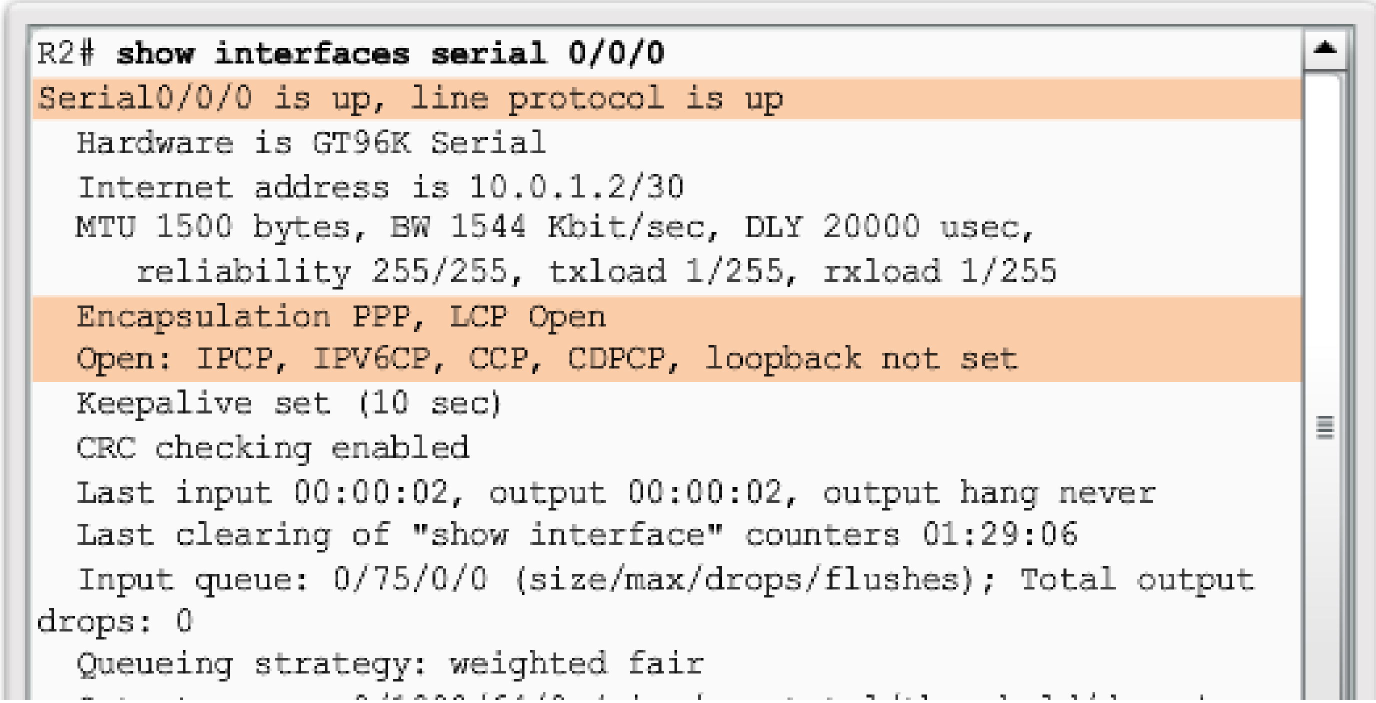
```
hostname R4
!
interface Multilink 1
 ip address 10.0.1.2 255.255.255.252
 ipv6 address 2001:db8:cafe:1::2/64
 ppp multilink
 ppp multilink group 1
!
interface Serial 0/0/0

 encapsulation ppp
 ppp multilink
 ppp multilink group 1
!
interface Serial 0/0/1
 no ip address
 encapsulation ppp
 ppp multilink
 ppp multilink group 1
```

Overenie a diagnostika

```
Router#show interface

Router#show interface serial

Router#debug ppp ?
  authentication  CHAP and PAP authentication
  bap             BAP protocol transactions
  cbcp            Callback Control Protocol negotiation
  elog            PPP ELOGs
  error           Protocol errors and error statistics
  forwarding      PPP layer 2 forwarding
  mppe            MPPE Events
  multilink       Multilink activity
  negotiation     Protocol parameter negotiation
  packet          Low-level PPP packet dump

Router#undebug all
```

Overenie a diagnostika

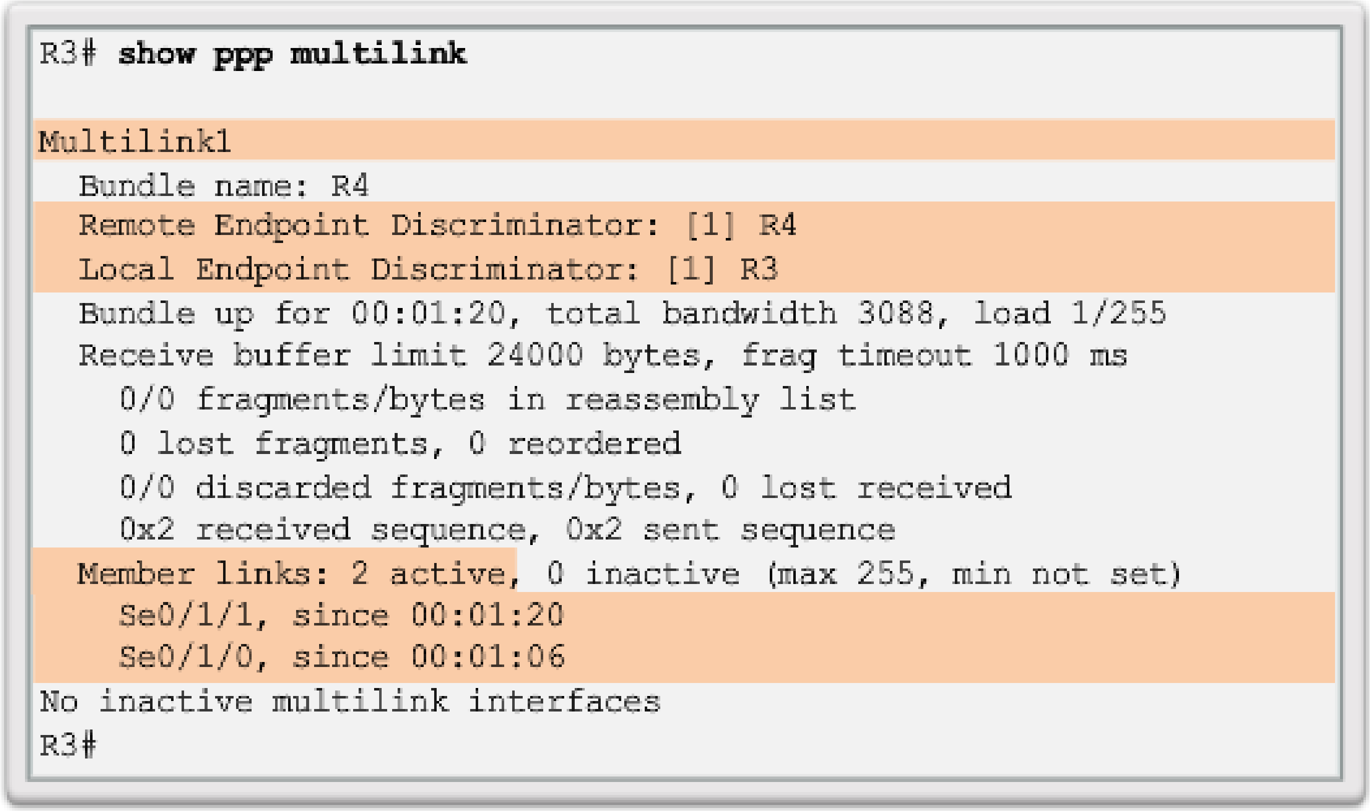
```
Router#show interface


Router#show interface serial
```



```
R2# show interfaces serial 0/0/0
Serial0/0/0 is up, line protocol is up
   Hardware is GT96K Serial
   Internet address is 10.0.1.2/30
   MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
      reliability 255/255, txload 1/255, rxload 1/255
   Encapsulation PPP, LCP Open
   Open: IPCP, IPV6CP, CCP, CDPCP, loopback not set
   Keepalive set (10 sec)
   CRC checking enabled
   Last input 00:00:02, output 00:00:02, output hang never
   Last clearing of "show interface" counters 01:29:06
   Input queue: 0/75/0/0 (size/max/drops/flushes); Total output
drops: 0
   Queueing strategy: weighted fair
```

Overenie a diagnostika

```
Router#show ppp multilink
```



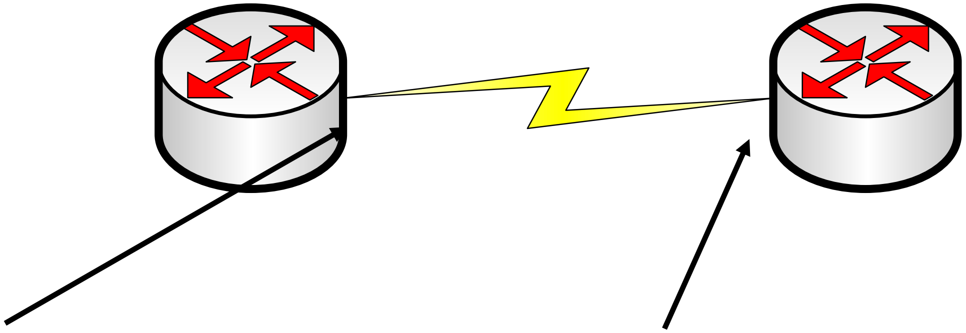
```
R3# show ppp multilink

Multilink1
  Bundle name: R4
  Remote Endpoint Discriminator: [1] R4
  Local Endpoint Discriminator: [1] R3
  Bundle up for 00:01:20, total bandwidth 3088, load 1/255
  Receive buffer limit 24000 bytes, frag timeout 1000 ms
    0/0 fragments/bytes in reassembly list
    0 lost fragments, 0 reordered
    0/0 discarded fragments/bytes, 0 lost received
    0x2 received sequence, 0x2 sent sequence
  Member links: 2 active, 0 inactive (max 255, min not set)
    Se0/1/1, since 00:01:20
    Se0/1/0, since 00:01:06
No inactive multilink interfaces
R3#
```

Overenie PPP – linka OK

```
Router#debug ppp packet
PPP packet display debugging is on
Router#
*Mar  1 01:28:47.975: Se1/0 LCP: O ECHOREQ [Open] id 2 len 12 magic 0x006CEBBF
*Mar  1 01:28:48.003: Se1/0 LCP-FS: I ECHOREP [Open] id 2 len 12 magic 0x016CEB4A
*Mar  1 01:28:48.003: Se1/0 LCP-FS: Received id 2, sent id 2, line up
*Mar  1 01:28:52.067: Se1/0 LCP-FS: I ECHOREQ [Open] id 2 len 12 magic 0x016CEB4A
*Mar  1 01:28:52.067: Se1/0 LCP-FS: O ECHOREP [Open] id 2 len 12 magic 0x006CEBBF
*Mar  1 01:28:58.215: Se1/0 LCP: O ECHOREQ [Open] id 3 len 12 magic 0x006CEBBF
*Mar  1 01:28:58.227: Se1/0 LCP-FS: I ECHOREP [Open] id 3 len 12 magic 0x016CEB4A
*Mar  1 01:28:58.227: Se1/0 LCP-FS: Received id 3, sent id 3, line up
*Mar  1 01:29:02.287: Se1/0 LCP-FS: I ECHOREQ [Open] id 3 len 12 magic 0x016CEB4A
*Mar  1 01:29:02.287: Se1/0 LCP-FS: O ECHOREP [Open] id 3 len 12 magic 0x006CEBBF
```

```
Lavy#debug ppp negotiation
PPP protocol negotiation debugging is on
*Mar  1 03:22:41.579: Se1/0 PPP: Phase is ESTABLISHING
*Mar  1 03:22:41.579: Se1/0 LCP: O CONFREQ [Open] id 59 len 10
*Mar  1 03:22:41.579: Se1/0 LCP:    MagicNumber 0x00D57203 (0x050600D57203)
*Mar  1 03:22:41.587: Se1/0 LCP: I CONFACK [REQsent] id 59 len 10
*Mar  1 03:22:41.587: Se1/0 LCP:    MagicNumber 0x00D57203 (0x050600D57203)
*Mar  1 03:22:41.587: Se1/0 LCP: I CONFREQ [ACKrcvd] id 221 len 18
*Mar  1 03:22:41.587: Se1/0 LCP:    MagicNumber 0x01D571FE (0x050601D571FE)
*Mar  1 03:22:41.587: Se1/0 LCP:    EndpointDisc 1 Pravy (0x130801507261796)
*Mar  1 03:22:41.587: Se1/0 LCP: O CONFACK [ACKrcvd] id 221 len 18
*Mar  1 03:22:41.587: Se1/0 LCP:    MagicNumber 0x01D571FE (0x050601D571FE)
*Mar  1 03:22:41.587: Se1/0 LCP:    EndpointDisc 1 Pravy (0x130801507261796)
*Mar  1 03:22:41.587: Se1/0 LCP: State is Open
*Mar  1 03:22:41.591: Se1/0 PPP: Phase is FORWARDING, Attempting Forward
*Mar  1 03:22:41.591: Se1/0 PPP: Phase is ESTABLISHING, Finish LCP
*Mar  1 03:22:41.591: Se1/0 PPP: Phase is UP
*Mar  1 03:22:41.591: Se1/0 IPCP: O CONFREQ [Closed] id 1 len 10
*Mar  1 03:22:41.595: Se1/0 IPCP:    Address 1.1.1.1 (0x030601010101)
*Mar  1 03:22:41.595: Se1/0 CDPCP: O CONFREQ [Closed] id 1 len 4
*Mar  1 03:22:41.595: Se1/0 PPP: Process pending ncp packets
*Mar  1 03:22:41.595: Se1/0 CDPCP: I CONFREQ [REQsent] id 1 len 4
*Mar  1 03:22:41.595: Se1/0 CDPCP: O CONFACK [REQsent] id 1 len 4
*Mar  1 03:22:41.595: Se1/0 IPCP: I CONFREQ [REQsent] id 1 len 10
*Mar  1 03:22:41.595: Se1/0 IPCP:    Address 1.1.1.2 (0x030601010102)
*Mar  1 03:22:41.595: Se1/0 IPCP: O CONFACK [REQsent] id 1 len 10
*Mar  1 03:22:41.595: Se1/0 IPCP:    Address 1.1.1.2 (0x030601010102)
*Mar  1 03:22:41.603: Se1/0 IPCP: I CONFACK [ACKsent] id 1 len 10
*Mar  1 03:22:41.607: Se1/0 IPCP:    Address 1.1.1.1 (0x030601010101)
*Mar  1 03:22:41.607: Se1/0 IPCP: State is Open
*Mar  1 03:22:41.611: Se1/0 CDPCP: I CONFACK [ACKsent] id 1 len 4
*Mar  1 03:22:41.611: Se1/0 CDPCP: State is Open
*Mar  1 03:22:41.627: Se1/0 IPCP: Install route to 1.1.1.2
```

Overenie PPP - Príklad 1



```
Router(config-if)#encapsulation ppp
```

```
Ostane default cHDLC
```

```
Router#sh int s 1/0
Serial1/0 is up, line protocol is down
  Hardware is M4T
  Internet address is 1.1.1.1/8
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: IPCP, CDPCP, crc 16, loopback not set
  Keepalive set (10 sec)
  Restart-Delay is 0 secs
```

```
Router#sh ip int brief
Interface                  IP-Address      OK? Method Status
   Protocol
FastEthernet0/0            unassigned      YES unset  administratively down down
FastEthernet0/1            unassigned      YES unset  administratively down down
Serial1/0                  1.1.1.1         YES manual up                    down
```

Overenie PPP - Príklad 1

```
Router#debug ppp packet
*Mar  1 01:15:13.815: Se1/0 PPP: O pkt type 0x0207, datagramsize 324
*Mar  1 01:15:13.827: Se1/0 PPP: I pkt type 0x008F, datagramsize 324 link[illegal]
*Mar  1 01:15:13.827: Se1/0 UNKNOWN(0x008F): Non-NCP packet, discarding
*Mar  1 01:15:15.847: Se1/0 LCP: O ECHOREQ [Open] id 19 len 12 magic 0x0035EB56
*Mar  1 01:15:15.847: Se1/0 LCP: echo_cnt 2, sent id 19, line up
*Mar  1 01:15:18.979: Se1/0 PPP: I pkt type 0x008F, datagramsize 24 link[illegal]
*Mar  1 01:15:18.979: Se1/0 UNKNOWN(0x008F): Non-NCP packet, discarding
*Mar  1 01:15:26.087: Se1/0 LCP: O ECHOREQ [Open] id 20 len 12 magic 0x0035EB56
*Mar  1 01:15:26.087: Se1/0 LCP: echo_cnt 3, sent id 20, line up
*Mar  1 01:15:28.983: Se1/0 PPP: I pkt type 0x008F, datagramsize 24 link[illegal]
*Mar  1 01:15:28.983: Se1/0 UNKNOWN(0x008F): Non-NCP packet, discarding
*Mar  1 01:15:29.983: Se1/0 PPP: I pkt type 0x008F, datagramsize 18 link[illegal]
*Mar  1 01:15:29.983: Se1/0 UNKNOWN(0x008F): Non-NCP packet, discarding
```

Overenie PPP - Príklad 1

```
Router#debug ppp negotiation
PPP protocol negotiation debugging is on
*Mar  1 01:17:39.171: Se1/0 LCP: Timeout: State Listen
*Mar  1 01:17:39.175: Se1/0 LCP: O CONFREQ [Listen] id 164 len 10
*Mar  1 01:17:39.179: Se1/0 LCP:    MagicNumber 0x0062F739 (0x05060062F739)
*Mar  1 01:17:41.187: Se1/0 LCP: Timeout: State REQsent
*Mar  1 01:17:41.191: Se1/0 LCP: O CONFREQ [REQsent] id 165 len 10
*Mar  1 01:17:41.191: Se1/0 LCP:    MagicNumber 0x0062F739 (0x05060062F739)
*Mar  1 01:17:43.203: Se1/0 LCP: Timeout: State REQsent
*Mar  1 01:17:43.207: Se1/0 LCP: O CONFREQ [REQsent] id 166 len 10
*Mar  1 01:17:43.207: Se1/0 LCP:    MagicNumber 0x0062F739 (0x05060062F739)
*Mar  1 01:17:45.219: Se1/0 LCP: Timeout: State REQsent
*Mar  1 01:17:45.219: Se1/0 LCP: O CONFREQ [REQsent] id 167 len 10
*Mar  1 01:17:45.219: Se1/0 LCP:    MagicNumber 0x0062F739 (0x05060062F739)
*Mar  1 01:17:47.235: Se1/0 LCP: Timeout: State REQsent
*Mar  1 01:17:47.239: Se1/0 LCP: O CONFREQ [REQsent] id 168 len 10
*Mar  1 01:17:47.239: Se1/0 LCP:    MagicNumber 0x0062F739 (0x05060062F739)
*Mar  1 01:17:49.251: Se1/0 LCP: Timeout: State REQsent
```

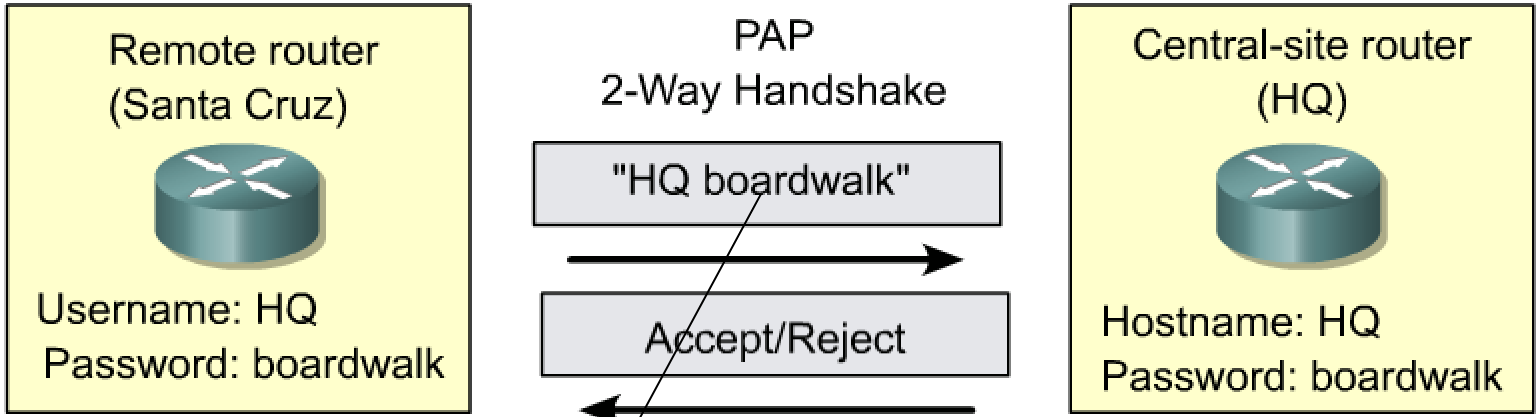
we're talking ppp, but the other end doesn't.

PPP autentifikácia

Autentifikácia v PPP

- PPP podporuje autentifikáciu (overenie identity) komunikujúcich uzlov
- Tradične PPP podporuje dva mechanizmy
  - Password Authentication Protocol (PAP)
  - Challenge Handshake Authentication Protocol (CHAP)
  - Voliteľne je možné používať aj pokročilejšie druhy autentifikácie pomocou Extensible Authentication Protocol (EAP)

Password Authentication Protocol (PAP)



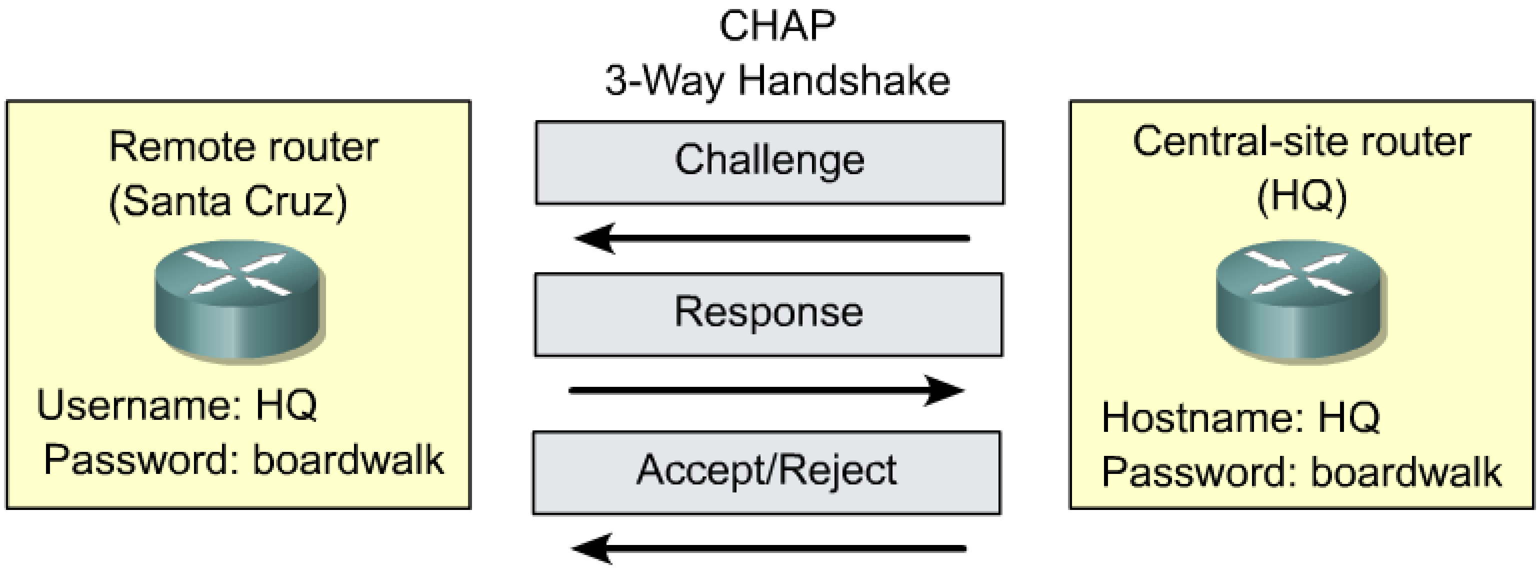
- Heslo posielané ako text
- Opakovane posielané až kým druhá strana nepotvrdí = **PROBLÉM (trial-and-error attacks)**

- PAP je jednoduchý plain-text autentifikačný protokol
  - Strana, ktorá má preukázať svoju identitu (klient), pošle svoje meno a heslo
  - Strana, ktorá požaduje preukázanie identity (ISP), toto meno a heslo overí a informuje klienta o (ne)úspechu
  - Proces autentifikácie začína klient

Password Authentication Protocol (PAP)

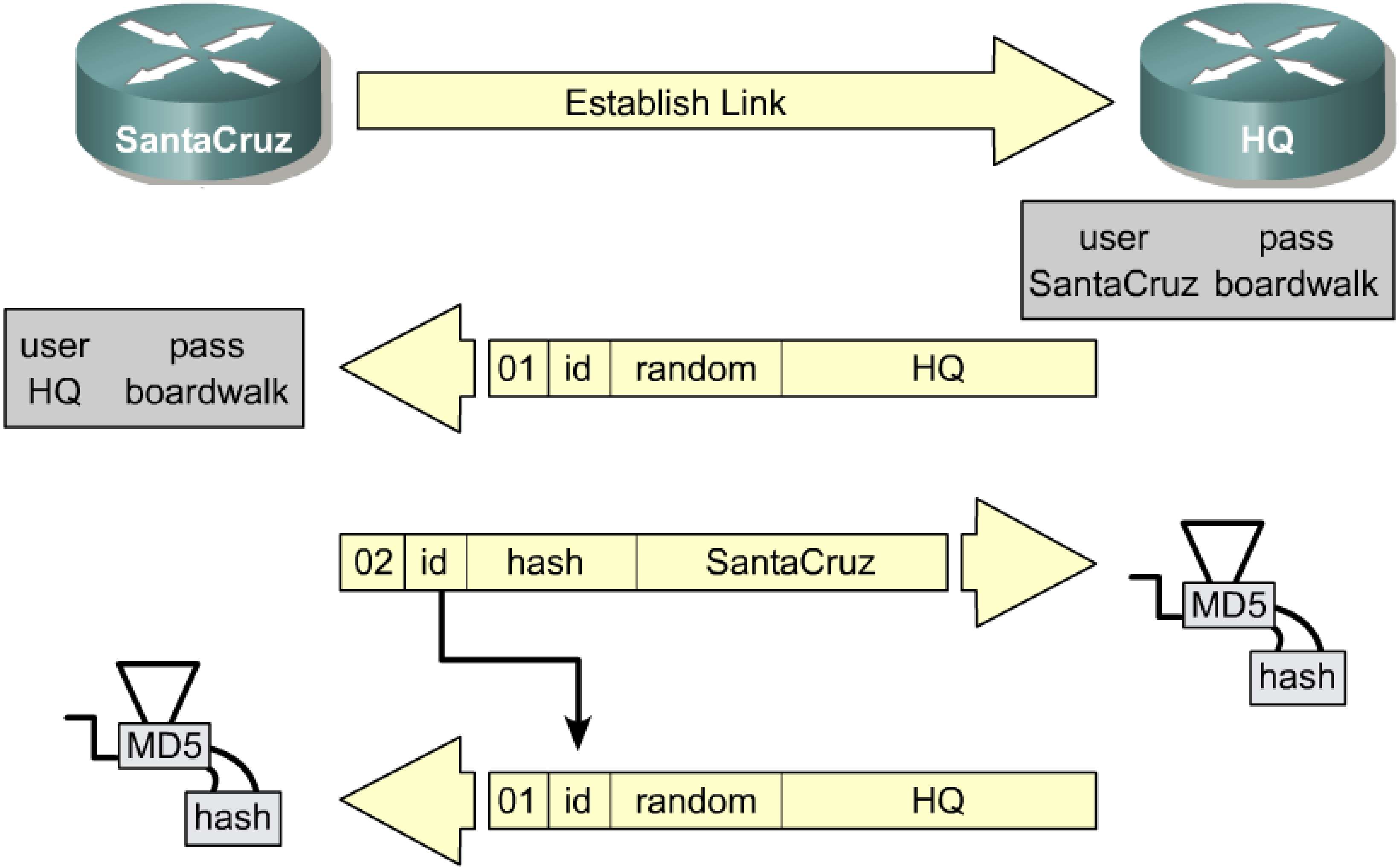
- PAP je jednoduchý a funkčný, avšak má zásadné nevýhody
  - Citlivé údaje prenáša ako plain text
  - Autentifikácia začína ako aktivita klienta a ISP nemá možnosť priebežne si klientovu identitu opätovne overiť
  - Pri opakovanom prihlásení sa prenášajú tie isté údaje, ktoré možno zachytiť a replikovať
- Tieto nevýhody rieši CHAP

Challenge Handshake Authentication Protocol (CHAP)



- CHAP je kryptografický autentifikačný protokol na báze zdieľaného hesla a výzvy
- CHAP poskytuje ochranu voči „playback“ útokom
  - používa náhodný challenge mechanizmus
- Heslo nie je posielané
  - je zdieľané medzi autentifikujúcimi smerovačmi

Autentifikačný proces v CHAP

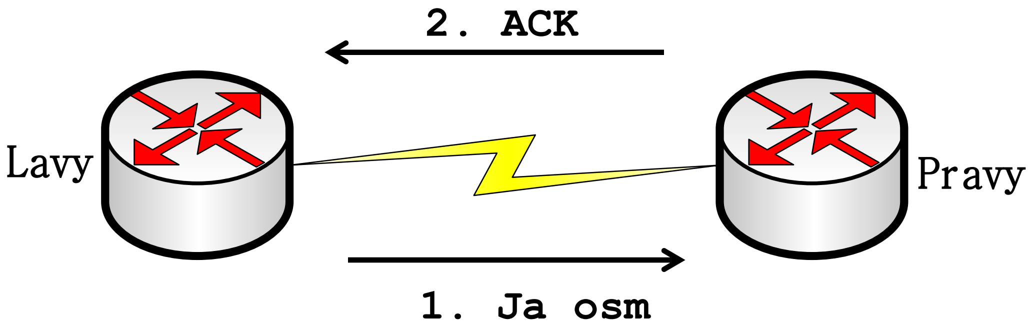


Challenge Handshake Authentication Protocol (CHAP)

- Algoritmus CHAP má oproti PAP zásadné výhody
  - Citlivé údaje sa nikdy neprenášajú v plain-text tvare
  - Z prenesených viditeľných údajov sa nedá rozumne usúdiť na tvar zdieľaného hesla
  - Pretože hodnota náhodného reťazca (výzvy – challenge) sa pri každej autentifikácii mení, je vylúčený replay attack
  - Autentifikáciu môže ISP kedykoľvek zopakovať, pretože je to práve ISP, ktorý začína autentifikačný dialóg
- Je tu však i istá, skôr teoretická, nevýhoda
  - Pri obojstrannej autentifikácii (klient voči ISP, ISP voči klientovi) je nutné použiť to isté zdieľané heslo

Konfigurácia autentifikácie

PAP autentifikácia



```
Pravy(config)#username Lavy password heslo
Pravy(config)#int serial 1/0
Pravy(config-if)#encapsulation ppp
Pravy(config-if)#ppp authentication pap
```

```
Lavy(config)#int s 1/0
Lavy(config-if)#encapsulation ppp
Lavy(config-if)#ppp pap sent-username Lavy password heslo
```

Pozn. Rozhrania musia mať samozrejme IP adresy a byť aktívne

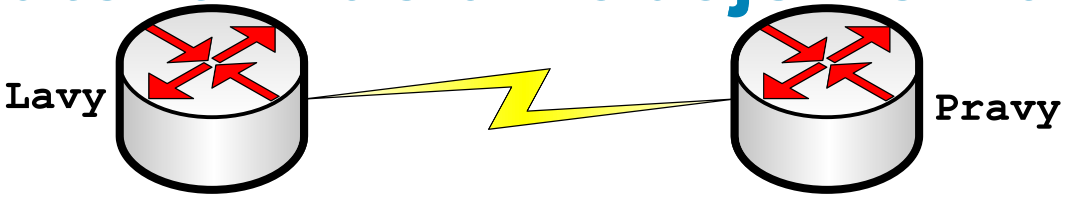
Overenie PPP PAP autentifikácie

```
Lavy#debug ppp authentication
*Mar  1 02:20:15.299: %LINK-3-UPDOWN: Interface Serial1/0, changed state
   to up
…
…]
*Mar  1 02:20:15.315: Se1/0 PPP: Authorization required
*Mar  1 02:20:15.343: Se1/0 PPP: No authorization without authentication
*Mar  1 02:20:15.343: Se1/0 PAP: Using hostname from interface PAP
*Mar  1 02:20:15.343: Se1/0 PAP: Using password from interface PAP
*Mar  1 02:20:15.343: Se1/0 PAP: O AUTH-REQ id 2 len 15 from "Lavy"
*Mar  1 02:20:15.351: Se1/0 PAP: I AUTH-ACK id 2 len 5
*Mar  1 02:20:16.351: %LINEPROTO-5-UPDOWN: Line protocol on Interface
   Serial1/0, change to up
```

Chybná autentifikácia – zlé heslo

```
Lavy#debug ppp authentication
Lavy(config)#conf t
Lavy(config)#int s 1/0
Lavy(config-if)#pap sent-username Lavy password ine_heslo
Lavy(config-if)#shut
Lavy(config-if)#no shut

*Mar  1 02:51:28.027: Se1/0 PPP: Authorization required
*Mar  1 02:51:28.055: Se1/0 PPP: No authorization without authentication
*Mar  1 02:51:28.055: Se1/0 PAP: Using hostname from interface PAP
*Mar  1 02:51:28.059: Se1/0 PAP: Using password from interface PAP
*Mar  1 02:51:28.059: Se1/0 PAP: O AUTH-REQ id 9 len 19 from "lavy"
*Mar  1 02:51:28.087: Se1/0 PAP: I AUTH-NAK id 9 len 26 msg is "Authentication
   failed"
```

PAP autentifikácia - obojsmerná

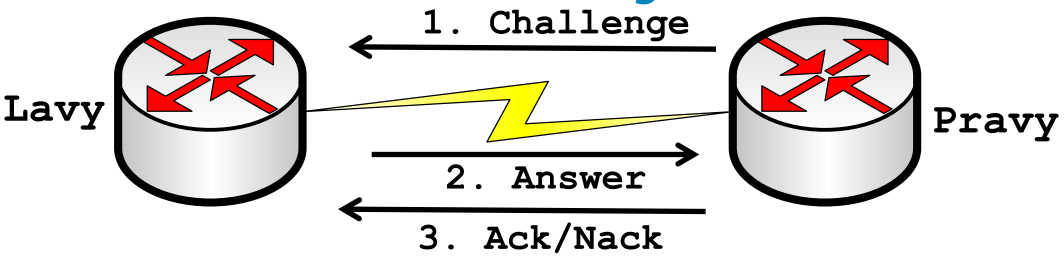


```
Pravy(config)#username Lavy password heslo_2
Pravy(config)#int serial 1/0
Pravy(config-if)#encapsulation ppp
Pravy(config-if)#ppp authentication pap
Pravy(config-if)#ppp pap sent-username Pravy password heslo_1
```

```
Lavy(config)#username Pravy password heslo_1
Lavy(config)#int serial 1/0
Lavy(config-if)#encapsulation ppp
Lavy(config-if)#ppp authentication pap
Lavy(config-if)#ppp pap sent-username Lavy password heslo_2
```

Pozn. Heslo musí byť zhodné na oboch stranách

CHAP autentifikácia - jednosmerná



```
Pravy(config)#username Lavy password heslo
Pravy(config)#int serial 1/0
Pravy(config-if)#encapsulation ppp
Pravy(config-if)#ppp authentication chap
```

```
Lavy(config)#username Pravy password heslo
Lavy(config)#int serial 1/0
Lavy(config-if)#encapsulation ppp
```

Pozn. Heslo musí byť zhodné na oboch stranách

Databázy musia byť naoboch stranách

Overenie PPP CHAP autentifikácie

```
Lavy#debug ppp authentication
Lavy(config)#
*Mar  1 03:04:05.971: Se1/0 PPP: Authorization required
*Mar  1 03:04:05.987: Se1/0 PPP: No authorization without authentication
*Mar  1 03:04:06.011: Se1/0 CHAP: I CHALLENGE id 1 len 26 from "Pravy"
*Mar  1 03:04:06.027: Se1/0 CHAP: Using hostname from unknown source
*Mar  1 03:04:06.027: Se1/0 CHAP: Using password from AAA
*Mar  1 03:04:06.031: Se1/0 CHAP: O RESPONSE id 1 len 25 from "Lavy"
*Mar  1 03:04:06.051: Se1/0 CHAP: I SUCCESS id 1 len 4

Lavy(config)#do sh ip int brief
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            unassigned      YES unset  administratively down down
FastEthernet0/1            unassigned      YES unset  administratively down down
Serial1/0                  1.1.1.1         YES manual up                    up
Serial1/1                  unassigned      YES unset  administratively down down
Serial1/2                  unassigned      YES unset  administratively down down
Serial1/3                  unassigned      YES unset  administratively down down
```

CHAP – neexistuje meno v DB

```
Pravy(config)#username Lavy password heslo
Pravy(config)#int serial 1/0
Pravy(config-if)#encapsulation ppp
Pravy(config-if)#ppp authentication chap
```

```
Lavy#debug ppp auth
PPP authentication debugging is on
Lavy(config)#username Iny_router password heslo
Lavy(config)#int serial 1/0
Lavy(config-if)#encapsulation ppp
Lavy#

*Mar  1 03:34:21.303: Se1/0 PPP: Authorization required
*Mar  1 03:34:21.303: Se1/0 PPP: No authorization without authentication
*Mar  1 03:34:19.303: Se1/0 CHAP: I CHALLENGE id 3 len 26 from "Pravy"
*Mar  1 03:34:19.303: Se1/0 CHAP: Unable to authenticate for peer
*Mar  1 03:34:21.315: Se1/0 PPP: Authorization required
*Mar  1 03:34:21.375: Se1/0 PPP: No authorization without authentication
```

Autentifikácie PAP a CHAP môžeme kombinovať

```
! LEN CHAP
Pravy(config-if)#ppp authentication chap

! LEN PAP
Pravy(config-if)#ppp authentication pap

! VYKONAJ OBE PAP PRVY, POTOM CHAP
Pravy(config-if)#ppp authentication pap chap

! VYKONAJ OBE CHAP PRVY, POTOM PAP
Pravy(config-if)#ppp authentication chap pap
```

Ďalšie zdroje

- Understanding and Configuring PPP CHAP Authentication
  - http://www.cisco.com/c/en/us/support/docs/wan/point-to-point-protocol-ppp/25647-understanding-ppp-chap.html
- Understanding debug ppp negotiation Output
  - http://www.cisco.com/c/en/us/support/docs/wan/point-to-point-protocol-ppp/25440-debug-ppp-negotiation.html
- Configuration Examples and TechNotes
  - http://www.cisco.com/c/en/us/tech/wan/point-to-point-protocol-ppp/tech-configuration-examples-list.html

ĎAKUJEM