Linková vrstva v počítačových sítích

Doc. Karel Burda, CSc.

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Obsah přednášky

Linková vrstva

1. Úvod
2. Ethernetové sítě
3. Virtuální sítě LAN
4. Protokol STP
5. Bezpečnost v ethernetových sítích
6. Závěr

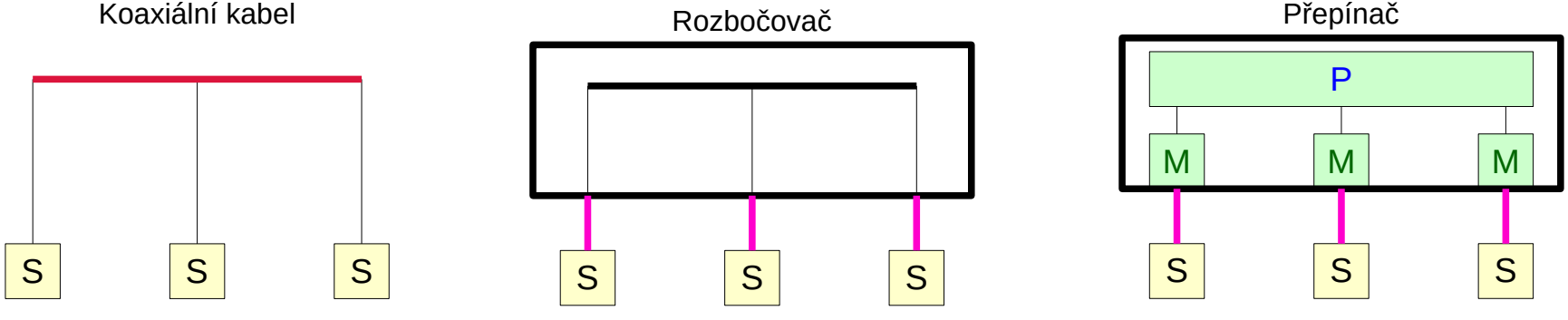
1. Úvod

Linková vrstva

- Datové jednotky protokolů linkové vrstvy budeme nazývat rámce ("frame").
- Protokoly linkové vrstvy kromě samotného přenosu rámců mohou zajišťovat:
  - detekci přenosových chyb,
  - potvrzení o doručení rámce odesílateli,
  - řízení toku (přizpůsobení objemu přenášených dat kapacitě spoje),
  - multiplexování (více nezávislých přenosů dat).
- Linková vrstva využívá služeb fyzické vrstvy (tj. přenos signálových prvků) a poskytuje služby (tj. přenos datových jednotek) síťové vrstvě.
- Existuje řada protokolů pro různé typy spojů nebo různé požadavky.
- Každý linkový protokol je dán strukturou svého rámce a použitými komunikačními a protichybovými technikami.
- Linkové přenosové protokoly v počítačových sítích:
  - pro dvoubodové spoje: PPP (např. mezi směrovači páteřní sítě),
  - pro dvoubodové i vícebodové spoje: IEEE 802.3 (tzv. Ethernet).
- Obsahem přednášky budou protokoly podle IEEE 802.3, protože protokol PPP je již na ústupu.

Vývoj pojmu linková vrstva

- V 80. létech počítače S v jednotlivé lokalitě komunikovaly po koaxiálním kabelu na základě přístupové metody CSMA/CD (obr. vlevo). Tyto lokality byly s jinými lokalitami propojovány IP sítěmi a v architektuře TCP/IP proto byly tyto lokální komunikační systémy (fakticky vícebodový spoj) označovány jako linková vrstva.
- Časem byla koaxiální sběrnice ethernetového spoje nahrazena kabely s kroucenými páry a stanice se připojovaly k rozbočovačům (obr. uprostřed). Stále se však fakticky jednalo o vícebodový spoj s řízením přístupu metodou CSMA/CD.
- Počátkem 90. let se objevily tzv. přepínače, které pomocí pamětí M pro dočasné ukládání rámců změnily vícebodový spoj na ethernetovou síť (obr. vpravo). Každá stanice mohla duplexně komunikovat se svojí pamětí M a procesor P přepínače předával rámce mezi těmito paměťmi. Popsaný vývoj vysvětluje proč jsou ethernetové sítě v architektuře TCP/IP zmatečně označovány jako linka, tj. spoj.



2. Ethernetové sítě

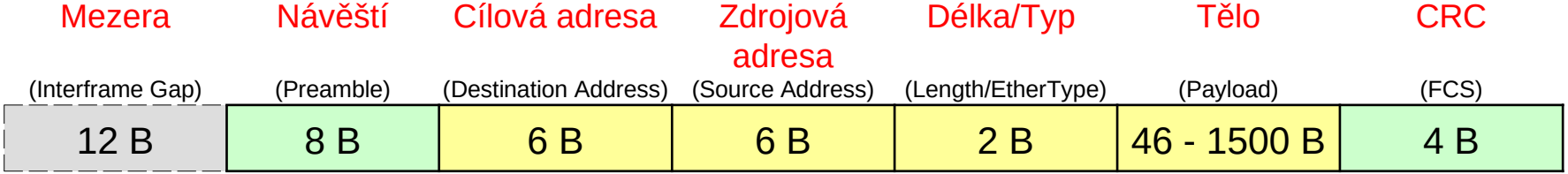
Rámec Ethernet II (1/2)

- V ethernetových spojích se lze setkat s několika typy linkových rámců. Zcela dominujícím je však rámec typu Ethernet II, jehož struktura je uvedena níže.
- Mezera: před zahájením vysílání každého rámce musí vysílací stanice čekat dobu, která odpovídá době přenosu 12 B = 96 bitů. Tato doba dává protistraně čas na zpracování předešlého přeneseného rámce.
- Návěští: vymezuje začátek rámce. Sestává z 8 bajtů v podobě $7\times(10101010)_2 + 1\times(10101011)_2$. V moderních spojích již fakticky není zapotřebí (např. u 100BASE-TX je začátek rámce vymezen ve fyzické vrstvě unikátní dvojicí pětic bitů J a K - viz předchozí přednáška), avšak pole Návěští je stále povinné.
- Adresy: cílová ethernetová adresa CA (tj. příjemce) a zdrojová ethernetová adresa ZA (tj. odesílatel). Podrobněji viz dále.

Mezera (Interframe Gap)	Návěští (Preamble)	Cílová adresa (Destination Address)	Zdrojová adresa (Source Address)	Délka/Typ (Length/EtherType)	Tělo (Payload)	CRC (FCS)
12 B	8 B	6 B	6 B	2 B	46 - 1500 B	4 B

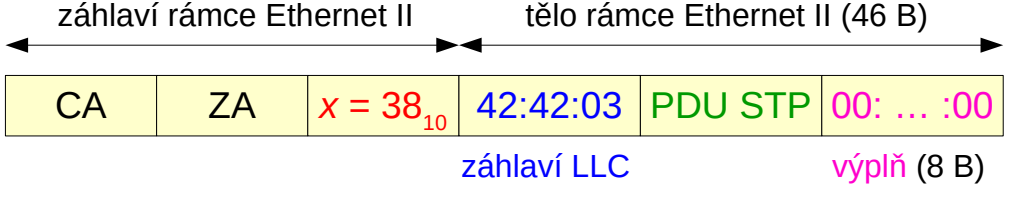
Rámec Ethernet II (2/2)

- Délka/Typ: buď počet platných bajtů v těle rámce, nebo identifikátor protokolu, jehož datová jednotka („Protocol Data Unit“ - PDU) je v těle rámce přenášena.
- Tělo: PDU protokolu, kterému je služba přenosu poskytována (např. IP paket). Minimální délka PDU musí být alespoň 46 B a maximální je obvykle 1500 B (podrobněji viz dále).
- CRC: kontrolní součet rámce vypočítaný cyklickým kódem. V průběhu příjmu přijímací stanice vypočítává vlastní kontrolní součet CRC´. Pokud CRC přijatého rámce je roven CRC´, tak je rámec akceptován a v opačném případě jednoduše ignorován. Protokol Ethernet tedy nezajišťuje spolehlivý přenos.
- Detekci konce rámce opět řeší fyzická vrstva (např. u 100BASE-TX dvě pětice bitů označené T a R).
- Na obrázku žlutě označené části rámce řeší software (linková vrstva operačního systému stanice). Šedou a zelené části má na starosti síťová karta (tj. HW).



Pole Délka/Typ (1/2)

- Pole Délka/Typ obsahuje dvoubajtové číslo x, jehož hodnota určuje význam pole.
- Pokud $x < 0600_{16} = 1536_{10}$, tak přenášená PDU je kratší než 46 bajtů a hodnota x vyjadřuje kolik bajtů v poli Tělo je platných. Za platnými bajty totiž musí být výplňové bajty, aby byla zajištěna minimální délka rámce 64 bajtů pro zaručenou detekci kolize ve vícebodovém ethernetovém spoji s technikou CSMA/CD.
- K určení protokolu, jemuž PDU náleží, se v tomto případě obvykle používá záhlaví LLC („Logical Link Control“). Toto záhlaví tvoří první 3 bajty v poli Tělo a definuje význam dalších bajtů.
- Pokud je například $x = 38_{10}$, tak v těle rámce je 38 bajtů platných dat, přičemž posledních (46−38) = 8 nulových bajtů je výplň. Dejme tomu, že první 3 bajty (tj. záhlaví LLC) mají hodnotu 42:42:03. Ty určují, že zbývajících (38−3) = 35 platných bajtů je datovou jednotkou protokolu STP (viz dále).

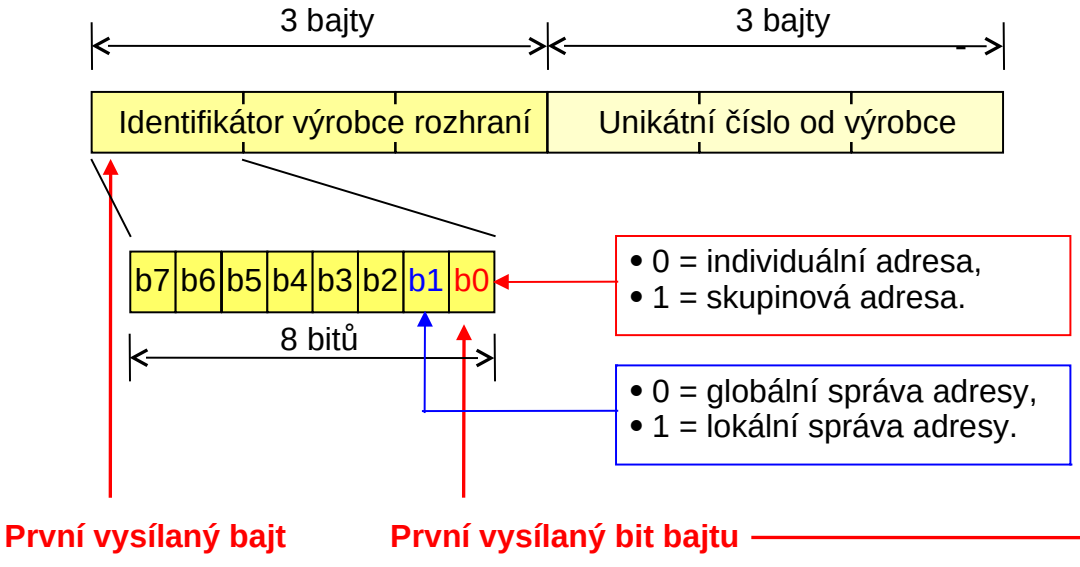


Pole Délka/Typ (2/2)

- Problém maximální délky přenášené PDU (obvykle do 1500 bajtů) řeší protokoly vyšších vrstev, které si zjišťují maximální délku PDU na lince, případně i v přenosové cestě (Path MTU Discovery – viz následující přednáška).
- Poslední instancí je v každém případě IP protokol. Ten případný paket, který se nevejde do těla rámce, rozdělí na více kratších paketů - tzv. fragmentace (viz následující přednáška).
- Pokud pole Délka/Typ obsahuje číslo $x \geq 0600_{16}$, tak toto pole explicitně definuje protokol, jehož PDU jsou v těle rámce přenášeny. Tato varianta je zcela nejčastější.
- Příklady nejpoužívanějších hodnot EtherType:
  - 0800_{16} = IPv4 („Internet Protocol version 4“),
  - $86DD_{16}$ = IPv6 („Internet Protocol version 6“),
  - 0806_{16} = ARP („Address Resolution Protocol“),
  - 0811_{16} = VLAN (rámec virtuální sítě LAN - viz dále).

Struktura adresy podle IEEE 802.3

- Adresy stanic podle IEEE 802.3 (tzv. MAC adresy - „Media Access Control“) mají délku 6 B = 48 bitů.
- Struktura adresy MAC:



Identifikátory vybraných výrobců:
- Novell: 00:00:1B,
- 3Com: 00:20:AF,
- Realtek: 00:E0:4C.

Například bajt:
4C = 01001100

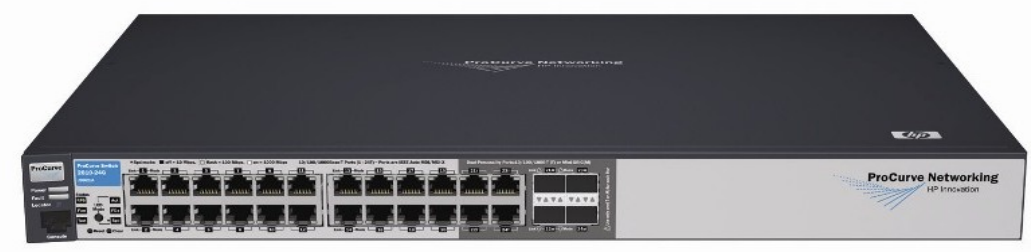
- Na rozdíl od standardů ITU se u standardů IEEE a RFC vysílají bajty podle zápisu zleva doprava, avšak bity každého bajtu se vysílají zprava doleva.

Typy adres podle IEEE 802.3

- MAC adresy lze klasifikovat na individuální, skupinové a globální.
- Individuální adresa ("individual") je adresa, která je v dané ethernetové síti přidělena jedinému zařízení. Může být zdrojová i cílová.
- Skupinová adresa ("multicast") je adresa, která je v dané ethernetové síti přidělena více zařízením. Tyto adresy mohou být pouze cílové. Například skupinovou adresou všech přepínačů v síti je adresa (01:80:C2:00:00:00). Velké množství skupinových MAC adres se také používá k přenosu IP paketů s IP skupinovými adresami. V tomto případě se MAC adresa tvoří tak, že k 01:00:5E se připojí nulový bit následovaný posledními 23 bity IP adresy (tzv. mapování).
- Globální adresa ("broadcast") je adresa s hodnotou (FF:FF:FF:FF:FF:FF). Je rovněž pouze cílová a adresátem jsou v tomto případě všechna zařízení v dané ethernetové síti. Typicky se používá pokud přenášená PDU je IP paket s IP adresou lokálního oběžníku (cílová adresa jsou samé jedničky) nebo ARP dotaz.
- Rámce s cílovými adresami, které nejsou v síťové kartě nastaveny, jsou ignorovány. V moderních kartách však lze MAC adresu karty softwarově měnit. Rovněž ji lze nastavit do tzv. promiskuitního režimu, kdy na vícebodovém spoji karta předává operačnímu systému stanice i rámce adresované jiným stanicím.

Přepínač

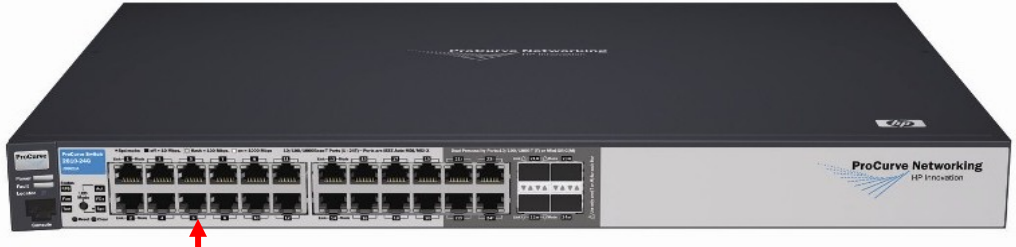
- Přepínač ("switch") je základní síťový prvek linkové vrstvy u standardů IEEE 802.3.
- Má porty (kabelové zásuvky), které umožňují připojování stanic, směrovačů a jiných přepínačů a zajišťuje přepojování přenášených rámců mezi těmito porty.
- Od rozbočovače se liší tím, že mezi porty předává celé rámce - rozbočovač předává mezi porty jen signál. Přepínač rámec přijme, uloží do paměti a následně jej podle jeho cílové adresy odvysílá jen do portů, za nimiž se nacházejí adresáti rámce.
- Jednotlivé porty přepínače nemají vlastní MAC adresy. Pro vzdálenou správu se však přepínači zpravidla přiděluje individuální MAC adresa MAC_P. Jakýkoliv port pak rámec s cílovou adresou MAC_P předává řídící jednotce daného přepínače. Podobně je tomu i u rámců se speciálními skupinovými adresami (např. skupinová adresa přepínačů).



Princip přepínače

- Přepínač si vede tabulku (MAC adresa → číslo portu) obvykle ve velmi rychlé paměti typu CAM („Content Addressable Memory“). Tato přepínací tabulka se nastavuje ručně, nebo si ji přepínač vytvoří automaticky („learning“).
- Automaticky ji sestavuje podle zdrojových adres. Pokud na portu P_X přijme rámec se zdrojovou adresou MAC_{ZA}, tak si vytvoří záznam $MAC_{ZA} \rightarrow P_X$, tj. zařízení s adresou MAC_{ZA} se v síti nachází za portem P_X. Skupinové adresy automaticky nastavit nelze, protože ty nejsou zdrojové. Moderní přepínače to však řeší analýzou údajů z PDU síťové vrstvy (skupinové IP adresy a typy zpráv).
- Záznam se aktualizuje s každým rámcem od stanice s adresou MAC_{ZA}. Záznam, který nebyl za stanovenou dobu (obvykle 5 minut) aktualizován, je vymazán.

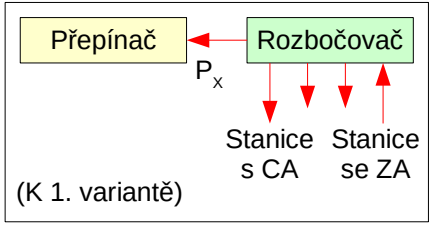
Přepínací tabulka:
...
...
$MAC_{ZA} \rightarrow P_X$
...



NÁVĚŠTÍ	MAC_{CA}	MAC_{ZA}	TYP	TĚLO	CRC

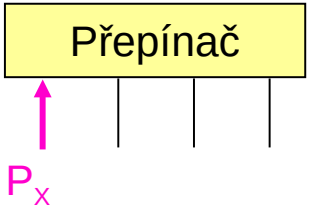
Fungování přepínače

- Předpokládejme, že na portu P_X byl přijat rámec s cílovou adresou CA a zdrojovou adresou ZA.
- Adresa ZA je použita k aktualizaci přepínací tabulky (ZA → P_X).

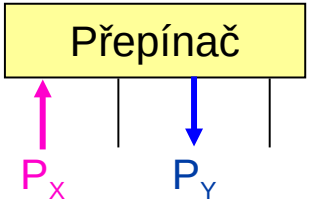


- Adresa CA je použita k rozhodnutí podle následujícího algoritmu:
  1. CA je individuální a je zapsána u portu P_X, odkud byl rámec přijat? => Ignorovat. Přenos byl již uskutečněn ve vícebodovém spoji, který je k tomuto portu připojen.
  2. CA je individuální a je zapsána na portu $P_Y \neq P_X$? => Předat do P_Y.
  3. CA je skupinová a uvedena v tabulce? => Rozeslat do určených portů kromě P_X.
  4. Jinak? (Tj. buď je CA globální, nebo není v přepínací tabulce) => Rozeslat do všech portů kromě P_X.

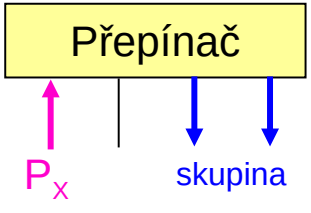
1.
CA psána u P_X



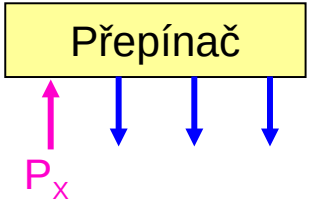
2.
CA psána u P_Y



3.
Skupinová CA

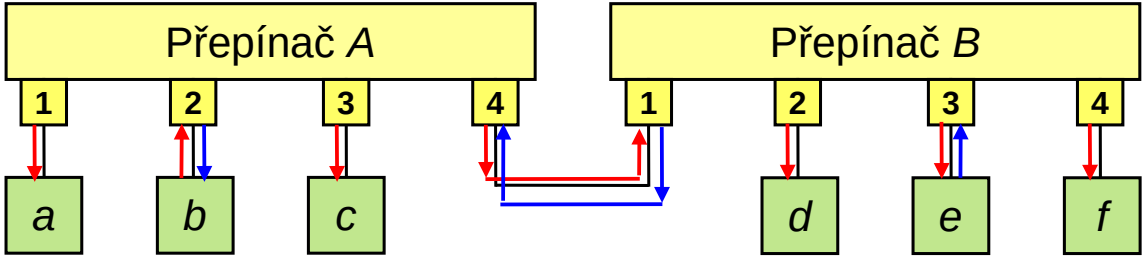


4.
Jinak



Vytváření přepínací tabulky prakticky

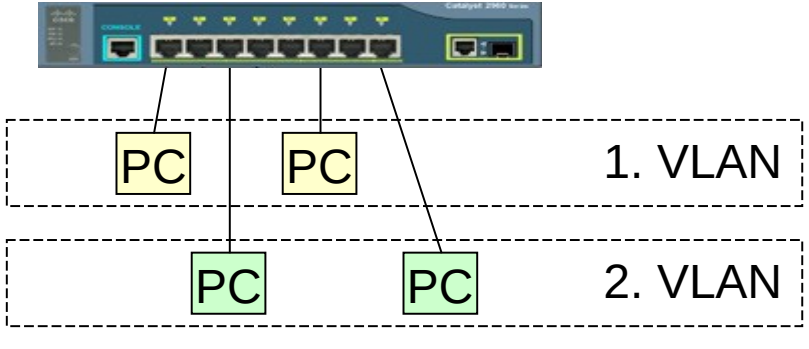
- Přepínací tabulky se zpravidla vytvářejí na základě protokolu ARP (viz následující přednáška). Předpokládejme, že oba přepínače na obrázku neznají žádné adresy.
- Dejme tomu, že stanice *b* vyslala ARP dotaz, v němž se dotazuje na MAC adresu stanice s IP adresou IP_e, což je stanice *e*. ARP dotazy mají globální cílovou MAC adresu a unikátní zdrojovou MAC adresu odesílatele. Přepínač *A* si aktualizuje tabulku o záznam ($MAC_b \rightarrow A2$) a daný rámec rozešle do všech ostatních portů.
- Přes port *A*4 se rámec dostane na *B*1, tj. na přepínač *B*. Přepínač *B* si aktualizuje tabulku o záznam ($MAC_b \rightarrow B1$) a rámec rozešle do všech svých ostatních portů.
- Stanice *e* odpoví stanici *b* zprávou ARP odpověď, která bude v rámci s cílovou adresou MAC_b (zná z dotazu) a s vlastní zdrojovou adresou MAC_e. *B* si nyní aktualizuje ($MAC_e \rightarrow B3$) a rámec podle přepínací tabulky přepne do portu *B*1.
- Přepínač *A* tento rámec obdrží přes port *A*4, podle zdrojové adresy si aktualizuje svoji tabulku ($MAC_e \rightarrow A4$) a rámec přepne do portu *A*2.
- Další komunikace mezi *b* a *e* pak již probíhá bez všesměrového přepínání.



3. Virtuální sítě LAN

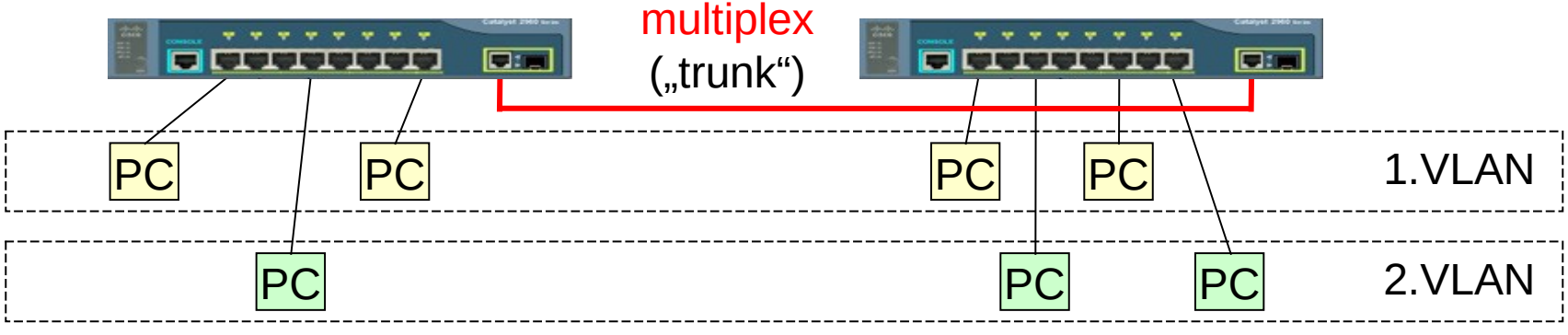
Virtuální LAN

- Virtuální síť LAN (VLAN) je síť, která vznikne logickým oddělením skupiny stanic od ostatních stanic ethernetové sítě. Logické oddělení stanic zajišťují přepínače.
- Na přepínači správce sítě nakonfiguruje informace, mezi kterými porty lze rámce přepínat. Tím se dosáhne toho, že stanice dané skupiny si mohou vyměňovat jen rámce mezi sebou. Na obrázku vidíme, že přepínač bude přepínat rámce jen mezi porty číslo 1 a 6 (1. VLAN) a mezi 3 a 8 (2. VLAN).
- Komunikaci mezi stanicemi různých sítí VLAN zajišťuje až síťová vrstva pomocí směrovačů nebo L3 přepínačů.
- Výhodami sítí VLAN je:
  - vyšší bezpečnost (stanice jedné VLAN může útočit jen na stanice téže VLAN),
  - menší zatížení sítě (rámce s globální adresou jsou rozesílány jen v příslušné VLAN).



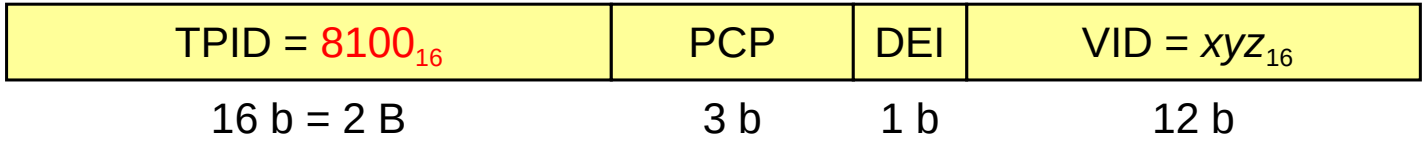
Síť VLAN na více přepínačích

- Pokud jsou virtuální sítě organizovány na více přepínačích, tak je zapotřebí mezi přepínači spolu s rámcem přenášet i informaci o tom, do které sítě VLAN daný rámec náleží.
- Spoje mezi přepínači je zapotřebí nakonfigurovat jako tzv. multiplexy („trunk“). V tomto případě se ve spoji přenášejí i informace o příslušnosti rámce ke konkrétní VLAN v tzv. značkách („tag“). Standard pro VLAN je IEEE 802.1Q.
- Značkování rámců se ukázalo být velmi životaschopnou technikou. S dalšími typy značek se seznámíme v poslední přednášce věnované perspektivám sítí.



Značka podle IEEE 802.1Q

- Značka má délku 4 bajty. Sestává z následujících polí.
- TPID („Tag Protocol Identifier“): identifikátor typu značky. Ve standardech IEEE 802.3 je definováno více typů značek. Pro VLAN je stanovena hodnota 8100_{16}.
- PCP („Priority code point“): kód priority rámce o délce 3 bity. Hodnota 0 reprezentuje nejnižší prioritu a 7 nejvyšší prioritu. Toto pole umožňuje řešit kvalitu služeb (QoS) na linkové vrstvě.
- DEI („Drop eligible indicator“): bit, který síťovým zařízením indikuje, že v případě přetížení sítě mohou rámce dané VLAN zlikvidovat (DEI = 1).
- VID („VLAN identifier“): 12 bitů, které identifikují síť VLAN.
- Lze definovat $2^{12}-2 = 4094$ sítí VLAN. Hodnota 000_{16} indikuje, že účelem značky je řešit jen priority (využívá se pole PCP). Hodnota FFF_{16} se nesmí přenášet a používá se pouze při správě, kdy reprezentuje všechny sítě VLAN.



Rámec podle IEEE 802.1Q

- Původní rámec vyslaný počítačem:

Návěští	Cílová adresa	Zdrojová adresa	Typ	Tělo	CRC

- Značka VLAN se v ethernetovém rámci umísťuje za zdrojovou adresu.
- Rámec přenášený mezi přepínači (tj. ve spoji typu multiplex):

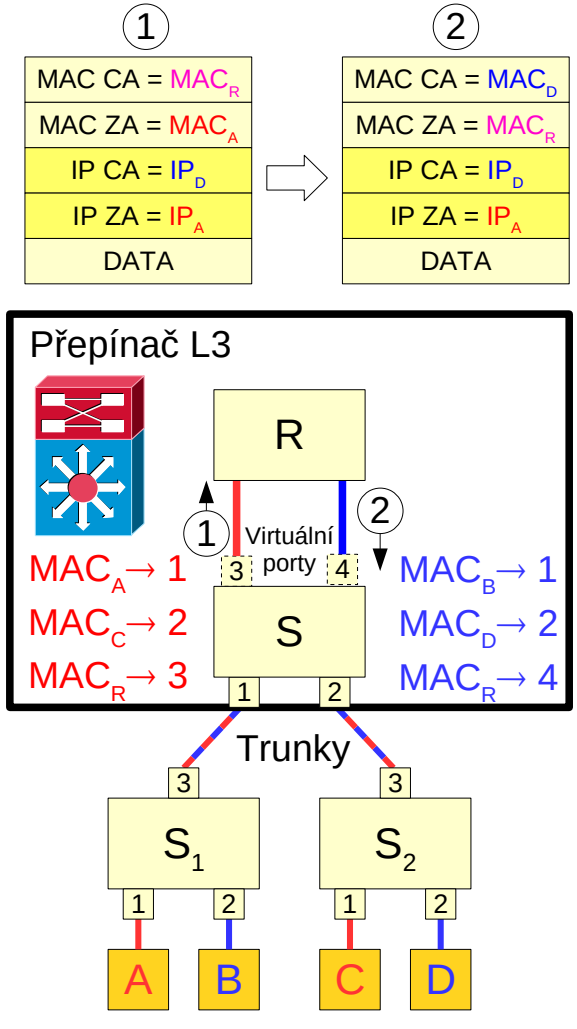
Návěští	Cílová adresa	Zdrojová adresa	Značka (zejména VID)	Typ	Tělo	CRC (upraveno)

- Logické oddělení virtuálních sítí na spojích mezi přepínači se dosahuje rozlišováním rámců podle hodnoty VID.

- Nevýhodou techniky značkování je nutnost přepočítávat kontrolní součty CRC rámců.

Přepínač L3

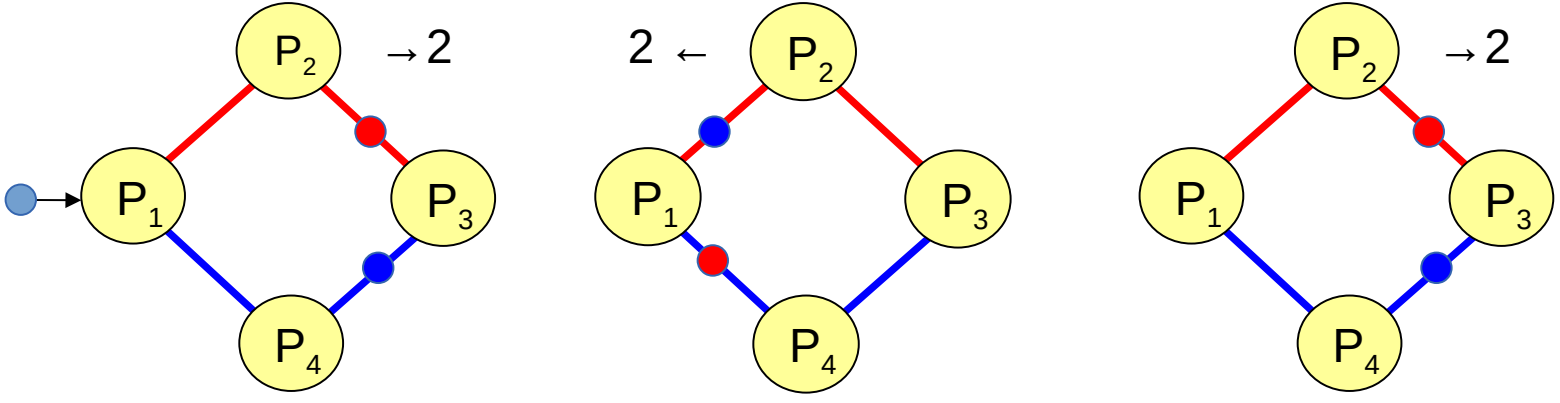
- Přepínač L3 je kombinace přepínače (S) a směrovače (R) s rychlými obvody ASIC.
- Přepínač L3 je primárně určen ke směrování mezi subsítěmi, které jsou definovány nad sítěmi VLAN.
- Kvůli přepínači S jsou porty L3 (na obr. porty 1 a 2) výhradně typu Ethernet.
- Příklad:
  - Mějme VLAN1 (pro počítače A a C) a VLAN2 (pro počítače B a D).
  - Nad VLAN1 je definována subsíť s IP adresou 192.168.1.0/24 a nad VLAN2 je subsíť s adresou 192.168.2.0/24.
  - Přepínače S, S_1 a S_2 přepínají rámce mezi zařízeními VLAN1 i mezi zařízeními VLAN2.
  - Směrovač R přenáší pakety mezi VLAN1 a VLAN2. Když stanice podle cílové IP adresy zjistí, že jej má odeslat do jiné IP sítě (tj. do jiné VLAN), tak paket vkládá do rámce, jehož cílová MAC adresa je adresa L3 přepínače.



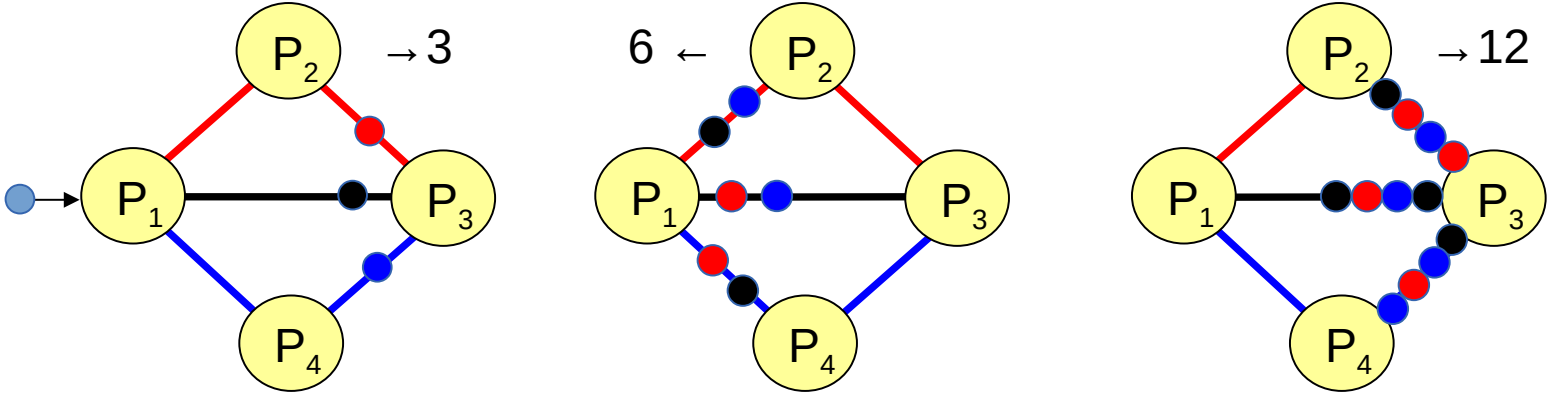
4. Protokol STP

Problém smyček

- Smyčka v síti Ethernet způsobí, že všesměrové rámce (kroužky) v síti přetrvávají.



- Více smyček způsobí exponenciální růst počtu všesměrových rámců.



Řešení problému smyček

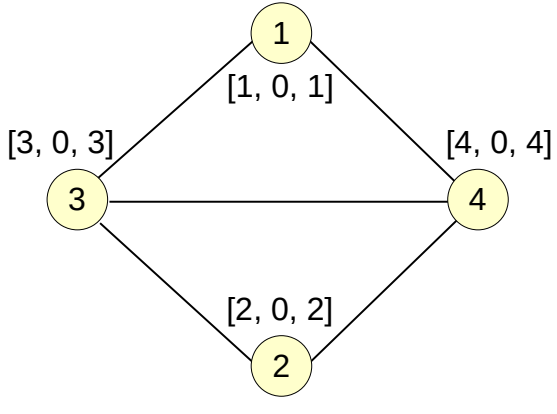
- V roce 1998 byl publikován standard IEEE 802.1D-1990, který definoval protokol STP („Spanning Tree Protocol“).
- Protokol STP umožňuje přepínačům, které jsou topologicky propojeny do libovolného souvislého grafu, sjednat společný strom, což je podgraf dané sítě bez smyček. Spoje, které do tohoto stromu nepatří, jsou pak na portech přepínačů pro běžný provoz zablokovány.
- V roce 2001 se objevil standard IEEE 802.1w, který definuje protokol Rapid STP (RSTP). Protokol RSTP umožňuje rychlejší adaptaci na změny struktury sítě (z desítek sekund pod 2 sekundy).
- Nevýhodou protokolů STP a RSTP je, že spoje nezařazené do stromu nejsou využity a uplatní se jen v případu výpadku některého se spojů stromu.
- V roce 2002 proto byl publikován standard IEEE 802.1s, který aplikuje protokol STP na několik sítí VLAN současně („Multiple STP“ – MSTP).
- Principem MSTP je, že na jedné fyzické síti Ethernet je definováno více sítí VLAN a pro každou z nich se pomocí protokolu STP určuje její strom. Vzniklé stromy jsou obecně různé a tak každý spoj sítě může být součástí alespoň jedné VLAN. Tím se dosáhne využití všech spojů v naší síti.

Protokol STP (1/5)

- STP (Spanning Tree Protocol, IEEE 802.1D): protokol, kterým se v redundantní ethernetové síti určuje přenosová kostra (souvislý podgraf sítě bez smyček).
- Následující popis je jen zjednodušený. Zejména předpokládáme, že každá dvojice přepínačů je propojena pouze jedním spojem.
- Přepínače mají určeno unikátní identifikační číslo ID. Kostra je konstruována na principu postupného připojování spojů a přepínačů k tzv. kořeni (k přepínači s nejnižším ID). Kritériem pro připojování je nejkratší cesta ke kořeni. V případě více nejkratších cest mají přednost přepínače s nejmenším ID.
- Přepínače budeme v dalším nazývat uzly. Každý uzel X má unikátní identifikátor ID(X). Uzel K s nejmenší hodnotou ID nazveme kořen.
- Vzdálenost uzlu X ke kořeni K označíme L(X). Je to počet hran na nejkratší cestě mezi X a K.
- Uzly periodicky (zpravidla po 2 s) do všech svých portů (i blokovaných) vysílají rámce se skupinovou cílovou MAC adresou 01:80:C2:00:00:00 (skupinová adresa přepínačů), v nichž se nachází STP zpráva.
- STP zprávu vyslanou uzlem X označíme Z(X) = [R(X), L(X), ID(X)], kde R(X) je nejmenší ID, které je uzlu X známo.

Protokol STP (2/5)

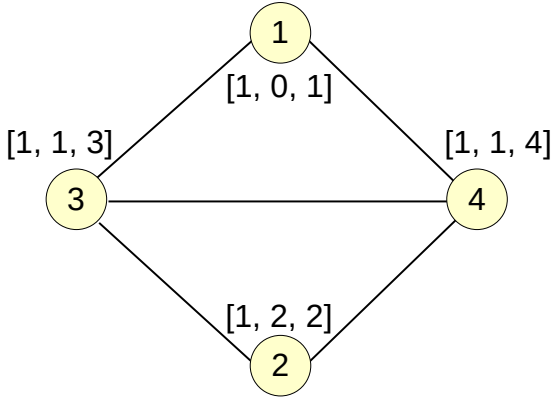
- Na počátku každý uzel X vyšle všem svým sousedům zprávu [X, 0, X]. Příklad je na obr. vlevo.
- Každý uzel X ze své a z přijatých zpráv nalezne zprávu Z(Y), jejíž R(Y) je nejmenší ze všech. Pokud R(Y) = X, tak nová zpráva uzlu X bude opět [X, 0, X]. V opačném případě bude nová zpráva Z(X) = [R(Y), L(Y)+1, ID(X)]. Uzel tak informuje své sousedy o existenci uzlu Y s nejmenším jemu známým ID a o vzdálenosti, kterou k němu má. Informace o kořeni se tak postupně šíří sítí.
- Například ve 3. uzlu jsou následující zprávy: vyslaná [3, 0, 3] a přijaté [1, 0, 1], [2, 0, 2] a [4, 0, 4]. Nejmenší R(Y) = 1 (je ze zprávy od 1. uzlu) a tak nová zpráva 3. uzlu bude Z(3) = [R(1), L(1)+1, ID(3)] = [1, 1, 3]. Nové zprávy od všech uzlů vidíme v tabulce vpravo.



Uzel	Zprávy v uzlu	Nová zpráva
1. uzel	[1, 0, 1], [3, 0, 3], [4, 0, 4]	[1, 0, 1]
2. uzel	[2, 0, 2], [3, 0, 3], [4, 0, 4]	[2, 0, 2]
3. uzel	[1, 0, 1], [2, 0, 2], [3, 0, 3], [4, 0, 4]	[1, 1, 3]
4. uzel	[1, 0, 1], [2, 0, 2], [3, 0, 3], [4, 0, 4]	[1, 1, 4]

Protokol STP (3/5)

- Po několika vysíláních se všechny uzly dozví o kořeni K a zprávy se již přestanou měnit. Kořen K bude opakovaně vysílat [K, 0, K] a ostatní uzly X budou vysílat Z(X) = [K, L(X), ID(X)]. Pro náš příklad vidíme ustálený stav sítě na obr. vlevo.
- Na základě zpráv vyměňovaných se sousedy si každý nekořenový uzel X může určit svého předka Y. Je jím uzel, který je o jeden spoj blíže na cestě z X ke kořeni. Pokud má takovouto vlastnost více uzlů, tak předkem je z nich uzel s nejmenším ID. Uzel X zároveň nazveme potomek uzlu Y.
- Například předek uzlu 2 je uzel 3. Stejnou vzdálenost ke kořeni má sice i další soused, kterým je uzel 4, ale ID(4) je větší než ID(3). Viz tabulka vpravo.

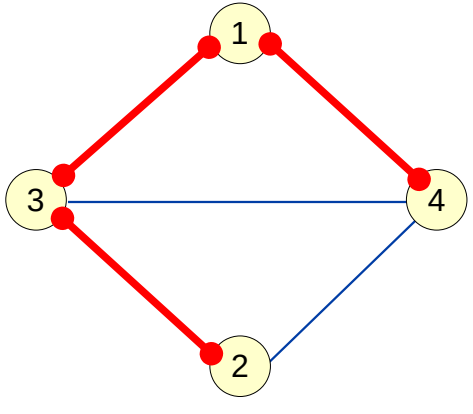


Potomek	Předek
1	-
2	3
3	1
4	1

Protokol STP (4/5)

- Pokud nyní všechny předky propojíme s jejich potomky, tak získáme kostru grafu, kterou známe z teorie grafů (červeně na obr. dole). Kolečko na konci čáry vyjadřuje, že příslušný port přepínače předává rámce mezi spojem a tímto přepínačem, tj. provoz mezi přepínačem a připojeným spojem neblokuje.
- V naší síti ještě musíme k této kostře připojit zbývající spoje grafu (modré). Na obrázku se jedná o spoje (3, 4) a (2, 4). Každý spoj mezi přepínači totiž může být obecně vícebodový spoj (např. může obsahovat rozbočovače). Tyto spoje však musíme připojit jednostranně, aby nevznikly smyčky. Jednostranně připojené spoje nazveme pahýly.
- Otázkou je, ke kterému uzlu (tj. předkovi) který pahýl připojit.

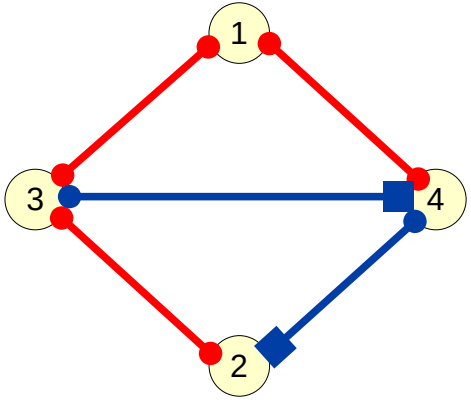
Potomek	Předek
1	-
2	3
3	1
4	1



Protokol STP (5/5)

- Pokud pro pahýl mezi uzlem X a W platí, že L(X) < L(W), tak jej do kostry připojíme přes uzel X, tj. pahýl připojujeme k uzlu s kratší cestou ke kořeni. V našem příkladu platí u pahýlu (2, 4), že L(4) < L(2), takže pahýl bude do kostry připojen přes uzel 4. V uzlu 2 bude port zablokován (obdélník na konci čáry), tj. v tomto portu nebudou přenášeny rámce ze spoje do přepínače a naopak.
- Zbývající možností je, že L(X) = L(W), tj. oba uzly mají ke kořeni stejnou vzdálenost - případ pahýlu (3, 4). V tomto případě se pahýl připojuje přes uzel s menším ID.
- Tím byla vytvořena kostra grafu. V případě výpadku, či přidání některého ze spojů, či uzlů se popsaný postup opakuje.

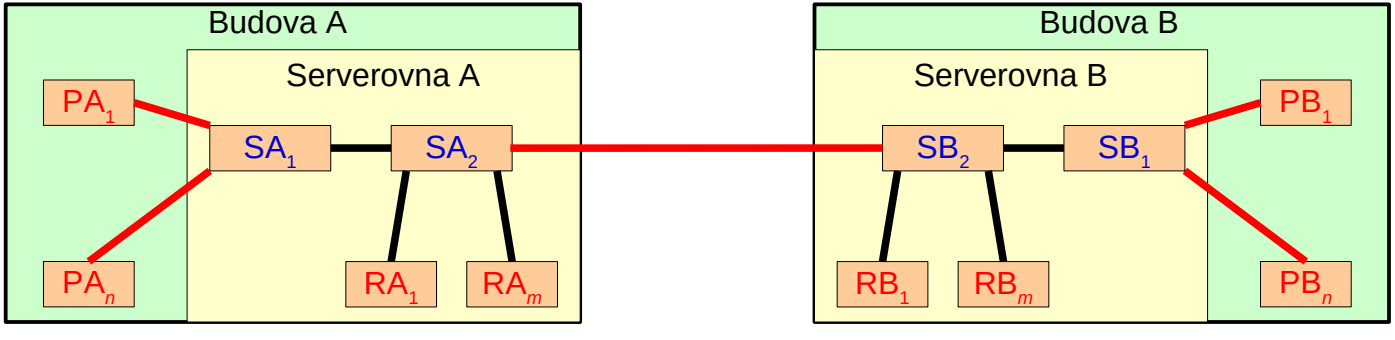
Potomek	Předek
1	-
2	3
3	1
4	1



5. Bezpečnost v ethernetových sítích

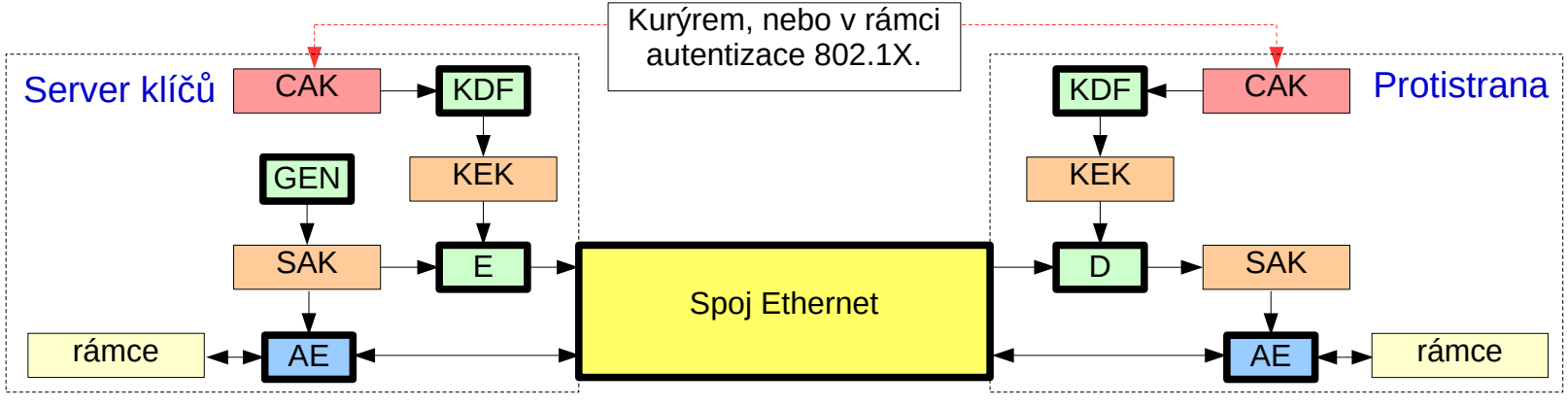
Kryptografické zabezpečení ethernetových sítí

- Kryptografické zabezpečení ethernetových rámců definuje standard IEEE 802.1AE (tzv. MACsec). Pozn.: U standardů IEEE je zapotřebí rozlišovat i velikost písmen.
- Rámce jsou šifrovány a autentizovány ve spojích mezi sousedícími zařízeními (na obrázku červeně). V přepínačích (SA a SB) jsou tedy rámce v nezašifrované podobě.
- Spoje typu MACsec je výhodné použít zejména v dálkových spojích (např. mezi budovami) a také v přístupových spojích, jimiž se připojují uživatelské stanice (PA a PB) do LAN. Uvedené spoje jsou ohroženy nejvíce.
- Spoje mezi ostatními síťovými zařízeními (např. přepínači, servery RA a RB) jsou vedeny obvykle v kontrolovaných prostorech (např. v serverovně) a útočníci k těmto spojům nemají fyzicky přístup.



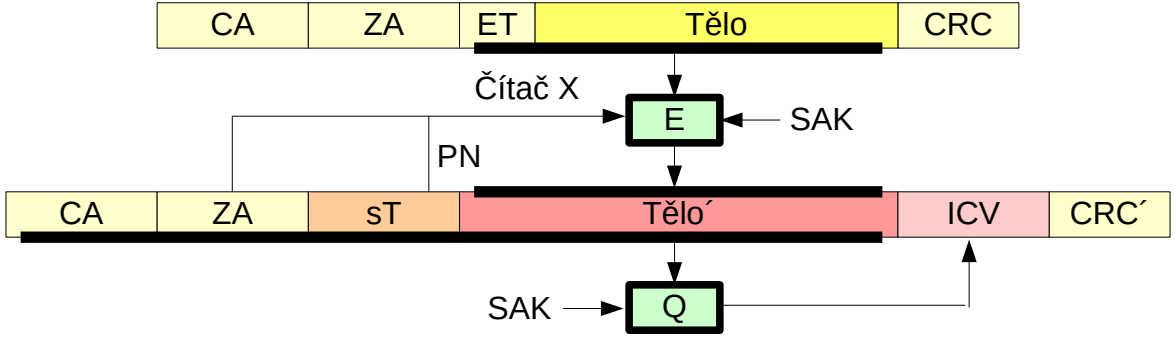
MACsec – správa klíčů

- Hlavním klíčem pro dvojici zařízení na daném spoji je připojovací klíč CAK. Pro spojení mezi síťovými zařízeními je klíč CAK přednastavený ručně. U uživatelských stanic se odvozuje v průběhu autentizace uživatele (standard IEEE 802.1X - viz 9. přednáška).
- Z klíče CAK se pomocí jednosměrné funkce KDF odvodí distribuční klíč KEK = KDF(CAK). Klíč KEK slouží k šifrovanému přenosu provozních klíčů SAK.
- Jedno ze zařízení na daném spoji je tzv. serverem klíčů. Tento server podle potřeby generuje (GEN) nové klíče SAK a protistraně je předává zašifrované pomocí klíče KEK, tj. předává se kryptogram C = E(SAK, KEK).
- Klíčem SAK jsou šifrovány a autentizovány (funkce AE) přenášené rámce.



Struktura rámce MACsec

- Původní rámec: CA a ZA = cílová a zdrojová MAC adresa, ET = EtherType, Tělo = data, CRC = kontrolní součet rámce.
- Zabezpečený rámec: CA a ZA = cílová a zdrojová MAC adresa, sT = secTAG (viz dále), Tělo´ = zašifrovaná data mezi ZA a CRC původního rámce, ICV = pečeť zabezpečeného rámce, CRC´ = kontrolní součet zabezpečeného rámce.
- secTAG: pole o délce 8B. Obsahuje identifikátor protokolu MACsec = $88E5_{16}$, 2B služebních bitů (příznaky) a 4B pořadového čísla rámce PN.

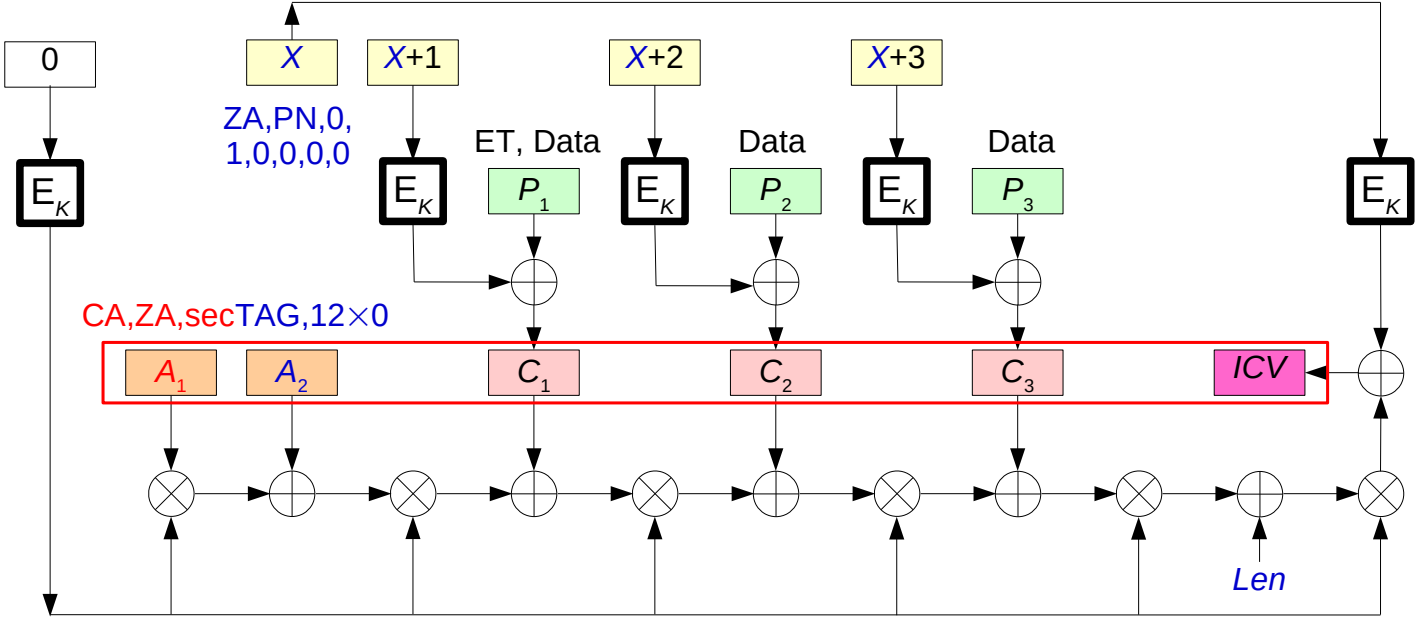


Provoz GCM

- V IEEE 802.1AH je zatím standardizován jediný druh provozu, kterým je GCM-AES-128. Jedná se o provoz typu GCM prostřednictvím blokové šifry AES o délce klíče 128 bitů.
- Provoz GCM je kombinace autentizačního provozu GMAC („Galois Message Authentication Mode“) a utajovacího provozu CTR („Counter Mode“).
- Výhodou tohoto provozu je vysoká rychlost na běžném HW a jednodušší správa klíčů. K šifrování i pečetění se totiž používá jeden a tentýž klíč (SAK).
- Unikát, kterým se individualizuje zabezpečení *i*-tého rámce, je jeho pořadové číslo PN_i. Jedná se o 32 bitů dlouhé číslo, které se uvádí v poli secTAG.
- Hodnotu PN_i příjemce nejprve porovná s číslem PN_{i-1} předešlého rámce, přičemž musí platit, že $PN_i > PN_{i-1}$. Tato kontrola znemožňuje útok opakováním dříve odeslaných rámců.
- PN se také používá k odvození hodnoty čítače pro provoz CTR. Po vyčerpání všech 2^{32} hodnot se hodnota PN vynuluje a změní se klíč SAK.

Provoz GCM-AES-128 pro nejkratší možný rámec (1/2)

- Výchozí rámec (64B): CA (6B), ZA (6B), ET (2B), Data (46B), CRC (4B).
- Výsledný rámec (88B): CA, ZA, secTAG (8B), zašifrovaná ET a Data (48B), ICV (16B), CRC´(4B).
- Klíč *K* = SAK. Násobení (⊗) se provádí v konečném tělese GF(2^{128}).



- Pozn.: Zkratky jsou vysvětleny na následujícím snímku.

Provoz GCM-AES-128 pro nejkratší možný rámec (2/2)

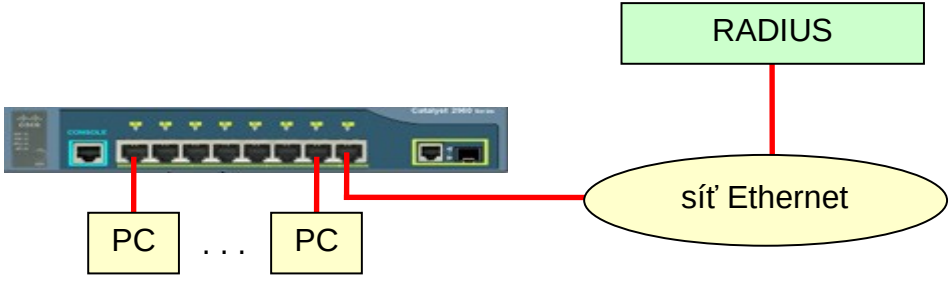
- Výchozí rámec (64B): CA (6B), ZA (6B), ET (2B), Data (46B), CRC (4B). kde CA = cílová adresa, ZA = zdrojová adresa, ET = EtherType, Data = tělo rámce, CRC = kontrolní součet rámce.
- Výsledný rámec (88B): CA, ZA, sT (8B), zašifrovaná ET a Data (48B), ICV (16B), CRC´(4B), kde sT = secTAG, ICV = pečeť a CRC´ = nový kontrolní součet rámce.
- A_1 = první blok autentizovaných dat = CA ‖ SA ‖ (první 4B z sT).
- A_2 = druhý blok autentizovaných dat = zbývající 4B z sT a 12 nulových bajtů výplně. Výplňové bajty se nepřenáší.
- P_1 = první šifrovaný blok = ET ‖ (prvních 14B z Data).
- P_2 / P_3 = druhý / třetí šifrovaný blok = 16B z Data.
- C_1 / C_2 / C_3 = první / druhý / třetí zašifrovaný blok.
- sT = $88E5_{16}$ ‖ 2B příznaků ‖ 4B PN (pořadové číslo rámce).
- X = čítač = 6B ZA ‖ 4B PN ‖ 0001_{16} ‖ 4 nulové bajty. Poslední nulové bajty se postupně inkrementují.
- Len = délka autentizovaných dat (20B = 160b) ‖ délka zašifrovaných dat (48B = 384b), tj. Len = 160 ‖ 384. Každá z délek je přitom vyjádřena 8 bajty.

Bezpečnost v sítích Ethernet - přepínače

- Asi nejznámější je útok přetečením paměti přepínače ("MAC flooding").
- Pokud je útočník připojen k nějakému portu přepínače, tak může sledovat pouze rámce vysílané, nebo adresované do spoje na daném portu.
- Aby útočník mohl monitorovat provoz v celé síti, tak se může pokusit o převedení přepínače do všesměrového provozu tzv. útokem přetečením paměti přepínače.
- Přepínač si vede přepínací tabulku (MAC adresa - číslo portu). Útočník vysílá na svém portu sérii rámců s různými MAC adresami. Přepínač tak musí aktualizovat svoji přepínací tabulku až do doby, kdy vyčerpá přidělenou paměťovou kapacitu. Od toho okamžiku některé přepínače začnou vysílat rámce všesměrově, tj. přijaté rámce vysílají do všech portů.
- Útočník tímto způsobem do spoje ve svém portu soustředí veškeré rámce zpracovávané daným přepínačem.
- Ochrana spočívá v tom. že moderní přepínače dovolují na svých portech přednastavit povolené zdrojové MAC adresy, nebo dovolují zablokovat port, ze kterého přicházejí rámce s více zdrojovými MAC adresami, než je nastaveno.

Bezpečnost v sítích Ethernet - řízení přístupu

- Před útokem připojením cizího počítače na port přepínače slouží funkce autentizace uživatele podle IEEE 802.1X (viz 9. přednáška).
- V tomto případě součástí sítě musí být autentizační server RADIUS, který obsahuje uživatelská jména (Log) a hesla (Psw) všech uživatelů sítě.
- Jakmile počítač (PC) po svém zapnutí provede nějakou síťovou aktivitu (např. požádá o přidělení IP adresy), tak jej přepínač vyzve k autentizaci.
- Počítač zašle své jméno a heslo, které přepínač zašifruje a odešle ke kontrole serveru RADIUS. Ten provede ověření. V kladném případě povolí připojení PC do sítě. V opačném případě je port zablokován.
- Autentizační komunikace se uskutečňuje protokolem „EAP over LAN“ ("Extensible Authentication Protocol over LAN"). Pole EtherType má v tomto případě hodnotu $888E_{16}$.



6. Závěr

Shrnutí

- Linková vrstva zajišťuje přenos rámců spojem.
- Často řeší i opravy chyb, potvrzení o doručení, řízení toku a multiplexování protokolů.
- Na dvoubodových spojích (spoje WAN nebo spoje k poskytovatelům internetu) se používá často protokol PPP.
- Ve vícebodových, ale i dvoubodových kabelových spojích lokálních sítí se používá protokol podle standardu IEEE 802.3.
- Opravy chyb a řízení toku jsou v obou těchto protokolech jen na minimální úrovni (detekce chyby => ignorování rámce, není dostatek paměti => ignorování rámce). O spolehlivý přenos se musejí postarat vyšší vrstvy.
- Všeobecně je bezpečnost linkové vrstvy na nízké úrovni. Vyšší úroveň bezpečnosti musí zajistit podřízená, nebo nadřízené vrstvy. Výjimkou jsou moderní bezdrátové sítě (IEEE 802.11 = WLAN), kde je bezpečnost na dobré úrovni (protokol WPA2). U standardů Ethernet je perspektivní kryptografické zabezpečení podle IEEE 802.1AE (protokol MACsec).

Orientace

Témata pro přípravu ke zkoušce:

1. Přenosy podle IEEE 802.3 (Struktura rámce Ethernet II. Struktura MAC adresy. Fungování přepínače.)
2. Sítě VLAN (Princip a výhody VLAN. Rámec podle IEEE 802.1Q. Fungování přepínače L3.)
3. Protokol STP (Účel. Popis fungování.)
4. Protokol MACsec (Použití. Správa klíčů. Struktura rámce MACsec.)