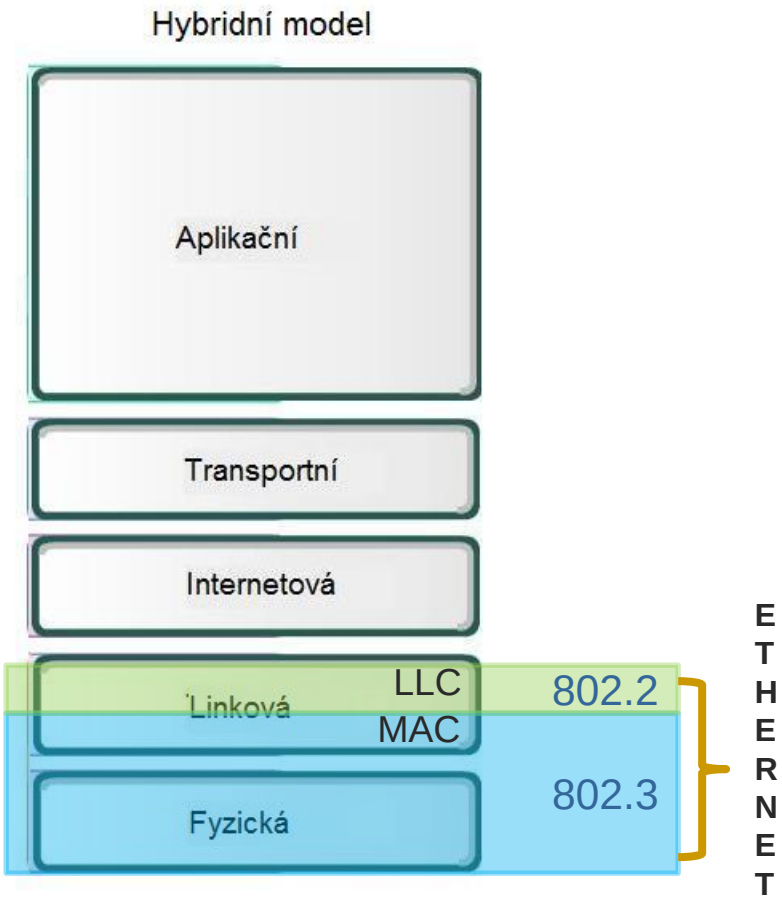
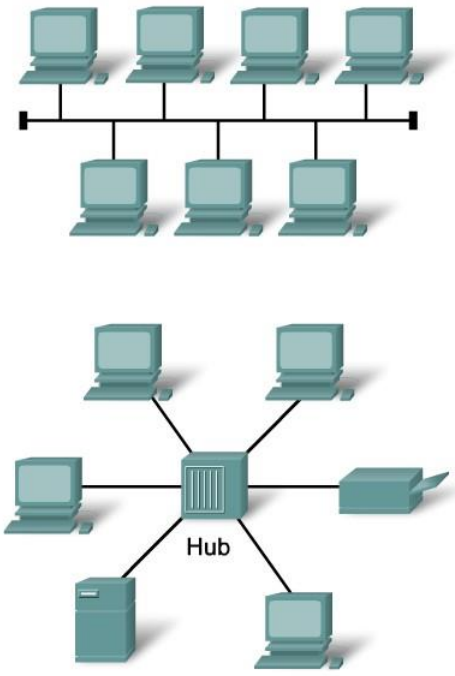
Linková vrstva

- Přístup ke sdílen. médiu.
- Přepínač
  - Popis, princip.
  - Přepínací tabulka.
- Základy VLAN.
- IEEE 802.1x
- Homeplug / PLC.
- WAN technologie na L2.
  - MPLS.
  - Metro (Carrier) Ethernet.
  - (A)DSL.



Přístup ke sdílenému médiu. Naučit se!

1. CSMA/CD.
    1. Princip.
    2. Kde se používá.
2. CSMA/CA.
    1. Princip.
    2. Kde se používá.
3. CSMA/CD vs. CSMA/CA.
4. Základní literatura!

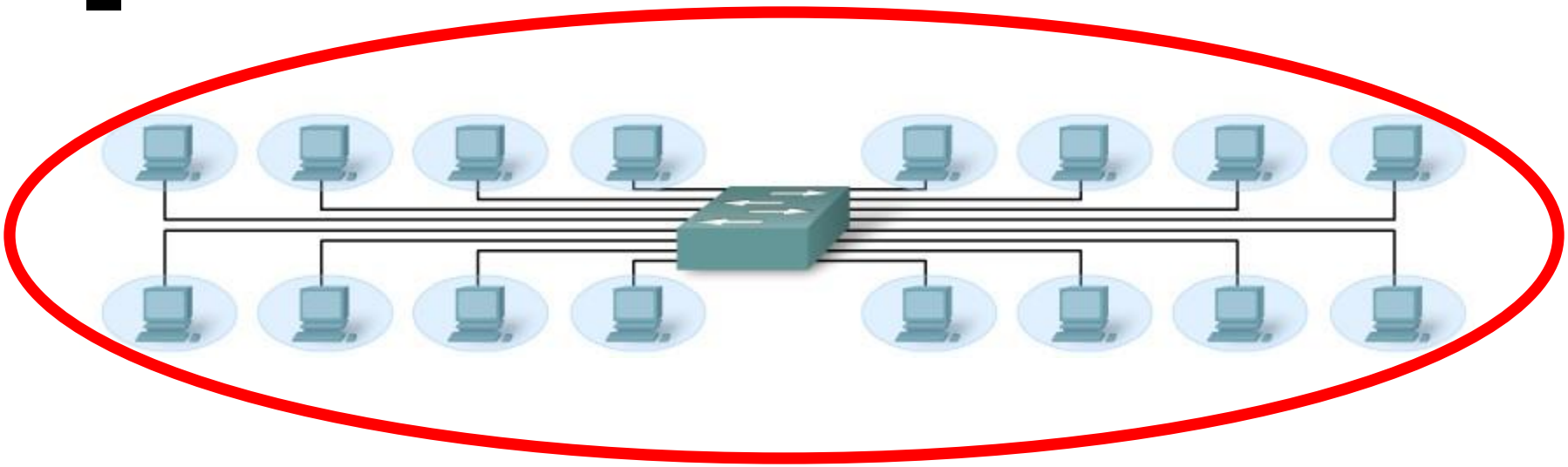


VÝVOJ

Přepínač (Switch)

- Typické zařízení druhé vrstvy.
- Částečně ulehčuje práci síťové kartě (a tím pádem i samotnému koncovému zařízení).
- Oproti rozbočovači neposílá data na všechny aktivní porty, ale tzv. přepíná.
  - Implementuje ostatní funkce rozbočovače (především zesílení signálu).
- Eliminuje (zmenšuje) kolizní domény.
- Umožňuje konfigurovat VLAN (resp. umí číst extra velikost rámce s touto informací – viz. standard IEEE 802.1Q).

Kolizní domény



- Pokud se místo rozbočovače umístí jako hlavní aktivní prvek přepínač je každý počítač na síti kolizní doménou jen sem se sebou!

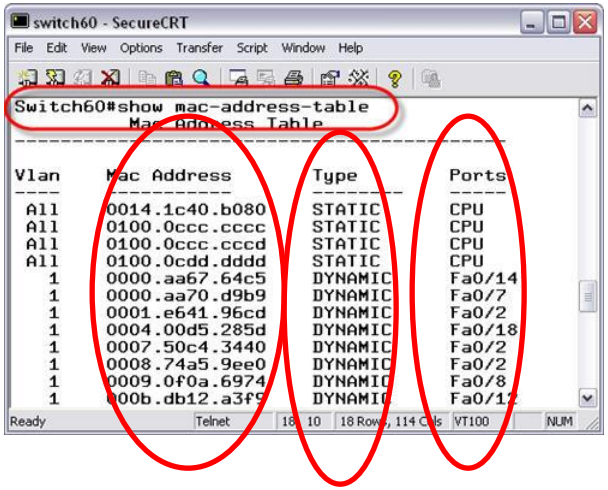
Přepínání

- Přepínač „směruje“ data na příslušné aktivní porty na základě cílové MAC adresy. Tzn. data se vysílají jen do rozhraní, jímž je připojen jejich adresát.
  - MAC adresu zjistí z hlavičky rámce příchozích dat.
  - *Z výše uvedeného principu je jasné, že přepínač nelze použít pro sniffování síťového provozu, protože data, které pro Vás nejsou určena se k Vám nedostanou!**
- Přepínač má uloženu tzv. přepínací tabulku.
  - Zjednodušeně se jedná o tabulku kde ke každému aktivnímu portu přepínače je přiřazena MAC adresa připojeného zařízení.

* Za předpokladu neexistence duplicitní MAC adresy.

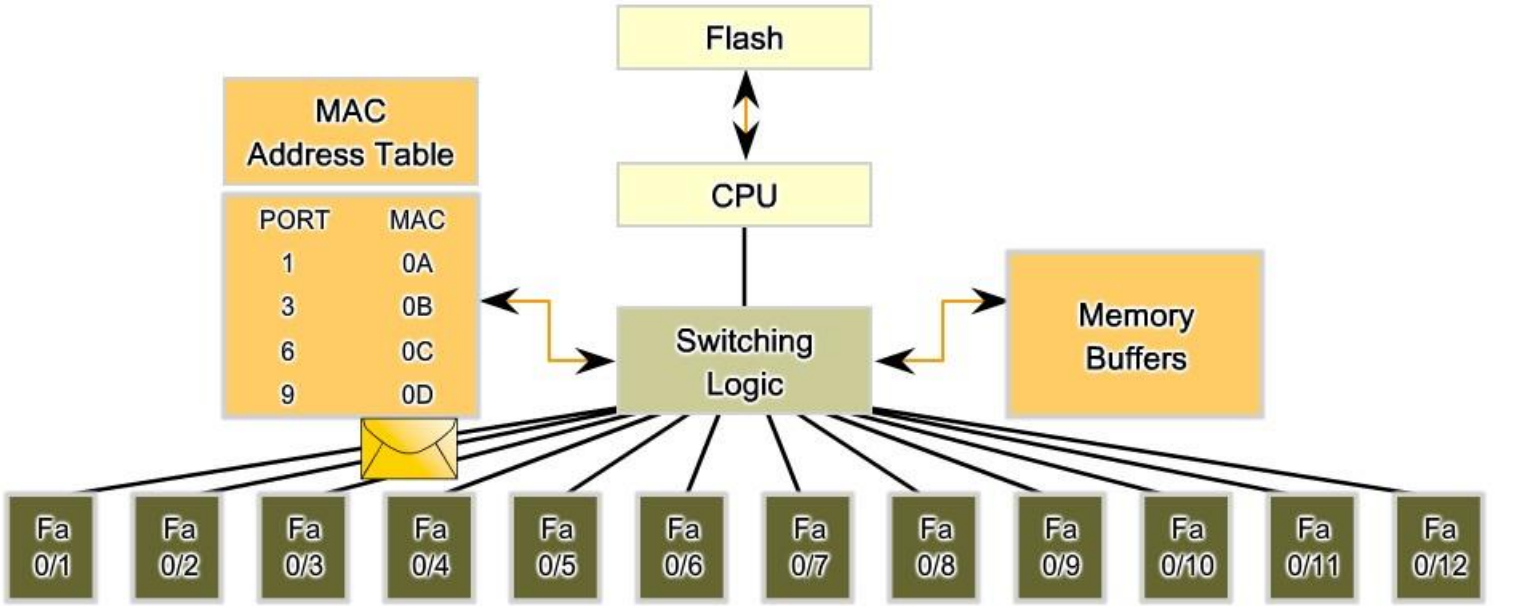
Přepínací tabulka

- Jak již bylo uvedeno obsahuje relace mezi MAC adresou a portem.
- Relace si přepínač do tabulky plní automaticky ze síťového provozu.



- Pokud přepínač dostane k doručení rámec směřující na jemu dosud neznámou adresu, chová se jako rozbočovač (hub) a rozešle rámec do všech ostatních rozhraní (kromě toho ze kterého data přišla).
- Stanice s odpovídající adresou pravděpodobně odpoví a přepínač se tak vzápětí dozví, kde se nachází (a zařadí ji do tabulky).
- Pokud přijde rámec z portu kterému přísluší jak zdrojová tak cílová MAC adresa pak je rámec zahozen!

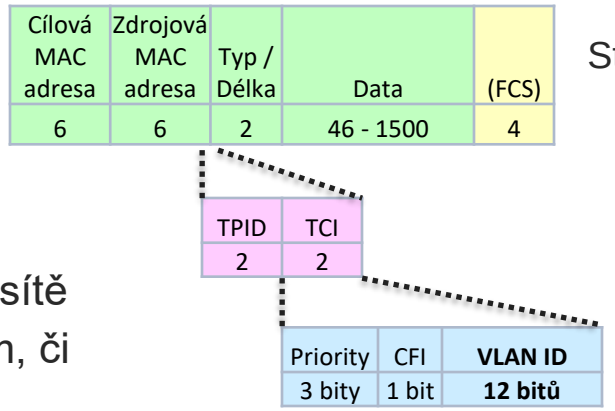
Ukázka přepínání



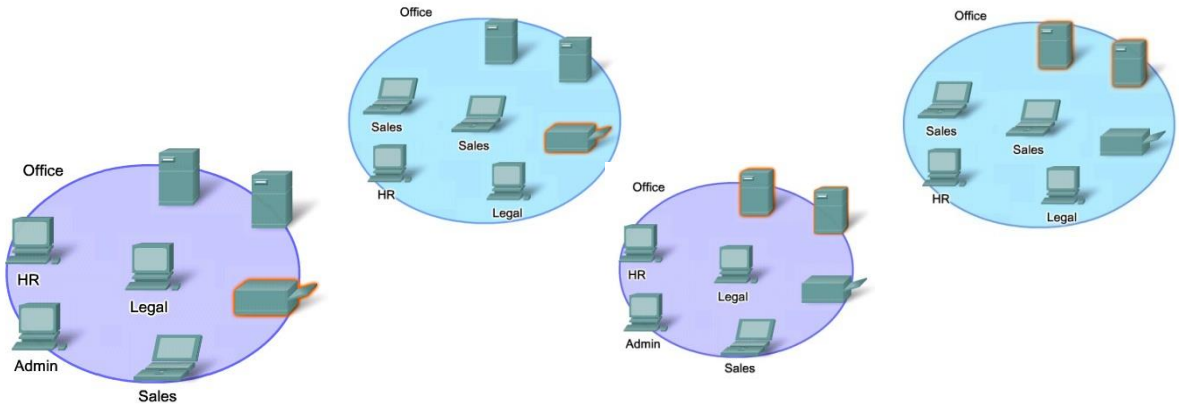
	Preamble	Destination Address	Source Address	Type	Data	Pad	CRC
FRAME 1		0C	0A				
FRAME 2		0C	0B				

Virtual LAN (VLAN)

- Rozšíření standardního ethernet rámce o další 4 bajty (IEEE 802.3ac) nesoucí ID VLAN, do které rámec přísluší.
  - Standard 802.1Q = VLAN Tagging.
- VLAN není nic jiného než rozdělení fyzické sítě (topologie) na logické části, ať už na jednom, či více zařízení (switch).
  - Usnadňuje správu, zvyšuje možnosti dalšího zabezpečení, zvyšuje výkon a umožňuje nastavit síť dle logických parametrů (např. organizační struktura firmy).

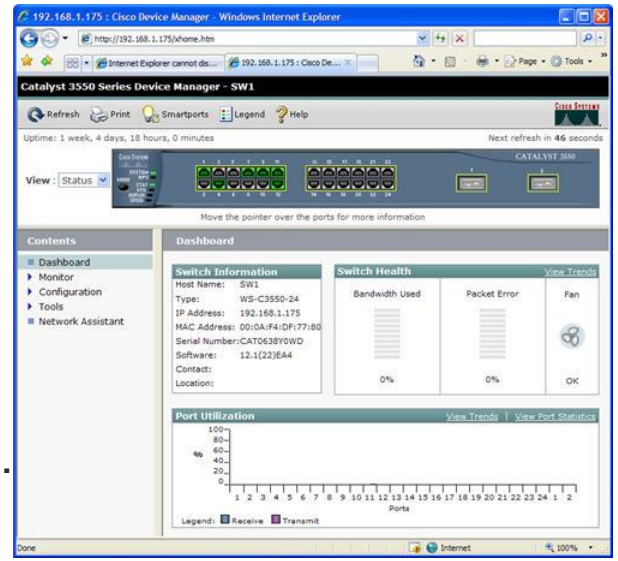


TPID nahrazuje pole Typ/délka pole u netagovaných rámců (je umístěno na stejném místě). Má hodnotu 8100 (hex).



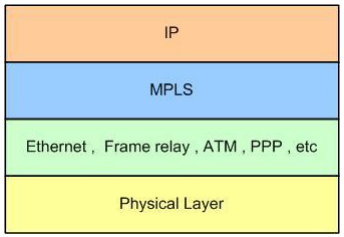
L3 Switch (MLS)

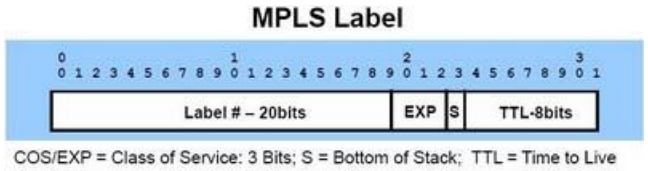
- Přepínač nemusí vykonávat pouze funkci zařízení druhé vrstvy, ale může zastávat základní funkce třetí vrstvy (směrování, ACL).
- MLS nebo směrovač je nutný k tomu aby mohly jednotlivé VLAN mezi sebou komunikovat.
- V dnešní době i levné typy přepínačů mají základní management.
  - Lze nastavovat filtrování MAC adres.
  - Porty přepínače mají vlastní MAC adresy.
  - Lze sledovat téměř vše jako na příkazovém řádku, ale v grafické podobě.
  - Konfigurace omezená (Cisco).

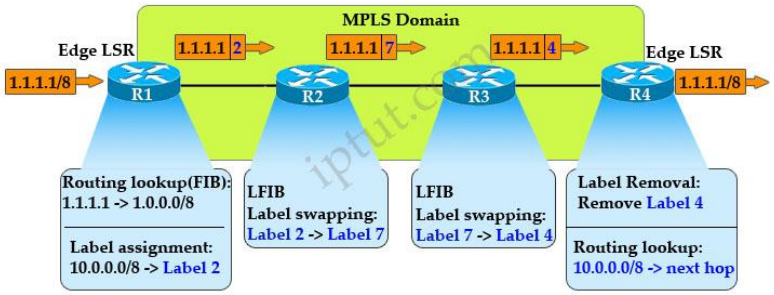


MPLS

- MultiProtocol Label Switching.
  - 2.5 vrstva
- Původně Cisco proprietární protokol.
- Záměr bylo zrychlit forwardování paktů na L3.
- Většinou v rámci WAN AS.
- Namísto IP adres používá LABELy.
  - Tj. forwarduje se na základě LABELů.
  - Vyvaruje se tím zdržování při vyhledávání v rout. tab.
  - LABEL je krátká identifikace IP headeru.
  - Analýza IP headeru a přiřazení odpovídajícího LABELu.
  - IP adresa je prozkoumána pouze prvním routerem a ostatní routery již „podvádí“ pomocí LABELů.
  - Na posledním routeru v topologii se LABEL odstraní a dále se již provádí standardní IP routing.
- Label Switched Router (LSR).
  - MPLS Edge Router.
  - MPLS Core Router.
- VPLS

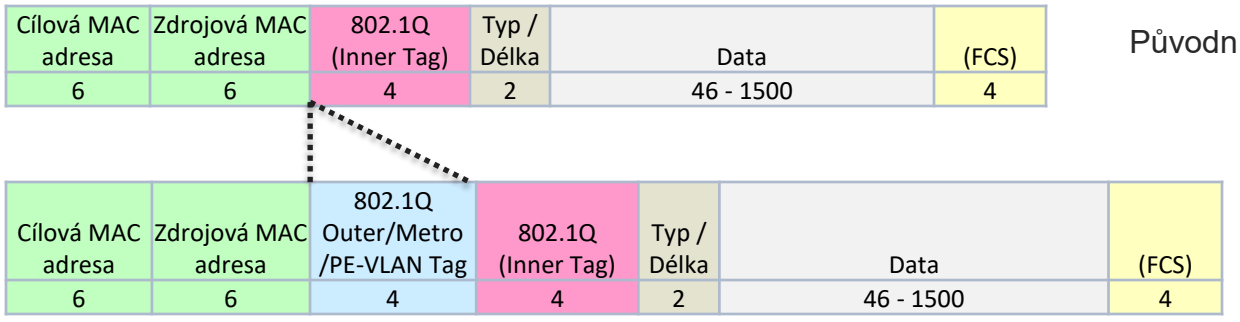






Metro / Carrier Ethernet

- Potřeba rozšíření původního standardu 802.1Q.
  - Činnosti jsou známé jako HVLAN (Hierarchical VLAN).
- Několik přístupů:
  - Q-inQ; Double Q tagging (IEEE 802.1ad)
    - C-TAG vs. S-TAG.
  - Mac-in-Mac (IEEE 802.1ah).



Původní tagovaný rámec

Carrier Ethernet tagovaný rámec

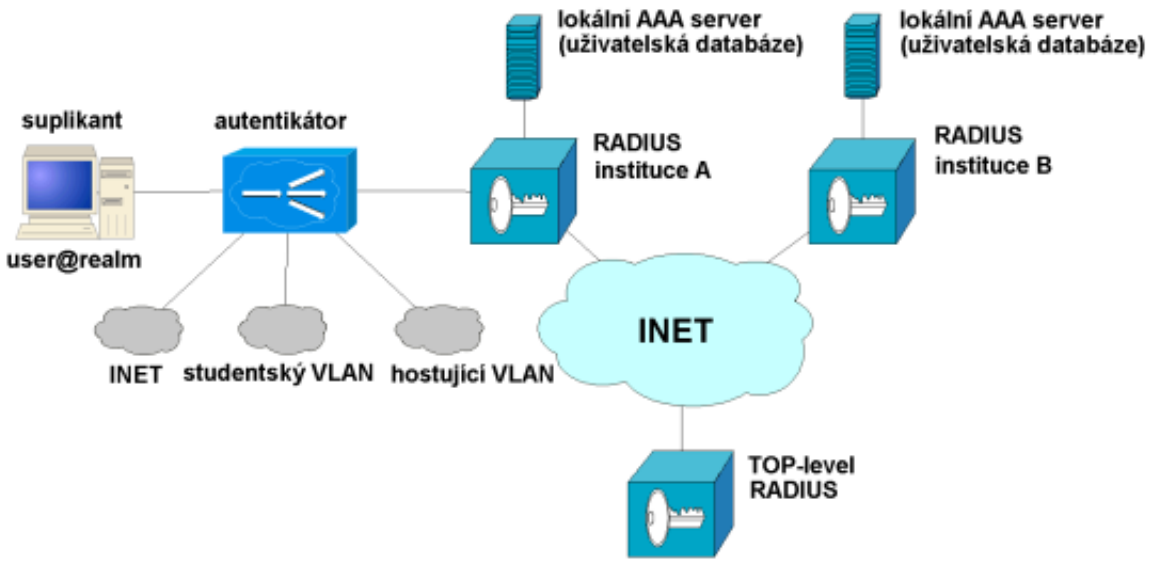
Ověřování IEEE 802.1x

- Protokol sloužící k autentizace uživatelů počítačových sítí.
- Jedná se o fyzickou autentizaci.
  - Pokud je do síťového portu (např. switche) připojeno nové zařízení, je port zablokován (neumožňuje přenos dat) dokud nejsou poskytnuty autentizační údaje (např. uživatelské jméno a heslo).
- IEEE 802.1x se nastavuje na přepínači (tzn. zabezpečení je na druhé vrstvě ISO/OSI modelu).
- Uplatňuje se také v bezdrátových sítích, v případech kdy volné připojení by mohlo být snadno zneužito.
  - Problém fyzické zabezpečení připojení k síti.

Princip fungování IEEE 802.1x

- Pokud se uživatel připojí na síťový port, má blokovanou veškerou komunikaci kromě EAP protokolu, který zajišťuje autentizaci. Ta proběhne takto:
  - Speciální program (suplikant), běžící na straně klienta, zahájí ověření přes EAP protokol (vyšle přes EAP protokol žádost o autentizaci na přepínač nebo AP).
  - Aktivní prvek naváže spojení na RADIUS server a zprostředkuje ověření suplikantu vůči RADIUSu. .
  - Proběhne ověření uživatele .
  - Pokud je uživatel lokální, proběhne jeho ověření přímo na RADIUS serveru.
  - Pokud uživatel lokální není, proběhne žádost o autentizaci přes strukturu RADIUS serverů až k uživatelově domovské síti.
  - O výsledku autentizace je informován přepínač (nebo AP), které další síťový provoz buď povolí nebo zakáže.
- Jako reakci na některé zranitelnosti protokolu WEP, nasazují někteří výrobci 802.1X pro bezdrátové přístupové body.

Princip fungování IEEE 802.1x



RADIUS

- Remote Authentication Dial In User Service.
  - Může pracovat jak lokálně tak v roamingu.
- AAA protokol.
- RADIUS server ověřuje pravost informace použitím autentizačních schémat jako PAP, CHAP nebo EAP.
- Pokud je uživatelské jméno a heslo přijato, server autorizuje přístup k poskytovateli internetu a vybere IP adresu (popřípadě rozsah adres) a další parametry spojení.
- RADIUS je jako autentizační protokol běžně používán v IEEE 802.1x bezpečnostním standardu.
- Používá UDP protokol.
- Oficiálně přidělené čísla UDP portů pro RADIUS protokol jsou pro autentizaci 1812 a pro účtování 1813.
  - Cisco používá porty 1645 resp. 1646.

Výhody, nevýhody

- Blokování neautorizovaných osob v síti nebo osob, které mají z určitých důvodů přístup k síti zakázaný (šíření virů, spam…).
- V kombinaci s různými dalšími technologiemi je možné umístit nežádoucí uživatele do tzv. VLAN, což je vlastně pořád ta samá síť, ale s výrazným karanténním omezením. Uživatel může využívat minimum síťových zdrojů, ale stále má přístup k nástrojům na případně odvirování počítače, instalaci nejnovějších aktualizací apod.
- Počítač, který je připojený na neautorizovaný port nemá k síti přístup.

PowerLine (PLC) / Homeplug

- Hodí se tam, kde není k dispozici datová síť a WiFi signál je nestabilní.
  - Je spolehlivější než bezdrát!
  - Ale také dražší.
- Elektrické dráty pak slouží jako fyzická vrstva pro přenos dat.
- Princip fungování je velmi obdobný technologii ADSL.
  - Frekvence v rozsahu 1 – 30 MHz (krátké vlny).
- Pomalejší a méně efektivní než klasický Ethernet.
- HomePlug AV (up to 500mbps).
  - AV2 standard (up to 2Gbps).
    - Paper na Moodle.
- Samoopravný kód zajišťuje bezpečný průchod dat na dlouhou vzdálenost a přes překážky (jističe, apod.), ale na druhé straně zpomaluje reálný přenos dat.
- Podmínkou je jedna fáze.

IEEE 802.11 rámec

- Standard IEEE 802.11ac viz. dokumenty na Moodle.
- Rozdíly oproti IEEE 802.11n?