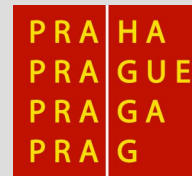


SPS Úvod Technologie Ethernetu



Y36SPS

- Přednášející i cvičící:
 - Jan Kubr
 - kubr@fel.cvut.cz, místnost E-414, (22435) 7504

- literatura

Dostálek L., Kabelová A.: Velký průvodce protokoly TCP/IP.
???

- WWW

<http://dsn.felk.cvut.cz>

- organizace předmětu

přednáška, laboratorní cvičení
?semestrální práce?

Osnova přednášek

1. Úvod, technologie Ethernetu, VLAN, autorizace
2. Bezpečnostní architektura počítačových sítí - firewall, VPN
3. Směrovací protokoly autonomních systémů - RIP, OSPF
4. Směrovací mechanismy páteří - EGP, BGP
5. Jmenné služby, adresace - DNS, DHCP
6. Jmenné služby – LDAP
7. Pošta
8. Správa síťových prvků – protokoly
9. Správa síťových prvků – aplikace
10. Bezpečné připojení klientů a bezpečný přenos dat - RADIUS, ssh, ssl, IPsec
11. Datové toky v počítačových sítích - QoS, mechanismy řízení toku
12. Sledování dostupnosti služeb - SLA (nebo něco úplně jiného)
13. Rezerva

Osnova cvičení

1. Úvodní cvičení
2. ~~Dynamické směrování - cvičení~~
3. ~~Dynamické směrování - Laboratorní cvičení~~
4. Firewalling - cvičení
5. Firewalling - Laboratorní cvičení
6. Domain name system - cvičení
7. Domain name system - Laboratorní cvičení
8. Konzultační cvičení
9. Mailserver Y36SPS: Mailserver laboratoř
10. Dohledové systémy - cvičení
11. Dohledové systémy - Laboratorní cvičení
12. Prezentace a odevzdání semestrálních prací
13. Prezentace, zápočet

Požadavky

Cvičení:

- absolvovaná laboratorní cvičení,
- zápočet nelze získat po zápočtovém týdnu.

Zkouška:

- získané hodnocení ze cvičení (zápočet),
- finální laboratoř,
- případná písemná zkouška s možností ústního přezkoušení.

Sít'ová správa

- oblasti
 - fault management
 - configuration management
 - accounting management
 - performance management
 - security management
- reaktivní a proaktivní správa
- správa počítačových sítí
 - konfigurace sít'ových prvků
 - konfigurace služeb

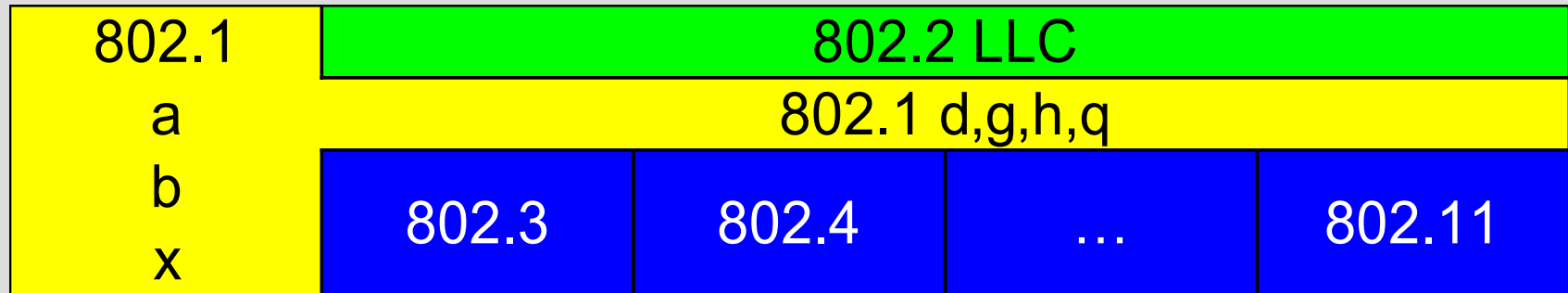
IEEE a sítě

- 802.1 rozhraní pro vyšší vrstvy
- 802.2 LLC
- 802.3 Ethernet, CSMA/CD
 - 802.3a – 10Base2
 - 802.3i – 10BaseT
 - 802.3j – 10BaseFX
 - 802.3u – 100BaseT
 - 802.3ab – 1000BaseT
 - 802.3z – 1000BaseX
 - 802.3ae – 10Gbit Ethernet
- 802.4 Token Bus
- 802.5 Token Ring
- 802.11 bezdrátové sítě LAN

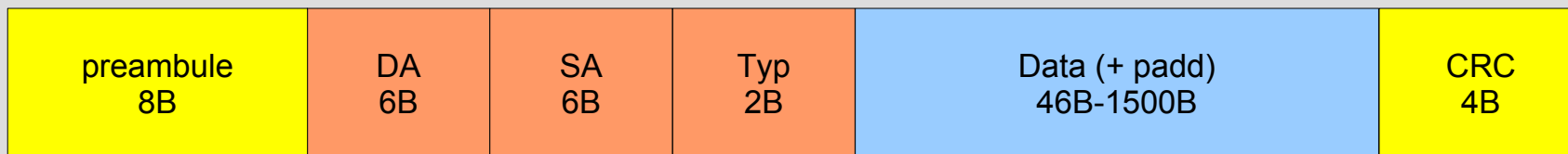
IEEE 802.1

- a – úvod a architektura
- b – správa a řízení
- d – bridging
- e – zavádění systému
- f – definice a procedury pro správu
- g – propojení vzdálených sítí přes 802.1d
- h – propojení sítí s rámcem Ethernet II
- p – priority
- q – VLAN
- x – řízení přístupu k portům

Architektura IEEE 802



Ethernet II (DIX)



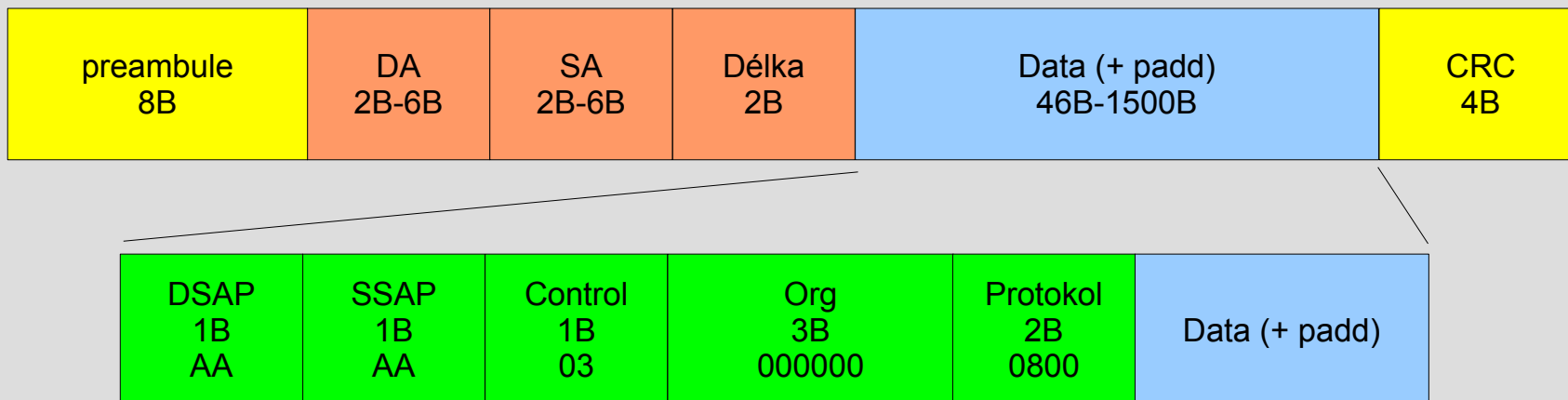
- preamble 10101010....101011
- DA, SA – adresa cíle, adresa zdroje
 - 3B výrobce
 - XXXXXXFB
 - F – 0..globální, 1..firemní
 - B – 0..adresa karty, 1..multicast
 - 111...111 broadcast
- typ – ID protokolu
 - 0800 ... IP
 - 0806 ... ARP
 - 8035 ... RARP
 - 86DD ... IPv6
 - 88A2 ... ATA over Ethernet

IEEE 802.3 (ISO 8802-3)



- délka 0-5dc
- data
 - přímo rámce IEEE 802.3 – Novell IPX
 - rámce IEEE 802.2 – nelze IP, protože chybí ARP
 - rámce IEEE 802.2 SNAP

IEEE 802.2 (ISO 8802-2)

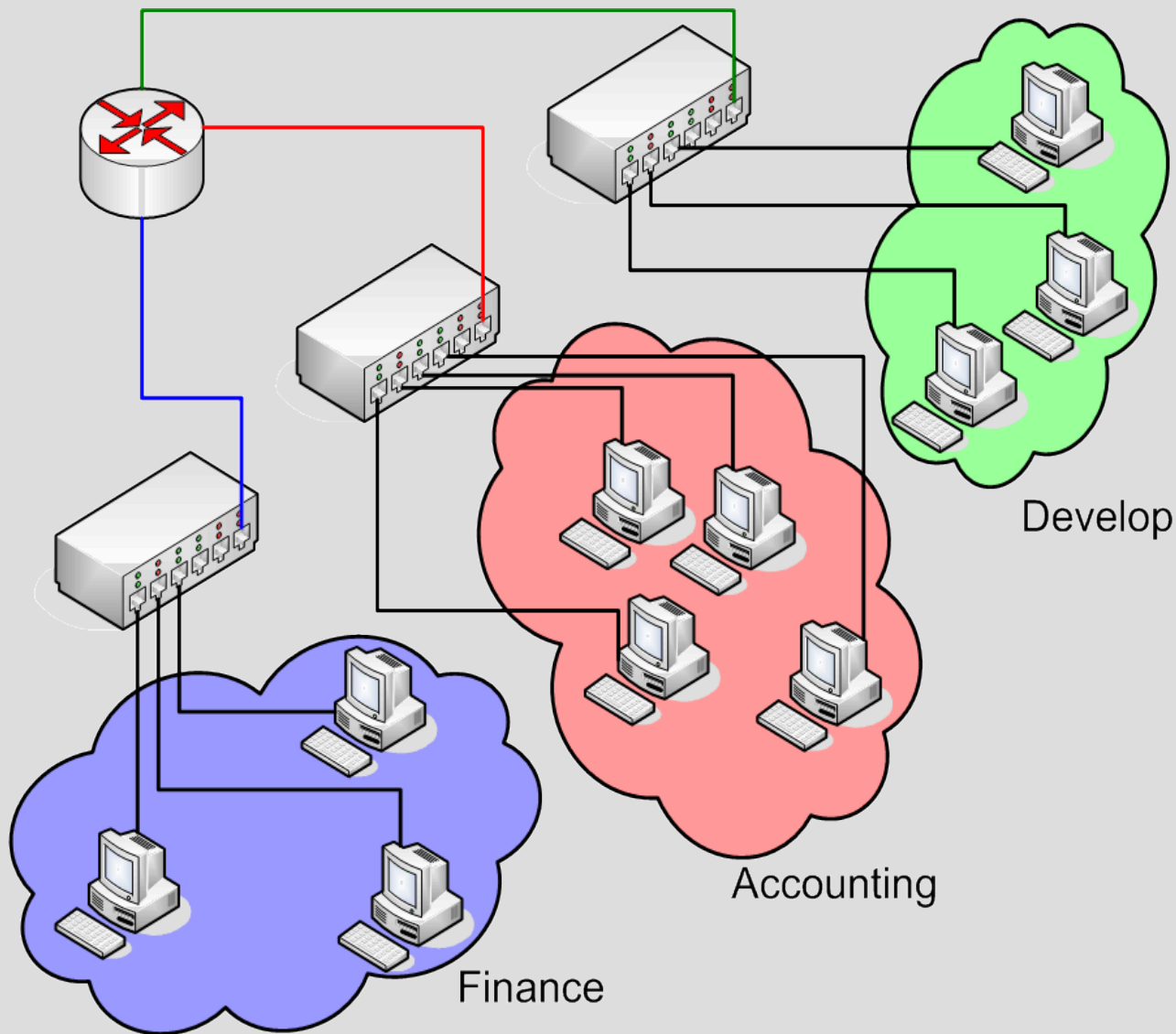


- DSAP, SSAP – Destination/Source Service Access Point
 - aa,ab ... SNAP
 - e0 ... Novell Netware
 - f0 ... IBM NetBIOS
- control – odpovídá HDLC
 - pro SNAP U-rámec UI (Unnumbered Information)
- org – identifikace organizace
 - 000000 ... Ethernet II typ, jinak definovaný organizací

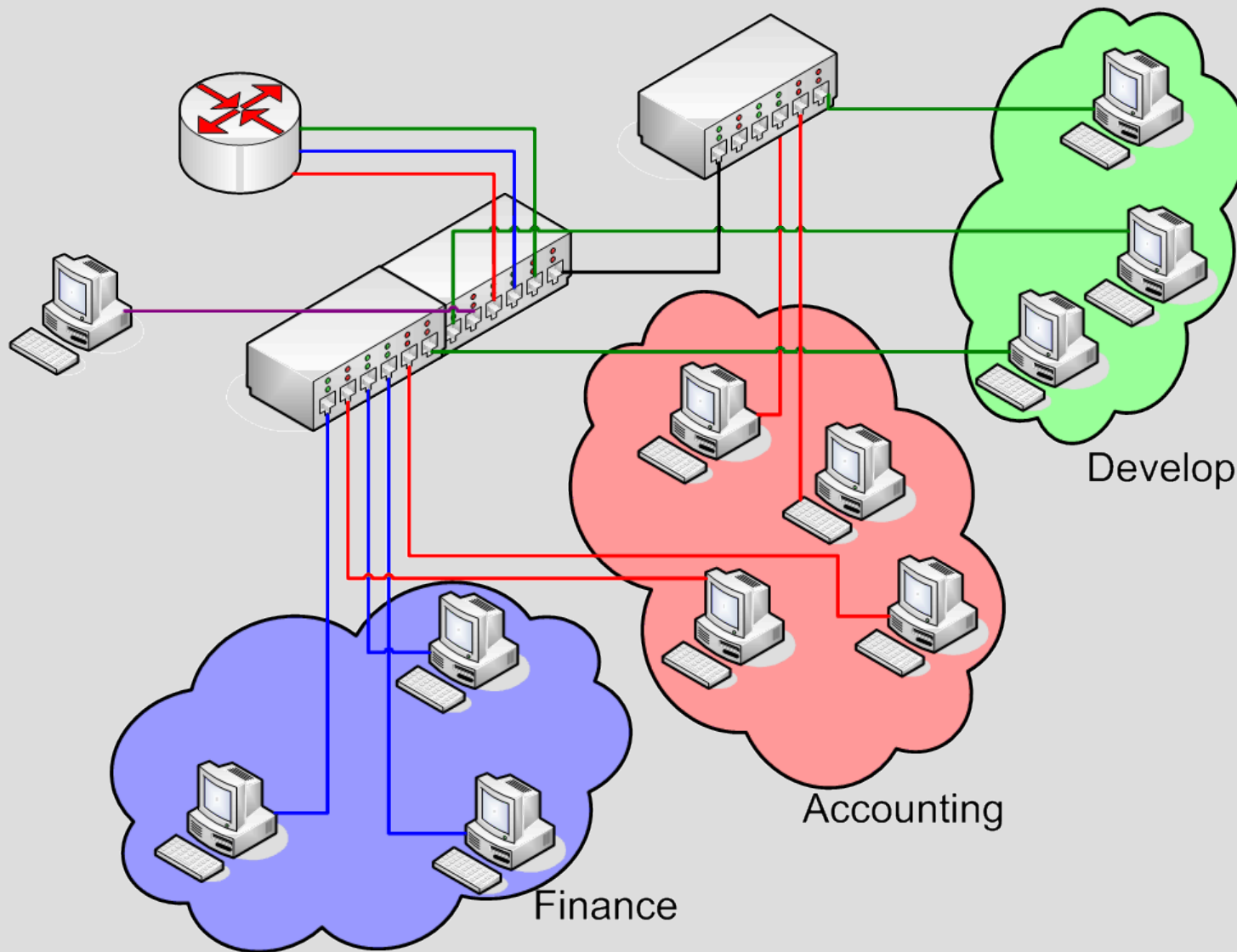
Virtuální lokální sítě - VLAN

- typy VLAN
 - podle portů,
 - podle MAC,
 - podle protokolu (adresy vyšší vrstvy),
 - podle skupinového vysílání,
 - podle autentizace,
- statické x dynamické
- tagované x netagované
- protokoly
 - IEEE 802.10 – Cisco
 - IEEE 802.1q
 - VTP (VLAN Trunking Protocol) – Cisco
 - GVRP (GARP VLAN Registration Protocol)

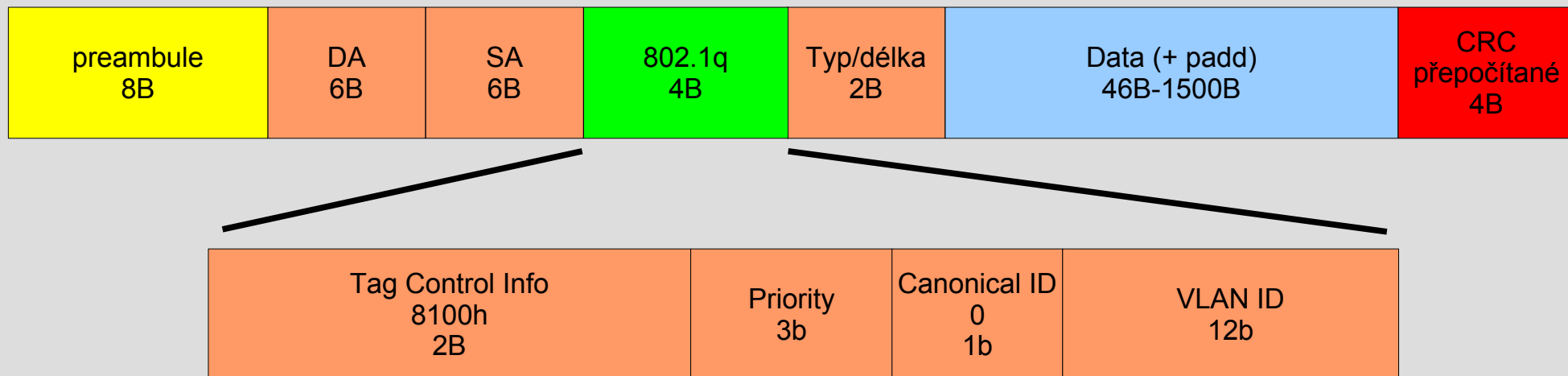
Sít' bez VLAN



Sít' s VLAN



IEEE 802.1q



- TCI – 8100h
- P – 0-7 podle IEEE 802.1p (0 nejnižší)
- C – typ adres Ethernet, TokenRing
- VID – 1-4094
 - 0 priorita
 - 4095 rezerva

VLAN a ostatní

- GVRP
 - GARP VLAN Registration Protocol
 - Generic VLAN Registration Protocol
- DHCP
 - Dynamic Host Configuration Protocol
- STP
 - Spanning Tree Protocol
- RSTP
 - Rapid Spanning Tree Protocol

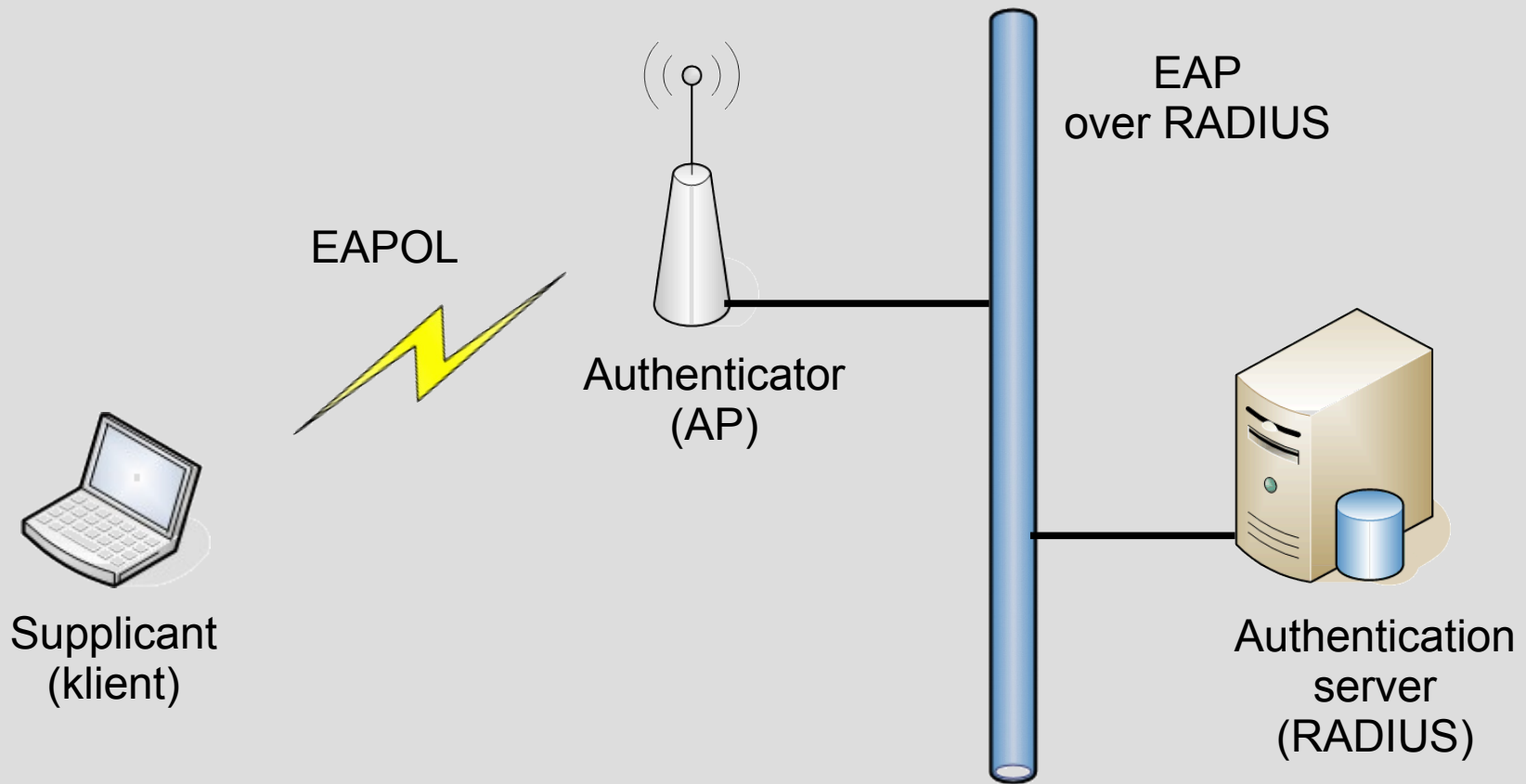
Řízení přístupu k portům I

- IEEE 802.1x
- EAP (Extensible Authentication Protocol)
 - navazuje na PPP
 - transportní mechanismus pro ověřovací metody
- především bezdrátové spoje
- možnost spolupráce s technologií VLAN
- části
 - supplicant – koncový uzel
 - authenticator – uzel požadující službu autorizace
 - authentication server – ověřuje koncový uzel

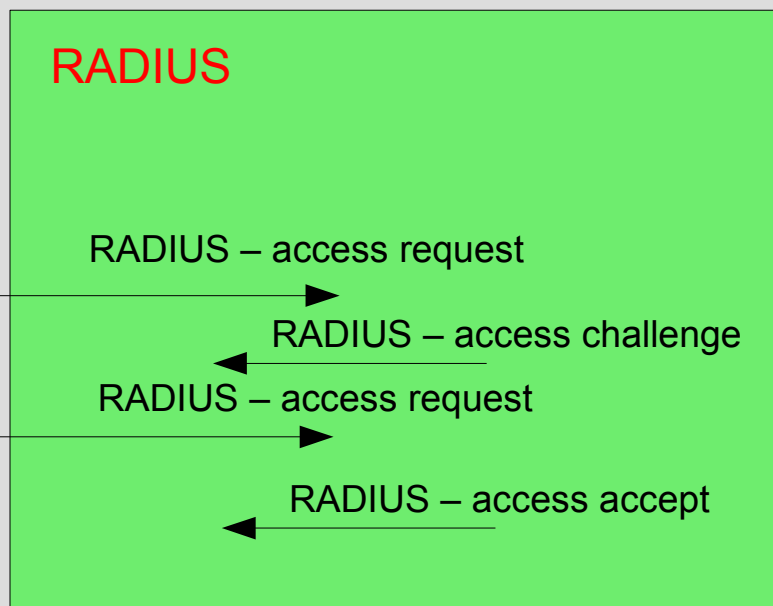
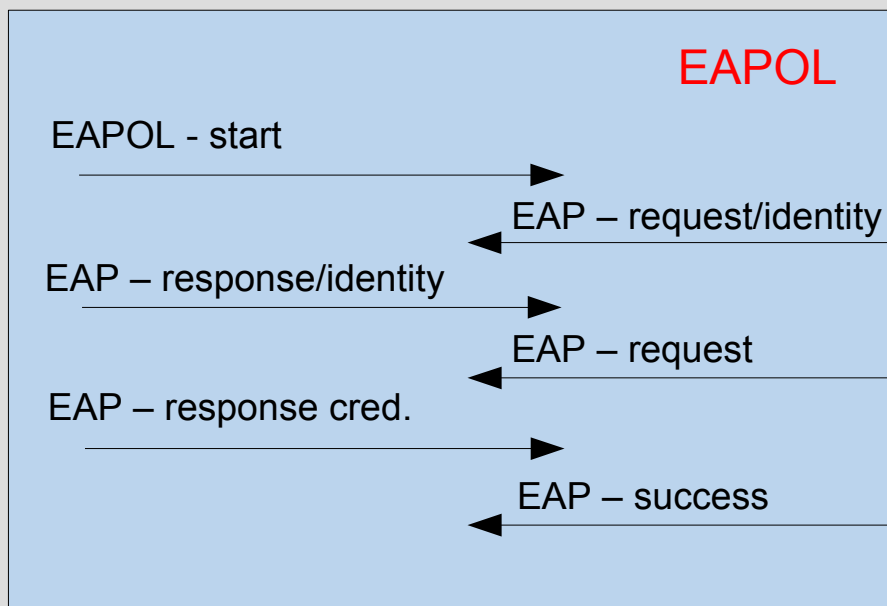
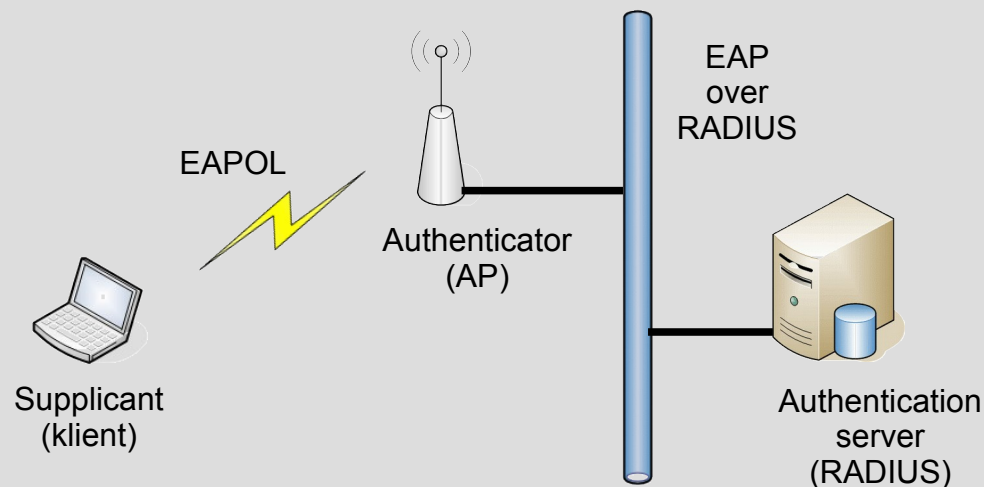
Řízení přístupu k portům II

- logické porty – PAE (Port Access Entity)
 - fyzické porty
 - MAC adresy
 - WLAN asociace
- logické porty
 - řízené (controlled) – pracovní stav, po úspěšné autorizaci
 - neřízené (uncontrolled) – omezená komunikace, výměna autorizačních informací

IEEE 802.1x – schéma



IEEE 802.1x – ověřování



Ověřovací metody

- EAP-MD5
- EAP-OTP
- EAP-TLS
- EAP-LEAP
- EAP-TTLS
- EAP-PEAP
- ...
- vytvoření sdíleného tajemství (WEP heslo)
- přiřazení do VLAN
- předání informace na authenticator

podporované prvky?
koexistence

...