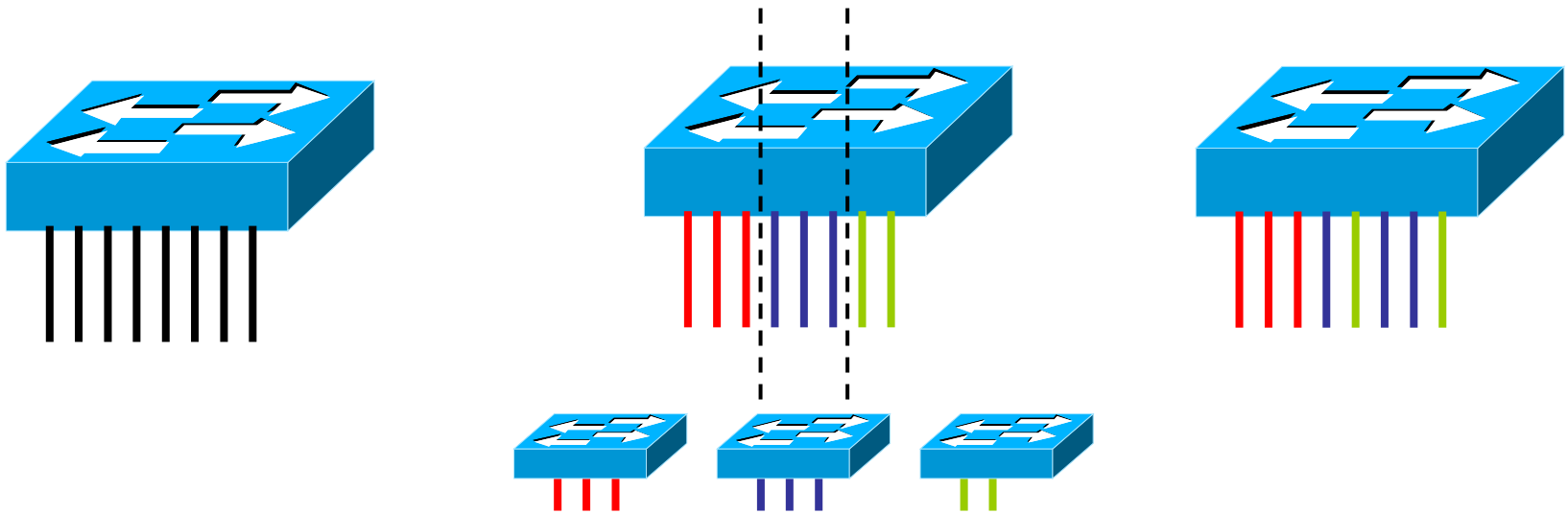
Virtuální lokální sítě v prostředí Linuxu

Petr Grygárek

Co jsou virtuální lokální sítě ?

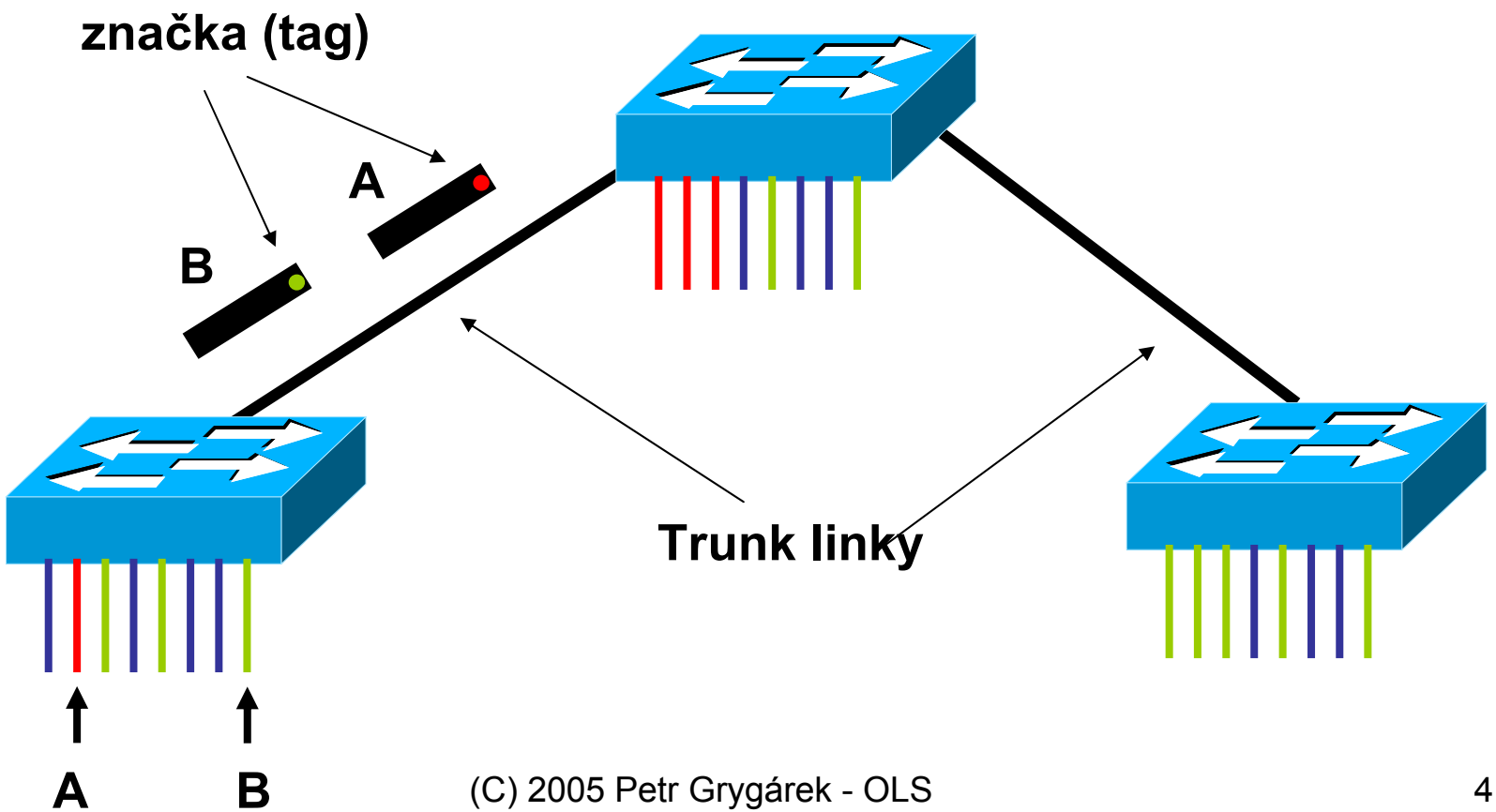
VLAN na jednom přepínači

- Možnost definice oddělených LAN realizovaných ze skupin portů přepínače čistě softwarovou konfigurací přepínače
- Oddělení logické struktury sítě od fyzické topologie



Zvláštní přepínací tabulka pro každou VLAN

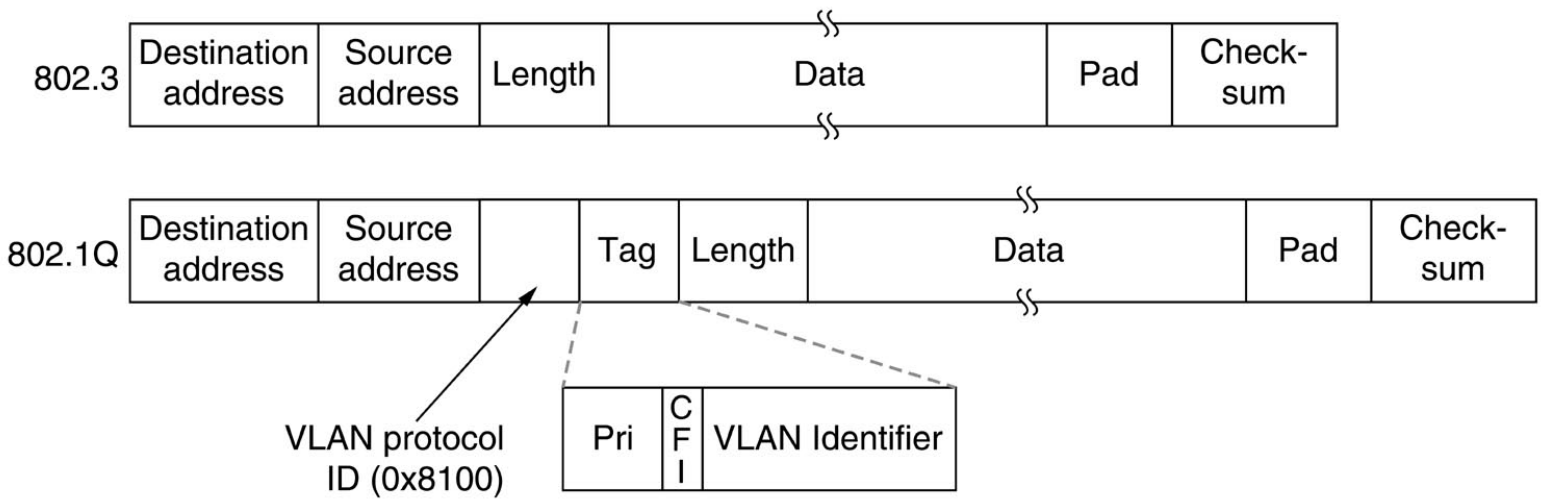
VLAN na více přepínačích



Způsob značkování – IEEE 802.1q

http://standards.ieee.org/getieee802/download/802.1Q-1998.pdf

- Modifikace (prodloužení) rámce o 2B
  - musí podporovat síťové rozhraní přepínače
    - (příp. síťová karta routeru nebo serveru)
- Přítomnost značky indikována vyhrazenou hodnotou EtherType
- Virtuální sítě identifikovány čísly (0-4096)

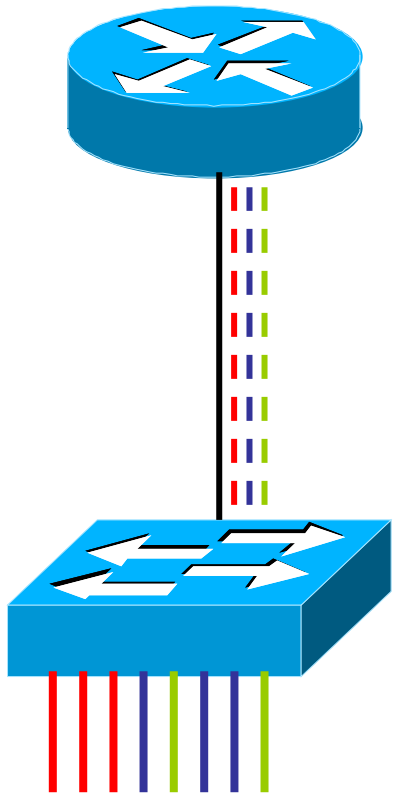


Kde značky podle 802.1q najdeme ?

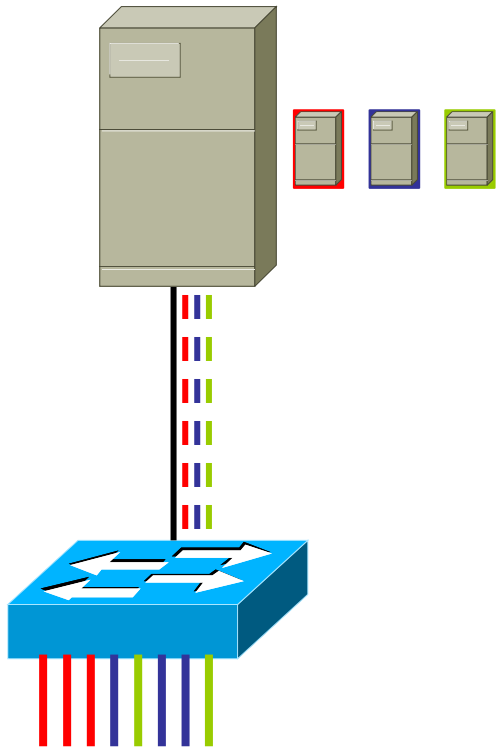
- Na trunk spojích mezi přepínači
  - Explicitní konfigurace příslušných portů jako trunk
- Na trunk spoji z přepínače do routeru
  - pro směrování mezi VLAN
- Na trunk spoji z přepínače do serveru se síťovou kartou podporující VLAN

Při přeposílání rámce na stanici připojenou běžnou (non-trunk) linkou přiřazenou do jediné VLAN je 802.1q hlavička odstraněna

Trunk linka z přepínače do routeru

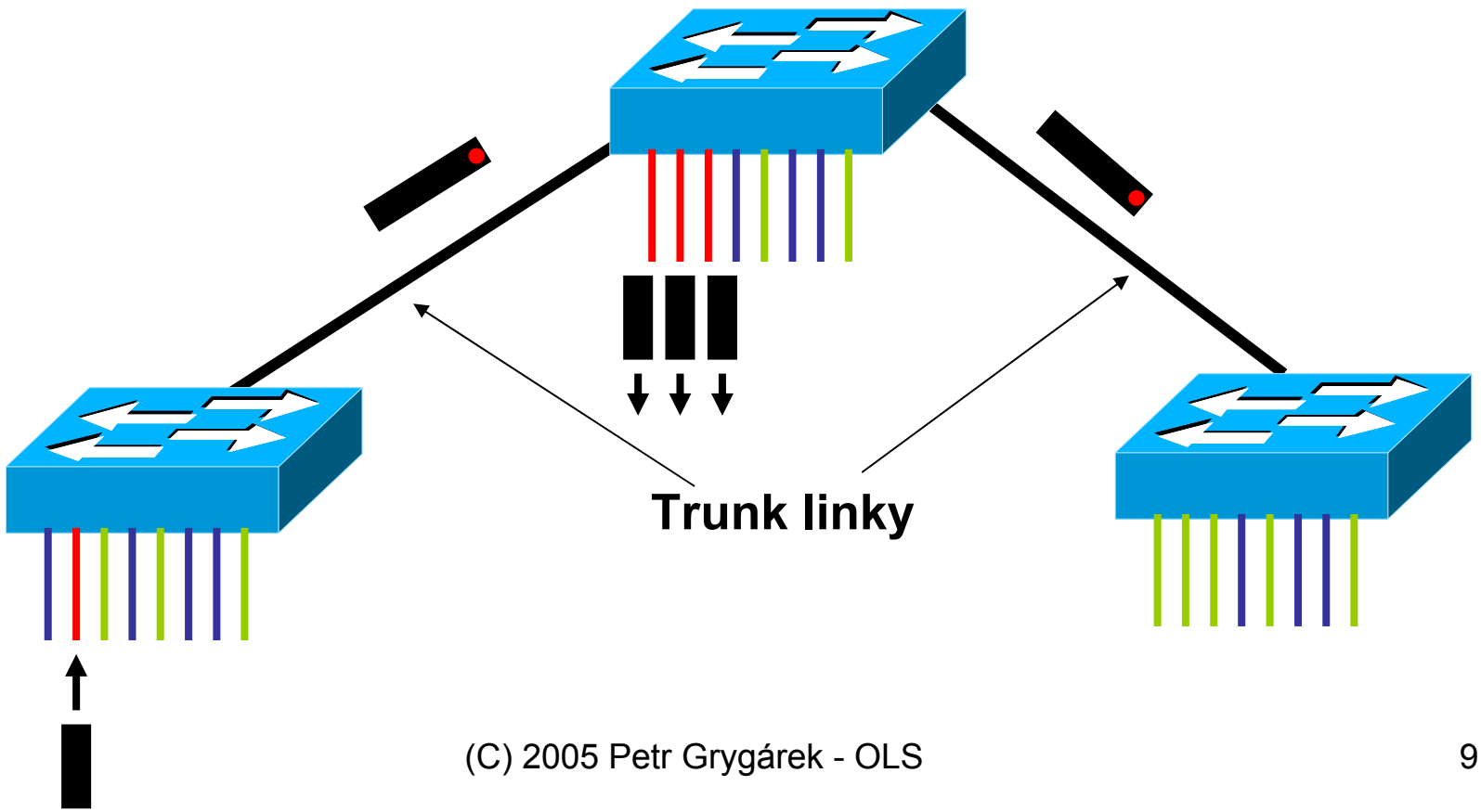


Trunk linka k serveru podporujícímu VLAN

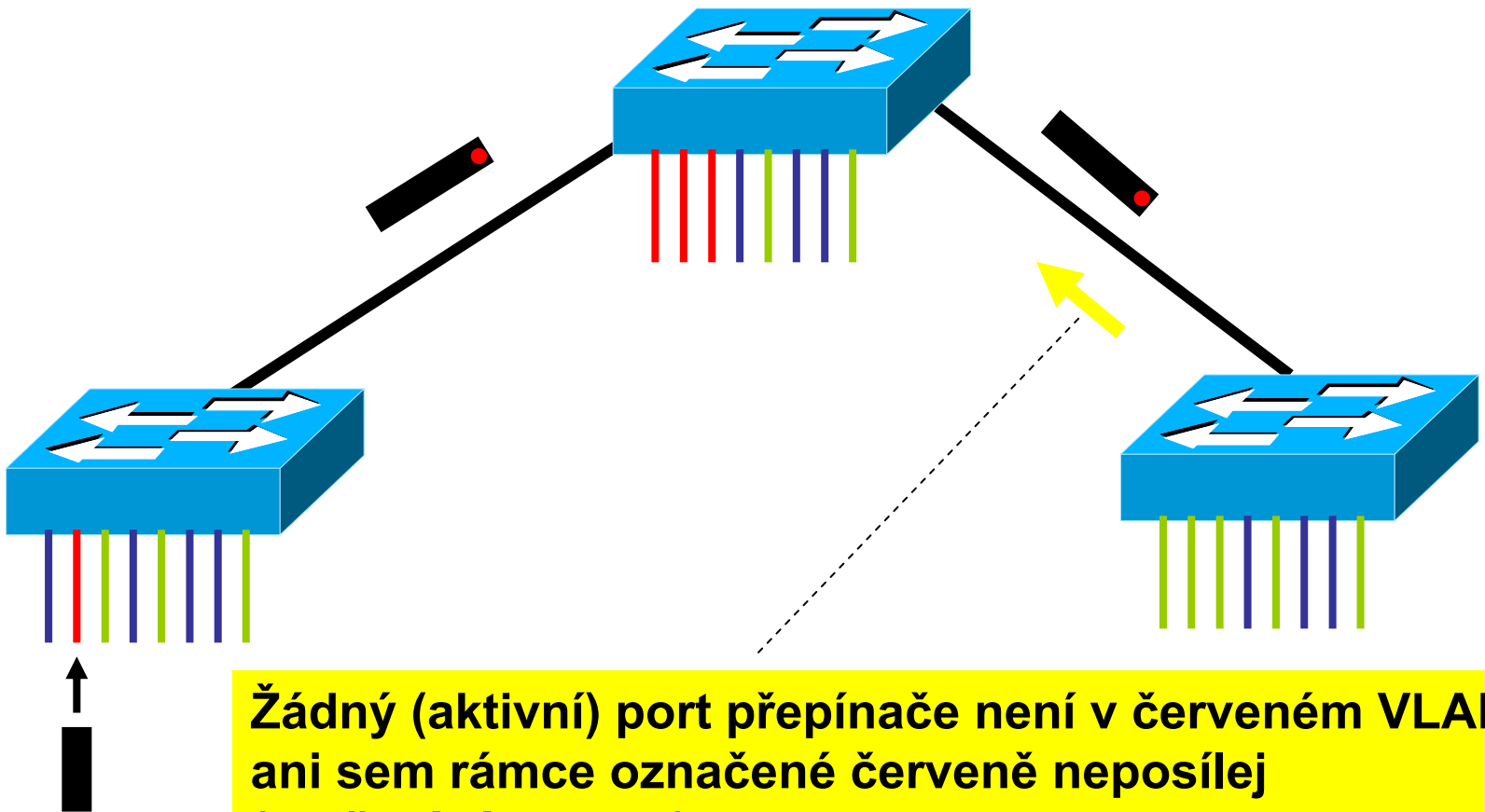


Kam všude se může rámec dostat ?

Broadcast rámec nebo rámec s neznámou cílovou MAC adresou



Dynamické prořezávání VLAN (pruning)



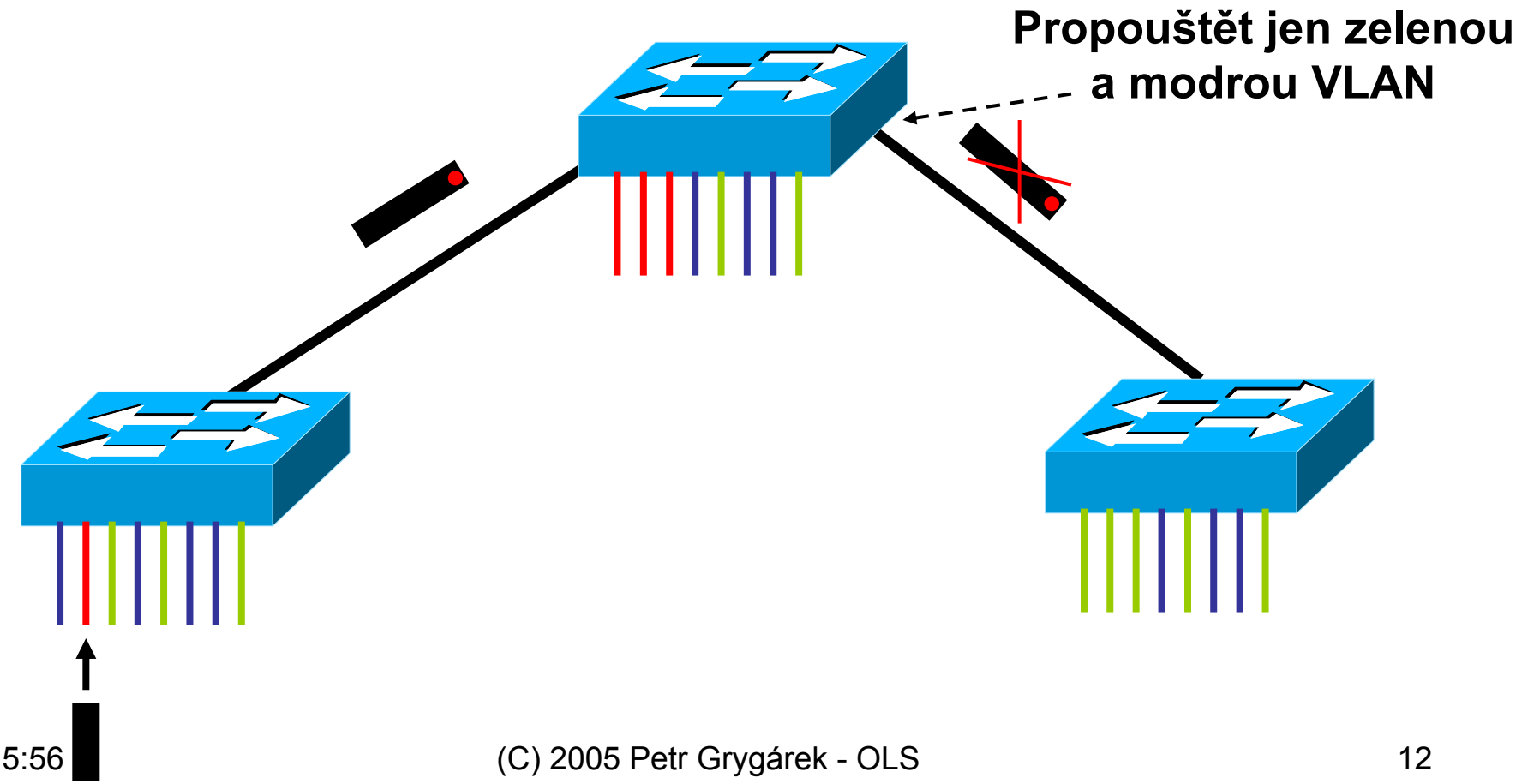
Žádný (aktivní) port přepínače není v červeném VLAN, ani sem rámce označené červeně neposílej (prořezání stromu)

Protokol zpráv pro prořezávání stromů jednotlivých VLAN

- Cisco: VLAN Trunking Protocol (VTP)
  - Proprietární
  - Žádosti o prořezání VLAN bez klientů (prune)
- GVRP – GARP VLAN Registration Protocol
  - IEEE (802.1q,p)
  - Používá Generic Attribute Registration Protocol (GARP)
  - Žádosti o připojení do stromu, jsou-li klienti (join)
  - Zatím podporováno sporadicky
    - (Cisco CatOS, HP Series 2500 Procurve, …)

Filtrace VLAN na trunk linkách

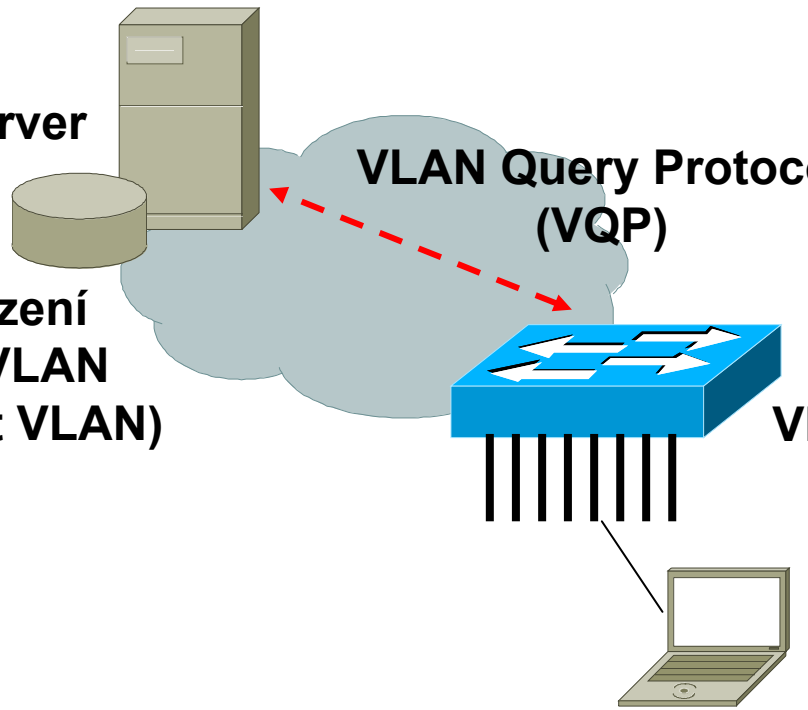
Každému trunk portu lze staticky přiřadit, ze kterých VLAN smí propouštět rámce.



Členství ve VLAN

- Staticky (port-based)- každému portu přepínače staticky přiřazena VLAN
- Dynamicky - podle (zdrojové) MAC adresy
  - Teoreticky i např. podle protokolu nebo adresy 3. vrstvy
  - Vazba dvojic <MAC adresa, číslo VLAN> udržována ve zvláštní databázi
    - Cisco: VLAN Membership Server (VMPS)
      - implementují vyšší (a dražší) modely přepínačů Catalyst
  - Při výskytu nové zdrojové MAC adresy na portu přepínače se přepínač ptá VMPS serveru na její přiřazení do VLAN
    - Cisco: port jako celek se přiřadí do příslušného VLAN
      - je-li stanic na portu více, musí všechny patřit do stejného VLAN

Dynamické přiřazování do VLAN na portech přepínače (Cisco)



Uživatelské zařízení s danou MAC adresou (pošle např. DHCP request)

VLAN Query Protocol (VQP)

- Proprietární, ale dokumentace v rámci projektu OpenVMPS (SourceForge)
  - Popis v češtině viz Reference
- Nad UDP
  - cílový port 1589
  - zdrojový port dočasný (ephemeral)
  - Identifikace VQP klienta zdrojovou IP adresou
- VQP klient posílá textově jméno rozhraní, kam se klient připojil a MAC adresu uživatele
  - ve skutečnosti celý první rámec došlý na rozhraní => pro přiřazování do VLAN možno použít i dalších údajů
    - (protokol >=L3 a jeho parametry – IP adresy, QoS, …)
- VQP server odpovídá zprávami Accept/Reject/Shutdown
  - ve zprávě Accept jméno VLAN pro přiřazení na port
    - pro technické použití musí být jméno přemapováno na číslo

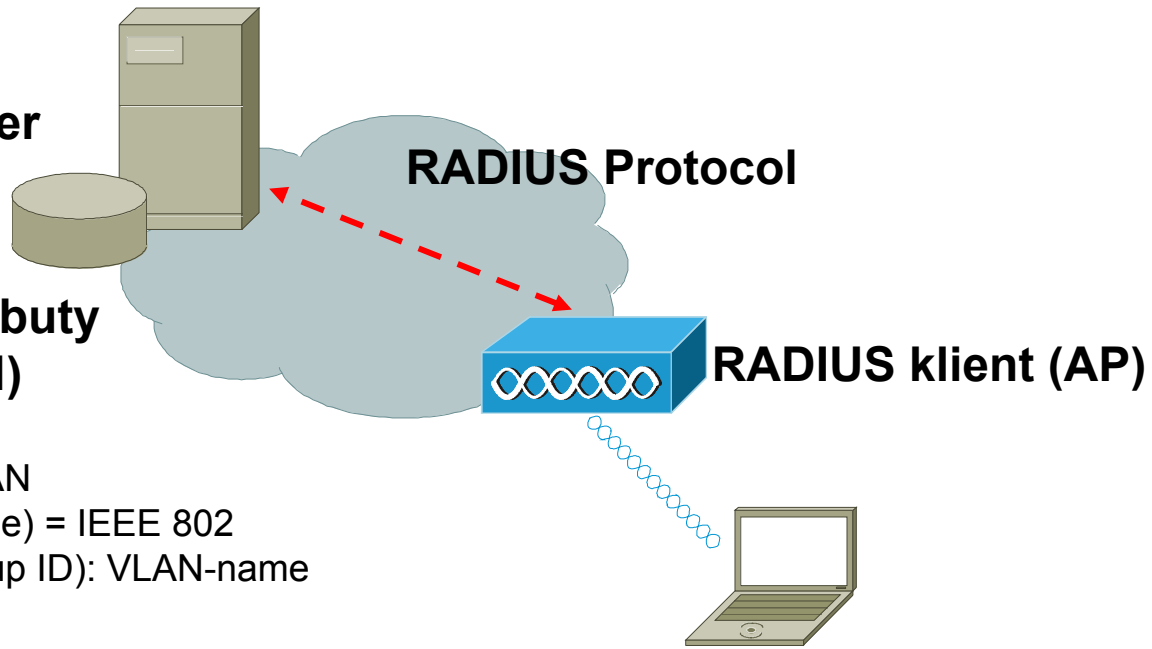
Odkud se vezmou jména VLAN ?

- VMPS server odpovídá **jménem** VLAN, ne přímo číslem použitelným ve značkách 802.1q
  - Přiřazení jmen jednotlivých VLAN konfigurováno na přepínačích
  - Může se mezi přepínači šířit pomocí protokolu VLAN Trunking Protocol (Cisco)
    - mezi všemi přepínači označenými jako členy určité logické skupiny – „VTP domény“
    - aby se jména nemusela definovat na všech přepínačích zvlášť
- Ve VQP se posílá i jméno VTP domény, v rámci níž jsou jména VLAN platná
  - v OpenVMPS lze ignorovat

VMPS: omezení vstupu do VLAN z portů přepínačů

- U konkrétního uživatele (MAC adresy) lze omezit, ke kterému VMPS klientovi (přepínači) se může připojit
- Lze jít až na úroveň jmen konkrétních portů jednotlivých VMPS klientů (přepínačů)

Dynamické přiřazování na přístupovém bodu sítě WiFi (AP)



IETF 64 (Tunnel Type) = VLAN
IETF 65 (Tunnel Medium Type) = IEEE 802
IETF 81 (Tunnel Private Group ID): VLAN-name

Uživatelské zařízení s danou MAC adresou (pošle např. DHCP request)

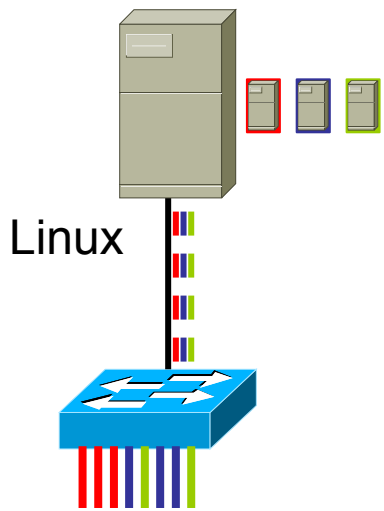
(RADIUS = Remote Dial-in User Access Server)

A jak s tím vším souvisí Linux ?

Použití Linuxu s VLAN

- Hostování služeb na jednotlivých VLAN přivedených jedinou (trunk) linkou
- Směrování mezi VLAN
- Provozování RADIUS a OpenVMPS serveru pro dynamické přiřazování uživatelů do VLAN
- …

Jak Linux naučit pracovat s VLANy



Co je k tomu třeba ?

- Síťová karta podporující značkování IEEE 802.1q
- Podpora v jádře
  - CONFIG_VLAN_8021Q=yes
  - nebo i modul 8021q
- Konfigurační utilita vconfig
  - http://www.candelatech.com/~greear/vlan.htm (zdrojové kódy i binární forma)
  - lze obvykle instalovat i z balíčku

Jak virtuální sítě na Linuxu nakonfigurovat ?

- Logická síťová rozhraní (subinterfaces)
  - eth0.1, eth0.2, eth0.3, …
- Každé logické rozhraní je vázáno na jednu konkrétní VLAN
  - tedy přebírá z trunk linky rámce označené určitou značkou a naopak tuto značku přidává do rámců odesílaných na trunk linku
- Další použití logických rozhraní stejné jako u normálních síťových rozhraní

Konfigurace logických síťových rozhraní

- **vconfig add <interface-name> <vlan-id>**
  - Vytvoření logického rozhraní a přiřazení VLAN
  - Příklad: vconfig add eth0 2
    - přiřadí VLAN 2 na nově vytvořené rozhraní eth0.2
- **vconfig rem <logical-interface>**
  - Zruší zadané logické rozhraní

Nastavení speciálních parametrů logického rozhraní

vconfig set_flag <logical_interface> <flag-num> <0 | 1>

Příklad parametru:

- REORDER_HDR - z Ethernet rámců bude/nebude odstraněna hlavička 802.1Q
  - (kvůli kompatibilitě se SW, co ji nepředpokládá, např. dhcpd)

Pojmenovávání logických rozhraní

vconfig set_name_type <id_konvence>

- DEV_PLUS_VID_NO_PAD (**eth0.5**)
- DEV_PLUS_VID (**eth0.0005**),
- VLAN_PLUS_VID_NO_PAD (**vlan5**),
- VLAN_PLUS_VID (**vlan0005**),

Platí od nastavení pro nově přidávané VLAN

Co lze ještě nastavit ?

- Unikátnost čísel VLAN
  vconfig bind_type
  - PER_DEVICE
  - PER_KERNEL

- MAC adresu každého logického rozhraní
  - není nutné, MAC adresy mezi VLAN se stejně vzájemně „nevidí“

Informace o nastavení logických rozhraní

```
# cat /proc/net/vlan/config

  VLAN Dev name    | VLAN ID
  Name-Type:
  VLAN_NAME_TYPE_PLUS_VID_NO_PAD
  eth0.2           | 2  | eth0
  eth0.3           | 3  | eth0
```

Informace o konkrétním logickém rozhraní

```
# cat /proc/net/vlan/eth0.2

  eth0.2  VID: 2   REORDER_HDR: 1  dev-
  >priv_flags: 1
           total frames received            0
            total bytes received            0
         Broadcast/Multicast Rcvd           0

         total frames transmitted          87
          total bytes transmitted       12204
               total headroom inc           0
              total encap on xmit          87
  Device: eth0
  INGRESS priority mappings: 0:0  1:0  2:0
  3:0  4:0  5:0  6:0 7:0
  EGRESSS priority Mappings:
```

Neznačkovaná VLAN (native VLAN)

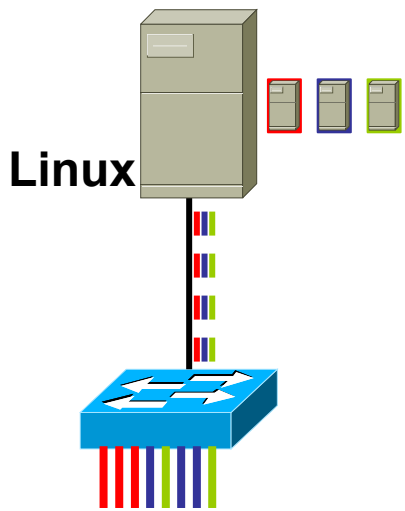
IEEE 802.1q dovoluje na trunk lince i neznačkované rámce

- Neznačkované rámce přicházejí na / odcházejí z „hlavního“ síťového rozhraní (např. eth0)
  - (různé) IP adresy mohou být současně na hlavním rozhraní i na jeho logických rozhraních přiřazených do jednotlivých VLAN

Jak poznáme, že Linux opravdu značkuje rámce ?

- Sledování provozu na logických rozhraních softwarovým síťovým analyzátorem
  - výborný a zdarma je Ethereal (www.ethereal.com)
- Na hlavním rozhraní (eth0) vidíme rámce včetně 802.1q značky
  - včetně rámců patřící všem logickým rozhraním na eth0
- Na logickém rozhraní vidíme rámce bez 802.1q hlavičky
  - Kvůli některým službám, které s rámcem pracují, ale o 802.1q značce nevědí (dhcpd apod.)
  - Zpřístupnění značky 802.1q na logickém rozhraní lze zajistit správným nastavením flagu č.1 (REORDER_HDR)
    vconfig set_flag eth0.2 1 0
  - výsledek nastavení je vidět v /proc/net/vlan/<subif-name>
- Z (IP) adresy na hlavním rozhraní rámce odcházejí neznačkované
  - a naopak přicházející neznačkované rámce jdou na ně

Hostování nezávislých služeb na jednotlivých VLAN



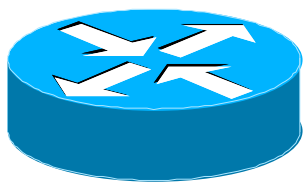
Hostování oddělených služeb pro jednotlivé zákazníky na jednom Linuxovém stroji

- Spuštění nezávislých serverů pro jednotlivé VLAN
- Každá instance služby (proces) navázána na jinou z adres přiřazených na logická rozhraní odpovídající jednotlivým VLAN
  - V konfiguraci většiny služeb možno zadat „bind address“ – IP adresu, na které služba „poslouchá“

Na co je dobré dát pozor ?

- I při vypnutí směrování v jádře Linux dovolí průchod paketů z virtuální sítě na rozhraní na tomtéž serveru, které patří do jiné VLAN
  - tedy i na server jiného zákazníka
  - paket pro cizí síť se na Linuxový stroj dostane díky nastavení výchozí brány v klientech
- Lze řešit například filtrací s použitím IPTables

Směrování mezi VLAN

Linux 

Konfigurace Linux směrovače (1)

- Vytvoření logických rozhraní pro jednotlivé VLAN (vconfig)
- Povolení směrování paketů v jádře
  `echo 1 > /proc/sys/net/ipv4/ip_forward`
- Volitelně možnost speciální konfigurace jednotlivých logických rozhraní v /etc/network/interfaces (rozšíření pro VLAN viz **man vlan-interfaces)**

- **`iface eth0.1 inet static`**
  `address 192.168.1.1`
  `netmask 255.255.255.0`
  `ip-proxy-arp 0|1`
  `ip-rp-filter 0|1|2`
  `hw-mac-address <mac-addr>`

Konfigurace Linux směrovače (2)

- Pro směrování mezi VLAN připojenými přes trunk není nic dalšího třeba
- Možnost zapojení do složitější síťové struktury a konfigurace statického nebo dynamického směrování
  - Příkaz **route**
  - Quagga (OSPF, RIP, BGP, ISIS, …)

Konfigurace VLAN na přepínači Cisco Catalyst

- **Vytvoření VLAN**

```
vlan database
 vlan 2 name DVA
 vlan 3 name TRI
 exit
```

- **Přiřazení VLAN na porty přepínače**

```
interface FastEthernet 0/1
 switchport mode access
 switchport access vlan 2

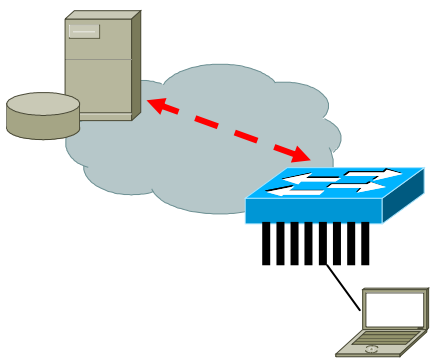
interface FastEthernet 0/2
 switchport mode access
 switchport access vlan 3
```

- **Konfigurace portu přepínače do režimu trunk**

```
interface FastEthernet 0/10
 switchport mode trunk
```

Dynamické přiřazování stanic do VLAN s použitím serverů na Linuxu

Linux VMPS/RADIUS server



OpenVMPS

OpenVMPS - VMPS server na Linuxu

- SourceForge projekt OpenVMPS
  - (aktuálně verze 1.3 – 10/2004)
  - http://sourceforge.net/project/showfiles.php?group_id=47375&package_id=40323&release_id=279202
- Výrazná úspora financí
  - není třeba vyšší model Cisco Catalyst přepínače, který VMPS implementuje
- Dostupnost i pro prostředí jen s nižšími modely přepínačů Cisco Catalyst
  - které téměř všechny umí pracovat jako VMPS klient, ale nikdy jako VMPS server

Daemon vmpsd

```
# ./vmpsd –h

    Options:
          -a ip      address to bind to (any)
          -d         do not detach, log to stderr also
          -e path    use external program for mac to vlan
                      assignment
         -f file    read VMPS database from file (/etc/vmps.db)
          -l level   set logging level:
                        0x0100 - fatal,
                        0x0200 - info,
                        0x0400 - warning,
                        0x0800 - debug,
                        0x0001 - system,
                        0x0002 - parser,
                        0x0004 – vqp
          -p port    port to listen on (1589)
```

Databáze VMPS serveru
(/etc/vmps.db)

- `vmps domain MYDOMAIN`
  - specifikace VTP domény, pro kterou vyřizujeme požadavky
- `vmps mode open`
  - v případě neúspěšné autentizace uživatele na portu nebudeme port zakazovat (stav err-disabled vyžaduje zásah administrátora)
- `vmps fallback "GUEST-VLAN"`
  - pokud není MAC adresa v databázi, přiřadíme uživatele do „GUEST-VLAN“ (volitelné)
  - Řetězec –NONE– zakazuje přiřazování do implicitní VLAN
- `vmps no-domain-req allow`
  - umožníme i dotazy neobsahující specifikaci VTP domény
- `vmps-mac-addrs`
  `address 00d0.597f.15c2 vlan-name DVA`
  …
  - definice MAC adres a jejich přiřazení do VLAN

Konfigurace VMPS klienta (přepínač Cisco Catalyst 2940)

- vmps server 10.0.0.101
  - nastavení VMPS serveru, který přiřazování do VLAN řeší
- interface range fastEthernet 0/1-10
  switchport access vlan dynamic
  - nastavení portů do režimu dynamického přiřazování VLAN
  - **show port capabilities** umožní zjistit, které z portů dynamické přiřazení podporují
- interface vlan1
  ip address 10.0.0.100 255.255.255.0
  no shutdown
  - aktivace management rozhraní (kvůli IP konektivitě mezi přepínačem a VMPS serverem)

Kontrola stavu VMPS klienta (1)

```
Switch#show vmps

  VQP Client Status:
  ---------------------
  VMPS VQP Version:   1
  Reconfirm Interval: 60 min
  Server Retry Count: 3
  VMPS domain server: 10.0.0.101
  (primary, current)
```

Statistiky vmps klienta

```
Switch#sh vmps statistics
  VMPS Client Statistics
  ----------------------
  VQP  Queries:                5
  VQP  Responses:              5
  VMPS Changes:                0
  VQP  Shutdowns:              0
  VQP  Denied:                 0
  VQP  Wrong Domain:           0
  VQP  Wrong Version:          0
  VQP  Insufficient Resource: 0
```

Sledování funkce VMPS (1)

Připojení PC s MAC adresou přiřazenou do VLAN „DVA“ do portu FastEthernet 0/3 – úspěšné přiřazení:

- **Switch: debug vqp all**
  - **03:47:45: %LINK-3-UPDOWN: Interface FastEthernet0/3, changed state to up**
    03:47:47: VQPC PAK: sending query to VMPS
    03:47:47: VQPC PAK: xmt transaction ID = 0x00000005
    03:47:47: VQPC PAK: rcvd packet from VMPS
    03:47:47: VQPC PAK: transaction ID = 0x00000005
    03:47:47: VQPC PAK: VLAN name TLV, vlanName = DVA
    03:47:47: VQPC PAK: Cookie TLV, cookie = 00d0.597f.15c2, length = 6
    03:47:47: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up

- **vmpsd –d (Linux):**
  ALLOW: 00d0597f15c2 -> DVA, switch 10.0.0.100 port Fa0/3

Sledování funkce VMPS (2)

Připojení PC s neznámou MAC adresou do portu FastEthernet 0/3:

- **Switch:**
  ```
  04:12:49: %VQPCLIENT-2-DENY: Host 00d0.597f.15c2
  denied on interface Fa0/3
  ```
- **VMPS server:**
  ```
  DENY: 00d0597f15c2 -> (null), switch 10.0.0.100 port
  Fa0/3
  ```
- vmpsd produkuje log, který nám umožní zjistit, který uživatel je právě na kterém portu
- **Přiřazení portu do VLAN trvá cca 2-3 vteřiny**

Co ještě můžeme v databázi VMPS nastavit ?

`vmps no-domain-req deny`

- Nedovolíme dotazy z VMPS klientů, kteří nemají nastavenu doménu
- POZOR, když není doména na přepínači nenastavena vůbec, OpenVMPS hlásí domain mitchmatch i při **no-domain-req allow**

```
DOMAIN MISMATCH: 00d0597f15c2 -> (null), switch
10.0.0.100 port Fa0/3
```

`vmps mode secure`

- Port, na kterém proběhla neúspěšné přiřazení klienta do VLAN, bude zakázán (odpověď SHUTDOWN, stav err-disable)

Omezení připojování do VLAN jen z některých portů

- /etc/vmps.db:
  `vmps-port-policies vlan-name DVA device 10.0.0.100 port Fa0/2`
  - Pozor na zkrácené jméno interface (!)

- Lze i více řádků pro různé porty nebo použít port-groups:

```
vmps-port-group PGRP
 device 10.0.0.100 port Fa0/2
 device 10.0.0.100 port Fa0/4
vmps-port-policies vlan-name DVA
  port-group PGRP
```

- Lze i míchat omezení pro port groups a jednotlivé porty
- Lze použít i VLAN groups pro společné povolení vstupu do skupiny VLAN z portu nebo z pojmenované skupiny portů jedním příkazem **vmps-port-policies**

Implicitní VLAN závislý na portu (1)

- ```
  vmps-port-group PGRP1
   fallback-vlan DVA
   device 10.0.0.100 port Fa0/2
   device 10.0.0.100 port Fa0/3
  !
  vmps-port-group PGRP2
   fallback-vlan TRI
   device 10.0.0.100 port Fa0/4
   device 10.0.0.100 port Fa0/5
  ```

- ```
  vmps-vlan-group VSECHNY_VLAN
   vlan-name DVA
   vlan-name TRI
   vlan-name CTYRI
  ```

- ```
  vmps-port-policies vlan-group VSECHNY_VLAN port-group
  PGRP1
  vmps-port-policies vlan-group VSECHNY_VLAN port-group
  PGRP2
  ```

- lze zkombinovat i s globální fallback-vlan
  ```

Implicitní VLAN závislý na portu (2)

Výsledek (log VMPS serveru):

```
ALLOW: 00d0597f15c2 -> DVA, switch
10.0.0.100 port Fa0/2
ALLOW: 00d0597f15c2 -> DVA, switch
10.0.0.100 port Fa0/3
ALLOW: 00d0597f15c2 -> TRI, switch
10.0.0.100 port Fa0/4
ALLOW: 00d0597f15c2 -> TRI, switch
10.0.0.100 port Fa0/5
```

Rozšíření OpenVMPS

- K MAC adresám v databázi lze přiřadit SPEED a DUPLEX podle schopností klientovy karty
  - Při vpuštění daného klienta do sítě OpenVMPS umí pomocí SNMP SET nastavit duplex a rychlost na příslušném portu daného portu
    - V konfiguraci musí být nastavena SNMP komunita pro RW
      - snmp community <rw-comm-name>
    - Musí být přeloženo s podporou SNMP
- Plus cokoli dalšího si doprogramujete – zdrojové texty máte ;-)
  - lákavě vypadá přiřazování do VLAN na základě jiných parametrů, než MAC adresa

Testování VMPS serveru bez použití přepínače

```
$ vqpcli.pl

  Options:
  -s ip       VMPS Server to query
  -v domain   VMPS/VTP Domain to query
  -w ip       client switch IP to query for
  -i iface    client switch Interface name
  -m macaddr  attached device MAC address
                in nnnn.nnnn.nnnn format
  -c vlan     Vlan to reconfirm membership to
```

Použití externího programu pro přiřazení uživatele do VLAN

- **vmpsd –e <program>**
- Parametry do i z externího programu textově (stdin/stdout)
  - Program očekává na stdin:
    - DOMAIN, CLIENT_IP, PORT_NAME, MAC
  - Na stdout má vypsat:
    - ALLOW <VLANname>
    - DENY/SHUTDOWN
- V distribuci je ukázkový shell script přiřazující na základě pevné textové databáze

FreeRadius

FreeRadius

- http://www.freeradius.org
- Volně dostupná a v reálném provozu ověřená implementace RADIUS protokolu
  - dokumentace bohužel dosti chudá
- Lze instalovat i z balíčku

Mapování uživatelů WIFI do VLAN s použitím RADIUS serveru

Probíhá v rámci autentizace přístupu do sítě (MAC address authentication)

1. Uživatel se asociuje s AP s použitím libovolného SSID konfigurovaného na AP
   - (např. Cisco Aironet 1100 umí více SSID)
   - Se SSID je svázáno implicitní číslo VLAN
2. AP (RADIUS klient) autentizuje nového uživatele podle MAC adresy na RADIUS serveru
   - IP adresa/port serveri + šifrovací klíč RADIUS protokolu na AP nakonfigurovány
3. RADIUS server přístup do sítě povolí nebo zamítne a navíc může (podle své konfigurace) poslat volitelný atribut přiřazující MAC adresu daného uživatele do VLAN
   - Pokud MAC adresu do VLAN nepřiřadí, zůstane uživatel ve VLAN svázaném se SSID, přes který se přihlásil

Atributy RADIUS protokolu pro přiřazování do VLAN

IETF 64 (Tunnel Type): “VLAN”
IETF 65 (Tunnel Medium Type): “802”
IETF 81 (Tunnel Private Group ID): VLAN-ID

- V požadovaných hodnotách atributů se mohou AP jednotlivých výrobců AP lišit
- Liší se i způsob zadání hodnot těchto atributů do databáze RADIUS serveru (často nedokumentováno)
- Formát pro FreeRadius:

```
00012481618f Auth-Type := Local, User-Password == "00012481618f”
      Tunnel-Type:1 = 13,
      Tunnel-Medium-Type:1 = 6,
      Tunnel-Private-Group-Id:1 = <VLAN_ID>
```

Na rozdíl od VMPS serveru se zde VLAN identifikují číslem (802.1q tag)

Konfigurace přiřazování WiFi zařízení do VLAN pomocí server RADIUS

(FreeRadius – Cisco Aironet 1100)

1. Konfigurace protokolu RADIUS

- Přístupový bod
  - konfigurace management rozhraní v rámci bridge group pro VLAN 1
  - konfigurace RADIUS serveru a sdíleného klíče

```
interface BVI 1
 ip address 10.0.0.1 255.255.255.224

aaa new-model
radius-server host 10.0.0.2 auth-port 1812 acct-port
1813
radius-server key 7 NASKLIC
```

- FreeRadius: konfigurace RADIUS klienta oprávněného k přístupu a sdíleného klíče: /etc/freeradius/clients.conf

```
client 10.0.0.1 {
 secret  = NASKLIC
 shortname =  mojeAP
 nastype = cisco
}
```

2. Konfigurace databáze RADIUS serveru

- Konfigurace MAC adres oprávněných uživatelů a (volitelně) jejich přiřazení do VLAN: /etc/freeradius/users

```
# Toshiba PDA -> VLAN 2
00012481618f Auth-Type := Local, User-Password ==
"00012481618f“
   Tunnel-Type:1 = 13,
   Tunnel-Medium-Type:1 = 6,
   Tunnel-Private-Group-Id:1 = 2

# Notebook Compaq -> VLAN 3
00022d8e36d8 Auth-Type := Local, User-Password ==
"00022d8e36d8"
```

- POZOR: formát zápisu MAC adresy a heslo závisí na výrobci AP (RADIUS klienta)
- Restart RADIUS serveru: /etc/init.d/freeradius restart
- Ověření správného startu v /var/log/freeradius/radius.log

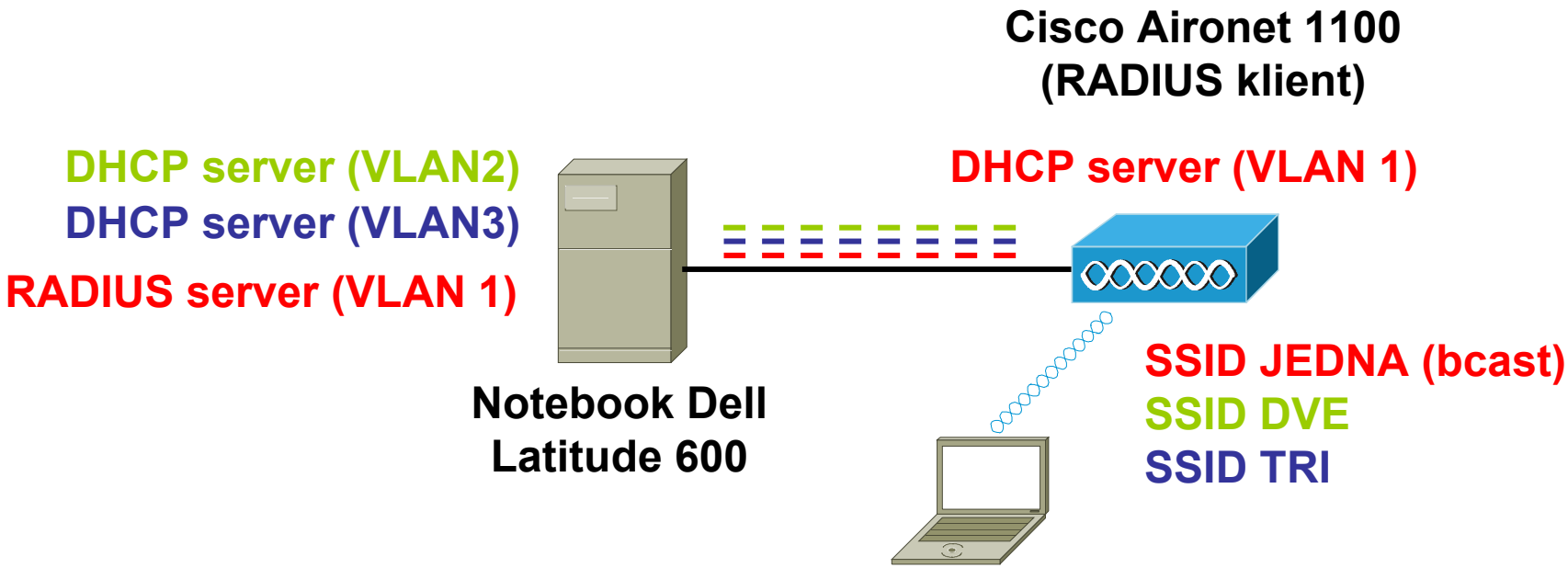
3. Konfigurace přístupového bodu

- Konfigurace FastEthernet rozhraní pro připojení do infrastruktury do režimu trunk
  - Konfigurace subinterfaces a jejich přiřazení do VLAN
- Konfigurace subinterfaces rádiového rozhraní odpovídající jednotlivým VLAN
- Konfigurace přemosťování (bridging) vždy mezi odpovídajícími subinterfaces FastEthernet a rádiového rozhraní
  - definice samostatné bridge group pro každou dvojici subinterfaces
- Konfigurace (aspoň jednoho) SSID na rádiovém rozhraní a přiřazení VLAN implicitně přidělovaného uživatelům asociovaným s tímto SSID
  - Pokud během asociace RADIUS server předá pro uživatele přiřazené číslo VLAN, uživatel do ní bude přeřazen
- Vyžádání autentizace na RADIUS serveru podle MAC adres během asociace uživatelů s jednotlivými SSID přístupového bodu

Varianty konfigurace

- Jeden SSID a jemu přiřazený VLAN
  - Uživatelé, pro něž RADIUS nepřiřadí VLAN (ale ověří jejich MAC adresu), zůstanou ve VLAN přiřazené SSID
- Více SSID s různými přiřazenými VLAN
  - Uživatelé mohou přistupovat přes různé SSID, podle toho jsou (po ověření MAC adresy) zařazeni do VLAN přiřazené jejich SSID
    - podle normy AP propaguje (broadcast) jen jedno z těchto SSID, některé AP ale umí propagovat i více SSID
  - RADIUS dovoluje i ověřování, zda uživatel může přistoupit přes daný SSID (neodzkoušeno)

Zařazování bezdrátových uživatelů do VLAN pomocí FreeRADIUS (1)



Uživatelské zařízení s danou MAC adresou, VLAN přiřazena z RADIUS nebo podle SSID, IP adresa z DHCP

Zařazování bezdrátových uživatelů do VLAN pomocí FreeRADIUS (2)

- AP přiděluje adresy v rámci VLAN1 (DHCP)
- Management rozhraní AP i Linux s RADIUS serverem na VLAN1
- Linux připojen trunk linkou, tou k němu jde VLAN 1, 2 a 3
- Pro uživatele na VLAN 2 a 3 Linux přiděluje adresy pomocí daemona dhcpd

Úplné konfigurační soubory k dispozici na WWW

Výsledky testování zařazování do VLAN pomocí FreeRADIUS

- Vše funkční
- Do sítě lze vstoupit přes libovolné SSID
  - Pokud v databázi RADIUS serveru není pro MAC adresu uživatele přiřazena VLAN, uživatel zůstane ve VLAN přiřazené k SSID
  - Pokud VLAN přiřazena je, uživatel je do této VLAN okamžitě po autentizaci přemístěn
- Stále zůstává riziko podvržení MAC adres, přiřazování do VLAN podle MAC adres je vhodné zkombinovat ještě s autentizací uživatele např. pomocí certifikátu a EAP-TLS

Sledování funkce

- Linux server

  `freeradius -x`

  `dhcpd -d`
  - zůstanou na popředí a na stdout vypisují log

- AP

  `debug radius`

  `show radius statistics`

Sledování funkce: Připojení stanice s MAC adresou z VLAN 3. RADIUS server

```
linux# freeradius –x

rad_recv: Access-Request packet from host 10.0.0.1:21645,
 id=195, length=108
      User-Name = "00022d8e36d8”
      User-Password = "00022d8e36d8”
      Called-Station-Id = "0011.21b9.2630“
       Calling-Station-Id = "0002.2d8e.36d8„
      NAS-Port-Type = Wireless-802.11
      NAS-Port = 464
      Service-Type = Framed-User
      NAS-IP-Address = 10.0.0.1

 Sending Access-Accept of id 195 to 10.0.0.1:21645
      Framed-IP-Address = 255.255.255.254
      Framed-MTU = 576
      Service-Type = Framed-User
      Tunnel-Type:1 = VLAN
      Tunnel-Medium-Type:1 = IEEE-802
      Tunnel-Private-Group-Id:1 = "3"
```

Sledování funkce: dhcpd

```
linux# dhcpd –d eth0.2 eth0.3
DHCPDISCOVER from 00:02:2d:8e:36:d8 via eth0.3
DHCPOFFER on 30.0.0.4 to 00:02:2d:8e:36:d8 via eth0.3
DHCPREQUEST for 30.0.0.4 from 00:02:2d:8e:36:d8 via
eth0.3
DHCPACK on 30.0.0.4 to 00:02:2d:8e:36:d8 via eth0.3
```

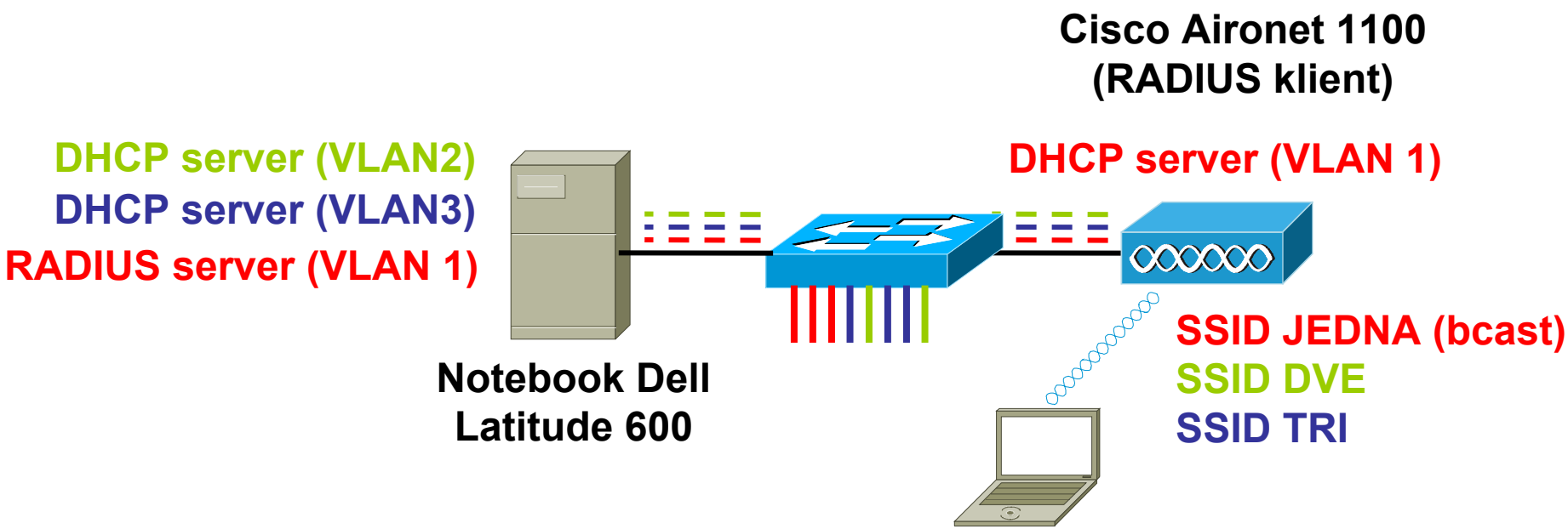
Sledování funkce: Přístupový bod (AP)

```
ap#sh dot11 associations all-client
  Address             : 0002.2d8e.36d8     Name                : 
  IP Address          : 30.0.0.4           Interface           : Dot11Radio 0
  Device              :    -               Software Version    : 

  State               : MAC-Assoc          Parent              : self
  SSID                : JEDNA              VLAN                : 3
  Hops to Infra       : 1                  Association Id      : 208
  Clients Associated  : 0                  Repeaters associated: 0
  Key Mgmt type       : NONE               Encryption          : Off
  Current Rate        : 11.0               Capability          :Supported
  Rates   : 1.0 2.0 5.5 11.0
  Signal Strength     : -48  dBm           Connected for       : 278 seconds
  Signal Quality      : N/A                Activity Timeout    : 16 seconds
  Power-save          : Off                Last Activity       : 44 sec ago

  Packets Input       : 85                 Packets Output      : 111
  Bytes Input         : 11479              Bytes Output        : 12666
  Duplicates Rcvd     : 0                  Data Retries        : 0
  Decrypt Failed      : 0                  RTS Retries         : 0
  MIC Failed          : 0
```

Reálná aplikace: připojení do přepínané struktury s VLAN



Možnosti integrace řešení s VMPS a RADIUS servery

Nechceme udržovat odděleně databázi MAC adres pro VMPS a RADIUS

- Primární databáze na VMPS serveru
  - Možno zkonfigurovat RADIUS, aby se ptal VMPS serveru
    - Možná rozšířit – zdrojové texty k dispozici
    - VMPS klient v Perlu je k dispozici (vqpcli)
- **Primární databáze na RADIUS serveru**
  - VMPS server může pro účely zjištění přiřazení MAC-> VLAN volat externí program (příklad je k dispozici)
    - Může jít o RADIUS klienta

Shrnutí - ověřené konfigurace

- Přepínač Cisco Catalyst 2940 propojený trunk linkou s notebookem Dell Latitude 600 Linux Ubuntu kernel 2.6.1.10
  - Konfigurace VLAN
  - Směrování mezi VLAN
  - Hostování serverů na různých VLAN
- Přístupový bod Cisco Aironet 1100 propojený trunk linkou s notebookem Dell, FreeRADIUS + dhcpd
  - Autentikace uživatelů rádiové sítě (PDA Toshiba a notebook Compaq Armada 110) MAC adresou na RADIUS serveru a jejich přiřazování do VLAN
- Přepínače Cisco Catalyst 1900/2940/2950 propojené vždy standardní Ethernet linkou s notebookem Dell a OpenVMPS
  - Přiřazovní klientů do VLAN podle databáze VMPS serveru, přiřazování do implicitní VLAN, odmítnutí klienta s určitou MAC adresou, omezení připojování do VLAN jen na určité porty

Co je dobré o virtuálních sítích ještě tušit ?

aneb kdyby nám zbyla ještě trocha času…

- Multi-VLAN porty
- Spanning Tree a VLAN
  - Common Spanning Tree (802.1q)
  - Per-VLAN Spanning Tree
  - Multi-Instance Spanning Tree (802.1s)
- Tunelování VLAN
- …

Reference

- Semestrální projekty předmětu Směrované a přepínané sítě, VŠB-TU Ostrava, červen 2005, http://www.cs.vsb.cz/grygarek/TPS/Projekty0405Z.html:
  - Jaššo, P., Chalupka, T.: Podpora QoS na Cisco 3550 a 2950T.
  - Staněk, F.: VLAN Membership Policy Server a protokol VQP - dynamické přiřazování do VLANů.
  - Huňka, T.: Konfigurace RADIUS serveru pro ověřování uživatelů pomocí certifikátu a EAP-TLS.
- www.cisco.com – dokumentace k produktům