

VLAN Membership Policy Server a protokol VQP

Dynamické přiřazování do VLANů.

Úvod

Protokol VLAN Query Protocol (dále jen VQP) je proprietární protokol firmy Cisco Systems (dále jen Cisco) pro dynamické přiřazování koncových stanic do VLANů (Virtual LAN – Virtuální síť LAN). Přiřazování stanic do jednotlivých VLANů probíhá na základě jejich MAC adresy. Funguje na principu klient—server, kde klienty jsou „koncové“ přepínače řady Catalyst (v současné době ověřeny modely 1900, 2950 a 3750) a jako server slouží přepínače řady 5000 a 6000. Server je celým názvem v terminologii firmy Cisco označován jako VLAN Membership Policy Server (dále jen VMPS).

Na serveru se definuje databáze obsahující informaci které MAC adresy patří do kterého VLANu. Klientský přepínač, který má na svém portu připojené koncové zařízení s nějakou MAC adresou, tuto zjistí po prvním přijatém rámci koncového zařízení (zdrojová MAC adresa, např. DHCP dotazu) a zašle dotaz na VMPS server. Podle obdržené odpovědi tento VLAN nastaví.

Tolik krátký úvod. Nyní se podíváme trochu blíže na protokol VQP jako takový.

VLAN Query Protocol – VQP

Dotazy klientského přepínače na VMPS server a odpovědi serveru zpět jsou realizovány pomocí dotazů/odpovědí protokolu VQP. Pro přenos zpráv VQP protokolu se používají datagramy protokolu UDP. VMPS server standardně poslouchá na portu UDP/1589. Informace zasílané ve zprávách VQP protokolu jsou většinou ve tvaru čistého textu (např. název VLANu, portu kde je připojené koncové zařízení), nebo celého kladného čísla (např. IP adresa, MAC adresa).

Struktura zpráv VQP je následující:

Dotaz:

```
-----
| MSG_TYPE | RET_CODE | MAG_CON1 | SID | U_VAR1 | PORT + LN + STR |
=====
| 2B       | 1B       | 4B       | 2B  | 9B       | 3B  + 2B + 5B  |
-----
```

```
-----
| VLAN + LN + STR | DOMAIN + LN + STR | U_VAR3 | REQ_MAC |
=====
| 3B  + 2B + 32B | 3B      + 2B + 32B | 7B     | 11B    |
-----
```

Odpověď:

MSG_TYPE	RET_CODE	MAG_CON2	SID	VLAN	LN	STR	REP_MAC
2B	1B	4B	2B	3B	2B	32B	11B

Dotaz a odpověď se od sebe rozlišují druhým bajtem ve zprávě (první bajt má vždy hodnotu 01).

Inicializační dotaz má hodnotu 01.

Opakovaný dotaz (pracovně nazván "ReRequest") má hodnotu 03.

Odpověď má hodnotu 02, ovšem rozlišuje se zde několik "podtypů". Tyto jsou jednoznačně identifikovány třetím bajtem, dle situace:

a) hodnota 00 - port je povolen, vrací se známý VLAN.

b) hodnota 01 -

c) hodnota 03 - port zůstává neaktivní (není "shozen")

d) hodnota 04 - port je "shozen" (shutdown), tedy VLAN nenastaven

e) hodnota 05 - "špatně formulovaný" dotaz (např. neplatný název VTP domény), port zůstává v původním stavu

ad a) platí i pro případ přidělení portu do "default" VLANu, v případě kdy není známá MAC adresa. V tomto případě se tedy vrací název tohoto VLANu.

Osmý bajt jednoznačně identifikuje relaci dotaz-odpověď (pracovně nazván "Session ID").

Parametry:

1) port klientského switch-e (který má být přiřazen do patřičného VLANu)

2) název VLANu

3) název VTP domény

4) MAC adresa (klienta na daném portu přepínače) v požadavku

jsou ve zprávách předávány jako řetězec. Tyto texty jsou pomocí dvou bajtů jednoznačně identifikovány jako výše uvedený typ (1 až 3). Za touto "deklarací typu" následuje informace o délce tohoto řetězce (2B). Samotný řetězec je ještě "pro jistotu" ukončen nulou (00), má maximální délku 32 znaků.

00 0C 01 - U_VAR1: neznámo, délka 4, vždy následuje sekvence bytů: 01 01 01 03

00 0C 02 - například: Fa0/2

00 0C 03 - například: vlan_2

00 0C 04 - například: MYVMPSDOMAIN

00 0C 06 - REQ_MAC: MAC adresa klienta v odpovědi

00 0C 07 - U_VAR3: neznámo, délka

00 0C 08 - REP_MAC: MAC adresa klienta v odpovědi

MAG_CON1 - 06 00 00 00

MAG_CON2 - 02 00 00 00

VLAN Membership Policy Server – VMPS

VMPS server má databázi vazeb dvojic MAC adres koncových stanic a VLANů. Server naslouchá dotazům a po přijetí korektního dotazu klientského přepínače prohledá tuto databázi. Najde-li v databázi dotazovanou MAC adresu a k ní přiřazený VLAN, odpoví klientskému přepínači s uvedeným názvem VLANu.

Je-li ovšem k dané adrese asociovaný VLAN omezen na tzv. *skupinu portů (port group)*, porovná navíc VMPS server port uvedený v požadavku klienta s porty uvedenými ve skupině portů se kterými je MAC adresa a VLAN asociován. Je-li port z požadavku shodný s portem ve skupině portů, odpoví VMPS server klientskému přepínači s uvedeným názvem VLANu.

VMPS vždy pracuje v jednom ze dvou možných bezpečnostních módů: *secure* a *open*.

V případě korektních dotazů klientských přepínačů, obsahujících MAC adresu pro kterou je přiřazen VLAN (a případně i shodným portu patřícího do skupiny portů daného VLANu) se oba módy od sebe nijak neliší.

Ovšem situace se mění v případech kdy:

- v dotazu je uvedena MAC adresa, která není v databázi
- v dotazu je MAC adresa s VLANem, který patří do jiné skupiny portů, než kde je povolen v databázi

V těchto případech se v módu *secure* daný port *administrativně shodí (port shutdown)* zasláním odpovědi obsahující příkaz pro tuto operaci. Je-li VMPS v módu *open*, zašle se pouze odpověď *odepření přístupu (access denied)*, ovšem port zůstane *nahozený*.

Situaci v módu *open* ještě může změnit nastavení parametru *fallback VLANu*. Je-li takovýto VLAN *poslední záchrany* nastaven, je v odpovědi na dotaz právě jeho název.

VMPS ve svém nastavení podporuje také explicitní zákaz přidělení VLANu konkrétní MAC adrese. Realizuje se tak pomocí nastavení VLANu s názvem *--NONE--* konkrétní MAC adrese. V případě obdržení dotazu s takovouto MAC adresou VMPS zašle odpověď typu *odepření přístupu*, nebo *administrativního shození*, v závislosti na módu (*open* resp. *Secure*).

Přepínače podporující dynamické přidělování VLANů

Zjištění podpory dynamického přidělování VLANů pomocí VQP protokolu lze zjistit na klientském přepínači po zadání příkazu:

```
show port capabilities
```

Konfigurace VMPS

1. nastavení VMPS domény – stejná jako VTP (VLAN Trunking Protocol) doména, čísla a názvy VLANů jsou potom stejné na serveru i klientech
2. nastavení bezpečnostního módu – možné hodnoty jsou open a secure
3. (případné) nastavení fallback VLANu – hodící se pouze pro určité konfigurace, nutnost bezpečnostního módu open
4. nastavení nutnosti domény v požadavku – takto lze ovlivnit, zdali v požadavku musí být uvedena VMPS doména
5. nastavení vazeb MAC adres a názvů VLANů
6. (případné) nastavení skupin portů – takto lze přiřadit více portů do jedné logické skupiny
7. (případné) nastavení skupin VLANů – takto lze přiřadit více VLANů do jedné skupiny
8. (případné) nastavení politiky pro porty

Nastavení skupin v bodech 6 a 7 je vhodné pro snazší manipulaci s více porty/VLANy.

Konkrétní konfigurace VMPS

- (1)
`vmips domain MYVMPSDOMAIN`
- (2)
`vmips mode open`
- (3)
`vmips fallback --NONE--`
- (4)
`vmips no-domain-req deny`
- (5)
`vmips-mac-addr`
`address 0002.b32b.69a9 vlan-name ORANGE`
`address 0002.b32b.69f6 vlan-name BLUE`
- (6)
`vmips-port-group myports`
`device 192.168.0.2 port 0/3`
`device 192.168.0.2 port 0/4`
`device 192.168.0.3 all-ports`
- (7)
`vmips-vlan-group myvlans`
`vlan-name ORANGE`
`vlan-name RED`
- (8)
`vmips-port-policies vlan-group myvlans`
`port-group myports`

Konfigurace klientského přepínače

1. nastavení VMPS serveru
2. nastavení přiřazování VLANu na portech
3. (případně) nastavení VTP/VMPS domény

Konkrétní konfigurace klientského přepínače

```
enable
configure terminal
```

(1)

```
vmps server 192.168.0.1
```

(2)

```
interface fastEthernet 0/2
    switchport access vlan dynamic
```

(3)

```
vtp domain MYVMPSDOMAIN
```

Realizace VMPS serveru na OS Linux – případová studie

Po předchozí analýze VQP protokolu lze funkci VMPS serveru realizovat pomocí programu pracujícím nejlépe v operačním systému GNU/Linux. Výhody jsou především cena, dostupnost, možnost jednoduché vzdálené správy atd.

Vhodná varianta je k dispozici na internetu na adrese:

http://sourceforge.net/project/showfiles.php?group_id=47375&package_id=40323&release_id=279202

K zprovoznění této aplikace je potřeba vykonat následující:

1. Stáhnout zdrojové kódy aplikace. Jde o balík `vmpsd-X.Y.tar.gz`, kde X a Y jsou čísla verze aplikace.
2. Rozbalit zdrojové kódy:

```
tar -zxvf vmpsd-X.Y.tar.gz -C /usr/local/src
```
3. Připravit kompilaci zdrojových kódů:

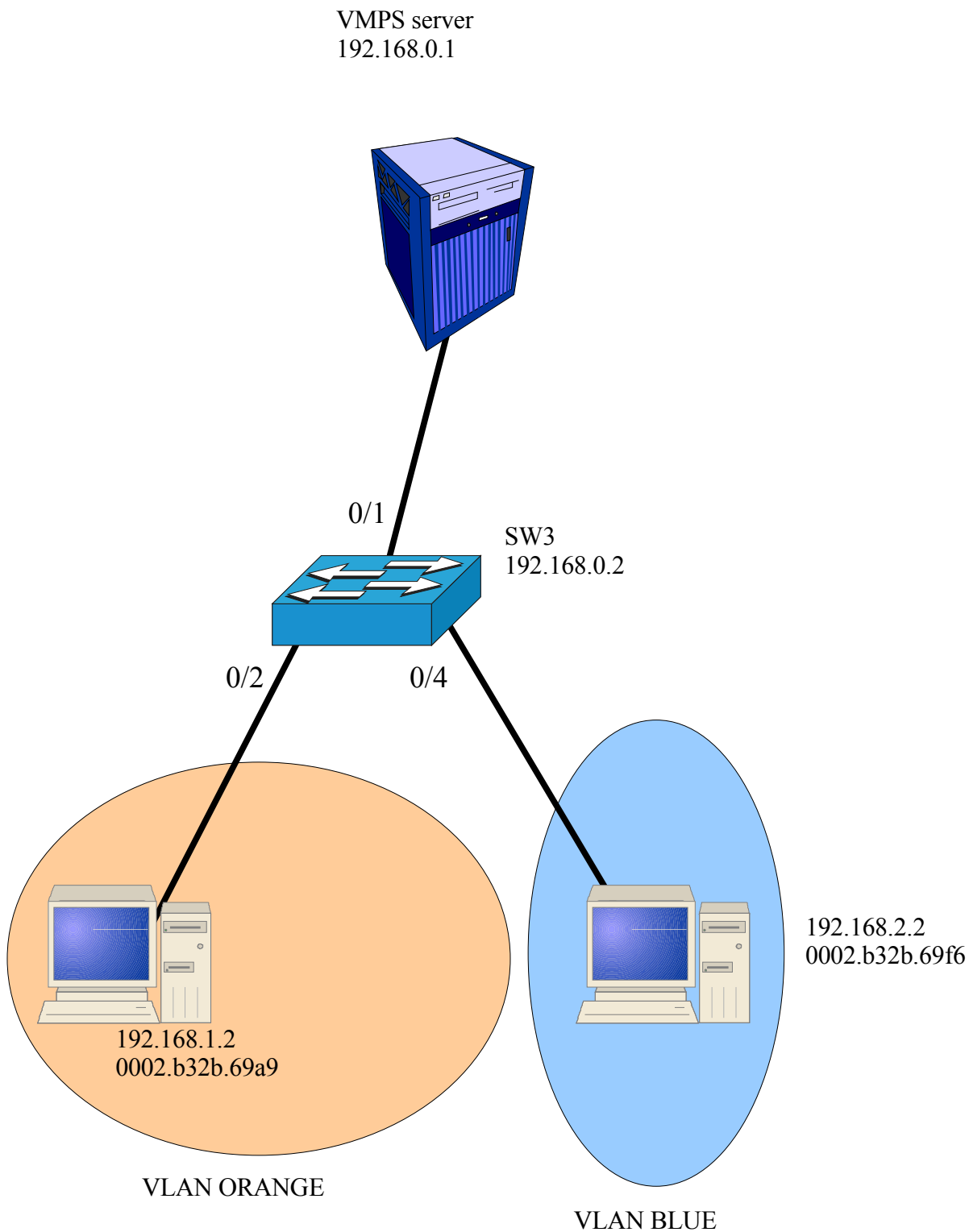
```
cd /usr/local/src/vmpsd
./configure --prefix=/usr/local/vmpsd
```
4. Zkompilovat zdrojové kódy:

```
make
```
5. Nainstalovat aplikaci:

```
make install
```
6. Zkonfigurovat aplikaci, přesněji nakonfigurovat VMPS server.
Editovat soubor `/usr/local/vmpsd/etc/vlan.db`
7. Spustit aplikaci:

```
/usr/local/vmpsd/bin/vmpsd -f /usr/local/vmpsd/etc/vlan.db
```

Případová studie konkrétní konfigurace VMPS serveru (implementace VMPSD na OS Linux) a koncového klienta (přepínač Cisco Catalyst 2950):



Konfigurace VMPS serveru, soubor **vlan.db**:

```
!vmps domain <domain-name>
! The VMPS domain must be defined.
!vmps mode { open | secure }
! The default mode is open.
!vmps fallback <vlan-name>
!vmps no-domain-req { allow | deny }
!

vmps domain MYVMPSDOMAIN
vmps mode open
vmps fallback --NONE--
vmps no-domain-req deny

!
!MAC Addresses
!
vmps-mac-addrs
!
! address <addr> vlan-name <vlan_name>
!
! vlan ORANGE restricted
address 0002.b32b.69a9 vlan-name ORANGE
! vlan BLUE unrestricted
address 0002.b32b.69f6 vlan-name BLUE

!
!Port Groups
!
!vmps-port-group <group-name>
! default-vlan <vlan-name>
! fallback-vlan <vlan-name>
! device <device-id> { port <port-name> | all-ports }
!
vmps-port-group myports
  device 192.168.0.2 port 0/3
  device 192.168.0.2 port 0/4

!
!VLAN groups
!
!vmps-vlan-group <group-name>
! vlan-name <vlan-name>
!
vmps-vlan-group myvlans
  vlan-name ORANGE

!
!VLAN port Policies
!
!vmps-port-policies {vlan-name <vlan_name> | vlan-group <group-name> }
! { port-group <group-name> | device <device-id> port <port-name> }
!
vmps-port-policies vlan-group myvlans
  port-group myports
```

Konfigurace klientského přepínače SW3 (příkazy IOSu):

```
enable
!      vlan database
!      vtp transparent
!      vlan 2 name ORANGE
!      vlan 3 name BLUE
!      vlan 4 name RED
!      apply

configure terminal
    vtp domain MYVMPSDOMAIN

    vmps server 192.168.0.1

    interface vlan 1
        ip address 192.168.0.254 255.255.255.0
        no shutdown

    interface fastEthernet 0/1
        switchport mode access
        switchport access vlan 1

    interface fastEthernet 0/2
        switchport access vlan dynamic

    interface fastEthernet 0/4
        switchport access vlan dynamic
```