# ROUTAGE VIRTUEL AVEC VRF

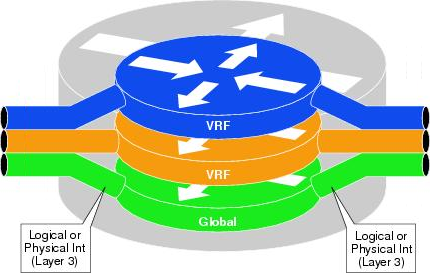
Description du thème

|  |  |
| --- | --- |
| Propriétés | Description |
| **Intitulé long** | Initiation au routage virtuel avec VRF |
| **Formation(s) concernée(s)** | BTS Services Informatiques aux Organisations, option SISR |
| **Matière(s)** | SISR5 - en fin de seconde année. |
| **Présentation** | Démontrer comment on peut séparer, au sein d’un routeur de prestataire, les réseaux client indépendamment de l’usage d’ACL ou de pare-feux.  Attention : il s’agit d’un thème d’exploration situé en bordure de ce qui est demandé en BTS SIO. La ressource est proposée aux enseignants en mode « auto-formation » et pourra être proposée à certains étudiants en fin de deuxième année. |
| **Savoirs** | Routage, VLAN, sous-interfaces, routage virtuel |
| **Compétences** | Installer et configurer un protocole d'administration d’un élément d'interconnexion réseau Sécuriser une infrastructure réseau |
| **Transversalité** | - |
| **Prérequis** | Maîtrise des VLAN et du routage. |
| **Outils** | Routeurs CISCO (1801 et 1760) et un commutateur de niveau 2 Le routeur 1801 qui implémente VRF est en version 15.1 |
| **Mots-clés** | Routage, routage virtuel, VRF |
| **Durée** | 4h |
| **Auteur(es)** | Eve-Marie Gallot, avec le concours de Patrice Dignan et Denis Gallot, relecture Yann Barrot, David Duron |
| **Version** | v 1.0 |
| **Date de publication** | avril 2018 |

Côté Labo : routage virtuel avec VRF   
Virtual Routing and Forwarding (Cisco)

#### Présentation

VRF est une technologie Cisco qui permet de segmenter un routeur physique en plusieurs routeurs virtuels. Le mode VRF permet à un routeur de gérer simultanément plusieurs tables de routage. Ces tables de routage sont indépendantes, **il est donc possible d’utiliser des adresses IP identiques ou qui se chevauchent** dans les réseaux des clients. Le VRF permet une segmentation des routeurs au niveau 3, un peu comme les VLAN permettent une segmentation des commutateurs au niveau 2.



*Source : cisco.com*

Cette technologie est intéressante pour les opérateurs ou les hébergeurs qui souhaitent isoler les tables de routages de leurs clients. Le VRF peut être couplé avec du VPN et des protocoles de routage dynamiques.

##### Le contexte

Un hébergeur gère des services (hébergement, FAI) pour deux clients One et Two. Chaque client a deux sites distants reliés à un même routeur physique.

L’objectif consiste à mettre en place deux routeurs virtuels (VRF) isolés sur le routeur de l’hébergeur, un pour chaque client.

##### L’atelier de test

**Préambule**

Cette ressource concerne un thème non encore abordé dans le cadre du Certa et situé aux limites du programme de la spécialité SISR. Elle est proposée pour auto-formation aux enseignants mais elle peut-être également proposée à des étudiants aguerris dans le cadre d’un TP de 3 à 4 heures.

Le travail sur un routeur de fournisseur d’accès est peu courant en BTS SIO.

L’utilisation de sous-interfaces peut compliquer la compréhension de l’activité mais cela permet de s’affranchir de la contrainte du nombre limité d’interfaces des routeurs et même de travailler avec des routeurs munis de seulement deux interfaces.

Dans un premier temps, on se limitera à représenter les sites clients par de simples ordinateurs selon les schémas logique et physique ci-dessous.

Dans un contexte réel, le routeur Rt-H ci-dessous serait connecté aux points d’arrivée des liens distants avec les sites clients.

Schéma logique

Le poste A1 représente par exemple le site A1 du client One ; le poste B2, le site B2 du client Two

On a donc deux réseaux clients et quatre sites au total

Schéma physique



Remarque : On peut se contenter de deux postes client et les affecter successivement dans les différents VLAN en modifiant le paramétrage IP

On utilise un routeur Cisco 1801 et un commutateur HP Procurve 2620. Les caractéristiques des équipements sont décrites en annexe du document. Il est nécessaire d’utiliser un routeur Cisco pour mettre en place VRF.

On affecte les sous-interfaces du port fa0 aux quatre sites clients. Chaque interface transporte un VLAN séparé. Le n° de VLAN correspond au troisième octet de l’adresse IP attribuée à la sous-interface.

Le routeur est relié au port 25 du commutateur en mode *étiqueté* pour le transport de vlan (T : port Taggué) qui gère les quatre VLAN 11, 12, 21 et 22. Le poste A1 est par exemple relié au port 11 qui est affecté au VLAN 11.

Un poste d’administration (non représenté sur le schéma) permet de configurer les équipements réseaux en mode console ou en accès Telnet.

Note :

On utilise ici des sous-interfaces de l’interface fa0 du routeur RtH. On pourrait également mettre en place cette activité sans sous-interface si on disposait de routeurs dotés d’au moins quatre interfaces.

#### La mise en œuvre

*La mise en œuvre se déroulera selon les étapes suivantes :*

1. Étape 1 : mise en place des équipements et du routage simple sans routage virtuel ;
2. Étape 2 : mise en place du routage virtuel avec VRF ;
3. Étape 3 : adresses IP identiques dans les deux VRF ;
4. Étape 4 : test du routage virtuel avec un routeur sur un site client.

##### Étape 1 : mise en place d’un routage simple sans routage virtuel

**Objectif :** Mettre en place et valider l’infrastructure réseau.

**Mise en place**

*L’infrastructure est conforme aux schémas précédents.*

* Mettre en place les branchements physiques.
* Configurer l’architecture de VLAN dans le commutateur.
  + Création des VLAN et configuration des ports

Switch(config)#**VLAN 11**

Switch(vlan-11)#name A1

Switch(vlan-11)#untagged 11

Switch(vlan-11)#tagged 25

Switch(config)#**VLAN 12**

Switch(vlan-12)#name A2

Switch(vlan-12)#untagged 12

Switch(vlan-12)#tagged 25

Switch(config)#**VLAN 21**

Switch(vlan-21)#name B1

Switch(vlan-21)#untagged 21

Switch(vlan-21)#tagged 25

Switch(config)#**VLAN 22**

Switch(vlan-22)#name B2

Switch(vlan-22)#untagged 22

Switch(vlan-22)#tagged 25

* Configurer les interfaces du routeur.
  + Configurer chaque sous-interface, par exemple :

Rt-H(config)#**interface fa0.11**

Rt-H(config-subif)#**encapsulation dot1Q 11**

Rt-H(config-subif)#**ip address 192.168.11.254 255.255.255.0**

* + Activer le port Fa0

Rt-H(config)#**interface fa0**

Rt-H(config-if)#**no shutdown**

* Effectuer la configuration IP des postes.

**Tests de Validation**

* Afficher la table de routage du routeur : les quatre routes, connectées chacune à un réseau client, doivent s’afficher.

Rt-H#**show ip route**

Codes: L - local, C - connected,

Gateway of last resort is not set

192.168.11.0/24 is variably subnetted, 2 subnets, 2 masks

**C 192.168.11.0/24 is directly connected, FastEthernet0.11**

L 192.168.11.254/32 is directly connected, FastEthernet0.11

192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks

**C 192.168.12.0/24 is directly connected, FastEthernet0.12**

L 192.168.12.254/32 is directly connected, FastEthernet0.12

192.168.21.0/24 is variably subnetted, 2 subnets, 2 masks

**C 192.168.21.0/24 is directly connected, FastEthernet0.21**

L 192.168.21.254/32 is directly connected, FastEthernet0.21

192.168.22.0/24 is variably subnetted, 2 subnets, 2 masks

**C 192.168.22.0/24 is directly connected, FastEthernet0.22**

L 192.168.22.254/32 is directly connected, FastEthernet0.22

* Tester la connectivité entre les postes : tous les postes doivent communiquer entre eux.

**Configuration des équipements (extrait)**

|  |  |
| --- | --- |
| *Commutateur HP* | *Routeur Cisco 1801* |
| Switch# show running-config  vlan 11  name "A1"  untagged 11  tagged 25  exit  vlan 12  name "A2"  untagged 12  tagged 25  exit  vlan 21  name "B1"  untagged 21  tagged 25  exit  vlan 22  name "B2"  untagged 22  tagged 25  exit | Rt-H# show running-config  !  interface FastEthernet0.11  encapsulation dot1Q 11  ip address 192.168.11.254 255.255.255.0  !  interface FastEthernet0.12  encapsulation dot1Q 12  ip address 192.168.12.254 255.255.255.0  !  interface FastEthernet0.21  encapsulation dot1Q 21  ip address 192.168.21.254 255.255.255.0  !  interface FastEthernet0.22  encapsulation dot1Q 22  ip address 192.168.22.254 255.255.255.0  ! |

##### Étape 2 : mise en place du routage virtuel avec VRF

**Objectif :** Il s’agit de mettre en place l’étanchéité des tables de routage de chacun des clients One et Two.

**Mise en place**

L’infrastructure physique et le plan d’adressage IP sont inchangés. On ajoute deux VRF, un pour chaque client.

* Mettre en place les deux VRF, one et two (attention le routeur est sensible à la casse)

Rt-H(config)#**ip vrf one**

Rt-H(config-vrf)#exit

Rt-H(config)#**ip vrf two**

Rt-H(config-vrf)#exit

* Assigner les interfaces aux VRF, par exemple :

Rt-H(config)#**interface fa0.11**

Rt-H(config-subif)#**ip vrf forwarding one**

% Interface Fa0.11 IPv4 disabled and address(es) removed due to disabling VRF one (\*)

Rt-H(config-subif)#**ip address 192.168.11.254 255.255.255.0**

Rt-H(config-subif)#exit

(\*) Le fait d’assigner l’interface à un VRF efface l’adresse IP de l’interface. Il faut donc la remettre.

* Vérifier la configuration des VRF

Rt-H#**show ip vrf**

Name Default RD Interfaces

one <not set> Fa0.11

Fa0.12

two <not set> Fa0.21

Fa0.22

Remarque : RD signifie « Route Distinguisher ». Un RD est un identifiant unique permettant d’identifier les routes associées à un VRF lors de la propagation des routes. Il est nécessaire pour garantir l’unicité des routes en cas de chevauchement des adresses IP entre les VRF. Par exemple :

Router(config)#**ip vrf one**

Router (config-vrf)#**rd 100.1**

**Validation**

* Afficher la table de routage globale devenue vide et la table de routage de chacun des VRF. Chaque VRF dispose d’une table de routage en propre, étanche de l’autre VRF.

Table de routage globale :

Rt-H#**show ip route**

Gateway of last resort is not set

 La table de routage globale est bien devenue vide

Table de routage des VRF one et two :

Rt-H#**sh ip route vrf one**

vrf

Routing Table: one

Gateway of last resort is not set

192.168.11.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.11.0/24 is directly connected, FastEthernet0.11

L 192.168.11.254/32 is directly connected, FastEthernet0.11

192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.12.0/24 is directly connected, FastEthernet0.12

L 192.168.12.254/32 is directly connected, FastEthernet0.12

Rt-H#**sh ip route vrf two**

vrf

Routing Table: two

Gateway of last resort is not set

192.168.21.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.21.0/24 is directly connected, FastEthernet0.21

L 192.168.21.254/32 is directly connected, FastEthernet0.21

192.168.22.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.22.0/24 is directly connected, FastEthernet0.22

L 192.168.22.254/32 is directly connected, FastEthernet0.22

* Tester la connectivité entre les postes d’un même client et tester l’étanchéité des communications entre les postes de clients différents. Un ping entre un poste du client One et un poste du client Two ne doit pas aboutir

Remarque : pour tester la connectivité vers un poste depuis le routeur, il faut préciser le VRF utilisé.

Rt-H# **ping vrf one** **192.168.11.1**

Fichier de configuration du routeur Cisco 1801 (extrait)

Rt-H#**show running-config**

hostname Rt-H

...

no ip dhcp use vrf connected

!

ip vrf one

ip vrf two

...

!

interface FastEthernet0.11

encapsulation dot1Q 11

ip vrf forwarding one

ip address 192.168.11.254 255.255.255.0

!

interface FastEthernet0.12

encapsulation dot1Q 12

ip vrf forwarding one

ip address 192.168.12.254 255.255.255.0

!

interface FastEthernet0.21

encapsulation dot1Q 21

ip vrf forwarding two

ip address 192.168.11.254 255.255.255.0

!

interface FastEthernet0.22

encapsulation dot1Q 22

ip vrf forwarding two

ip address 192.168.22.254 255.255.255.0

**!**

##### Étape 3 : adresses IP *identiques* dans les deux VRF

**Objectif :** Vérifier l’étanchéité des tables de routage de chacun des VRF en utilisant une adresse IP identique dans des réseaux de deux VRF différents.



On modifie le plan d’adressage du réseau du site B2 en mettant une adresse identique au site A2.

**Mise en place**

Le schéma physique est inchangé.

* Modifier l’adresse IP de l’interface fa0.22

Rt-H(config)#int fa0.22

Rt-H(config-subif)#ip address 192.168.12.254 255.255.255.0

Rt-H(config-subif)#exit

* Modifier l’adresse IP du poste B2 en 192.168.12.2 et sa passerelle.

**Validation**

* Afficher les tables de routage des VRF : la table de routage du VRF two a changé et on constate la route identique dans les deux VRF.

Rt-H# **sh ip route vrf one**

Routing Table: one

192.168.11.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.11.0/24 is directly connected, FastEthernet0.11

L 192.168.11.254/32 is directly connected, FastEthernet0.11

192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks

**C 192.168.12.0/24 is directly connected, FastEthernet0.12**

L 192.168.12.254/32 is directly connected, FastEthernet0.12

Rt-H#**sh ip route vrf two**

Routing Table: two

192.168.21.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.21.0/24 is directly connected, FastEthernet0.21

L 192.168.21.254/32 is directly connected, FastEthernet0.21

192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks

**C 192.168.12.0/24 is directly connected, FastEthernet0.22**

L 192.168.12.254/32 is directly connected, FastEthernet0.22

* Tester la connectivité entre les postes d’un même client et tester l’étanchéité des communications entre les postes de clients différents.
* Remettre l’adresse IP d’origine sur le réseau B2 (192.168.22.0).

##### Étape 4 : test du routage virtuel avec un routeur sur un site client

**Objectif** : Il s’agit de tester le routage avec un routeur supplémentaire installé sur le site A1 du client One.

Schéma logique :



**192.168.11.0/24**

**192.168.12.0/24**

**192.168.21.0/24**

**192.168.22.0/24**

**Client A: one**

**Client B: two**

**A1**

**B1**

**A2**

**B2**



Rt-A1

**192.168.10.0/24**

.1

.10

Schéma physique :



Le second routeur est un Cisco 1760 dont les caractéristiques sont décrites en annexe du document. Il n’est pas nécessaire d’utiliser un routeur qui implémente VRF

**Mise en place**

* Mettre en place l’infrastructure du site A1 :
* Branchements des équipements ;
* Configuration IP du poste client ;
* Paramétrage des interfaces du routeur : adresses IP et activation des interfaces.
* Ajout de la route par défaut sur le routeur rt-A1

Rt-A1(config)#**ip route 0.0.0.0 0.0.0.0 192.168.11.254**

* Ajout de la route vers le réseau A1 sur le routeur rt-H : cette route fait partie de table de routage du VRF one.

Rt-A1(config)#**ip route vrf one 192.168.10.0 255.255.255.0 192.168.11.1**

**Validation**

* Fichier de configuration du routeur Cisco 1760 (extrait).

Rt-A1#**sh run**

…

interface Ethernet0/0

ip address 192.168.10.1 255.255.255.0

!

interface FastEthernet0/0

ip address 192.168.11.1 255.255.255.0

!

ip route 0.0.0.0 0.0.0.0 192.168.11.254

* Afficher les tables de routage : on doit y visualiser les routes statiques précédentes.

Table de routage de la VRF one

Rt-H# **sh ip route vrf one**

Routing Table: one

Gateway of last resort is not set

**S 192.168.10.0/24 [1/0] via 192.168.11.1**

192.168.11.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.11.0/24 is directly connected, FastEthernet0.11

L 192.168.11.254/32 is directly connected, FastEthernet0.11

192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks

**C** 192.168.12.0/24 is directly connected, FastEthernet0.12

L 192.168.12.254/32 is directly connected, FastEthernet0.12

Table de routage (globale) de rt-A1

Rt-A1#**sh ip route**

**Gateway of last resort is 192.168.11.254 to network 0.0.0.0**

C 192.168.10.0/24 is directly connected, Ethernet0/0

C 192.168.11.0/24 is directly connected, FastEthernet0/0

**S\* 0.0.0.0/0 [1/0] via 192.168.11.254 192.168.11.0/24 is variably subnetted 2 masks**

* Tester la connectivité entre les postes d’un même client et tester l’étanchéité des communications entre les postes de clients différents : la situation reste inchangée par rapport à l’étape précédente.

**Annexe : Les équipements utilisés**

1. **Routeur de l’hébergeur/FAI : Cisco 1801**

Le CISCO 1801 est un routeur à services intégrés (ISR - Integrated Service Router).



Le routeur propose :

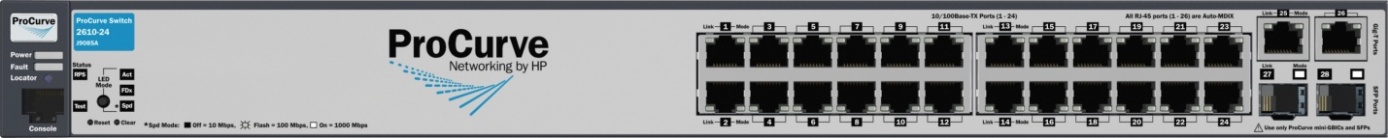
* 8 ports **FA1** à **FA8** pouvant être utilisés à la fois pour le routage inter-VLAN et la commutation.
* 1 port **FA0** spécifique dédié au routage
* 1 port **console** pour l’administration du routeur via une liaison série et le langage IOS
* 1 port pour une liaison ADSL
* 1 port pour une liaison par modem « AUX »

Le routeur dispose d’une adresse IP dans le VLAN d’administration (Vlan 1) et d’un accès sécurisé en Telnet.

Version du firmware : 15.1(4m)

1. **Commutateur : HP Procurve 2620**

Les HP Procurve 2620 sont des commutateurs administrables de niveau 3.   
La configuration actuelle du commutateur est au niveau 2.



*port console*

*Le commutateur propose:*

* un port console RJ45
* 24 ports Fastethernet à 100 Mbits/s: **1** à **24**
* ports Gigabit RJ45: **25** et **26**
* ports Gigabit GBIC(SFP) : **27** et **28**Les modules optiques SFP ne sont installés dans les emplacements Gbic.

Le commutateur dispose d’une adresse IP dans le VLAN d’administration (Vlan 1 par défaut), et d’un d’accès sécurisé en mode Telnet.

1. **Routeur du site client : Cisco 1760**

Le CISCO 1760 est un routeur dédié aux solutions d'accès internet et intranet pour les PME.



Le routeur propose un **port console** pour l’administration du routeur via une liaison série et le langage IOS et 2 ports spécifiques dédiés au routage:

* 1 port FastEthernet: **Fa0/0**
* 1 port ethernet à 10 Mbits/s: **eth0/0**