

M2 MMI - Cloud Computing et Virtualization

Travaux Pratiques N°2 : Virtualisation des Réseaux – Routage inter-vlan & contrôle d'accès

Objectifs:

Dans cette deuxième partie, l'étudiant implémentera une solution dite « Router on the stick » en vue de permettre la communication inter-vlan. Un filtrage sera, par la suite, imposé afin de ne permettre l'accès qu'aux serveurs publiques de chaque client, protégeant ainsi les serveurs locaux, privés.

Topologie :

Réutiliser la topologie créée précédemment dans la partie 1.



Table d'adressage

Appareil	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
	G0/1,10	172.17.10.1	255.255.255.0	N/A
R1	G0/1,20	172.17.20.1	255.255.255.0	N/A
	G0/1,30	172.17.30.1	255.255.255.0	N/A
Server0	Carte réseau	172.17.10.10	255.255.255.0	172.17.10.1
Server1	Carte réseau	172.17.10.11	255.255.255.0	172.17.10.1
Server2	Carte réseau	172.17.20.10	255.255.255.0	172.17.20.1
Server3	Carte réseau	172.17.20.11	255.255.255.0	172.17.20.1
Server4	Carte réseau	172.17.30.10	255.255.255.0	172.17.30.1
Server5	Carte réseau	172.17.30.11	255.255.255.0	172.17.30.1
Server6	Carte réseau	172.17.10.12	255.255.255.0	172.17.10.1

Conditions requises

Partie 2 : routage inter-vlan

a) Configurez le routage inter-VLAN sur R1 en fonction de la table d'adressage.

đ	₹R1 COX	
	CLI Attributes	
	IOS Command Line Interface	
	Router>enable	
	Router‡configure terminal Enter configuration commands one per line End with CNTL/Z	
	Router(config) #interface g0/1.10	
	Router(config-subif) #encapsulation dot1q 10 2	
	Router(config-subif) #ip address 172.17.10.1 255.255.255.0	
	Router (config-subif) #encapsulation dot1g 20	
	Router(config-subif) #ip address 172.17.20.1 255.255.255.0	
	Router(config-subif) #interface g0/1.30	
	Router(config-subif) #encapsulation dotig 30 Router(config-subif) #ip address 172,17,30,1 255,255,255,0	
	Router(config-subif) #interface g0/1 5	
	Router(config-if)#no shutdown	
	Router(config-if)#	
	%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up	
	<pre>%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up</pre>	
	changed state to up	
	%LINK-5-CHANGED: Interface GigabitEthernet0/1.10, changed state to up	
	E SLINEPPOTO-5-UPDOWN: Line protocol on Interface	
	GigabitEthernet0/1.10, changed state to up	
	*LINK-S-CHANGED: Interface GigabitEthernet0/1.20, Changed state to up	
	Ctrl+F6 to exit CLI focus Copy Paste	
_		
)	Afin de creer un port virtuel a partir du port physique « g0/1 », il suffit d'ajouter le suffixe « .10 », le nom com	plet du p
	will del est doite « $g0/1.10$ ». Il est recommande d'employer le meme numero que ridentificateur du vian asso g0/1.10 représentera la passerelle du vian 10. Pour ce faire, exécuter la commande : <i>interface $g0/1.10$</i>	cie, allis
	Avant de configurer l'adressage IP du port virtuel, il est impératif d'activer le protocole de trunking 802 1g pui	s associ
	ce port au vlan 10. C'est ce qui rend effectivement « g0/1.10 » une passerelle pour le vlan 10. Exécuter la com	mande
	encapsulation dot1q 10	
	Attribuer la première adresse d'hôte au port virtuel ainsi que le masque sous réseau. Commande :	
	ip address 172.17.10.1 255.255.255.0	
	Procéder pareillement à la configuration des ports virtuels « g0/1.20 », « g0/1.30 », représentant, respectivem	nent, les
	passerelles des vlans 20 et 30.	
)	Un port du routeur est désactivé par défaut. Afin de pouvoir activer, à la fois, tous les ports virtuels, exécuter l	la
	commande no shutdown au niveau du port physique parent « g0/1 ».	
U	rrer la liaison Trunk entre le commutateur S1 et le routeur R1.	
I	liaison entre le routeur et le commutateur doit permettre le transfert des trafics de tous les vlans. C'est pourqu	oi elle d

b)

Physical Config CLI Attributes	
IOS Command Line Interface	
	,
Switch>	
Switch>	
Switch>	
Switch>	
Switch>enable	
Enter configuration commands, one per line.	End with CNTL/Z.
Switch(config) #interface g0/1	
Switch(config-if) #switchport mode trunk 1 Switch(config-if) #	
Switch(config-if) #	
Switch(config-if) #	
Switch(config-if) # Switch(config-if) #	
Switch(config-if) #	
Switch(config-if)#	
Switch(config-if) #	
Switch(config-if) #	
Switch (config-if) #	
Switch(config-if) #	
Switch(config-if) #	
Switch(config-if)#	~
entern(county mala	
Ctrl+F6 to exit CLI focus	Copy Paste
Mettre le port g0/1 du commutateur S1 au mode Trunk. E	xécuter la commande : switchport mode trunk
érifiez la connectivité. Tous les Serveurs doivent pouvoir s'er	nvover des requêtes <i>ping</i> les uns aux autres.
	···· · · · · · · · · · · · · · · · · ·
r0	
ces Desktop Programming Attributes	
and Prompt	
ket Tracer SERVER Command Line 1.0	
ket Tracer SERVER Command Line 1.0 >ping 172.17.20.10	
ket Tracer SERVER Command Line 1.0 >ping 172.17.20.10 ging 172.17.20.10 with 32 bytes of data:	
ket Tracer SERVER Command Line 1.0 >ping 172.17.20.10 ging 172.17.20.10 with 32 bytes of data: uest timed out.	
<pre>ket Tracer SERVER Command Line 1.0 >ping 172.17.20.10 ging 172.17.20.10 with 32 bytes of data: uest timed out. ly from 172.17.20.10: bytes=32 time<1ms TTL=127 ly from 172.17.20.10: bytes=32 time<1ms TTL=127</pre>	
<pre>ket Tracer SERVER Command Line 1.0 >ping 172.17.20.10 ging 172.17.20.10 with 32 bytes of data: uest timed out. ly from 172.17.20.10: bytes=32 time<1ms TTL=127 ly from 172.17.20.10: bytes=32 time<1ms TTL=127 ly from 172.17.20.10: bytes=32 time<1ms TTL=127</pre>	
<pre>ket Tracer SERVER Command Line 1.0 >ping 172.17.20.10 ging 172.17.20.10 with 32 bytes of data: uest timed out. ly from 172.17.20.10: bytes=32 time<1ms TTL=127 ly from 172.17.20.10: bytes=32 time<1ms TTL=127 ly from 172.17.20.10: bytes=32 time<1ms TTL=127</pre>	
<pre>ket Tracer S2RVER Command Line 1.0 >ping 172.17.20.10 ging 172.17.20.10 with 32 bytes of data: uest timed out. ly from 172.17.20.10: bytes=32 time<1ms TTL=127 ly from 172.17.20.10: bytes=32 time<1ms TTL=127 ly from 172.17.20.10: bytes=32 time<1ms TTL=127 g statistics for 172.17.20.10: Packets: Sent = 4, Received = 3, Lost = 1 (25% loss), roximate round trip times in milli-seconds:</pre>	
<pre>ket Tracer SERVER Command Line 1.0 >ping 172.17.20.10 ging 172.17.20.10 with 32 bytes of data: uest timed out. ly from 172.17.20.10: bytes=32 time<1ms TTL=127 ly from 172.17.20.10: bytes=32 time<1ms TTL=127 ly from 172.17.20.10: bytes=32 time<1ms TTL=127 g statistics for 172.17.20.10: Packets: Sent = 4, Received = 3, Lost = 1 (25% loss), roximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms</pre>	

Partie 3 : Filtrage et contrôle d'accès

a) Configurer un service Web au niveau de « Server2 » du client 2. Ce dernier sera un serveur à accès publique avec une page d'accueil nommée « index.html »

SERVICES	0	HTTP		SERVICES	Ella Nama: Jadau html
HTTP				HTTP	File Rane. Index.mail
DHCP	HTTP	HTTPS		DHCP	<html></html>
DHCPv6	0 0 0 0 0 0		0.04	DHCPv6	<center>Cisco Packet Tracer</center>
TETP		e on	O on	TFTP	<nr>Bienvenu aux ste du Client 2.</nr>
DNS	The Marcola State			DNS	<pre> doca clinic.</pre>
SYSLOG	File Manager	5.0		SYSLOG	Copyrights</td></tr><tr><td>444</td><td>File Name</td><td>Edit</td><td>Delete</td><td>444</td><td><pre>
dhref=" image.html="">image page
NTP	1 copyrights.html	(edit)	(delete)	NTP	
EMATI			(4-1-1-)	EMATI	
FTP	2 cscoptiogo1//x111.jpg		(delete)	FTP	
IoT	3 helloworld.html	(edit)	(delete)	IoT	
VM Management	a summer or		in the second se	VM Management	
Radius FAP	4 image.html	(edit)	(delete)	Radius FAP	
Roulds CAP	5 index.html	(edit) 2	(delete)	Rounds LAP	
		Nous	in most		Få Managar Sava

- 1) Assurez-vous que le protocole http est activé
- 2) Cliquez sur « edit » afin de modifier la page d'accueil « index.html »
- Remplacer la phrase "Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open" par «Bienvenus au Site de Client 2 »
- 4) Cliquer *save*
- b) Dans « Server2 », configurer également le service DNS et ajouter une entrée associant l'URL <u>www.client2.dz</u> à l'adresse IP de « Server2 » (voir la table d'adressage)

SERVICES	Ì	DNS	
HTTP DHCP	DNS Service	On 3	Off
DHCPv6			
TFTP	Resource Records		
DNS 2	Name www.client2	2.dz 4	Type A Record \lor
SYSLOG			
AAA	Address 172.17.20.10	5	
NTP	Add 6	Save	Remove
EMAIL			
FTP	No. Name	Туре	Detail
IoT	0 www.client2.dz	ARecord	172.17.20.10
VM Management			
Radius EAP			

- 6) Cliquer sur « Add » pour créer l'association URL/Adresse IP
- 7) Assurez-vous que l'enregistrement a été créé avec succès puis cliquez sur « Save »

visical Config S	Services Desiton Programming Attributes
lysical connig a	Services Desktop Programming Autobates
Configuration	x
P Configuration	
O DHCP	Static
PAddress	172.17.10.10
Subnet Mask	255.255.255.0
Default Gateway	172.17.10.1
DNS Server	172.17.20.10
Pv6 Configuration	
Pv6 Configuration	Auto Config
Pv6 Configuration DHCP	Auto Config Static
Pv6 Configuration DHCP Pv6 Address	Auto Config Static / FE80:'2D0:D3EE:FEBA:9AD6
Pv6 Configuration DHCP Pv6 Address Link Local Address Pv6 Gateway	Auto Config Static / FE80::2D0:D3FF:FEBA:9AD6
Pv6 Configuration DHCP Pv6 Address Link Local Address Pv6 Gateway Rv6 DNS Server	Auto Config Static / FE80::2D0:D3FF:FEBA:9AD6
Pv6 Configuration DHCP Pv6 Address Link Local Address Pv6 Gateway Pv6 DNS Server	Auto Config Static FE80::2D0:D3FF:FEBA:9AD6
Pv6 Configuration DHCP Pv6 Address Link Local Address IPv6 Gateway IPv6 DNS Server 802.1X	Auto Config Static FE80::2D0:D3FF:FEBA:9AD6
Pv6 Configuration DHCP Pv6 Address Link Local Address Pv6 Gateway Pv6 DNS Server 802.1X Use 802.1X Security	Auto Config Static FE80::2D0:D3FF:FEBA:9AD6 FE80::2D0:D3FF:FEBA:9AD6
Pv6 Configuration DHCP Pv6 Address Link Local Address Pv6 Gateway Pv6 DNS Server 302.1X Use 802.1X Security Authentication	Auto Config Static FE80::2D0:D3FF:FEBA:9AD6 MD5
Pv6 Configuration DHCP Pv6 Address Link Local Address Pv6 Gateway Pv6 DNS Server 302.1X Use 802.1X Security Authentication Username	Auto Config Static FE80::2D0:D3FF:FEBA:9AD6 MD5

d) Depuis Server0, accéder au site du client2 en saisissant l'URL <u>www.client2.dz</u> dans le navigateur, afin de tester le DNS.

Rever0	
Physical Config Services Desktop Programming Attributes	
Web Browser	х
< > URL http://www.client2.dz 3 Go	Stop
Cisco Packet Tracer	
Bienvenus au site du client 2 4	
Quick Links:	
<u>A small page</u>	
Copyrights	
Image page	
Image	
1) Cliquer sur Server0 puis choisir l'onglet « Desktop »	
2) Cliquer sur « Web Browser »	
 Saisir <u>www.client2.dz</u> dans la barre d'adresse 	
 Vous devez voir la page d'accueil après une courte période de temps fonctionnels 	s. Cela prouvera que les
TONCTIONNEIS	

e) Dans Server3, activer et configurer le service FTP. Ajouter l'utilisateur « client2 » avec le mot de passe « 1234 ». Ajouter une entrée DNS pour ce serveur en lui attribuant l'URL ftp.client2.dz

	Servi	ces	esktop	Programming	Attributes	
SERVICES	·			FT	ΓP	
HTTP					4	
DHCP		Serv	ice		On 🖪	⊖ of
DHCPv6						
TFTP		US	er Setup			
DNS		Us	ername client	2	Password 1234	
SYSLOG			Write 🔽	Read De		
AAA						
NTP			Username	Password	Permission	Add 6
EMAIL		1	cisco	cisco	RWDNL	Aug
FTP	2				-	0
IoT		2	client2	1234	RWDNL	Save
VM Management						
Radius EAP						Remove

- 1) Cliquer sur Server3, choisir l'onglet « Service »
- 2) Cliquer sur « FTP »
- 3) S'assurer que le service FTP est activé
- 4) Créer un nouvel utilisateur « client2 » ayant le mot de passe « 1234 »
- 5) Attribuer à cet utilisateur tous les privilèges
- 6) Ajouter le nouvel utilisateur
- 7) Vous devez voir le nouvel utilisateur dans la liste des utilisateurs

Création d'entrée DNS du service FTP de Server3

Server2					
Physical Config	Services	Desktop P	rogramming Att	ributes	
SERVICES	\wedge		DNS		
HTTP					
DHCP	DNS Se	ervice	On	O Off	
DHCPv6					
TFTP	Resour	rce Records			
DNS	Name	ftp.clien	t2.dz	Туре	A Record \lor
SYSLOG					
AAA	Addres	ss 172.16.20.1	1		
NTP		Add	Save		Remove
EMAIL		Add	ouro		THE INDIANA STREET
FTP	No.	Name	Тур	e	Detail
IoT	0	ftp.client2.dz	ARecord	172	.16.20.11
VM Management					
Radius EAP	1	www.client2.	dz A Record	172	.16.20.10

f) Depuis Server0 tester le service FTP configuré dans Server3. Dans le « Command Prompt », saisir la commande ftp ftp.client2.dz.

hysical Config Services Desktop Programming Attribu	tes
command Promot	X
	~
Packet Tracer SERVER Command Line 1.0	
C:\>ftp ftp.client2.dz	
Trying to connectftp.client2.dz	
Connected to ftp.client2.dz	
220- Welcome to PT Ftp server	
Username:client2	
331- Username ok, need password	
Password:	
230- Logged in	
(passive mode on)	
lop-ull	
Listing /ftp directory from ftp.client2.dz:	
0 : asa842-k8.bin	5571584
1 : asa923-k8.bin	30468096
2 : cl841-advipservicesk9-mz.124-15.Tl.bin	33591768
3 : cl841-ipbase-mz.123-14.T7.bin	13832032
4 : c1841-ipbasek9-mz.124-12.bin	16599160
5 : c1900-universalk9-mz.SPA.155-3.M4a.bin	33591768
6 : c2600-advipservicesk9-mz.124-15.T1.bin	33591768
7 : c2600-i-mz.122-28.bin	5571584
8 : c2600-ipbasek9-mz.124-8.bin	13169700
9 : c2800nm-advipservicesk9-mz.124-15.TL.bin 10 : c2800nm-advipservicesk9-mz.124-15.TL.bin	50938004
10 : c2800nm-advipservicesk9-m2.151-4.M4.bin	5571594
12 : c2800nm-ipbasek9-mz 124-8 bin	15522644
13 : c2900-universalk9-mz_SPA_155-3_M4a_bin	33591768
14 : c2950-i6g412-mz.121-22.EA4.bin	3058048
15 : c2950-i6g412-mz.121-22.EA8.bin	3117390

g) Les services Web et DNS du client2 sont censés être publiques, alors que l'FTP doit être à accès privé. En vue d'appliquer ces contraintes, créer une ACL étendue nommée NO-FTP, au niveau du port g0/1.20 du routeur R1.

rnysical	Config	CLI	Attributes	3	
			IOS	Command Line Interface	
Router (config)	\$		4-	1
Router (config)	<pre>#ip acc</pre>	ess-lis	t extended NO-FTP 💶	
Router (config-	ext-nac	:1) #! re:	fuser le trafic FTP	
Router (config-	ext-nac	:1) #deny	tcp any 172.17.20.11 0.0.0.0 eq 20 🛵	
Router (config-	ext-nac	1) #deny	tcp any 172.17.20.11 0.0.0.0 eq 21 🧲	
Router	config-	ext-nac	1) #! pe:	rmettre http au Server2	
Router	config-	ext-nac	1) #perm	it tcp any 172.17.20.10 0.0.0.0 eq 80 🕄	
Router	config-	ext-nac	1) #! pe:	rmettre DNS au Server2	
Router	config-	ext-nac	1) #perm	it tcp any 172.17.20.10 0.0.0.0 eq 53 4	
Router	config-	ext-nac	1) #! em	pecher les autres connexions	
Router	config-	ext-nac	1) #deny	ip any any 5	
Router	config-	ext-nac	1) #exit	-	
Router	config)	#! appl	iquer A	CL au port g0/1.20	
Router	config)	#interf	ace g0/	1.20 6	
Router	config-	subif) #	ip acces	ss-group NO-FTP out	
Router	config-	subif) #	exit		
Doutor	config)	*			

- Le service FTP requiert 2 connexion, l'une pour le transfert des données (port 20), l'autre pour contrôler le transfert (port 21), par conséquent, deux règle *Deny* sont nécessaires pour refuser les connexions à chaque port.
- 3) Permettre les connexion Http (port 80) au Server2
- 4) Permettre les connexions DNS (port 53) au Server2
- 5) Interdire toute autre connexion. Cette commande est facultative puisqu'elle sera ajoutée implicitement à la fin de l'ACL
- 6) Une ACL est appliquée au niveau d'un port du routeur. Client2 a une autorité sur le port g0/1.20
- 7) Une ACL est appliquée sur un trafic entrant ou sortant du routeur. Le trafic en provenance de l'extérieur et sortant de R1 via g0/1.20 sera filtré afin de ne permettre que les connexions Http et DNS.

h) Vérifier si l'ACL a bien assuré le filtrage du trafic FTP. Lancer une connexion FTP depuis Server0 du client1, ensuite à partir de Server2 du client2.

Connexion depuis Server0

Physical Config Services Desktop Programming Attributes Command Prompt X	Physical Config Services Desktop Programming Attributes Command Prompt >	Physical Config Services Desktop Programming Attributes Command Prompt C:\> C:\> C:\> C:\>ftp ftp.client2.dz Trying to connectftp.client2.dz	Server0						
Command Prompt X	Command Prompt	Command Prompt X C:\> C:\>ftp ftp.client2.dz Trying to connectftp.client2.dz	Physical	Config	Services	Desktop	Programming	Attributes	
	C:\>	C:\> C:\>ftp ftp.client2.dz Trving to connectftp.client2.dz	Command	Prompt					х
		C:\>ftp ftp.client2.dz Trving to connectftp.client2.dz		Prompt					X

Connexion depuis Server2

Command Prompt	x
command Prompt	x
Command Prompt	X
Packet Tracer SERVER Command Line 1.0	
C:\>ftp ftp.client2.dz	
Trying to connectftp.client2.dz	
Connected to ftp.client2.dz	
Connected to ftp.client2.dz 220- Welcome to PT Ftp server	