

Guide SDN de mise en place de VLANs et de MSSID

1. Sujet d'expérience

Définissez multi-VLAN pour les clients câblés. Faites des clients de différents VLANs pour obtenir des adresses IP de différents segments réseau. Tous les VLAN peuvent accéder à Internet mais ne peuvent pas accéder les uns aux autres.

2. Scénario d'application

En général, une entreprise compte plusieurs départements, comme le service de R&D, le département pe et ainsi de suite. L'administrateur de réseau de bureau doit séparer la communication entre les différents ministères parce que chaque ministère dispose de ses ressources privées. Afin de faciliter la distinction et la gestion des différents départements, nous leur usually assignons habituellement différents segments réseau d'adresses IP. En même temps, il faut également s'assurer que tous les ministères peuvent accéder à Internet.

3. Directeur de travail

Dans le contrôleur Omada SDN, nous pouvons définir plusieurs réseaux pour différents départementss. Chaque département appartients à un réseau. Chaque réseau est en mesure de créer une interface L3 et son propre serveur DHCP, de sorte que différents départements peuvent obtenir différents segments d'adresses IP.

La création d'une interface L3 permettra aux différents réseauxd'accéder les uns aux autres. Il faut donc définir ACL pour séparer la communication.

4. Exigence réseau

Configurer le réseau pour créer différents départements pour obtenir différents segments d'adresses IP.

Appliquez le profil pour changer de ports. Chaque réseau générera automatiquement un profil. Lorsque l'applicationing du profil au port de commutateur, ce port appartient au réseau correspondant.

Définissez ACL pour séparer la communication entre les différents départements.

5. Objectifs

1. Découvrez la configuration pour la création d'un nouveau réseau, l'ajout d'appareils au réseau et l'utilisation d'ACL pour séparer les périphériques.

2. Renseignez-vous sur les principes de base du réseau,, du profil et de l'ACL.



6. Équipement expérimental

- 1. Trois PCs
- 2. Un Routeur TL-ER6120v3
- 3. Un commutateur Niveau3 T1600G-28PS
- 4. La plateforme Contrôleur Omada SDN installée
- 5. Un Lien Internet FAI
- 6. Câbles RJ45 6A

7. Topologie réseau



8. Étapes de configuration

1) Connecter les appareils selon la topologie ci-dessus.

Connectez le lien FAI à WAN1 du routeur. Faites wan1 obtenir l'adresse IP de FAI. Connectez un PC au port LAN du routeur. Définissez l'adresse IP dynamique de ce PC. Ce PC est utilisé pour accéder au contrôleur Omada SDN.

Connectez le commutateur au port LAN du routeur.

Connectez deux PC au port 1 et au port 2 de l'interrupteur. Définissez l'adresse IP dynamique pour les deux PC.

2) Connectez-vous au contrôleur Omada SDN.

Installez le contrôleur Omada SDN sur le PC connecté au routeur. Ensuite, connectez-vous à ce contrôleur. Si vous avez le compte du contrôleur Basé sur Omada Cloud, vous n'avez pas besoin d'installer le contrôleur, de vous connecter au contrôleur cloud et d'adopter vos appareils.



3) Créer du réseau.

Dans **Paramètres->Réseaux câblés->RÉSEAUX LAN->Réseaux,** cliquez sur Créer un nouveau réseau local pour ajouter un nouveau réseau.

P	tp-link omado	2							Sites:	Default	🖌 Q, 🚨 E
98	Settings		Settin	ngs > Wired Networks	S > LAN Networks						
C	Site		⊕ N	etworks 📄 Profiles	Switch Settings						
	Wired Networks	^		NAME	PURPOSE	SUBNET	PORTAL	ACCESS CONTROL RULE	RATE LIMIT	VLAN	ACTION
٥	Internet			LAN	interface	192.168.0.1/24	~			1	C
6	LAN Networks			PE_department	interface	192.168.200.1/24		~		200	2 1
Q	Wireless Networks										71 0
Ë	Firewall & ACL	~		RD_Department	interface	192.168.100.1/24		~		100	
	Transmission	~	_	Showing 1-3 of 3 records	s < 1 >	10 /page 🗸 🗸	Go To page:				
	VPN		(+ Create New L	AN						
	Profiles	~	_								

Dans les nouveaux paramètres réseau, nous devons configurer le nom, le but, l'interface LAN, Vlan, gateway/subnet.

Pour ce but, choisissez **Interface**. Je signifie que le système va créer une interface L3 pour ce réseau.

Pour LAN Interface choisir LAN1, cette étape est de lier le réseau au port de routeur physique.



Pour VLAN, parce que le **Département_RD** appartiennent à VLAN100, donc placez 100 ici.

Pour Gateway/Subnet, définir le 192.168.100.1/24. Cliquez sur Mettre à jour la plage DHCP, le système générera automatiquement la plage DHCP.



P	tp-link omâdo	c	
00	Settings		Settings > Wired Networks > LAN Networks
C	Site		Networks Profiles Switch Settings
	Wired Networks	^	Edit Network
٥	Internet		Name: RD_Department
뎹	LAN Networks		Purpose: Interface VLAN
Q	Wireless Networks		LAN Interfaces: LAN1 LAN2 LAN3
岜	Firewall & ACL	~	Vlan: 100 (1-4090) ()
	Transmission	~	Gateway/Subnet: 192 . 168 . 100 . 1 / 24 ① Update DHCP Range
	VPN		Gateway IP: 192.168.100.1
	Profiles	~	Network IP Count: 254
	Authentication	~	Network IP Range: 192.168.100.1 - 192.168.100.254 Network Subnet Mask: 255.255.255.0
	Services		Domain Name: (Optional)
	Controller		IGMP Snooping: Enable ()
	Cloud Access		DHCP Server: 🕑 Enable
	Maintenance		DHCP Range: 192 . 168 . 100 . 1 - 192 . 168 . 100 . 254
8	Migration		Manual
Ø	Auto Backup		Lease Time: 120 minutes (2-2880)

Le **Département_PE** est configuré de la même manière. Enfin, il y a deux nouveaux réseaux comme le ci-dessous.

NAME	PURPOSE	SUBNET	PORTAL	ACCESS CONTROL RULE	RATE LIMIT	VLAN	ACTION
LAN	interface	192.168.0.1/24				1	C
PE_Department	interface	192.168.200.1/24		~		200	
RD_Department	interface	192.168.100.1/24		~		100	
Showing 1-3 of 3 record	s < 1 >	10 /page 🗸	Go To page:				

4) Vérifier Profile

Le contrôleur générera automatiquement le profil du réseau. Il y a donc deux nouveaux profils correspondant aux nouveaux réseaux.



NAME	POE	NATIVE NETWORK	ISOLATION	STORM CONTROL	ACTION
All	Keep the Device's Settings	LAN		Off	\odot
Disable	Keep the Device's Settings	None		Off	\odot
LAN	Keep the Device's Settings	LAN		Off	\odot
PE_department	Keep the Device's Settings	PE_department		Off	•
RD_Department	Keep the Device's Settings	RD_Department		Off	• 🔟

5) Apply le profil pour changer de ports.

Dans Paramètres->Réseaux câblés->Réseaux LAN->Paramètres de commutation, cliquez sur Modifier le rofile port Ppour appliquerle profil aux ports de commutation. Appliquez au port 1 le profil du Département_RD profil et appliquez au port 2 le profil Département_PE

Settings > Wired Networks > LAN I	Vetworks	
Networks Profiles Switc	th Settings	
DEVICE NAME	PROFILES	Edit Port Profile
CC-32-E5-69-B5-B0	All: Port1,Port3,Port4,Port5,Port6,Port7,Port8,Port9,Port10;RD_Department:	
Showing 1-1 of 1 records <	1 > 10 /page V Go To page:	

Appliquer au port 1 le profil Département_RD et, le profil Département_PE au port2.



← CC-32-E5-69-B5 CONNECTED × >	CC-32-E5-69-B5 CONNECTED ×
1 3 5 7 9	1 3 5 7 9
	2 4 6 8 10
Disabled ■ Disconnected ■ 1000 Mbps ■ 10/100 Mbps 4 PoE ▲ Uplink ④ Mirroring ② STP Blocking	■ Disabled ■ Disconnected ■ 1000 Mbps ■ 10/100 Mbps
Details Ports Clients Config Statistics	Details Ports Clients Config Statistics
Edit Port1	Edit Port2
Name:	Name:
Profile:	Profile:
RD_Department Vanage Profiles Profile Overrides Vanage Profiles	PE_Department
Apply Cancel	Apply Cancel

Jusqu'à présent, deux PC devraient être en mesure d'obtenir les adresses IP de différents segments de réseau. Et peut également accéder à Internet. Le dernier paramètre que nous devons faire est de définir ACL pour séparer leur communication.

6) Configurer ACL

Dans **Paramètres->Pare-feu & ACL>ACL->Switch ACL**, définissez une règle ACL « refuser » pour le département RD et le département PE, afin d'isoler la communication entre deux départements.

₽	🖓 tp-link omâda Sites: Defaut 🗸 🔍 💲 :										
98	Settings		Set	stings > Firewall & ACL > ACL							
C	Site		Gat	Gateway ACL Switch ACL EAP ACL							
	Wired Networks	~		INDEX	ENABLED	NAME	POLICY	PROTOCOLS	SOURCE	DESTINATION	ACTION
٥	Wireless Networks			1	•	1	Deny	All	Network:RD_Department	Network:PE_department	2 🗇
6	Firewall & ACL	^		Showing 1-1 of	1 records <	1 >	50 /page 🗸 Go	To page:			
Q	ACL			+ Create	New Rule						
Ë	URL Filtering										

Définissez la stratégie comme refuser, la source est réseau de département RD, la destination est département PE. Choisissez le type de liaison ACL comme VLAN 100(DÉPARTEMENT RD), puis tous les clients appartiennent à VLAN100 et VLAN200 ne communiquera pas les uns avec les autres.





9. Test

Après la configuration terminée. Nous pouvons utiliser deux PC pour pinguer l'un etl'autre et accéder à Internet, pour vérifier que l'expérience a été couronnée de succès.

Dar	ovomnlo	ci DC1	a l'adrassa	ID du	192 168 100 135/24
Pdl	exemple,	SIPUL	a l'auresse	IP UU	192.100.100.133/24.

Name:	1		
Status:	V E	nable	
Policy:	● P	leny Iermit	
Protocols:	All		~
Rule:			
Source			Destination
Type: Network	~		Type: Network ~
LAN RD_Department PE_department		Deny	 LAN RD_Department ✓ PE_department
1/3 Items			1/3 Items
ACL Binding			
Binding Type:	OP	orts	
	• v	LAN	
VLAN:	100)(RD_Department)	~

IPv4 Address
Subnet Mask
Lease Obtained : 20200 20 200 0 0 11:22:48
Lease Expires 2020🛛 2🖾 20🖾 🖾 🖾 13:22:46
Default Gateway
DHCP Server
DHCPv6 IAID 60087936
DHCPv6 Client DUID 00-01-00-01-24-A0-FC-FA-94-DE-80-57-AD
DNS Servers

PC2 a obtenu l'adresse IP de 192.168.200.246/24.

en0:	flags=8863 <up,broadcast,smart,running,simplex,multicast> mtu 1500</up,broadcast,smart,running,simplex,multicast>
	options=b <rxcsum,txcsum,vlan_hwtagging></rxcsum,txcsum,vlan_hwtagging>
	ether 58:b0:35:f8:04:6d
	<pre>inet6 fe80::4f9:b63b:ba36:c3b8%en0 prefixlen 64 secured scopeid 0x4</pre>
	inet 192.168.200.246 netmask 0xffffff00 broadcast 192.168.200.255
	nd6 options=201 <performnud,dad></performnud,dad>
	<pre>media: autoselect (1000baseT <full-duplex>)</full-duplex></pre>
	status: active

PC1 ne pouvait pas ping PC2.



C:\Users\Administrator>ping 192.168.200.246 -t
Pinging 192.168.200.246 with 32 bytes of data:
Request timed out.

10. Explication supplémentaire(Facultatif)

Sur la base des paramètres ci-dessus, nous pouvons également atteindre la fonctionnalité de multi-SSID. Create deux SSID, et les faire avoir des sous-réseaux différents et ne peuvent pas accéder les uns aux autres.



1) Topologie

Connectez omada EAP au port 3 de l'interrupteur.

2) Paramètres

Dans **Paramètres->Réseaux sans fil**, cliquez sur Créer un nouvel etwork sans filpourajouter denouveaux SSID.

Ptp-link omãdo							Sites: Default		~ Q 🚨			
96	Settings		Settings > Wireless Networks									
C	Site		WLAN Group: Default	~ (1 🗹 ท							
	Wired Networks	~	SSID NAME	SECURITY	BAND	GUEST	Portal	ACCESS CONTROL	RATE LIMIT	VLAN	ACTION	
٥	Wireless Networks					ne monar		RULE				
6	Firewall & ACL	~	PE_Department	None	2.4GHz, 5GHz					200	2 🗊	
Q	Transmission	~	RD_Department	None	2.4GHz, 5GHz					100	2	
Ë	VPN		TP_Hotel	None	2.4GHz, 5GHz		~				2	
	Profiles	~	Showing 1-3 of 3 records	(1 > Go To page	e 📃							
	Authentication	~	+ Create New Wireles	s Network								
	Services											

Configurons le SSID pour le Département_RD au début.

Nous devons mettre en place le nom, la sécurité ainsi que le VLAN.

lci, nous avons défini la sécurité comme aucun, et il faut définir le VLAN comme 100 parce que Département_RD utilise VLAN 100. Cliquez ensuite sur **Apply** pour terminer l'ajout de SSID.



P	tp-link omâdo	¢				
88	Settings		Se	ttings > Wireless Networks		
C	Site			Edit Wireless Network		
	Wired Networks	~		Network Name (SSID):	RD_Department	
D	Wireless Networks			Band:	 ✓ 2.4GHz ✓ 5GHz 	
ය	Firewall & ACL	~		Guest Network:	Enable ()	
Q	Transmission	~		Security:	None	
Ë	VPN				WEP WPA-Personal	
	Profiles	~			WPA-Enterprise	
	Authentication	~		Advanced Settings		
				SSID Broadcast:	Enable	
	Services			VLAN:	Enable 100	(1-4094)
	Controller			Rate Limit:	Enable (i)	
	Cloud Access			+ WLAN Schedule		
	Maintenance			+ 802.11 Rate Control (j)		
	Migration			+ MAC Filter		
	Auto Backup			Apply Cancel		

Ensuite, configurezz le SSID pour Département_PE de la même manière.

↓ p-link omâda								Sites: Default		🔹 Q 🚨 🗄	
88	Settings		Settings > Wireless Networks								
C	Site		WLAN Group: Default	~	0 🗹 🗊						
	Wired Networks	v	SSID NAME	SECURITY	BAND	GUEST NETWORK	Portal	ACCESS	RATE LIMIT	VLAN	ACTION
D	Wireless Networks							RULE			
۲	Firewall & ACL	~	PE_Department	None	2.4GHz, 5GHz					200	2 🖬
Q	Transmission	~	RD_Department	None	2.4GHz, 5GHz					100	2 🖬
Ë	VPN		TP_Hotel	None	2.4GHz, 5GHz		~				2 🖻
	Profiles	~	Showing 1-3 of 3 records	< 1 > Go To page	e:						
	Authentication	~	+ Create New Wireles	ss Network							
_	Services										

Finallement, nous obtenons deux nouveaux SSID comme ci-dessous.



3) Test

Utilisez deux téléphones se connecter à deux SSID. Les téléphones obtiendront différents segments d'adresses IP et ne peuvent pas accéder les uns aux autres.

Status	Connected	Status	Connected
Signal strength	Excellent	Signal strength	Excellent
Link speed	866Mbps	Link speed	866Mbps
Security	WPA2 PSK	Security	None
IP address	192.168.100.45	IP address	192.168.200.45
Subnet mask	255.255.255.0	Subnet mask	255.255.255.0
Gateway	192.168.100.1	Gateway	192.168.200.1
Proxy	None >	Proxy	None >
IP settings	DHCP >	IP settings	DHCP >

Le résultat de Ping est le suivant. Cela signifie qu'il n'a pas ping avec succès.

÷	Ping	Stop
192.1	68.100.45 (19)	
• 18	192.168.100.45 192.168.100.45	
0 17	192.168.100.45 192.168.100.45	
0 16	192.168.100.45 192.168.100.45	
• 15	192.168.100.45 192.168.100.45	
@ 14	192.168.100.45 192.168.100.45	
0 13	192.168.100.45 192.168.100.45	
0 12	192.168.100.45 192.168.100.45	
@ 11	192.168.100.45 192.168.100.45	
o 10	192.168.100.45 192.168.100.45	
9	192.168.100.45 192.168.100.45	