MỤC LỤC

MỤC LỤC1
BÀI 1. CÁC LỆNH CLI VÀ MỘT SỐ THAO TÁC THƯỜNG DÙNG4
BÀI 2. ĐỊA CHỈ IP VÀ MỘT SỐ CÀI ĐẶT CƠ BẢN5
BÀI 3. ĐIỀU HƯỚNG MẠNG LAN RA WAN TUỲ Ý
1. Mô hình mạng:6
2. Thực hành:
2.1. Cách 1: sử dụng phương pháp danh sách Address List6
2.2. Cách 2: sử dụng phương pháp In. Interface
BÀI 4. VLAN VÀ TRUNKING10
1. Mô hình mạng:10
2. Thực hành:10
2.1. Trên Router:
2.2. Trên Switch:
3. Kiểm tra:17
BÀI 5. LINK AGGREGATION CONTROL PROTOCOL 802.3ad18
1. Lý thuyết:
2. Mô hình mạng:
3. Thực hành:
3.1. Trên Router
3.2. Trên Switch:
BÀI 6. VLAN MANAGEMENT
1. Giới thiệu:
2. Mô hình mạng:
3. Thực hành:
3.1. Trên router:

3.2.	Trên switch:
BÀI 7.	FIREWAL CƠ BẢN31
1. Y	êu cầu:
2. T	nực hiện trên router31
BÀI 8.	CÂN BẰNG TẢI VỚI PHƯƠNG PHÁP PER CONNECTION CLASSIFIER
VÀ FAIL	OVER
1. G	iới thiệu:
2. M	ô hình mạng35
3. T	nực hành
3.1.	Cấu hình cân bằng tải và fail over bằng dòng lệnh35
3.2.	Cấu hình cân bằng tải bằng giao diện38
3.3.	Cho phép một lớp mạng không qua cân bằng tải:40
3.4.	NAT một địa chỉ IP/dịch vụ đi vào/ra đường internet được chỉ định Error!
Book	mark not defined.
BÀI 9.	NAT
BÀI 9. 1. G	
BÀI 9.1. G2. M	0 hình mạng
 BÀI 9. 1. G 2. M 3. T 	NAT
 BÀI 9. 1. G 2. M 3. T 3.1. 	NAT
 BÀI 9. 1. G 2. M 3. T 3.1. 3.2. 	NAT
 BÀI 9. 1. G 2. M 3. T 3.1. 3.2. 3.3. 	NAT
 BÀI 9. 1. G 2. M 3. T 3.1. 3.2. 3.3. BÀI 10. 	NAT .42 iới thiệu: .42 ô hình mạng. .42 nực hành .43 NAT để truy cập internet. .43 NAT port .45 Hairpin NAT .47 DHCP SNOOPING .48
 BÀI 9. 1. G 2. M 3. T 3.1. 3.2. 3.3. BÀI 10. 1. M 	NAT
 BÀI 9. 1. G 2. M 3. T 3.1. 3.2. 3.3. BÀI 10. 1. M 2. T 	NAT
 BÀI 9. 1. G 2. M 3. T 3.1. 3.2. 3.3. BÀI 10. 1. M 2. T BÀI 11. 	NAT
 BÀI 9. 1. G 2. M 3. T 3.1. 3.2. 3.3. BÀI 10. 1. M 2. T BÀI 11. 1. G 	NAT
 BÀI 9. 1. G 2. M 3. T 3.1. 3.2. 3.3. BÀI 10. 1. M 2. T BÀI 11. 1. G 2. M 	NAT 42 iới thiệu: 42 ô hình mạng. 42 nực hành 43 NAT để truy cập internet. 43 NAT để truy cập internet. 43 NAT port 45 Hairpin NAT 47 DHCP SNOOPING 48 ô hình mạng. 48 cÀi ĐĂT QOS Error! Bookmark not defined. iới thiệu 49 ô hình mạng: 49

Tài liệu thực hành Mikrotik

3.	Th	ực hành	.49
3	.1.	Giới hạn băng thông cho một địa chỉ IP	.49
3	.2.	Giới hạn băng thông cho một lớp mạng	50
3	.3.	Giới hạn băng thông bằng script	.52
BÀI 1	2. V	VPN L2TP/IPSec	54
1.	Gi	ới thiệu:	54
2.	Má	ô hình mạng:	.54
3.	Th	ực hành:	.54

BÀI 1. CÁC LỆNH CLI VÀ MỘT SỐ THAO TÁC THƯỜNG DÙNG

-	Bật romon:	tool romon set enabled=yes							
-	Đặt tên cho router:	system identity set name=CoreRouter							
-	In địa chỉ IP:	ip add print							
-	Cho phép nhận DHCP:	ip dhcp-client add interface=ether1 disable=no							
-	Set địa chỉ IP:	ip	address	add	address=192.168.10.1/24				
	interface=ether1								
-	Trích xuất file script:	expor	t file=myco	onfig					
-	Cập nhật firmware:	IP >>	IP >> Package >> Check For Updates						

BÀI 2. ĐỊA CHỈ IP VÀ MỘT SỐ CÀI ĐẶT CƠ BẢN

BÀI 3. ĐIỀU HƯỚNG MẠNG LAN RA WAN TUỲ Ý

1. Mô hình mạng:

2. Thực hành:

2.1. Cách 1: sử dụng phương pháp danh sách Address List

- Bước 1: Vào IP >> Firewall, tại tab Address Lists bấm dấu + để bắt đầu thêm danh sách địa chỉ mới.
 - Name: đặt tên cho danh sách.
 - Address: có thể là 1 địa chỉ IP, một đoạn, hoặc một lớp mạng.

New Firewall Address List	
Name: X	ОК
Address: 192.168.10.0/24	Cancel
Timeout:	Apply
Creation Time: May/30/2021 11:03:47	Diaphla
	Disable
	Comment
	Сору
	Remove
enabled	

Hình 3.1. Cửa số tạo Address List

Sau khi tạo xong, tab Address List có dạng như sau:



Hình 3.2. Tab address list sau khi tạo xong danh sách địa chỉ.

- Bước 2: vẫn trong cửa sổ Firewall, vào tab Mangle, bấm dấu + để thêm luật Mangle mới.
- Bước 3: tại màn hình New Mangle Rule, tab General, mục Chain: chọn prerouting. Ta còn có thể định tuyến cho dịch vụ mạng bằng cách chọn mục Protocol và chọn Dst. Port là port dịch vụ tương ứng.



Hình 3.3. Tab general của New Mangle Rule

 Bước 4: trong tab Advanced, mục Src. Address List: chọn tên của danh sách địa chỉ đã tạo ở bước 1.

New Mangle R	ule					
General Ad	vanced	Extra	Action	Statistics	L.	ОК
Src. A	ddress Li	st: 📃 [×	₹ ▲		Cancel
Dst. A	ddress Li	st:		•		Apply
Laye	r7 Protoc	ol:		•		Disable
	Conter	nt:		•		Comment
Conne	ction Byte	es:				Сору
Conne	ection Rat	te:		-		Remove
Per Connectio	on Classifi	er:				Reset Counters
Src. M/	AC Addres	SS:		•		Reset All Counters
Out.	Bridge Po	rt:		•		
In.	Bridge Po	rt:		•		
In. Bridg	ge Port Li	st:		•		
Out. Bridg	ge Port Li	st:		•		
IF	Psec Polic	y:		•		
	TLS Ho	st:		•		
Ingr	ress Priori	ty:		•		
	Priori	ty:		•		
D	SCP (TO	S):		•	•	
enabled						

Hình 3.4. Tab advanced của New Mangle Rule

- Buróc 5: trong tab Action,

- Muc Action: chon mark routing.
- Mục New Routing Mark: đánh dấu đường đi ra WAN mong muốn (đặt tên là "DiRaWan1")
- Check vào ô Passthrough



Hình 3.5. Tab action của cửa sổ Mangle Rule

 Bước 6: vào IP >> Route, bấm kép vào đường WAN mong muốn cho danh sách đánh dấu đi ra, chọn copy.

Route List						×
Routes	Nexthops Rules	3 VRF				
+ -		T		Find	all	₹
	Ost. Address	Gateway	Distance	Routing Mark	Pref. Source	▼
AS I	0000/0	192 168 122 1 reachable ether9-oppoeout 1	1	DiRaWan1		
DAS	0.0.0.0/0	192.168.122.1 reachable ether9-pppoeout1	1			
DS	0.0.0.0/0	192.168.1.1 reachable ether10-pppoeout2	1			
DAC	> 192.168.1.0/24	ether10-pppoeout2 reachable	0		192.168.1.83	
DAC	192.168.10.0/	vlan-10 reachable	0		192.168.10.1	
DAC	192.168.20.0/	vlan-20 reachable	0		192.168.20.1	
DAC	192.168.122.0	ether9-pppoeout1 reachable	0		192.168.122.69	
7 items (1	selected)					

Hình 3.6. Cửa sổ Route List

- Bước 7: trong cửa số New Route,
 - Check Gateway: chọn mục ping

• Routing Mark: chọn đường đánh dấu đã đặt tên ở bước 5 (DiRaWan1)

New Route				
General Attribu	es		. [ОК
Dst. Address:	0.0.0/0			Cancel
Gateway:	192.168.122.1	Ŧ		Apply
Check Gateway:	ping			Disable
Туре:	unicast		Ŧ	Comment
Distance:	1		^	Сору
Scope:	30			Remove
Target Scope:	10			
Routing Mark:	DiRaWan1			
Pret. Source:			•	
enabled		active		



2.2. Cách 2: sử dụng phương pháp In. Interface

- Trong cửa số New Mangle Rule, tab General,
 - Mục Chain: chọn prerouting
 - Mục In. Interface: chọn interface mong muốn.

OK Cancel
Cancel
Apply
Disable
Comment
Сору
Remove
Reset Counters
Reset All Counters

Hình 3.8. Sử dụng In. Interface để điều hướng mạng lan

BÀI 4. VLAN VÀ TRUNKING



1. Mô hình mạng:

Hình 4.1. Mô hình mạng vlan và trunking trên mikrotik

2. Thực hành:

2.1. Trên Router:

- Bước 1: Vào Bridge, tạo bridge-vlan

Bridge												
Bridge	Ports	Port Exte	nsions	VLANs	MSTIs	Port MS	ST Overrides	Filters	NAT	Hosts	MDB	
+ -		X 🖻	T	Settings							[Find
Na	ame	A	Туре			L2 MTU	Tx		Rx			Tx Pa 🔻
R 🖀	bridge-	vlan	Bridge			65535		6.1 kbp	s		0 b	ps
4												+
1 item out	of 13											

Hình 4.2. Tạo bridge-vlan

 Bước 2: Trong cửs sổ Bridge, vào tab Ports, thêm port ether 1 làm port trunk vào bridge-vlan.



Hình 4.3. Thêm port ether1 làm port trunk vào bridge-vlan

- Bước 3: Vào Interfaces >> VLAN, tạo ra các VLAN và gán các VLAN này vào Interface bridge-vlan đã tạo ở bước 1.
 - Name: nhập tên đại diện vlan
 - VLAN ID: nhập số ID của vlan
 - Interface: bridge-vlan

Interface <vlan-10></vlan-10>			
General Loop Protect	Status Traffic		ОК
Name: vlan-10			Cancel
Type: VLAN			Apply
MTU: 1500			Disable
Actual MTU: 1500			Comment
L2 MTU: 65531			Conv
MAC Address: 0C:58:C4:62	2:30:00		Сору
ARP: enabled		₹	Remove
ARP Timeout:			Torch
VLAN ID: 10			
Interface: bridge-vlan		₹	
Use Serv	ice Tag		
enabled	nunning	slave	
		0.010	

Hình 4.4. Tạo ra các vlan và gán vào Interface bridge-vlan

- Bước 4: Vào IP >> Address, gán địa chỉ IP cho các VLAN vừa tạo.
 - Address: địa chỉ ip của vlan
 - Network: lớp mạng
 - Interface: chọn vlan

Address <192.168.10.1/24>	
Address: 192.168.10.1/24	ОК
Network: 192.168.10.0	Cancel
Interface: vlan-10	Apply
	Disable
	Comment
	Сору
	Remove
enabled	

Hình 4.5. Gán địa chỉ IP cho VLAN

Hình 4.6. Tạo địa chỉ ip của vlan và gán vào interface vlan tương ứng.

 Bước 5: Vào IP >> DHCP Server, bấm vào nút DHCP Setup, lần lượt tạo DHCP Server cấp địa chỉ IP cho các vlan.

DHCP Networks I	Leases Options	Option Sets	Vendor Classes	Alerts		
	DHCP Confi	DHCP Se				
		g	etup			Find
Name 🗠	Interface	Relay	Lease Time	Address Pool	Add AR	•
dhcp1	vlan-10		00:10	:00 dhcp_pool0	no	
dhcp2	vlan-20		00:10	:00 dhcp_pool1	no	
2 items						



2.2. Trên Switch:

- Bước 1: Vào Bridge, tạo bridge-sw.

Bridge												
Bridge	Ports	Port Exte	ensions	VLANs	MSTI	Port MS	ST Overrides	Filters	NAT	Hosts	MDB	
+ -		× 🖻	7	Settings								Find
N	ame	1	Туре			L2 MTU	Tx		Rx			Tx Pa 🔻
R 都	bridge-	sw	Bridge			65535		0 b	ps		01	ops
												•
1.1												•
I item our	torii											

Hình 4.8. Tạo bridge-sw

 Bước 2: Bấm kép vào bridge-sw vừa tạo, vào tab VLAN, check vào ô "VLAN Filtering". Các mục còn lại để mặc định.

Interface <bridge-sw></bridge-sw>			
General STP VLAN Sta	atus Traffic		OK
VLAN Filterin	ng		Cancel
EtherType: 0x8100		₹	Apply
PVID: 1			Disable
Frame Types: admit all	ina	₹	Comment
	ing (Сору
			Remove
			Torch
enabled	running	slave	



Bước 3: Trong cửa sổ Bridge, vào tab Ports, thêm vào các port có liên quan đến VLAN, kể cả port ether1 là port trunk

Bridge														
Bridge	Ports	Port Extensio	ons VL	ANs N	MSTIs	Port N	IST Over	rides	Filters	NAT	Hosts	MDB		
+ -		× 🖻	7										Find	
#	Interfa	ice	Bridge			Horizon	Trusted	Priorit	y (h	Path Cos	t Ro	е		R▼
0	🛎 eth	ner1	bridge-	sw			no		80		10 des	ignated p	oort	
1	👗 eth	ner3	bridge-	sw			no		80		10 des	ignated p	oort	
2	🛎 eth	ner4	bridge-	sw			no		80		10 des	ignated p	oort	
•														•
3 items														

Hình 4.10. Thêm các port có liên quan đến vlan

Bước 4: Vẫn trong tab Ports, gán vlan vào port bằng cách bấm kép vào từng port.
 Đối với port ether 1 là port trunk, tại tab VLAN của port này, ta để mặc định và không chỉnh sửa.

Bridge Port <ether1></ether1>			
General STP VLAN	Status		ОК
PVID: 1			Cancel
Frame Types: admit all		₹	Apply
Ingress Fi	litering		Disable
	King		Comment
			Сору
			Remove
an abla d			

Hình 4.11. Port trunk ether1, trong tab VLAN để mặc định.

Bước 5: Vẫn trong tab Ports, tiếp tục bấm kép vào các port còn lại, vào tab VLAN của port đó:

- Mục PVID: gán vlan tương ứng.
- Muc Frame Types: chon admit only untagged and priority tagged.
- Check vào ô Ingress Filtering

Bridge Port <ether3></ether3>			
General STP VLAN	Status		ОК
PVID: 10 Frame Types: admit only u ♥ Ingress Fi	ntagged and priority tagged iltering king		Cancel Apply Disable Comment Copy Remove
enabled	inactive	Hw. Offlo	ad

Hình 4.12. Cấu hình cho port access (port giải mã vlan)

- Bước 6: Trong cửa sổ Bridge, vào tab VLANs,
 - Bridge: bridge-sw
 - VLAN IDs: nhập vào ID của vlan
 - Tagged: port làm port trunk
 - Untagged: port giải mã vlan



Hình 4.13. Cấu hình cho vlan đi qua port trunk và port access

Tiếp tục thực hiện với các vlan còn lại. Sau khi làm xong ta có bảng VLANs như sau:

Tài liệu thực hành Mikrotik

Bridge											
Bridge	Ports	Port Exte	ensions	VLANs	MSTIs	Port MST Overrides	Filters	NAT	Hosts	MDB	
+ -		* 🖻	7								Find
Bridge	e	∨L	AN IDs		Current 1	lagged	7	Curre	nt Untag	ged	•
bridge-sw 10 ether1						ether	3				
bridge	e-sw	20)		ether1			ether	4		
D bridge	e-sw	1						bridge	e-sw, eth	er1	
											•
3 items											

Hình 4.14. Bảng VLANs

3. Kiểm tra:

Trên Pc1, vào web console gõ lệnh ip dhcp, nếu nhận được ip thì thành công.

GNS3 console	PC1	×			-	×
Welcome to Virtual PC Sim Dedicated to Daling. Build time: Apr 10 2019 Copyright (c) 2007-2015, All rights reserved.	mulator, y 16:35:00 Paul Meng	version 0. g (mirnshi	.8.1 i@gmail.com)			A
VPCS is free software, d Source code and license For more information, pl	istributed can be fou ease visit	d under th und at vpo t wiki.fre	ne terms of the cs.sf.net. eecode.com.cn.	e "BSD" licer	ice.	
Press '?' to get help.						
Executing the startup fi	le					
PC1> ip dhcp DORA IP 192.168.10.254/2	4 GW 192.3	168.10.1				
PC1> []						

Hình 4.15. Kiểm tra trên Pc1

Trong Core Router, cửa sổ DHCP Server tại tab Leases, sẽ thấy có IP cấp cho PC1.

DHCP	Server										
DHCP	Networks	Leases	Options	Option Sets	Vendo	r Classes	Alert	s			
+	- 🖉 🔛	[Chec	k Status						Find	
A	ddress 🗸	MAC Add	dress	Client ID		Server		Active Address	Active MA	CAddre	. A 🔻
D 1	92.168.10.254	00:50:79	:66:68:00	1:0:50:79:60	6:68:0	dhcp1		192.168.10.254	00:50:79:6	6:68:00	PC1
D 1	92.168.20.254	00:50:79	:66:68:01	1:0:50:79:66	5:68:1	dhcp2		192.168.20.254	00:50:79:6	6:68:01	PC2
♦ 2 items											•

Hình 4.16. IP cấp cho Pc1

BÀI 5. LINK AGGREGATION CONTROL PROTOCOL 802.3ad

1. Lý thuyết:

Khi mà dữ liệu truyền tải quá lớn đến nỗi đường truyền không đáp ứng được thì thay vì ta phải nâng cấp hay mua thiết bị mới thì ta sẽ nghĩ tới việc mở thêm nhiều kết nối dây giữa các Switch để cân bằng tải dữ liệu.

Ví dụ: Ta có hai Switch đang kết nối với nhau bằng cổng Fast Ethernet 100 Mbit trong khi các PC Host kết nối Switch thì dùng cổng Fast với băng thông 1000 Mbit. Hiển nhiên khi mà PC muốn truyền tải một lượng lớn dữ liệu hơn 100 Mbit đi thì tại Switch sẽ xảy ra hiện tượng nghẽn Traffic, các gói tin trong hàng đợi khi quá ngưỡng Cache thi sẽ bị Drop bỏ.

LACP (Link Aggregation Control Protocol): là giao thức cấu hình EtherChannel chuẩn quốc tế IEEE 802.3ad và có thể dùng được cho hầu hết các thiết bị thuộc các hãng khác nhau, LACP hỗ trợ ghép tối đa 16 Link vật lý thành một Link luận lý (8 Port Active – 8 Port Passive).

LACP có 3 chế độ:

- On: Chế độ cấu hình EtherChannel tĩnh, chế độ này thường không được dùng vì các Switch cấu hình EtherChannel có thể hoạt động được và cũng có thể không hoạt động được vì các Switch được cầu hình bằng tay phục thuộc vào con người nên hoàn toàn không có bước thương lượng trao đổi chính sách giừa bên dẫn đến khả năng Loop cao và bị STP Block.
- Active: Chế độ tự động Tự động thương lượng với đối tác
- Passive: Chế độ bị động Chờ được thương lượng



2. Mô hình mạng:

Hình 5.1. Mô hình mạng kết hợp bonding và vlan trunking trên mikrotik

3. Thực hành:

3.1. Trên Router

- Bước 1: Vào Interfaces >> Bonding, tạo bonding-router, thêm port ether1 và ether 2 vào bonding-router.
 - Slaves: ether1 và ether 2
 - Mode: 802.3ad
 - Transmit Hash Policy: layer 2 and 3

New Interface			
General Bonding	Status Traffic		ОК
Slaves:	ether1	Ŧ \$	Cancel
	ether2	₹ \$	Apply
Mode:	802.3ad	•	Disable
Primary:	none	₹	Comment
Transmit Hash Policy:	laver 2 and 3	▼	Сору
Min. Links:	0		Remove
Down Delay:	0	ms	Torch
Up Delay:	0	ms	Monitor Slaves
LACP Rate:	30 s	₹	
MII Interval:	100	ms	
enabled	running	slave	

Hình 5.2. Thêm port vào bonding

Kết quả sau khi tạo bonding-router:



Hình 5.3. Bảng bonding

- **Bước 2:** Trong cửa sổ Bridge, tạo bridge-vlan. Vào tab Ports, thêm port bondingrouter làm port trunk vào bridge-vlan.

Bridge Port <bonding-router></bonding-router>	
General STP VLAN Status	ОК
Interface: bonding-router	Cancel
Bridge: bridge-vlan	Apply
Horizon:	Disable
Leam: auto	Comment
✓ Unknown Unicast Flood	Сору
 Unknown Multicast Flood 	Remove
✓ Broadcast Flood	
Trusted	
✓ Hardware Offload	
Multicast Router: Temporary Query	
Fast Leave	
enabled inactive Hw. Office	ad

Hình 5.4. Thêm port bonding-trunk làm port trunk vào bridge-vlan

- Bước 3: Vào Interfaces >> VLAN, tạo ra các VLAN và gán các VLAN này vào Interface bridge-vlan đã tạo ở bước 1.
 - Name: nhập tên đại diện vlan
 - o MTU: 1496 (đối với GNS3)
 - VLAN ID: nhập số ID của vlan
 - Interface: bridge-vlan

New Interface			
General Loop Protect	Status Traffic		ОК
Name: vlan-10			Cancel
Type: VLAN			Apply
MTU: 1496			Disable
Actual MTU:			Comment
MAC Address:			Сору
ARP: enabled		₹	Remove
ARP Timeout:		•	Torch
VLAN ID: 10			
Interface: bridge-vlan		₹	
Use Ser	vice Tag		
enabled	running	slave	

Hình 5.5. Tạo ra các vlan và gán vào Interface bridge-vlan

Bước 4: Vào IP >> Address, tạo địa chỉ IP cho các VLAN. Gán địa chỉ IP này cho Interface vlan tương ứng.

Address <192.168.10.1/24>	
Address: 192.168.10.1/24	ОК
Network: 192.168.10.0	Cancel
Interface: vlan-10	Apply
	Disable
	Comment
	Сору
	Remove
enabled	

Hình 5.6. Tạo địa chỉ ip của vlan và gán vào interface vlan tương ứng.

 Bước 5: Vào IP >> DHCP Server, bấm vào nút DHCP Setup, lần lượt tạo DHCP Server cấp địa chỉ IP cho các vlan.

DHCP Serve	r									
DHCP N	etworks	Leases	Options	Option Sets	Vendor	Classes	Alerts			
+		7	DHCP Conf	fig DHCP S	etup					Find
Name		Interface	ce	Relay	Lease	Time	Add	lress Pool	Add AR	•
dhcp1		vlan-1(0			00:10:0	00 dhc	p_pool0	no	
dhcp2		vlan-20	0			00:10:0	00 dhc	p_pool1	no	

Hình 5.7. Tạo DHCP Server cấp địa chỉ IP cho các vlan

3.2. Trên Switch:

Bước 1: tạo bonding: tương tự như trên router, tạo bonding-sw chứa port ether1 và ether2.

Interface <bonding-sw< th=""><th>></th><th></th><th></th></bonding-sw<>	>		
General Bonding	Status Traffic		ОК
Slaves:	ether1	₹ \$	Cancel
	ether2	₹ \$	Apply
Mode:	802.3ad	₹	Disable
Primary:	none	▼	Comment
Link Monitoring:	mii		Сору
Min. Links:	0		Remove
Down Dolay:	0		Torch
Up Delay:	0	ms	Monitor Slaves
LACP Rate:	30 s	₹	
MII Interval:	100	ms	
enabled	running	slave	

Hình 5.8. Bonding trên switch

- Bước 2: Vào Bridge, tạo bridge-sw.

Bridge											
Bridge	Ports F	Port Extensions	VLANs	MSTIs	Port MS	ST Overrides	Filters 1	TAV	Hosts	MDB	
+ -	<pre></pre>	8 🖻 🍸	Settings								Find
N	ame	∠ Type		_	L2 MTU	Tx		Rx			Tx Pa 🔻
R 🏼	bridge-sv	v Bridge			65535		0 bps	3		01	ops
•											•
1 item out	t of 11										

Hình 5.9. Tạo bridge-sw

 Bước 2: Bấm kép vào bridge-sw vừa tạo, vào tab VLAN, check vào ô "VLAN Filtering". Các mục còn lại để mặc định.

Interface <bridge-sw></bridge-sw>			
General STP VLAN St	atus Traffic		ОК
VLAN Filteri	ng		Cancel
EtherType: 0x8100		₹	Apply
PVID: 1			Disable
Frame Types: admit all	ring		Comment
	y		Сору
			Remove
			Torch
enabled	running	slave	

Hình 5.10. Check vào ô "VLAN Filtering"

Bước 3: Trong cửa sổ Bridge, vào tab Ports, thêm vào các port có liên quan đến VLAN, kể cả port bonding-sw là port trunk

Bridge												
Bridge	Ports Port Extension	ons VLANs	MSTIs	Port M	IST Over	ides	Filters	NAT	Hosts	MDB		
+ -		ĩ									Find	
#	Interface	Bridge	I	Horizon	Trusted	Priority	y (h	Path Cost	Rol	е		R▼
0	🖀 bonding-sw	bridge-sw			no		80	1	0 des	ignated (port	
1	🖀 ether3	bridge-sw			no		80	1	0 des	ignated (port	
2	🚢 ether4	bridge-sw			no		80	1	0 des	ignated j	port	
												•
3 items												

Hình 5.11. Thêm các port có liên quan đến vlan vào bridge-sw

Bước 4: Vẫn trong tab Ports, gán vlan vào port bằng cách bấm kép vào từng port.
 Đối với port bonding-sw là port trunk, tại tab VLAN của port này, ta để mặc định và không chỉnh sửa.

Bridge Port <bonding-sw></bonding-sw>			
General STP VLAN	Status		ОК
PVID: 1			Cancel
Frame Types: admit all		₹	Apply
Ingress F	iltering		Disable
I ag Stac	king		Comment
			Сору
			Remove
enabled	inactive	Hw. Offloa	ad

Hình 5.12. Port trunk ether1, trong tab VLAN để mặc định.

- Bước 5: Vẫn trong tab Ports, tiếp tục bấm kép vào các port còn lại, vào tab VLAN của port đó:
 - $\circ~$ Mục PVID: gán vlan tương ứng.
 - Muc Frame Types: admit all.

Bridge Port <ether2></ether2>			□×
General STP VLAN St	atus		ОК
PVID: 10			Cancel
Frame Types: admit all		₹	Apply
Ingress Filte	ring		Disable
ag Stackir	ng		Comment
			Сору
			Remove
enabled	nactive	Hw. Offload	1

Hình 5.13. Cấu hình cho port access (port giải mã vlan)

- **Bước 6:** Sau cùng ta có bảng VLANs như sau:

Tài liệu thực hành Mikrotik

Bridge											
Bridge	Ports	Port E	xtensions	VLANs	MSTIs	Port MST Overrides	Filters	NAT	Hosts	MDB	
+ -		8	· 7								Find
Bridge	•	Δ.	VLAN IDs		Current T	agged		Currer	nt Untag	ged	-
D bridge	-sw		1					bridge	e-sw, bor	nding-sw	
bridge	-sw		10		bonding-	SW		ether:	3		
bridge	-sw		20		bonding-	SW		ether4	4		
•											•
3 items											

Hình 5.14. Bảng VLANs

BÀI 6. VLAN MANAGEMENT

1. Giới thiệu:

• • •

2. Mô hình mạng:

•••

3. Thực hành:

3.1. Trên router:

- Bước 1: khởi tạo vlan99 (vlan management). Vào Interface chọn VLAN. Bấm dấu + để tạo vlan mới.
 - **Name:** vlan99 (tên đại diện, bạn có thể thay đổi tuỳ ý)
 - VLAN ID: 99
 - Interface: bridge-router

Interface <vlan99></vlan99>			
General Loop Protect St	atus Traffic		ОК
Name: vlan99			Cancel
Type: VLAN			Apply
MTU: 1500			Disable
Actual MTU: 1500			Comment
L2 MTU: 15/6	44-70		Сору
ARP: enabled	4A.7C		Remove
ARP Timeout:			Torch
VLAN ID: 99 Interface: bridge-router	æ Tag	Ŧ	
enabled	running	slave	

Hình 6.1. Tạo vlan quản lý

- Bước 2: đặt địa chỉ IP cho vlan quản lý. Vào IP, chọn address, bấm dấu + để tạo địa chỉ mới.
 - **Muc Address:** 192.168.99.1/24
 - Network: 192.168.99.0

• Interface: vlan99

Address <192.168.99.1/24>	
Address: 192.168.99.1/24	ОК
Network: 192.168.99.0	Cancel
Interface: vlan99	Apply
	Disable
	Comment
	Сору
	Remove
enabled	



3.2. Trên switch:

- Bước 1: gán vlan99 vào bridge-sw. Vào Bridge chọn VLANs, bấm dấu + để thêm VLAN mới.
 - VLAN IDs: 99
 - **Tagged:** chọn interface kết nối trực tiếp với router, có thể chọn tiếp interface mà muốn chuyển vlan này đi tiếp, chọn interface bridge-sw.

Bridge VLAN <99>		
Bridge:	bridge-sw ₹	ОК
VLAN IDs:	99 🗢	Cancel
Tagged:	bonding-trunk 🗧 🖨	Apply
	bonding-trunk-port21+23 🛛 🗸 🗢	
	bridge-sw	Disable
Untagged:	\$	Comment
Current Tagged:	bridge-sw	Сору
	bonding-trunk	Remove
	bonding-trunk-port21+23	
Current Untagged:		
enabled		

Hình 6.3. Thêm vlan quản lý vào bridge-sw

- Bước 2: Tạo vlan 99 và gán vlan id 99 vào interface bridge-sw. Vào Interface, chọn VLAN, bấm dấu + để thêm vlan mới.
 - Name: vlan99

- **VLAN ID:** 99
- Interface: bridge-sw

Interface <vlan99></vlan99>			
General Loop Protect Sta	atus Traffic		ОК
Name: vlan99			Cancel
Type: VLAN			Apply
MTU: 1500			Disable
Actual MTU: 1500			Comment
L2 MTU: 1588			Сору
MAC Address: 08:55:31:C0:4	C:F5		Pomovo
ARP: enabled			Temove
ARP Timeout:		L	Torch
VLAN ID: 99			
Interface: bridge-sw		•	
Use Service	e Tag		
enabled	running	slave	

Hình 6.4. Gán vlan id 99 cho interface bridge-sw

- Bước 3: gán địa chỉ IP cho vlan 99. Vào IP >> Address. Bấm dấu + để thêm địa chỉ IP mới.
 - Address: 192.168.99.2/24
 - Network: 192.168.99.0
 - Interface: vlan99

Address <1	92.168.99.2/24>	
Address:	192.168.99.2/24	ОК
Network:	192.168.99.0	Cancel
Interface:	vlan99 Ŧ	Apply
		Disable
		Comment
		Сору
		Remove
enabled		



Bước 4: tạo route đến gateway của vlan 99. Vào IP >> Route, bấm dấu + để tạo route mới. Mục gateway: nhập vào địa chỉ IP của vlan 99 ở router: 192.168.99.1.

Route <0.0.0/0>	,				
General Attribu	tes				OK
Dst. Address:	0.0.0/0				Cancel
Gateway	192.168.99.1	₹	reachable vlan99	\$	Apply
Check Gateway:					Disable
Туре:	unicast			₹	Comment
Distance:	1			▲	Сору
Scope:	30				Remove
Target Scope:	10				
Routing Mark:				•	
Pref. Source:				•	
enabled			active	static	

Hình 6.6. Tạo route đến gateway vlan 99 ở router.

BÀI 7. FIREWAL CƠ BẢN

1. Yêu cầu:

- Mặc định các vlan trên Mikrotik đều là intervlan. Do đó, ta phải điều chỉnh lại để cho một số vlan không nhìn thấy nhau. Yêu cầu:
- Không cho các địa chỉ trong vlan public thấy các địa chỉ trong vlan private và gateway của các vlan khác, chỉ được phép thấy gateway của vlan chính nó.
- Không cho địa chỉ ip giữa các vlan public thấy lẫn nhau.

2. Thực hiện trên router

- Tóm tắt các bước:
 - Tạo hai danh sách interface dành cho các vlan private và public, sau đó thêm các vlan interface vào hai danh sách.
 - Tạo một danh sách địa chỉ (address list) và thêm các gateway của vlan vào danh sách.
 - Sử dụng
- Bước 1: vào Interface >> Interface List, bấm dấu vào nút Lists để bắt đầu thêm danh sách mới. Bấm Ok sau khi tạo xong danh sách.
 - Danh sách 1: ListPublic
 - Danh sách 2: ListPrivate

OK
Cancel
Apply
Comment
Сору
Remove

Hình 7.1. New interface list

Bước 2: trở lại màn hình Interface List, bấm dấu + để thêm member vào danh sách. Tiếp tục thêm các member khác cho đến hết.

Interface List Member <listprivate phong="" vlan10_van=""></listprivate>	
List: ListPrivate ∓	ОК
Interface: vlan10_van phong ∓	Cancel
	Apply
	Disable
	Comment
	Сору
	Remove
enabled	

Hình 7.2. Thêm member vào Interface List

Tương tự, thực hiện tiếp với danh sách ListPublic.

Bước 3: vào IP >> Firewall, Address Lists, tạo danh sách các gateway của các vlan thuộc ListPrivate:

Firewall										
Filter Rules	NAT	Mangle	Raw	Service Ports	Connections	Address Lists	Layer7 Protoco	ls		
+ - <	/ 22	2	7					Find	all	Ŧ
Name		1	Addre	SS	∇ Timeout	Creatio	n Time			
 Danh 	SachGa	teWay	192.1	68.99.1		Jun/27	/2021 20:			
Danh	SachGa	teWay	192.1	68.88.1		Jun/27	/2021 20:			
 Danh 	SachGa	teWay	192.1	68.45.1		Jun/27	/2021 20:			
 Danh 	SachGa	teWay	192.1	68.10.1		Jun/27	/2021 20:			
4 items										

Hình 7.3. Danh sách các gateway các vlan của ListPrivate

- **Bước 4:** vào IP >> Firewall, tab Filter Rules, bấm dấu + để thêm luật mới.

Ý nghĩa các chain forward và input:

- Chain forward: dữ liệu đi qua router
- Chain input: dữ liệu đi vào router.

Không cho các vlan trong danh sách public thấy các vlan trong danh sách private. Để làm được điều này, ta tạo một chain forward với action là drop.

- Chain: forward,
- In. Interface List: ListPublic,
- Out. Interface List: ListPrivate,
- Action: drop

Firewall Rule <>			
General Advanced	Extra Action Statistics	. [ОК
Chain:	forward	₹ [Cancel
Src. Address:		• [Apply
Dst. Address:		- ┌	Disable
Protocol:		▾╎┌	Comment
Src. Port:		• Ē	Сору
Dst. Port:			Remove
Any. Port:		Ţ	Reset Counters
Out. Interface:		- [Reset All Counters
In. Interface List:	ListPublic Ŧ	•	
Out. Interface List:	ListPrivate T	•	
Packet Mark:		•	
Connection Mark:		-	
Routing Mark:		•	
Routing Table:		•	
Connection Type:		•	
Connection State:		•	
Connection NAT State:		•	
enabled			

Hình 7.4. Không cho danh sách public thấy danh sách private

Không cho các địa chỉ ip trong danh sách public thấy nhau.

- Chain: forward,
- In. Interface List: ListPublic,
- Out. Interface List: ListPublic,
- Action: **drop**

Không cho vlan thuộc ListPublic ping tới gateway của các vlan thuộc ListPrivate. Để làm được điều này, ta tạo một luật với chain input và action là drop.

- Chain: input
- In. Interface List: ListPublic
- o Dst. Address List: DanhSachGateWay
- Action: **drop**

New Firewall Rule				1		
General Advanced	Extra	Action	Statistics			ОК
Chain:	input			₹] [Cancel
Src. Address:				•	• [Apply
Dst. Address:						Disable
Protocol:						Comment
Src. Port:						Сору
Dst. Port:						Remove
Any. Port:						Reset Counters
Out. Interface:	:				. [Reset All Counters
In. Interface List:		stPublic			-	
Out. Interface List:						
Packet Mark:						
Connection Mark:						
Routing Mark:						
Routing Table:				•		
				•		
Connection Type:						
Connection Type: Connection State:					·	

Hình 7.5. Không cho ListPublic ping tới gateway của ListPrivate

Kết quả sau khi làm xong:

Firew	all														
Filte	r Rules	NAT	Mangle R	law Service	Ports Connec	tions Addr	ess Lists L	ayer7 Protoco	ols						
÷	- 🗸	×	- 7	💿 Reset Co	unters (O R	eset All Count	ers						Find	all	₹
#	Actio	n	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Inter	Out. Int	In. Interface List	Out. Interface List	Src. Ad	Dst. Addre	ss 🔻
	drop traffic	c from	vlan public to	vlan private											
0	🗱 d	rop	forward								ListPublic	ListPrivate			
	drop traffic	c from	vlan public to	vlan public											
1	🗱 d	rop	forward								ListPublic	ListPublic			
	drop traffic	c from	vlan public to	gateway vlan	private										
2	💢 d	rop	input								ListPublic			DanhSach	nGate\
•															•
3 iter	ns (1 selec	ted)													

Hình 7.6. Filter Rules

BÀI 8. CÂN BẰNG TẢI VÀ FAIL OVER

1. Giới thiệu:

MikroTik hỗ trợ cân bằng tải nhiều đường WAN dựa trên tính năng gọi là "PCC – Per Connection Classifier". Dữ liệu trong mạng nội bộ đi ra Internet sẽ được chia đều các gói tin ra ngoài theo các đường WAN ngẫu nhiên.

Để làm được điều này, ta phải "mark" (đánh dấu) kết nối và đường đi gói tin hợp lý để một gói tin khi đi ra ngoài internet bằng đường WAN với IP Local nào thì khi quay lại nó sẽ phải đi vào đúng đường WAN nó đã đi ra. Cùng với đó là việc kết hợp thêm "PCC" và chỉnh lại Routes để đặt đường đi, cài đặt độ ưu tiên cho đường WAN (Failover).

Công thức của PCC rất đơn giản, sử dụng thuật toán băm theo tỷ lệ. Ví dụ hai đường WAN có cùng tốc độ: WAN1: 100Mb/s và WAN2: 100Mb/s, lúc này tỉ lệ sẽ là 1:1. Do đó tỉ lệ PCC sẽ là 2/0 và 2/1.

Trường hợp hai đường WAN có tốc độ khác nhau, giả sử WAN1: 100Mb/s, WAN2: 50Mb/s, tỉ lệ lúc này sẽ là 2:1. Do đó tỉ lệ PCC cho WAN1(100Mb/s) là hai phần 3/0 và 3/1, của WAN2 (50Mb/s) là một phần 3/2

2. Mô hình mạng

Các bước thực hiện:

- Tạo prerouting chấp nhận cho các lớp mạng bên trong nội bộ không cần đi qua cân bằng tải.
- Đánh dấu các kết nối đi vào từ internet.
- Đánh dấu các kết nối đi ra internet từ trong mạng lan.
- Cân bằng tải
- Kết nối đi vào từ wan nào thì chỉ đường đi ra lại đúng wan đó.
- Tạo route cho các kết nối đánh dấu đi ra đúng wan tương ứng

3. Thực hành

3.1. Cấu hình cân bằng tải và fail over bằng dòng lệnh

Giả sử ta cần cấu hình cân bằng tải trên hai đường WAN VNPT_1 và VNPT_2 kiểu **both-addresses-and-ports** và dự phòng (failover)

 Bước 1: tạo luật mangle chấp nhận lưu lượng trong mạng nội bộ sẽ không bị ảnh hưởng bởi các luật mangle của firewall.

- dst-address: là lớp mạng sẽ chấp nhận không đi qua cân bằng tải.
- In-interface: là interface trong mạng nội bộ

Luật mangle này kiểm tra mọi traffic có đích đến (dst-address) là mạng LAN (192.168.10.0/24) và interface tiếp nhận traffic là BridgeLAN. Action "accept" với mục đích dừng không xử lý traffic này với các rule kế tiếp sau. Để bắt traffic đi qua các rule bên dưới tiếp theo, cần khai báo trường "passthrough=yes".

```
/ ip firewall mangle
```

```
add chain=prerouting dst-address=192.168.10.0/24
action=accept in-interface=BridgeLAN
```

Bước 2: đánh dấu kết nối khởi tạo từ bên ngoài đi vào mạng nội bộ (interface pppoe-out1 và pppoe-out 2). Những kết nối chưa được đánh dấu (no-mark) sẽ được đánh dấu (mark) là "danhdauVNPT1" và "danhdauVNPT2"

```
add chain=prerouting in-interface=pppoe-out1 connection-
mark=no-mark action=mark-connection new-connection-
mark=danhdauVNPT1
add chain=prerouting in-interface=pppoe-out2 connection-
mark=no-mark action=mark-connection new-connection-
mark=danhdauVNPT2
```

- Bước 3: đánh dấu kết nối khởi tạo bên trong mạng nội bộ đi ra internet, sử dụng thuật toán pcc (per-connection-classifier). Trong đó:
 - o both-address: chỉ cân bằng tải
 - o both-address-and-ports: cân bằng tải và gộp băng thông

```
add chain=prerouting in-interface=BridgeLAN connection-
mark=no-mark dst-address-type=!local per-connection-
classifier=both-addresses-and-ports:2/0 action=mark-
connection new-connection-mark=danhdauVNPT1
add chain=prerouting in-interface=BridgeLAN connection-
mark=no-mark dst-address-type=!local per-connection-
```

Tài liệu thực hành Mikrotik

```
classifier=both-addresses-and-ports:2/1 action=mark-
connection new-connection-mark=danhdauVNPT2
```

 Bước 4: những traffic khởi tạo từ interface BridgeLAN sẽ đánh dấu là "diraVNPT1" hoặc "diraVNPT2".

```
add chain=prerouting connection-mark=danhdauVNPT1 in-
interface=BridgeLAN action=mark-routing new-routing-
mark=diraVNPT1
add chain=prerouting connection-mark=danhdauVNPT2 in-
interface=BridgeLAN action=mark-routing new-routing-
mark=diraVNPT2
```

 Bước 5: đối với những traffic đi ra ngoài (output) được đánh dấu là "danhdauVNPT1" hoặc "danhdauVNPT2", ta sẽ đánh dấu đường đi cho nó là "diraVNPT1" hoặc "diraVNPT2"

```
add chain=output connection-mark=danhdauVNPT1 action=mark-
routing new-routing-mark=diraVNPT1
add chain=output connection-mark=danhdauVNPT2 action=mark-
routing new-routing-mark=diraVNPT2
```

 Bước 6: cấu hình cho bảng định tuyến, gán gateway pppoe-out1 cho đánh dấu "diraVNPT1" và ppoe-out2 cho đánh dấu "diraVNPT2"

```
/ ip route
add check-gateway=ping distance=1 gateway=pppoe-out1
routing-mark=diraVNPT1
add check-gateway=ping distance=1 gateway=pppoe-out2
routing-mark=diraVNPT2
```

- Bước 7: cấu hình failover

```
/ip route
```

```
add check-gateway=ping distance=1 gateway=pppoe-out1
add check-gateway=ping distance=2 gateway=pppoe-out2
```

- 3.2. Cấu hình cân bằng tải bằng giao diện
- Bước 1: khai báo pppoe cho pppoe-out 1: vào Interface >> Bấm dấu +, chọn New Interface. Tại tab Dial Out:
 - User: điền vào username pppoe
 - Password: nhập mật khẩu
 - o Tích chọn Add Default Route
 - Default Route Distance: 1+n với n là số đường truyền kế tiếp

iew Interface			
General Dial Out Stat	us Traffic		OK
Service:		•	Cancel
AC Name:		•	Apply
User:	69961 130		Disable
Password:		•	Comment
Profile:	default	Ŧ	Сору
Keepalive Timeout:	10	•	Remove
	Dial On Demand		Torch
	Use Peer DNS		PPPoE Sca
	Add Default Route		
Default Route Distance:	1		
Allow:	mschap2 ✓ mschap1 ✓ pap		

Hình 8.1. Tab dial out của màn hình New Interface

Lặp lại bước 1 cho các đường Wan tiếp theo.

Bước 2: tạo Interface List đưa các đường WAN vào danh sách. Vào Interface
 >> tab Interface List >> bấm nút List để thêm danh sách. Name: đặt tên cho danh sách Interface. >> OK.

Interface List <list_wan></list_wan>	
Name: List_Wan	ОК
Include:	Cancel
Exclude:	Apply
	Comment
	Сору
	Remove

Hình 8.2. New Interface List

- Bước 3: quay lại tab Interface List, bấm dấu +,
 - List: chọn tên danh sách interface vừa tạo ở bước 2.
 - Interface: thêm vào các interface pppoe





Sau khi thêm xong, màn hình Interface List như sau:

Interface Lis	st 🗌									⊐ ×
Interface	Interface List	Etheme	et EoIP Tunnel	IP Tunnel	GRE Tunnel	VLAN	VRRP	Bonding	LTE	
+ -	/ 🛛 🖻	7	Lists			Fi	nd	all		₹
List		A	nterface							•
List_Wa	n	e	ther1							
List_Wa	n	e	ther2							
_										
2 items										

Hình 8.4. Màn hình Interface List sau khi thêm interface

- Bước 4: tạo luật NAT để truy cập được internet: vào IP >> Firewall >> tab NAT. Bấm dấu + để thêm luật NAT mới. Tại tab General:
 - Chain: srcnat
 - Out. Interface List: chọn danh sách interface đã tạo

New NAT Rule			
General Advance	Extra Action Statistics		ОК
Chain:	cnat	₹	Cancel
Src. Address:		▼	Apply
Dst. Address:		▼	Disable
Protocol:		▼	Comment
Src. Port:		▼	Сору
Dst. Port:		_	Remove
In Interface:		¥	Reset Counters
Out. Interface:			Reset All Counters
In. Interface List:		_	
Out. Interface List:	List_Wan		
Packet Mark:		▼	
Connection Mark:		▼	
Routing Mark:		▼	
Routing Table:		▼	
Connection Type:		▼	
enabled			

Hình 8.5. Tab general của màn hình New Nat Rule

 Bước 5: cũng trong màn hình New Nat Rule, chọn tab Action, mục Action: chọn masquerade

3.3. Tạo danh sách địa chỉ IP bỏ qua cân bằng tải:

Khi cấu hình cân bằng tải, một số trang thanh toán trực tuyến sẽ không cho phép thao tác hoặc bị lỗi vì chúng chỉ chấp nhận một địa chỉ IP WAN trong suốt quá trình giao dịch. Để sửa lỗi này, ta có thể định tuyến các máy tính cần sử dụng dịch vụ trên theo đường WAN cụ thể, hoặc đơn giản là loại bỏ các máy này ra khỏi cân bằng tải.

- Bước 1: tạo danh sách địa chỉ IP (Address List) bỏ qua cân bằng tải. Vào IP >>
 Firewall >> Address Lists. Thêm IP các máy tính cần loại ra khỏi cân bằng tải và
 đặt tên cho danh sách, ví dụ "List_Khong_CBT".
- Bước 2: trong Mangle Rule, ta thêm vào rule như hình sau và kéo lên vị trí trên cùng:

Mangle Rule 🗢		New Mangle Rule		New Mangle Rule	
General Advanced Extra Action Statistics	ОК	General Advanced Extra Action Statistics	ОК	General Advanced Extra Action Statistics	OK
Chain: prerouting	Cancel	Src. Address List: 🗌 IP Ke Toen 🛛 🔻 🔺	Cancel	Action: accept	Cancel
Sro. Address:	Apply	Dat. Address List:	Apply	Log	Apply
Dst. Address:	Disable	Layer7 Protocol:	Disable	Log Prefix:	Disable
Protocol:	Comment		Comment		Comment
Src. Port:	Copy	Content:	Сору		Сору
Dat. Port:	Remove	Connection Bytes:	Remove		Remove
Any. Port:	- Reset Counters	Connection Hate:	Reset Counters		Reset Counters
in. Interface:	Reset Al Counters	Per Connection Classifier:	Reset Al Counters		Reset Al Counters
Out. Interface:		Src. MAL Address:			
In. Interface List:	•	Out. Bridge Port:			
Out. Interface List:	r				

Hình 8.6. Rule mangle chấp nhận cho danh sách địa chỉ IP không qua cân bằng tải

- Ngoài cách tạo danh sách địa chỉ IP như trên, ta còn có thể dùng cách gán Src. Address.
 - Bước 1: vào IP >> Firewall >> Tab Mangle, bấm nút + để thêm luật mới
 - Bước 2: trong New Mangle Rule, tab General
 - Chain: chọn prerouting
 - Src. Address: nhập vào lớp mạng hoặc một địa chỉ IP, một port dịch vụ cho phép bỏ qua qua cân bằng tải.



Hình 8.7. Tab general của màn hình New Mangle Rule

- Bước 3: tại tab Action, mục Action: chọn accept

New Mangle Rule	
General Advanced Extra Action Statistics	ОК
Action: accept	Cancel
Log	Apply
Log Prefix:	Disable
	Comment
	Сору
	Remove
	Reset Counters
	Reset All Counters
enabled	

Hình 8.8. Tab action của màn hình New Mangle Rule

- **Bước 4:** kéo lệnh prerouting vừa tạo lên đầu danh sách Mangle.

Firewall							
Filter Rules NAT Mangle	Raw Servic	e Ports Conne	ections Addre	ess Lists	Layer7 Pr	otocols	
+-~~~	Co Reset (Counters (O I	Reset All Count	ers	Find	all	₹
# Action	Chain	Src. Address	Dst. Address	Proto	Src. Port	Dst. Port	In. Inter. 🔻
0 📌 accept	prerouting	192.168.10.0					
2 mark routing	prerouting						
2 maik rouung	prerodurig						
•							•
3 items							

Hình 8.9. Màn hình tab Mangle của cửa sổ Firewall

BÀI 9. NAT

1. Giới thiệu:

NAT (Network Address Translation) là kỹ thuật cho phép một hay nhiều địa chỉ IP nội bộ được ánh xạ với một hay nhiều địa chỉ IP mạng ngoài. Các địa chỉ IP nội bộ có thể chạy các dịch vụ như web, mail hay đầu ghi lưu trữ camera,... hoặc chỉ đơn giản sử dụng Internet bình thường. NAT được thực hiện ở router biên, nơi kết nối giữa mạng LAN nội bộ và mạng Internet.

NAT giúp tiết kiệm được địa chỉ IP public IPv4 (với tổng địa chỉ khả dụng là hơn 4 tỉ) nhờ cơ chế xử lý của mình. Với NAT, hàng chục đến hàng trăm người dùng trong mạng có thể dùng "chung" một địa chỉ IP public.

Với router Mikrotik, ta cần quan tâm đến các hình thức NAT đó là NAT port, Hairpin NAT và NAT ra Internet

2. Mô hình mạng.

•••

3. Thực hành

3.1. NAT để truy cập internet

Hay còn gọi là Source NAT, nghĩa là đổi địa chỉ nguồn (source) từ local thành địa chỉ ip public trên cổng WAN để đi ra ngoài Internet. Hình thức NAT phổ biến và đơn giản nhất là NAT động masquerade. Gói tin sẽ được đổi địa chỉ nguồn và router sẽ đánh port nguồn ra ngoài theo một cổng "mặt nạ" nào đó mà router chưa được dùng đến. Khi gói tin đi vào thì router cũng sẽ theo cổng này để đưa đúng gói tin trở lại IP local như cũ.

Bước 1: vào IP >> DNS, nhập DNS là 8.8.8 và 8.8.4.4 hoặc 1.1.1.1. Check vào ô Allow Remote Request.

DNS Settings		
Servers:	<u>8.8.8.8</u> ♦	OK
	8.8.4.4	Cancel
Dynamic Servers:		Apply
Use DoH Server:		Static
	Verify DoH Certificate	Cache
	✔ Allow Remote Requests	
Max UDP Packet Size:	4096]
Query Server Timeout:	2.000 s	
Query Total Timeout:	10.000 s	
Max. Concurrent Queries:	100]
Max. Concurrent TCP Sessions:	20]
Cache Size:	2048 KiB	
Cache Max TTL:	7d 00:00:00]
Cache Used:	25 KiB]

Hình 9.1. Cửa sổ DNS Settings

- **Bước 2:** vào IP >> Firewall >> NAT. Bấm dấu + để thêm NAT mới.
- Bước 3: trong cửa sổ New NAT Rule, tại tab General
 - Chain: srcnat
 - Out. Interface: interface di ra internet

	New NAT Rule	
	General Advanced Extra Action	ОК
Chain: srcnat	Chain: srcnat 🔾 🗲	Cancel
	Src. Address:	Apply
	Dst. Address:	Disable
	Protocol:	Comment
	Src. Port:	Сору
Out. Interface là	Dst. Port:	Remove
internet	In Interface:	Reset Counters
	Out. Interface: ether9 T	Reset All Counters
	In. Interface List:	
	Out. Interface List:	
	Packet Mark:	
	Connection Mark:	
	Routing Mark:	
	· · · · · · · · · · · · · · · · · · ·	
	enabled	

Hình 9.2. Tab general của cửa số New NAT Rule

- Bước 4: tại tab Action, chọn Action là masquerade

New NAT Rule	
Advanced Extra Action Statistics	ОК
Action: masquerade	Cancel
	Apply
Log Prefix:	Disable
To Ports:	Comment
	Сору
	Remove
	Reset Counters
	Reset All Counters
enabled	



3.2. NAT port

NAT port là hình thức phổ biến để truy cập dịch vụ nội bộ từ bên ngoài Internet qua địa chỉ IP Public. Ta cần xác định địa chỉ IP public cần NAT trên cổng WAN, Địa chỉ IP local và port/protocol cần để NAT.

Giả sử cần NAT đầu ghi camera IP có địa chỉ 192.168.68.22, port là 8022 để có thể xem được từ bên ngoài Internet.

- Bước 1: vào IP >> Firewall >> NAT, bấm dấu + để thêm luật NAT mới. Trong màn hình NAT Rule, tab General.
 - Chain: dstnat
 - Dst. Address là địa chỉ IP tĩnh của đường WAN (trong trường hợp không có IP tĩnh có thể tham khảo cấu hình DDNS trong phần IP >> Cloud)
 - Protocol: 6 (tcp)
 - Dst. Port: port cần NAT từ internet (8080)



Hình 9.4. Tab general của cửa số New NAT Rule

Ngoài cách gán địa chỉ IP Public vào mục Dst. Address như trên, ta còn có thể dùng In. Interface để gán. Mục In. Interface chọn Interface kết nối với internet (pppoe-out1)

	New NAT Rule	
	General Advanced Extra Action Statistics	ОК
	Chain: dstnat	Cancel
	Src. Address:	Apply
	Dst. Address:	Disable
	Protocol: 6 (tcp) 🗧 🔺	Comment
Giao thức tcp, port	Src. Port:	Сору
dịch vụ 8080	Dst. Port:	Remove
	/in. Interface: ether9-pppoeout1 ∓▲	Reset Counters
	Out. Interface:	Reset All Counters
Truy cập từ internet vào	In. Interface List:	
công pppoe-out1	Out. Interface List:	
	Packet Mark:	
	Connection Mark:	
	Routing Mark:	
	Routing Table:	
	Connection Type:	
	enabled	

Hình 9.5. Tab general cửa sổ New NAT rule cách NAT bằng In. Interface

- Bước 2: cũng trong cửa số NAT Rule, chọn tab Action
 - Action: dst-nat
 - To Addresses: 192.168.1.254 (địa chỉ IP của đầu ghi)
 - To Ports: 8080



Hình 9.6. Tab action của màn hình NAT Rule

3.3. Hairpin NAT

Hairpin NAT được sử dụng khi người dùng muốn truy cập đến thiết bị bên trong mạng nội bộ bằng IP public.

- Bước 1: vào IP >> Firewall >> NAT, bấm dấu + để thêm rule NAT mới. Tại tab General,
 - Chain: srcnat
 - Src. Address: dải địa chỉ IP local cần truy cập đến thiết bị
 - Dst. Address: địa chỉ IP của thiết bị
 - Protocol: 6(tcp)
 - Dst. Port: port muốn truy cập đến
 - Out. Interface: Interface mà traffic đi ra.



Hình 9.7. Tab general của màn hình New NAT Rule

- Bước 2: vẫn trong cửa sổ New NAT Rule, tại tab Action, mục Action: chọn masquerade

New NAT Rule	
Advanced Extra Action Statistics	ОК
Action: masquerade	Cancel
Log	Apply
Log Prefix:	Disable
To Ports:	Comment
	Сору
	Remove
	Reset Counters
	Reset All Counters
enabled	

Hình 9.8. Tab action trong màn hình New NAT Rule

BÀI 10. DHCP SNOOPING

1. Mô hình mạng

2. Thực hành

. . . .

BÀI 11. Simple Queues

1. Giới thiệu

There are a lot of articles on the Internet devoted to speed limits and traffic dividing on MikroTik equipment, but almost all of them consider only Queue Tree, which requires deep understanding and are redundant in many tasks and can be replaced by Simple Queues.

Simplified queues - the mechanism of dividing the bandwidth of the channel and prioritizing traffic associated with a specific goal (target). Incoming and outgoing traffic is calculated relative to the target.

2. Mô hình mạng:

•••

3. Thực hành

3.1. Giới hạn băng thông cố định cho một địa chỉ IP

- Vào Queue, chọn tab Simple Queues. Bấm dấu + để thêm simple queue mới.
 - Name: đặt tên cho simple queue
 - Target: mục tiêu muốn giới hạn băng thông
 - Max Limit: giới hạn băng thông tối đa cho phép sử dụng.
 - Burst Limit: băng thông ban đầu khi chưa bị giới hạn
 - Burst threshold: băng thông khi người dùng cố tình sử dụng quá mức giới hạn sẽ bị giới hạn tiếp.
 - Burst time: thời gian bắt đầu giới hạn băng thông.



Hình 11.1. Tab general của bảng Simple Queue

3.2. Giới hạn băng thông cố định cho một lớp mạng

- Bước 1: vào Queues, chọn tab Queue Types. Trong danh sách, bấm kép vào mục pcq-download-default. Bấm nút copy để tạo Queue Type mới.
 - Type Name: đặt tên
 - Classifier: chọn Src. Address

	New Queue Type			⊟ ×
	Type Name:	Bang thong download		OK
	Kind:	pcq	₹	Cancel
	Rate:	10M	bits/s	Apply
	Queue Size:	50	КiB	Сору
	Total Queue Size:	2000	KiB	Remove
	Burst Rate:		bits/s	
	Burst Threshold:		•	
	Burst Time:	00:00:10		
	Classifier:	✓ Src. Address ✓ Dst. Address		
Từ trong mạng nội bộ đị		Src. Port Dst. Port		
ra ngoài nên mục	Src. Address Mask:	32		
Classifier ta chọn Src.	Dst. Address Mask:	32		
Address	Src. Address6 Mask:	128		
	Dst. Address6 Mask:	128		

Hình 11.2. New queue type giới hạn băng thông download

Bước 2: vẫn trong danh sách queue type, bấm kép vào mục pcq-upload-default.
 Bấm nút copy để tạo Queue Type mới.

	Queue Type <pcq-uplo< th=""><th>pad-default></th><th></th><th></th></pcq-uplo<>	pad-default>		
	Type Name:	Gioi han bang thong upload		ОК
	Kind:	pcq	∓	Cancel
Giới hạn bằng thông	Rate:	10M	bits/s	Apply
download là 10M	Queue Size:	50	KiB	Сору
	Total Queue Size:	2000	KiB	Remove
	Burst Rate:		▼ bits/s	
	Burst Threshold:		•	
	Burst Time:	00:00:10		
	Classifier:	Src. Address Dst. Address		
Từ trong mang nôi bô đi		Src. Port Dst. Port		
ra ngoài nên mục	Src. Address Mask:	32		
Classifier ta chon Src.	Dst. Address Mask:	32		
Address	Src. Address6 Mask:	128		
	Dst. Address6 Mask:	128		
	default			

Hình 11.3. New queue type giới hạn băng thông upload

- Bước 3:

New Simple Queue	
General Advanced Statistics Traffic Total Total Statistics	ОК
Name: Gioi han bang thong lop mang 192.168.1.0/24	Cancel
Target: 192.168.1.0/24 🗧	Apply
Dst.:	Disable
Target Upload Target Download	Comment
Max Limit: unlimited ∓ unlimited ∓ bits/s	Сору
	Remove
Burst Limit: unlimited	
Burst Threshold: unlimited	Reset Counters
Burst Time: 0 0 s	Reset All Counters
-▼· Time	Torch
enabled	



- Bước 4: vào tab Advance

Simple Queue <	gioi han bang thong:	>			
General Adv	anced Statistics	Traffic Total	Total Statistics		ОК
Packet Marks:				\$	Cancel
		Target Upload	Т	Farget Download	Apply
Limit At:	unlimited	₹	unlimited	₹ bits/s	Disable
Priority:	8		8		Comment
Bucket Size:	0.100		0.100	ratio	Сору
Queue Type:	Bang thong upload	₹	Bang thong downlo	oad ₹	Remove
Parent:	none			₹	Reset Counters
					Reset All Counters
					Torch
enabled					

Hình 11.5. Tab advanced của màn hình Simple queue

3.3. Giới hạn băng thông linh hoạt

- Bước 1: vào Queue → Queue Type → bấm kép vào pcq-download-default → copy.
- Bước 2: tạo queue có tên "PCQ-Download". Cài đặt như hình bên dưới và làm tương tự cho "PCQ-Upload"



Hình 11.6. Queue Type: "PCQ-Download"

Bước 3: bấm vào tab Simple Queues, bấm dấu + để tạo luật "Limit-All" như sau:

Queue List								
Simple Queues	Interface Queues	Queue Tree	Queue Types					
+ - •	× 🗆 🍸 (Reset Counter 	rs (O Reset Al	l Counters				Find
# Name		△ Target		Upload Max	Limit Down	nload Max Limit	Packet M	Marks 🔻
0 💻 Lim	it-All	0.0.0/0		140M	1401	1		
1 item (1 selected) 0 B (queued		0 packets que	eued			

Hình 11.7. Tab Simple Queues

Max Limit: tổng băng thông cho phép của đường truyền



Hình 11.9. Tab advanced

3.4. Giới hạn băng thông bằng script

- Sử dụng script sau để giới hạn băng thông cho một lớp mạng.

for e from 2 to 254 do={ /queue simple add name="IP-\$e"
target="192.168.1.\$e" max-limit=3M/3M burst-limit=40M/40M
burst-threshold=1M/1M burst-time=2/2s}

BÀI 12. VPN L2TP/IPSec

1. Giới thiệu:

•••

2. Mô hình mạng:

•••

- 3. Thực hành:
- Bước 1: khởi tạo dải IP cho VPN user. Vào IP >> Pool. Trong tab Pools, bấm dấu + để thêm pool mới.
 - Name: đặt tên cho dải IP
 - Address: 172.11.12.2-172.11.12.100

New IP Pool	
Name: Dai IP VPN L2TP	OK
Addresses: 172.11.12.2-172.11.12	Cancel
Next Pool: none 🛛 🗸 🔺	Apply
	Comment
	Сору
	Remove

Hình 12.1. New IP Pool cho dải IP VPN

- Bước 2: khởi tạo nhóm người dùng kết nối L2TP. Nhóm người dùng này chứa các thông tin về băng thông kết nối, loại IP ... Vào PPP, chọn Profiles, bấm dấu + để thêm profiles mới.
 - Name: tên nhóm
 - Local Address: địa chỉ IP gateway
 - **Remote Address:** pool đã tạo ở bước 1

New PPP Pr	ofile				
General	Protocols	Limits	Queue	Scripts	ОК
	Name: 🚺	hom VPI	N L2TP		Cancel
Local A	ddress: 1	92.168.1	0.1	₹ ▲	Apply
Remote A	ddress: D	ai IP VPI	N L2TP	₹ ▲	Comment
	Bridge:				Сору
Bridge Port	Priority:			-	Remove
Bridge Pa	th Cost:			•	L
Bridge I	Horizon:			•	
Incomin	ng Filter:				
Outgoin	ng Filter:			•	
Addre	ess List:			\$	
Interfa	ice List:			•	
DNS	Server: 1	92.168.1	0.1		
WINS	Server:			\$	
– Change T	CP MSS -				
Cino (🛾 yes 🖲	default			
- Use UPn	P				
Cino (yes 🕫	default			

Hình 12.2. Tab general của màn hình New PPP Profile

 Bước 3: giới hạn băng thông cho user VPN. Vào tab Limits, mục Rate Limit: nhập 20M/20M

PPP Profile <nhom l2tp="" vpn=""></nhom>	
General Protocols Limits Queue Scripts	OK
Session Timeout:	Cancel
Idle Timeout:	Apply
Rate Limit (rx/tx): 20M/20M	Comment
- Only One	Сору
⊂no ⊂yes	Remove

Hình 12.3. Tab Limits của màn hình New PPP Profile

- Sau khi thực hiện xong, tab Profiles của màn hình PPP như sau:

РРР						
Interface PPPoE Servers Secrets	Profiles Active	Connections	L2TP Se	crets		
+ - 6 7					F	ïnd
Name 🛆 Local Address	Remote Address	Bridge	Rate Limit	Only One		•
R Nhom VPN 192.168.10.1	Dai IP VPN L2TP	-	20M/20M	default		
* 🚱 default				default		
* \varTheta default-encr				default		
3 items						

Hình 12.4. Tab profiles của màn hình PPP

- Bước 4: tạo user VPN. Vẫn trong màn hình PPP, vào tab Secrets. Bấm dấu + để thêm user mới.
 - Name: tên đăng nhập
 - Password: mật khẩu
 - **Profile:** chọn nhóm VPN L2TP đã tạo trước.

New PPP Secret	
Name: vpnuser1	ОК
Password:	Cancel
Service: any	Apply
Caller ID:	Diaphla
Profile: Nhom VPN L2TP	Disable
Local Address:	Comment
Remote Address:	Сору
	Remove
Routes:	
Limit Bytes In:	
Limit Bytes Out:	
Last Logged Out:	
enabled	



- Bước 5: bật dịch vụ L2TP. Vẫn trong màn hình PPP, vào tab Interface, bấm nút L2TP Server,
 - o check vào ô Enabled.
 - o Use Ipsec: yes
 - Ipsec Secret: mã bí mật của IPsec

L2TP Server		
	Enabled	OK
Max MTU:	1450	Cancel
Max MRU:	1450	Apply
MRRU:	▼	
Keepalive Timeout:	30 🔺	
Default Profile:	default-encryption 🗧	
Max Sessions:	▼	
Authentication:	✓ mschap2 ✓ mschap1	
	✔ chap ✔ pap	
Use IPsec:	yes 🔻	
IPsec Secret:	*****	
Caller ID Type:	ip address 🗧	
	One Session Per Host	
	Allow Fast Path	

Hình 12.6. Bật dịch vụ L2TP