### **BAB IV**

## **RANCANGAN JARINGAN USULAN**

### 4.1. Jaringan Usulan

Pada bab ini penulis ingin mengajukan jaringan usulan dari apa yang penulis telah analisa sebelumnya setelah riset pada salah satu klien PT. Remala Abadi. Di dalam skripsi ini penulis ingin memberikan jaringan usulan agar kantor cabang dan pusat dapat saling berkomunikasi layaknya seperti dalam satu jaringan.

### 4.1.1. Topologi Jaringan

Dalam mengusulkan topologi jaringan yang akan diimplementasikan pada klien PT. Remala Abadi, penulis tidak akan merubah bentuk topologi yang sudah ada, hal ini karena bentuk topologi yang ada sekarang sudah sangat baik. Topologi jaringan kantor pusat dan cabang menggunakan topologi *star*. Penulis mengusulkan untuk menggunakan VPN (*Virtual Private Network*) untuk berkomunikasi atau pertukaran data antar kantor menjadi lebih aman.



Gambar IV.1. Topologi Jaringan Usulan

### 4.1.2. Skema Jaringan

Pada rancangan jaringan usulan ini, di sisi router kantor pusat yang sudah terkonfigurasi ip publik untuk akses internet 115.100.100.2 dan ip private 192.168.0.1 sebgai *gateway* LAN, maka ditambahkan sebuah konfigurasi baru dengan menambahkan IP *Tunnel* 10.10.10.1/30 pada router Mikrotik. Kemudian di sisi cabang yang sudah terkonfigurasi ip publik untuk internet 202.200.200.2 dan ip private 172.16.10.1 sebgai *gateway* LAN, maka ditambahkan sebuah *tunnel* dengan IP *Tunnel* 10.10.10.2/30. IP *Tunnel* ini nantinya yang akan menghubungkan komunikasi data dari kantor pusat dan kantor cabang melalui jaringan internet.



Gambar IV.2. Skema Jaringan Usulan

## 4.1.3. Keamanan Jaringan

Untuk keamanan jaringan yang digunakan pada implementasi kali ini kami menggunakan fitur kemanan dengan menggunakan tunneling, Metode tunneling membuat proses transfer data dari satu jaringan ke jaringan lain memanfaatkan jaringan internet secara terselubung (tunneling). Ketika paket berjalan menuju ke node tujuan, paket ini melalui suatu jalur yang disebut tunnel. Dan kami juga menerapkan *filter rule* pada *firewall* di mikrotik untuk membatasi akses ke server hanya dari ip *address* tertentu.

Dalam juga penulis membedakan jaringan pada kantor pusat dan kantor cabang. Dari sisi kantor pusat, penulis menggunakan Net ID 192.168.0.0/24 dan pada kantor cabang menggunakan Net ID 172.16.10.0/24. Selain itu juga tidak memberlakukan *mode bridge* dikarenakan Net ID Pusat dan Cabang yang berbeda serta menjauhi adanya *broadcast* virus dari cabang ke kantor pusat ataupun sebaliknya. Untuk itu routing dibuat terpisah, yaitu routing ke arah internet dan routing ke arah jaringan LAN kantor.

### 4.1.4. Rancangan Aplikasi

Untuk menggunakan jaringan VPN dengan menggunakan protokol EoIP maka harus dilakukan konfigurasi pada router kantor pusat dan router cabang salah satu klien PT. Remala Abadi. Tahapannya adalah sebagai berikut :

#### 1. Konfigurasi Router Kantor Pusat

Pada sisi router kantor pusat membuat eoip *tunnel*, menambahkan ip *point-to-point* dan menambahkan *routing* ke kantor cabang.

a. Membuat EoIP *Tunnel* 

Untuk membuat EoIP Tunnel langkah-langkahnya adalah sebagai berikut:

 Pada Winbox klik pada menu Interfaces, kemudian pilih tab Add (+) seperti berikut:

0	admin@192.168.0.1	l (MikroTik) - WinBox v5.1	1 on x86 (x8	6)			_			×
ю	Ca Safe Mode	]					✓ Hide	Pa	sswords	
	Interfaces 1									
	Wireless			Interface <	eoip-tunne	əl1>	•			×
	Bridge			General	Traffic		6	]	ок	
	PPP	Interface List		3	Name:	eoip+unnel1			Cance	
	Mesh 2	Interface Ethemet EoIP	<sup>o</sup> Tunnel II		Type:	FolP Tunnel			Analy	·
	IP P	+ - 🗸 🗙 🗂	Ţ		мтн.	1500		Ц	Афріу	-4
	IPv6	Name 🗡	Туре			05505			Disable	<u> </u>
	MPLS P	R ieoip-tunnel1 I	EoIP Tunne		L2 MTU:	65535			Comme	nt
	Routing			MAC	Address:	02:AC:78:CE:17:78			Сору	
	Queues				ARP:	enabled	₹	Ì	Remov	e
	Files			Local	Address:		•			-1
	Log		4	Remote	Address:	202,200,200,2		٦l	Iorch	
×	Radius		-	Т	unnel ID:	10		L		
B	Tools D					10				
/in	New Terminal			Keepalive	Interval:		•			
$\leq$	ISDN Channels									
00	KVM									
<u>te</u>	Make Supout.rif	•								
no	Manual	I item out of 3 (I selected)		enabled		nunning	slave			
R	Exit		I C		_	- Comming	Sidiro		_	

## Gambar IV.3 Membuat EoIP Tunnel

- 2) Kemudian isi kolom **Name** dengan **eoip-tunnel1**.
- Pada Remote Address isikan IP *Public* lawan. Dalam hal ini adalah IP Publik kantor cabang.
- 4) Pada Tunnel ID isikan identitas *tunnel* yang akan dibuat. Yaitu 10. *Tunnel* ID ini harus sama dari kedua sisi router. Jika berbeda maka kedua kota tersebut tidak bisa saling berkomunikasi dalam satu jaringan.

# b. Menambahkan IP Address EoIP Tunnel

EoIP *tunnel Address* adalah alamat IP *Address* yang harus dikonfigurasi menjadi *Address tunnel*. Syarat IP *Address eoip-tunnel* ini adalah IP harus satu *network* dengan *eoip-tunnel Address* yang dikonfigurasikan di sisi Cabang.

	admin@192.168.0.1	l (MikroTik) - WinBox v5	.11 on x86 (x86)		_		×
¢	Cafe Mode			•	Hide F	asswords	
in Box	Safe Mode       Interfaces       Wireless       Bridge       PPP       Mesh       IP       PV6       MPLS       Routing       System       Queues       Files       Log       Radius       Tools       New Terminal	Terminal Wireless Tables Interfaces Nstreme Di ARP Accounting Addresses 2 DHCP Client DHCP Relay DHCP Server DNS Firewall Hotspot IPsec Neidbhors	Addres List Addres 2 10.10.10.1/30 Addres 2 10.10.10.1/30 Addres 2 10.10.10.1/30 Cancel Interface: eoip+unnel T Apply 5 Disable Comment Copy Remove enabled		ffer	Passwords Wireless Si c   Tx Dro	1000per 28 Rx [
S W	ISDN Channels	Packing	determine the selected se	•			
0 U	KVM Malas Sussait of	Pool					
Route	Manual	SNMP					
		Jervices					

## Gambar IV.4. Menambahkan EoIP Tunnel Address

Langkah-langkah untuk Menambahkan EoIP Tunnel Address yaitu:

- 1) Klik Tab **IP** lalu Pilih **Addresses**
- 2) Isikan Address 10.10.10.1/30
- 3) Pilih **Interface** eoip-tunnel1
- 4) Lalu **Apply** dan **OK**.
- c. Membuat Routing ke Kantor Cabang

Agar koneksi antar lokasi dapat terjadi, kita harus melakukan routing ke kantor cabang seperti berikut:

- 1) Pada Tab **IP** pilih **Routes**
- 2) Pada Tab General kita isikan dst-Address 172.16.10.0/24
- 3) Lalu pada Gateway eoip-tunnel cabang isikan 10.10.10.2
- 4) Kemudian isikan klik **Apply** dan **OK**

🔘 admin@192.168.0.1	(MikroTik) - WinBox v	/5.11 on x86 (x86)			
ら 🖓 🛛 Safe Mode					
Interfaces					
Wireless					
Bridge					
PPP	Route List				
Mesh		Deute <172.10.10.0			
IP 1 D	ARP		U/24>	:	
IPv6 D	Accounting	Gerieral Attribute	15	<u>'</u>	ок
MPLS N	Addresses	Dst. Address:	172.16.10.0/24	- L	Cancel
Routing 1	DHCP Client	3 Gateway:	10.10.10.2 Freachable eoip+tunnel1	÷ 🛓	Apply
System	DHCP Relay			_	
		Charle Cataway		-	Dieable
Queues	DHCP Server	Check Gateway:		•	Disable
Queues Files	DHCP Server DNS	Check Gateway: Type:	unicast a	F	Disable Comment
Queues Files Log	DHCP Server DNS Firewall	Check Gateway: Type: Distance:	unicast	▼   F	Disable Comment Copy
Queues Files Log Radius	DHCP Server DNS Firewall Hotspot	Check Gateway: Type: Distance:	unicast (1	▼   ■	Disable Comment Copy Remove
Queues Files Log Radius Tools	DHCP Server DNS Firewall Hotspot IPsec	Check Gateway: Type: Distance: Scope:	unicast (1 1 30		Disable Comment Copy Remove
Queues Files Log Radius Tools N New Terminal	DHCP Server DNS Firewall Hotspot IPsec Neighbors	Check Gateway: Type: Distance: Scope: Target Scope:	unicast 4	<ul> <li>▼</li> <li>■</li> </ul>	Disable Comment Copy Remove
Queues Files Log Radius Tools New Terminal ISDN Channels	DHCP Server DNS Firewall Hotspot IPsec Neighbors Packing	Check Gateway: Type: Distance: Scope: Target Scope: Routing Mark:	unicast 4		Disable Comment Copy Remove
Queues Files Log Radius Tools N New Terminal ISDN Channels KVM	DHCP Server DNS Firewall Hotspot IPsec Neighbors Packing Pool	Check Gateway: Type: Distance: Scope: Target Scope: Routing Mark: Pref. Source:	unicast 4		Disable Comment Copy Remove
Queues Files Log Radius Tools N New Terminal ISDN Channels KVM Make Supout.rf	DHCP Server DNS Firewall Hotspot IPsec Neighbors Packing Pool Routes <b>2</b>	Check Gateway: Type: Distance: Scope: Target Scope: Routing Mark: Pref. Source:	unicast 4		Comment Copy Remove
Queues Files Log Radius Tools P New Terminal ISDN Channels KV/M Make Supout.nf Manual	DHCP Server DNS Firewall Hotspot IPsec Neighbors Packing Paol Routes SNMP	Check Gateway: Type: Distance: Scope: Target Scope: Routing Mark: Pref. Source:	unicast         1           1         .           30         .           10         .           .         .		Disable Comment Copy Remove

Gambar IV.5. Membuat Routing ke arah kantor cabang

### 2. Konfigurasi Router Cabang

Untuk dapat memanfaatkan fitur EoIP *Tunnel*. Selain dari sisi kantor pusat, maka router Mikrotik yang berada di kantor cabang juga harus di konfigurasi sebagai berikut:

1) Konfigurasi Interface EoIP *Tunnel* cabang

Untuk membuat EoIP Tunnel langkah-langkahnya adalah sebagai berikut:

- a. Pada Winbox klik pada menu Interfaces, kemudian pilih tab Add (+)
- b. Kemudian centang isi kolom Name dengan eoip tunnel1
- c. Pada Remote Address isikan IP *Public* lawan. Dalam hal ini adalah IP *Public* kantor pusat.
- d. Pada Tunnel ID disini isikan identitas *tunnel* yang akan dibuat. Yaitu 10.
   *Tunnel* ID ini harus sama dari kedua sisi router. Jika berbeda maka kedua kota tersebut tidak bisa saling berkomunikasi dalam satu jaringan.

ds 📕 🛅
ind
Drops 🔽
0
0
+

# Gambar IV.6. Membuat interface EoIP Tunnel pada Router Cabang

$\bigcirc$	admin@202.200.20	0.2 (MikroTik) - WinBox	v5.11	on x86 (x86)		—	
ø	Cafe Mode					Hide Pa	asswords 🔳 🛅
	Interfaces Wireless						
	Bridge	Interface List					
	PPP	Interface Ethernet 3	Add	ress List		:	
	Mesh		+	- • × 🗅 🍸	Find		Find
	IP <b>1</b> ⊵	Ann		Address <10.10.10.2/30>		Tx Pac.	Rx Pac 🔽
	IPv6 ₿			Address: 10.10.10.2/30	_ 6 ок	5	0 0
	MPLS D	DHCP Client		Network: 10.10.10.0	Cancel		
	Routing D	DHCP Belay		Interface: eoip-tunnel1	▼ 5 Apply		
	System 🗅	DHCP Server	4		Disable		
	Queues	DNS			Disable		
	Files	Firewall			Comment		
×	Log	Hotspot			Сору		
B	Radius	IPsec			Remove		
Vin	Tools D	Neighbors		enabled			
>	New Terminal	Packing					
ő	ISDN Channels	Pool	3 ite	ms (1 selected)			+
E	KVM	Routes	1				
OU	Make Supout.nt	SNMP					
R	Manual	Services					

# 2) Menambahkan IP Address EoIP Tunnel

Gambar IV.7. Memberikan EoIP Tunnel Address kantor cabang

Langkah-langkah untuk Menambahkan EoIP Tunnel Address yaitu:

- a. Klik Tab IP lalu Pilih Addresses
- b. Isikan Address 10.10.10.2/30
- c. Pilih Interface eoip-tunnel1
- d. Lalu **Apply** dan **OK**.
- 3) Membuat Routing ke kantor pusat

Sadmin@202.200.200 🕲	0.2 (MikroTik) - WinBox	c v5.11 on x86 (x86	5)					
い 🖓 Safe Mode								
Interfaces								
Wireless	Paula List							
Bridge	Route List							
PPP	Nexthops F	Nexthops Fulles VRF						
Mesh	+ - < ×	General Anthur	0/24/				r	
IP 🌓	ARP	Attribute	es					<b>D</b> OK
IPv6 🗈	Accounting 3	Dst. Address:	192.168.0.0/24	1				Cancel
MPLS D	Addresses	Gateway:	10.10.10.1	1	reachable eoip-tunnel1		<b>\$</b>	4 Apply
Routing D	DHCP Client	Chaols Catoway						Disable
System D	DHCP Relay	check Galeway.					· · ·	Comment
Queues	DHCP Server	lype:	unicast				•	Comment
Files	DNS	Distance:	1				<b></b>	Сору
Log	Firewall	Scope:	30					Remove
Radius	Hotspot	Target Seener	10					
Tools D	IPsec	Target Scope.						
New Terminal	Neighbors	Routing Mark:						
ISDN Channels	Packing	Pref. Source:					•	
KVM	Pool							
Make Supout.rif	Routes 2							
Manual	SNMP							
Exit	Services							1

# Gambar IV.8. Membuat Routing ke arah kantor pusat

- a. Pada Tab **IP** pilih **Routes**
- b. Pada Tab General kita isikan dst-Address 172.16.10.0/24
- c. Lalu pada Gateway eoip-tunnel cabang isikan 10.10.10.2
- d. Kemudian isikan klik **Apply** dan **OK**

Konfigurasi EoIP Tunnel di Mikrotik pada kedua kantor pusat dan kantor

cabang telah kita buat. Sekarang kita akan masuk ke tahap pengujian jaringan.

#### 4.1.5. Manajemen Jaringan

Setelah penulis menganalisa sistem jaringan berjalan pada salah satu klien PT. Remala Abadi, maka penulis mengusulkan sebuah jaringan menggunakan VPN (*Virtual Private Network*) dengan menggunakan protokol *Ethernet Over IP* (EoIP) untuk menghubungkan kantor pusat dengan cabang. Dan di fungsikan untuk menjembatani antara kantor pusat dan kantor cabang dengan memanfaatkan koneksi *internet* yang dimiliki tersebut.

Dengan menggunakan *router* Mikrotik yang sudah ada, kemudian dikonfigurasi untuk menerapkan sistem jaringan VPN baik disisi kantor pusat maupun kantor cabang. Dengan ini antara kantor pusat, kantor cabang dan *remote client* akan lebih mudah untuk melakukan komunikasi, pengiriman data perusahaan serta memonitoring jaringan akan lebih aman.

### 4.2. Pengujian Jaringan

Pengujian jaringan dilakukan di awal sebelum EoIP Tunnel dibuat dan sesudah EoIP Tunnel dibuat pada konfigurasi diatas. Hasil akhir pengujian yang dilakukan adalah dengan dengan melakukan *traceroute* atau lompatan dari *host* satu ke *host* lainnya. Pengujian dilakukan pada sisi user yang berada di kantor cabang dan kantor pusat.

### 4.2.1. Pengujian Jaringan Awal

Pada pengujian Awal. Mikrotik harus dapat Akses ke Internet. Pengujian ini dilakukan ketika fitur NAT dan DNS sudah diaktifkan pada Mikrotik. Pengujian dilakukan dengan tes ping ke IP Publik milik kantor cabang dan kantor pusat seperti gambar berikut

C:\Windows\system32\cmd.exe	×
Microsoft Windows [Version 6.1.7601] Copyright (c) 2009 Microsoft Corporation. All rights reserved	-
C:\Users\E6410>ping 202.200.200.2	
Pinging 202.200.200.2 with 32 bytes of data: Reply from 202.200.200.2: bytes=32 time<1ms TTL=64 Reply from 202.200.200.2: bytes=32 time<1ms TTL=64 Reply from 202.200.200.2: bytes=32 time<1ms TTL=64 Reply from 202.200.200.2: bytes=32 time<1ms TTL=64	
Ping statistics for 202.200.200.2: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = Oms, Maximum = Oms, Average = Oms	
C:\Users\E6410>	
	·

Gambar IV.9. Tes ping ke arah IP publik kantor cabang

📓 🕢 anto : bash	$\odot$	$\otimes$
File Edit View Scrollback Bookmarks Settings Help		
<pre>[anto@vm ~]\$ ping 115.100.100.2 PING 115.100.100.2 (115.100.100.2) 56(84) bytes of data. 64 bytes from 115.100.100.2: icmp_seq=1 ttl=64 time=1.50 ms 64 bytes from 115.100.100.2: icmp_seq=3 ttl=64 time=0.690 ms 64 bytes from 115.100.100.2: icmp_seq=3 ttl=64 time=0.459 ms 64 bytes from 115.100.100.2: icmp_seq=4 ttl=64 time=0.535 ms 64 bytes from 115.100.100.2: icmp_seq=5 ttl=64 time=0.512 ms 64 bytes from 115.100.100.2: icmp_seq=6 ttl=64 time=0.491 ms 64 bytes from 115.100.100.2: icmp_seq=7 ttl=64 time=0.491 ms 64 bytes from 115.100.100.2: icmp_seq=8 ttl=64 time=0.457 ms 64 bytes from 115.100.100.2: icmp_seq=9 ttl=64 time=0.457 ms 64 bytes from 115.100.100.2: icmp_seq=9 ttl=64 time=0.616 ms 64 bytes from 115.100.100.2: icmp_seq=9 ttl=64 time=0.521 ms ^c  115.100.100.2 ping statistics 10 packets transmitted, 10 received, 0% packet loss, time 9055ms rtt min/avg/max/mdev = 0.457/0.630/1.501/0.299 ms [anto@vm ~]\$</pre>		
anto : bash		~

Gambar IV.10. Tes ping ke IP Publik kantor pusat

C:\Windows\system32\cmd.exe	8
C:\Users\E6410> C:\Users\E6410> C:\Users\E6410>ping 172.16.10.1	*
Pinging 172.16.10.1 with 32 bytes of data: Reply from 115.100.100.1: Destination net unreachable. Reply from 115.100.100.1: Destination net unreachable. Reply from 115.100.100.1: Destination net unreachable. Reply from 115.100.100.1: Destination net unreachable.	
Ping statistics for 172.16.10.1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),	
C:\Users\E6410>tracert -d 172.16.10.1	
Tracing route to 172.16.10.1 over a maximum of 30 hops	
1 <1 ms <1 ms <1 ms 192.168.0.1 2 115.100.100.1 reports: Destination net unreachable.	
Trace complete.	
C:\Users\E6410>	-
< III	► ad

Gambar IV.11. Tes routing ke kantor cabang

📕 ftp.p	pcapng						
File E	édit View G	o Capture Ana	lyze Statistics Teleph	ony Wireless	Tools Help		
4.1	0 🔘 🎴	📠 🔀 🖸 🔍 ४	⇔ ⇒ ≅ T 🛓 🖬	. 0	Q. #		
ftp							kpression +
No.	Time	Source	Destination	Protocol Le	ngth Info		*
260	3 16.086823	172.16.26.104	172.16.26.38	FTP	68 Request: STOR tes.txt		
260	38 16.087454	172.16.26.38	172.16.26.104	FTP	76 Response: 150 Ok to send data.		
261	4 16.110559	172.16.26.38	172.16.26.104	FTP	78 Response: 226 Transfer complete.		
261	6 16.110925	172.16.26.104	172.16.26.38	FTP	83 Request: MDTM 20170717120817 tes.txt		
261	7 16.111174	172.16.26.38	172.16.26.104	FTP	87 Response: 213 File modification time set.		
261	.8 16.112262	172.16.26.104	172.16.26.38	FTP	62 Request: TYPE A		
261	.9 16.112563	172.16.26.38	172.16.26.104	FTP	84 Response: 200 Switching to ASCII mode.		
262	.0 16.113005	172.16.26.104	172.16.26.38	FTP	60 Request: PASV		
262	1 16.113380	172.16.26.38	172.16.26.104	FTP	105 Response: 227 Entering Passive Mode (172,16,26,38,11)	1,115).	
262	.2 16.113542	172.16.26.104	172.16.26.38	FTP	63 Request: LIST -a		
262	.7 16.114594	172.16.26.38	172.16.26.104	FTP	93 Response: 150 Here comes the directory listing.		
265	4 16.115392	172.16.26.38	172.16.26.104	FTP	78 Response: 226 Directory send UK.		
890	3 46.365515	172.16.26.104	172.16.26.38	FTP	62 Request: TYPE 1		
890	4 46.366111	172.16.26.50	172.16.26.104	FTP	85 Response: 200 Switching to Binary mode.		
<pre>▷ Tran ▷ File</pre>	ısmission Co ≞ Transfer P	ntrol Protocol, rotocol (FTP)	Src Port: 49410, D	st Port: 21,	, Seq: 20, Ack: 92, Len: 14		
0000 0010 0020 0030 0040	08 00 27 fa 00 36 0f 49 1a 26 c1 02 00 fd 9c 0a 78 74 0d 0a	c5 c6 c0 cb 3 40 00 80 06 5 00 15 8a 67 00 00 53 54	38 42 c2 bb 08 00 45 5e ca ac 10 1a 68 ac 75 23 68 ab 80 39 5¢ 4f 52 20 74 65 73 2r	00 10 .6.1g 18 .& 274 xt			
07	Frame (frame	-) 68 hytes				Packets: 15594 · Disolaved: 24 (0.2%) · Load time: 0:0.374	Profile: Default

# Gambar IV.12. Tes transfer data dengan Wireshark

Pada pengujian jaringan awal dari LAN dilakukan *traceroute* ke arah IP LAN kantor cabang. Hasil dari gambar di atas adalah terdapat pesan "*Destination host unreachable*" artinya *host* tujuan tidak dikenal. Kantor cabang dan kantor pusat tidak dapat melakukan resource kearah kedua jaringan yang ada dikarenakan tidak adanya routing yang mengarah ke LAN kantor cabang, maka dari itu dibuat konfigurasi seperti di Sub bab 4.1.4. agar jaringan yang berada di belakang mikrotik dapat saling terhubung layaknya satu jaringan.

### 4.2.2. Pengujian Jaringan Akhir

Pada hasil akhir pengujian jaringan ini dilakukan berdasarkan tes ping dan *traceroute* ke arah kantor pusat dan cabang untuk mengetahui bahwa jalur data yang dikirim baik dari sisi pusat ke cabang atau sebaliknya adalah jalur melalui *gateway eoip tunnel* yang sudah dikonfigurasi sebelumnya.

Applications Pl	aces System 🥹 🍙 🗾 🛛 Mon Jul 25, 10:13 PM user 1 😭 🎪	<b>P</b>
and the second s	and the second se	
100	🗉 user1@localhost:~ _	D X
	File Edit View Search Terminal Help	
Computer	inet6 addr: ::1/128 Scope:Host	1
-	UP LOOPBACK RUNNING MTU:65536 Metric:1	
ŝ	RX packets:8 errors:0 dropped:0 overruns:0 trame:0	
user11s Home	collisions:0 txqueuelen:0	
9119116 71960	RX bytes:480 (480.0 b) TX bytes:480 (480.0 b)	
	[USEFI@localnost ~]\$ ping 192.108.0.10 PTNG 192 168 0 10 (192 168 0 10) 56(84) bytes of data	
Trash	64 bytes from 192.168.0.10: icmp seq=1 ttl=126 time=2.53 ms	
	64 bytes from 192.168.0.10: icmp_seq=2 ttl=126 time=3.76 ms	
and the second second	64 bytes from 192.168.0.10: icmp_seq=3 ttl=126 time=2.99 ms	
and the second se	64 bytes from 192.168.0.10: icmp_seq=4 (((=126 (ime=3.19 ms	
Anna	64 bytes from 192.168.0.10: icmp_seq=6 ttl=126 time=2.72 ms	
and the second se	64 bytes from 192.168.0.10: icmp_seq=7 ttl=126 time=2.84 ms	5
and the second se	64 bytes from 192.168.0.10: icmp_seq=8 ttl=126 time=2.84 ms	
and the second se	64 bytes from 192.168.0.10: 1cmp_seq=9 ttl=126 time=3.61 ms 64 bytes from 192.168.0.10: icmp_seq=10 ttl=126 time=2.85 ms	
and a second sec	^C	
and the second se	192.168.0.10 ping statistics	- 1
and the second se	10 packets transmitted, 10 received, 0% packet loss, time 10013ms	
	rtt min/avg/max/mdev = 2.531/3.044/3.760/0.366 ms	
	Transi Yékong Jan	
5 19 (BE) 198	Contraction and the second second second second	
user renocarnos	3L	10 10 10 10 10 10 10 10 10 10 10 10 10 1

Gambar IV.13 Pengujian dengan Ping ke arah LAN kantor pusat

C:\Windows\system32\cmd.exe
C:\Users\E6410>ping 172.16.10.100
Pinging 172.16.10.100 with 32 bytes of data: Reply from 172.16.10.100 bytes=32 time=1ms TTL=61
Reply from 172.16.10.100: bytes=32 time=2ms TIL=61
Reply from 172.16.10.100: bytes=32 time=2ms IIL-61 Reply from 172.16.10.100: bytes=32 time=2ms IIL=61
Ping statistics for 172.16.10.100: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 1ms, Maximum = 2ms, Average = 1ms
C:\Users\E6410>tracert -d 172.16.10.100
Tracing route to 172.16.10.100 over a maximum of 30 hops
1 <1 ms <1 ms <1 ms 192.168.0.1
2 1 MS 1 MS 1 MS 202.200.200.2 3 2 MS 2 MS 2 MS 172.16.10.100
Trace complete.
C:\Users\E6410>
· · · · · · · · · · · · · · · · · · ·

Gambar IV.14 Pengujian dengan traceroute

🚄 smb eoip.pcapng						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
📶 🔳 🖉 📵 📙 🛅 🎗 🖶 🗢 🕾 🗑 👲 🚍 🗐 🍳 🔍 🕮						
Apply a display filter <ct< td=""><td>trl-/&gt;</td><td></td><td>2</td><td></td><td></td><td>Expression +</td></ct<>	trl-/>		2			Expression +
No. Time Sou	Ince	Destination	Protocol Leng	th Infe		A
135 64,200678 192	2.168.137.1	172.16.29.10	FTP	68 Request: STOR tes.txt		
136 64.201056 192	2.168.137.1	172.16.29.10	TCP	66 49365 → 10290 [SYN] Seg=0 Win=8192 Len=0 MSS=1460 W	S=256 SACK PERM=1	
137 64.202793 172	2.16.29.10	192.168.137.1	TCP	66 10290 → 49365 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=	0 MSS=1368 SACK_PERM=1 WS=64	
138 64.202861 192	2.168.137.1	172.16.29.10	TCP	54 49365 → 10290 [ACK] Seq=1 Ack=1 Win=65536 Len=0		
139 64.203404 192	2.168.137.1	172.16.29.10	TCP	54 [TCP Window Update] 49365 → 10290 [ACK] Seq=1 Ack=1	Win=4194304 Len=0	
140 64.204472 172	2.16.29.10	192.168.137.1	FTP	76 Response: 150 Ok to send data.		
141 64.204688 192	2.168.137.1	172.16.29.10	FTP-D	60 FTP Data: 6 bytes		
142 64.204715 192	2.168.137.1	172.16.29.10	TCP	54 49365 → 10290 [FIN, ACK] Seq=7 Ack=1 Win=4194304 Let	n=0	
143 64.206026 172	2.16.29.10	192.168.137.1	TCP	54 10290 → 49365 [ACK] Seq=1 Ack=7 Win=14656 Len=0		
144 64.206263 172	2.16.29.10	192.168.137.1	TCP	54 10290 → 49365 [FIN, ACK] Seq=1 Ack=8 Win=14656 Len=	0	
145 64.206290 192	2.168.137.1	1/2.16.29.10	TCP	54 49365 → 10290 [ACK] Seq=8 AcK=2 Win=4194304 Len=0		
140 04.20/510 1/2	2.10.29.10	192.100.157.1	TCD	76 Response: 226 Transfer complete.		
147 64.207547 192	2.100.157.1	172.16.29.10	ETD	54 49557 + 21 [ACK] SEq=75 ACK=555 Win=256 Len=0		
140 64 208003 172	2 16 29 10	192 168 137 1	FTD	87 Decourse: 213 File modification time set		
150 64 200763 102	2 168 137 1	172 16 29 10	FTD	62 Request: TVDE A		
151 64,210917 172	2.16.29.10	192.168.137.1	FTP	84 Response: 200 Switching to ASCII mode.		Ξ.
h farm data ta hata		hites of hites an		hite) an interfere A		
P Frame 135: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface 0 Frame 135: 68 bytes on Single (544 bits), 68 bytes captured (544 bits)						
P Ethernet II, Src: McScompLe0154:09 (00:00/27/00:54:09), UST: PCSCOMPL_1917a105 (00:00/27/1917a105)						
Transfer House Televist for the second						
4 File Transfer Protocol (FTP)						
<pre>4 STOR tes.txt\r\n</pre>	1					
Request comma	and: STOR					
Request arg: tes.txt						
0000 08 00 27 f9 fd	b5 08 00 27	00 54 89 08 00 45 0	a <sup>.</sup>	1.TE.		
0010 00 36 06 15 40	00 80 06 el	e8 c0 a8 89 01 ac 10	.6@			
0020 1d 0a c0 b9 00	15 37 e6 ce	cd e7 2f 72 bf 50 1	3	/r.P.		
0030 01 00 9e 07 00	00 53 54 4f	52 20 74 65 73 2e 74	4ST	OR tes.t		
0040 78 74 0d 0a			xt			
0.7						
💛 🗹 smb eoip					Packets: 183 · Displayed: 183 (100.0%) · Load time: 0:0.15	Profile: Default

Gambar IV.15. Pengujian dengan wireshark

Dari gambar di atas dapat dijelaskan bahwa jalur yang dilewati untuk mencapai ke arah jaringan lokal (LAN) yang ada di cabang dengan IP Address 172.16.10.100 adalah melalui IP Address 192.168.0.1 yaitu IP Address Gateway LAN di kantor pusat. Kemudian diteruskan melalui IP Gateway Tunnel kantor cabang yaitu 10.10.10.2 dan terakhir sampai di IP 172.16.10.100.

Ketika melakukan *tracerroute* ke *host* tujuan maka IP *Public* yang seharusnya menjadi *gateway* untuk berkomunikasi ke internet tidak akan terdeteksi sebab IP Address yang diminta dari user adalah bagian dari jaringan LAN kantor cabang dengan *gateway eoip-tunnel address* yang sudah di konfigurasikan.

Sehingga data yang dilewati untuk mencapai host tertentu yang ada di cabang seakan-akan tidak melewati jalur internet.



Gambar IV.16 Tes folder sharing kearah kantor Cabang

Setelah terjadinya koneksi intranet yang ada di kantor pusat dan kantor cabang , maka kita dapat berbagi akses dan kemudahan untuk membentuk satu jaringan berskala *Wide Area Network* (WAN) sehingga seluruh staff dapat memanfaatkan *resource* seluruh jaringan yang ada untuk terhubung ke jaringan LAN yang ada di kantor pusat dan cabang tanpa harus membuat suatu autentifikasi user terlebih dahulu. Untuk hak akses folder dapat diatur oleh sistem administrator sehingga tidak semua user dapat mengakses folder yang bukan pada divisi terkait.