In-depth Analysis for L-2 Frames and Tunnel Protocols using GNS3 dan Wireshark

(Ethernet, VLAN 802.1Q, QinQ, PPPoE, EoIP, L2TP, EoIP over L2TP, VLAN over EoIP)

Yohanes Gunawan Yusuf

MikroTik Certified Trainer

1

Topics of Discussion

1. We are going to look and learn Ethernet and L-2 Frames
2. Analyse L2 frames dan Tunnels using GNS3 and Wireshark, such as:
   - Ethernet
   - VLAN (802.1Q)
   - VLAN Tunnel (QinQ)
   - PPPoE
   - EoIP Tunnel
   - ARP
   - L2TP VPN Tunnel
   - VLAN over EOIP Tunnel
   - Demo and Discussion

2

UBAYA
UNIVERSITAS SURABAYA

About Me

(yohanesgunawan@staff.ubaya.ac.id)

- My Name is Yohanes Gunawan Yusuf, form Indonesia. I am a full time lecturer of University of Surabaya (Ubaya).
- I have learn and teach in Department of Electrical Enginering (EE) and IT since 1986.
- MikroTik Certified Trainer (TR0639) and Mikrotik Academy Trainer (ACTR0244) for EUTC with certifications: MTCNA, MTCRE, MTCUME, MTCWE, MTCTCE and MTCINE

EUTC
Elektro Ubaya Training Center

3

UBAYA
UNIVERSITAS SURABAYA

University of Surabaya (Ubaya)

4

UBAYA
UNIVERSITAS SURABAYA

Universitas Surabaya (Ubaya)




5

UBAYA
UNIVERSITAS SURABAYA

Elektro Ubaya

(te.ubaya.ac.id)

EUTC
Elektro Ubaya Training Center

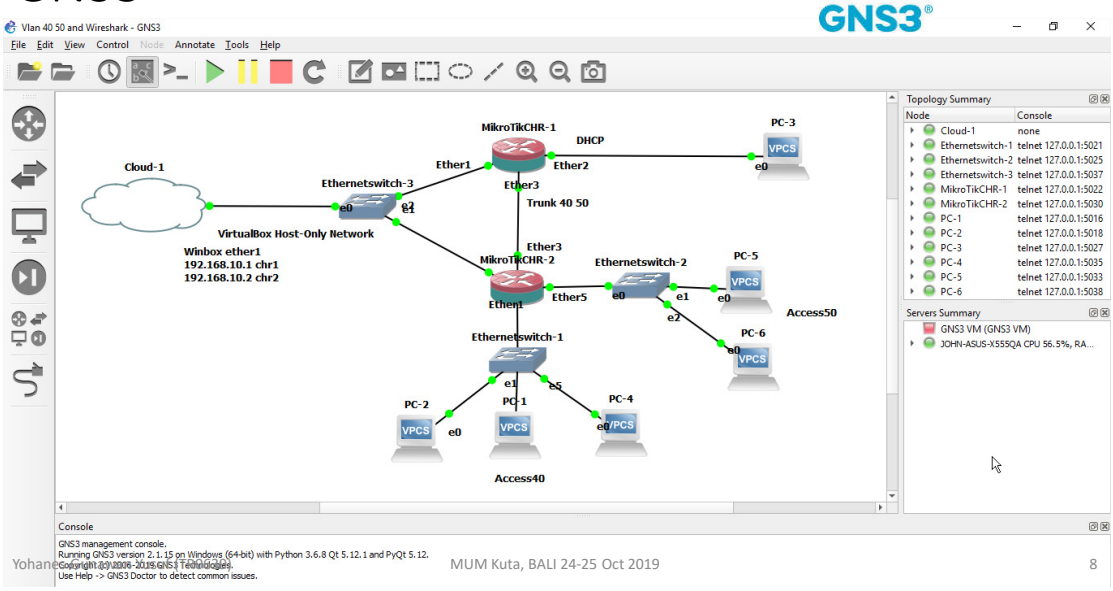
6

Akreditasi A

- Universitas Surabaya (Ubaya) ,terakreditasi A dari BANPT dan merupakan Perguruan Tinggi Swasta tebaik (ranking 1) di Jawa Timur
- Program Studi Teknik Elektro Ubaya juga terakreditasi A

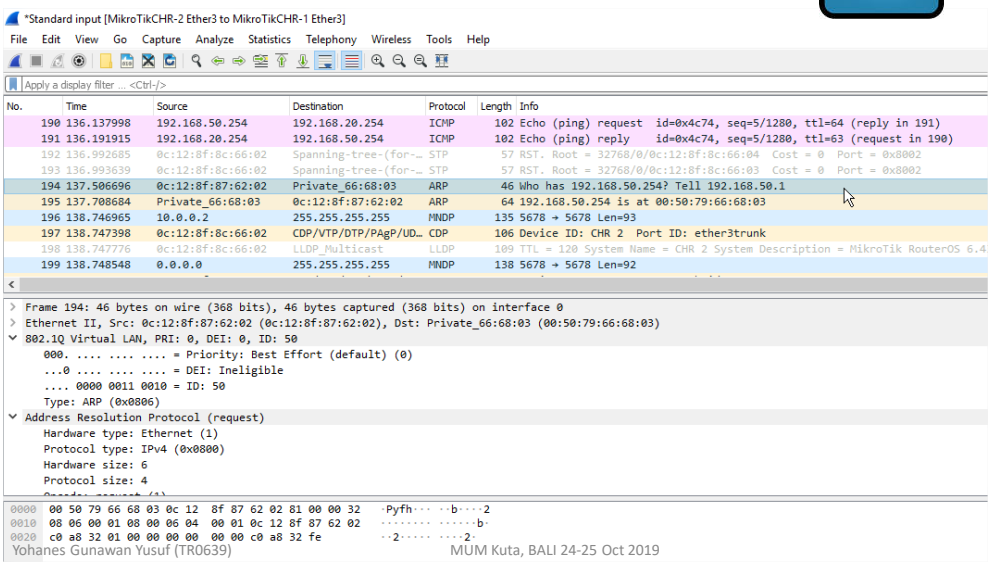
7

GNS3



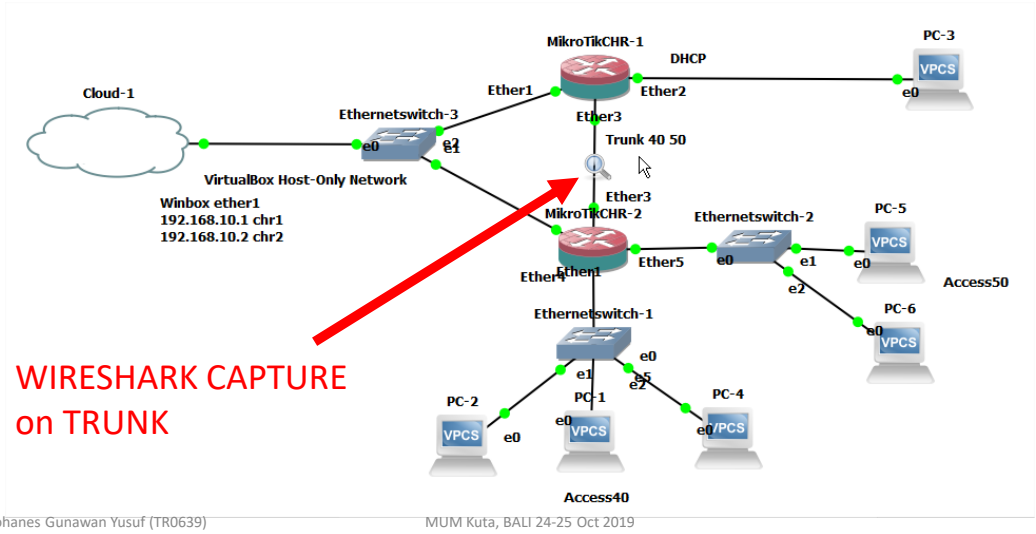
8

Wireshark



9

GNS3 and Wireshark



10

Frames to be analysed

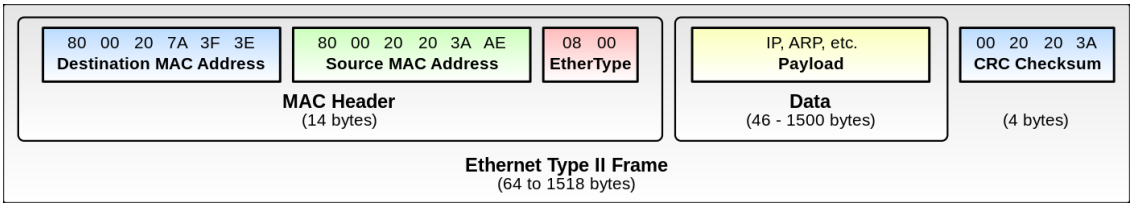
- Ethernet Standard
- VLAN (802.1Q)
- VLAN in VLAN (QinQ)
- PPPoE
- EoIP
- L2TP
- Tunnel in Tunnel
  (EoIP o L2TP and VLAN o EoIP)

11

Ethernet Standard (Type II) Frame

12

Ethernet Frame (Standard Type II)



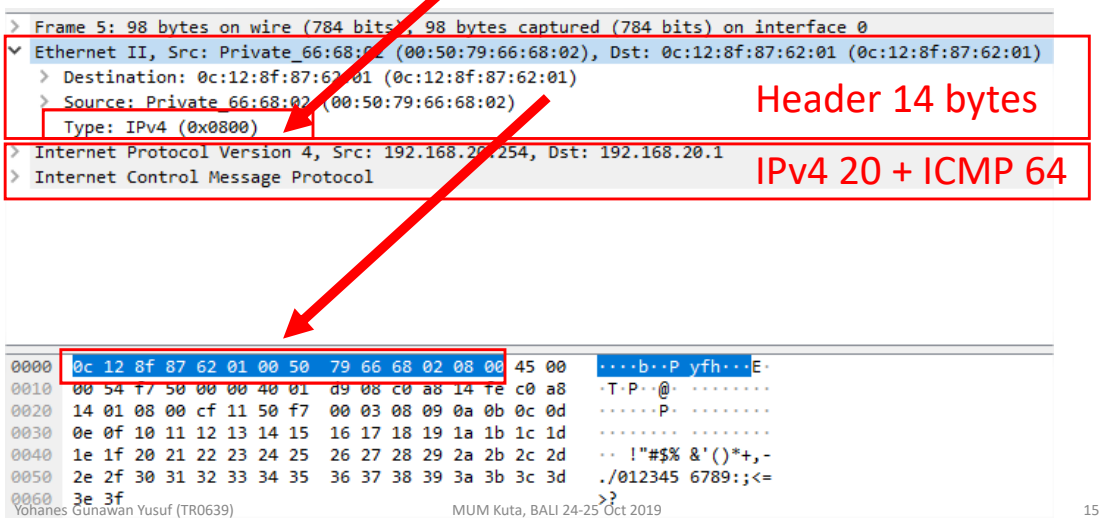
- Destination MAC (6 byte)
- Source MAC (6 byte)
- Type (2 byte)
- Payload (46 – 1500 byte) → IP, TCP or UDP, ARP, DHCP, ICMP, HTML etc

Ether Type

(It is used to indicate which protocol is encapsulated in the payload of the frame.)

- 0x0800 : IPv4 - Internet Protocol V4
- 0x0806 : ARP - Address Resolution Protocol
- 0x8100 : VLAN - Virtual LAN (with tag id)
- 0x86DD: IPv6 - Internet Protocol V6
- 0x8847 - 0x8848 : MPLS
- 0x8863 - 0x8864: PPPoE
- 0x9100 : VLAN (double tagging)

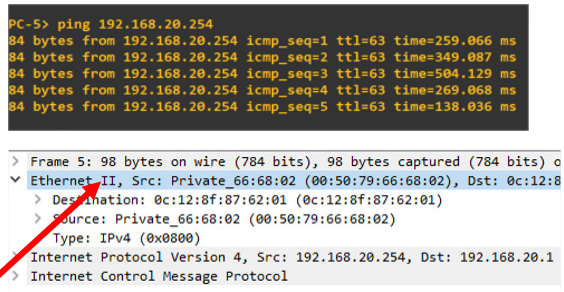
Ethernet Standard IPv4 Frame (0x0800)



15

Ethernet Standard Frame Analysis (for ICMP)

- ICMP Data = 56 bytes
- ICMP Header (reply) = 8 bytes
- IPv4 Header = 20 bytes
- Total byte Ping = 56 + 8 + 20
  = 84 bytes
- Ethernet Header = 14 bytes
- Total Ethernet Frame = 14 + 84 = 98 bytes



16

UBAYA
UNIVERSITAS SURABAYA

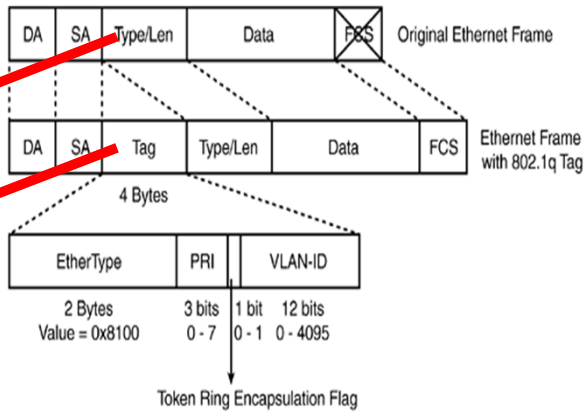
MikroTik

VLAN (802.1Q) Frame

17

Ethernet Type (Standard vs VLAN)

- 0x0800 --> IPv4 ethernet packet type
- 0x8100 --> VLAN ethernet packet type



18

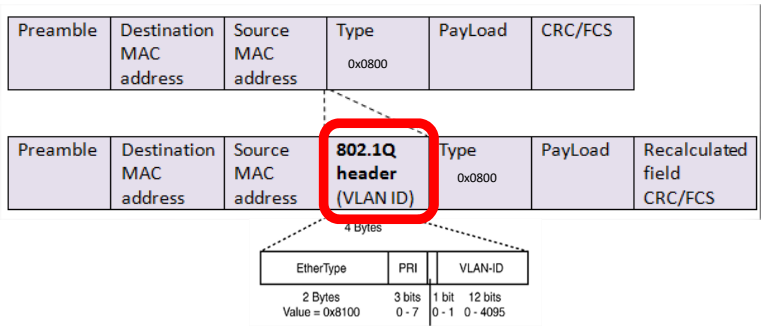
How VLAN work ?

- Tagged Ethernet frame with VLAN ID tag
- UnTagged Ethernet frame from VLAN ID tag

19

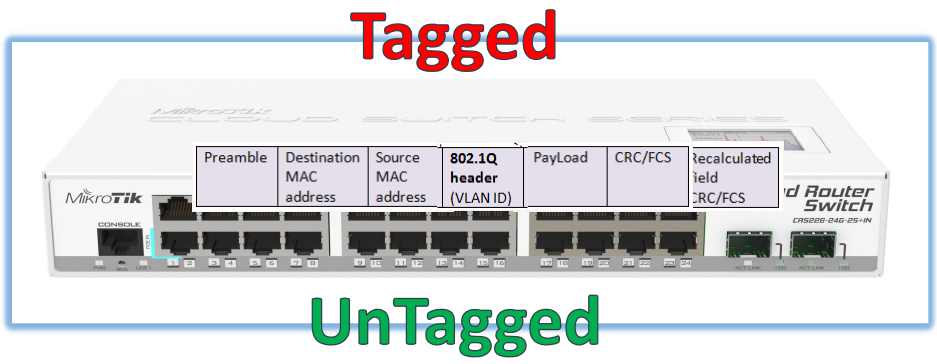
IEEE 802.1Q

- IEEE 802.1Q is a standardized encapsulation protocol that defines how to insert (tagged) a four-byte VLAN identifier into Ethernet header.
- RouterOS supports up to 4095 VLAN interfaces, each with a unique VLAN ID, per interface (exception: 0,1 and 4095)



20

IEEE 802.1Q

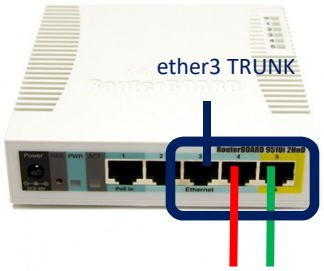


Ether Type: 0x0800 (IP4) , 0x8100 (802.1Q)

21

VLAN Example (Trunk) CHR1

/interface ethernet
set [find default-name=ether3] name=ether3-trunk
/interface vlan
add interface=ether3-trunk name=vlan40-eth3 vlan-id=40
add interface=ether3-trunk name=vlan50-eth3 vlan-id=50
/interface bridge port
add interface=ether3-trunk
/interface bridge vlan
add tagged=ether3-trunk vlan-ids=40
add tagged=ether3-trunk vlan-ids=50
add address=10.0.0.1/30 interface=ether3-trunk network=10.0.0.0
add address=192.168.40.1/24 interface=vlan40-eth3 network=192.168.40.0
add address=192.168.50.1/24 interface=vlan50-eth3 network=192.168.50.0

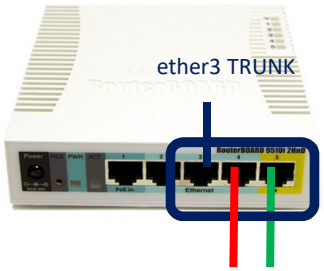


VLAN 40 50

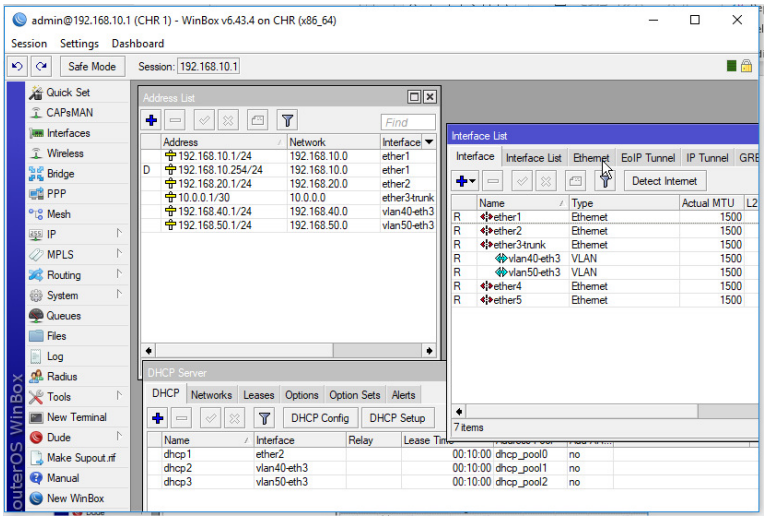
22

VLAN Example (Access) CHR2

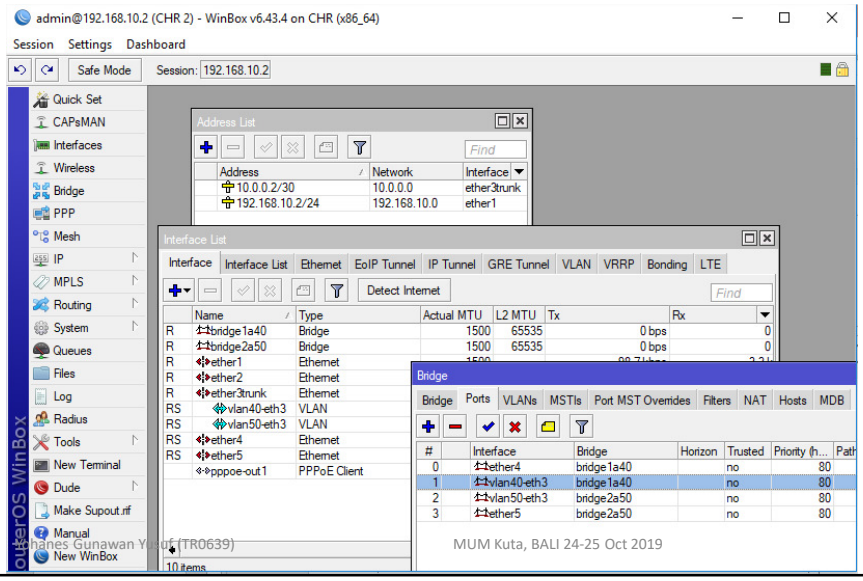
/interface bridge
add fast-forward=no name=bridge1a40
add fast-forward=no name=bridge2a50
/interface ethernet
set [find default-name=ether3] name=ether3trunk
/interface vlan
add interface=ether3trunk name=vlan40-eth3 vlan-id=40
add interface=ether3trunk name=vlan50-eth3 vlan-id=50
/interface bridge port
add bridge=bridge1a40 interface=ether4
add bridge=bridge1a40 interface=vlan40-eth3
add bridge=bridge2a50 interface=vlan50-eth3
add bridge=bridge2a50 interface=ether5



Trunk (ether3) and DHCP Server on CHR1



Trunk (ether3) and Access on CHR 2



25

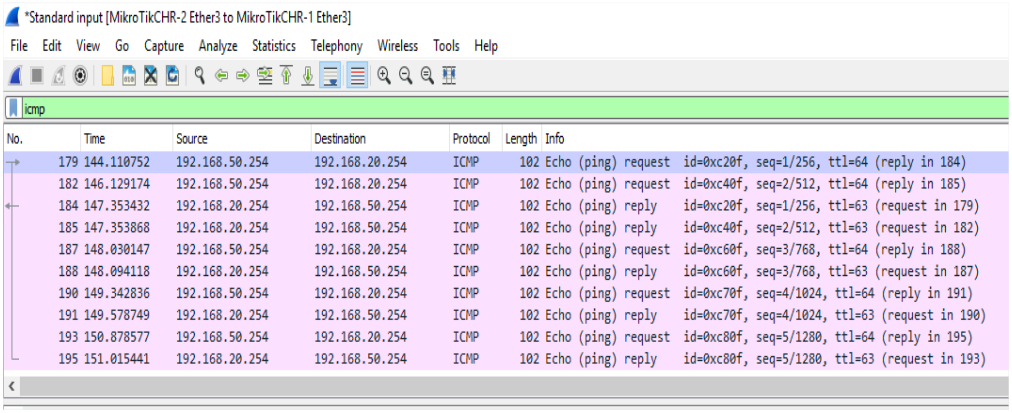
PC5 ping to PC3 thru Trunk

```
Welcome to Virtual PC Simulator, version 0.6.1
Dedicated to Daling.
Build time: Jun  1 2015 11:42:32
Copyright (c) 2007-2014, Paul Meng (mirnshi@gmail.com)
All rights reserved.

VPCS is free software, distributed under the terms of th
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.

Press '?' to get help.

Executing the startup file


PC-3> ip dhcp
DORA IP 192.168.20.254/24 GW 192.168.20.1

PC-3>
```

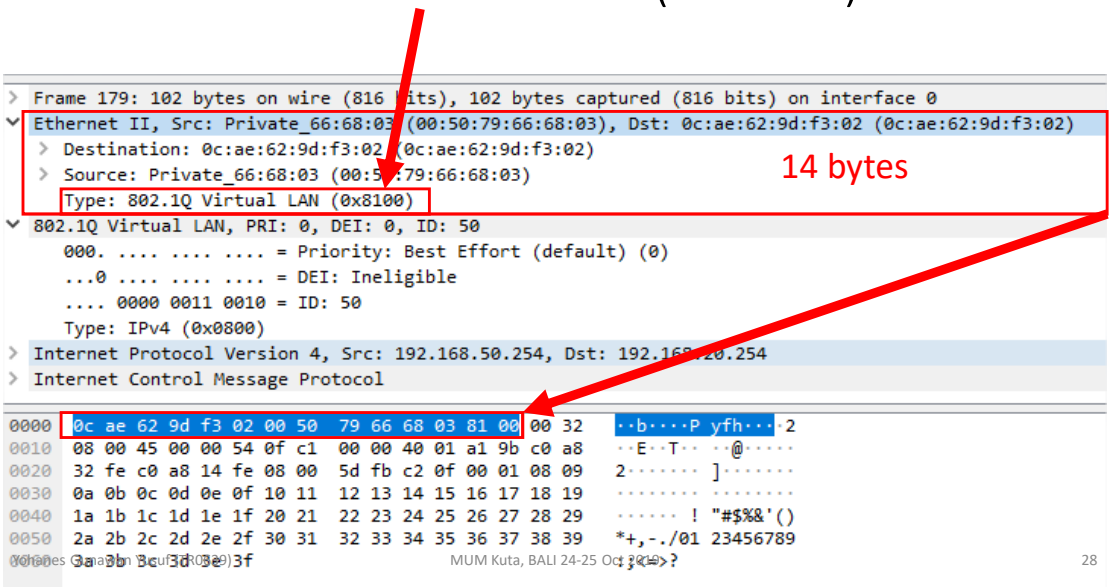
```
PC-5> show ip

NAME        : PC-5[1]
IP/MASK     : 192.168.50.254/24
GATEWAY     : 192.168.50.1
DNS         :
DHCP SERVER : 192.168.50.1
DHCP LEASE  : 562, 600/300/525
MAC         : 00:50:79:66:68:03
LPORT       : 10034
RHOST:PORT  : 127.0.0.1:10035
MTU:        : 1500

PC-5> ping 192.168.20.254
84 bytes from 192.168.20.254 icmp_seq=1 ttl=63 time=259.066 ms
84 bytes from 192.168.20.254 icmp_seq=2 ttl=63 time=349.087 ms
84 bytes from 192.168.20.254 icmp_seq=3 ttl=63 time=504.129 ms
84 bytes from 192.168.20.254 icmp_seq=4 ttl=63 time=269.068 ms
84 bytes from 192.168.20.254 icmp_seq=5 ttl=63 time=138.036 ms

PC-5>
```


26

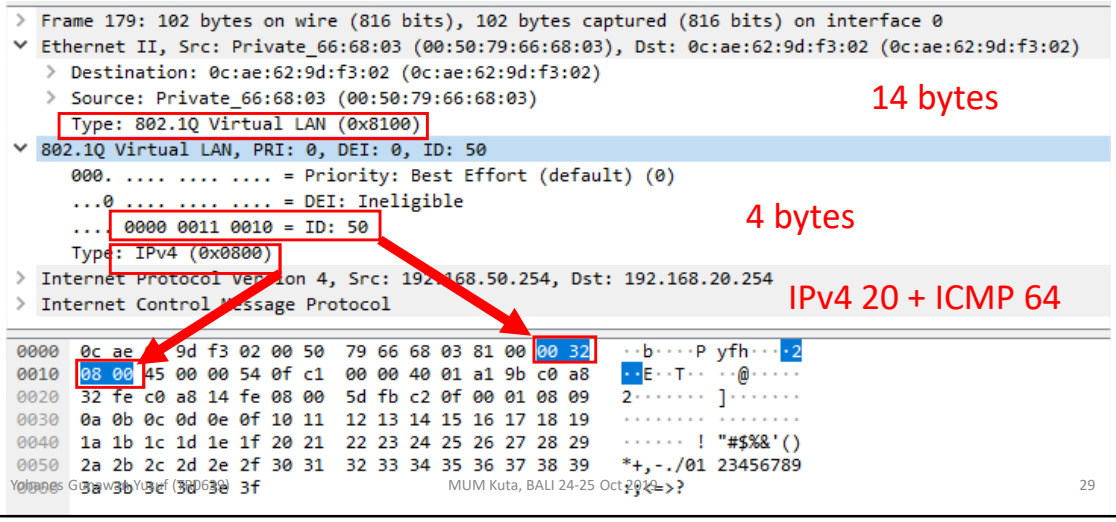
Wireshark – Captured Trunk



Ethernet with VLAN Frame (0x8100)



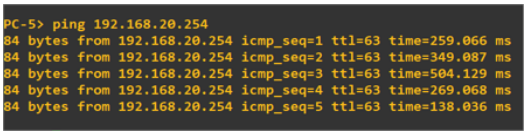
VLAN (802.1Q) Tag

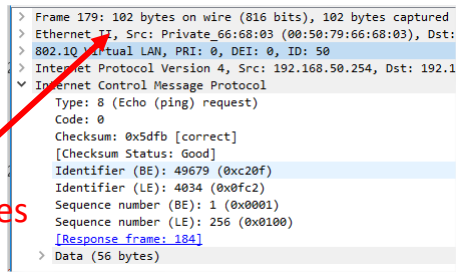


29

802.1Q Frame Analysis (for ICMP)

- ICMP Data = 56 bytes
- ICMP Header (reply) = 8 bytes
- IPv4 Header = 20 bytes
- Total byte Ping = 56 + 8 + 20 = 84 bytes
- 802.1Q VLAN (Id 50) = 4 bytes
- Ethernet Header = 14 bytes
- Total VLAN 802.1Q = 4 + 14 + 84 = 102 bytes





30

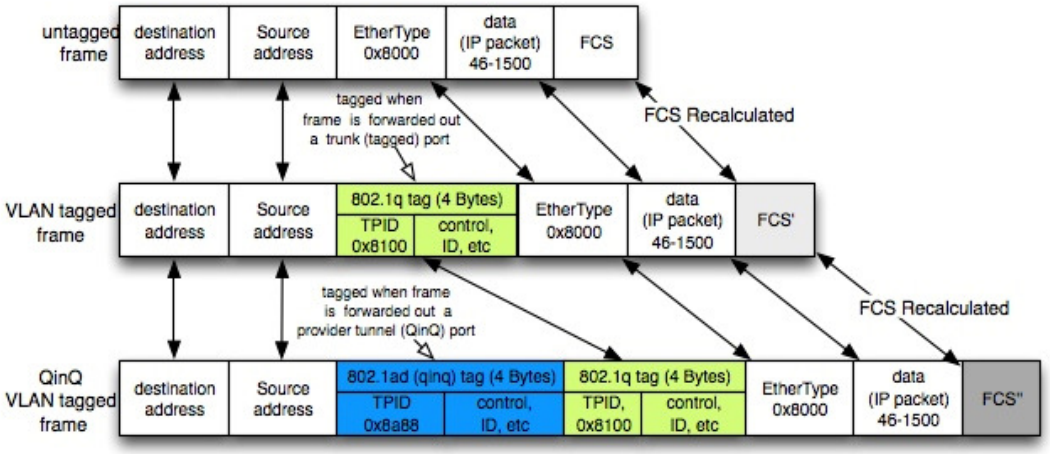
UBAYA
UNIVERSITAS SURABAYA

MikroTik

VLAN in VLAN (QinQ) Frame

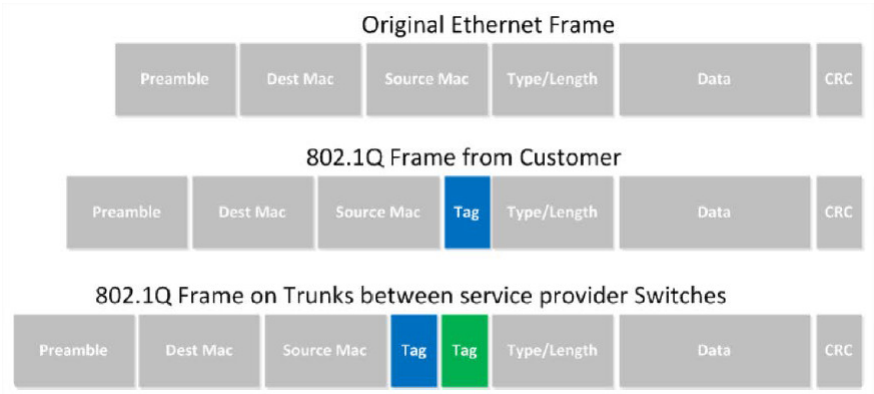
31

IEEE 802.1ad

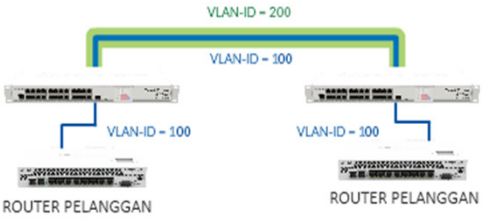


32

QinQ @ MikroTik

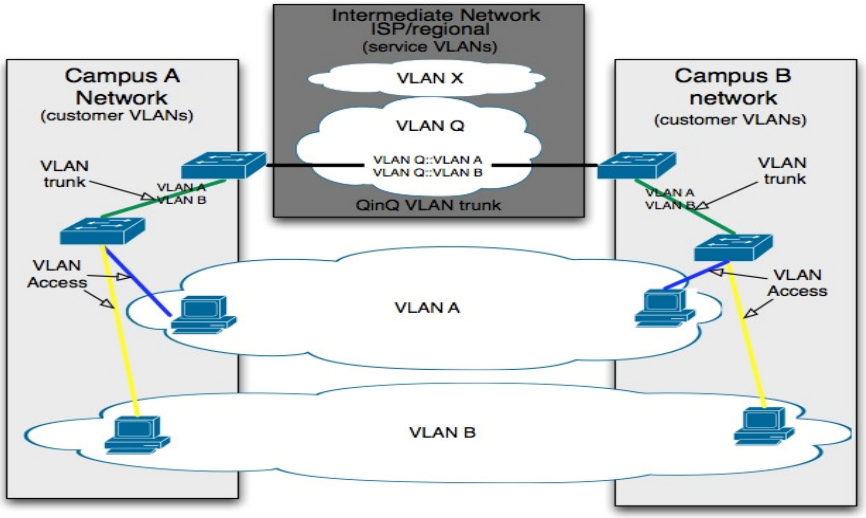


Why QinQ ?



- QinQ is tunnelling 802.1Q
- Often used by Ethernet Providers as a layer2 VPN for customers.
- Easy to implement, you don't need exotic hardware and we don't have to run any routing protocols between the service provider and customer.
- From the customer's perspective, it's just like their sites are directly connected on layer2 (Switch)

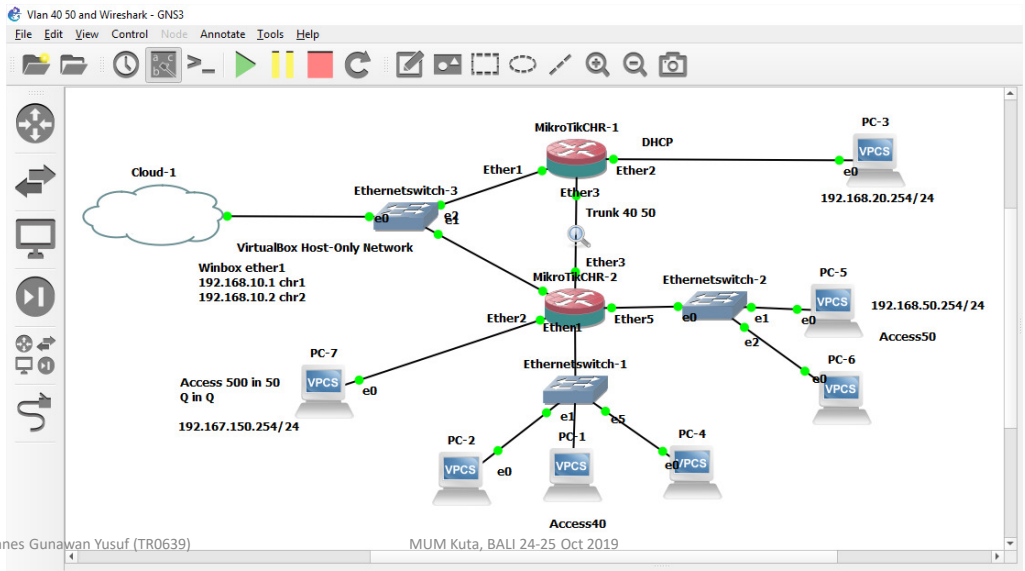
QinQ Implementation



Source -> https://groups.geni.net/geni/wiki/QinqResults

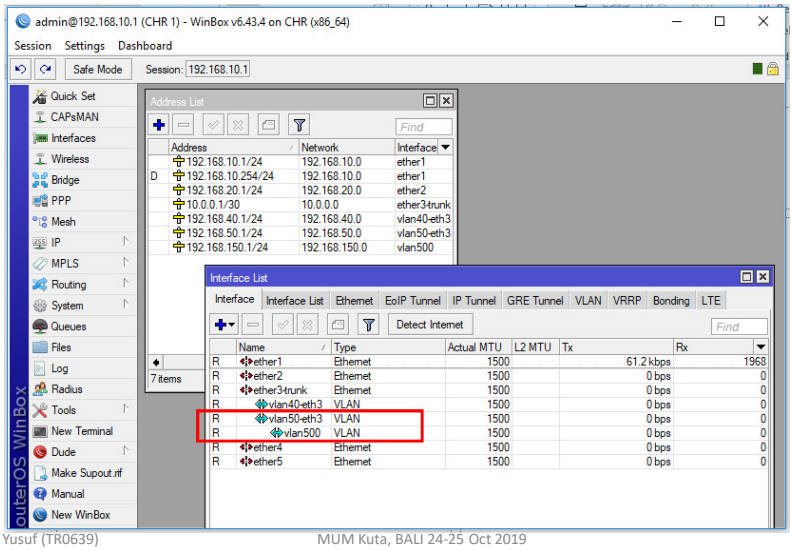
35

QinQ Simulation on GNS3 (Vlan 500 in 50)



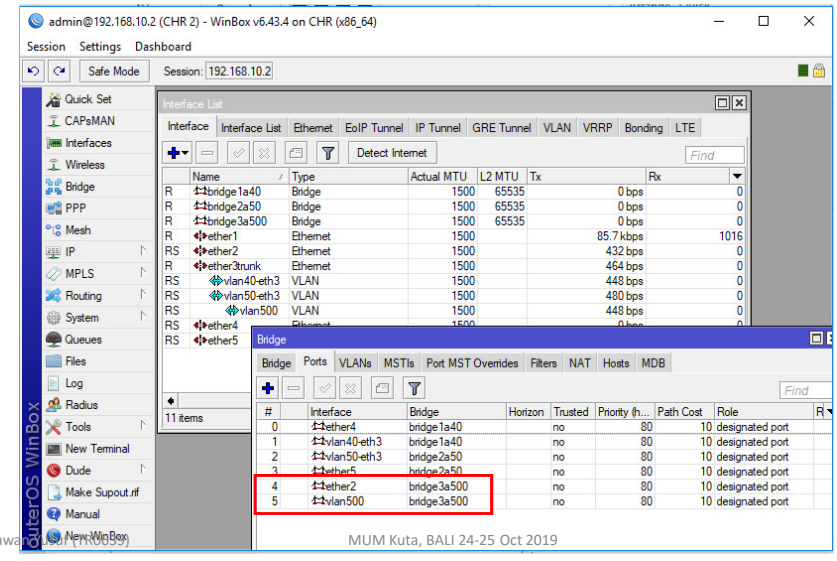
36

Setting QinQ (Access 500 in 50) CHR1



37

Access 500 on CHR2 (Ether2)



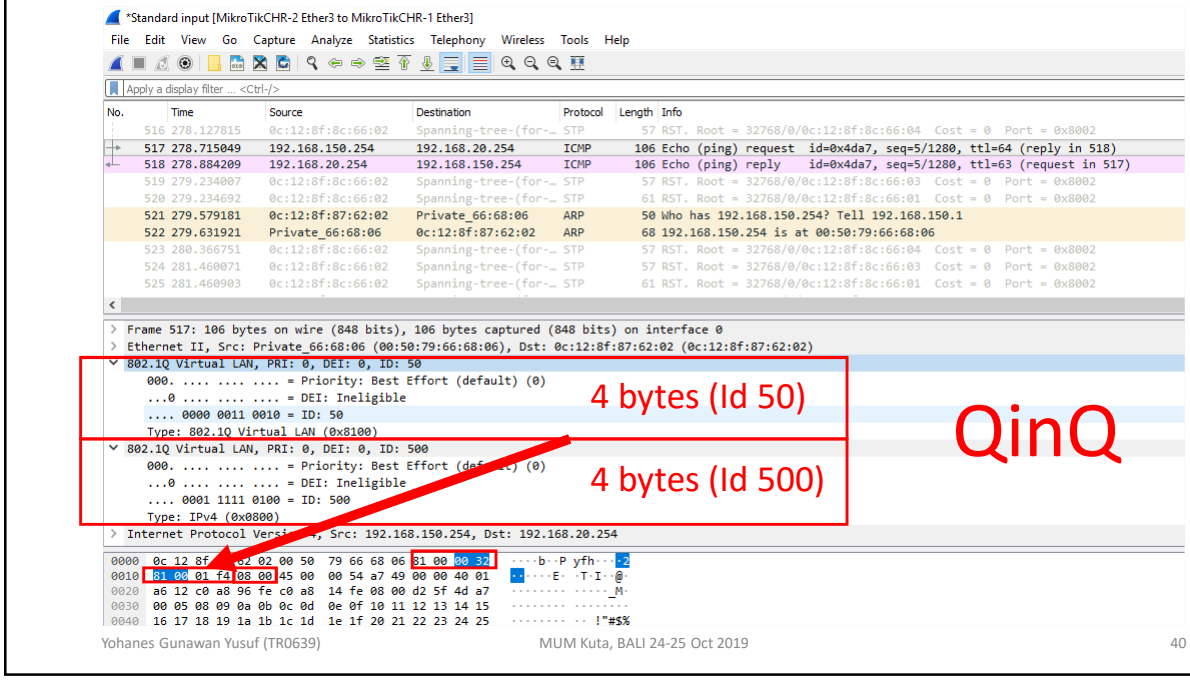
38

PC7 ping to PC3 thru Trunk Q in Q (500 in 50)

```
VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.

Press '?' to get help.

Executing the startup file


PC-3> ip dhcp
DDORA IP 192.168.20.254/24 GW 192.168.20.1

PC-3>
```

```
PC-7> ping 192.168.20.254
84 bytes from 192.168.20.254 icmp_seq=1 ttl=63 time=360.079 ms
84 bytes from 192.168.20.254 icmp_seq=2 ttl=63 time=701.177 ms
84 bytes from 192.168.20.254 icmp_seq=3 ttl=63 time=355.094 ms
84 bytes from 192.168.20.254 icmp_seq=4 ttl=63 time=486.122 ms
84 bytes from 192.168.20.254 icmp_seq=5 ttl=63 time=520.125 ms

PC-7>
```

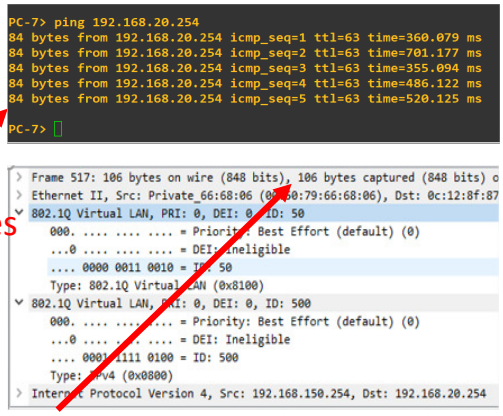

39



40

QinQ Frame Analysis (for ICMP)

- ICMP Data = 56 bytes
- ICMP Header (reply) = 8 bytes
- IPv4 Header = 20 bytes
- Total byte Ping = 56 + 8 + 20 = 84 bytes
- 802.1Q VLAN (Id 500) = 4 bytes
- 802.1Q VLAN (Id 50) = 4 bytes
- Ethernet Header = 14 bytes
- Total VLAN 802.1Q = 4 + 4 + 14 + 84 = 106 bytes



41

Frame Analysis – 802.1Q and QinQ

use	header size	tag size	MTU	FCS	total frame size
standard ethernet	14	0	1500	4	1518
802.1q VLAN trunk	14	+4	1500	4	1522
802.1ad (QinQ) VLAN "tunnel"	14	+4 +4	1500	4	1526

- Ethernet MTU = IP Header + TCP Header + Payload = 1500 bytes
- IP Header = 20 bytes
- TCP Header = 20 bytes
- Payload = 1460 bytes
- If packet size more than MTU will be fragmented

42

UBAYA
UNIVERSITAS SURABAYA

MikroTik

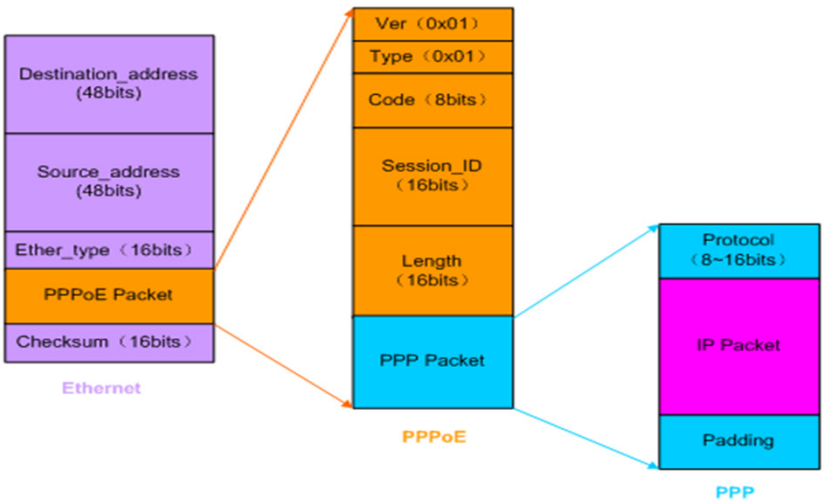
PPPoE Frame

Point-to-Point Protocol over Ethernet (PPPoE) is a network protocol for encapsulating PPP frames inside Ethernet frames.

43

PPPoE Frame

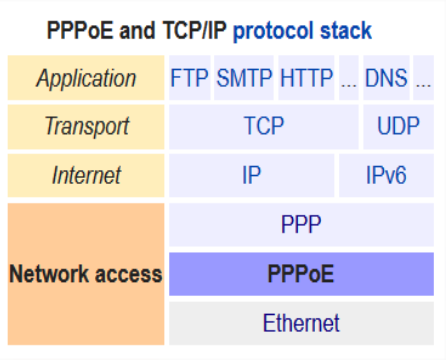
(source: www.h3c.com.hk)



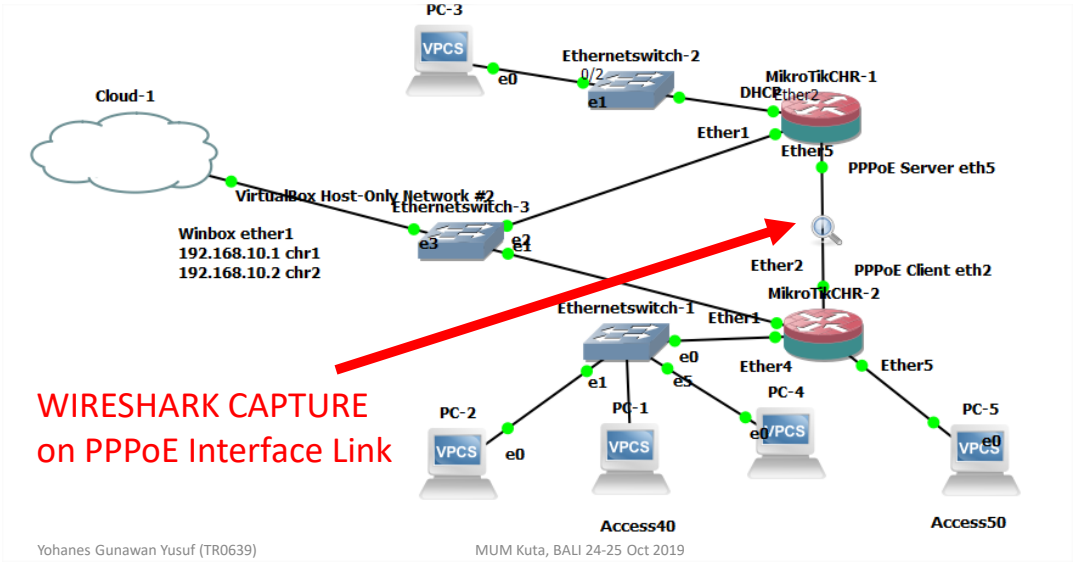
44

PPP Packet

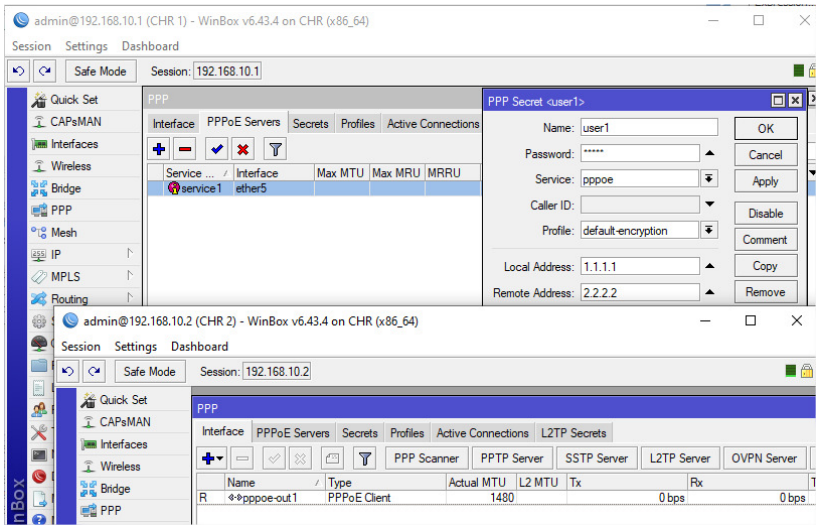
- **Point-to-Point Protocol** (**PPP**) is a data link layer (layer 2) communications protocol between two routers directly without any host or any other networking in between.
- PPP may include the following LCP options. It can provide connection authentication, transmission encryption, and compression.
- **Point-to-Point Protocol over Ethernet (PPPoE)** is derivatives of PPP



PPPoE Server and Client

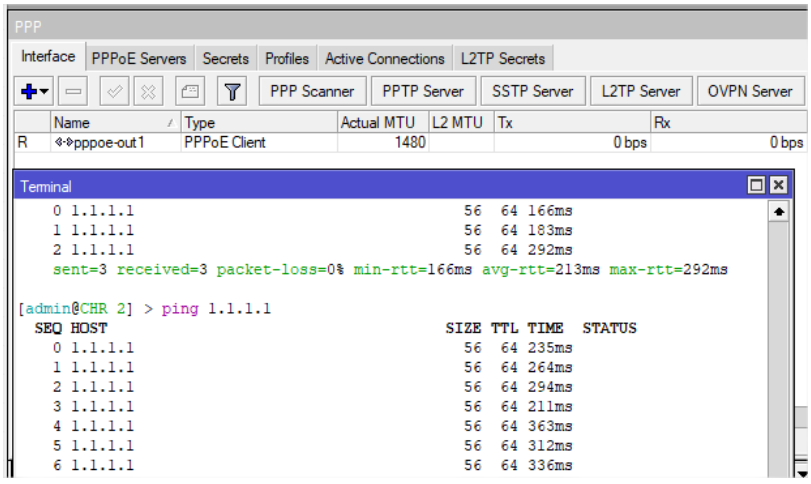


PPPoE Setting



47

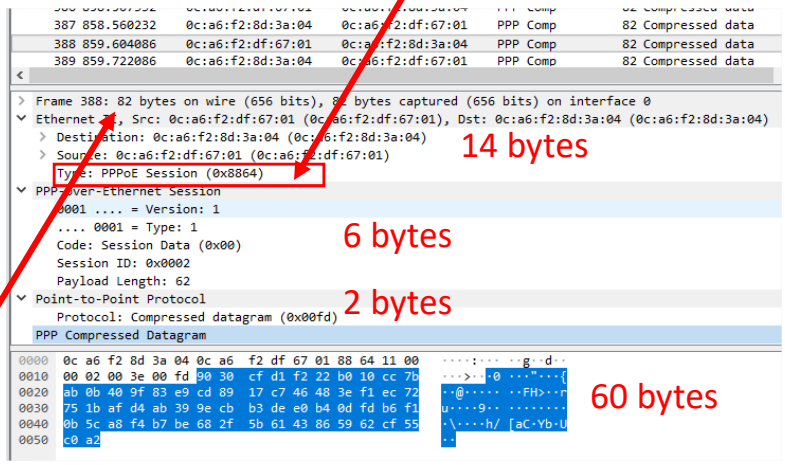
Ping from PPPoE Client to Server



48

Ethernet with PPPoE Session Frame (0x8864)

- PPP Datagram (Compresed Ping) = 60 bytes (56 + 4 bytes comp header)
- PPPoE Session = 6 bytes
- PtP Protocols = 2 bytes
- Ethernet Header = 14 bytes
- PPPoE total bytes = 60+ 6+2+14 = 82 bytes

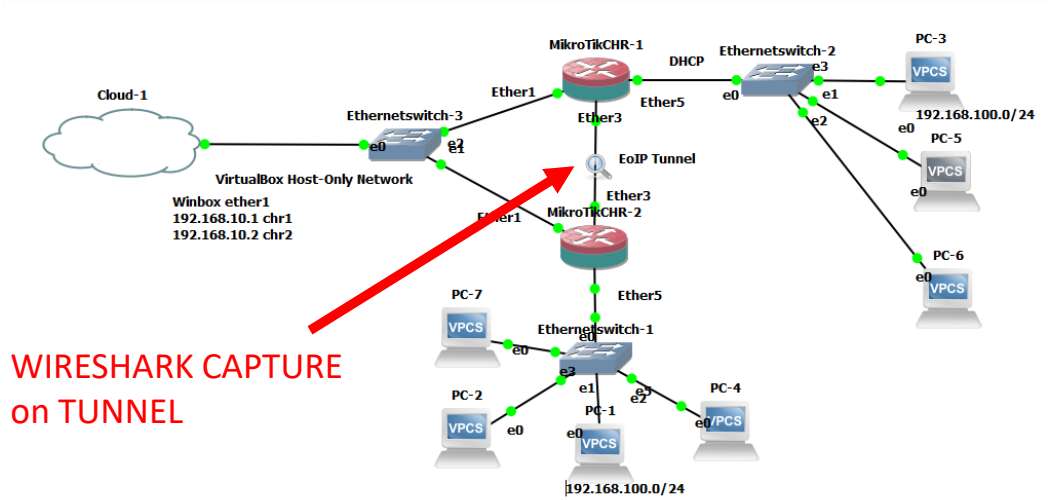


UBAYA UNIVERSITAS SURABAYA

MikroTik

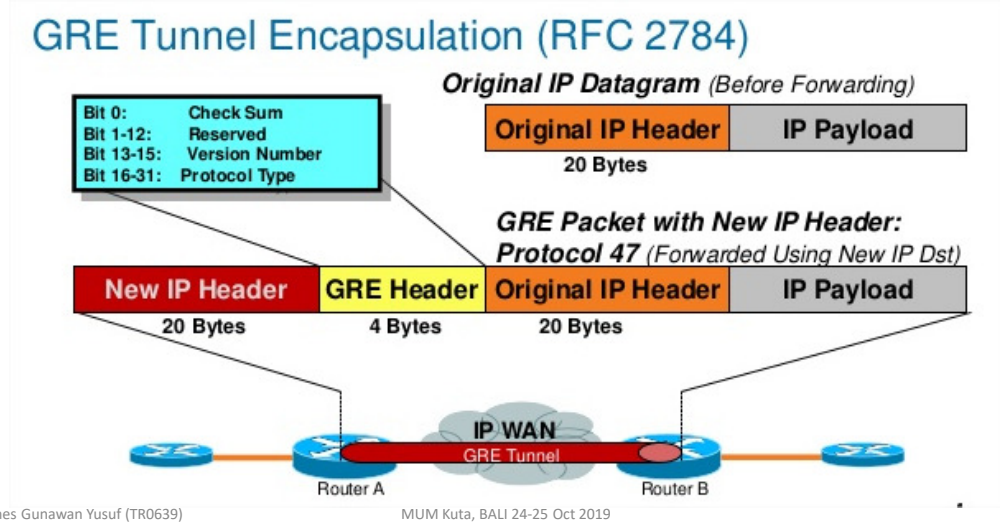
EoIP Tunnel Frame

EoIP Tunnel



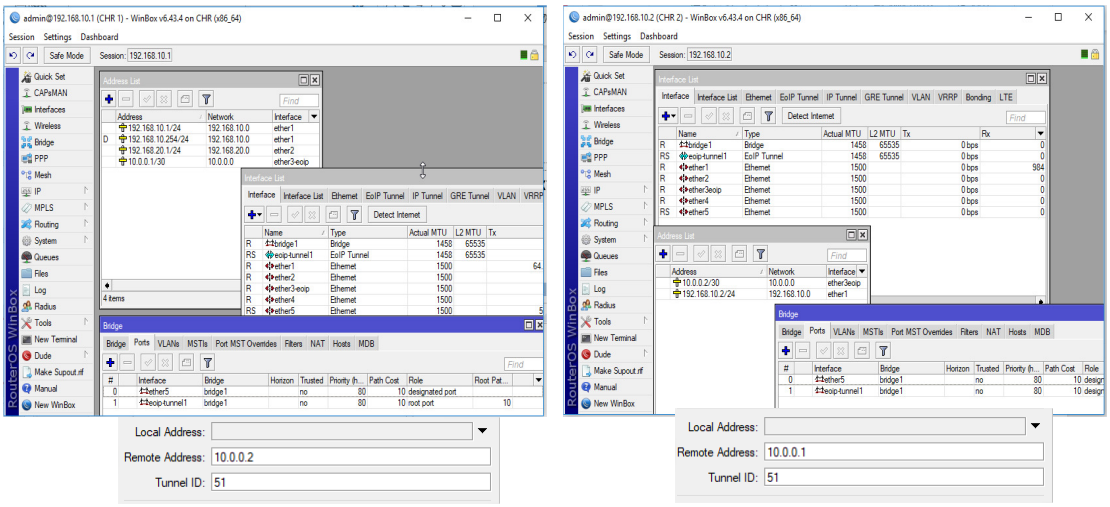
51

EoIP Frame (Using GRE Protocol)

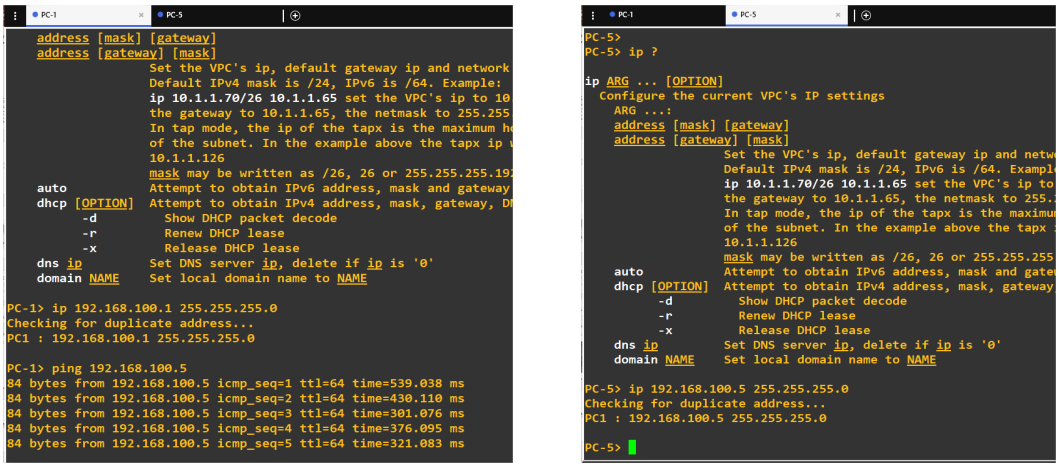


52

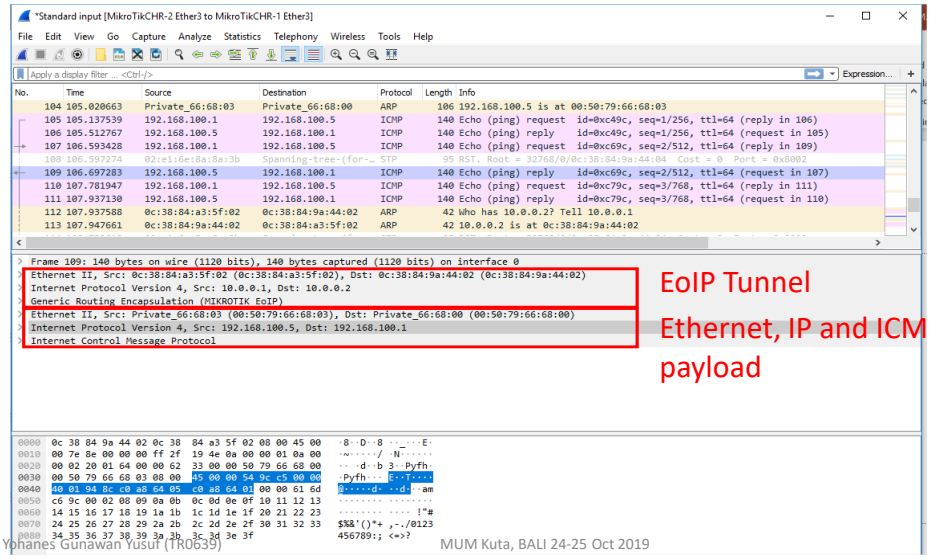
EoIP Setting



Ping PC1 to PC5 thru EoIP Tunnel

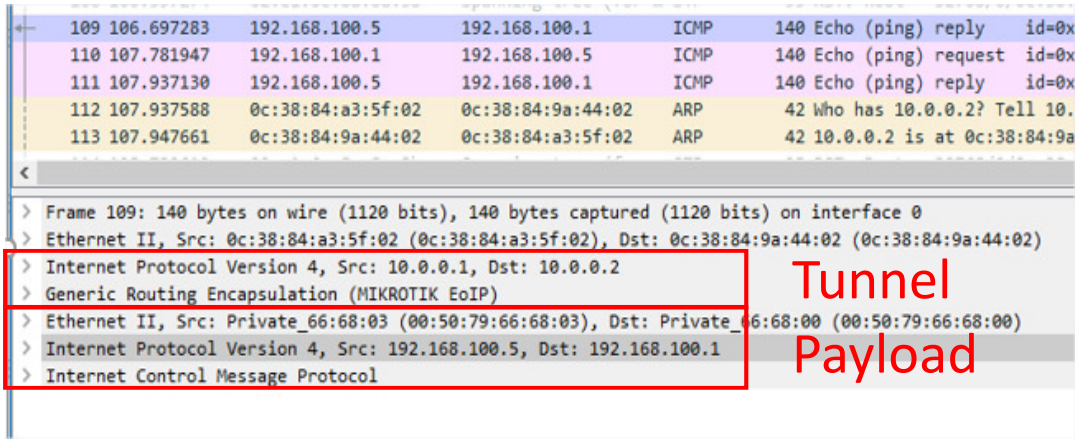


EoIP Encapsulated Frame



55

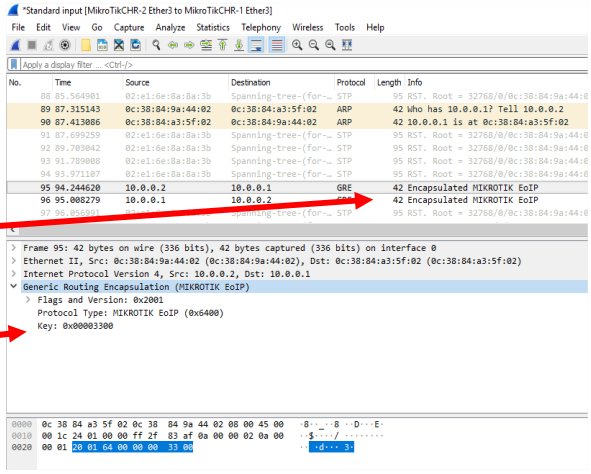
EoIP Tunnel and Payload



56

EoIP Frame Analysis – GRE Protocol

- GRE (MikroTik EoIP) = 8 bytes
- IPv4 Header = 20 bytes
- Ethernet Header = 14 bytes
- EoIP GRE Tunnel = 14+ 8+ 20 = 42 bytes

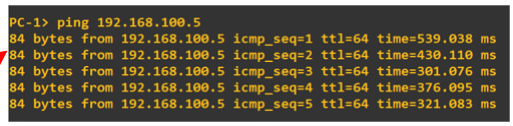


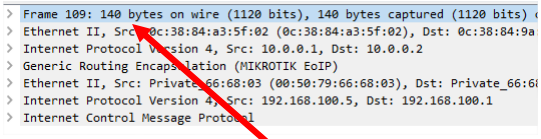
- Tunnel ID = 51 = 0x00003300

57

EoIP Frame Analysis (for ICMP)

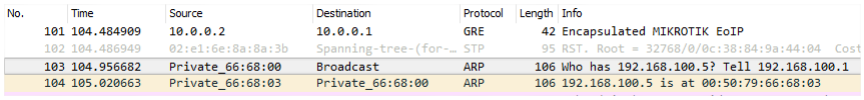
- ICMP Data = 56 bytes
- ICMP Header (reply) = 8 bytes
- Inner IP Header = 20 bytes
- Total byte Ping = 56 + 8 + 20 = 84 bytes
- Inner Ethernet Header = 14 bytes
- GRE (MikroTik EoIP) = 8 bytes
- Outer IP Header = 20 bytes
- Outer Ethernet Header = 14 bytes
- EoIP Tunnel = 14+ 8+ 20 + 14 = 42 + 14 = 56 bytes
- Total EoIP Frame = EoIP Tunnel header + Ping = 56 + 84 = 140 bytes





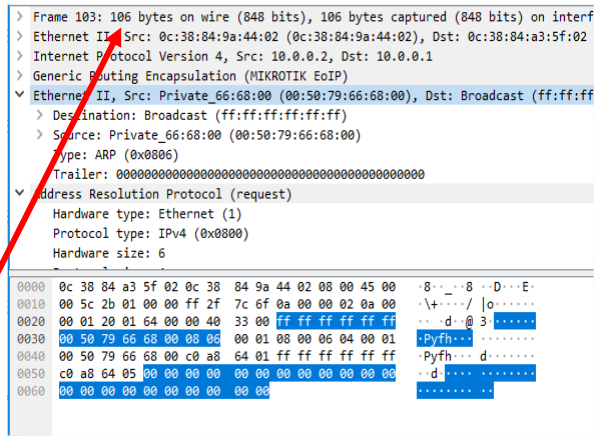
58

EoIP Frame Analysis (for ARP Request)



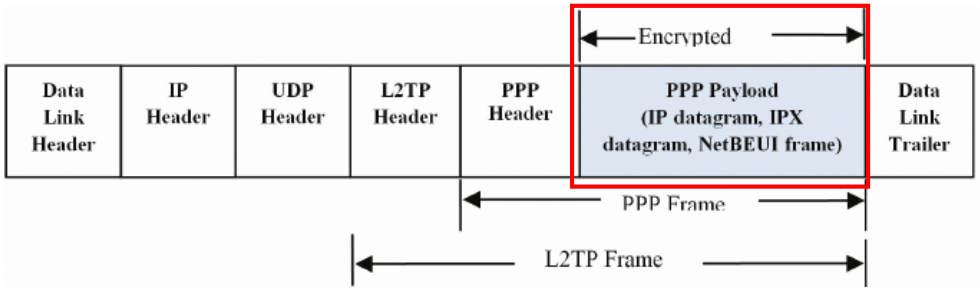
No.	Time	Source	Destination	Protocol	Length	Info
101	104.484909	10.0.0.2	10.0.0.1	GRE	42	Encapsulated MIKROTIK EoIP
102	104.486949	02:e1:6e:8a:8a:3b	Spanning-tree-(for-…	STP	95	RST. Root = 32768/0/0c:38:84:9a:44:04 Cost
103	104.956682	Private_66:68:00	Broadcast	ARP	106	Who has 192.168.100.5? Tell 192.168.100.1
104	105.020663	Private_66:68:03	Private_66:68:00	ARP	106	192.168.100.5 is at 00:50:79:66:68:03

- ARP Request = 28 bytes
- Inner Ethernet Header = 14 bytes
- Inner Ethernet Trailer = 22 bytes
- Total ARP = 28 + 14 + 22 = 64 bytes
- GRE (MikroTik EoIP) = 8 bytes
- Outer IP Header = 20 bytes
- Outer Ethernet Header = 14 bytes
- EoIP Tunnel = 14+ 8+ 20 = 42 bytes
- Total EoIP ARP Frame = EoIP Tunnel + Total ARP = 42 + 64 = 106 bytes



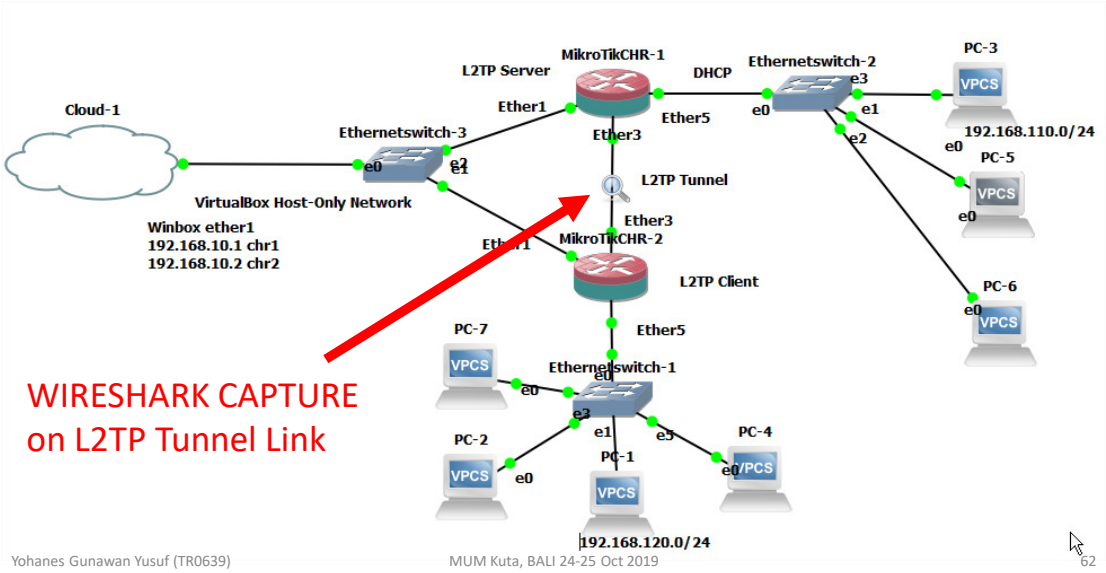
L2TP Tunnel Frame

L2TP Frame Format (use PPP packet frame)



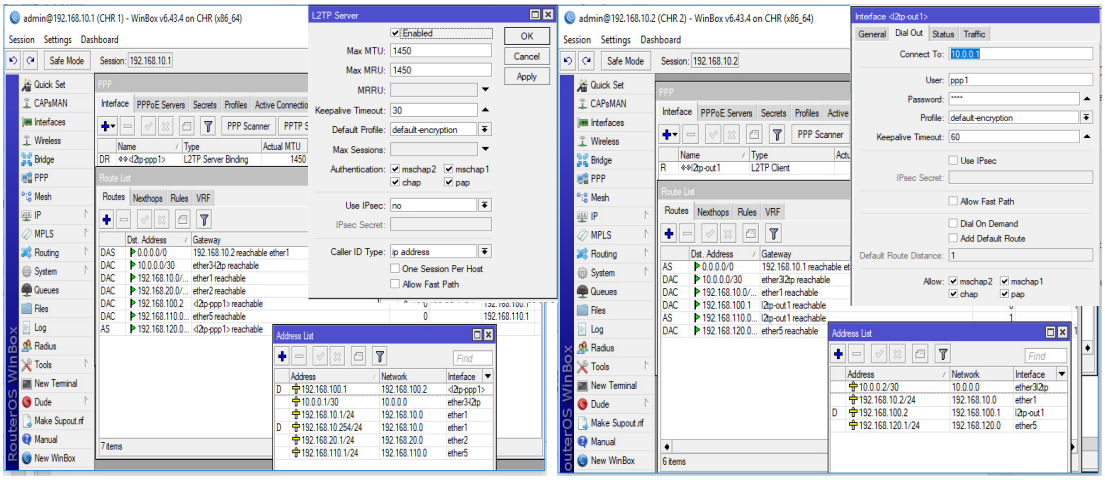
61

L2TP



62

L2TP – Server and Client (No IPsec)



63

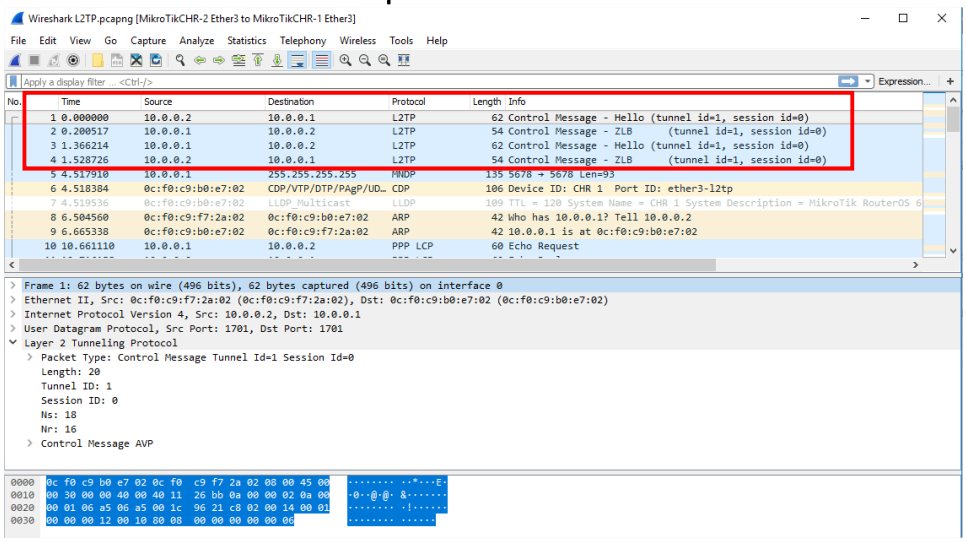
Ping PC1 to PC5

```
PC-1>
PC-1>
PC-1> ip 192.168.120.120 255.255.255.0 192.168.120.1
Checking for duplicate address...
PC1 : 192.168.120.120 255.255.255.0 gateway 192.168.120.1

PC-1> ping 192.168.120.1
84 bytes from 192.168.120.1 icmp_seq=1 ttl=64 time=215.189 ms
84 bytes from 192.168.120.1 icmp_seq=2 ttl=64 time=112.901 ms
84 bytes from 192.168.120.1 icmp_seq=3 ttl=64 time=21.008 ms
84 bytes from 192.168.120.1 icmp_seq=4 ttl=64 time=208.050 ms
84 bytes from 192.168.120.1 icmp_seq=5 ttl=64 time=15.938 ms

PC-1> ping 192.168.110.110
84 bytes from 192.168.110.110 icmp_seq=1 ttl=62 time=505.129 ms
84 bytes from 192.168.110.110 icmp_seq=2 ttl=62 time=480.185 ms
84 bytes from 192.168.110.110 icmp_seq=3 ttl=62 time=726.186 ms
84 bytes from 192.168.110.110 icmp_seq=4 ttl=62 time=281.070 ms
84 bytes from 192.168.110.110 icmp_seq=5 ttl=62 time=437.108 ms
```

```
Welcome to Virtual PC Simulator, version 0.6.1
Dedicated to Daling.
Build time: Jun  1 2015 11:42:32
Copyright (c) 2007-2014, Paul Meng (mirnshi@gmail.com)
All rights reserved.

VPCS is free software, distributed under the terms of the "BSD"
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.

Press '?' to get help.

Executing the startup file


PC-5> ip 192.168.110.110 255.255.255.0 192.168.110.1
Checking for duplicate address...
PC1 : 192.168.110.110 255.255.255.0 gateway 192.168.110.1
```

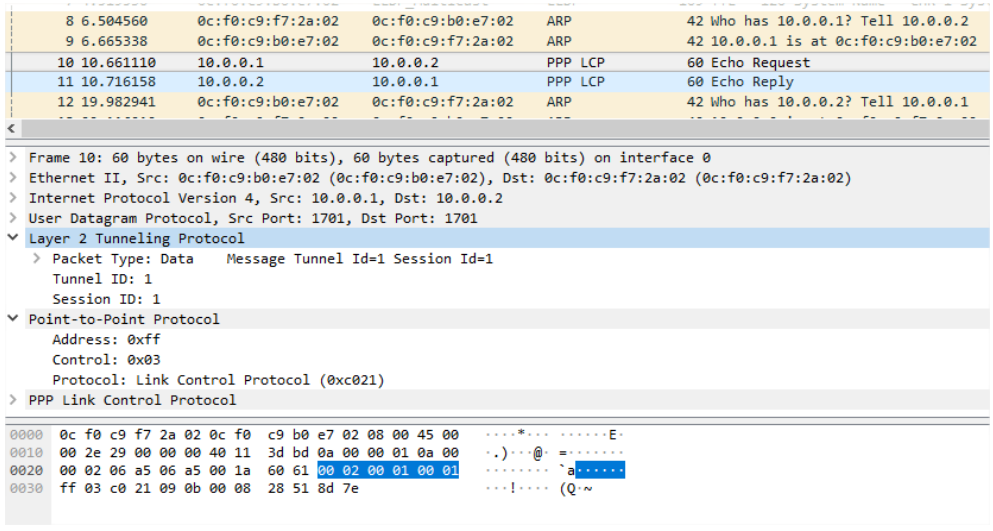

64

L2TP Tunnel Setup



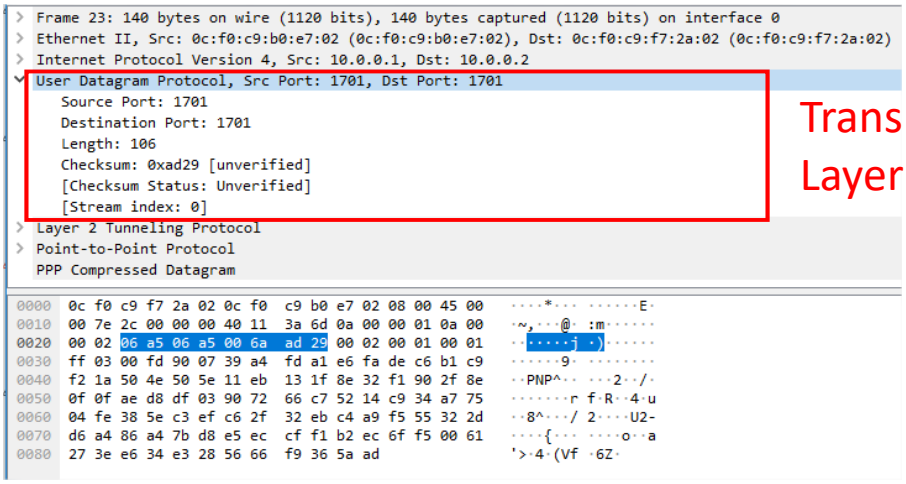
65

L2TP – LCP (link Control Protocol)



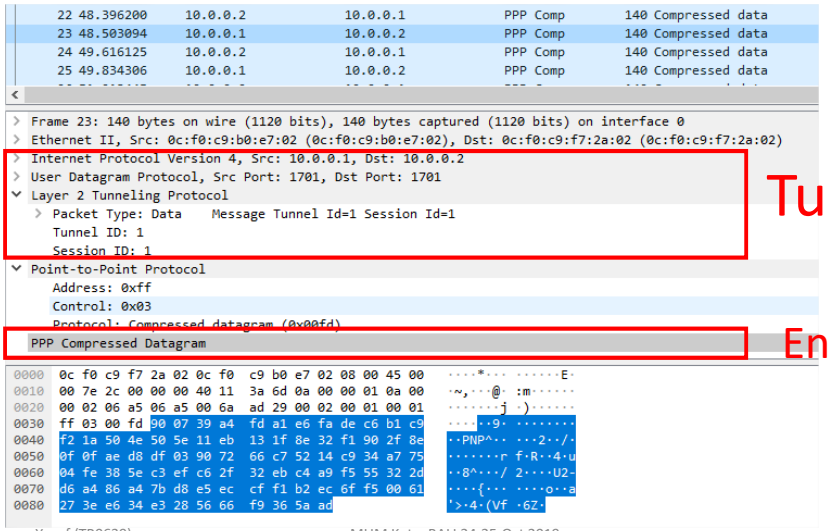
66

L2TP – Use UDP (port 1701)



Transport Layer UDP

L2TP – Ping as PPP Compressed Datagram (Encrypted)

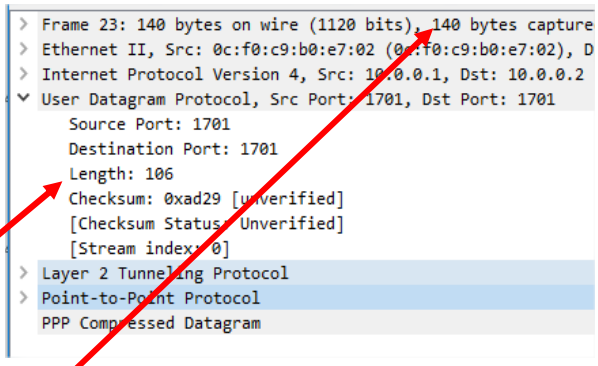


Tunnel

Encrypted

L2TP Frame Analysis (for ICMP as PPP Dtgrm)

- PPP Datagram (ICMP) = 88 bytes
- PtPP Header = 4 bytes
- L2TP Header = 6 bytes
- UDP Header = 8 bytes
- Total UDP Length = 88 + 4 + 6 + 8 = 106 bytes
- IPv4 Header = 20 bytes
- Ethernet Header = 14 bytes
- L2TP frame length = 20 + 14 + 106 = 140 bytes

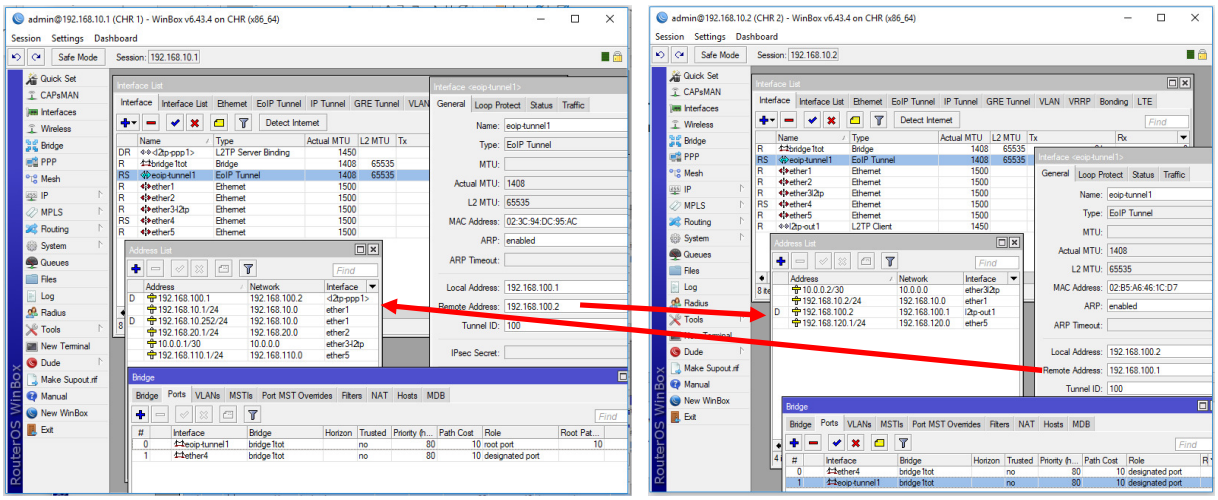


UBAYA UNIVERSITAS SURABAYA

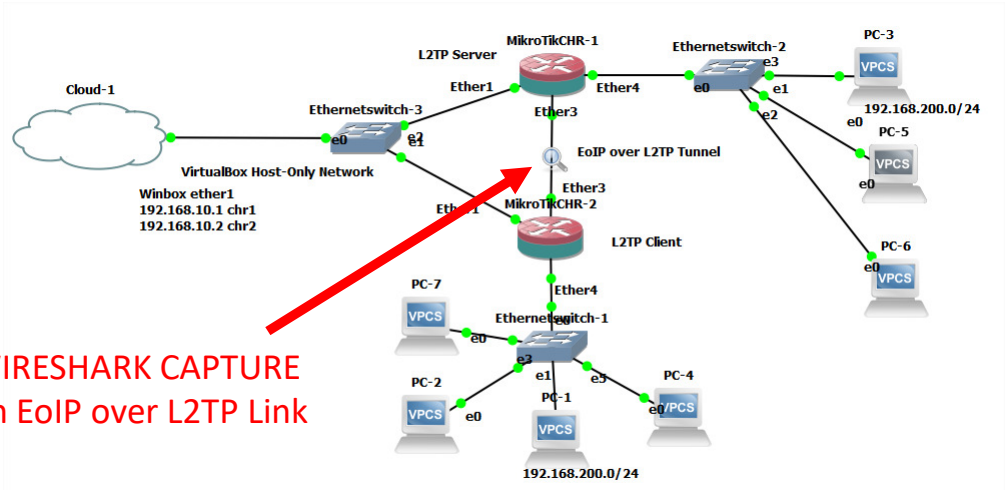
MikroTik

EoIP over L2TP Frame

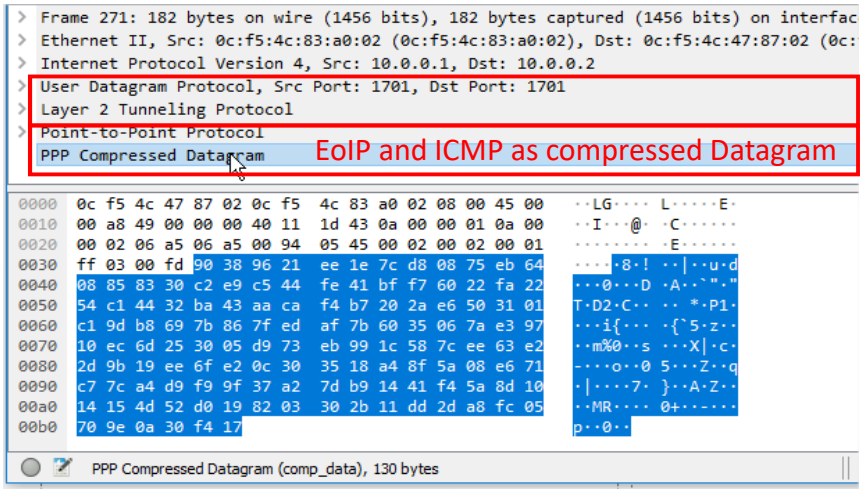
EoIP over L2TP



EoIP over L2TP Tunnel



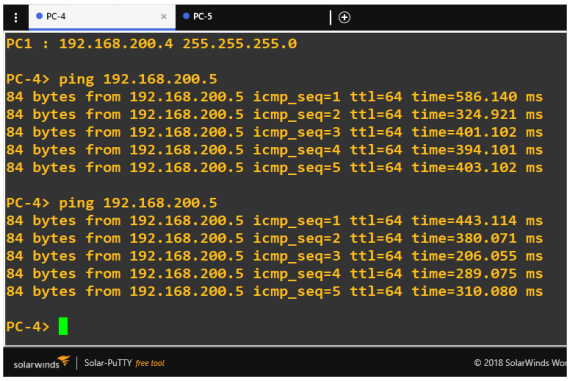
EoIP over L2TP Tunnel

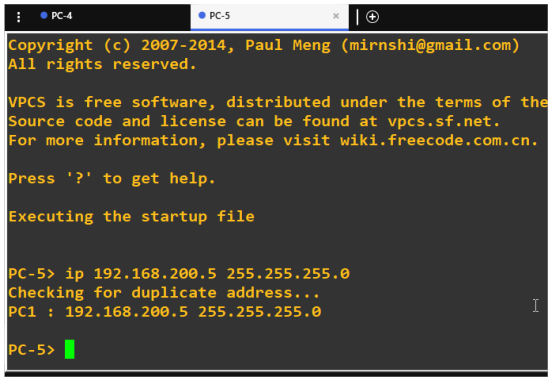


L2TP Tunnel

73

Ping PC4 to PC5



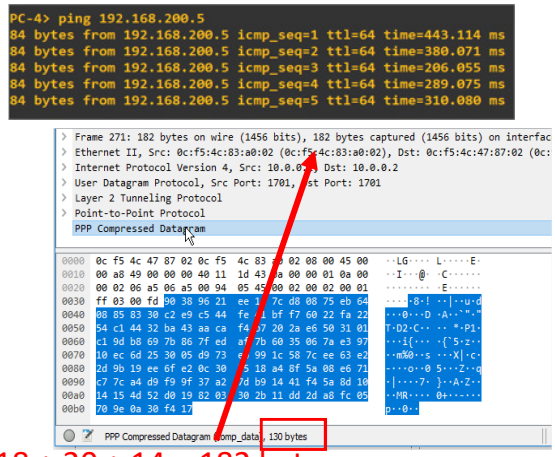


74

EoIP over L2TP Frame Analysis

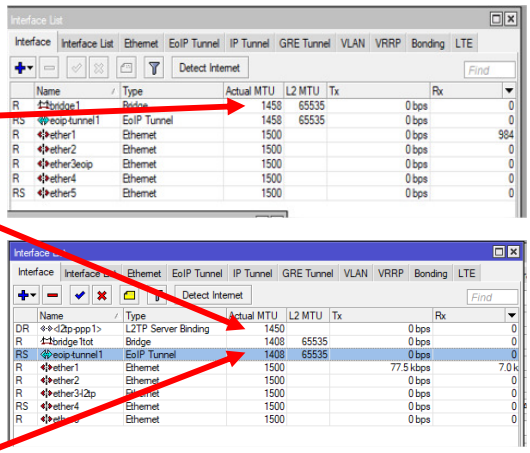
Ping and EoIP (as PPP Compressed Datagram = 130 bytes)

- PPP Compr Datagram 130 bytes:
  - Ping (ICMP) total = 84 bytes
  - PPtP Header = 4 bytes
  - EoIP Header = 42 bytes
- PPtP Header = 4 bytes
- L2TP Header = 6 bytes
- UDP Header = 8 bytes
- IPv4 Header = 20 bytes
- Ethernet Header = 14 bytes
- EoIP over L2TP frame length = 130 + 18 + 20 + 14 = 182 bytes



Actual MTU Decreased for EoIP over L2TP

- Actual MTU For Single Tunnel
  - EoIP = 1458 bytes
  - L2TP = 1450 bytes
- EoIP Header length = 42 bytes
- Actual MTU for EoIP over L2TP:
  - = Actual Bridge Interface
  - = 1450 – 42 = 1408 bytes



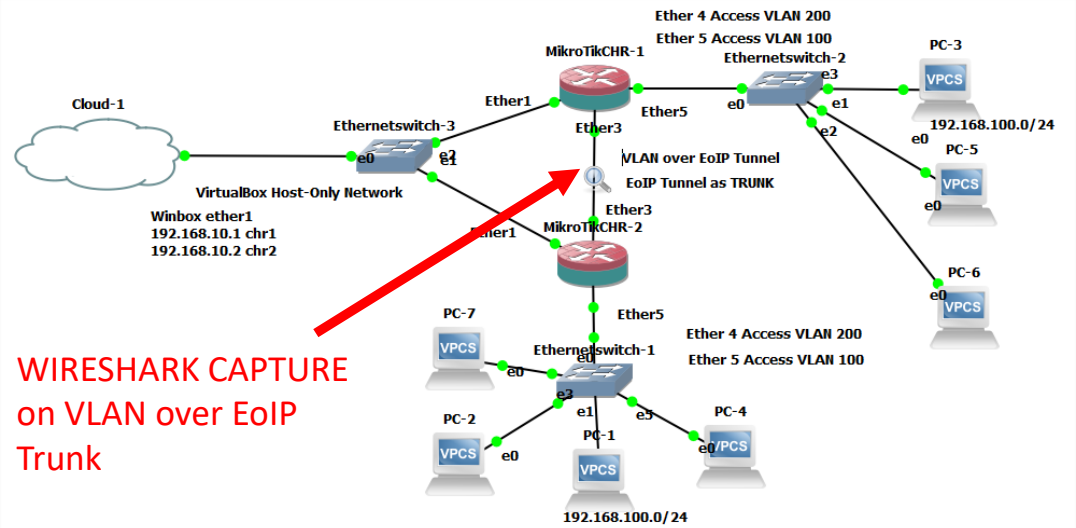
UBAYA
UNIVERSITAS SURABAYA

MikroTik

VLAN over EoIP Frame

77

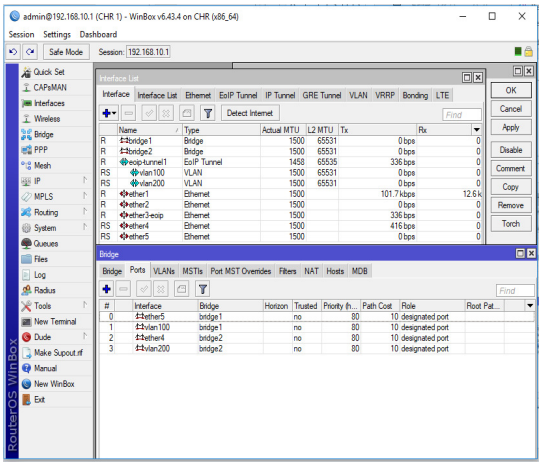
VLAN over EoIP Tunnel

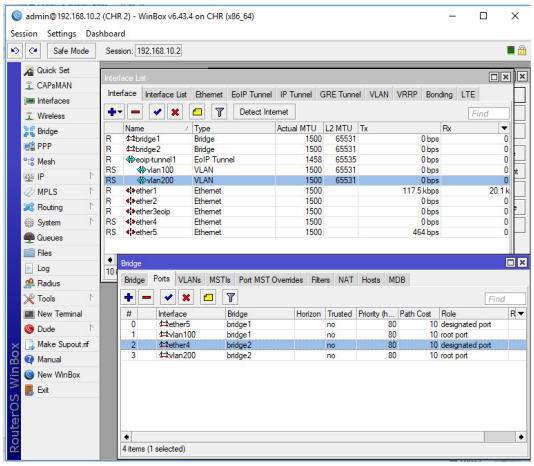


WIRESHARK CAPTURE on VLAN over EoIP Trunk

78

VLAN over EoIP Setup



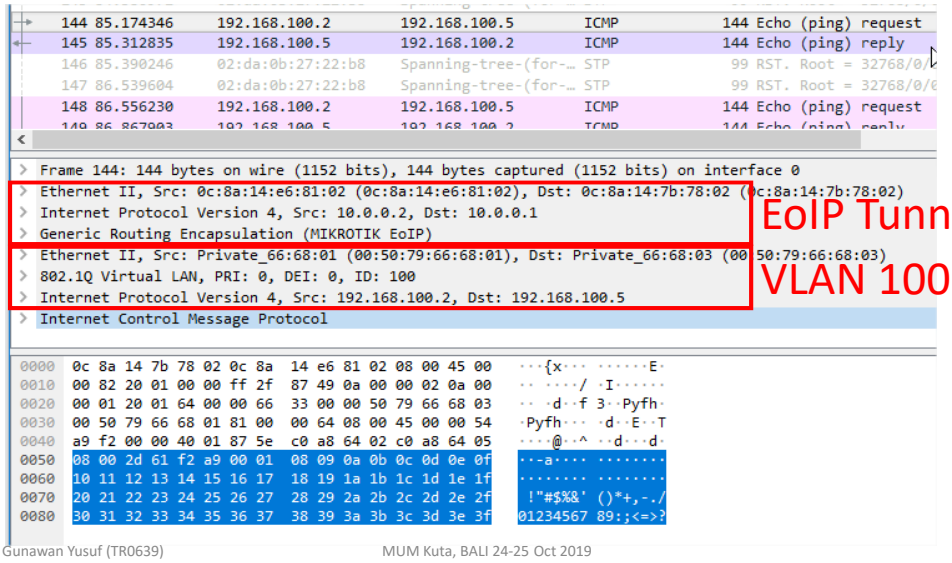


Ping PC2 to PC5

```
PC-2

VPCS is free software, distributed under the terms of the "BSD
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.

Press '?' to get help.

Executing the startup file


PC-2> ip 192.168.100.2 255.255.255.0
Checking for duplicate address...
PC1 : 192.168.100.2 255.255.255.0

PC-2> ping 192.168.100.5
84 bytes from 192.168.100.5 icmp_seq=1 ttl=64 time=180.044 ms
84 bytes from 192.168.100.5 icmp_seq=2 ttl=64 time=312.090 ms
84 bytes from 192.168.100.5 icmp_seq=3 ttl=64 time=393.099 ms
84 bytes from 192.168.100.5 icmp_seq=4 ttl=64 time=328.980 ms
84 bytes from 192.168.100.5 icmp_seq=5 ttl=64 time=292.072 ms

PC-2> ping 192.168.100.5
84 bytes from 192.168.100.5 icmp_seq=1 ttl=64 time=478.124 ms
84 bytes from 192.168.100.5 icmp_seq=2 ttl=64 time=485.125 ms
84 bytes from 192.168.100.5 icmp_seq=3 ttl=64 time=199.051 ms
```

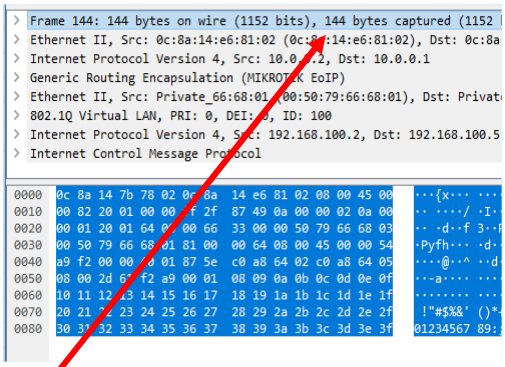
```
PC-5

Welcome to Virtual PC Simulator, version 0.6.1
Dedicated to Daling.
Build time: Jun  1 2015 11:42:32
Copyright (c) 2007-2014, Paul Meng (mirnshi@gmail.com)
All rights reserved.

VPCS is free software, distributed under the terms of the
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.

Press '?' to get help.

Executing the startup file


PC-5> ip 192.168.100.5 255.255.255.0
Checking for duplicate address...
PC1 : 192.168.100.5 255.255.255.0

PC-5>
```

VLAN over EoIP Frame

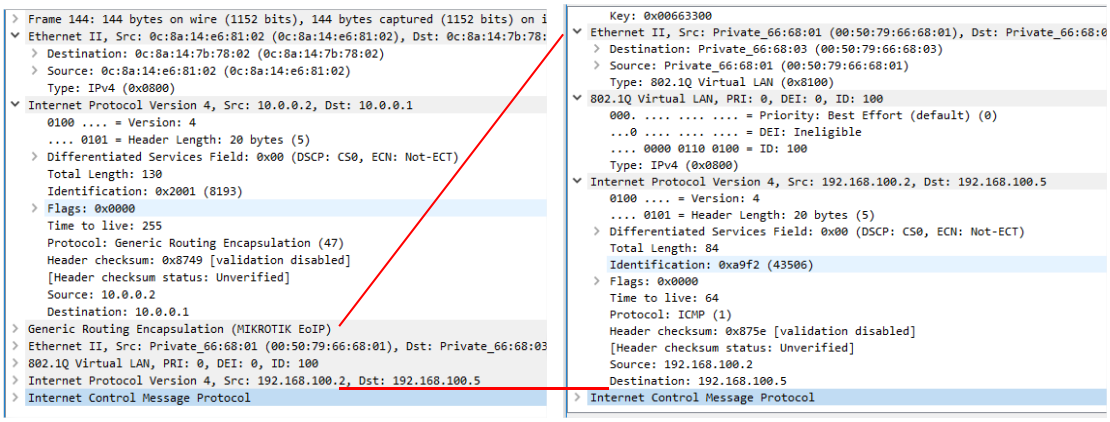


VLAN over EOIP Frame Analysis

- Ping Data (ICMP) = 64 bytes
- IPv4 Inner Header = 20 bytes
- 802.1Q Header = 4 bytes
- Inner Ethernet Header = 14 bytes
- GRE Header = 8 bytes
- IPv4 outer Header = 20 bytes
- Outer Ethernet Header = 14 bytes
- Total frame length = 102 + 42 = 144 bytes



L-2 for EoIP and VLAN Frames

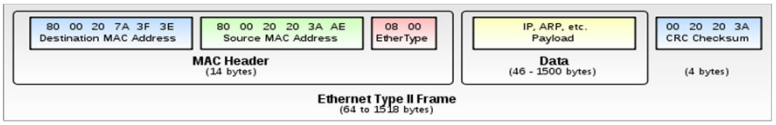


UBAYA
UNIVERSITAS SURABAYA

MikroTik

Conclusion

Conclusion



- For one PING Request (ICMP 84 bytes) the total length L2 Ethernet frame are:
  - Ethernet Standard 98 bytes
  - 802.1Q 102 bytes
  - QinQ 104 bytes
  - PPPoE 82 bytes (ICMP 56)
  - EoIP Tunnel 140 bytes
  - L2TP 140 bytes
  - EoIP over L2TP 182 bytes
  - VLAN over EoIP 144 bytes

- Added bytes in Ethernet frame:
  - Ethernet Standard 0 bytes
  - 802.1Q 4 bytes
  - QinQ 8 bytes (for 2 Vlan)
  - PPPoE 12 bytes (w comp 4B)
  - EoIP Tunnel 42 bytes
  - L2TP 50 bytes (with UDP 8B)
  - EoIP over L2TP 84 bytes
  - VLAN over EoIP 46 bytes

Actual MTU = 1500 – (Added bytes) for L3 MTU

If L3 payload include IP header = 20 bytes, TCP header = 20 bytes then
Maximum Payload (bytes) = Actual MTU – 20 – 20

If total frames size more than Actual MTU link size, the frame will be fragmented by Router (if the protocol can do fragmentation!), so it will take more delay time and more bandwidth for the link.

UBAYA
UNIVERSITAS SURABAYA

MikroTik

Let's discuss it....

Thank you