



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



About Me

(yohanesgunawan@staff.ubaya.ac.id)



- My Name is Yohanes Gunawan Yusuf, from 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



Yohanes Gunawan Yusuf (TR0639)

MUM Kuta, BALI 24-25 Oct 2019

3

3



University of Surabaya (Ubaya)



Yohanes Gunawan Yusuf (TR0639)

MUM Kuta, BALI 24-25 Oct 2019

4

4



Universitas Surabaya (Ubaya)



Yohanes Gunawan Yusuf (TR0639)

MUM Kuta, BALI 24-25 Oct 2019

5

5



Elektro Ubaya (te.ubaya.ac.id)



Yohanes Gunawan Yusuf (TR0639)

MUM Kuta, BALI 24-25 Oct 2019

6

6

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

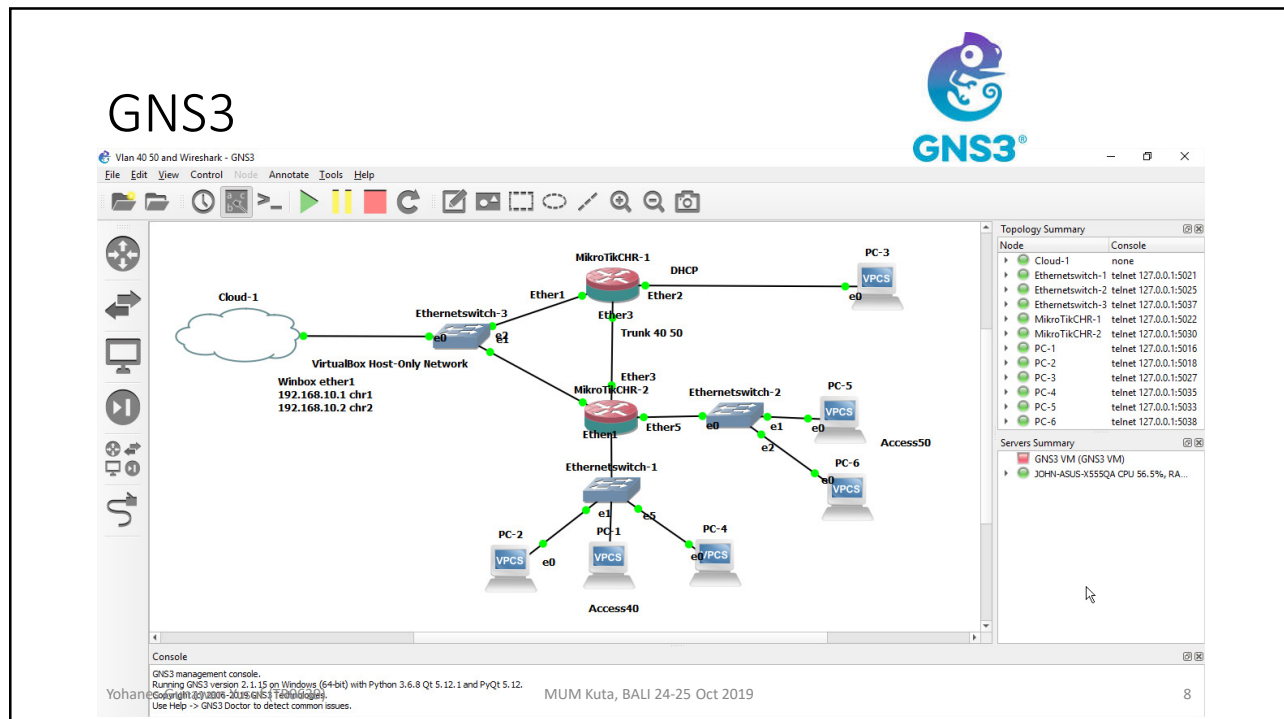


Yohanes Gunawan Yusuf (TR0639)

MUM Kuta, BALI 24-25 Oct 2019

7

7



GNS3

Vlan 40 50 and Wireshark - GNS3

File Edit View Control Node Annotate Tools Help

VirtualBox Host-Only Network

Winbox ether1
192.168.10.1 chr1
192.168.10.2 chr2

Cloud-1

EthernetSwitch-3

MikroTikCHR-1

Ether1

Ether3

DHCP

Ether2

PC-3

VPCS

e0

Trunk 40 50

MikroTikCHR-2

Ether3

Ether5

EthernetSwitch-2

PC-5

VPCS

e0

Access50

PC-6

VPCS

Access40

PC-2

VPCS

PC-1

VPCS

PC-4

VPCS

EthernetSwitch-1

e1

e5

Topology Summary

Node	Console
Cloud-1	none
EthernetSwitch-1	telnet 127.0.0.1:5021
EthernetSwitch-2	telnet 127.0.0.1:5025
EthernetSwitch-3	telnet 127.0.0.1:5037
MikroTikCHR-1	telnet 127.0.0.1:5022
MikroTikCHR-2	telnet 127.0.0.1:5030
PC-1	telnet 127.0.0.1:5016
PC-2	telnet 127.0.0.1:5018
PC-3	telnet 127.0.0.1:5027
PC-4	telnet 127.0.0.1:5035
PC-5	telnet 127.0.0.1:5033
PC-6	telnet 127.0.0.1:5038

Servers Summary

- GNS3 VM (GNS3 VM)
- JCHN-ASUS-X555QA CPU 56.5%, RA...

Console

GNS3 management console.
Running GNS3 version 2.1.15 on Windows (64-bit) with Python 3.6.8 Qt 5.12.1 and PyQt 5.12.
Copyright (c) 2006-2019 GNS3 Technologies.
Use Help -> GNS3 Doctor to detect common issues.

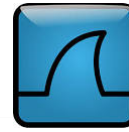
Yohanes Gunawan Yusuf (TR0639)

MUM Kuta, BALI 24-25 Oct 2019

8

8

Wireshark



*Standard input [MikroTikCHR-2 Ether3 to MikroTikCHR-1 Ether3]

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
190	136.137998	192.168.50.254	192.168.20.254	ICMP	102	Echo (ping) request id=0x4c74, seq=5/1280, ttl=64 (reply in 191)
191	136.191915	192.168.20.254	192.168.50.254	ICMP	102	Echo (ping) reply id=0x4c74, seq=5/1280, ttl=63 (request in 190)
192	136.993685	0c:12:8f:8c:66:02	Spanning-tree (for-- STP	57	RST. Root = 32768/0/0c:12:8f:8c:00:04 Cost = 0 Port = 0x8002	
193	136.993639	0c:12:8f:8c:66:02	Spanning-tree (for-- STP	57	RST. Root = 32768/0/0c:12:8f:8c:66:03 Cost = 0 Port = 0x8002	
194	137.506696	0c:12:8f:87:62:02	Private_66:68:03	ARP	46	who has 192.168.50.254? Tell 192.168.50.1
195	137.708684	Private_66:68:03	0c:12:8f:87:62:02	ARP	64	192.168.50.254 is at 00:50:79:66:68:03
196	138.746965	10.0.0.2	255.255.255.255	MNDP	135	5678 + 5678 Len=93
197	138.747398	0c:12:8f:8c:66:02	CDP/VTP/DTP/PagP/UD.. CDP	106	Device ID: CHR 2 Port ID: ether3trunk	
198	138.747776	0c:12:8f:8c:66:02	LLDP_Multicast	LLDP	109	TTL = 120 System Name = CHR 2 System Description = MikroTik RouterOS 6.4
199	138.748548	0.0.0.0	255.255.255.255	MNDP	138	5678 + 5678 Len=92

<

> Frame 194: 46 bytes on wire (368 bits), 46 bytes captured (368 bits) on interface 0
 > Ethernet II, Src: 0c:12:8f:87:62:02 (0c:12:8f:87:62:02), Dst: Private_66:68:03 (00:50:79:66:68:03)

Virtual LAN, PRI: 0, DEI: 0, ID: 50
 000. = Priority: Best Effort (default) (0)
 ...0 = DEI: Ineligible
 ... 0000 0011 0010 = ID: 50
 Type: ARP (0x0806)

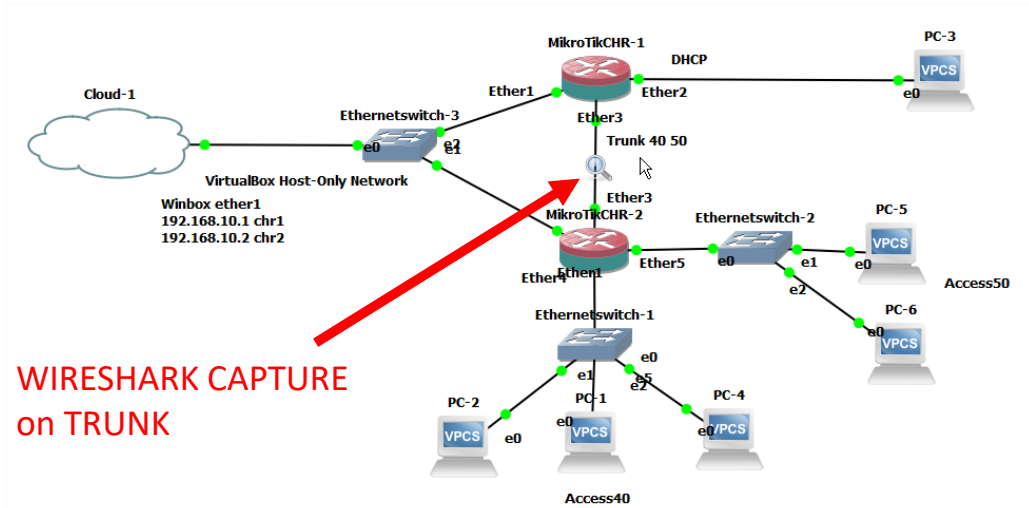
Address Resolution Protocol (request)
 Hardware type: Ethernet (1)
 Protocol type: IPv4 (0x0800)
 Hardware size: 6
 Protocol size: 4

0000 00 50 79 66 68 03 0c 12 8f 87 62 02 81 00 00 32 Pyfh... ..b....2
 0010 00 06 00 01 00 00 06 04 00 01 0c 12 8f 87 62 02b-
 0020 c0 a8 32 01 00 00 00 00 00 c0 a8 32 fe ..2.....-2-

Yohanes Gunawan Yusuf (TR0639) MUM Kuta, BALI 24-25 Oct 2019 9

9

GNS3 and Wireshark



10

Frames to be analysed

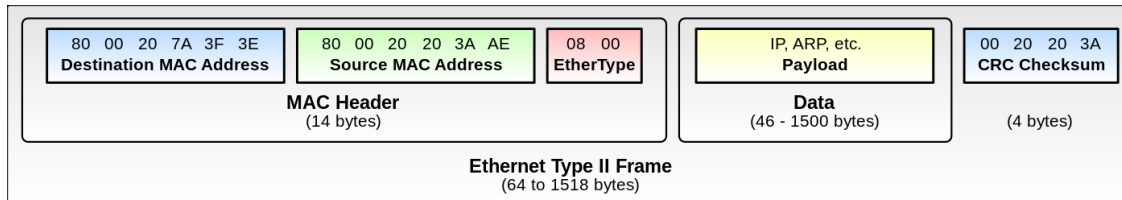
- Ethernet Standard
- VLAN (802.1Q)
- VLAN in VLAN (QinQ)
- PPPoE
- EoIP
- L2TP
- Tunnel in Tunnel
(EoIP o L2TP and VLAN o EoIP)

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

13

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)

14

Ethernet Standard IPv4 Frame (0x0800)

```

> Frame 5: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
✓ Ethernet II, Src: Private_66:68:02 (00:50:79:66:68:02), Dst: 0c:12:8f:87:62:01 (0c:12:8f:87:62:01)
  > Destination: 0c:12:8f:87:62:01 (0c:12:8f:87:62:01)
  > Source: Private_66:68:02 (00:50:79:66:68:02)
  > Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.168.20.254, Dst: 192.168.20.1
> Internet Control Message Protocol

```

Header 14 bytes

IPv4 20 + ICMP 64

```

0000  0c 12 8f 87 62 01 00 50 79 66 68 02 08 00 45 00  ...b..P yfh...E-
0010  00 54 17 50 00 00 40 01 d9 08 c0 a8 14 1e c0 a8  ..T.P..@. ....
0020  14 01 08 00 cf 11 50 f7 00 03 08 09 0a 0b 0c 0d  ....P. ....
0030  0e 0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d  ....
0040  1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d  .. !"#%&'()*+,-
0050  2e 2f 30 31 32 33 34 35 36 37 38 39 3a 3b 3c 3d  ./012345 6789:;<=
0060  3e 3f                                     >>
Yohanes Gunawan Yusuf (TR0639)                MUM Kuta, BALI 24-25 Oct 2019                15

```

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

```

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

```

```

> Frame 5: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) o
✓ Ethernet II, Src: Private_66:68:02 (00:50:79:66:68:02), Dst: 0c:12:8
  > Destination: 0c:12:8f:87:62:01 (0c:12:8f:87:62:01)
  > Source: Private_66:68:02 (00:50:79:66:68:02)
  > Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.168.20.254, Dst: 192.168.20.1
> Internet Control Message Protocol

```

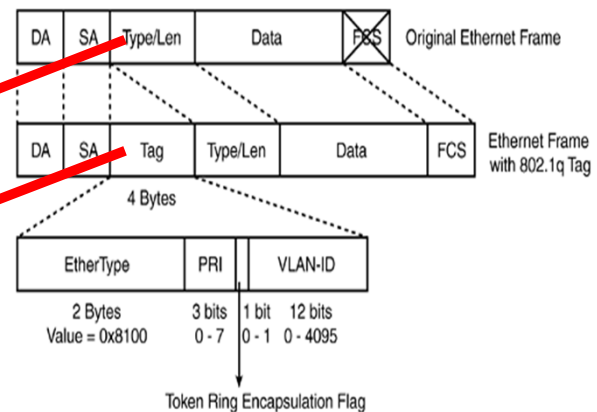
16

VLAN (802.1Q) Frame

17

Ethernet Type (Standard vs VLAN)

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



18

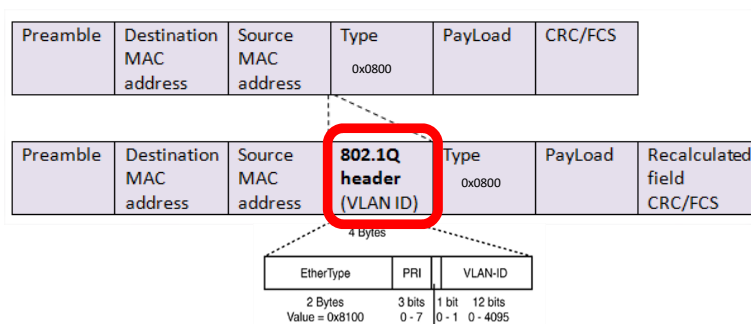
How VLAN work ?

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

19

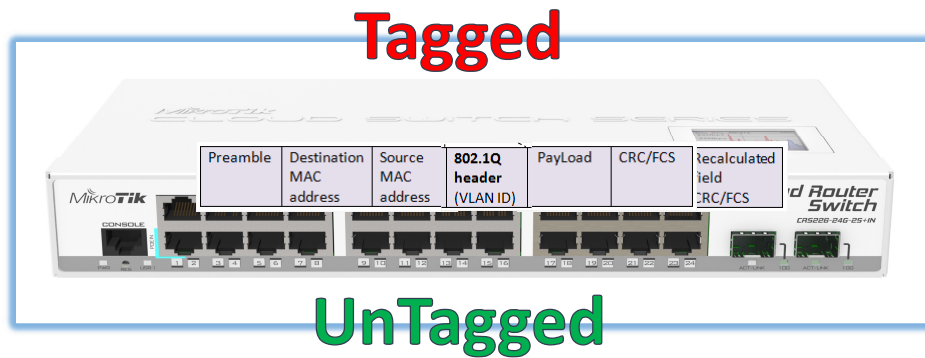
IEEE 802.1Q

- 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)

Yohanes Gunawan Yusuf (TR0639)

MUM Kuta, BALI 24-25 Oct 2019

21

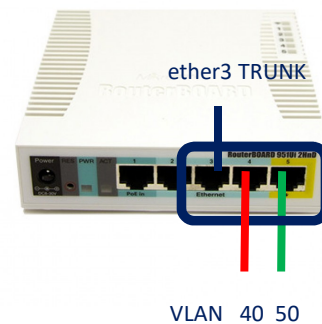
21

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

```



Yohanes Gunawan Yusuf (TR0639)

MUM Kuta, BALI 24-25 Oct 2019

22

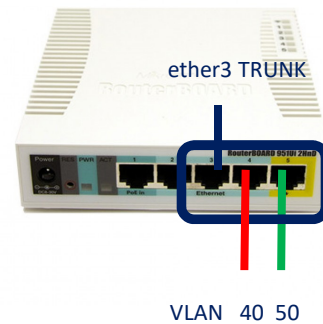
22

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

```



Yohanes Gunawan Yusuf (TR0639)

MUM Kuta, BALI 24-25 Oct 2019

23

23

Trunk (ether3) and DHCP Server on CHR1

Address	Network	Interface
192.168.10.1/24	192.168.10.0	ether1
192.168.10.254/24	192.168.10.0	ether1
192.168.20.1/24	192.168.20.0	ether2
10.0.0.1/30	10.0.0.0	ether3trunk
192.168.40.1/24	192.168.40.0	vlan40-eth3
192.168.50.1/24	192.168.50.0	vlan50-eth3

Interface	Interface List	Ethernet	EoIP Tunnel	IP Tunnel	GRE
R	ether1	Ethernet			
R	ether2	Ethernet			
R	ether3trunk	Ethernet			
R	vlan40-eth3	VLAN			
R	vlan50-eth3	VLAN			
R	ether4	Ethernet			
R	ether5	Ethernet			

Name	Interface	Relay	Lease Time
dhcp1	ether2		00:10:00 dhcp_pool0
dhcp2	vlan40-eth3		00:10:00 dhcp_pool1
dhcp3	vlan50-eth3		00:10:00 dhcp_pool2

Yohanes Gunawan Yusuf (TR0639)

MUM Kuta, BALI 24-25 Oct 2019

24

24

Trunk (ether3) and Access on CHR 2

The screenshot displays the Mikrotik WinBox configuration interface for a CHR 2 device. The 'Address List' window is open, showing two entries: 10.0.0.2/30 on interface ether3trunk and 192.168.10.2/24 on interface ether1. The 'Interface List' window shows a list of interfaces including bridge1a40, bridge2a50, ether1-5, and vlans. The 'Bridge' window shows a bridge configuration with ports ether4, ether5, and vlans40eth3, 50eth3.

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 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-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> █

```

Yohanes Gunawan Yusuf (TR0639)

MUM Kuta, BALI 24-25 Oct 2019

26

26

VLAN (802.1Q) Tag

```

    > Frame 179: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface 0
    > Ethernet II, Src: Private_66:68:03 (00:50:79:66:68:03), Dst: 0c:ae:62:9d:f3:02 (0c:ae:62:9d:f3:02)
    > Destination: 0c:ae:62:9d:f3:02 (0c:ae:62:9d:f3:02)
    > Source: Private_66:68:03 (00:50:79:66:68:03)
    Type: 802.1Q Virtual LAN (0x8100)
    > 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 50
    000. .... = Priority: Best Effort (default) (0)
    ...0 .... = DEI: Ineligible
    ... 0000 0011 0010 = ID: 50
    Type: IPv4 (0x0800)
    > Internet Protocol Version 4, Src: 192.168.50.254, Dst: 192.168.20.254
    > Internet Control Message Protocol
  
```

14 bytes

4 bytes

IPv4 20 + ICMP 64

0000	0c ae 9d f3 02 00 50 79 66 68 03 81 00 00 32	..b...P yfh...2
0010	08 00 45 00 00 54 0f c1 00 00 40 01 a1 9b c0 a8	..E..T...@.....
0020	32 fe c0 a8 14 fe 08 00 5d fb c2 0f 00 01 08 09	2.....].....
0030	0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 17 18 19
0040	1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 ! "#\$%&'()
0050	2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 36 37 38 39	*+,-./01 23456789

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

```

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
  
```

```

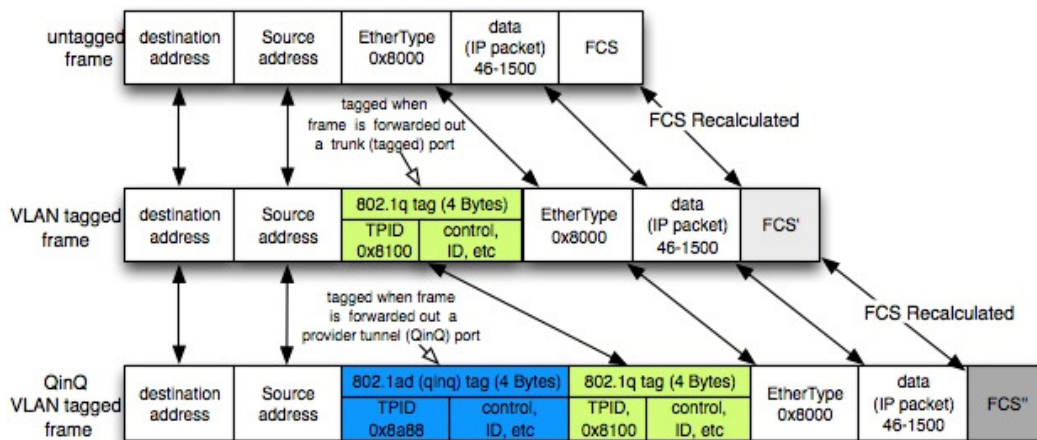
    > Frame 179: 102 bytes on wire (816 bits), 102 bytes captured
    > Ethernet II, Src: Private_66:68:03 (00:50:79:66:68:03), Dst:
    > 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 50
    > Internet Protocol Version 4, Src: 192.168.50.254, Dst: 192.1
    > Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x5dfb [correct]
    [Checksum Status: Good]
    Identifier (BE): 49679 (0xc20f)
    Identifier (LE): 4034 (0x0fc2)
    Sequence number (BE): 1 (0x0001)
    Sequence number (LE): 256 (0x0100)
    [Response frame: 184]
    > Data (56 bytes)
  
```

30

VLAN in VLAN (QinQ) Frame

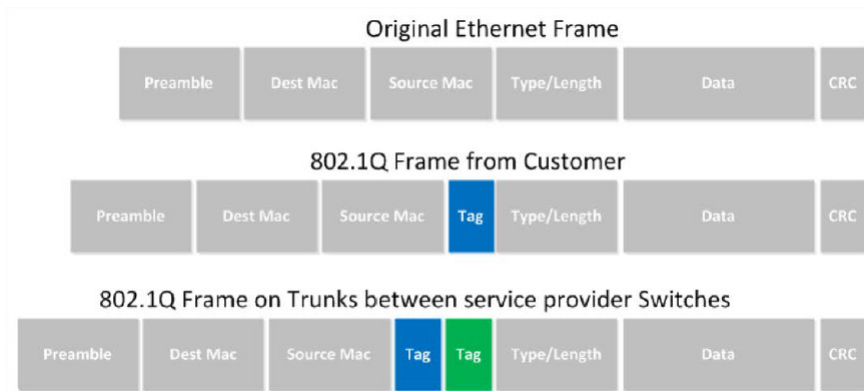
31

IEEE 802.1ad



32

QinQ @ MikroTik



Yohanes Gunawan Yusuf (TR0639)

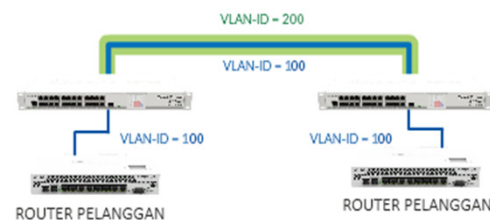
MUM Kuta, BALI 24-25 Oct 2019

33

33

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)



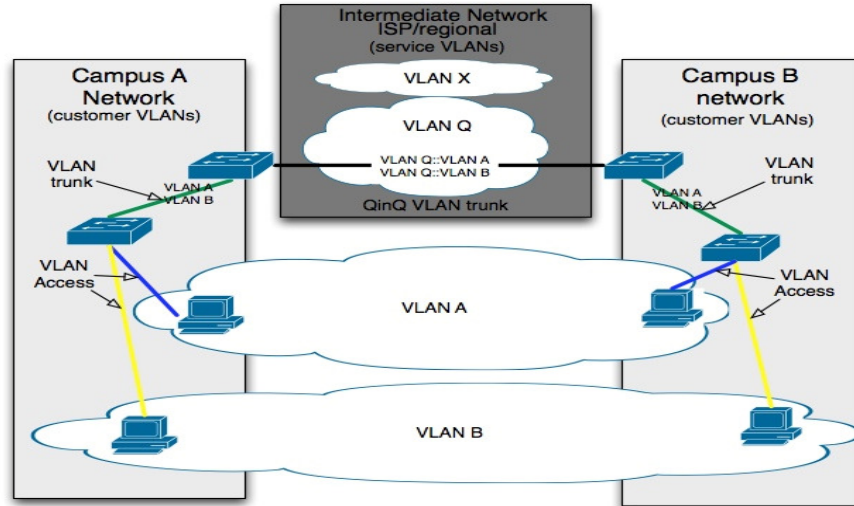
Yohanes Gunawan Yusuf (TR0639)

MUM Kuta, BALI 24-25 Oct 2019

34

34

QinQ Implementation

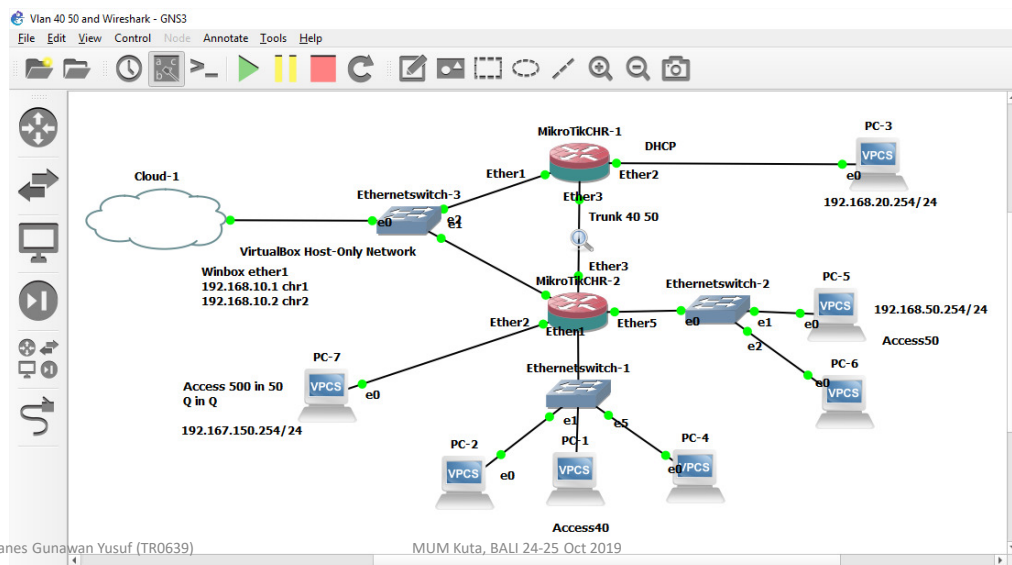


Yohanes Gunawan Yusuf (TR0639) MUM Kuta, BALI 24-25 Oct 2019
 Source -> <https://groups.geni.net/geni/wiki/QinqResults>

35

35

QinQ Simulation on GNS3 (Vlan 500 in 50)

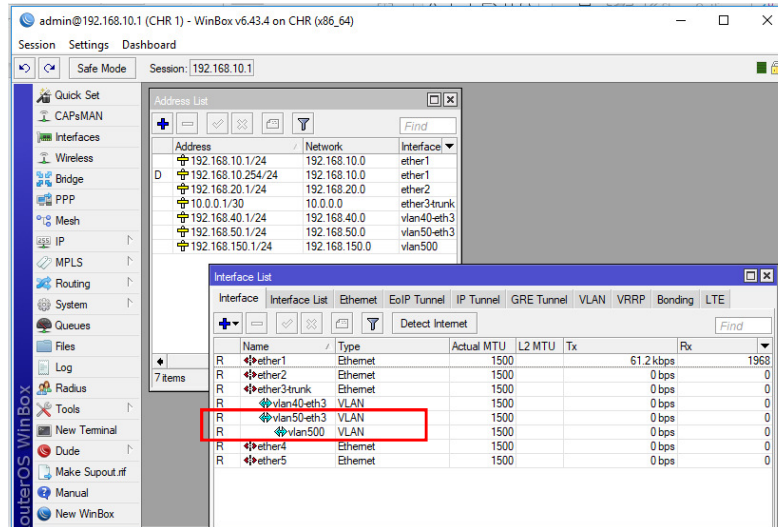


Yohanes Gunawan Yusuf (TR0639) MUM Kuta, BALI 24-25 Oct 2019

36

36

Setting QinQ (Access 500 in 50) CHR1



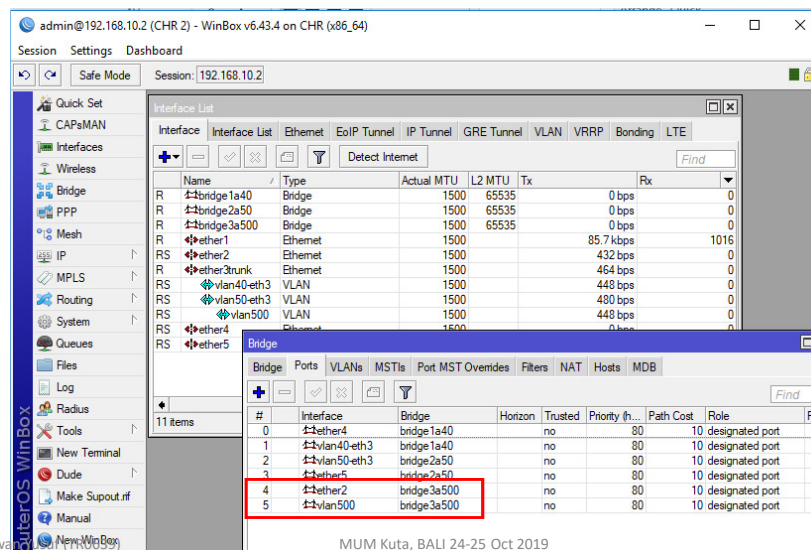
Yohanes Gunawan Yusuf (TR0639)

MUM Kuta, BALI 24-25 Oct 2019

37

37

Access 500 on CHR2 (Ether2)



Yohanes Gunawan Yusuf (TR0639)

MUM Kuta, BALI 24-25 Oct 2019

38

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> █
```

Yohanes Gunawan Yusuf (TR0639)

MUM Kuta, BALI 24-25 Oct 2019

39

39

The image shows a Wireshark packet capture of an ICMP ping. The packet list pane shows frame 517: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface 0. The packet details pane shows Ethernet II, Src: Private_66:68:06 (00:50:79:66:68:06), Dst: 0c:12:8f:87:62:02 (0c:12:8f:87:62:02). The 802.1Q Virtual LAN section is expanded, showing two entries: one for ID 50 (Priority: Best Effort, DEI: Ineligible) and one for ID 500 (Priority: Best Effort, DEI: Ineligible). Red boxes highlight these two entries with the text "4 bytes (Id 50)" and "4 bytes (Id 500)". The packet bytes pane shows the raw data, with a red arrow pointing to the 4-byte QoS field at offset 12.

Yohanes Gunawan Yusuf (TR0639)

MUM Kuta, BALI 24-25 Oct 2019

40

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

```
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> []
```

```
> Frame 517: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on
> Ethernet II, Src: Private_66:68:06 (08:00:79:66:68:06), Dst: 0c:12:8f:87
  802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 50
    000. .... = Priority: Best Effort (default) (0)
    ...0 .... = DEI: Ineligible
    ....0000 0011 0010 = ID: 50
    Type: 802.1Q Virtual LAN (0x8100)
  802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 500
    000. .... = Priority: Best Effort (default) (0)
    ...0 .... = DEI: Ineligible
    ....0001 1111 0100 = ID: 500
    Type: IPv4 (0x0800)
  Internet Protocol Version 4, Src: 192.168.150.254, Dst: 192.168.20.254
```

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

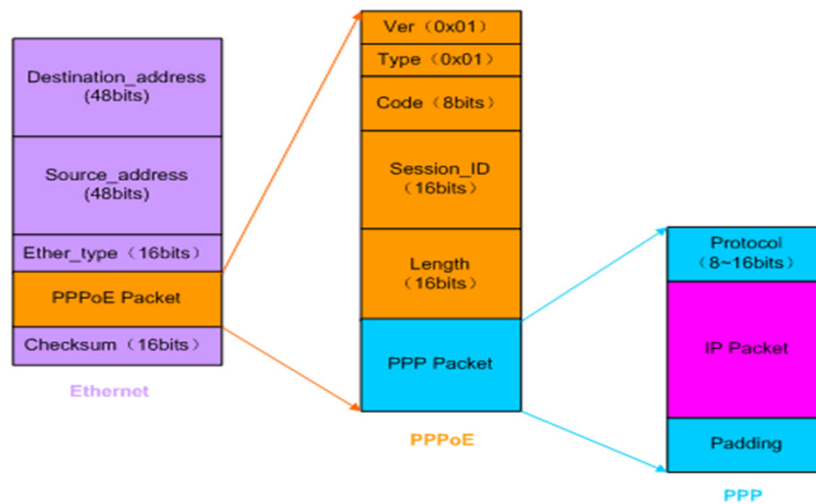
PPPoE Frame

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

43

PPPoE Frame

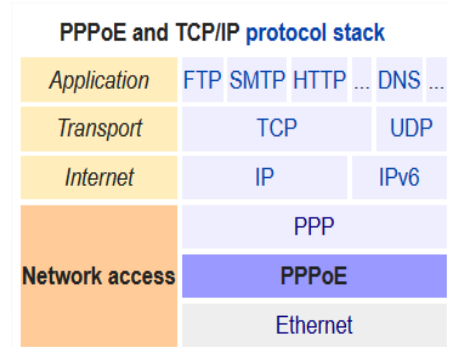
(source: www.h3c.com.hk)



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



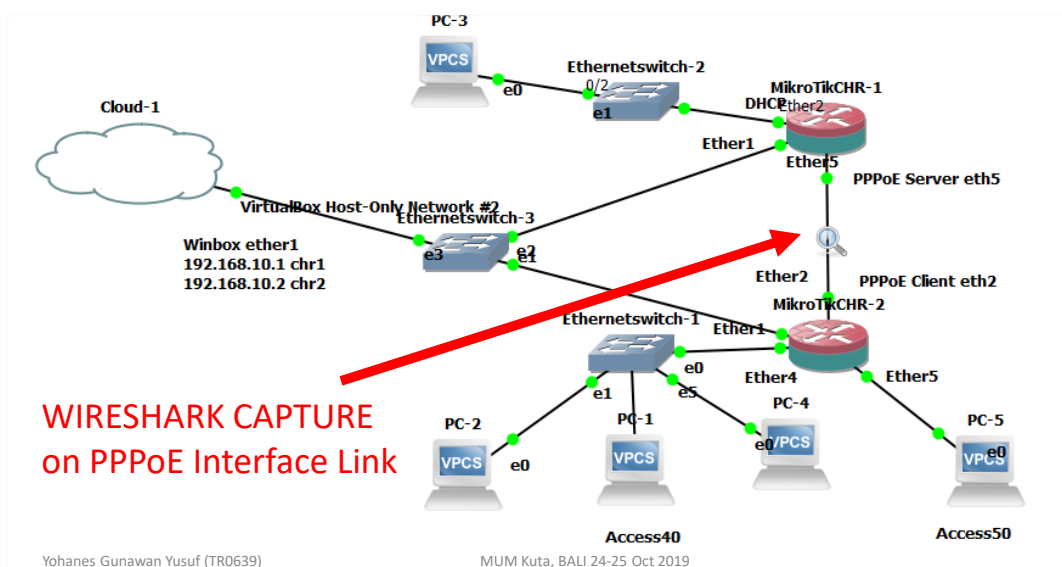
Yohanes Gunawan Yusuf (TR0639)

MUM Kuta, BALI 24-25 Oct 2019

45

45

PPPoE Server and Client



Yohanes Gunawan Yusuf (TR0639)

MUM Kuta, BALI 24-25 Oct 2019

46

46

PPPoE Setting

The screenshot displays two instances of WinBox v6.43.4. The top instance is at IP 192.168.10.1 and shows the 'PPP Secret' configuration window for 'user1'. The bottom instance is at IP 192.168.10.2 and shows the 'PPP' configuration window with a table of active connections.

Name	Type	Actual MTU	L2 MTU	Tx	Rx
pppoe-out1	PPPoE Client	1480		0 bps	0 bps

Yohanes Gunawan Yusuf (TR0639)

MUM Kuta, BALI 24-25 Oct 2019

47

47

Ping from PPPoE Client to Server

```

0 1.1.1.1          56 64 166ms
1 1.1.1.1          56 64 183ms
2 1.1.1.1          56 64 292ms
sent=3 received=3 packet-loss=0% min-rtt=166ms avg-rtt=213ms max-rtt=292ms

[admin@CHR 2] > ping 1.1.1.1
SEQ HOST          SIZE TTL TIME STATUS
0 1.1.1.1          56 64 235ms
1 1.1.1.1          56 64 264ms
2 1.1.1.1          56 64 294ms
3 1.1.1.1          56 64 211ms
4 1.1.1.1          56 64 363ms
5 1.1.1.1          56 64 312ms
6 1.1.1.1          56 64 336ms

```

Yohanes Gunawan Yusuf (TR0639)

MUM Kuta, BALI 24-25 Oct 2019

48

48

Ethernet with PPPoE Session Frame (0x8864)

- PPP Datagram (Compressed 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

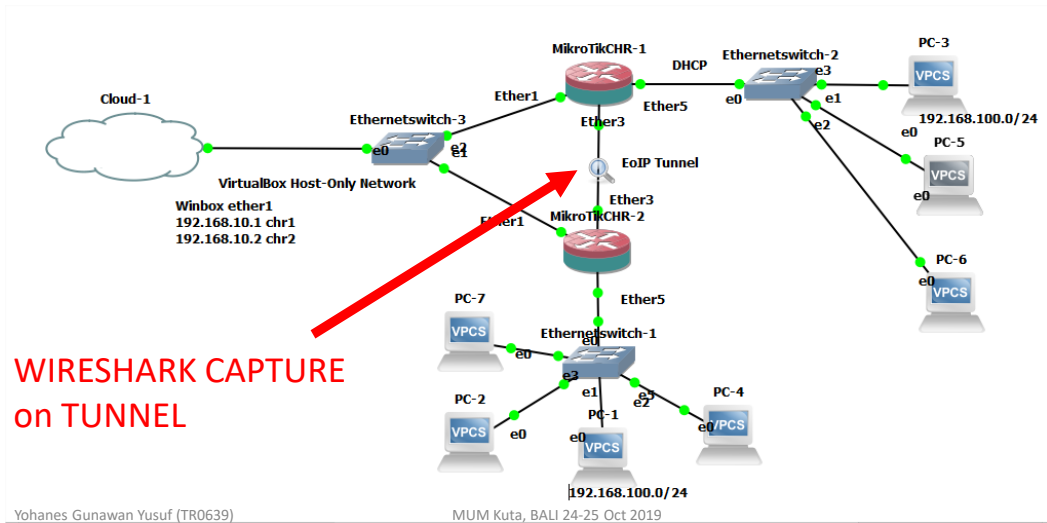
Wireshark packet capture analysis showing the structure of a PPPoE session frame. The frame is 82 bytes on wire. The components are:

- Ethernet II Header: 14 bytes
- PPPoE Session: 6 bytes
- Point-to-Point Protocol: 2 bytes
- PPP Compressed Datagram: 60 bytes



EoIP Tunnel Frame

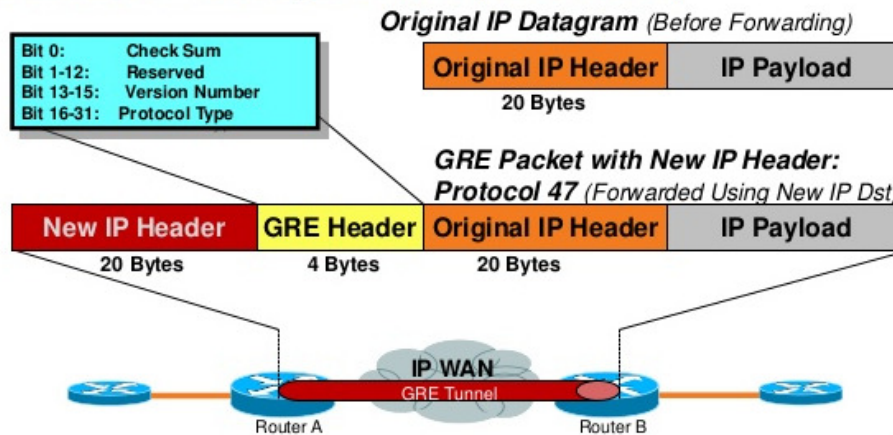
EoIP Tunnel



51

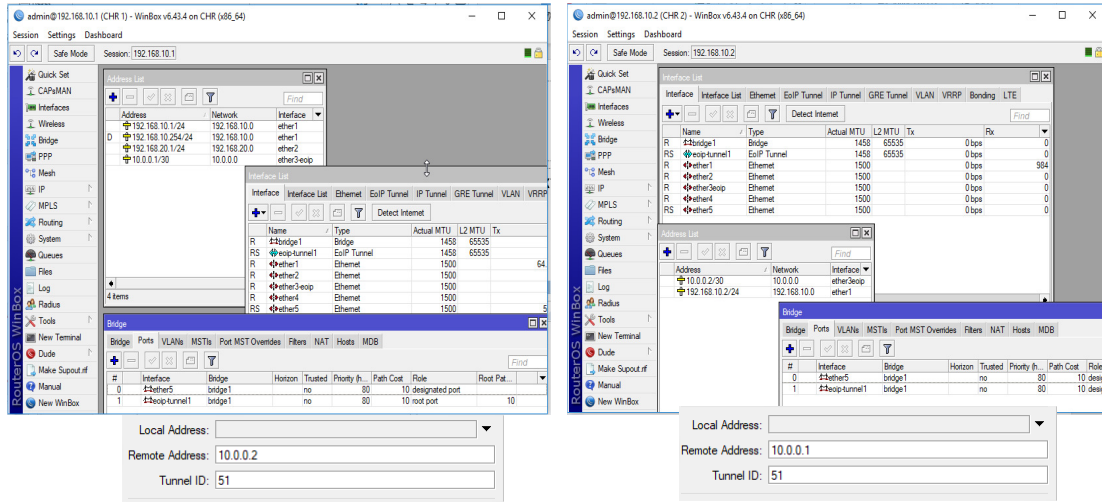
EoIP Frame (Using GRE Protocol)

GRE Tunnel Encapsulation (RFC 2784)



52

EoIP Setting



Yohanes Gunawan Yusuf (TR0639)

MUM Kuta, BALI 24-25 Oct 2019

53

53

Ping PC1 to PC5 thru EoIP Tunnel

```

PC-1> address [mask] [gateway]
address [gateway] [mask]
Set the VPC's ip, default gateway ip and network
Default IPv4 mask is /24, IPv6 is /64. Example:
ip 10.1.1.70/26 10.1.1.65 set the VPC's ip to 10
the gateway to 10.1.1.65, the netmask to 255.255
In tap mode, the ip of the tapx is the maximum h
of the subnet. In the example above the tapx ip
10.1.1.126
mask may be written as /26, 26 or 255.255.255.19
Attempt to obtain IPv6 address, mask and gateway
dhcp [OPTION] Attempt to obtain IPv4 address, mask, gateway, D
-d Show DHCP packet decode
-r Renew DHCP lease
-x Release DHCP lease
dns ip Set DNS server ip, delete if ip is '0'
domain NAME Set local domain name to NAME

PC-1> ip 192.168.100.1 255.255.255.0
Checking for duplicate address...
PC1 : 192.168.100.1 255.255.255.0

PC-1> ping 192.168.100.5
84 bytes from 192.168.100.5 icmp_seq=1 ttl=64 time=539.038 ms
84 bytes from 192.168.100.5 icmp_seq=2 ttl=64 time=430.110 ms
84 bytes from 192.168.100.5 icmp_seq=3 ttl=64 time=301.076 ms
84 bytes from 192.168.100.5 icmp_seq=4 ttl=64 time=376.095 ms
84 bytes from 192.168.100.5 icmp_seq=5 ttl=64 time=321.083 ms
    
```

```

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> ping 192.168.100.1
84 bytes from 192.168.100.1 icmp_seq=1 ttl=64 time=539.038 ms
84 bytes from 192.168.100.1 icmp_seq=2 ttl=64 time=430.110 ms
84 bytes from 192.168.100.1 icmp_seq=3 ttl=64 time=301.076 ms
84 bytes from 192.168.100.1 icmp_seq=4 ttl=64 time=376.095 ms
84 bytes from 192.168.100.1 icmp_seq=5 ttl=64 time=321.083 ms
    
```

Yohanes Gunawan Yusuf (TR0639)

MUM Kuta, BALI 24-25 Oct 2019

54

54

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

Local Address:

Remote Address:

Tunnel ID:

- Tunnel ID = 51 = 0x00003300

Standard input [MikroTikCHR-2 Ether3 to MikroTikCHR-1 Ether3]

No.	Time	Source	Destination	Protocol	Length	Info
88	05.564901	02:e1:6e:8a:8a:3b	Spanning-tree-(for... STP	95	RST	Root = 32768/0/0c:38:84:9a:44:02
89	07.315143	0c:38:84:9a:44:02	0c:38:84:a3:5f:02	ARP	42	Who has 10.0.0.1? Tell 10.0.0.2
90	07.413886	0c:38:84:a3:5f:02	0c:38:84:9a:44:02	ARP	42	10.0.0.1 is at 0c:38:84:a3:5f:02
91	07.699259	02:e1:6e:8a:8a:3b	Spanning-tree-(for... STP	95	RST	Root = 32768/0/0c:38:84:9a:44:02
92	09.793942	02:e1:6e:8a:8a:3b	Spanning-tree-(for... STP	95	RST	Root = 32768/0/0c:38:84:9a:44:02
93	09.793988	02:e1:6e:8a:8a:3b	Spanning-tree-(for... STP	95	RST	Root = 32768/0/0c:38:84:9a:44:02
94	93.971107	02:e1:6e:8a:8a:3b	Spanning-tree-(for... STP	95	RST	Root = 32768/0/0c:38:84:9a:44:02
95	94.244620	10.0.0.2	10.0.0.1	GRE	42	Encapsulated MIKROTIK EoIP
96	95.000279	10.0.0.1	10.0.0.2	GRE	42	Encapsulated MIKROTIK EoIP

Frame 95: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0

Ethernet II, Src: 0c:38:84:9a:44:02 (0c:38:84:9a:44:02), Dst: 0c:38:84:a3:5f:02 (0c:38:84:a3:5f:02)

Internet Protocol Version 4, Src: 10.0.0.2, Dst: 10.0.0.1

Generic Routing Encapsulation (MIKROTIK EoIP)

Flags and Version: 0x2001

Protocol Type: MIKROTIK EoIP (0x6400)

Key: 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

```
PC-1> ping 192.168.100.5
84 bytes from 192.168.100.5 icmp_seq=1 ttl=64 time=539.038 ms
84 bytes from 192.168.100.5 icmp_seq=2 ttl=64 time=430.110 ms
84 bytes from 192.168.100.5 icmp_seq=3 ttl=64 time=301.076 ms
84 bytes from 192.168.100.5 icmp_seq=4 ttl=64 time=376.095 ms
84 bytes from 192.168.100.5 icmp_seq=5 ttl=64 time=321.083 ms
```

Frame 109: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0

Ethernet II, Src: 0c:38:84:a3:5f:02 (0c:38:84:a3:5f:02), Dst: 0c:38:84:9a:44:02 (0c:38:84:9a:44:02)

Internet Protocol Version 4, Src: 10.0.0.1, Dst: 10.0.0.2

Generic Routing Encapsulation (MIKROTIK EoIP)

Ethernet II, Src: Private_66:68:03 (00:50:79:66:68:03), Dst: Private_66:68:03 (00:50:79:66:68:03)

Internet Protocol Version 4, Src: 192.168.100.5, Dst: 192.168.100.1

Internet Control Message Protocol

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	Spamming-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

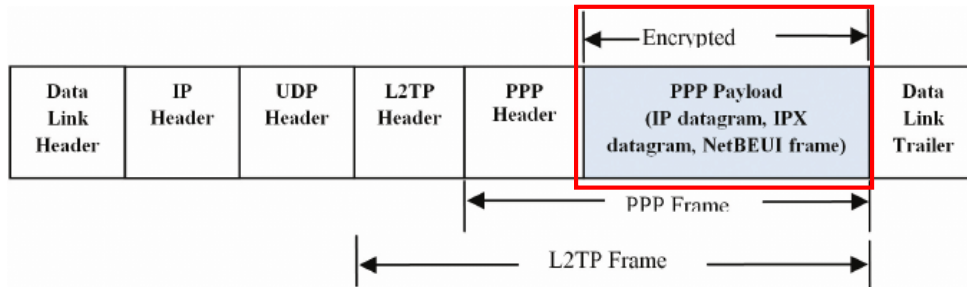
- ARP Request = 28 bytes
- Inner Ethernet Header = 14 bytes
- Inner Ethernet Trailer = 22 bytes
- Total ARP = 28 + 14 + 22 = 64 bytes
- GRE (MikroTik EoIP) = 8 bytes
- Outer IP Header = 20 bytes
- Outer Ethernet Header = 14 bytes
- EoIP Tunnel = 14+ 8+ 20 = 42 bytes
- Total EoIP ARP Frame = EoIP Tunnel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

```

> Frame 103: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interf
> Ethernet II, Src: 0c:38:84:9a:44:02 (0c:38:84:9a:44:02), Dst: 0c:38:84:a3:5f:02
> Internet Protocol Version 4, Src: 10.0.0.2, Dst: 10.0.0.1
> Generic Routing Encapsulation (MIKROTIK EoIP)
  > Ethernet II, Src: Private_66:68:00 (00:50:79:66:68:00), Dst: Broadcast (ff:ff:ff
    > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
    > Source: Private_66:68:00 (00:50:79:66:68:00)
    > Type: ARP (0x0806)
    > Trailer: 0000000000000000000000000000000000000000000000000000000000000000
  > Address Resolution Protocol (request)
    > Hardware type: Ethernet (1)
    > Protocol type: IPv4 (0x0000)
    > Hardware size: 6
0000  0c 38 84 a3 5f 02 0c 38 84 9a 44 02 08 00 45 00  .8...8..D...E
0010  00 5c 2b 01 00 00 ff 2f 7c 6f 0a 00 00 02 0a 00  .\+.../|o....
0020  00 01 20 01 64 00 00 40 33 00 ff ff ff ff ff ff  ...d@3:.....
0030  00 50 79 66 68 00 08 06 00 01 08 00 06 04 00 01  .Pyfh.....
0040  00 50 79 66 68 00 c0 a8 64 01 ff ff ff ff ff ff  .Pyfh...d...
0050  c0 a8 64 05 00 00 00 00 00 00 00 00 00 00 00  .d.....
0060  00 00 00 00 00 00 00 00 00 00
  
```

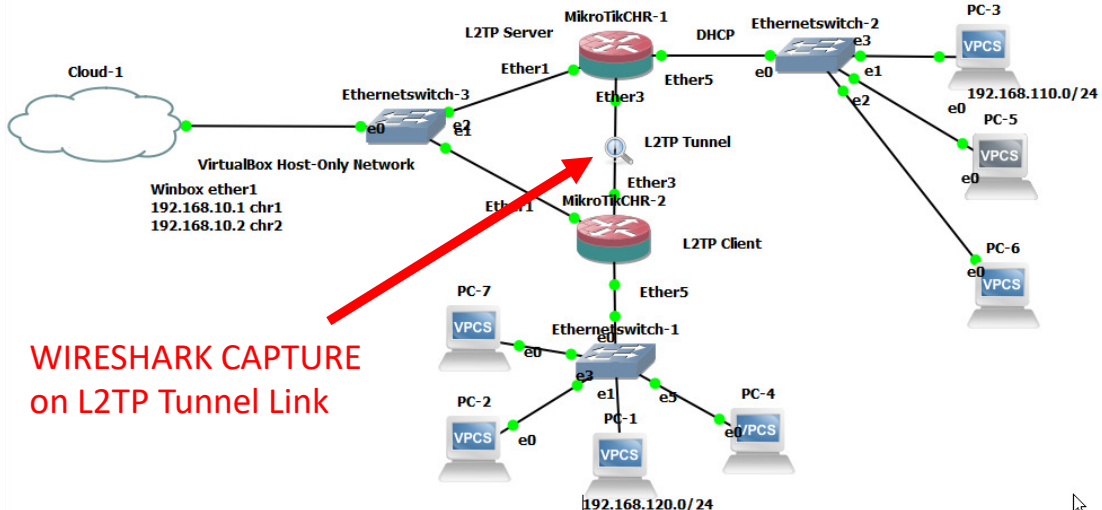
L2TP Tunnel Frame

L2TP Frame Format (use PPP packet frame)



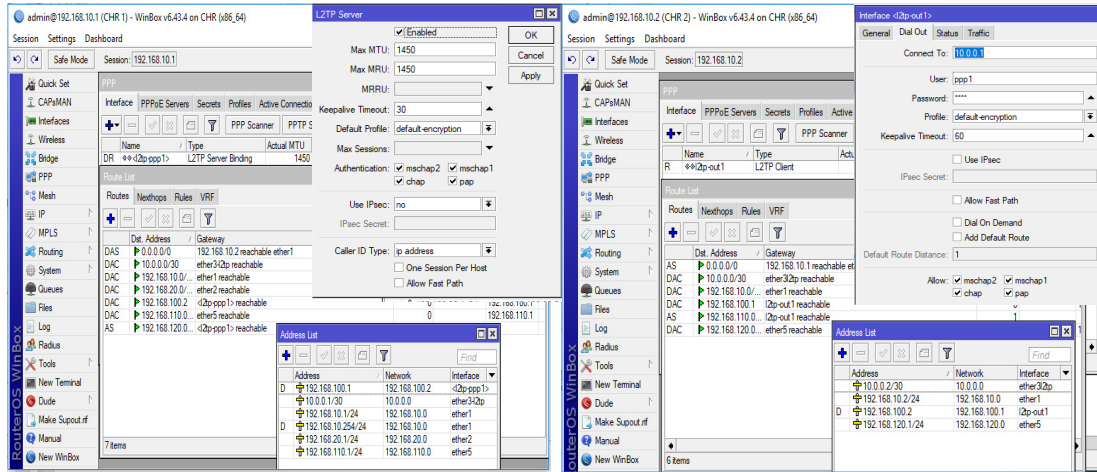
61

L2TP



62

L2TP – Server and Client (No IPsec)



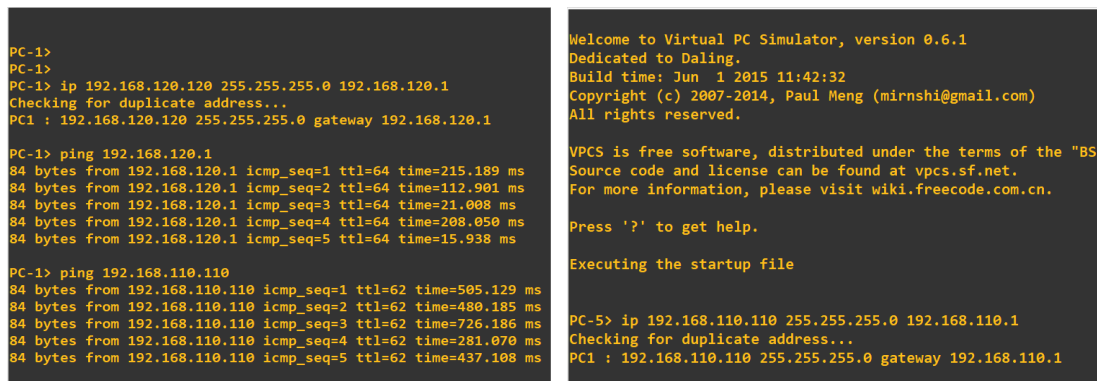
Yohanes Gunawan Yusuf (TR0639)

MUM Kuta, BALI 24-25 Oct 2019

63

63

Ping PC1 to PC5



Yohanes Gunawan Yusuf (TR0639)

MUM Kuta, BALI 24-25 Oct 2019

64

64

L2TP Tunnel Setup

Wireshark L2TP.pcapng [MikroTikCHR-2 Ether3 to MikroTikCHR-1 Ether3]

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.0.2	10.0.0.1	L2TP	62	Control Message - Hello (tunnel id=1, session id=0)
2	0.200517	10.0.0.1	10.0.0.2	L2TP	94	Control Message - ZLB (tunnel id=1, session id=0)
3	1.366214	10.0.0.1	10.0.0.2	L2TP	62	Control Message - Hello (tunnel id=1, session id=0)
4	1.528226	10.0.0.2	10.0.0.1	L2TP	94	Control Message - ZLB (tunnel id=1, session id=0)
5	4.517910	10.0.0.1	255.255.255.255	MNDP	135	5678 → 5678 Len=93
6	4.518384	0c:f0:c9:b0:e7:02		CDP/VTP/DTP/PAP/UD...	106	Device ID: CHR 1 Port ID: ether3-l2tp
7	4.519536	0c:f0:c9:b0:e7:02		LLDP_Multicast	109	TTL = 120 System Name = CHR 1 System Description = MikroTik RouterOS 6
8	6.504560	0c:f0:c9:f7:2a:02	0c:f0:c9:b0:e7:02	ARP	42	Who has 10.0.0.1? Tell 10.0.0.2
9	6.665338	0c:f0:c9:b0:e7:02	0c:f0:c9:f7:2a:02	ARP	42	10.0.0.1 is at 0c:f0:c9:b0:e7:02
10	10.661110	10.0.0.1	10.0.0.2	PPP LCP	60	Echo Request

Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface 0
 Ethernet II, Src: 0c:f0:c9:f7:2a:02 (0c:f0:c9:f7:2a:02), Dst: 0c:f0:c9:b0:e7:02 (0c:f0:c9:b0:e7:02)
 Internet Protocol Version 4, Src: 10.0.0.2, Dst: 10.0.0.1
 User Datagram Protocol, Src Port: 1701, Dst Port: 1701
 Layer 2 Tunneling Protocol
 Packet Type: Control Message Tunnel Id=1 Session Id=0
 Length: 20
 Tunnel ID: 1
 Session ID: 0
 Ns: 18
 Nr: 16
 Control Message AVP

Yohanes Gunawan Yusuf (TR0639)

MUM Kuta, BALI 24-25 Oct 2019

65

65

L2TP – LCP (link Control Protocol)

8	6.504560	0c:f0:c9:f7:2a:02	0c:f0:c9:b0:e7:02	ARP	42	Who has 10.0.0.1? Tell 10.0.0.2
9	6.665338	0c:f0:c9:b0:e7:02	0c:f0:c9:f7:2a:02	ARP	42	10.0.0.1 is at 0c:f0:c9:b0:e7:02
10	10.661110	10.0.0.1	10.0.0.2	PPP LCP	60	Echo Request
11	10.716158	10.0.0.2	10.0.0.1	PPP LCP	60	Echo Reply
12	19.982941	0c:f0:c9:b0:e7:02	0c:f0:c9:f7:2a:02	ARP	42	Who has 10.0.0.2? Tell 10.0.0.1

Frame 10: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
 Ethernet II, Src: 0c:f0:c9:b0:e7:02 (0c:f0:c9:b0:e7:02), Dst: 0c:f0:c9:f7:2a:02 (0c:f0:c9:f7:2a:02)
 Internet Protocol Version 4, Src: 10.0.0.1, Dst: 10.0.0.2
 User Datagram Protocol, Src Port: 1701, Dst Port: 1701
 Layer 2 Tunneling Protocol
 Packet Type: Data Message Tunnel Id=1 Session Id=1
 Tunnel ID: 1
 Session ID: 1
 Point-to-Point Protocol
 Address: 0xff
 Control: 0x03
 Protocol: Link Control Protocol (0xc021)
 PPP Link Control Protocol

Yohanes Gunawan Yusuf (TR0639)

MUM Kuta, BALI 24-25 Oct 2019

66

66

L2TP – Use UDP (port 1701)

```

> Frame 23: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
> Ethernet II, Src: 0c:f0:c9:b0:e7:02 (0c:f0:c9:b0:e7:02), Dst: 0c:f0:c9:f7:2a:02 (0c:f0:c9:f7:2a:02)
> Internet Protocol Version 4, Src: 10.0.0.1, Dst: 10.0.0.2
  User Datagram Protocol, Src Port: 1701, Dst Port: 1701
    Source Port: 1701
    Destination Port: 1701
    Length: 106
    Checksum: 0xad29 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  Layer 2 Tunneling Protocol
  Point-to-Point Protocol
  PPP Compressed Datagram
0000  0c f0 c9 f7 2a 02 0c f0 c9 b0 e7 02 08 00 45 00  ....*.....E
0010  00 7e 2c 00 00 00 40 11 3a 6d 0a 00 00 01 0a 00  ~.,...@.:m.....
0020  00 02 06 a5 06 a5 00 6a ad 29 00 02 00 01 00 01  ....:~).....
0030  ff 03 00 fd 90 07 39 a4 fd a1 e6 fa de c6 b1 c9  ....9.....
0040  f2 1a 50 4e 50 5e 11 eb 13 1f 8e 32 f1 90 2f 8e  ..PNP^...2../.
0050  0f 0f ae d8 df 03 90 72 66 c7 52 14 c9 34 a7 75  ....r f R 4 u
0060  04 fe 38 5e c3 ef c6 2f 32 eb c4 a9 f5 55 32 2d  ..8^.../ 2...U2-
0070  d6 a4 86 a4 7b d8 e5 ec cf f1 b2 ec 6f f5 00 61  ....{...o...a
0080  27 3e e6 34 e3 28 56 66 f9 36 5a ad                '>.4.(Vf -6Z.

```

Transport Layer UDP

67

L2TP – Ping as PPP Compressed Datagram (Encrypted)

22	48.396200	10.0.0.2	10.0.0.1	PPP Comp	140 Compressed data
23	48.503094	10.0.0.1	10.0.0.2	PPP Comp	140 Compressed data
24	49.616125	10.0.0.2	10.0.0.1	PPP Comp	140 Compressed data
25	49.834306	10.0.0.1	10.0.0.2	PPP Comp	140 Compressed data

```

> Frame 23: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
> Ethernet II, Src: 0c:f0:c9:b0:e7:02 (0c:f0:c9:b0:e7:02), Dst: 0c:f0:c9:f7:2a:02 (0c:f0:c9:f7:2a:02)
> Internet Protocol Version 4, Src: 10.0.0.1, Dst: 10.0.0.2
  User Datagram Protocol, Src Port: 1701, Dst Port: 1701
    Layer 2 Tunneling Protocol
      Packet Type: Data      Message Tunnel Id=1 Session Id=1
      Tunnel ID: 1
      Session ID: 1
    Point-to-Point Protocol
      Address: 0xff
      Control: 0x03
      Protocol: Compressed datagram (0x00fd)
  PPP Compressed Datagram
0000  0c f0 c9 f7 2a 02 0c f0 c9 b0 e7 02 08 00 45 00  ....*.....E
0010  00 7e 2c 00 00 00 40 11 3a 6d 0a 00 00 01 0a 00  ~.,...@.:m.....
0020  00 02 06 a5 06 a5 00 6a ad 29 00 02 00 01 00 01  ....:~).....
0030  ff 03 00 fd 90 07 39 a4 fd a1 e6 fa de c6 b1 c9  ....9.....
0040  f2 1a 50 4e 50 5e 11 eb 13 1f 8e 32 f1 90 2f 8e  ..PNP^...2../.
0050  0f 0f ae d8 df 03 90 72 66 c7 52 14 c9 34 a7 75  ....r f R 4 u
0060  04 fe 38 5e c3 ef c6 2f 32 eb c4 a9 f5 55 32 2d  ..8^.../ 2...U2-
0070  d6 a4 86 a4 7b d8 e5 ec cf f1 b2 ec 6f f5 00 61  ....{...o...a
0080  27 3e e6 34 e3 28 56 66 f9 36 5a ad                '>.4.(Vf -6Z.

```

Tunnel

Encrypted

68

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

```

> Frame 23: 140 bytes on wire (1120 bits), 140 bytes capture
> Ethernet II, Src: 0c:f0:c9:b0:e7:02 (0c:f0:c9:b0:e7:02), D
> Internet Protocol Version 4, Src: 10.0.0.1, Dst: 10.0.0.2
  > User Datagram Protocol, Src Port: 1701, Dst Port: 1701
    Source Port: 1701
    Destination Port: 1701
    Length: 106
    Checksum: 0xad29 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  > Layer 2 Tunneling Protocol
  > Point-to-Point Protocol
    PPP Compressed Datagram
  
```

69



EoIP over L2TP Frame

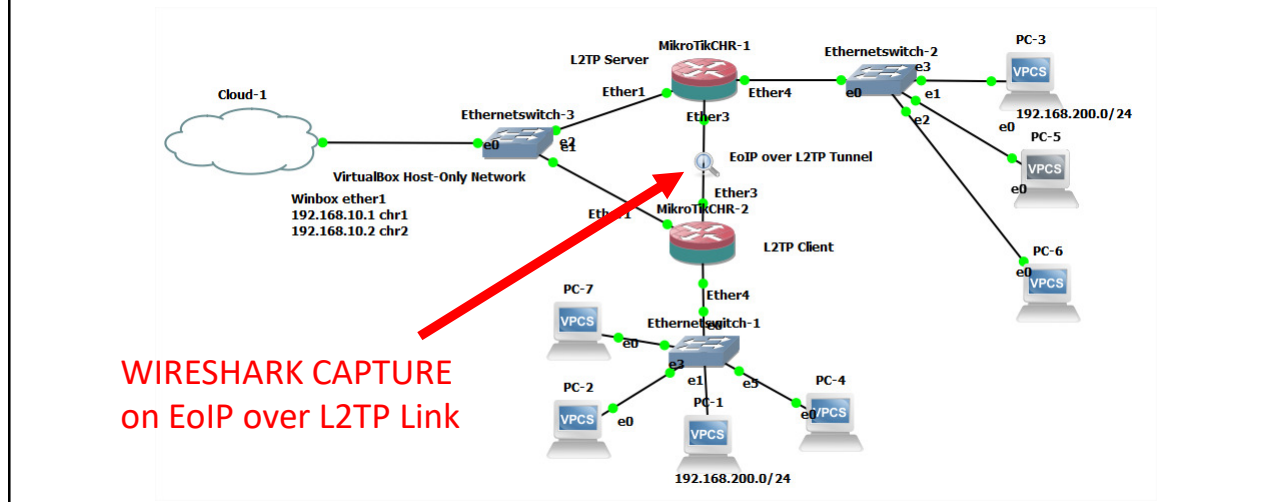
70

EoIP over L2TP

Yohanes Gunawan Yusuf (TR0639) MUM Kuta, BALI 24-25 Oct 2019

71

EoIP over L2TP Tunnel



Yohanes Gunawan Yusuf (TR0639) MUM Kuta, BALI 24-25 Oct 2019 72

72

EoIP over L2TP Tunnel

```

> Frame 271: 182 bytes on wire (1456 bits), 182 bytes captured (1456 bits) on interfac
> Ethernet II, Src: 0c:f5:4c:83:a0:02 (0c:f5:4c:83:a0:02), Dst: 0c:f5:4c:47:87:02 (0c:
> Internet Protocol Version 4, Src: 10.0.0.1, Dst: 10.0.0.2
> User Datagram Protocol, Src Port: 1701, Dst Port: 1701
> Layer 2 Tunneling Protocol
> Point-to-Point Protocol
> PPP Compressed Datagram
  
```

L2TP Tunnel

```

0000 0c f5 4c 47 87 02 0c f5 4c 83 a0 02 08 00 45 00  ..LG...L...E.
0010 00 a8 49 00 00 00 40 11 1d 43 0a 00 00 01 0a 00  ..I...@.-C.....
0020 00 02 06 a5 06 a5 00 94 05 45 00 02 00 02 00 01  ..0...D.A...".
0030 ff 03 00 fd 90 38 96 21 ee 1e 7c d8 08 75 eb 64  ...!.|..u.d
0040 08 85 83 30 c2 e9 c5 44 fe 41 bf f7 60 22 fa 22  ...0...D.A...".
0050 54 c1 44 32 ba 43 aa ca f4 b7 20 2a e6 50 31 01  T.D2.C...*P1.
0060 c1 9d b8 69 7b 86 7f ed af 7b 60 35 06 7a e3 97  ...i{...{5.z..
0070 10 ec 6d 25 30 05 d9 73 eb 99 1c 58 7c ee 63 e2  ...m%0.s..X|.c.
0080 2d 9b 19 ee 6f e2 0c 30 35 18 a4 8f 5a 08 e6 71  ...o05..Z..q
0090 c7 7c a4 d9 f9 9f 37 a2 7d b9 14 41 f4 5a 8d 10  .|...7.}..A.Z..
00a0 14 15 4d 52 d0 19 82 03 30 2b 11 dd 2d a8 fc 05  ..MR...0+.....
00b0 70 9e 0a 30 f4 17  p..0..
  
```

PPP Compressed Datagram (comp_data), 130 bytes

Yohanes Gunawan Yusuf (TR0639)

MUM Kuta, BALI 24-25 Oct 2019

73

73

Ping PC4 to PC5

```

PC1 : 192.168.200.4 255.255.255.0

PC-4> ping 192.168.200.5
84 bytes from 192.168.200.5 icmp_seq=1 ttl=64 time=586.140 ms
84 bytes from 192.168.200.5 icmp_seq=2 ttl=64 time=324.921 ms
84 bytes from 192.168.200.5 icmp_seq=3 ttl=64 time=401.102 ms
84 bytes from 192.168.200.5 icmp_seq=4 ttl=64 time=394.101 ms
84 bytes from 192.168.200.5 icmp_seq=5 ttl=64 time=403.102 ms

PC-4> ping 192.168.200.5
84 bytes from 192.168.200.5 icmp_seq=1 ttl=64 time=443.114 ms
84 bytes from 192.168.200.5 icmp_seq=2 ttl=64 time=380.071 ms
84 bytes from 192.168.200.5 icmp_seq=3 ttl=64 time=206.055 ms
84 bytes from 192.168.200.5 icmp_seq=4 ttl=64 time=289.075 ms
84 bytes from 192.168.200.5 icmp_seq=5 ttl=64 time=310.080 ms

PC-4>
  
```

```

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 192.168.200.5 255.255.255.0
Checking for duplicate address...
PC1 : 192.168.200.5 255.255.255.0

PC-5>
  
```

Yohanes Gunawan Yusuf (TR0639)

MUM Kuta, BALI 24-25 Oct 2019

74

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**

```
PC-> ping 192.168.200.5
84 bytes from 192.168.200.5 icmp_seq=1 ttl=64 time=443.114 ms
84 bytes from 192.168.200.5 icmp_seq=2 ttl=64 time=380.071 ms
84 bytes from 192.168.200.5 icmp_seq=3 ttl=64 time=206.055 ms
84 bytes from 192.168.200.5 icmp_seq=4 ttl=64 time=289.075 ms
84 bytes from 192.168.200.5 icmp_seq=5 ttl=64 time=310.080 ms
```

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

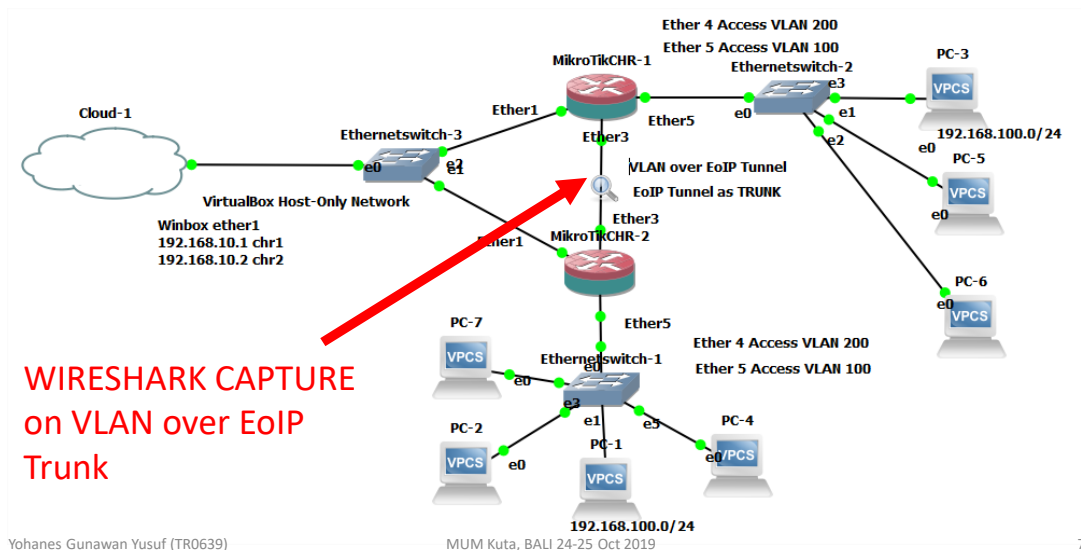
Interface	Type	Actual MTU	L2 MTU	Tx	Rx
R bridge1	Bridge	1450	65535	0 bps	0
RS eoip-tunnel1	EoIP Tunnel	1458	65535	0 bps	0
R ether1	Ethernet	1500	65535	0 bps	984
R ether2	Ethernet	1500	65535	0 bps	0
R ether3eoip	Ethernet	1500	65535	0 bps	0
R ether4	Ethernet	1500	65535	0 bps	0
RS ether5	Ethernet	1500	65535	0 bps	0

Interface	Type	Actual MTU	L2 MTU	Tx	Rx
DR d2p-ppp1	L2TP Server Binding	1450	65535	0 bps	0
R bridge1tot	Bridge	1408	65535	0 bps	0
RS eoip-tunnel1	EoIP Tunnel	1408	65535	0 bps	0
R ether1	Ethernet	1500	65535	77.5 kbps	7.0 k
R ether2	Ethernet	1500	65535	0 bps	0
R ether3-l2tp	Ethernet	1500	65535	0 bps	0
RS ether4	Ethernet	1500	65535	0 bps	0
R ether5	Ethernet	1500	65535	0 bps	0

VLAN over EoIP Frame

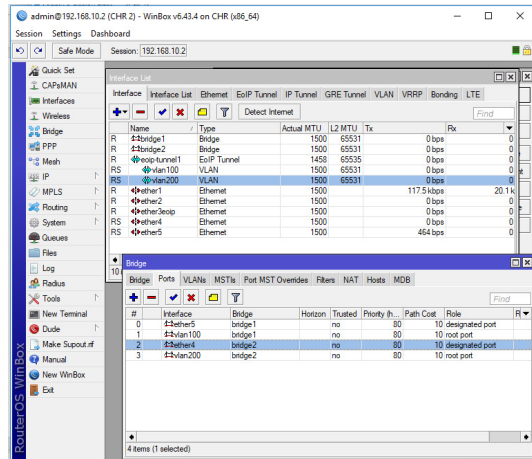
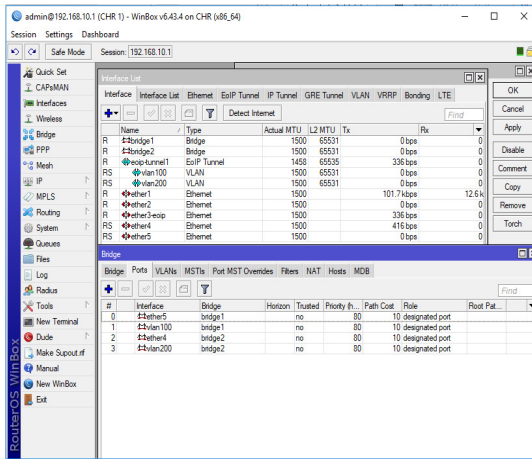
77

VLAN over EoIP Tunnel



78

VLAN over EoIP Setup



Yohanes Gunawan Yusuf (TR0639)

MUM Kuta, BALI 24-25 Oct 2019

79

79

Ping PC2 to PC5

```

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
    
```

```

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>
    
```

Yohanes Gunawan Yusuf (TR0639)

MUM Kuta, BALI 24-25 Oct 2019

80

80

VLAN over EoIP Frame

```

144 85.174346 192.168.100.2 192.168.100.5 ICMP 144 Echo (ping) request
145 85.312835 192.168.100.5 192.168.100.2 ICMP 144 Echo (ping) reply
146 85.390246 02:da:0b:27:22:b8 Spanning-tree-(for-... STP 99 RST. Root = 32768/0/0
147 86.539604 02:da:0b:27:22:b8 Spanning-tree-(for-... STP 99 RST. Root = 32768/0/0
148 86.556230 192.168.100.2 192.168.100.5 ICMP 144 Echo (ping) request
149 86.867003 192.168.100.5 192.168.100.2 ICMP 144 Echo (ping) reply

```

```

> Frame 144: 144 bytes on wire (1152 bits), 144 bytes captured (1152 bits) on interface 0
> Ethernet II, Src: 0c:8a:14:e6:81:02 (0c:8a:14:e6:81:02), Dst: 0c:8a:14:7b:78:02 (0c:8a:14:7b:78:02)
> Internet Protocol Version 4, Src: 10.0.0.2, Dst: 10.0.0.1
> Generic Routing Encapsulation (MIKROTIK EoIP)
> Ethernet II, Src: Private_66:68:01 (00:50:79:66:68:01), Dst: Private_66:68:03 (00:50:79:66:68:03)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 100
> Internet Protocol Version 4, Src: 192.168.100.2, Dst: 192.168.100.5
> Internet Control Message Protocol

```

```

0000 0c 8a 14 7b 78 02 0c 8a 14 e6 81 02 08 00 45 00 ...{x... ..E
0010 00 82 20 01 00 00 ff 2f 87 49 0a 00 00 02 0a 00 ... ..I...
0020 00 01 20 01 64 00 00 66 33 00 00 50 79 66 68 03 ...d..f 3..Pyfh
0030 00 50 79 66 68 01 81 00 00 64 08 00 45 00 00 54 ...Pyfh...d..E..T
0040 a9 f2 00 00 01 87 5e c0 a8 64 02 c0 a8 64 05 ...@..^..d...d
0050 08 00 2d 61 f2 a9 00 01 08 09 0a 0b 0c 0d 0e 0f ...-a... ..
0060 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f ... ..
0070 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f ...!#$%&'()*+,-./
0080 30 31 32 33 34 35 36 37 38 39 3a 3b 3c 3d 3e 3f ...01234567 89;<=>?

```

EoIP Tunnel
VLAN 100

81

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

```

> Frame 144: 144 bytes on wire (1152 bits), 144 bytes captured (1152
> Ethernet II, Src: 0c:8a:14:e6:81:02 (0c:8a:14:e6:81:02), Dst: 0c:8a
> Internet Protocol Version 4, Src: 10.0.0.2, Dst: 10.0.0.1
> Generic Routing Encapsulation (MIKROTIK EoIP)
> Ethernet II, Src: Private_66:68:01 (00:50:79:66:68:01), Dst: Privat
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 100
> Internet Protocol Version 4, Src: 192.168.100.2, Dst: 192.168.100.5
> Internet Control Message Protocol

```

```

0000 0c 8a 14 7b 78 02 0c 8a 14 e6 81 02 08 00 45 00 ...{x... ..E
0010 00 82 20 01 00 00 ff 2f 87 49 0a 00 00 02 0a 00 ... ..I...
0020 00 01 20 01 64 00 00 66 33 00 00 50 79 66 68 03 ...d..f 3..Pyfh
0030 00 50 79 66 68 01 81 00 00 64 08 00 45 00 00 54 ...Pyfh...d..E..T
0040 a9 f2 00 00 01 87 5e c0 a8 64 02 c0 a8 64 05 ...@..^..d...d
0050 08 00 2d 61 f2 a9 00 01 08 09 0a 0b 0c 0d 0e 0f ...-a... ..
0060 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f ... ..
0070 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f ...!#$%&'()*+,-./
0080 30 31 32 33 34 35 36 37 38 39 3a 3b 3c 3d 3e 3f ...01234567 89;<=>?

```

82

L-2 for EoIP and VLAN Frames

```

> Frame 144: 144 bytes on wire (1152 bits), 144 bytes captured (1152 bits) on i
v Ethernet II, Src: 0c:8a:14:e6:81:02 (0c:8a:14:e6:81:02), Dst: 0c:8a:14:7b:78:02
  > Destination: 0c:8a:14:7b:78:02 (0c:8a:14:7b:78:02)
  > Source: 0c:8a:14:e6:81:02 (0c:8a:14:e6:81:02)
  Type: IPv4 (0x0800)
v Internet Protocol Version 4, Src: 10.0.0.2, Dst: 10.0.0.1
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 130
  Identification: 0x2001 (8193)
  > Flags: 0x0000
  Time to live: 255
  Protocol: Generic Routing Encapsulation (47)
  Header checksum: 0x8749 [validation disabled]
  [Header checksum status: Unverified]
  Source: 10.0.0.2
  Destination: 10.0.0.1
  > Generic Routing Encapsulation (MIKROTIK EoIP)
  > Ethernet II, Src: Private_66:68:01 (00:50:79:66:68:01), Dst: Private_66:68:03
  > 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 100
  > Internet Protocol Version 4, Src: 192.168.100.2, Dst: 192.168.100.5
  > Internet Control Message Protocol
  Key: 0x00663300
v Ethernet II, Src: Private_66:68:01 (00:50:79:66:68:01), Dst: Private_66:68:03
  > Destination: Private_66:68:03 (00:50:79:66:68:03)
  > Source: Private_66:68:01 (00:50:79:66:68:01)
  Type: 802.1Q Virtual LAN (0x8100)
v 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 100
  000. .... = Priority: Best Effort (default) (0)
  ...0 .... = DEI: Ineligible
  .... 0000 0110 0100 = ID: 100
  Type: IPv4 (0x0800)
v Internet Protocol Version 4, Src: 192.168.100.2, Dst: 192.168.100.5
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 84
  Identification: 0xa9f2 (43506)
  > Flags: 0x0000
  Time to live: 64
  Protocol: ICMP (1)
  Header checksum: 0x875e [validation disabled]
  [Header checksum status: Unverified]
  Source: 192.168.100.2
  Destination: 192.168.100.5
  > Internet Control Message Protocol
  
```

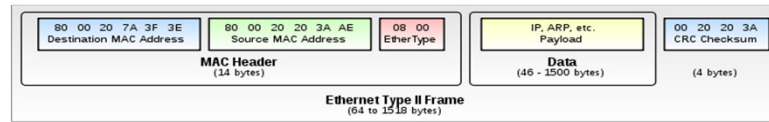
83



Conclusion

84

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.

85



Let's discuss it....
Thank you

86