

DCI (EoIP)

Data Center Interconnect
(Ethernet over IP)

ABOUT PRESENTER

Moez Aftab

Electrical Engineer

MTCRE, MTCNA

CCIE Data Center

(CCIE # 53316)

CCNA R&S

[Fb.com/3bits1byte](https://www.facebook.com/3bits1byte)

0092-321-3955279



WORK HISTORY

Moez Aftab

Allied Bank Limited

Network Projects 2017 – Present

CYBERNET Service Provider

Sr. TAC Engineer 2015 - 2017

Superior Connection

NOC Engineer 2014 - 2015

Starlite Telecommunication

Support Engineer 2013 - 2014



WORK HISTORY

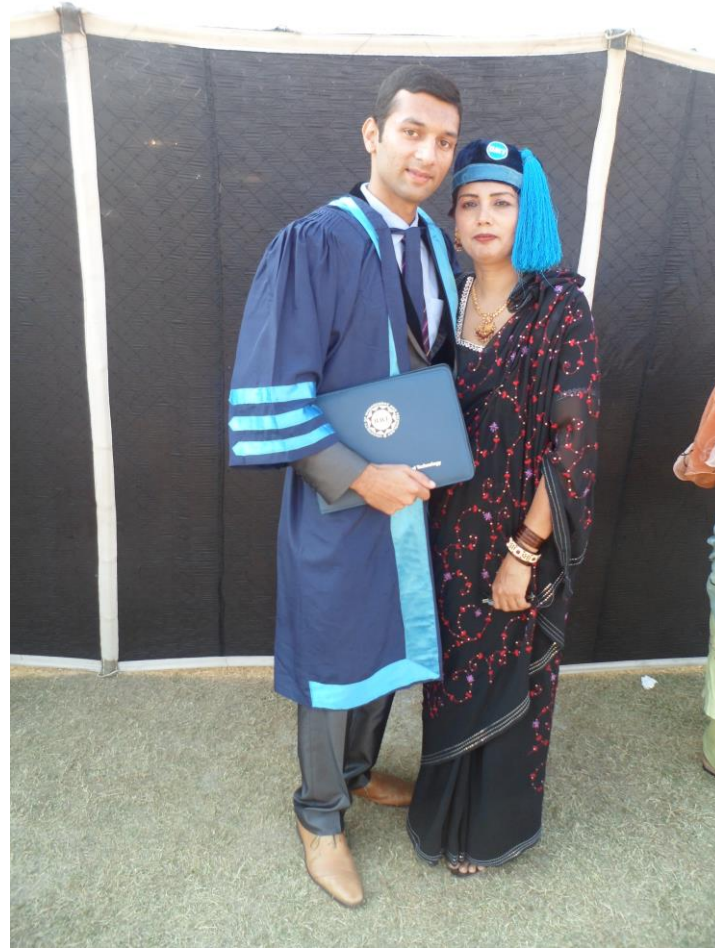
Moez Aftab

CORVIT Systems

Workshops on Mikrotik



Mother

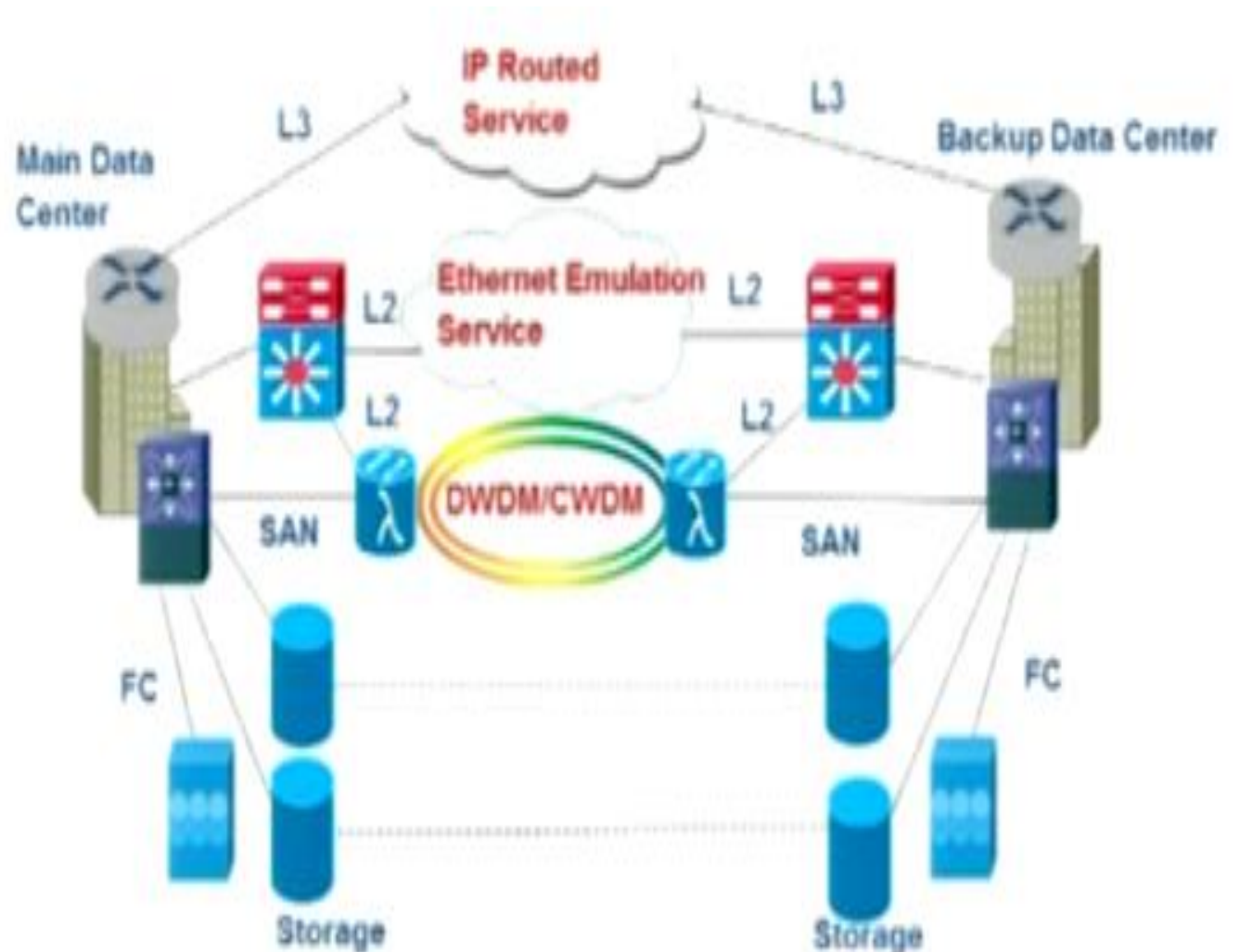


Agenda

- DCI technology
- DCI protocols Using IP/MPLS Domains
- Technical overview of EoIP
- Proposed design for DCI using EoIP
- Configuration steps

DCI Technology

- Data Center are expanding beyond traditional boundaries due to:
 - Extending operating system, file system cluster, data base cluster
 - Virtual/physical machine mobility due to load sharing, disaster prevention
 - Legacy devices/application with embedded IP addressing.
 - Time to deployment and operational reasons.
 - Extend DC to solve power/heat/space limitations.



Business Drivers for L2 connectivity

Business Drivers	IT Solutions
Disaster Prevention	Active / Standby migration
Business Continuance	Server HA clusters, “Geo-clustering”
Workload Mobility	Move, consolidate servers “Vmotion”

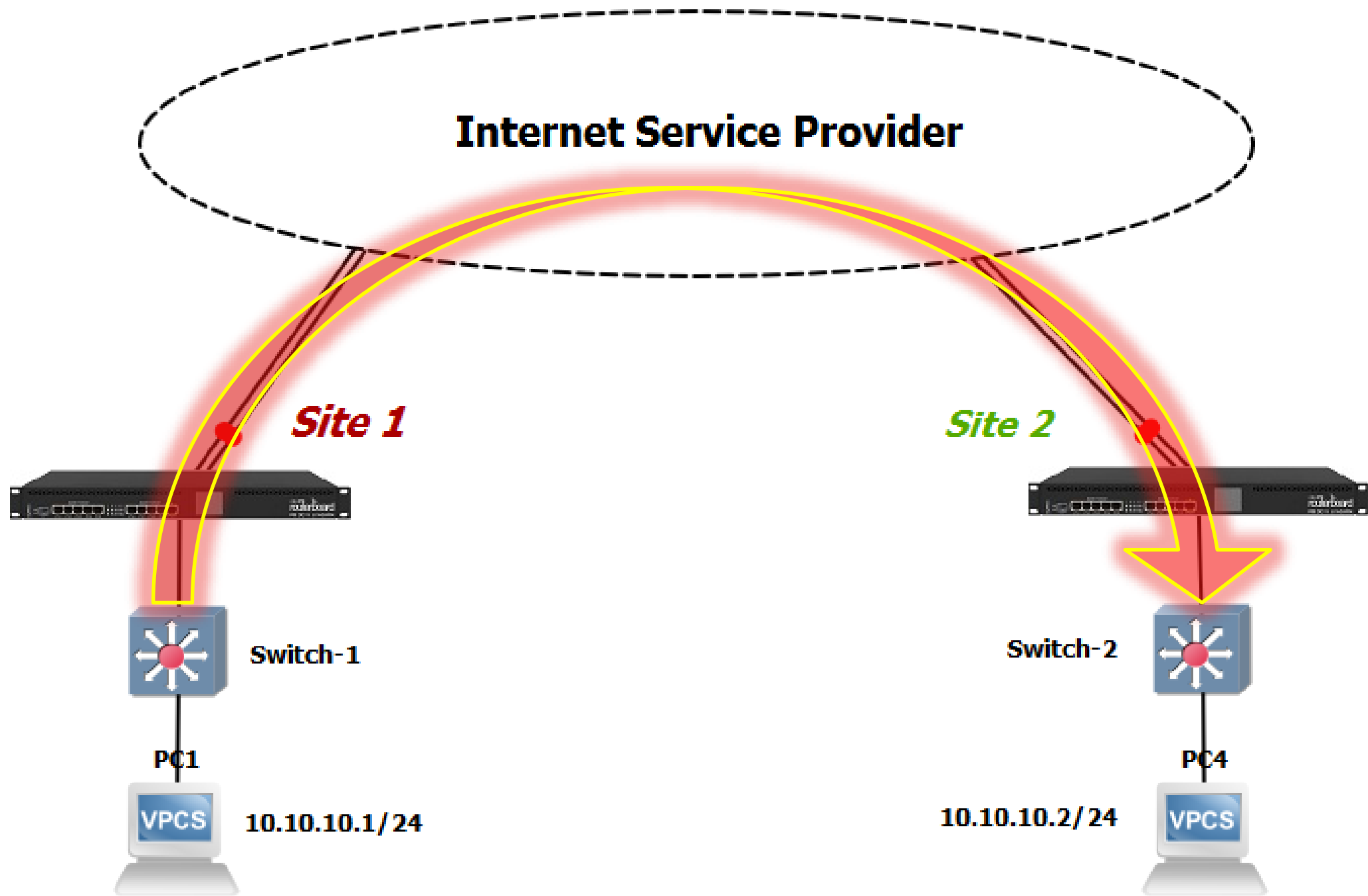
Layer 2 Extension (DCI) Protocols over IP/MPLS Based Network

IP	MPLS
L2TP	VPLS
EoIP	EVPN
EVPN	EVC
	NvGRE

Technical Overview of EoIP

EoIP

Ethernet over IP (EoIP) Tunneling is a MikroTik RouterOS protocol that creates an Ethernet tunnel between two routers on top of an IP connection.

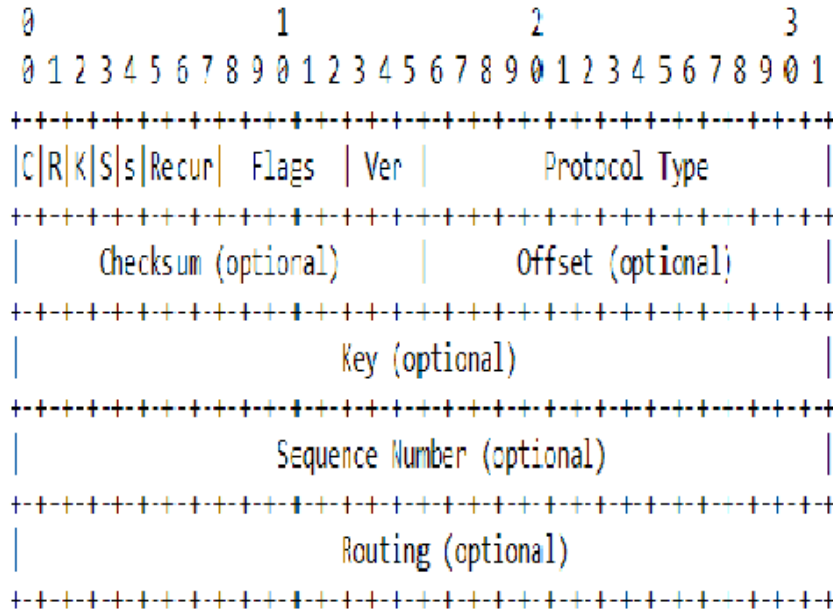


EoIP Header

- The EoIP protocol encapsulates Ethernet frames in GRE (IP protocol number 47) packets and sends them to the remote side of the EoIP tunnel.
- EoIP tunnel adds at least 42 byte overhead (8byte GRE + 14 byte Ethernet + 20 byte IP)

GRE vs EoIP Header

GRE Header



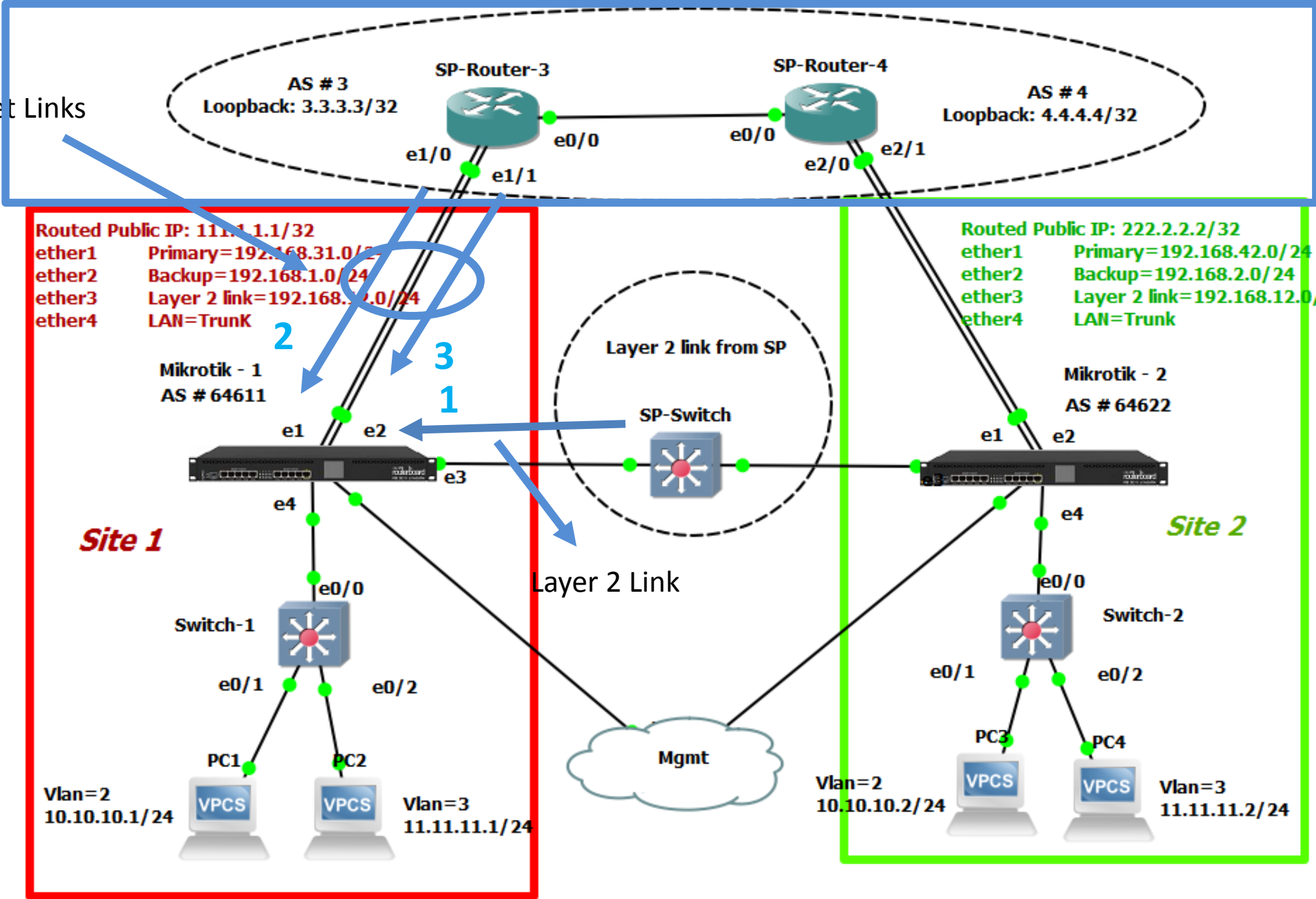
EoIP Header

```
→ 88 47.503007 10.10.10.1 10.10.10.2 ICMP 140 Echo (ping) request id=0x449b, seq=1/256
= 89 47.504874 10.10.10.2 10.10.10.1 ICMP 140 Echo (ping) reply id=0x449b, seq=1/256
▶ Frame 88: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
▶ Ethernet II, Src: 00:9d:c2:32:78:02 (00:9d:c2:32:78:02), Dst: 00:9d:c2:44:97:02 (00:9d:c2:44:97:02)
▶ Internet Protocol Version 4, Src: 192.168.12.1, Dst: 192.168.12.2
* Generic Routing Encapsulation (MIKROTIK EoIP)
  * Flags and Version: 0x2001
    0... .. = Checksum Bit: No
    .0.. .. = Routing Bit: No
    ..1. .. = Key Bit: Yes
    ...0 .. = Sequence Number Bit: No
    .... 0... .. = Strict Source Route Bit: No
    .... .000 .. = Recursion control: 0
    .... .. 0000 0... = Flags (Reserved): 0
    .... .. .. .001 = Version: Enhanced GRE (1)
  Protocol Type: MIKROTIK EoIP (0x6400)
  Key: 0x00020c00
  Ethernet II, Src: Private_66:68:00 (00:50:79:66:68:00), Dst: Private_66:68:02 (00:50:79:66:68:02)
  Internet Protocol Version 4, Src: 10.10.10.1, Dst: 10.10.10.2
  Internet Control Message Protocol
```

EoIP Proposed Design

From Client End
Perspective

Internet Links



Configuring EOIP tunnel

- Internet Link
 - Fiber (Primary Link)
 - RF (Backup Link)
- Layer 2 link

Configuration Steps

1. Configure routed pool given by your SP. In our case it's 111.1.1.1/32 for your site 1 and 222.2.2.2/32 for your site 2.
 - a) Primary Link = BGP & Static Route
 - b) Secondary Link = Static Route
2. Create the EoIP tunnel over this IP Prefix.
3. Create another EoIP tunnel over Layer 2 circuit.
4. Call both these EoIP tunnel's in Bridge/Bonding.

Basic Configuration

Site 1

R	ether1 - Primary	Ethernet	1500
R	ether2 - Backup	Ethernet	1500
R	ether3 - DarkCore	Ethernet	1500
RS	ether4 - LAN	Ethernet	1500

Address List			
Address	Network	Interface	
111.1.1.1	111.1.1.1	Loopback	
192.168.1.1/24	192.168.1.0	ether2 - Backup	
192.168.12.1/24	192.168.12.0	ether3 - DarkCore	
192.168.31.1/24	192.168.31.0	ether1 - Primary	
192.168.48.11/24	192.168.48.0	ether10 - Mgmt	

Site 2

R	ether1 - Primary	Ethernet	1500
R	ether2 - Backup	Ethernet	1500
R	ether3 - DarkCore	Ethernet	1500
RS	ether4 - LAN	Ethernet	1500

Address List			
Address	Network	Interface	
192.168.2.2/24	192.168.2.0	ether2 - Backup	
192.168.12.2/24	192.168.12.0	ether3 - DarkCore	
192.168.42.2/24	192.168.42.0	ether1 - Primary	
192.168.48.22/24	192.168.48.0	ether10 - Mgmt	
222.2.2.2	222.2.2.2	Loopback	

Name Interface
Assign IP address

BGP Pairing

Point to Ponder:
TTL for eBGP & iBGP

Define your AS in instance

In peers define the
neighbor parameters

Instance (Own AS)

Remote Address

Remote AS

Site 1

The screenshot shows the BGP configuration for Site 1. At the top, there are tabs for 'Instances', 'VRFs', 'Peers', 'Networks', and 'Aggreg'. Below these are several icons: a plus sign, a minus sign, a checkmark, an 'X', a folder, and a funnel. A table lists the BGP instances:

Name	AS	Router ID
default	64611	

Below the table, the 'BGP Peer <peer1>' configuration is shown. The 'General' tab is active, displaying the following fields:

- Name: peer1
- Instance: default
- Remote Address: 192.168.31.3
- Remote Port: (empty)
- Remote AS: 3
- TCP MD5 Key: (empty)
- Nexthop Choice: default
- Multihop
- Route Reflect
- Hold Time: 15

Site 2

The screenshot shows the BGP configuration for Site 2. At the top, there are tabs for 'Instances', 'VRFs', 'Peers', 'Networks', and 'Aggreg'. Below these are several icons: a plus sign, a minus sign, a checkmark, an 'X', a folder, and a funnel. A table lists the BGP instances:

Name	AS	Router ID
default	64622	

Below the table, the 'BGP Peer <peer1>' configuration is shown. The 'General' tab is active, displaying the following fields:

- Name: peer1
- Instance: default
- Remote Address: 192.168.42.4
- Remote Port: (empty)
- Remote AS: 4
- TCP MD5 Key: (empty)
- Nexthop Choice: default
- Multihop
- Route Reflect
- Hold Time: 15

BGP

**Point to Ponder:
Classless prefix advertisement
in BGP**

- Advertise the IP prefix in BGP.
- For internet, common practice for BGP scenario is given below
 - Upstream inject the default route to client
 - Upstream advertise a loopback to customer. Customer will add the default route towards that Loopback.

Point to Ponder:
Recursive routing

- Default Route towards the Loopback advertised by SP.
- For backup link, default route with higher administrative distance.

Routes

Site 1

The screenshot shows the 'Route List' interface for Site 1. It features tabs for 'Routes', 'Nexthops', 'Rules', and 'VRF'. Below the tabs are several control icons: a plus sign, a minus sign, a checkmark, an 'X', a document icon, and a funnel icon. A 'Find' input field is located on the right. The main table displays the following data:

	Dst. Address	Gateway	Distance
AS	0.0.0.0/0	3.3.3.3 recursive via 192.168.31.3 ether1 - Primary	1
S	0.0.0.0/0	192.168.1.3 reachable ether2 - Backup	200
DAb	3.3.3.3	192.168.31.3 reachable ether1 - Primary	20

Site 2

The screenshot shows the 'Route List' interface for Site 2. It features tabs for 'Routes', 'Nexthops', 'Rules', and 'VRF'. Below the tabs are several control icons: a plus sign, a minus sign, a checkmark, an 'X', a document icon, and a funnel icon. The main table displays the following data:

	Dst. Address	Gateway	Distance
S	0.0.0.0/0	192.168.2.4 reachable ether2 - Backup	200
AS	0.0.0.0/0	4.4.4.4 recursive via 192.168.42.4 ether1 - Primary	1
DAb	4.4.4.4	192.168.42.4 reachable ether1 - Primary	20

Routes (Recursive Routing)

Route <0.0.0.0/0>	
General	Attributes
Dst. Address:	0.0.0.0/0
Gateway:	3.3.3.3 recursive via 192.168.31.3 ether1 - Primary
Check Gateway:	
Type:	unicast
Distance:	1
Scope:	30
Target Scope:	40

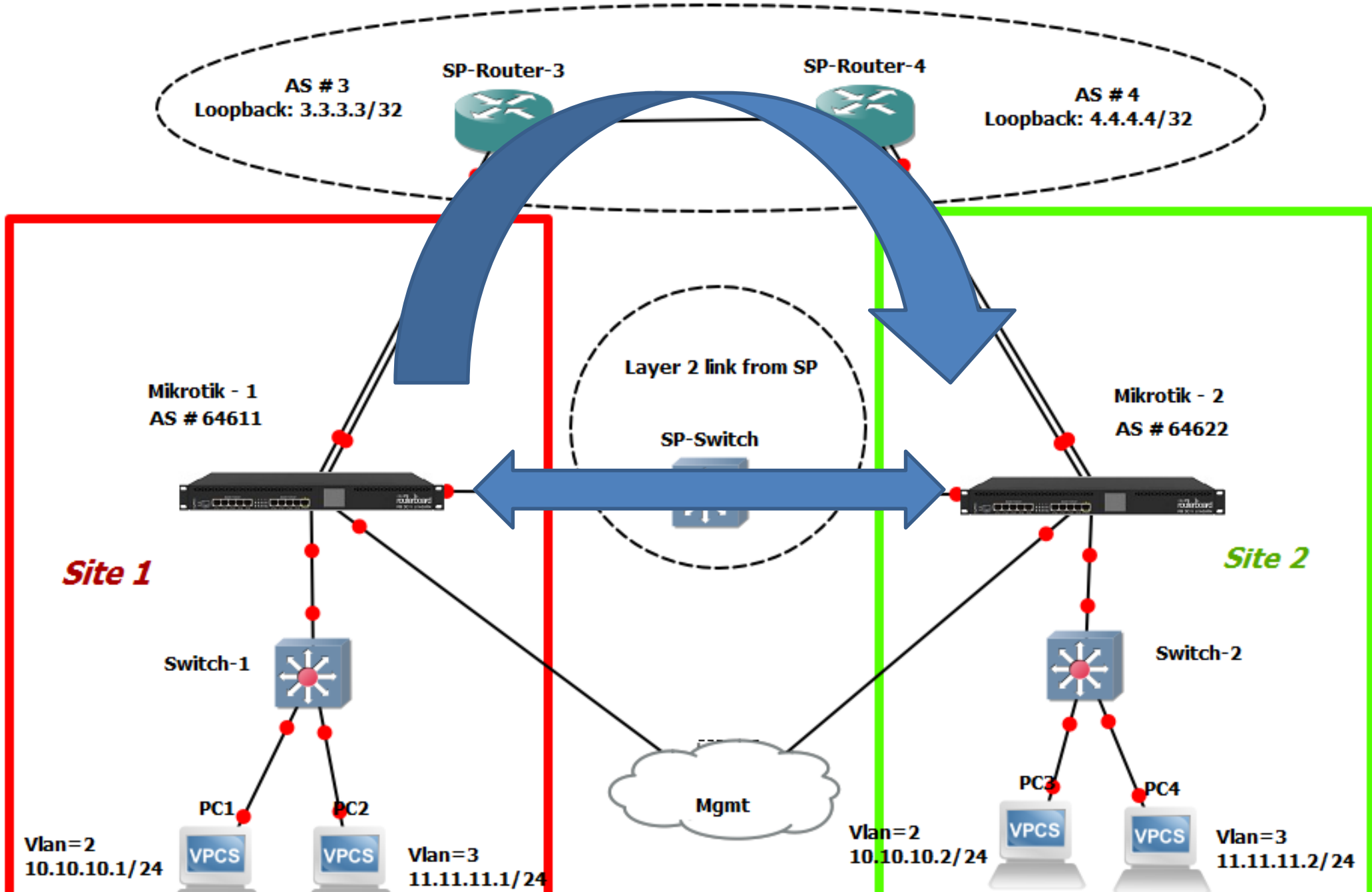
Route <0.0.0.0/0>	
General	Attributes
Dst. Address:	0.0.0.0/0
Gateway:	4.4.4.4 recursive via 192.168.42.4 ether1 - Primary
Check Gateway:	
Type:	unicast
Distance:	1
Scope:	30
Target Scope:	40

Food for thought:
Local Address in EOIP

Configuring EOIP

- Configure EOIP over Public IP
- Assign the IP address to Layer 2 link and configure the EOIP over it.

Site 1				Site 2			
Interface <eoip-tunnel1>		Interface <eoip-tunnel2>		Interface <eoip-tunnel1>		Interface <eoip-tunnel2>	
General	Loop Protect	Status	Traffic	General	Loop Protect	Status	Traffic
Name:	eoip-tunnel1			Name:	eoip-tunnel2		
Type:	EoIP Tunnel			Type:	EoIP Tunnel		
MTU:				MTU:			
Actual MTU:	1458			Actual MTU:	1458		
L2 MTU:	65535			L2 MTU:	65535		
MAC Address:	02:C2:5C:5E:4			MAC Address:	02:FE:EC:EA:57:1D		
ARP:	enabled			ARP:	enabled		
ARP Timeout:				ARP Timeout:			
Local Address:	111.1.1.1			Local Address:	192.168.12.1		
Remote Address:	222.2.2.2			Remote Address:	192.168.12.2		
Tunnel ID:	1			Tunnel ID:	2		

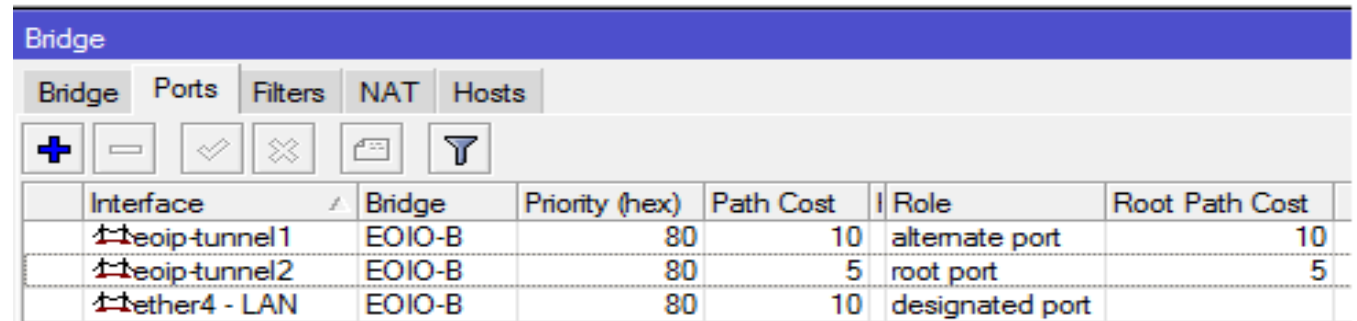


Food for thought:
Is it necessary to run STP

Bridge

- Call that EOIP in Bridge interface.
- Run STP on bridge interface and set the primary backup link using the cost of STP.

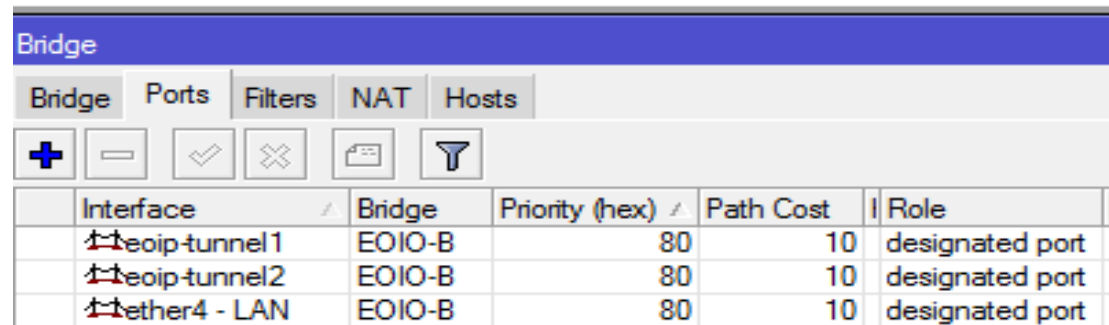
Site 1



The screenshot shows the configuration for a bridge at Site 1. The bridge is named 'EOIO-B'. Three interfaces are connected to it: 'eoip-tunnel1', 'eoip-tunnel2', and 'ether4 - LAN'. The STP role for each interface is configured as follows:

Interface	Bridge	Priority (hex)	Path Cost	Role	Root Path Cost
eoip-tunnel1	EOIO-B	80	10	alternate port	10
eoip-tunnel2	EOIO-B	80	5	root port	5
ether4 - LAN	EOIO-B	80	10	designated port	

Site 2



The screenshot shows the configuration for a bridge at Site 2. The bridge is named 'EOIO-B'. Three interfaces are connected to it: 'eoip-tunnel1', 'eoip-tunnel2', and 'ether4 - LAN'. The STP role for each interface is configured as follows:

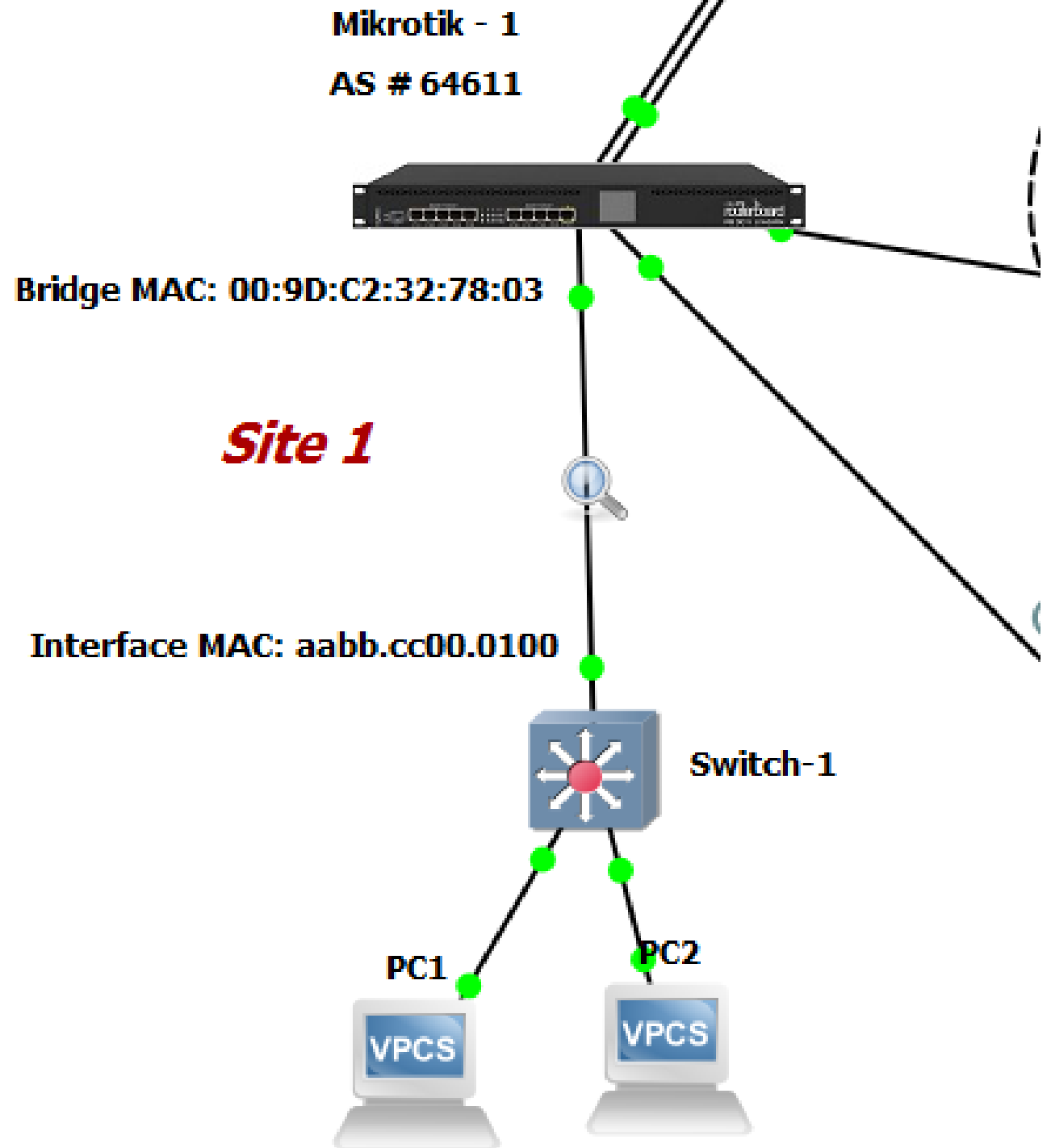
Interface	Bridge	Priority (hex)	Path Cost	Role	Root Path Cost
eoip-tunnel1	EOIO-B	80	10	designated port	
eoip-tunnel2	EOIO-B	80	10	designated port	
ether4 - LAN	EOIO-B	80	10	designated port	

Point to Ponder

- STP run on bridge don't need to leave Mikrotik.
- STP running at Network side encapsulate in EoIP tunnels and forwarded on both side.

STP Wireshark

Capturing the packet
between
Router and Switch



STP for Bridges

STP running on Bridge
send BPDU's down to the
Switch as-well. Which is
don't need of it.

Mikrotik Bridge MAC: 00:9D:C2:32:78:03
Switch Interface MAC: aabb.cc00.0100

The screenshot displays the configuration for interface <B-VLAN2> and a traffic capture log. The interface configuration shows it is a Bridge with MAC Address 00:9D:C2:32:78:03. The traffic capture log shows several STP frames, with frame 10 and 16 highlighted in red and green respectively. Frame 10 is a BPDU from source 00:9d:c2:32:78:03 to destination Spanning-tree-(for-bridges)_00. Frame 16 is a BPDU from source aa:bb:cc:00:01:00 to destination Spanning-tree-(for-bridges)_00. The capture details for frame 16 show it is a Spanning Tree Protocol (RSTP) frame with a Designated Port Role.

No.	Time	Source	Destination	Protocol
8	3.033782	aa:bb:cc:00:01:00	CDP/VTP/DTP/PAGP/UDLD	DTP
9	3.737973	aa:bb:cc:00:01:00	PVST+	STP
10	4.017457	00:9d:c2:32:78:03	Spanning-tree-(for-bridges)_00	STP
11	4.030000	aa:bb:cc:00:01:00	PVST+	STP
12	4.991190	aa:bb:cc:00:01:00	Spanning-tree-(for-bridges)_00	STP
13	5.742485	aa:bb:cc:00:01:00	PVST+	STP
14	6.014686	00:9d:c2:32:78:03	Spanning-tree-(for-bridges)_00	STP
15	6.004370	aa:bb:cc:00:01:00	PVST+	STP
16	6.994457	aa:bb:cc:00:01:00	Spanning-tree-(for-bridges)_00	STP

Frame 16 details:
Spanning Tree Protocol
Protocol Identifier: Spanning Tree Protocol (0x0000)
Protocol Version Identifier: Rapid Spanning Tree (2)
BPDU Type: Rapid/Multiple Spanning Tree (0x02)
BPDU flags: 0x3c, Forwarding, Learning, Port Role: Designated
Root Identifier: 32768 / 0 / 00:9d:c2:32:78:03
Root Path Cost: 0
Bridge Identifier: 32768 / 0 / 00:9d:c2:32:78:03
Port identifier: 0x8001
Message Age: 0
Max Age: 20
Hello Time: 2
Forward Delay: 15
Version 1 Length: 0

STP for Bridges

After configuring it to
Edge there is no BPDU
Coming down to network

The screenshot shows a network configuration interface for a bridge port. The 'Edge' checkbox is checked and highlighted with a red box. To the right, a packet capture table shows a BPDU frame (No. 52) with source and destination MAC addresses. Below the table, a packet capture analysis shows the frame details, including the Spanning Tree Protocol (STP) configuration BPDU type.

No.	Time	Source	Destination	Protocol	Length
51	19.017267	aa:bb:cc:00:01:00	PVST+	STP	
52	19.017330	aa:bb:cc:00:01:00	Spanning-tree-(for-bridges)_00	STP	
53	19.764741	aa:bb:cc:00:01:00	PVST+	STP	
54	21.024706	aa:bb:cc:00:01:00	PVST+	STP	
55	21.024831	aa:bb:cc:00:01:00	Spanning-tree-(for-bridges)_00	STP	
56	21.764449	aa:bb:cc:00:01:00	PVST+	STP	
57	23.029144	aa:bb:cc:00:01:00	PVST+	STP	
58	23.029195	aa:bb:cc:00:01:00	Spanning-tree-(for-bridges)_00	STP	
59	23.772638	aa:bb:cc:00:01:00	PVST+	STP	
60	25.033259	aa:bb:cc:00:01:00	PVST+	STP	
61	25.033324	aa:bb:cc:00:01:00	Spanning-tree-(for-bridges)_00	STP	
62	25.776767	aa:bb:cc:00:01:00	PVST+	STP	

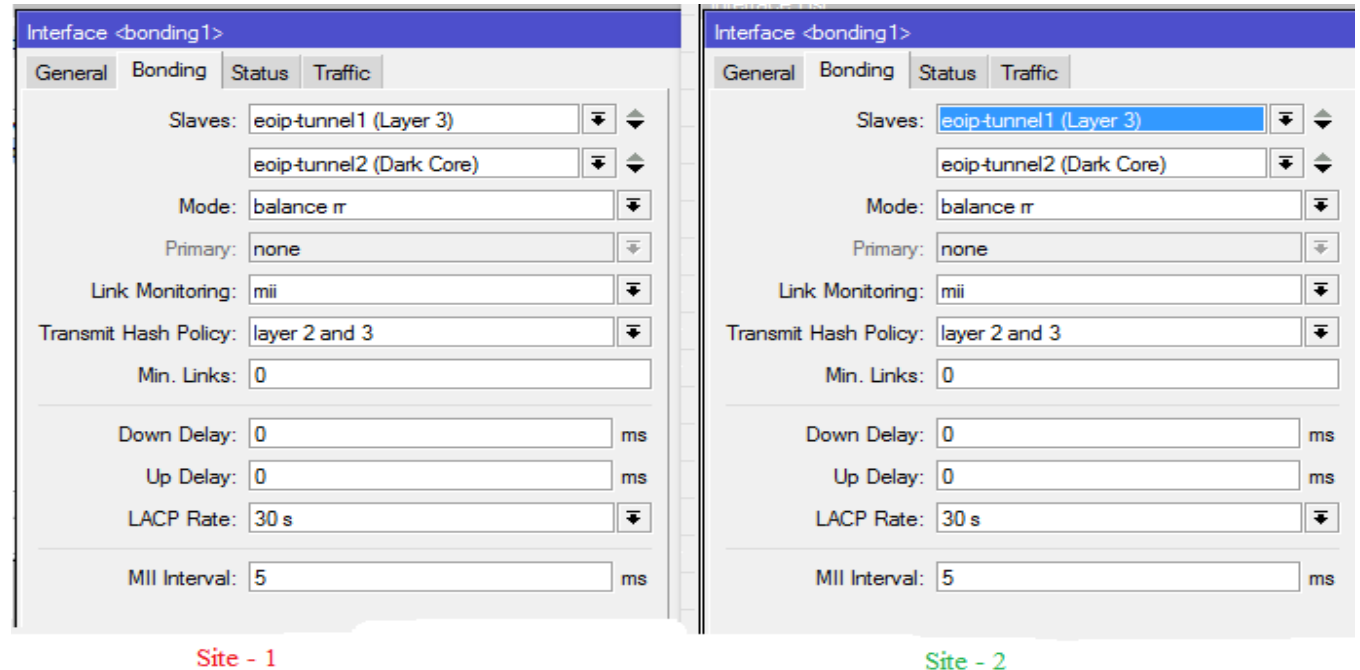
Frame 52: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface
IEEE 802.3 Ethernet
Logical-Link Control
Spanning Tree Protocol
Protocol Identifier: Spanning Tree Protocol (0x0000)
Protocol Version Identifier: Spanning Tree (0)
BPDU Type: Configuration (0x00)
BPDU flags: 0x00
Root Identifier: 32768 / 1 / aa:bb:cc:00:01:00
Root Path Cost: 0
Bridge Identifier: 32768 / 1 / aa:bb:cc:00:01:00

Second Solution: Bonding

- To increase the uptime and throughput, we use multiple links. And configure them in such a way that we achieve **Load Balance** alongside of **Failover**

Second Solution: Bonding

By using bonding, we can increase the throughput by utilizing all links alongside of failover.




```
PC1 - SecureCRT
File Edit View Options Transfer Script Tools Window Help
Enter host <Alt+R>

PC1 x
NAME      : PC1[1]
IP/MASK   : 10.10.10.1/24
GATEWAY   : 0.0.0.0
DNS       :
MAC       : 00:50:79:66:68:00
LPORT    : 10007
RHOST:PORT : 192.168.48.128:10010
MTU      : 1500

PC1> ping 10.10.10.2
84 bytes from 10.10.10.2 icmp_seq=1 ttl=64 time=4.890 ms
84 bytes from 10.10.10.2 icmp_seq=2 ttl=64 time=4.331 ms
84 bytes from 10.10.10.2 icmp_seq=3 ttl=64 time=4.280 ms
84 bytes from 10.10.10.2 icmp_seq=4 ttl=64 time=3.689 ms
84 bytes from 10.10.10.2 icmp_seq=5 ttl=64 time=3.590 ms
```

```
PC3 - SecureCRT
File Edit View Options Transfer Script Tools Window Help
Enter host <Alt+R>

PC3 x
PC3>
PC3> sho ip
NAME      : PC3[1]
IP/MASK   : 10.10.10.2/24
GATEWAY   : 10.10.10.1
DNS       :
MAC       : 00:50:79:66:68:02
LPORT    : 10009
RHOST:PORT : 192.168.48.128:10012
MTU      : 1500

PC3> ping 10.10.10.1
84 bytes from 10.10.10.1 icmp_seq=1 ttl=64 time=10.704 ms
84 bytes from 10.10.10.1 icmp_seq=2 ttl=64 time=11.141 ms
84 bytes from 10.10.10.1 icmp_seq=3 ttl=64 time=10.881 ms
84 bytes from 10.10.10.1 icmp_seq=4 ttl=64 time=9.465 ms
84 bytes from 10.10.10.1 icmp_seq=5 ttl=64 time=8.068 ms
```

```
PC2 - SecureCRT
File Edit View Options Transfer Script Tools Window Help
Enter host <Alt+R>

PC2 x
NAME      : PC2[1]
IP/MASK   : 11.11.11.1/24
GATEWAY   : 0.0.0.0
DNS       :
MAC       : 00:50:79:66:68:01
LPORT    : 10013
RHOST:PORT : 192.168.48.128:10011
MTU      : 1500

PC2> ping 11.11.11.2
84 bytes from 11.11.11.2 icmp_seq=1 ttl=64 time=3.683 ms
84 bytes from 11.11.11.2 icmp_seq=2 ttl=64 time=4.021 ms
84 bytes from 11.11.11.2 icmp_seq=3 ttl=64 time=4.488 ms
84 bytes from 11.11.11.2 icmp_seq=4 ttl=64 time=3.712 ms
84 bytes from 11.11.11.2 icmp_seq=5 ttl=64 time=3.797 ms

PC2>
```

```
PC4 - SecureCRT
File Edit View Options Transfer Script Tools Window Help
Enter host <Alt+R>

PC4 x
PC4> sho ip
NAME      : PC4[1]
IP/MASK   : 11.11.11.2/24
GATEWAY   : 0.0.0.0
DNS       :
MAC       : 00:50:79:66:68:03
LPORT    : 10015
RHOST:PORT : 192.168.48.128:10014
MTU      : 1500

PC4> ping 11.11.11.1
84 bytes from 11.11.11.1 icmp_seq=1 ttl=64 time=4.875 ms
84 bytes from 11.11.11.1 icmp_seq=2 ttl=64 time=4.053 ms
84 bytes from 11.11.11.1 icmp_seq=3 ttl=64 time=3.945 ms
84 bytes from 11.11.11.1 icmp_seq=4 ttl=64 time=4.013 ms
84 bytes from 11.11.11.1 icmp_seq=5 ttl=64 time=4.013 ms

PC4>
```

EoIP Proposed Design

From SP Perspective

Additional things

- To extend a particular VLAN
 - Create a sub interface of that particular VLAN
 - Call that sub interface in the bridge
 - Apply the queue policy to EOIP interface to restrict the bandwidth.
- You can create multiple EOIP interface to extend multiple VLAN and apply the policy accordingly.

Question

Why are we creating multiple EoIP interface over different subnet?

We can create multiple EoIP tunnels by using the tunnel ID but you cannot apply the **Queue policy** in that scenario.

Multiple EoIP Interface

- There are many methods for multiple EoIP tunnels are to be reachable. Suggested method is given below.

Method 1: Configure GRE tunnel and run Routing Protocol on it

Method2: Configure GRE tunnel and add Static Routes

Creating GRE tunnel

Create a GRE tunnel over the Public IP

Site 1

Site 2

The image displays two side-by-side screenshots of a network configuration interface, likely from a Cisco IOS or similar device. Each screenshot shows the configuration for a GRE tunnel interface. The left screenshot is for Site 1, and the right screenshot is for Site 2. Both screenshots show the 'Interface List' tab with 'GRE Tunnel' selected. The configuration details for Site 1 are as follows:

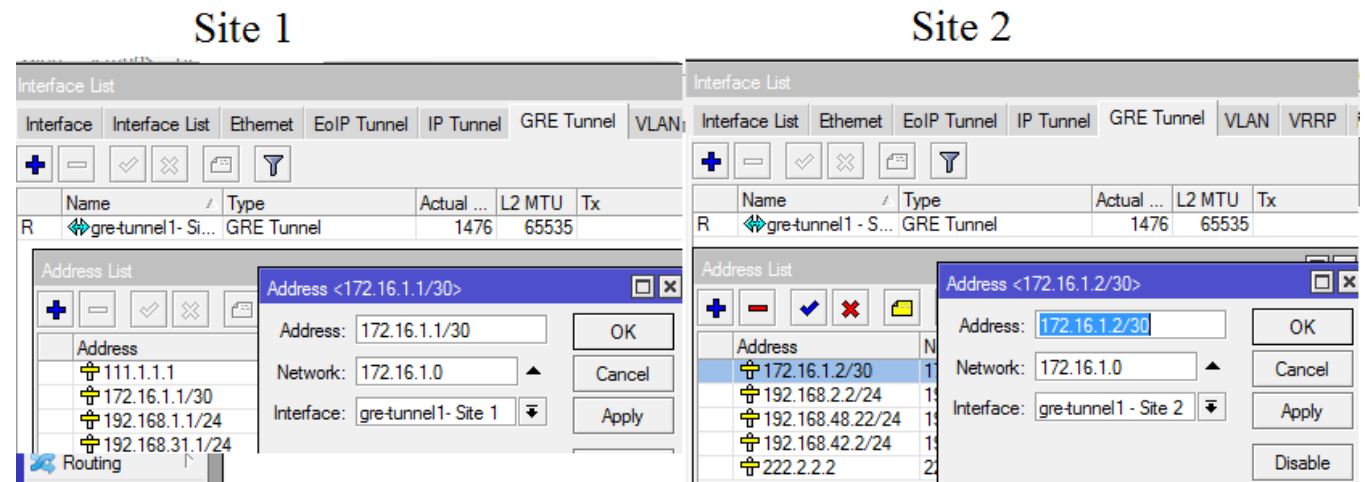
Field	Value
Name	gre-tunnel1 - Site 1
Type	GRE Tunnel
MTU	
Actual MTU	1476
L2 MTU	65535
Local Address	111.1.1.1
Remote Address	222.2.2.2

The right screenshot shows the configuration for Site 2:

Field	Value
Name	gre-tunnel1 - Site 2
Type	GRE Tunnel
MTU	
Actual MTU	1476
L2 MTU	65535
Local Address	222.2.2.2
Remote Address	111.1.1.1

Assign IP address to GRE

Assign the Private IP to GRE tunnel



Method1: Create and assign IP address on Interface and advertise in OSPF

- Create one Bridge Interface
- Configure multiple /32 IP on it
- Advertise the subnet and GRE interface IP in OSPF

The screenshot displays the configuration for two sites, Site 1 and Site 2, in a network management interface. A vertical red line separates the two sites.

Site 1 Configuration:

- Bridge:** Shows a bridge named 'B-EOIP' with two IP addresses assigned: 192.168.11.2 and 192.168.11.3, both on the 'B-EOIP' interface.
- OSPF:** Shows two networks advertised: 172.16.1.0/30 (backbone) and 192.168.11.0/24 (backbone).
- Route List:** Shows routes for 192.168.22.2 and 192.168.22.3, both with a gateway of 172.16.1.2 reachable via gre-tunnel1 - Site 1, with a distance of 110.

Site 2 Configuration:

- Bridge:** Shows a bridge named 'B-EOIP' with two IP addresses assigned: 192.168.22.2 and 192.168.22.3, both on the 'B-EOIP' interface.
- OSPF:** Shows two networks advertised: 172.16.1.0/30 (backbone) and 192.168.22.0/24 (backbone).
- Route List:** Shows routes for 192.168.11.2 and 192.168.11.3, both with a gateway of 172.16.1.1 reachable via gre-tunnel1 - Site 2, with a distance of 110.

Create EOIP tunnels

Create multiple EoIP tunnels over the Loopback configure at both end

The screenshot displays the configuration for two sites, Site 1 and Site 2, showing the configuration of EoIP tunnels. A vertical red line separates the two sites.

Site 1 Interface List:

Interface	Name	Type	Actual ...	L2 MTU	Tx	Rx
R	eoip-tunnel-VLAN2	EoIP Tunnel	1434	65535	0 bps	0
R	eoip-tunnel-VLAN3	EoIP Tunnel	1434	65535	0 bps	0

Site 1 Interface Configuration:

Interface	Name	Type	Actual MTU	L2 MTU	MAC Address	ARP	Local Address	Remote Address	Tunnel ID
<eoip-tunnel-VLAN2>	eoip-tunnel-VLAN2	EoIP Tunnel	1434	65535	02:A5:9D:4B:83:95	enabled	192.168.11.2	192.168.22.2	2
<eoip-tunnel-VLAN3>	eoip-tunnel-VLAN3	EoIP Tunnel	1434	65535	02:37:30:F2:51:BF	enabled	192.168.11.3	192.168.22.3	3

Site 2 Interface List:

Interface	Name	Type	Actual ...	L2 MTU	Tx	Rx
R	eoip-tunnel-VLAN2	EoIP Tunnel	1434	65535	0 bps	0 bps
R	eoip-tunnel-VLAN3	EoIP Tunnel	1434	65535	0 bps	0 bps

Site 2 Interface Configuration:

Interface	Name	Type	Actual MTU	L2 MTU	MAC Address	ARP	Local Address	Remote Address	Tunnel ID
<eoip-tunnel-VLAN2>	eoip-tunnel-VLAN2	EoIP Tunnel	1434	65535	02:C2:08:0C:F3:80	enabled	192.168.22.2	192.168.11.2	2
<eoip-tunnel-VLAN3>	eoip-tunnel-VLAN3	EoIP Tunnel	1434	65535	02:4A:69:AF:33:6D	enabled	192.168.22.3	192.168.11.3	3

Creating the Bridge for particular VLAN

Create a Bridge Interface and allocate the particular VLAN and EoIP tunnel into it

Site 1						Site 2					
Bridge						Bridge					
Bridge Ports Filters NAT Hosts						Bridge Ports Filters NAT Hosts					
+ - ✓ ✕ 📄 🔍						+ - ✓ ✕ 📄 🔍					
Interface	Bridge	Priority (...)	Path Cost	Role	Root P...	Interface	Bridge	Priorit...	Path Cost	Role	Root P...
↕eip-tunnel-VLAN2	B-VLAN2	80	10	designated port		↕eip-tunnel-VLAN2	B-VLAN2	80	10	root port	10
↕vlan2	B-VLAN2	80	10	designated port		↕vlan2	B-VLAN2	80	10	designated port	
↕eip-tunnel-VLAN3	B-VLAN3	80	10	designated port		↕eip-tunnel-VLAN3	B-VLAN3	80	10	root port	10
↕vlan3	B-VLAN3	80	10	designated port		↕vlan3	B-VLAN3	80	10	designated port	

Apply the Queue Policy

Use the destination IP address (Loopback IP of other end) in Queue policy.

Site 1

The screenshot shows the Mikrotik WinBox interface. The top window is the 'Queue List' dialog, which is open to the 'Simple Queues' tab. It displays a table with one entry: 'queue-VLAN2' with a target of '192.168.22.2' and upload/download max limits of '64k'. Below this, a 'Simple Queue <queue-VLAN2>' configuration window is open, showing 'Target Upload' and 'Target Download' settings. The 'Rate' is set to '1744 bps' and '1656 bps' respectively, with a 'Packet Rate' of '2 p/s'. A traffic graph shows upload and download rates. The bottom window is 'PC1 - SecureCRT', displaying a list of ICMP echo requests from 10.10.10.2 to 10.10.10.25, with response times ranging from approximately 3.28 ms to 4.32 ms.

#	Name	Target	Upload Max Limit	Download Max Limit	Packet Marks	Total M
0	queue-VLAN2	192.168.22.2	64k	64k		

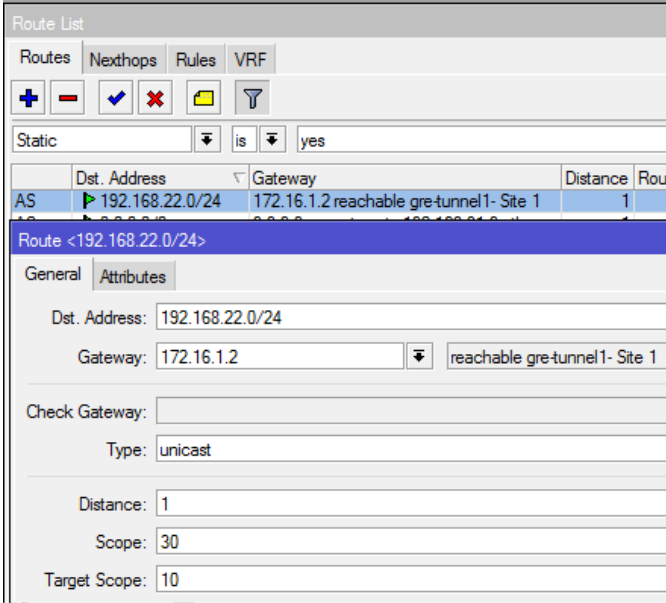
Rate	Target Upload	Target Download
Rate: 1744 bps	1744 bps	1656 bps
Packet Rate: 2 p/s	2 p/s	2 p/s

```
File Edit View Options Transfer Script Tools Window Help
Enter host <Alt+R>
PC1 x
84 bytes from 10.10.10.2: icmp_seq=360 ttl=64 time=3.286 ms
84 bytes from 10.10.10.2: icmp_seq=361 ttl=64 time=4.222 ms
84 bytes from 10.10.10.2: icmp_seq=362 ttl=64 time=3.562 ms
84 bytes from 10.10.10.2: icmp_seq=363 ttl=64 time=4.325 ms
84 bytes from 10.10.10.2: icmp_seq=364 ttl=64 time=3.829 ms
```

Method 2: By Static Route

Add the static for the subnet towards GRE tunnel destination

Site 1



Route List

AS	Dst. Address	Gateway	Distance	Route
AS	192.168.22.0/24	172.16.1.2 reachable gre-tunnel1- Site 1	1	

Route <192.168.22.0/24>

General

Dst. Address: 192.168.22.0/24

Gateway: 172.16.1.2 reachable gre-tunnel1- Site 1

Check Gateway:

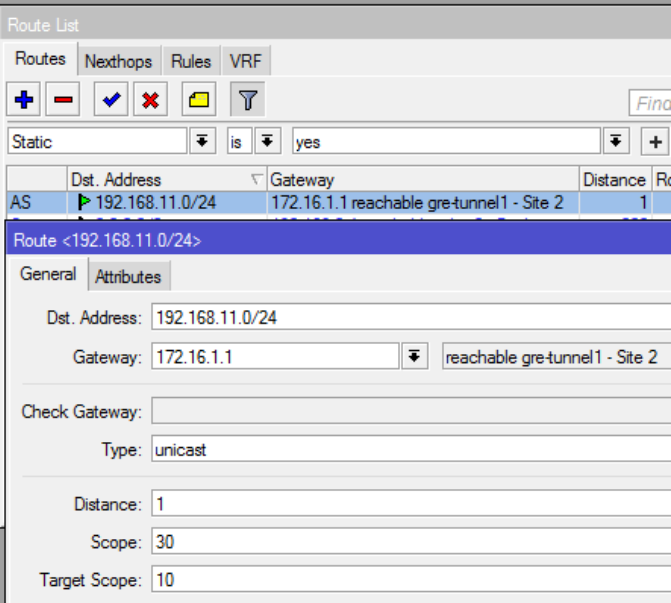
Type: unicast

Distance: 1

Scope: 30

Target Scope: 10

Site 2



Route List

AS	Dst. Address	Gateway	Distance	Route
AS	192.168.11.0/24	172.16.1.1 reachable gre-tunnel1 - Site 2	1	

Route <192.168.11.0/24>

General

Dst. Address: 192.168.11.0/24

Gateway: 172.16.1.1 reachable gre-tunnel1 - Site 2

Check Gateway:

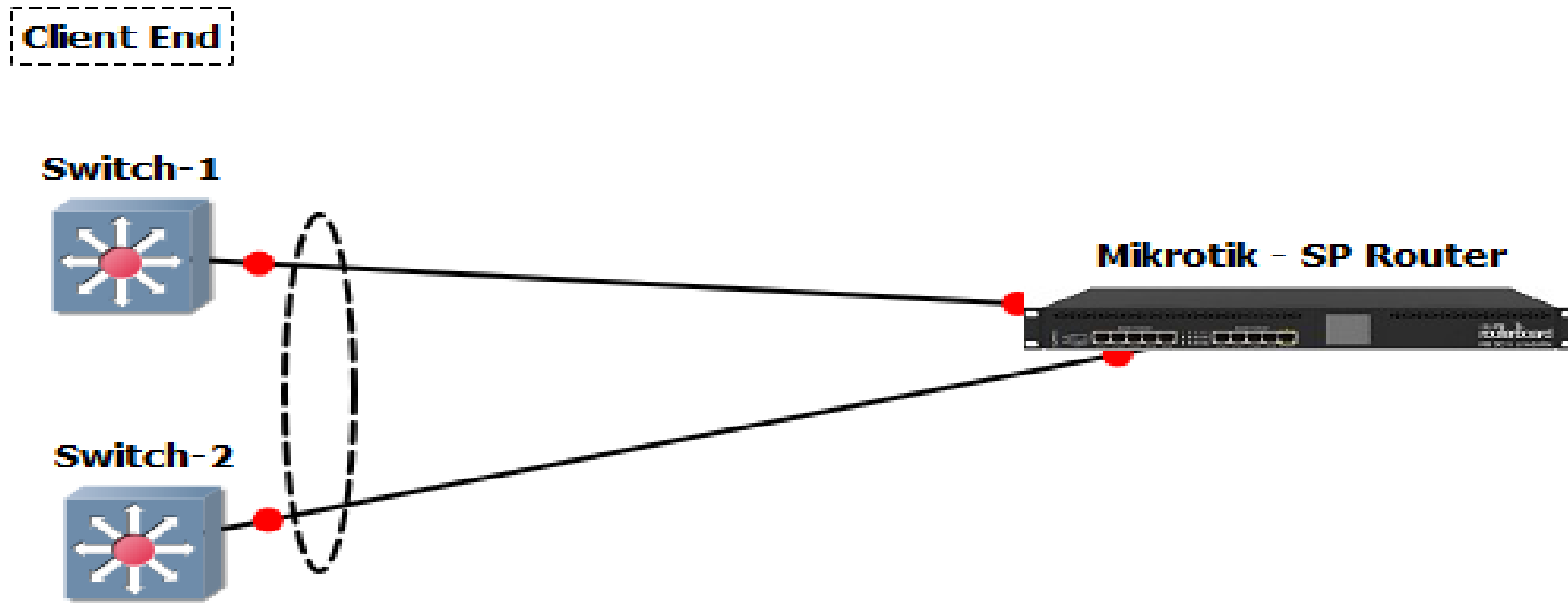
Type: unicast

Distance: 1

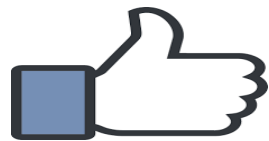
Scope: 30

Target Scope: 10

Home Assignment



MOEEZ AFTAB
0092-321-3955279



FB.COM/3BITS 1 BYTE