

# Manual:Interface/EoIP

From MikroTik Wiki  
< Manual:Interface

## Contents

- 1 Summary
- 2 Properties
- 3 Notes
- 4 Setup examples



## Summary

**Sub-menu:** /interface eoip

**Standards:** GRE RFC 1701

Ethernet over IP (EoIP) Tunneling is a MikroTik RouterOS protocol that creates an Ethernet tunnel between two routers on top of an IP connection. The EoIP tunnel may run over IPIP tunnel, PPTP tunnel or any other connection capable of transporting IP.

When the bridging function of the router is enabled, all Ethernet traffic (all Ethernet protocols) will be bridged just as if there where a physical Ethernet interface and cable between the two routers (with bridging enabled). This protocol makes multiple network schemes possible.

Network setups with EoIP interfaces:

- Possibility to bridge LANs over the Internet
- Possibility to bridge LANs over encrypted tunnels
- Possibility to bridge LANs over 802.11b 'ad-hoc' wireless networks

The EoIP protocol encapsulates Ethernet frames in GRE (IP protocol number 47) packets (just like PPTP) and sends them to the remote side of the EoIP tunnel.

## Properties

Property	Description
<code>arp</code> (disabled   enabled   proxy-arp   reply-only; Default: enabled)	Address Resolution Protocol mode. <ul style="list-style-type: none"><li>■ <code>disabled</code> - the interface will not use ARP</li><li>■ <code>enabled</code> - the interface will use ARP</li><li>■ <code>proxy-arp</code> - the interface will use the ARP proxy feature</li><li>■ <code>reply-only</code> - the interface will only reply to requests originated from combinations which are entered as static entries in the "/ip arp" table stored in the "/ip arp" table. Therefore for communications to be su</li></ul>
<code>clamp-tcp-mss</code> (yes	

<code>no</code> ; Default: <b>yes</b> )	
<b>dont-fragment</b> ( <i>inherit</i>   <i>no</i> ; Default: <b>no</b> )	
<b>dscp</b> ( <i>integer: 0-63</i> ; Default: <b>inherited</b> )	DSCP value of packet option means that dscp is inherited from packet to be encapsulated.
<b>ipsec-secret</b> ( <i>string</i> ; Default: )	When secret is specified for dynamic ipsec peer to address with pre-shared policy with default value phase2 uses sha1/aes local-address and remote-address the tunnel must be specified on the router to create valid ipsec tunnel
<b>keepalive</b> ( <i>integer[/time]</i> , <i>integer</i> ; 0..4294967295; Default: <b>10s,10</b> )	Tunnel keepalive parameter

time interval in which running flag will remain at remote end of tunnel. The configured time, retrieval of running flag is removed. The following are written in following format: KeepaliveInterval, KeepaliveRetries, where KeepaliveInterval is the keepalive interval and KeepaliveRetries is the number of retry attempts. The keepalive is set to 10 seconds and 10 retries.

12mtu (integer; read-only)

Layer2 Maximum tran

	Not configurable for E more>>
<code>local-address</code> (IP; Default: )	Source address of the packets, local on the r
<code>mac-address</code> (MAC; Default: )	Media Access Contro interface. The address authority IANA allows MAC addresses in the <b>00:00:5E:80:00:00 -</b> <b>00:00:5E:FF:FF:FF</b> fre
<code>mtu</code> (integer; Default: 1500)	Layer3 Maximum tran
<code>name</code> (string; Default: )	Interface name
<code>remote-address</code> (IP; Default: )	IP address of remote

# tunnel

`tunnel-id` (integer:  
65536; Default: )


# Unique tunnel identifier match other side of the

## Notes

`tunnel-id` is method of identifying tunnel. It must be unique for each EoIP tunnel.

`mtu` should be set to 1500 to eliminate packet refragmentation inside the tunnel (that allows transparent bridging of Ethernet-like networks, so that it would be possible to transport full-sized Ethernet frame over the tunnel).

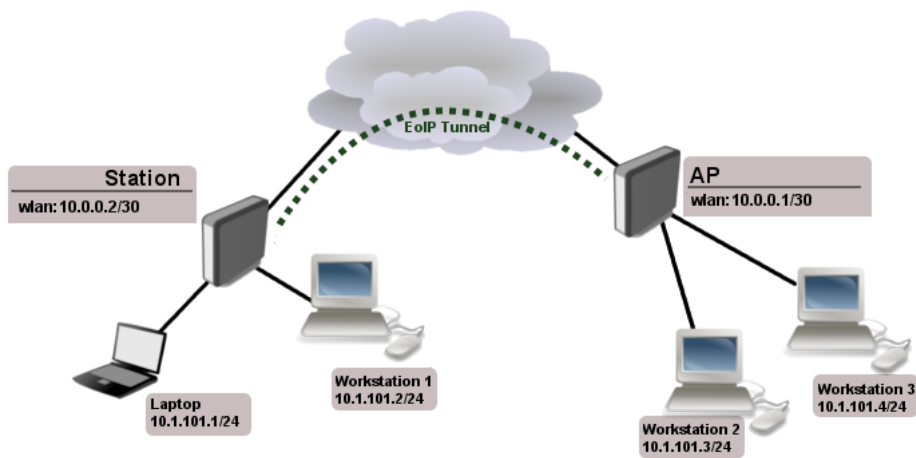
When bridging EoIP tunnels, it is highly recommended to set unique MAC addresses for each tunnel for the bridge algorithms to work correctly. For EoIP interfaces you can use MAC addresses that are in the range from **00:00:5E:80:00:00** - **00:00:5E:FF:FF:FF**, which IANA has reserved for such cases. Alternatively, you can set the second bit of the first byte to modify the auto-assigned address into a 'locally administered address', assigned by the network administrator and thus use any MAC address, you just need to ensure they are unique between the hosts connected to one bridge.

 **Note:** EoIP tunnel adds at least 42 byte overhead (8byte GRE + 14 byte Ethernet + 20 byte IP)

## Setup examples

Let us assume we want to bridge two networks: 'Office LAN' and 'Remote LAN'. By using EoIP setup can be made so that Office and Remote LANs are in the same Layer2 broadcast domain.

Consider following setup:



As you know wireless station cannot be bridged, to overcome this limitation (not involving WDS) we will create EoIP tunnel over the wireless link and bridge it with interfaces connected to local networks.

We will not cover wireless configuration in this example, let's assume that wireless link is already established

At first we create EoIP tunnel on our gateway ...

```
[admin@Our_GW] interface eoip> add name="eoip-remote" tunnel-id=0 \
\... remote-address=10.0.0.2
[admin@Our_GW] interface eoip> enable eoip-remote
[admin@Our_GW] interface eoip> print
Flags: X - disabled, R - running
0 name=eoip-remote mtu=1500 arp=enabled remote-address=10.0.0.2 tunnel-id=0
[admin@Our_GW] interface eoip>
```

... and on Remote router

```
[admin@Remote] interface eoip> add name="eoip" tunnel-id=0 \
\... remote-address=10.0.0.1
[admin@Remote] interface eoip> enable eoip-main
[admin@Remote] interface eoip> print
Flags: X - disabled, R - running
0 name=eoip mtu=1500 arp=enabled remote-address=10.0.0.1 tunnel-id=0
[admin@Remote] interface eoip>
```

Next step is to bridge local interfaces with EoIP tunnel On Our GW ...

```
[admin@Our_GW] interface bridge> add
[admin@Our_GW] interface bridge> print
Flags: X - disabled, R - running
0 R name="bridge1" mtu=1500 arp=enabled mac-address=00:00:00:00:00:00
protocol-mode=none priority=0x8000 auto-mac=yes
admin-mac=00:00:00:00:00:00 max-message-age=20s forward-delay=15s
transmit-hold-count=6 ageing-time=5m
[admin@Our_GW] interface bridge> port add bridge=bridge1 interface=eoip-remote
[admin@Our_GW] interface bridge> port add bridge=bridge1 interface=office-eth
[admin@Our_GW] interface bridge> port print
Flags: X - disabled, I - inactive, D - dynamic
# INTERFACE BRIDGE PRIORITY PATH-COST
0 eoip-remote bridge1 128 10
1 office-eth bridge1 128 10
[admin@Our_GW] interface bridge>
```

... and Remote router:

```
[admin@Remote] interface bridge> add
[admin@Remote] interface bridge> print
Flags: X - disabled, R - running
0 R name="bridge1" mtu=1500 arp=enabled mac-address=00:00:00:00:00:00
```

```
protocol-mode=none priority=0x8000 auto-mac=yes
admin-mac=00:00:00:00:00:00 max-message-age=20s forward-delay=15s
transmit-hold-count=6 ageing-time=5m
[admin@Remote] interface bridge> port add bridge=bridge1 interface=ether
[admin@Remote] interface bridge> port add bridge=bridge1 interface=eoip-main
[admin@Remote] interface bridge> port print
Flags: X - disabled, I - inactive, D - dynamic
#   INTERFACE      BRIDGE  PRIORITY  PATH-COST
0   ether          bridge1 128       10
1   eoip-main      bridge1 128       10
[admin@Remote] interface bridge>
```

Now both sites are in the same Layer2 broadcast domain. You can set up IP addresses from the same network on both sites.

**[ Top | Back to Content ]**

Retrieved from "<https://wiki.mikrotik.com/index.php?title=Manual:Interface/EoIP&oldid=29729>"

Categories: [Manual](#) | [VPN](#) | [Interface](#)

- This page was last edited on 6 September 2017, at 12:06.