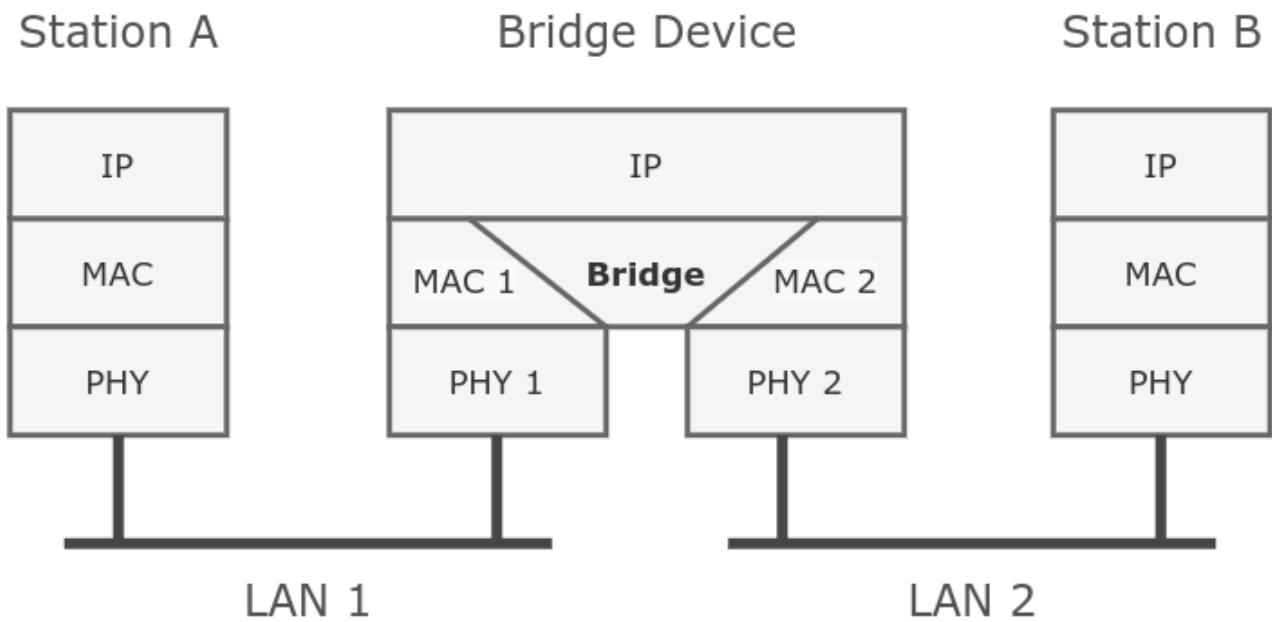


Bridging and Switching

- [Bridging and Switching](#)

Bridging and Switching

Summary



1. 桥接和交换 (桥接, Ethernet over IP, IEEE 802.11, AP, WDS, VLAN)

2. MAC 地址和 IP 地址的分配和冲突。桥接设备在 LAN 1 和 LAN 2 之间

3. LAN 1 和 LAN 2 之间的桥接设备 (EoIP) 和桥接设备 (IP

4. 桥接设备在 LAN 1 和 LAN 2 之间

5. 桥接设备在 LAN 1 和 LAN 2 之间

6. 桥接设备在 LAN 1 和 LAN 2 之间

7. 桥接设备在 LAN 1 和 LAN 2 之间

8. 桥接设备在 LAN 1 和 LAN 2 之间 (R/M)STP

9. 桥接设备在 LAN 1 和 LAN 2 之间

10. 桥接设备在 LAN 1 和 LAN 2 之间

11. 桥接设备在 LAN 1 和 LAN 2 之间

12. 桥接设备在 LAN 1 和 LAN 2 之间

13. 桥接设备在 LAN 1 和 LAN 2 之间

14. 桥接设备在 LAN 1 和 LAN 2 之间

15. 桥接设备在 LAN 1 和 LAN 2 之间

16. 桥接设备在 LAN 1 和 LAN 2 之间

17. 桥接设备在 LAN 1 和 LAN 2 之间

18. 桥接设备在 LAN 1 和 LAN 2 之间

19. 桥接设备在 LAN 1 和 LAN 2 之间

20. 桥接设备在 LAN 1 和 LAN 2 之间

21. 桥接设备在 LAN 1 和 LAN 2 之间

22. 桥接设备在 LAN 1 和 LAN 2 之间

23. 桥接设备在 LAN 1 和 LAN 2 之间

24. 桥接设备在 LAN 1 和 LAN 2 之间

25. 桥接设备在 LAN 1 和 LAN 2 之间

26. 桥接设备在 LAN 1 和 LAN 2 之间

27. 桥接设备在 LAN 1 和 LAN 2 之间

28. 桥接设备在 LAN 1 和 LAN 2 之间

29. 桥接设备在 LAN 1 和 LAN 2 之间

30. 桥接设备在 LAN 1 和 LAN 2 之间

31. 桥接设备在 LAN 1 和 LAN 2 之间

32. 桥接设备在 LAN 1 和 LAN 2 之间

33. 桥接设备在 LAN 1 和 LAN 2 之间

34. 桥接设备在 LAN 1 和 LAN 2 之间

35. 桥接设备在 LAN 1 和 LAN 2 之间

36. 桥接设备在 LAN 1 和 LAN 2 之间

37. 桥接设备在 LAN 1 和 LAN 2 之间

38. 桥接设备在 LAN 1 和 LAN 2 之间

39. 桥接设备在 LAN 1 和 LAN 2 之间

40. 桥接设备在 LAN 1 和 LAN 2 之间

41. 桥接设备在 LAN 1 和 LAN 2 之间

42. 桥接设备在 LAN 1 和 LAN 2 之间

43. 桥接设备在 LAN 1 和 LAN 2 之间

44. 桥接设备在 LAN 1 和 LAN 2 之间

45. 桥接设备在 LAN 1 和 LAN 2 之间

46. 桥接设备在 LAN 1 和 LAN 2 之间

47. 桥接设备在 LAN 1 和 LAN 2 之间

48. 桥接设备在 LAN 1 和 LAN 2 之间

49. 桥接设备在 LAN 1 和 LAN 2 之间

50. 桥接设备在 LAN 1 和 LAN 2 之间

51. 桥接设备在 LAN 1 和 LAN 2 之间

52. 桥接设备在 LAN 1 和 LAN 2 之间

53. 桥接设备在 LAN 1 和 LAN 2 之间

54. 桥接设备在 LAN 1 和 LAN 2 之间

55. 桥接设备在 LAN 1 和 LAN 2 之间

56. 桥接设备在 LAN 1 和 LAN 2 之间

57. 桥接设备在 LAN 1 和 LAN 2 之间

58. 桥接设备在 LAN 1 和 LAN 2 之间

59. 桥接设备在 LAN 1 和 LAN 2 之间

60. 桥接设备在 LAN 1 和 LAN 2 之间

61. 桥接设备在 LAN 1 和 LAN 2 之间

62. 桥接设备在 LAN 1 和 LAN 2 之间

63. 桥接设备在 LAN 1 和 LAN 2 之间

64. 桥接设备在 LAN 1 和 LAN 2 之间

65. 桥接设备在 LAN 1 和 LAN 2 之间

66. 桥接设备在 LAN 1 和 LAN 2 之间

67. 桥接设备在 LAN 1 和 LAN 2 之间

68. 桥接设备在 LAN 1 和 LAN 2 之间

69. 桥接设备在 LAN 1 和 LAN 2 之间

70. 桥接设备在 LAN 1 和 LAN 2 之间

71. 桥接设备在 LAN 1 和 LAN 2 之间

72. 桥接设备在 LAN 1 和 LAN 2 之间

73. 桥接设备在 LAN 1 和 LAN 2 之间

74. 桥接设备在 LAN 1 和 LAN 2 之间

75. 桥接设备在 LAN 1 和 LAN 2 之间

76. 桥接设备在 LAN 1 和 LAN 2 之间

77. 桥接设备在 LAN 1 和 LAN 2 之间

78. 桥接设备在 LAN 1 和 LAN 2 之间

79. 桥接设备在 LAN 1 和 LAN 2 之间

80. 桥接设备在 LAN 1 和 LAN 2 之间

81. 桥接设备在 LAN 1 和 LAN 2 之间

82. 桥接设备在 LAN 1 和 LAN 2 之间

83. 桥接设备在 LAN 1 和 LAN 2 之间

84. 桥接设备在 LAN 1 和 LAN 2 之间

85. 桥接设备在 LAN 1 和 LAN 2 之间

86. 桥接设备在 LAN 1 和 LAN 2 之间

87. 桥接设备在 LAN 1 和 LAN 2 之间

88. 桥接设备在 LAN 1 和 LAN 2 之间

89. 桥接设备在 LAN 1 和 LAN 2 之间

90. 桥接设备在 LAN 1 和 LAN 2 之间

91. 桥接设备在 LAN 1 和 LAN 2 之间

92. 桥接设备在 LAN 1 和 LAN 2 之间

93. 桥接设备在 LAN 1 和 LAN 2 之间

94. 桥接设备在 LAN 1 和 LAN 2 之间

95. 桥接设备在 LAN 1 和 LAN 2 之间

96. 桥接设备在 LAN 1 和 LAN 2 之间

97. 桥接设备在 LAN 1 和 LAN 2 之间

98. 桥接设备在 LAN 1 和 LAN 2 之间

99. 桥接设备在 LAN 1 和 LAN 2 之间

100. 桥接设备在 LAN 1 和 LAN 2 之间

<p>auto-mac (yes no; Default: yes)</p>	<p>auto-mac=yes 启用自动 MAC 地址生成。当设备检测到没有配置 MAC 地址的接口时，将自动为该接口生成 MAC 地址。</p> <ol style="list-style-type: none"> 生成随机 MAC 地址； 如果接口类型为 Wi-Fi 接口，则生成 Wi-Fi 接口的 MAC 地址； 如果接口类型为有线接口，则生成有线接口的 MAC 地址。 <p>默认情况下，设备会为所有接口生成 MAC 地址。如果希望为特定接口禁用自动 MAC 地址生成，可以在接口视图下配置 auto-mac=no。此外，还可以通过配置 admin-mac 来指定接口的 MAC 地址。</p> <p>auto-mac=no 禁用自动 MAC 地址生成，admin-mac 指定接口的 MAC 地址。</p>
<p>comment (string; Default:)</p>	<p>配置接口的描述信息。</p>
<p>dhcp-snooping (yes no; Default: no)</p>	<p>启用 DHCP Snooping 功能。该功能可以防止非法 DHCP 服务器在网络上分发 IP 地址，提高网络的安全性。配置 fast-path 和 fasttrack 可以优化 DHCP Snooping 的性能。</p>
<p>disabled (yes no; Default: no)</p>	<p>禁用接口。</p>
<p>ether-type (0x9100 0x8100 0x88a8; Default: 0x8100)</p>	<p>EtherType 值。EtherType 值用于标识 VLAN 帧的封装类型。默认值为 0x8100。可以通过配置 ether-type 来更改封装类型。vlan-filtering 用于配置 VLAN 过滤功能。</p> <p>yes 启用 VLAN 过滤功能。</p>
<p>fast-forward (yes no; Default: yes)</p>	<p>Fast Path 转发模式。该模式可以减少 CPU 的负担，提高转发效率。配置 2 个 Fast Path 可以进一步优化性能。</p>
<p>forward-delay (time; Default: 00:00:15)</p>	<p>转发延迟时间。该参数用于配置设备在转发数据包时的延迟时间。默认值为 15 秒。</p>

<p>forward-reserved-addresses (yes no; Default: no)</p>	<p>IEEE 802.1D 3024 MAC 01:80:C2:00:00:0x 01:80:C2:00:00:00 . R/M/STP 01:80:C2:00:00:00 01:80:C2:00:00:01 . 01:80:C2:00:00:02 . protocol-mode none 01:80:C2:00:00:00 . 01:80:C2:00:00:00 MAC 01:80:C2:00:00:00 01:80:C2:00:00:00 01:80:C2:00:00:00 01:80:C2:00:00:00 . 01:80:C2:00:00:00 (: 01:80:C2:00:00:00 , 01:80:C2:00:00:00 01:80:C2:00:00:00) 01:80:C2:00:00:00 01:80:C2:00:00:00 01:80:C2:00:00:00 01:80:C2:00:00:00 . RouterOS 01:80:C2:00:00:00 01:80:C2:00:00:00 MAC 01:80:C2:00:00:00 01:80:C2:00:00:00 .</p> <ul style="list-style-type: none"> • 01:80:C2:00:00:00 - 01:80:C2:00:00:00 (STP); • 01:80:C2:00:00:01 - 01:80:C2:00:00:01 ; • 01:80:C2:00:00:02 - 01:80:C2:00:00:02 (LACP); • 01:80:C2:00:00:03 - Dot1x 01:80:C2:00:00:03 01:80:C2:00:00:03 ; • 01:80:C2:00:00:08 - 01:80:C2:00:00:08 (802.1ad 01:80:C2:00:00:08 , ether-type=0x88a8 01:80:C2:00:00:08)); • 01:80:C2:00:00:0D - VLAN 01:80:C2:00:00:0D (802.1ad 01:80:C2:00:00:0D , ether-type=0x88a8 01:80:C2:00:00:0D)); • 01:80:C2:00:00:0E - 01:80:C2:00:00:0E , 01:80:C2:00:00:0E 01:80:C2:00:00:0E ; <p>MAC 01:80:C2:00:00:01 , 01:80:C2:00:00:01 .</p>
<p>frame-types (admit-all admit-only-untagged-and-priority-tagged admit-only-vlan-tagged; Default: admit-all)</p>	<p>01:80:C2:00:00:00 01:80:C2:00:00:00 01:80:C2:00:00:00 . 01:80:C2:00:00:00 vlan-filtering yes 01:80:C2:00:00:00 01:80:C2:00:00:00 .</p>
<p>igmp-snooping (yes no; Default: no)</p>	<p>01:80:C2:00:00:00 01:80:C2:00:00:00 01:80:C2:00:00:00 01:80:C2:00:00:00 01:80:C2:00:00:00 01:80:C2:00:00:00 01:80:C2:00:00:00 .</p>
<p>igmp-version (2 3; Default: 2)</p>	<p>01:80:C2:00:00:00 IGMP 01:80:C2:00:00:00 01:80:C2:00:00:00 01:80:C2:00:00:00 IGMP 01:80:C2:00:00:00 . 01:80:C2:00:00:00 igmp-snooping multicast-querier yes 01:80:C2:00:00:00 01:80:C2:00:00:00 .</p>
<p>ingress-filtering (yes no; Default: yes)</p>	<p>VLAN 01:80:C2:00:00:00 01:80:C2:00:00:00 . 01:80:C2:00:00:00 01:80:C2:00:00:00 VLAN 01:80:C2:00:00:00 VLAN ID 01:80:C2:00:00:00 01:80:C2:00:00:00 . 01:80:C2:00:00:00 VLAN 01:80:C2:00:00:00 VLAN 01:80:C2:00:00:00 (01:80:C2:00:00:00) 01:80:C2:00:00:00 . 01:80:C2:00:00:00 01:80:C2:00:00:00 (01:80:C2:00:00:00) 01:80:C2:00:00:00 . 01:80:C2:00:00:00 frame-types 01:80:C2:00:00:00 01:80:C2:00:00:00 , 01:80:C2:00:00:00 01:80:C2:00:00:00 01:80:C2:00:00:00 . 01:80:C2:00:00:00 vlan-filtering yes 01:80:C2:00:00:00 01:80:C2:00:00:00 . 01:80:C2:00:00:00 RouterOS v7 01:80:C2:00:00:00 01:80:C2:00:00:00 .</p>
<p>l2mtu (read-only; Default:)</p>	<p>L2MTU 01:80:C2:00:00:00 01:80:C2:00:00:00 MAC 01:80:C2:00:00:00 01:80:C2:00:00:00 01:80:C2:00:00:00 . L2MTU 01:80:C2:00:00:00 01:80:C2:00:00:00 , 01:80:C2:00:00:00 01:80:C2:00:00:00 L2MTU 01:80:C2:00:00:00 . 01:80:C2:00:00:00 01:80:C2:00:00:00 .</p>

<p>last-member-interval (<i>time</i>; Default: 1s)</p>	<p>IGMP/MLD 消息的发送间隔。当接口收到 IGMP/MLD 消息时，设备会向该接口发送成员查询消息。成员查询消息的发送间隔由 last-member-interval 参数决定。该参数的默认值为 1s。</p> <p>配置命令： <pre>last-member-interval <i>interval</i> last-member-query-count <i>count</i></pre> </p> <p>参数说明： <i>interval</i>：成员查询消息的发送间隔，单位为秒。 <i>count</i>：成员查询消息的发送次数。</p> <p>缺省配置： <pre>last-member-interval 1 last-member-query-count 2</pre> </p> <p>注意： 1. 该参数仅在接口上生效。 2. 该参数与 fast-leave 参数互斥。当 fast-leave 参数配置为 yes 时，该参数无效。</p>
<p>last-member-query-count (<i>integer: 0..4294967295</i>; Default: 2)</p>	<p>成员查询消息的发送次数。该参数的默认值为 2。</p> <p>配置命令： <pre>last-member-interval <i>interval</i> last-member-query-count <i>count</i></pre> </p> <p>参数说明： <i>count</i>：成员查询消息的发送次数。</p> <p>缺省配置： <pre>last-member-interval 1 last-member-query-count 2</pre> </p>
<p>max-hops (<i>integer: 6..40</i>; Default: 20)</p>	<p>MSTP 消息的发送跳数。该参数的默认值为 20。</p> <p>配置命令： <pre>max-hops <i>hops</i></pre> </p> <p>参数说明： <i>hops</i>：MSTP 消息的发送跳数。</p> <p>缺省配置： <pre>max-hops 20</pre> </p>
<p>max-learned-entries (<i>integer: 0..4294967295 auto unlimited</i>; Default: auto)</p>	<p>设备学习到的 MAC 地址表项的最大数量。该参数的默认值为 auto。</p> <p>配置命令： <pre>max-learned-entries <i>entries</i></pre> </p> <p>参数说明： <i>entries</i>：设备学习到的 MAC 地址表项的最大数量。支持 auto 和 unlimited 两种取值。</p> <p>缺省配置： <pre>max-learned-entries auto</pre> </p> <p>注意： 1. 该参数仅在接口上生效。 2. 当 RAM 容量较小时，该参数的取值应适当减小。支持的取值如下： <ul style="list-style-type: none"> 8192 (64 MB); 16384 (128 MB); 256MB: 32768; 512MB: 65536; 1024MB 及以上 : 131072. </p> <p>配置示例： <pre>max-learned-entries unlimited</pre> </p> <p>注意： 1. 该参数与 protocol-mode 参数互斥。当 protocol-mode 参数配置为 stp 或 rstp 时，该参数无效。 2. 该参数与 RouterOS 7.16 及以上版本互斥。当 RouterOS 版本为 7.16 及以上时，该参数无效。</p>
<p>max-message-age (<i>time: 6s..40s</i>; Default: 00:00:20)</p>	<p>BPDU 消息的 Max Age 值。该参数的默认值为 00:00:20。</p> <p>配置命令： <pre>max-message-age <i>age</i></pre> </p> <p>参数说明： <i>age</i>：BPDU 消息的 Max Age 值。</p> <p>缺省配置： <pre>max-message-age 00:00:20</pre> </p> <p>注意： 1. 该参数仅在接口上生效。 2. 该参数与 protocol-mode 参数互斥。当 protocol-mode 参数配置为 stp 或 rstp 时，该参数无效。</p>
<p>membership-interval (<i>time</i>; Default: 4m20s)</p>	<p>成员查询消息的发送间隔。该参数的默认值为 4m20s。</p> <p>配置命令： <pre>membership-interval <i>interval</i></pre> </p> <p>参数说明： <i>interval</i>：成员查询消息的发送间隔。</p> <p>缺省配置： <pre>membership-interval 4m20s</pre> </p> <p>注意： 1. 该参数仅在接口上生效。 2. 该参数与 igmp-snooping 参数互斥。当 igmp-snooping 参数配置为 yes 时，该参数无效。</p>

<p>mld-version (1 2; Default: 1)</p>	<p>MLD 1 2 3 MLD 1 2 3 . 1 2 3 MLD 1 2 3 MLD 1 2 3 1 2 3 . IPv6 1 2 3 , igmp-snooping 1 multicast-querier 1 yes 1 1 1 .</p>
<p>mtu (integer; Default: auto)</p>	<p>(MTU) 1 2 3 4 5 , 1 2 3 4 5 MTU 1 . 1 2 3 4 5 MTU 1 1500 . MTU 1 2 3 4 5 , L2MTU 1 2 3 4 5 L2MTU 1 2 . 1 2 3 4 5 L2MTU 1 actual-mtu (mtu 1 2 3 4 5) 1 2 3 , 1 2 3 4 5 mtu=auto 1 2 1 2 3 . VLAN 1 2 3 4 5 VLAN 1 2 3 1500 1 2 3 MTU 1 2 3 , 1 2 3 MTU 1 2 3 1 2 3 4 5 .</p>
<p>multicast-querier (yes no; Default: no)</p>	<p>IGMP/MLD 1 2 3 4 5 , 1 2 3 IGMP/MLD 1 2 3 IGMP/MLD 1 2 3 . PIM(1 2 3 4 5) 1 2 3 IGMP 1 2 3 4 5 . 1 2 3 IGMP/MLD 1 2 3 4 5 IGMP/MLD 1 2 3 4 5 1 2 3 . 1 2 3 Layer 2 1 2 3 4 5 (PIM 1 2 3 4 5 IGMP 1 2 3) 1 2 3 4 5 . Layer 2 1 2 3 4 5 1 2 3 4 5 (MDB) 1 2 3 4 5 1 2 3 , 1 2 3 4 5 IGMP/MLD 1 2 3 4 5 . 1 2 3 IGMP/MLD 1 2 3 4 5 . IGMP 1 2 3 IPv4 0.0.0.0 1 2 3 4 5 , MLD 1 2 3 4 5 1 2 3 IPv6 1 2 3 4 5 . 1 2 3 IGMP/MLD 1 2 3 4 5 1 2 3 4 5 1 2 3 (1 2 3 4 5 igmp-querier 1 2 3 mld-querier 1 2 3). 1 2 3 igmp-snooping 1 yes 1 2 3 4 5 1 2 3 .</p>

multicast-router (*disabled* | *permanent* | *temporary-query*; Default: **temporary-query**)

```
#####  #####  #####  #####  #####  #####
#####  #####  .#####  #####  #####
#####  IGMP/MLD #####  #####  #####  .#####
#####  #####  #####  #####  #####  #####
.#####  #####  #####  #####  #####
#####  #####  #####  #####  #####  #####
#####  #####  .#####  igmp-snooping ##### yes #####
#####  #####  #####  .

• disabled - #####  #####  #####
#####  #####  #####  #####
#####  #####  #####  #####  IGMP/MLD
#####  #####  #####  #####  #####
#####

• permanent - #####  #####  #####
#####  #####  #####  .#####  #####
#####  #####  IGMP/MLD #####  #####  #####
#####  #####  #####  .#####
#####  #####  #####  #####
#####

• temporary-query - IGMP/MLD #####  #####
#####  #####  #####  #####  #####
#####  #####
```

name (text; Default: **bridgeN**)

```
#####  #####  #####  .
```

port-cost-mode (*long | short*; Default: **long**)

配置端口成本时，可以指定使用 long 或 short 模式。path-cost 命令用于配置端口的成本，internal-path-cost 命令用于配置内部端口的成本。默认情况下，使用 long 模式。配置示例如下：

Data rate	Long	Short
100 Gbps	200,000	19
50 Gbps	400	1
40 Gbps	500	1
25 Gbps	800	1
10 Gbps	2,000	2
1 Gbps	20,000	4
100 Mbps	200,000	19
10 Mbps	2,000,000	100

配置端口成本时，可以指定使用 long 或 short 模式。path-cost 命令用于配置端口的成本，internal-path-cost 命令用于配置内部端口的成本。默认情况下，使用 long 模式。配置示例如下：

配置示例（：VLAN, EoIP, VXLAN）Wi-Fi, 60GHz 配置示例，配置示例 10 配置示例。

配置示例（：Wi-Fi, PPP, VPLS）配置示例，配置示例 20,000, 配置示例 10 配置示例。配置示例 datapath.bridge-cost 配置示例。

port monitor 配置示例 配置示例 配置示例 配置示例。

配置示例 protocol-mode stp, rstp, mstp 配置示例。

priority (*integer: 0..65535 decimal format or 0x0000-0xffff hex format*; Default: **32768 / 0x8000**)

配置 R/STP 根桥（root bridge）时，可以指定 priority 值。MSTP 根桥 CIST 根桥 IST 根桥（regional root bridge）配置示例。配置示例 protocol-mode none 配置示例。

protocol-mode (*none | rstp | stp | mstp*; Default: **rstp**)

配置 STP 模式时，可以指定 protocol-mode 为 none、rstp、stp 或 mstp。默认情况下，使用 rstp 模式。配置示例如下：

配置示例 (STP) 配置示例 配置示例 配置示例 (RSTP) 配置示例 LAN 配置示例 配置示例。

配置示例 RSTP 配置示例 配置示例 配置示例 配置示例 配置示例。

配置示例 MSTP 配置示例 VLAN 配置示例 配置示例 配置示例。

配置示例 01:80:C2:00:00:0x 配置示例 MAC 配置示例 配置示例 protocol-mode=none 配置示例，RouterOS v7.16 配置示例 forward-reserved-addresses 配置示例 配置示例。

pvid (*integer: 1..4094*; Default: **1**)

配置 VLAN ID (PVID) 时，可以指定 pvid 值。配置示例如下：

配置示例 VLAN 配置示例 IP 配置示例 配置示例 配置示例 vlan-filtering yes 配置示例。

querier-interval (<i>time</i> ; Default: 4m15s)	<pre> [admin@MikroTik] /interface bridge add [admin@MikroTik] /interface bridge print Flags: X - disabled, R - running 0 R name="bridge1" mtu=auto actual-mtu=1500 l2mtu=65535 arp=enabled arp-timeout=auto mac-address=5E:D2:42:95:56:7F protocol-mode=rstp fast-forward=yes igmp-snooping=no auto-mac=yes ageing-time=5m priority=0x8000 max-message-age=20s forward- </pre>
query-interval (<i>time</i> ; Default: 2m5s)	<pre> [admin@MikroTik] /interface bridge add [admin@MikroTik] /interface bridge print Flags: X - disabled, R - running 0 R name="bridge1" mtu=auto actual-mtu=1500 l2mtu=65535 arp=enabled arp-timeout=auto mac-address=5E:D2:42:95:56:7F protocol-mode=rstp fast-forward=yes igmp-snooping=no multicast-querier=yes auto-mac=yes ageing-time=5m priority=0x8000 max-message-age=20s forward- </pre>
query-response-interval (<i>time</i> ; Default: 10s)	<pre> [admin@MikroTik] /interface bridge add [admin@MikroTik] /interface bridge print Flags: X - disabled, R - running 0 R name="bridge1" mtu=auto actual-mtu=1500 l2mtu=65535 arp=enabled arp-timeout=auto mac-address=5E:D2:42:95:56:7F protocol-mode=rstp fast-forward=yes igmp-snooping=no multicast-querier=yes query-response-interval=10s auto-mac=yes ageing-time=5m priority=0x8000 max-message-age=20s forward- </pre>
region-name (<i>text</i> ; Default:)	<pre> [admin@MikroTik] /interface bridge add [admin@MikroTik] /interface bridge print Flags: X - disabled, R - running 0 R name="bridge1" mtu=auto actual-mtu=1500 l2mtu=65535 arp=enabled arp-timeout=auto mac-address=5E:D2:42:95:56:7F protocol-mode=rstp fast-forward=yes igmp-snooping=no multicast-querier=yes query-response-interval=10s region-name=rstp auto-mac=yes ageing-time=5m priority=0x8000 max-message-age=20s forward- </pre>
region-revision (<i>integer: 0..65535</i> ; Default: 0)	<pre> [admin@MikroTik] /interface bridge add [admin@MikroTik] /interface bridge print Flags: X - disabled, R - running 0 R name="bridge1" mtu=auto actual-mtu=1500 l2mtu=65535 arp=enabled arp-timeout=auto mac-address=5E:D2:42:95:56:7F protocol-mode=rstp fast-forward=yes igmp-snooping=no multicast-querier=yes query-response-interval=10s region-name=rstp region-revision=0 auto-mac=yes ageing-time=5m priority=0x8000 max-message-age=20s forward- </pre>
startup-query-count (<i>integer: 0..4294967295</i> ; Default: 2)	<pre> [admin@MikroTik] /interface bridge add [admin@MikroTik] /interface bridge print Flags: X - disabled, R - running 0 R name="bridge1" mtu=auto actual-mtu=1500 l2mtu=65535 arp=enabled arp-timeout=auto mac-address=5E:D2:42:95:56:7F protocol-mode=rstp fast-forward=yes igmp-snooping=no multicast-querier=yes query-response-interval=10s region-name=rstp region-revision=0 startup-query-count=2 auto-mac=yes ageing-time=5m priority=0x8000 max-message-age=20s forward- </pre>
startup-query-interval (<i>time</i> ; Default: 31s250ms)	<pre> [admin@MikroTik] /interface bridge add [admin@MikroTik] /interface bridge print Flags: X - disabled, R - running 0 R name="bridge1" mtu=auto actual-mtu=1500 l2mtu=65535 arp=enabled arp-timeout=auto mac-address=5E:D2:42:95:56:7F protocol-mode=rstp fast-forward=yes igmp-snooping=no multicast-querier=yes query-response-interval=10s region-name=rstp region-revision=0 startup-query-count=2 startup-query-interval=31s250ms auto-mac=yes ageing-time=5m priority=0x8000 max-message-age=20s forward- </pre>
transmit-hold-count (<i>integer: 1..10</i> ; Default: 6)	<pre> [admin@MikroTik] /interface bridge add [admin@MikroTik] /interface bridge print Flags: X - disabled, R - running 0 R name="bridge1" mtu=auto actual-mtu=1500 l2mtu=65535 arp=enabled arp-timeout=auto mac-address=5E:D2:42:95:56:7F protocol-mode=rstp fast-forward=yes igmp-snooping=no multicast-querier=yes query-response-interval=10s region-name=rstp region-revision=0 startup-query-count=2 startup-query-interval=31s250ms transmit-hold-count=6 auto-mac=yes ageing-time=5m priority=0x8000 max-message-age=20s forward- </pre>
vlan-filtering (<i>yes no</i> ; Default: no)	<pre> [admin@MikroTik] /interface bridge add [admin@MikroTik] /interface bridge print Flags: X - disabled, R - running 0 R name="bridge1" mtu=auto actual-mtu=1500 l2mtu=65535 arp=enabled arp-timeout=auto mac-address=5E:D2:42:95:56:7F protocol-mode=rstp fast-forward=yes igmp-snooping=no multicast-querier=yes query-response-interval=10s region-name=rstp region-revision=0 startup-query-count=2 startup-query-interval=31s250ms transmit-hold-count=6 vlan-filtering=no auto-mac=yes ageing-time=5m priority=0x8000 max-message-age=20s forward- </pre>

```

[admin@MikroTik] /interface bridge add
[admin@MikroTik] /interface bridge print
Flags: X - disabled, R - running
0 R name="bridge1" mtu=auto actual-mtu=1500 l2mtu=65535 arp=enabled arp-timeout=auto mac-address=5E:D2:42:95:56:7F protocol-mode=rstp fast-forward=yes igmp-snooping=no multicast-querier=yes query-response-interval=10s region-name=rstp region-revision=0 startup-query-count=2 startup-query-interval=31s250ms transmit-hold-count=6 vlan-filtering=no auto-mac=yes ageing-time=5m priority=0x8000 max-message-age=20s forward-

```

??

L2 `arp` `arp-timeout` `mac-address` `protocol-mode` `fast-forward` :

```

[admin@MikroTik] > interface bridge add
[admin@MikroTik] > interface bridge print
Flags: X - disabled, R - running
0 R name="bridge1" mtu=auto actual-mtu=1500 l2mtu=65535 arp=enabled arp-timeout=auto mac-address=5E:D2:42:95:56:7F protocol-mode=rstp fast-forward=yes igmp-snooping=no auto-mac=yes ageing-time=5m priority=0x8000 max-message-age=20s forward-

```

```
delay=15s transmit-hold-count=6 vlan-filtering=no
dhcp-snooping=no
```

???? ?????

?? ???? ? ? ???? monitor ???? .

?? ? : /interface bridge monitor

??	??
bridge-id (<i>priority.MAC address</i>)	?? ?? ???? ?? ???? .??? MAC ?? ???? ???? .
current-mac-address (<i>MAC address</i>)	???? ? MAC ?? .
designated-port-count (<i>integer</i>)	?? ?? ? ? .
declared-vlan-ids (<i>integer 1..4094</i>)	?? ???? MVRP ????_ ? ?? ?? VLAN.
fast-forward (<i>yes no</i>)	?? fast-forward? ???? ?? ? .
igmp-querier (<i>none interface & IPv4 address</i>)	?? IGMP ???? ?? ? ? IP ?? ???? .?? ? IGMP ???? ,?? ?? IGMP ?? (IGMP ?? ? PIM ??)? ???? ???? . ???? ? igmp-snooping ? ???? ?? ???? .
mld-querier (<i>none interface & IPv6 address</i>)	?? MLD ???? ?? ? ? IPv6 ?? ???? .?? ? MLD ???? ,?? ?? MLD ???? ???? .???? ? igmp- snooping ? ???? ? IPv6 ?? ? ?? ???? .
mst-config-digest (<i>integer</i>)	VLAN ???? MST ???? ID? ?? ? ? .
multicast-router (<i>yes no</i>)	?? ???? ???? ???? .???? ? igmp-snooping ? ???? ? ???? .
port-count (<i>integer</i>)	?? ?? ? .
regional-root-bridge-id (<i>priority.MAC address</i>)	?? ? ID? bridge-priority.bridge-MAC-address ???? ???? .? ?? MSTP? ???? ???? ???? .
registered-vlan-ids (<i>integer 1..4094</i>)	?? ???? MVRP ????_ ? ?? ?? VLANs.

root-bridge (yes no)	yes no
root-bridge-id (priority.MAC address)	priority ID MAC address
root-path-cost (integer)	integer
root-port (name)	name
state (enabled disabled)	state

```
[admin@MikroTik] /interface/bridge monitor bridge1
state: enabled
current-mac-address: 2C:C8:1B:FF:92:F4
bridge-id: 0x1000.2C:C8:1B:FF:92:F4
root-bridge: yes
root-bridge-id: 0x1000.2C:C8:1B:FF:92:F4
regional-root-bridge-id: 0x1000.2C:C8:1B:FF:92:F4
root-path-cost: 0
root-port: none
port-count: 2
designated-port-count: 2
mst-config-digest: d2b171a8ad95f593c241fc33d419a88c
fast-forward: no
multicast-router: no
igmp-querier: none
mld-querier: none
declared-vlan-ids: 1
registered-vlan-ids: 1
```

???? ? ???? ?

RouterOS `bridge` `monitor` `bridge1` `state: enabled` `current-mac-address: 2C:C8:1B:FF:92:F4` `bridge-id: 0x1000.2C:C8:1B:FF:92:F4` `root-bridge: yes` `root-bridge-id: 0x1000.2C:C8:1B:FF:92:F4` `regional-root-bridge-id: 0x1000.2C:C8:1B:FF:92:F4` `root-path-cost: 0` `root-port: none` `port-count: 2` `designated-port-count: 2` `mst-config-digest: d2b171a8ad95f593c241fc33d419a88c` `fast-forward: no` `multicast-router: no` `igmp-querier: none` `mld-querier: none` `declared-vlan-ids: 1` `registered-vlan-ids: 1`

RouterOS 支持 IEEE 802.1W 标准，支持 4096 个 VLAN ID。支持的 VLAN ID 范围：0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440。

STP 协议在 RouterOS 中支持 STP, RSTP, MSTP。STP 协议用于防止网络环路，通过阻塞冗余链路来实现。RSTP 是 STP 的改进版本，收敛速度更快。MSTP 支持基于 VLAN 的实例。在 RouterOS 中配置 STP 可以使用 `protocol-mode` 选项。

RouterOS 支持 (RouterOS bridge) 桥接模式下的 PVST 协议。PVST 使用 MAC 地址 01:00:0C:CC:CC:CD 作为桥接地址。RouterOS 支持 / 分隔符来配置不同的 VLAN。

IEEE 802.1ad 标准定义了 VLAN 帧格式，IEEE 802.1Q 标准定义了 VLAN 帧格式。BPDU 帧格式遵循 IEEE 802.1ad 标准。Layer2 帧格式支持 VLAN。RSTP 帧格式支持 (R/M)STP。

??? STP

STP 协议在 RouterOS 中支持 STP, RSTP, MSTP。STP 协议用于防止网络环路，通过阻塞冗余链路来实现。

(R/M)STP 支持 STP 和 BPDU 帧格式。RSTP 支持 (R/M)STP 帧格式。

?? ?? ??

BPDU 帧格式支持 BPDU 帧格式。BPDU 帧格式支持 BPDU 帧格式。

```

/interface bridge
add name=bridge1

/interface bridge port
add bridge=bridge1 interface=ether1 edge=yes
add bridge=bridge1 interface=ether2

```

??? BPDU? ??

ACL NAT STP/RSTP/MSTP BPDU BPDU
ACL BPDU
:

CRS3xx :

```
/interface ethernet switch rule
add dst-mac-address=01:80:C2:00:00:00/FF:FF:FF:FF:FF:FF new-dst-ports="" ports=ether1
switch=switch1
```

CRS1xx/CRS2xx (ACL) :

```
/interface ethernet switch acl
add action=drop mac-dst-address=01:80:C2:00:00:00 src-ports=ether1
```

ether1 BPDU .

BPDU BPDU
BPDU ID BPDU ,
BPDU (flap)

BPDU ?? ???

ether1 BPDU ,

```
/interface bridge
add name=bridg1
/interface bridge port
add bridge=bridg1 interface=ether1 bpdu-guard=yes
add bridge=bridg1 interface=ether2
```

?? ?? ???

1. 配置 ether1 接口，设置 restricted-role=yes，并配置 CIST 和 MSTI。

```

/interface bridge
add name=bridge1
/interface bridge port
add bridge=bridge1 interface=ether1 restricted-role=yes
add bridge=bridge1 interface=ether2
[admin@MikroTik] /interface/bridge/port monitor [find]
      interface: ether1                ether2
      status: in-bridge                in-bridge
      port-id: 0x80.1                  0x80.2
      role: alternate-port             designated-port
      edge-port: no                    yes
edge-port-discovery: yes              yes
point-to-point-port: yes              yes
      external-fdb: no                 no
      sending-rstp: yes                 yes
      learning: no                     yes
      forwarding: no                   yes
      actual-path-cost: 2000            2000
internal-root-path-cost: 2000
      designated-bridge-id: 0x7000.64:D1:54:C7:3A:6E
designated-internal-cost: 0             0
      designated-port-id: 0x80.1        0x80.2
designated-remaining-hops: 20           20
      tx-rx-bpdu: 2/363                 4/1049
discard-transitions: 0                 0
forward-transitions: 0                 0
      tx-rx-tc: 0/2                     2/4
      topology-changes: 0                1
last-topology-change:                  34m53s
      multicast-router: no               yes
      hw-offload-group: switch1          switch1
      declared-vlan-ids:
      registered-vlan-ids:
  
```


bridge-fast-path-packets (<i>integer</i> ; Default:)	Fast Path
bridge-fast-path-bytes (<i>integer</i> ; Default:)	Fast Path
bridge-fast-forward-packets (<i>integer</i> ; Default:)	Fast Forward
bridge-fast-forward-bytes (<i>integer</i> ; Default:)	Fast Forward

[ip-firewall](#) [Simple Queues](#) [Queue Trees](#) [postrouting](#)
[VLAN](#) [PPPoE](#) [Simple Queues](#) [Queue Trees](#)

?? ??

[ip-firewall](#) [Simple Queues](#) [Queue Trees](#) [postrouting](#)

[ip-firewall](#) : /interface bridge port

auto-isolate (<i>yes no</i> ; Default: no)	当接口启用此功能时，接口将阻止接收到的BPDU。这有助于防止非法设备连接到网络。默认情况下，此功能在边缘接口上禁用。
bpdu-guard (<i>yes no</i> ; Default: no)	BPDU Guard功能在接口上启用时，如果接口收到BPDU，接口将进入err-disable状态。这有助于防止非法设备连接到网络。默认情况下，此功能在边缘接口上禁用。
bridge (<i>name</i> ; Default: none)	在接口上启用桥接功能。
broadcast-flood (<i>yes no</i> ; Default: yes)	当接口启用此功能时，接口将向所有端口广播未知目的地的帧。这有助于防止非法设备连接到网络。默认情况下，此功能在边缘接口上启用。

<p>edge (<i>auto</i> <i>no</i> <i>no-discover</i> <i>yes</i> <i>yes-discover</i>; Default: auto)</p>	<p>此命令用于配置边缘端口是否接收并处理 STP 协议报文。默认情况下，边缘端口会接收并处理 STP 协议报文。当配置为 <code>no</code> 时，边缘端口将不会接收并处理 STP 协议报文。当配置为 <code>yes</code> 时，边缘端口将接收并处理 STP 协议报文。当配置为 <code>yes-discover</code> 时，边缘端口将接收并处理 STP 协议报文，并且会发送 STP 协议报文。当配置为 <code>auto</code> 时，边缘端口将根据 <code>protocol-mode</code> 参数的配置来决定是否接收并处理 STP 协议报文。</p> <ul style="list-style-type: none"> <code>no</code> - 边缘端口不会接收并处理 STP 协议报文。当配置为 <code>no</code> 时，边缘端口将不会接收并处理 STP 协议报文。当配置为 <code>yes</code> 时，边缘端口将接收并处理 STP 协议报文。当配置为 <code>yes-discover</code> 时，边缘端口将接收并处理 STP 协议报文，并且会发送 STP 协议报文。当配置为 <code>auto</code> 时，边缘端口将根据 <code>protocol-mode</code> 参数的配置来决定是否接收并处理 STP 协议报文。 <code>no-discover</code> - 边缘端口不会接收并处理 STP 协议报文，并且不会发送 STP 协议报文。当配置为 <code>no-discover</code> 时，边缘端口将不会接收并处理 STP 协议报文，并且不会发送 STP 协议报文。当配置为 <code>yes</code> 时，边缘端口将接收并处理 STP 协议报文。当配置为 <code>yes-discover</code> 时，边缘端口将接收并处理 STP 协议报文，并且会发送 STP 协议报文。当配置为 <code>auto</code> 时，边缘端口将根据 <code>protocol-mode</code> 参数的配置来决定是否接收并处理 STP 协议报文。 <code>yes</code> - 边缘端口接收并处理 STP 协议报文。当配置为 <code>yes</code> 时，边缘端口将接收并处理 STP 协议报文。当配置为 <code>yes-discover</code> 时，边缘端口将接收并处理 STP 协议报文，并且会发送 STP 协议报文。当配置为 <code>auto</code> 时，边缘端口将根据 <code>protocol-mode</code> 参数的配置来决定是否接收并处理 STP 协议报文。 <code>yes-discover</code> - 边缘端口接收并处理 STP 协议报文，并且会发送 STP 协议报文。当配置为 <code>yes-discover</code> 时，边缘端口将接收并处理 STP 协议报文，并且会发送 STP 协议报文。当配置为 <code>yes</code> 时，边缘端口将接收并处理 STP 协议报文。当配置为 <code>no-discover</code> 时，边缘端口不会接收并处理 STP 协议报文，并且不会发送 STP 协议报文。当配置为 <code>auto</code> 时，边缘端口将根据 <code>protocol-mode</code> 参数的配置来决定是否接收并处理 STP 协议报文。 <code>auto</code> - <code>no-discover</code> 时，边缘端口不会接收并处理 STP 协议报文，并且不会发送 STP 协议报文。当配置为 <code>yes</code> 时，边缘端口将接收并处理 STP 协议报文。当配置为 <code>yes-discover</code> 时，边缘端口将接收并处理 STP 协议报文，并且会发送 STP 协议报文。当配置为 <code>auto</code> 时，边缘端口将根据 <code>protocol-mode</code> 参数的配置来决定是否接收并处理 STP 协议报文。
<p>fast-leave (<i>yes</i> <i>no</i>; Default: no)</p>	<p>此命令用于配置边缘端口是否快速离开。默认情况下，边缘端口不会快速离开。当配置为 <code>yes</code> 时，边缘端口将快速离开。当配置为 <code>no</code> 时，边缘端口不会快速离开。</p> <p><code>igmp-snooping</code> <code>yes</code> 时，边缘端口将快速离开。</p>
<p>frame-types (<i>admit-all</i> <i>admit-only-untagged-and-priority-tagged</i> <i>admit-only-vlan-tagged</i>; Default: admit-all)</p>	<p>此命令用于配置边缘端口接收并处理帧的类型。默认情况下，边缘端口接收并处理所有帧。当配置为 <code>admit-only-untagged-and-priority-tagged</code> 时，边缘端口只接收并处理未标记和优先级标记的帧。当配置为 <code>admit-only-vlan-tagged</code> 时，边缘端口只接收并处理 VLAN 标记的帧。</p> <p><code>vlan-filtering</code> <code>yes</code> 时，边缘端口将接收并处理 VLAN 标记的帧。</p>
<p>ingress-filtering (<i>yes</i> <i>no</i>; Default: yes)</p>	<p>VLAN 过滤功能用于防止 VLAN 欺骗攻击。默认情况下，VLAN 过滤功能是启用的。当配置为 <code>no</code> 时，VLAN 过滤功能将禁用。当配置为 <code>yes</code> 时，VLAN 过滤功能将启用。当配置为 <code>yes</code> 时，边缘端口将只接收并处理与配置 VLAN ID 匹配的帧。当配置为 <code>no</code> 时，边缘端口将接收并处理所有帧。</p> <p><code>frame-types</code> <code>admit-only-vlan-tagged</code> 时，边缘端口将只接收并处理 VLAN 标记的帧。当配置为 <code>admit-only-untagged-and-priority-tagged</code> 时，边缘端口将只接收并处理未标记和优先级标记的帧。当配置为 <code>admit-all</code> 时，边缘端口将接收并处理所有帧。</p> <p><code>vlan-filtering</code> <code>yes</code> 时，边缘端口将接收并处理 VLAN 标记的帧。</p> <p>RouterOS v7 中，VLAN 过滤功能默认是启用的。</p>
<p>learn (<i>auto</i> <i>no</i> <i>yes</i>; Default: auto)</p>	<p>此命令用于配置边缘端口是否学习 MAC 地址。默认情况下，边缘端口会学习 MAC 地址。当配置为 <code>no</code> 时，边缘端口不会学习 MAC 地址。当配置为 <code>yes</code> 时，边缘端口会学习 MAC 地址。当配置为 <code>auto</code> 时，边缘端口将根据配置的模式来决定是否学习 MAC 地址。</p> <ul style="list-style-type: none"> <code>yes</code> - MAC 地址学习功能启用。当配置为 <code>yes</code> 时，边缘端口会学习 MAC 地址。当配置为 <code>no</code> 时，边缘端口不会学习 MAC 地址。当配置为 <code>auto</code> 时，边缘端口将根据配置的模式来决定是否学习 MAC 地址。 <code>no</code> - MAC 地址学习功能禁用。当配置为 <code>no</code> 时，边缘端口不会学习 MAC 地址。当配置为 <code>yes</code> 时，边缘端口会学习 MAC 地址。当配置为 <code>auto</code> 时，边缘端口将根据配置的模式来决定是否学习 MAC 地址。 <code>auto</code> - 根据配置的模式来决定是否学习 MAC 地址。当配置为 <code>ap-bridge</code>、<code>bridge</code>、<code>wds-slave</code> 时，边缘端口会学习 MAC 地址。当配置为 <code>bridge</code>、<code>wds-slave</code> 时，边缘端口不会学习 MAC 地址。当配置为 <code>ap-bridge</code> 时，边缘端口会根据配置的模式来决定是否学习 MAC 地址。

<p>multicast-router (<i>disabled permanent temporary-query</i>; Default: temporary-query)</p>	<pre> interface bridge port set [find interface=sfp28-1] !igmp-snooping yes </pre> <ul style="list-style-type: none"> disabled - 阻止 IGMP/MLD 消息在接口上发送和接收。默认情况下，IGMP/MLD 消息在接口上发送和接收。 permanent - 阻止 IGMP/MLD 消息在接口上发送和接收。默认情况下，IGMP/MLD 消息在接口上发送和接收。 temporary-query - IGMP/MLD 消息在接口上发送和接收。默认情况下，IGMP/MLD 消息在接口上发送和接收。
<p>horizon (<i>integer 0..429496729</i>; Default: none)</p>	<pre> split horizon bridging </pre>
<p>hw (<i>yes no</i>; Default: yes)</p>	<pre> HW </pre> <p>HW 命令用于配置硬件转发。默认情况下，硬件转发是启用的。您可以通过 <code>print</code> 命令查看配置。</p>
<p>internal-path-cost (<i>integer: 1..200000000</i>; Default:)</p>	<pre> MSTIO port-cost-mode internal-path-cost protocol-mode mstp </pre> <pre> /interface bridge port set [find interface=sfp28-1] !internal-path-cost </pre> <p>您可以通过 <code>port monitor</code> 命令查看配置。</p>
<p>interface (<i>name</i>; Default: none)</p>	<pre> </pre>

<p>tag-stacking (yes no; Default: no)</p>	<p>当配置 VLAN 时，默认情况下，VLAN ID 和 EtherType 字段将被设置为 0。通过启用 tag-stacking，可以在 VLAN 帧的头部添加 VLAN 标识符。配置示例： <pre> vlan-filtering yes </pre> </p>
<p>trusted (yes no; Default: no)</p>	<p>当启用了 DHCP snooping 功能后，默认情况下，所有接口都是非信任的。信任接口允许 DHCP 服务器通过该接口发送 DHCP 消息。配置示例： <pre> dhcp-snooping yes </pre> </p>
<p>unknown-multicast-flood (yes no; Default: yes)</p>	<p>当启用了未知多播洪水保护功能后，默认情况下，所有接口都是启用的。该功能可以防止未知多播流量泛滥。配置示例： <pre> igmp-snooping </pre> </p>
<p>unknown-unicast-flood (yes no; Default: yes)</p>	<p>当启用了未知单播洪水保护功能后，默认情况下，所有接口都是启用的。该功能可以防止未知单播流量泛滥。配置示例： <pre> igmp-snooping </pre> </p>

RouterOS 支持配置 **1024** 个 VLAN。配置示例：

```

/interface bridge port add bridge=bridge1 interface=ether1
/interface bridge port add bridge=bridge1 interface=ether2
/interface bridge port print

```

??

配置示例：

```

/interface bridge port add bridge=bridge1 interface=ether1
/interface bridge port add bridge=bridge1 interface=ether2
/interface bridge port print

```

```

[admin@MikroTik] /interface bridge port add bridge=bridge1 interface=ether1
[admin@MikroTik] /interface bridge port add bridge=bridge1 interface=ether2
[admin@MikroTik] /interface bridge port print

```


Flags: X - disabled, I - inactive, D - dynamic, H - hw-offload

#	INTERFACE	BRIDGE	HW	PVID	PRIORITY	PATH-COST	INTERNAL-PATH-COST	HORIZON
0	LAN2	bridge1	yes	1	0x80	10	10	none
1	D ether3	bridge1	yes	1	0x80	10	10	none
2	D ether4	bridge1	yes	1	0x80	10	10	none
3	LAN1	bridge1	yes	1	0x80	10	10	none
4	D ether1	bridge1	yes	1	0x80	10	10	none
5	D ether2	bridge1	yes	1	0x80	10	10	none

VLAN ????? ????? ??

RouterOS 7.17 `add name=vlan10 tagged` `add name=vlan20 untagged` `add name=vlan_tagged`
`add interface=ether2 list=vlan10_untagged`
`add interface=ether3 list=vlan10_untagged`
`add interface=ether4 list=vlan20_untagged`
`add interface=sfp-sfpplus1 list=vlan_tagged`

`add bridge=bridge1 frame-types=admit-only-vlan-tagged name=bridge1 vlan-filtering=yes`
`add bridge=bridge1 frame-types=admit-only-untagged-and-priority-tagged`
`interface=vlan10_untagged pvid=10`
`add bridge=bridge1 frame-types=admit-only-untagged-and-priority-tagged`
`interface=vlan20_untagged pvid=20`
`add bridge=bridge1 frame-types=admit-only-vlan-tagged interface=vlan_tagged`

`print`

```
/interface list
add name=vlan10_untagged
add name=vlan20_untagged
add name=vlan_tagged
/interface list member
add interface=ether2 list=vlan10_untagged
add interface=ether3 list=vlan10_untagged
add interface=ether4 list=vlan20_untagged
add interface=sfp-sfpplus1 list=vlan_tagged
/interface bridge
add frame-types=admit-only-vlan-tagged name=bridge1 vlan-filtering=yes
/interface bridge port
add bridge=bridge1 frame-types=admit-only-untagged-and-priority-tagged
interface=vlan10_untagged pvid=10
add bridge=bridge1 frame-types=admit-only-untagged-and-priority-tagged
interface=vlan20_untagged pvid=20
add bridge=bridge1 frame-types=admit-only-vlan-tagged interface=vlan_tagged
```

```
/interface bridge vlan
add bridge=bridge1 tagged=vlan_tagged vlan-ids=10
add bridge=bridge1 tagged=vlan_tagged vlan-ids=20
```

```
[admin@MikroTik] /interface bridge port print
```

```
Flags: D - DYNAMIC; H - HW-OFFLOAD
```

```
Columns: INTERFACE, BRIDGE, HW, PVID, PRIORITY, HORIZON
```

#	INTERFACE	BRIDGE	HW	PVID	PRIORITY	HORIZON
0	vlan10_untagged	bridge1	yes	10	0x80	none
1	DH ether2	bridge1	yes	10	0x80	none
2	DH ether3	bridge1	yes	10	0x80	none
3	vlan20_untagged	bridge1	yes	20	0x80	none
4	DH ether4	bridge1	yes	20	0x80	none
5	vlan_tagged	bridge1	yes	1	0x80	none
6	DH sfp-sfpplus1	bridge1	yes	1	0x80	none

```
[admin@MikroTik] /interface bridge vlan print
```

```
Flags: D - DYNAMIC
```

```
Columns: BRIDGE, VLAN-IDS, CURRENT-TAGGED, CURRENT-UNTAGGED
```

#	BRIDGE	VLAN-IDS	CURRENT-TAGGED	CURRENT-UNTAGGED
;;; added by pvid				
0	D bridge1	10		ether2 ether3
;;; added by pvid				
1	D bridge1	20		ether4
2	bridge1	10	sfp-sfpplus1	
3	bridge1	20	sfp-sfpplus1	

```
# make necessary changes to interface list members:
```

```
/interface list member add list=vlan20_untagged interface=ether5
```

```
/interface list member add list=vlan_tagged interface=sfp-sfpplus2
```

```
# verify changes in bridge port and vlan menus:
```

```
[admin@MikroTik] > /interface bridge port print
```

```
Flags: D - DYNAMIC; H - HW-OFFLOAD
```

```
Columns: INTERFACE, BRIDGE, HW, PVID, PRIORITY, HORIZON
```

#	INTERFACE	BRIDGE	HW	PVID	PRIORITY	HORIZON
0	vlan10_untagged	bridge1	yes	10	0x80	none
1	DH ether2	bridge1	yes	10	0x80	none

```

2 DH ether3          bridge1 yes 10 0x80 none
3  vlan20_untagged  bridge1 yes 20 0x80 none
4 DH ether4          bridge1 yes 20 0x80 none
5 DH ether5          bridge1 yes 20 0x80 none
6  vlan_tagged      bridge1 yes 1 0x80 none
7 DH sfp-sfpplus1   bridge1 yes 1 0x80 none
8 DH sfp-sfpplus2   bridge1 yes 1 0x80 none

```

```

[admin@MikroTik] > /interface bridge vlan print
Flags: D - DYNAMIC
Columns: BRIDGE, VLAN-IDS, CURRENT-TAGGED, CURRENT-UNTAGGED
#  BRIDGE  VLAN-IDS  CURRENT-TAGGED  CURRENT-UNTAGGED
;;; added by pvid
0 D bridge1      10                ether2
                        ether3

;;; added by pvid
1 D bridge1      20                ether4
                        ether5

2  bridge1      10  sfp-sfpplus1
                        sfp-sfpplus2
3  bridge1      20  sfp-sfpplus1
                        sfp-sfpplus2

```

???? ?? ?????

□□ □□ □ □□ □□□□□ monitor □□□ □□□□ .

□□ □□ : /interface bridge port monitor

actual-path-cost (integer: 1..200000000)	□□ □□ □□ □□ □□□□ . □□□□ □□□□ □□□□ □□ □□ □□ □□ □□ □□ □□ □□□□ .
declared-vlan-ids (integer 1..4094)	□□□□□□ MVRP □□□□ □□ □□ □□ □□ VLAN.
designated-bridge-id (priority.MAC address)	□□□ □□□□ □□□□ □□□ □□□ □□□ □□□□ □□□□ .
designated-cost (integer)	□□□ □□□□ □□□□ □□□ □□□ □□ □□ □□□□ □□□□ .

designated-internal-cost (<i>integer</i>)	指定内部成本。范围：1-65535。默认：30000。
designated-message-age (<i>time</i>)	指定消息的生存时间。范围：1-3600秒。默认：180秒。
designated-max-age (<i>time</i>)	指定消息的最大生存时间。范围：1-3600秒。默认：360秒。BPDUs 的 <code>max-message-age</code> 属性。
designated-port-id (<i>priority.integer</i>)	指定端口的 ID。范围：1-65535。默认：0。
designated-remaining-hops (<i>integer</i>)	指定消息的剩余跳数。范围：1-255。默认：255。
discard-transitions (<i>integer</i>)	指定丢弃消息的过渡次数。范围：0-255。默认：0。
edge-port (<i>yes no</i>)	指定是否为边缘端口。默认：no。
edge-port-discovery (<i>yes no</i>)	指定是否启用边缘端口发现。默认：no。
external-fdb (<i>yes no</i>)	指定是否启用外部 FDB 表。默认：no。
forwarding (<i>yes no</i>)	指定是否启用 (R/M)STP 转发。默认：no。
forward-transitions (<i>integer</i>)	指定转发消息的过渡次数。范围：0-255。默认：0。
hw-offload-group (<i>switchX</i>)	指定硬件卸载组。范围：1-255。默认：0。
interface (<i>name</i>)	指定接口名称。
last-topology-change (<i>time</i>)	指定上次拓扑变化的时间。范围：1-3600秒。默认：180秒。
learning (<i>yes no</i>)	指定是否启用 MAC 地址学习。默认：no。
multicast-router (<i>yes no</i>)	指定是否为组播路由器。范围：0-255。默认：0。igmp-snooping 属性。
registered-vlan-ids (<i>integer 1..4094</i>)	MVRP 注册 VLAN ID。范围：1-4094。默认：VLAN。
port-id (<i>priority.integer</i>)	指定端口 ID (STP)。范围：1-65535。默认：0。[16位] + 端口 ID。
point-to-point-port (<i>yes no</i>)	指定是否为点对点端口。范围：0-255。默认：0。

<p>role (<i>designated</i> <i>root-port</i> <i>alternate</i> <i>backup</i> <i>disabled</i>)</p>	<p>(R/M)STP 端口角色 :</p> <ul style="list-style-type: none"> disabled-port - 端口被禁用。 root-port - 根端口，连接到根桥的端口。根桥的根端口是根端口。根桥的根端口是根端口。根桥的根端口是根端口。 alternative-port - 替代端口，连接到根桥的端口。根桥的根端口是根端口。根桥的根端口是根端口。 designated-port - 指定端口，连接到根桥的端口。根桥的根端口是根端口。根桥的根端口是根端口。 backup-port - 备份端口，连接到根桥的端口。根桥的根端口是根端口。根桥的根端口是根端口。 <p>RouterOS 中，STP 端口角色可以通过 <code>show stp</code> 命令查看。RSTP 端口角色 (如 <code>alternate-port</code> 或 <code>backup-port</code>) 在 RSTP 模式下工作。STP 端口角色可以通过 <code>show stp</code> 命令查看。STP 端口角色可以通过 <code>show stp</code> 命令查看。STP 端口角色可以通过 <code>show stp</code> 命令查看。</p>
<p>root-path-cost (<i>integer</i>)</p>	<p>根路径成本，用于计算根桥的路径成本。</p>
<p>sending-rstp (<i>yes</i> <i>no</i>)</p>	<p>是否发送 RSTP 或 MSTP BPDU。默认情况下，STP 端口会发送 BPDU。RSTP/MSTP 端口会发送 RSTP BPDU。STP 端口会发送 STP BPDU。STP 端口会发送 STP BPDU。STP 端口会发送 STP BPDU。</p>
<p>status (<i>in-bridge</i> <i>inactive</i>)</p>	<p>端口状态 :</p> <ul style="list-style-type: none"> in-bridge - 端口在桥中。 inactive - 端口不在桥中。
<p>tx-rx-bpdu (<i>integer</i>)</p>	<p>发送/接收 BPDU 的速率。</p>
<p>tx-rx-tc (<i>integer</i>)</p>	<p>发送/接收 TCN 的速率。</p>
<p>topology-changes (<i>integer</i>)</p>	<p>拓扑变化的次数。</p>

```
[admin@MikroTik] /interface/bridge/port monitor [find interface=ether1]
interface: ether1
status: in-bridge
port-id: 0x80.1
role: root-port
edge-port: no
edge-port-discovery: yes
```

```

point-to-point-port: yes
  external-fdb: no
  sending-rstp: yes
    learning: yes
    forwarding: yes
  actual-path-cost: 20000
internal-root-path-cost: 20000
  designated-bridge-id: 0x1000.2C:C8:1B:FF:92:F4
designated-internal-cost: 0
  designated-port-id: 0x80.1
designated-remaining-hops: 20
  tx-rx-bpdu: 3/63
discard-transitions: 0
forward-transitions: 1
  tx-rx-tc: 2/0
topology-changes: 1
last-topology-change: 2m5s
multicast-router: no
hw-offload-group: switch1
declared-vlan-ids: 1
registered-vlan-ids: 1

```

???

MAC address: 00:00:00:00:00:00

bridge : /interface bridge host

Property	Description
bridge (read-only: name)	bridge name
disabled (read-only: flag)	bridge disabled flag
dynamic (read-only: flag)	bridge dynamic flag
external (read-only: flag)	bridge external flag (: MAC address)

invalid (read-only: flag)	invalid flag, indicates that the bridge is not operational.
local (read-only: flag)	local flag, indicates that the bridge is a local bridge.
mac-address (read-only: MAC address)	MAC address of the bridge.
on-interface (read-only: name)	Interface name of the bridge.

????

bridge table :

```
[admin@MikroTik] /interface bridge host print
Flags: X - disabled, I - invalid, D - dynamic, L - local, E - external
#      MAC-ADDRESS      VID ON-INTERFACE      BRIDGE
0      D      B8:69:F4:C9:EE:D7      ether1      bridge1
1      D      B8:69:F4:C9:EE:D8      ether2      bridge1
2      DL     CC:2D:E0:E4:B3:38      bridge1     bridge1
3      DL     CC:2D:E0:E4:B3:39      ether2      bridge1
```

?? ??

bridge table shows the MAC address of the bridge and the interface it is connected to. The table also shows the status of the bridge (valid/invalid) and the type of bridge (local/dynamic).

bridge table : /interface bridge host

bridge (name; Default: none)	MAC address of the bridge.
disabled (yes no; Default: no)	Whether the bridge is disabled or not.
interface (name; Default: none)	Interface name of the bridge.
mac-address (MAC address; Default:)	MAC address of the bridge.
vid (integer: 1..4094; Default:)	VLAN ID of the bridge.

配置接口，4C:5E:0C:4D:12:43 的接口 ether2 的 MAC 地址，
配置接口 ether2 的 MAC 地址：

```
/interface bridge host  
add bridge=bridge interface=ether2 mac-address=4C:5E:0C:4D:12:43
```

??????

IGMP/MLD 协议 (bridge) 的 IGMP/MLD 协议，配置
(MDB) 的接口 224.0.0.0/24 和 ff02::1 的接口 VLAN 的
配置。配置接口 ether2 的 MAC 地址。 `print` 配置。

配置接口： `/interface bridge mdb`

配置项	说明
bridge (read-only: name)	桥的名称。
group (read-only: ipv4 ipv6 MAC address)	桥的组地址。
on-interface (read-only: name)	桥的接口名称。
vid (read-only: integer)	桥的 VLAN ID。配置 <code>vlan-filtering</code> 接口。

```
[admin@MikroTik] /interface bridge mdb print  
Flags: D - DYNAMIC  
Columns: GROUP, VID, ON-PORTS, BRIDGE  
#  GROUP          VID  ON-PORTS  BRIDGE  
0  D  ff02::2         1  bridge1  bridge1  
1  D  ff02::6a        1  bridge1  bridge1  
2  D  ff02::1:ff00:0  1  bridge1  bridge1  
3  D  ff02::1:ff01:6a43  1  bridge1  bridge1  
4  D  229.1.1.1       10  ether2    bridge1  
5  D  229.2.2.2       10  ether3    bridge1  
   ether2  
6  D  ff02::2         10  ether5    bridge1  
   ether3  
   ether2  
   ether4
```

?? ??

RouterOS 7.7 IPv4 IPv6 MDB 。

： /interface bridge mdb

bridge (name; Default:)	MDB 。
disabled (yes no; Default: no)	MDB 。
group (ipv4 ipv6 MAC address; Default:)	IPv4, IPv6 MAC 224.0.0.0/24 ff02::1 VLAN 。
interface (name; Default:)	。
vid (integer: 1..4094; Default:)	MDB VLAN ID vlan-filtering VLAN ID VLAN 。

, VLAN 10 ether2 ether3 229.10.10.10 MDB

```
/interface bridge mdb
add bridge=bridge1 group=229.10.10.10 interface=ether2,ether3 vid=10
```

print

```
[admin@MikroTik] > /interface bridge mdb print where group=229.10.10.10
Columns: GROUP, VID, ON-PORTS, BRIDGE
# GROUP      VID  ON-PORTS  BRIDGE
12 229.10.10.10  10  ether2    bridge1
                        ether3
```

IPv6 ff02::2 MDB VLAN ports

```
/interface bridge mdb
add bridge=bridge1 group=ff02::2 interface=bridge1,ether2,ether3,ether4,ether5
```

```
[admin@MikroTik] > /interface bridge mdb print where group=ff02::2
```

```
Flags: D - DYNAMIC
```

```
Columns: GROUP, VID, ON-PORTS, BRIDGE
```

#	GROUP	VID	ON-PORTS	BRIDGE
0	ff02::2			bridge1
15	D ff02::2	1	bridge1	bridge1
16	D ff02::2	10	bridge1 ether2 ether3 ether4 ether5	bridge1
17	D ff02::2	20	bridge1 ether2 ether3	bridge1
18	D ff02::2	30	bridge1 ether2 ether3	bridge1

???

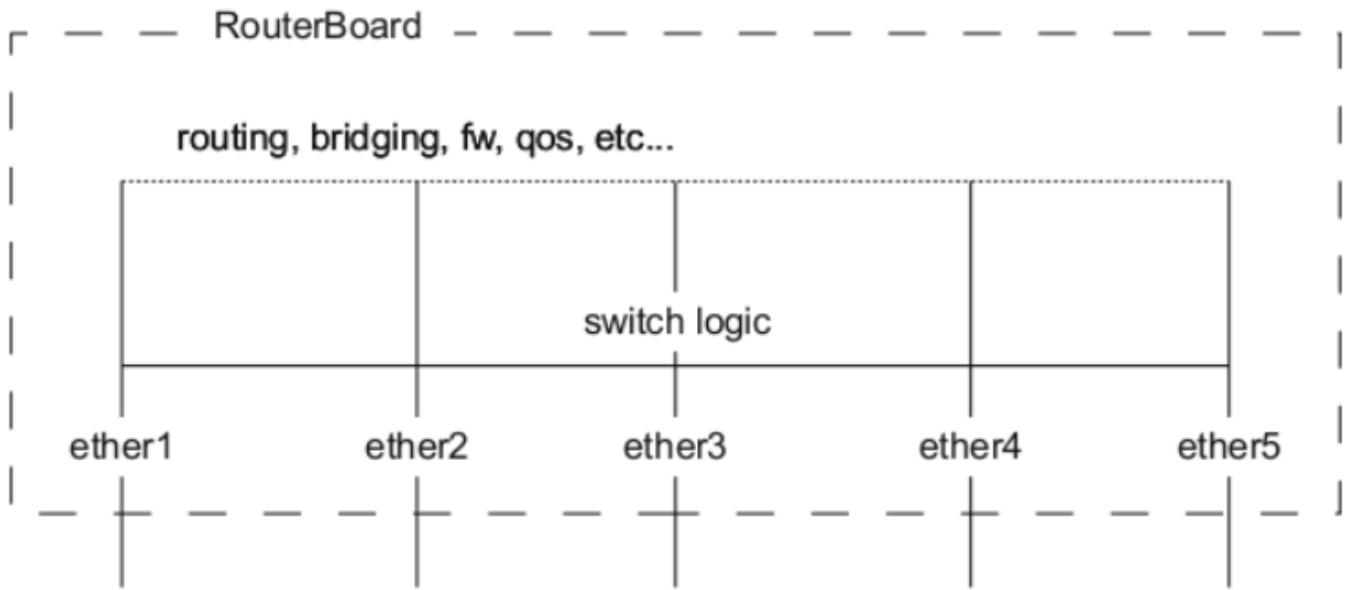
RouterOS v6.41 (64-bit) CPU 100%
Memory 100%
Disk 100%
CPU 100%
Memory 100%
Disk 100%

RouterOS v6.41 (64-bit) CPU 100%
Memory 100%
Disk 100%
CPU 100%
Memory 100%
Disk 100%

RouterOS v6.41 (64-bit) CPU 100%
Memory 100%
Disk 100%
CPU 100%
Memory 100%
Disk 100%

RouterOS v6.41 (64-bit) CPU 100%
Memory 100%
Disk 100%
CPU 100%
Memory 100%
Disk 100%

RouterBoard 内部结构图，展示了路由、桥接、防火墙、QoS 等功能模块，以及 switch logic 和 ether1 到 ether5 接口。



RouterBoard 内部结构图，展示了路由、桥接、防火墙、QoS 等功能模块，以及 switch logic 和 ether1 到 ether5 接口。

RouterBoard 内部结构图，展示了路由、桥接、防火墙、QoS 等功能模块，以及 switch logic 和 ether1 到 ether5 接口。

- [CRS1xx/2xx 系列](#)
- [CRS3xx, CRS5xx 系列](#) 及 [CCR2116, CCR2216 系列](#)
- [CRS 系列](#)

RouterBoard 内部结构图，展示了路由、桥接、防火墙、QoS 等功能模块，以及 switch logic 和 ether1 到 ether5 接口。

通过 VLAN 技术 (IVL) 可以在 Layer2 网络中实现广播域的隔离。通过配置 VLAN ID (pvid) 可以实现。

CRS3xx, CRS5xx 系列设备, CCR2116, CCR2216 系列设备, RTL8367, 88E6393X, 88E6191X, 88E6190, MT7621, MT7531, EN7562CT 系列设备 (RouterOS v7) 均支持 VLAN 技术。通过配置 VLAN 技术可以实现广播域的隔离。通过配置 VLAN 技术可以实现广播域的隔离。通过配置 VLAN 技术可以实现广播域的隔离。

??? VLAN ???

通过 VLAN 技术可以在 Layer2 网络中实现广播域的隔离。通过配置 VLAN ID (pvid) 可以实现。通过配置 VLAN 技术可以实现广播域的隔离。通过配置 VLAN 技术可以实现广播域的隔离。通过配置 VLAN 技术可以实现广播域的隔离。

配置命令: /interface bridge vlan

配置项	说明
bridge (name; Default: none)	指定 VLAN 所属的桥接设备名称。
disabled (yes no; Default: no)	是否禁用该 VLAN 配置。
tagged (interfaces; Default: none)	指定哪些接口属于该 VLAN 的 tagged 成员。例如: tagged=ether1,ether2。
untagged (interfaces; Default: none)	指定哪些接口属于该 VLAN 的 untagged 成员。例如: untagged=ether3,ether4。
vlan-ids (integer 1..4094; Default: 1)	指定该 VLAN 的 ID 范围。例如: vlan-ids=100-115,120,122,128-130。

vlan-ids 配置项用于指定 VLAN ID 的范围。通过配置 vlan-ids 可以实现广播域的隔离。通过配置 vlan-ids 可以实现广播域的隔离。通过配置 vlan-ids 可以实现广播域的隔离。

通过 VLAN 技术可以在 Layer2 网络中实现广播域的隔离。通过配置 VLAN ID (pvid) 可以实现。通过配置 VLAN 技术可以实现广播域的隔离。通过配置 VLAN 技术可以实现广播域的隔离。通过配置 VLAN 技术可以实现广播域的隔离。

在配置 VLAN 时，需要指定 VLAN 的 ID 和名称。VLAN ID 必须在 1 到 4094 之间，且不能与已有的 VLAN ID 冲突。VLAN 名称可以包含字母、数字、下划线和连字符，但不能以连字符开头或结尾。

CPU 的 VLAN 配置通常涉及到 CPU 的接口。在配置 CPU 的 VLAN 时，需要指定 CPU 的接口 ID 和 VLAN ID。配置完成后，CPU 就可以通过该 VLAN 与网络中的其他设备通信了。

在配置 VLAN 时，还需要配置 VLAN 的帧类型（frame-types）、 ingress 过滤（ingress-filtering）、PVID（pvid）和标签堆叠（tag-stacking）等属性。

???? ?? ??

在配置 VLAN 时，需要指定 VLAN 的 ID 和名称。VLAN ID 必须在 1 到 4094 之间，且不能与已有的 VLAN ID 冲突。VLAN 名称可以包含字母、数字、下划线和连字符，但不能以连字符开头或结尾。

配置命令：`/interface bridge port`

属性	配置说明
frame-types (<i>admit-all</i> <i>admit-only-untagged-and-priority-tagged</i> <i>admit-only-vlan-tagged</i> ; Default: admit-all)	指定 VLAN 帧类型的处理方式。支持的选项包括 <code>admit-all</code> 、 <code>admit-only-untagged-and-priority-tagged</code> 和 <code>admit-only-vlan-tagged</code> 。默认值为 <code>admit-all</code> 。
ingress-filtering (<i>yes</i> <i>no</i> ; Default: yes)	指定是否启用 VLAN 的 ingress 过滤功能。支持的选项包括 <code>yes</code> 和 <code>no</code> 。默认值为 <code>yes</code> 。
pvid (<i>integer 1..4094</i> ; Default: 1)	指定 VLAN 的 PVID（Port VLAN ID）。支持的选项为整数 1 到 4094。默认值为 1。
tag-stacking (<i>yes</i> <i>no</i> ; Default: no)	指定是否启用 VLAN 的标签堆叠功能。支持的选项包括 <code>yes</code> 和 <code>no</code> 。默认值为 <code>no</code> 。

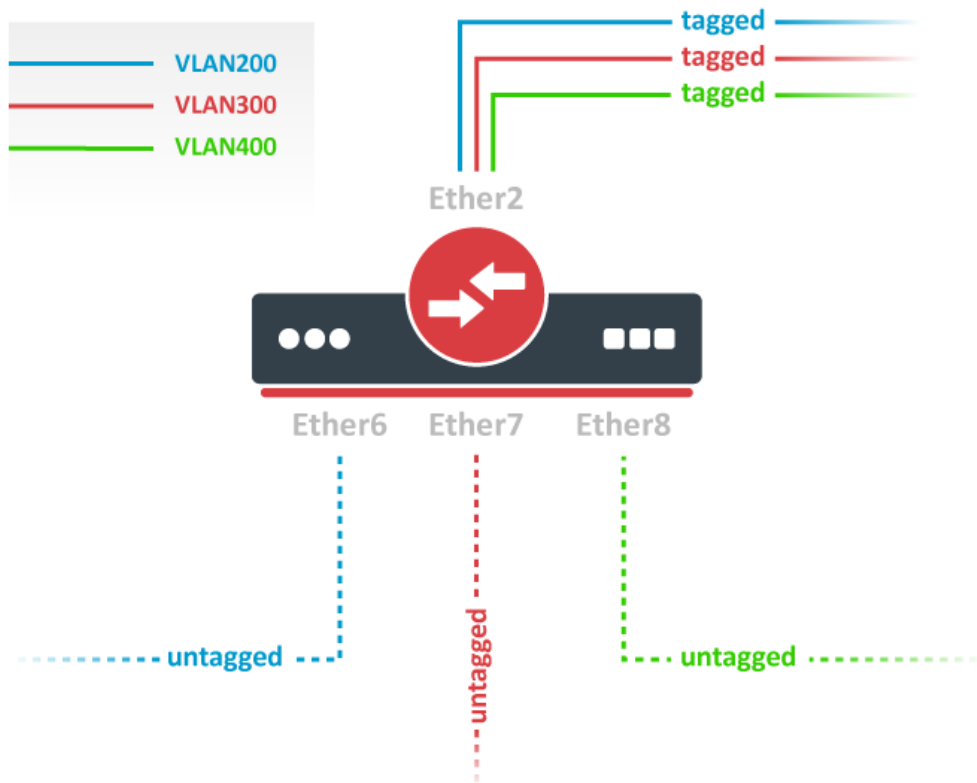
???? ???? ????

1. 配置 VLAN 过滤规则，使用 `vlan-filtering` 命令。
 2. 配置 VLAN ID 列表 (VLAN 列表 IVL)。

```

[admin@MikroTik] > /interface bridge host print where !local
Flags: X - disabled, I - invalid, D - dynamic, L - local, E - external
#      MAC-ADDRESS      VID ON-INTERFACE      BRIDGE
0      D      CC:2D:E0:E4:B3:AA  300 ether3             bridge1
1      D      CC:2D:E0:E4:B3:AB  400 ether4             bridge1
  
```

VLAN ?? - ??? ???? ???? ??



3. 配置 VLAN 过滤规则，使用 `vlan-filtering` 命令。
 4. 配置 VLAN ID 列表 (VLAN 列表 IVL)。

```

/interface bridge
add name=bridge1 vlan-filtering=no
  
```

5. 配置 VLAN 过滤规则，使用 `pvid` 命令。
 6. 配置 frame-types 命令。

```

/interface bridge port
add bridge=bridge1 interface=ether2 frame-types=admit-only-vlan-tagged
add bridge=bridge1 interface=ether6 pvid=200 frame-types=admit-only-untagged-and-priority-
tagged
add bridge=bridge1 interface=ether7 pvid=300 frame-types=admit-only-untagged-and-priority-
tagged
add bridge=bridge1 interface=ether8 pvid=400 frame-types=admit-only-untagged-and-priority-
tagged

```

```

VLAN 200 200 200 200 200 200 200 200 . frame-types admit-only-
untagged-and-priority-tagged 200 200 200 200 pvid VLAN 200 200 200
200 200 .

```

```

/interface bridge vlan
add bridge=bridge1 tagged=ether2 vlan-ids=200
add bridge=bridge1 tagged=ether2 vlan-ids=300
add bridge=bridge1 tagged=ether2 vlan-ids=400

```

```

200 200 VLAN 200 200 200 VLAN 200 200 .

```

```

/interface bridge set bridge1 vlan-filtering=yes

```

```

200 200 200 200 frame-types=admit-only-vlan-tagged 200 200 VLAN
1 (pvid=1) 200 200 .

```

```

/interface bridge set bridge1 frame-types=admit-only-vlan-tagged

```

VLAN ?? - ??? ????? ??



Ether6 Ether7 Ether8

