Mikrotik Ospf & Vpn

- Zhang Wei / 张维
- 189CSP / 上海万联信息科技有限公司

About me

- Name: Zhang Wei/张维
- E-mail: zhangwei@189csp.cn
- Telegram ID: @zhangwehi
- Telegram link: https://telegram.me/zhangwehi
- Mikrotik Forum ID: David007

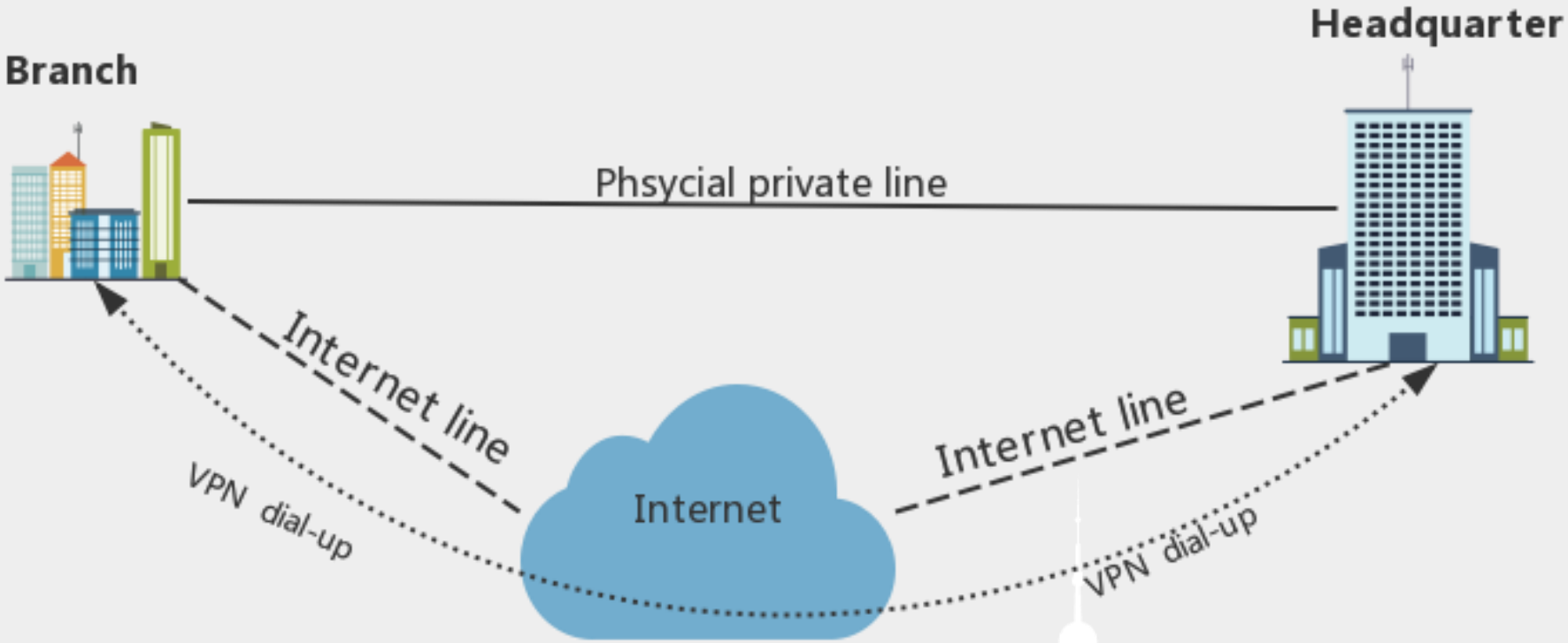
About me

- MikroTik Certified Network Administrator （MTCNA）
  MikroTik Certified Routing Engineer （MTCRE）

Topic

- VPN dial-up
- OSPF to implement automatic route switching.

①Theory - HOW

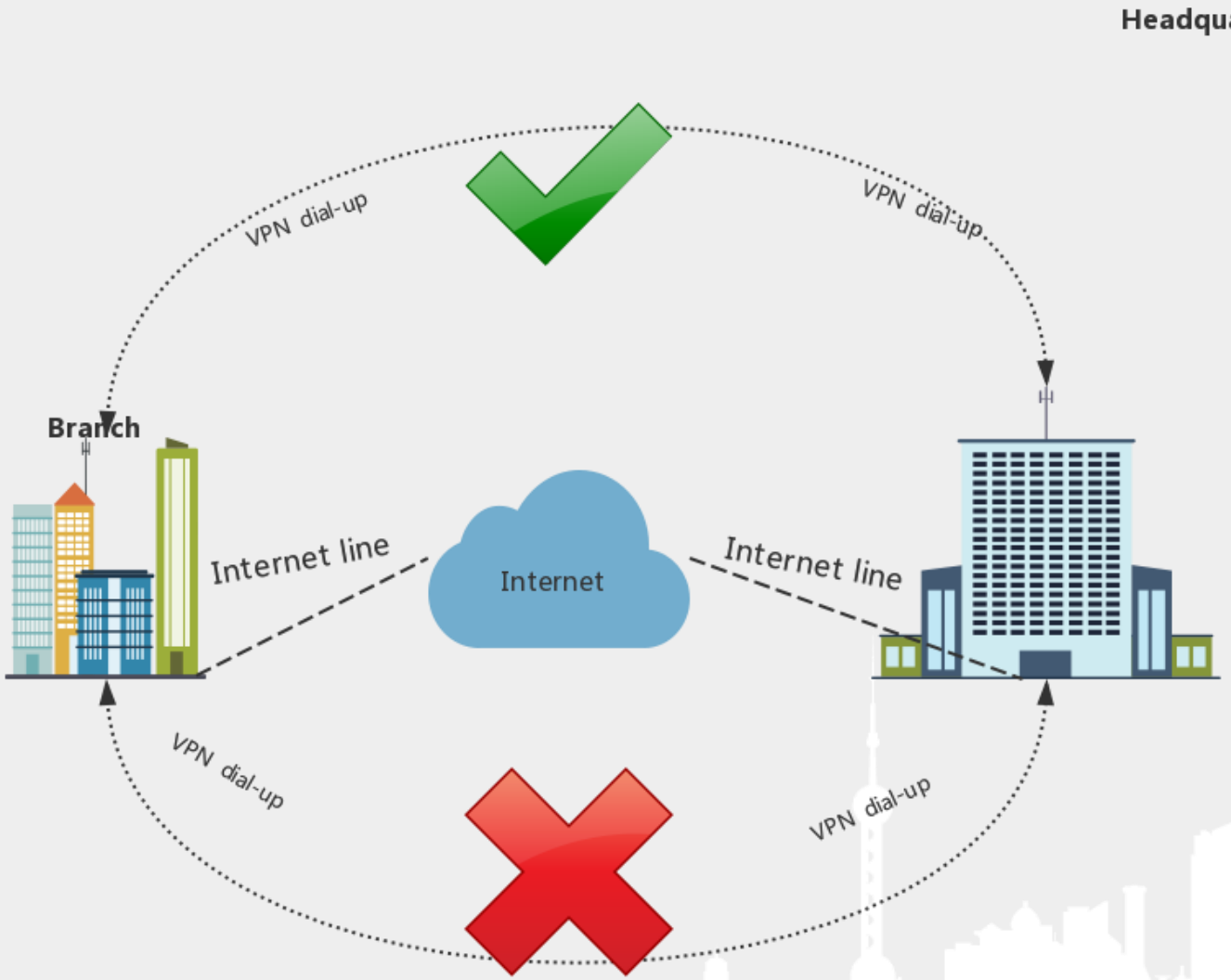

Branch
Headquarter
Phsycial private line
Internet line
VPN dial-up
Internet
Internet line
VPN dial-up

①Theory - HOW

- **How to set up internal channel between branch and headquarter?**

VPN dial-up	VS	Physical private lines
		
Cheap		Expensive

① Theory - HOW



① Theory - HOW

- How many VPN dial-up should be created?

TWO

Redundant

ONE

No Redundant

① Theory - HOW

Which VPN dial-up mode should be choose?

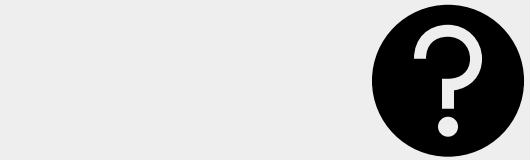


Table of Contents

① Theory – VPN

Types of VPN

- Site to Site
  - ISA
  - IPSec
- Remote Access
  - PPTP
    - TCP 1723
    - IP protocol ID 47
    - PPTP connections may be limited or impossible to setup though a masqueraded/NAT IP connection.)
  - L2TP
    - UDP 1701 and other udp port to transfer data
    - L2TP can be used with most firewalls and routers (even with NAT) by enabling UDP traffic to be routed through the firewall or router.)

① Theory – VPN

- Remote Access
  - OVPN

    Supported
    - TCP
    - bridging (tap device)
    - routing (tun device)
    - certificates
    - p2p mode (refer to OpenVPN V2.1 manual page)

    Unsupported
    - UDP
    - LZO compression

  - SSTP
    - TCP connection is established from client to server (by default on port 443);
    - SSL validates server certificate. If certificate is valid connection is established otherwise connection is torn down. (But see note below)
    - The client sends SSTP control packets within the HTTPS session which establishes the SSTP state machine on both sides.
    - PPP negotiation over SSTP. Client authenticates to the server and binds IP addresses to SSTP interface

① Theory - HOW

We choose OVPN & SSTP

① Theory – What is OSPF

Open Shortest Path First (**OSPF**) is a routing protocol for Internet Protocol (IP) networks.

It uses a link state routing (LSR) algorithm and falls into the group of interior gateway protocols (IGPs), operating within a single autonomous system (AS).

It is defined as OSPF Version 2 in RFC 2328 (1998) for IPv4.

The updates for IPv6 are specified as OSPF Version 3 in RFC 5340 (2008).

OSPF supports the Classless Inter-Domain Routing (CIDR) addressing model.

① Theory – What is OSPF

- OSPF is a link-state routing protocol that use bandwidth-based metrics.
- OSPF adopts the SPF algorithm to calculate the routing, which ensures that there is no routing loop.
- OSPF maintaining the routing through neighbor relationship avoids the consumption of bandwidth due to regular update.
- OSPF routing update efficiency is high, network convergence is fast, suitable for large and medium-sized networks.
- OSPF Packets are encapsulated in IP, protocol number 89, and multicast addresses 224.0.0.5 and 224.0.0.6.
- OSPF The default routing distance is 110, which can be manually modified.

Frame header	Source IP	Destnation IP 224.0.0.5	protocol 89(OSPF)	OSPF header	OSPF Packet payload

① Theory - Benefits vs RIP

OSPF is based on link-state technology that has several advantages over distance-vector protocols such as RIP:

- no hop count limitations;
- multicast addressing is used to send routing information updates;
- updates are sent only when network topology changes occur;
- logical definition of networks where routers are divided into areas
- transfers and tags external routes injected into AS.

① Theory – Configure easy

There are three basic elements of OSPF configuration:
•Enable OSPF instance
•OSPF area configuration
•OSPF network configuration

Instead of typing in each network, you can aggregate networks using appropriate subnet mask. For example, to aggregate 10.10.1.0/30, 10.10.1.4/30, 10.10.1.8/30 networks, you can set up following ospf network:

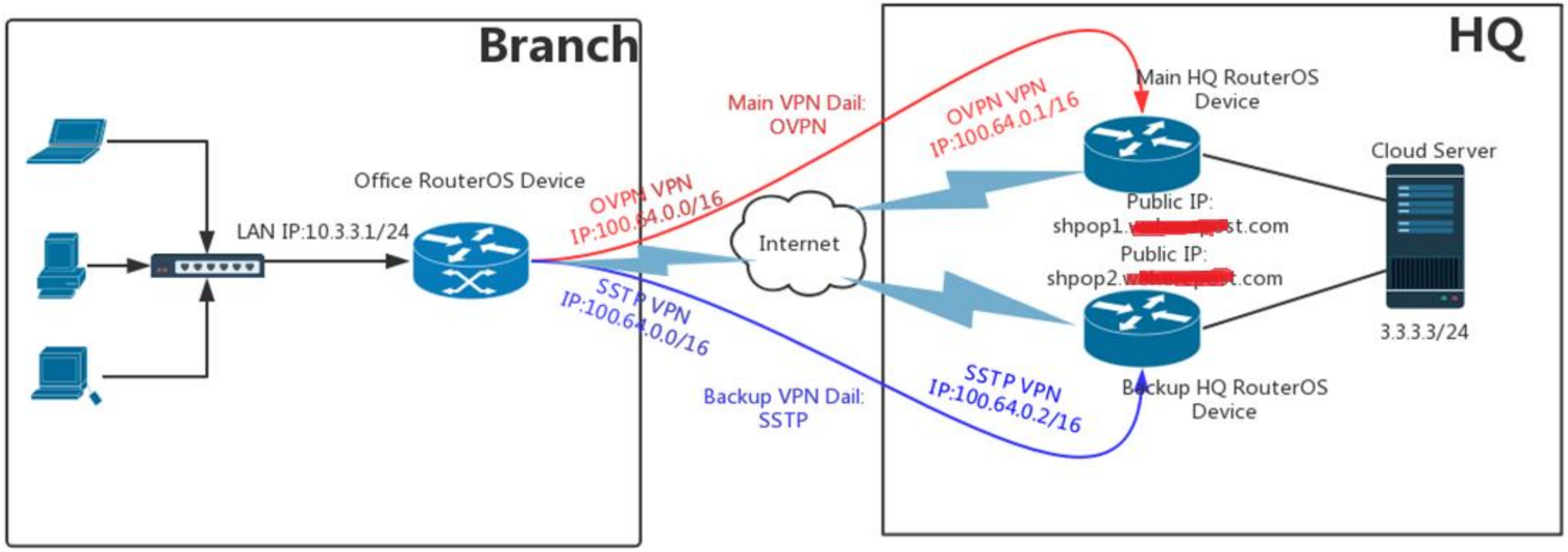
[admin@MikroTikR1] /routing ospf network> add network=10.10.1.0/24 area=backbone

① Theory – Information of OSPF

Show OSPF instance information:

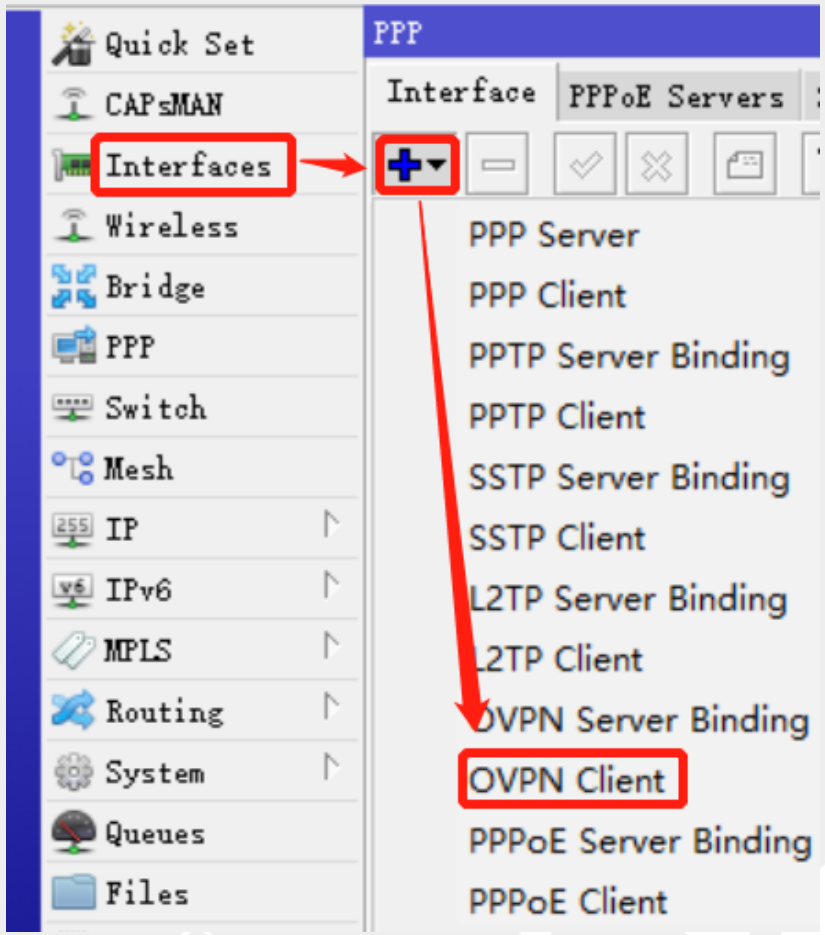
```
[admin@MikroTikR1] /routing ospf instance> print
Flags: X - disabled
          0 name="default" router-id=0.0.0.0 distribute-default=never
          redistribute-connected=as-type-1 redistribute-static=as-type-1
          redistribute-rip=no redistribute-bgp=no redistribute-other-ospf=no
          metric-default=1 metric-connected=20 metric-static=20 metric-rip=20
          metric-bgp=auto metric-other-ospf=auto in-filter=ospf-in
out-filter=ospf-out
```

② Network Topology



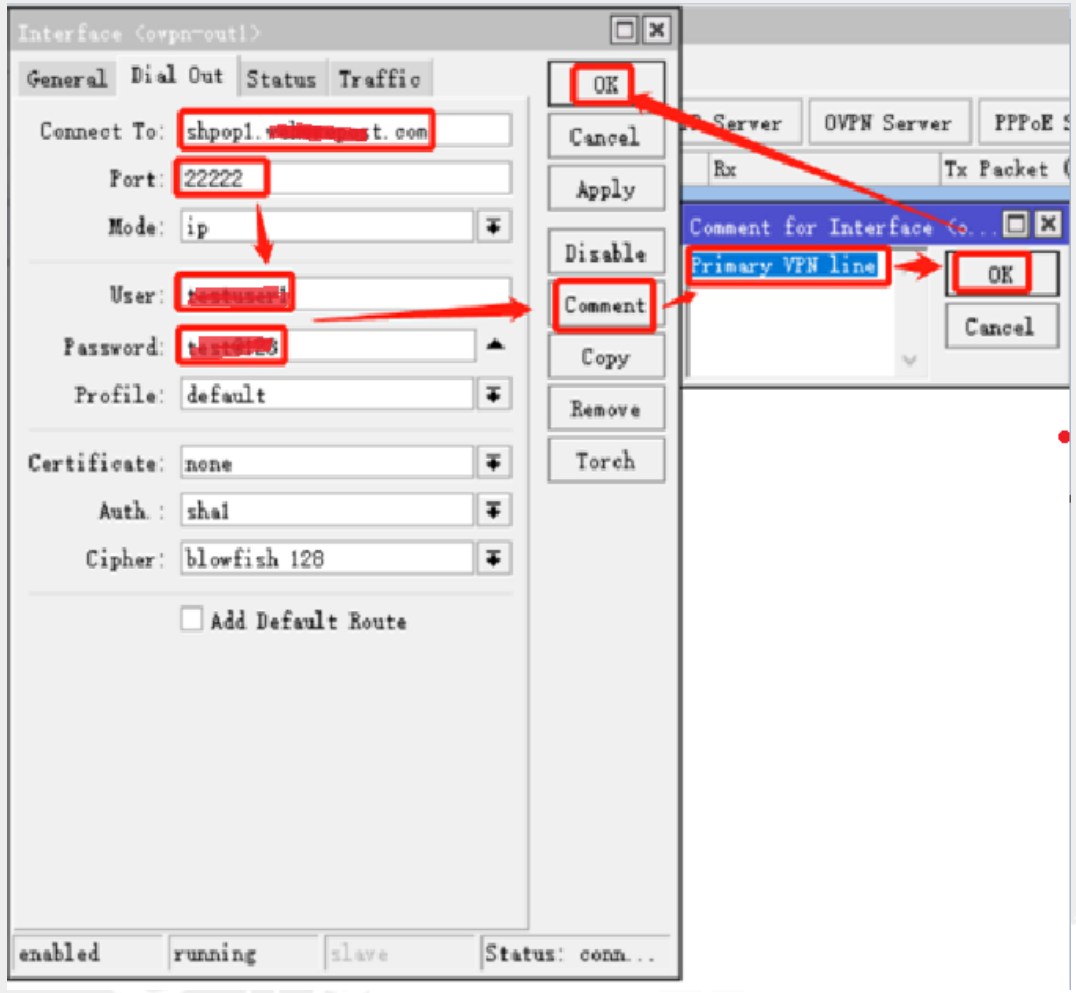
③ LAB 1 –How to Create Branch VPN Dialup

Step 1.1 – Create The Primary VPN Dialer Interface (OVPN)



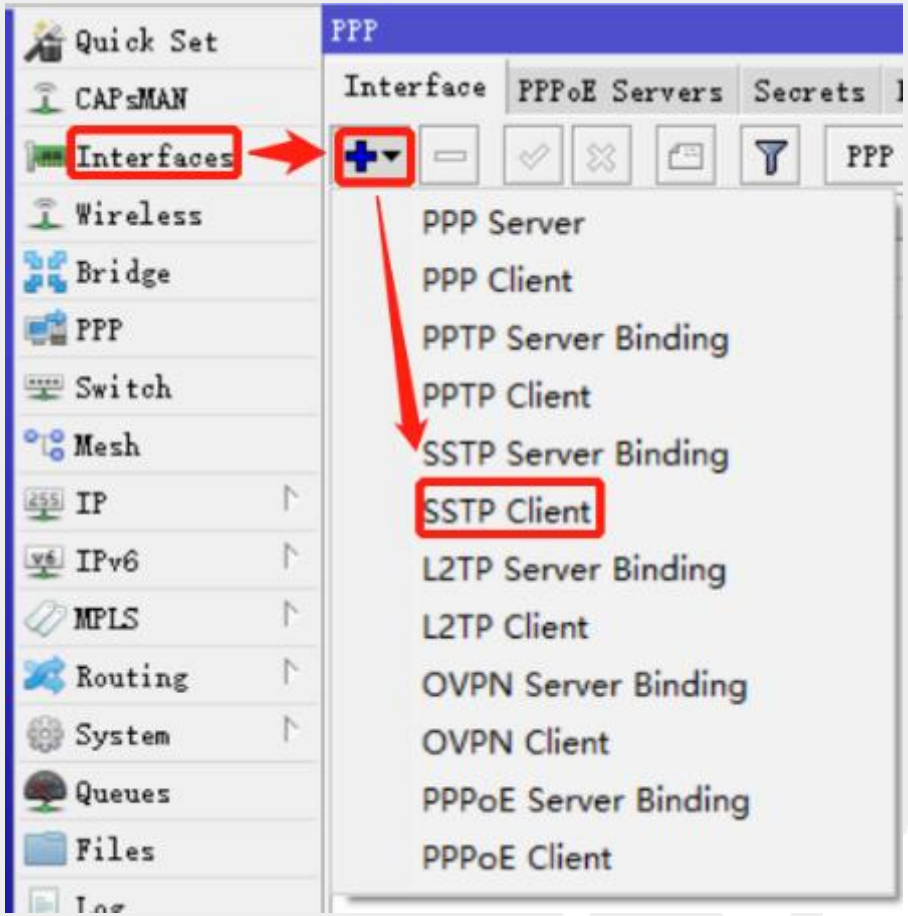
③ LAB 1–How to Create Branch VPN Dialup

Step 1.2 – Create The Primary VPN Dialer Interface (OVPN)



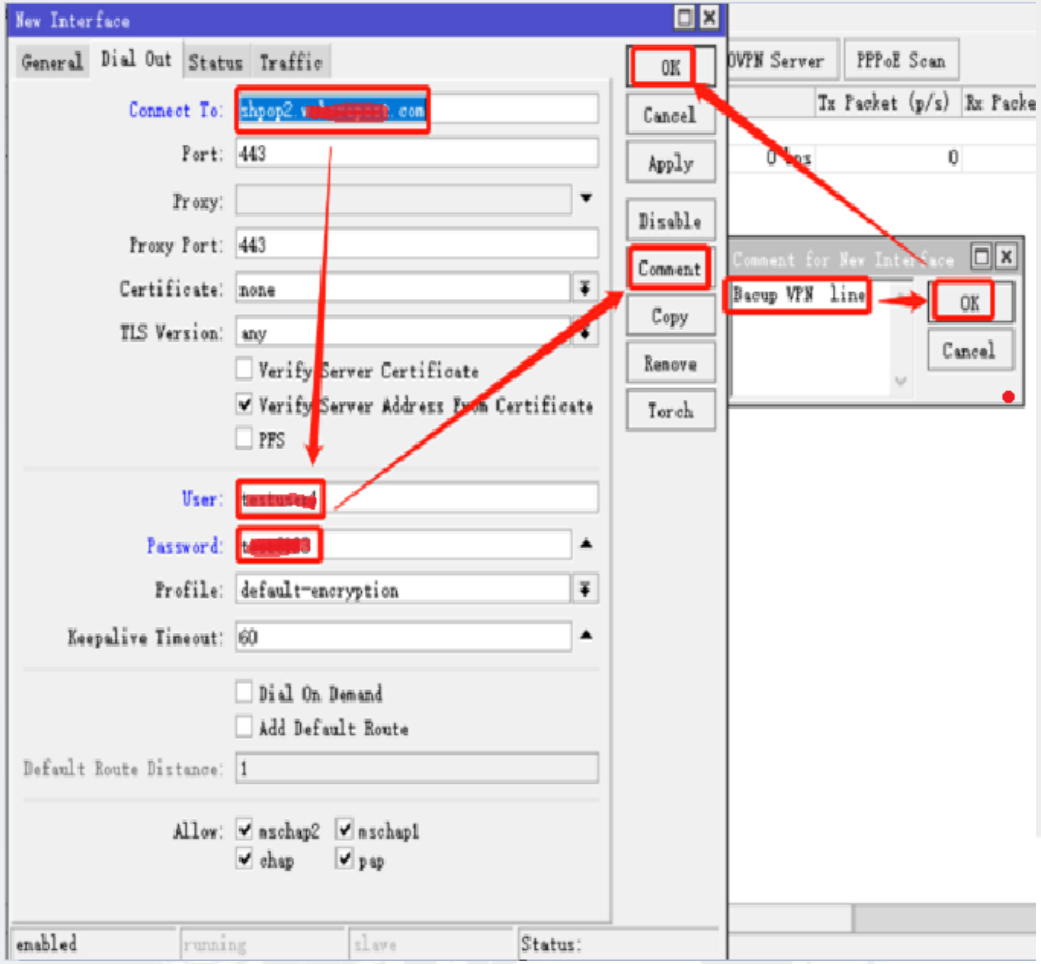
③ LAB 1–How To Create Branch VPN Dialup

Step 1.3 – Create The Backup VPN Dialer Interface (SSTP)



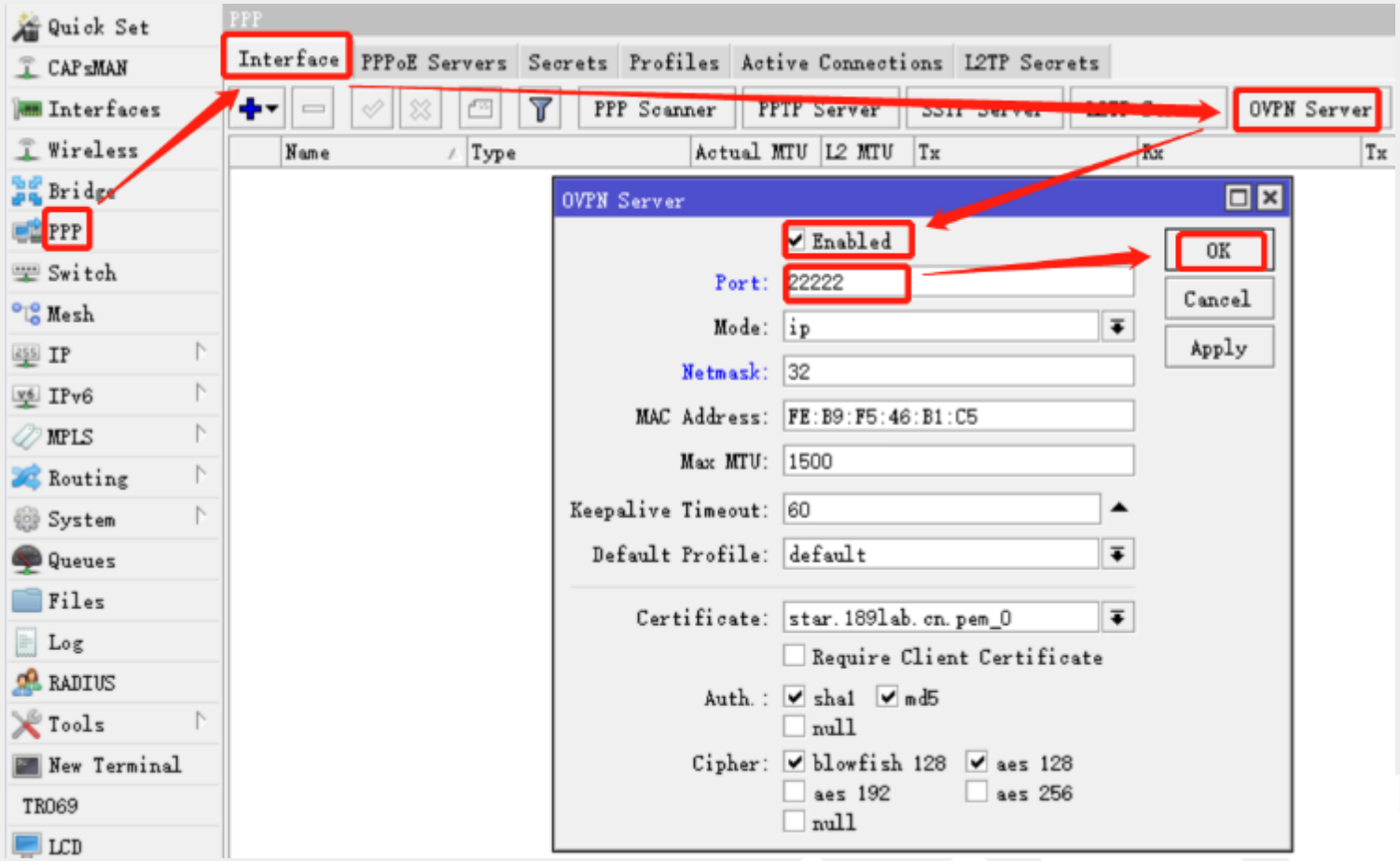
③ LAB 1–How To Create Branch VPN Dialup

Step 1.4 – Create The Backup VPN Dialer Interface (SSTP)



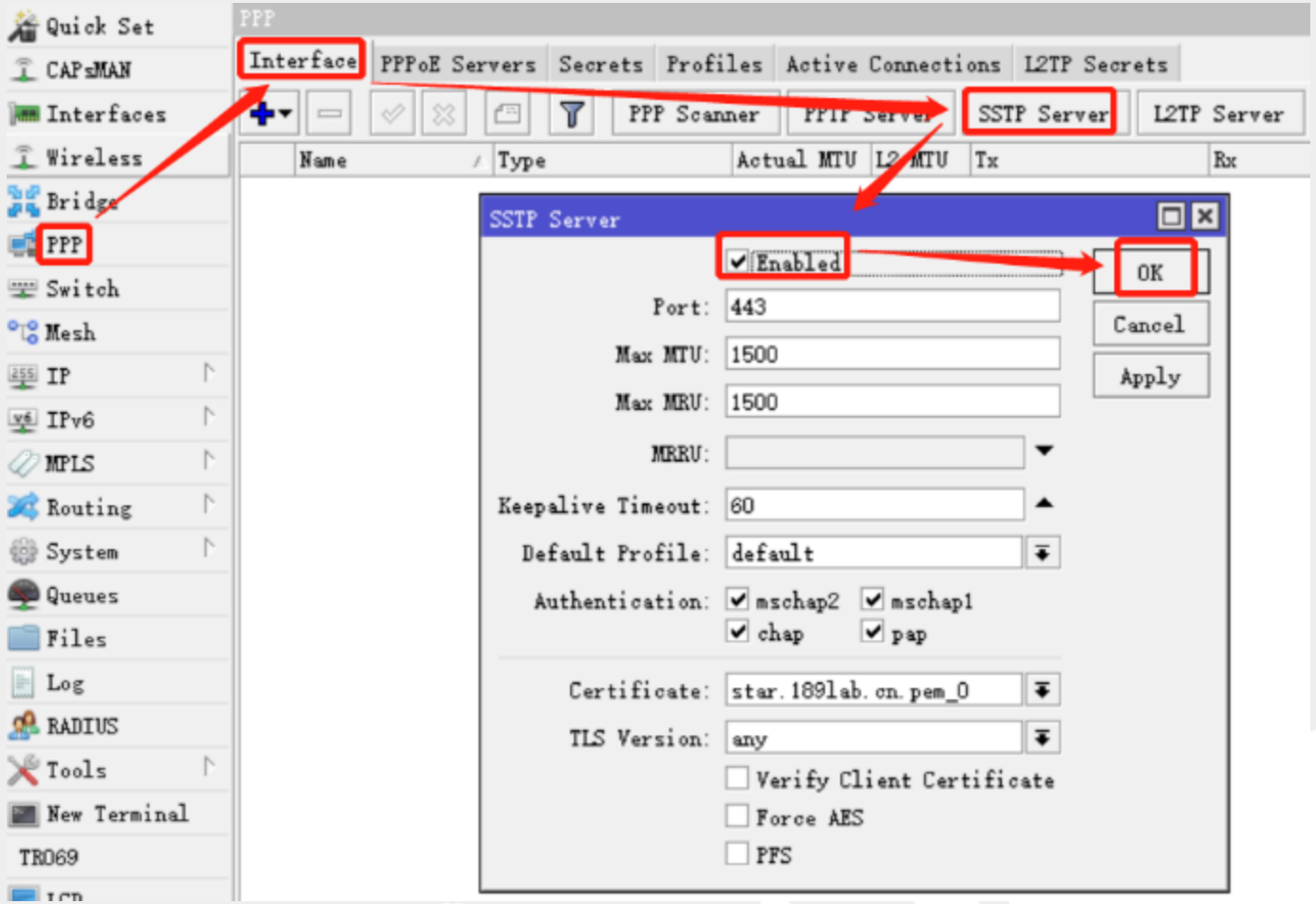
③ LAB 2– How to Enable Primary VPN HQ Server Configuration

Step 2.1 - Enable OVPN service configuration on the primary RouterOS devices in the HQ.



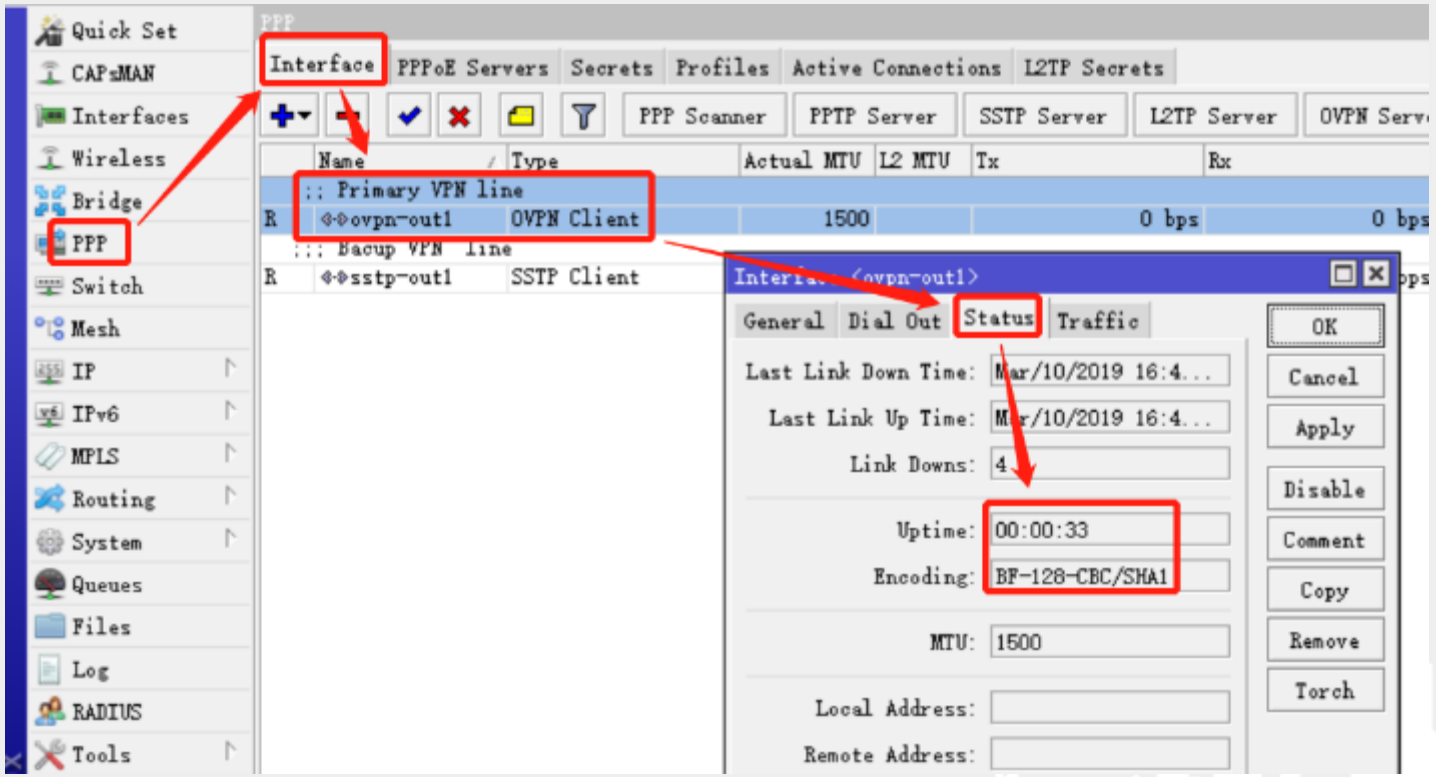
③ LAB 2– How to Enable Backup VPN HQ Server Configuration

Step 2.2 - Enable SSTP service configuration on the Backup RouterOS devices in the HQ.



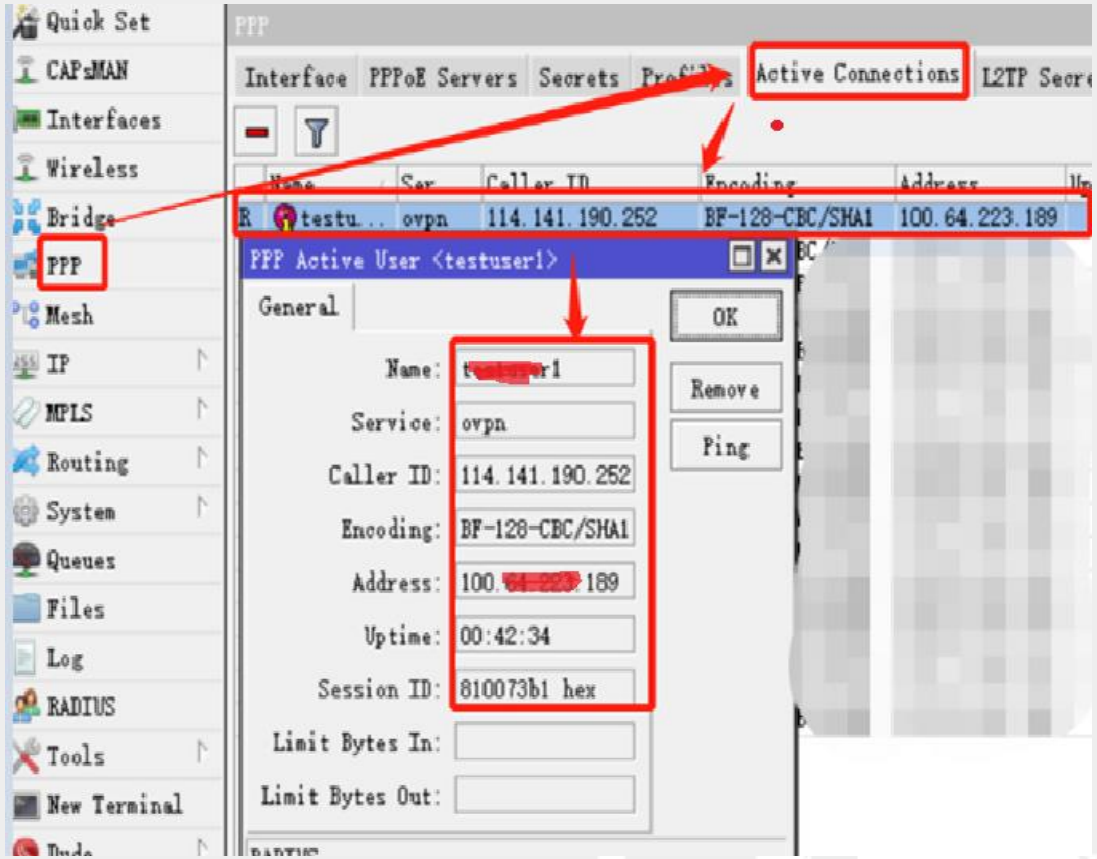
③ LAB 3– How To Check The Primary VPN Dialing Status

Step 3.1 - From The Branch RouterOS device To Check The Primary VPN Dialing Status



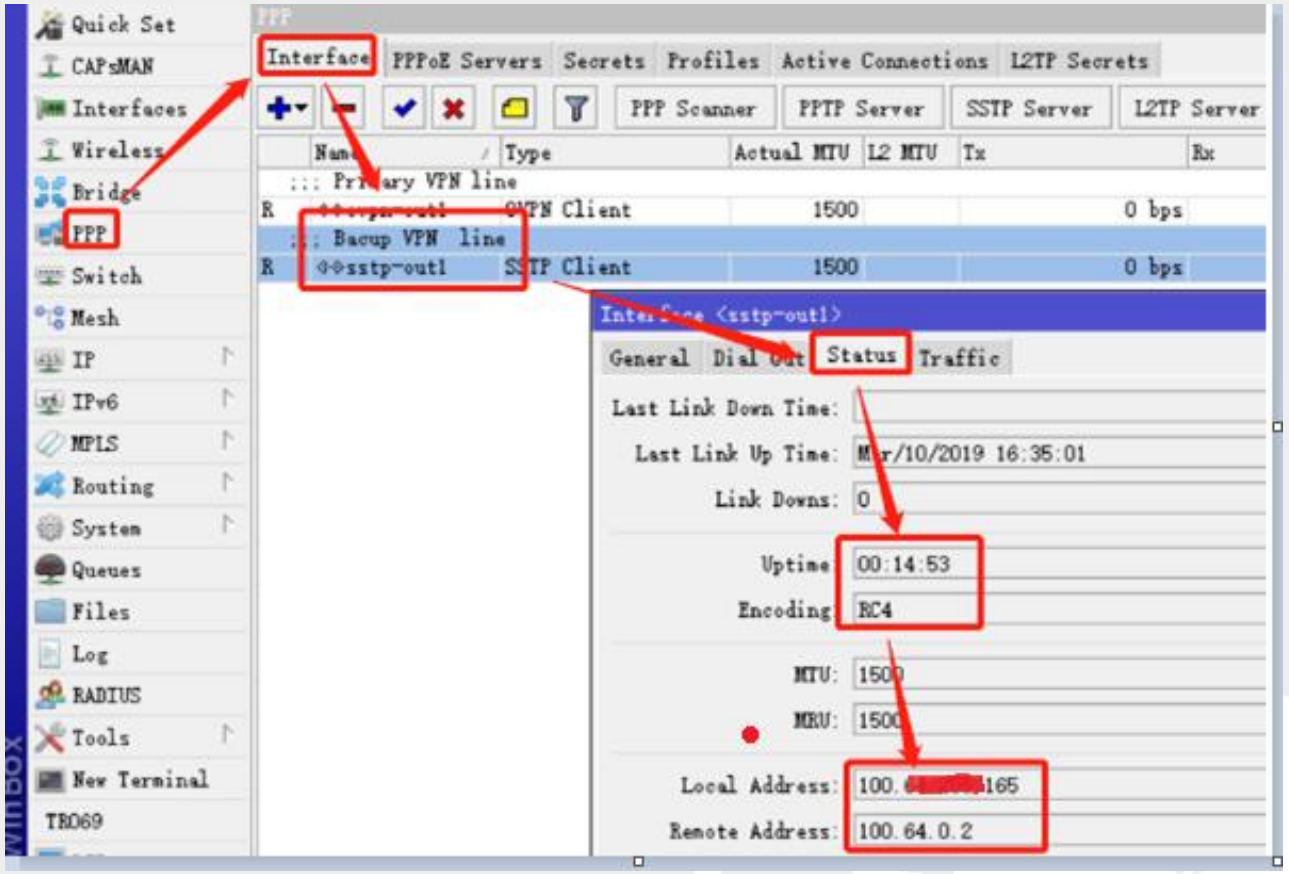
③ LAB 3– How To Check The Primary VPN Dialing Status

Step 3.2 - From The HQ RouterOS device To Check The Primary VPN Dialing Status



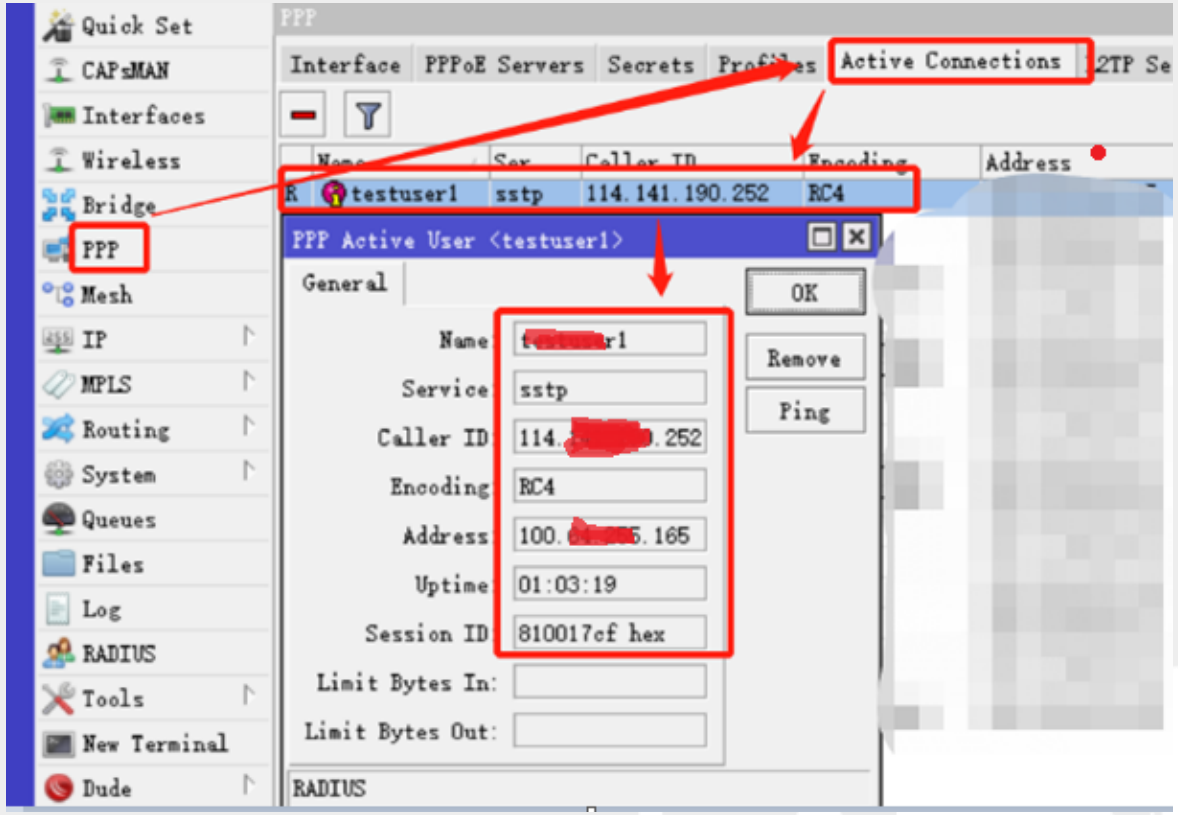
③ LAB 4– How To Check The Backup VPN Dialing Status

Step 4.1 - From The Branch RouterOS device To Check The Backup VPN Dialing Status



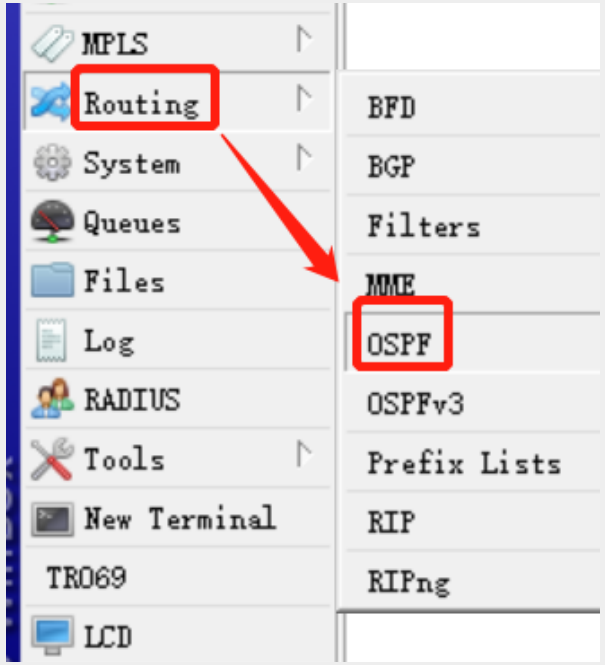
③ LAB 4– How To Check The Backup VPN Dialing Status

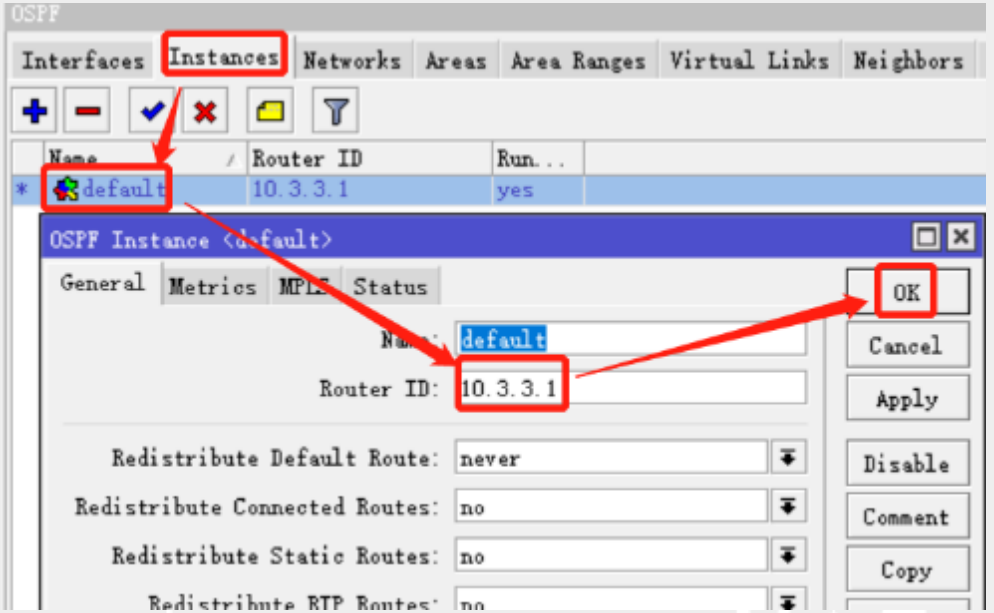
Step 4.2 - From The HQ RouterOS device To Check The Backup VPN Dialing Status



③ LAB 5– How To Configure OSPF In Branch RouterOS Device

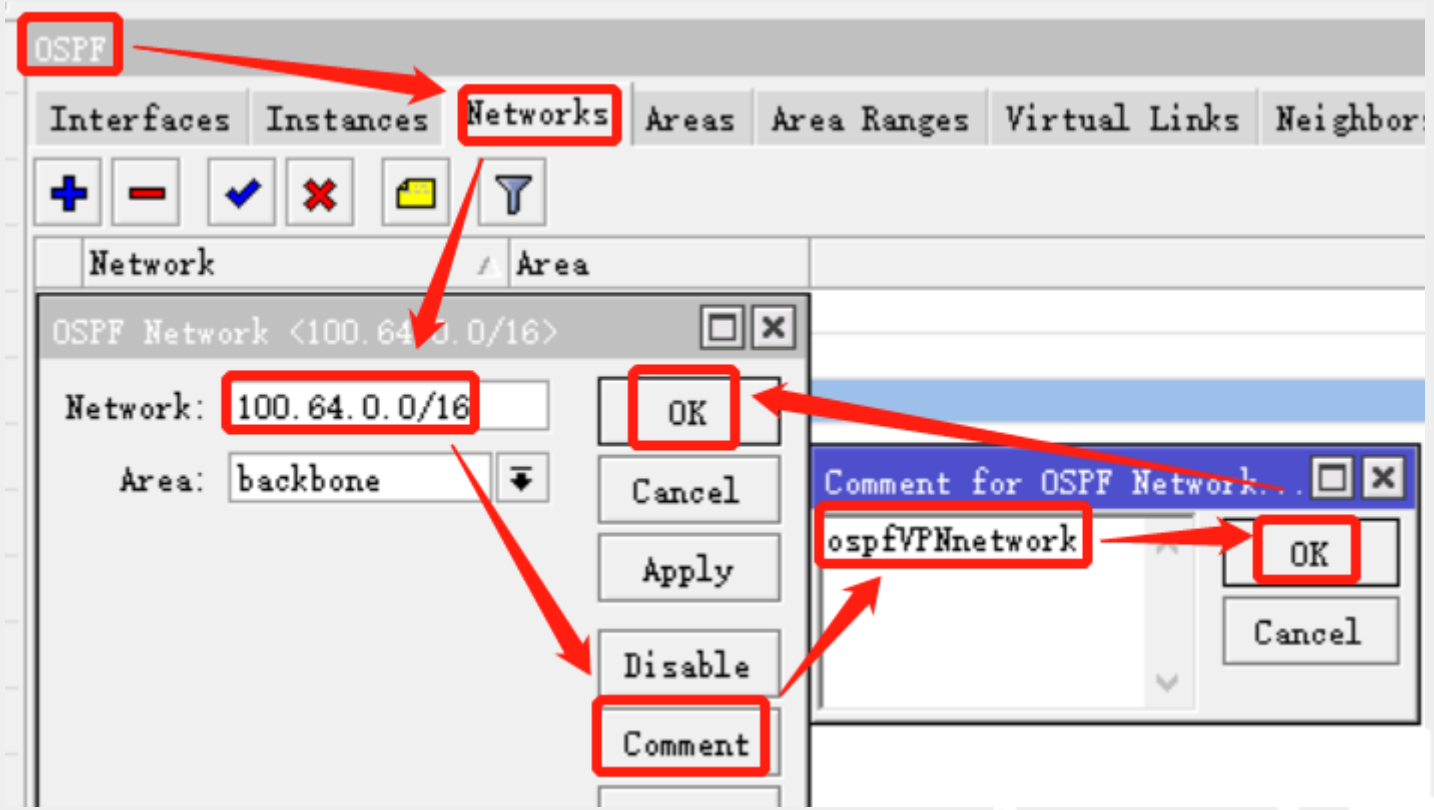
Step 5.1 – Configure OSPF Router-ID In Branch Router Device





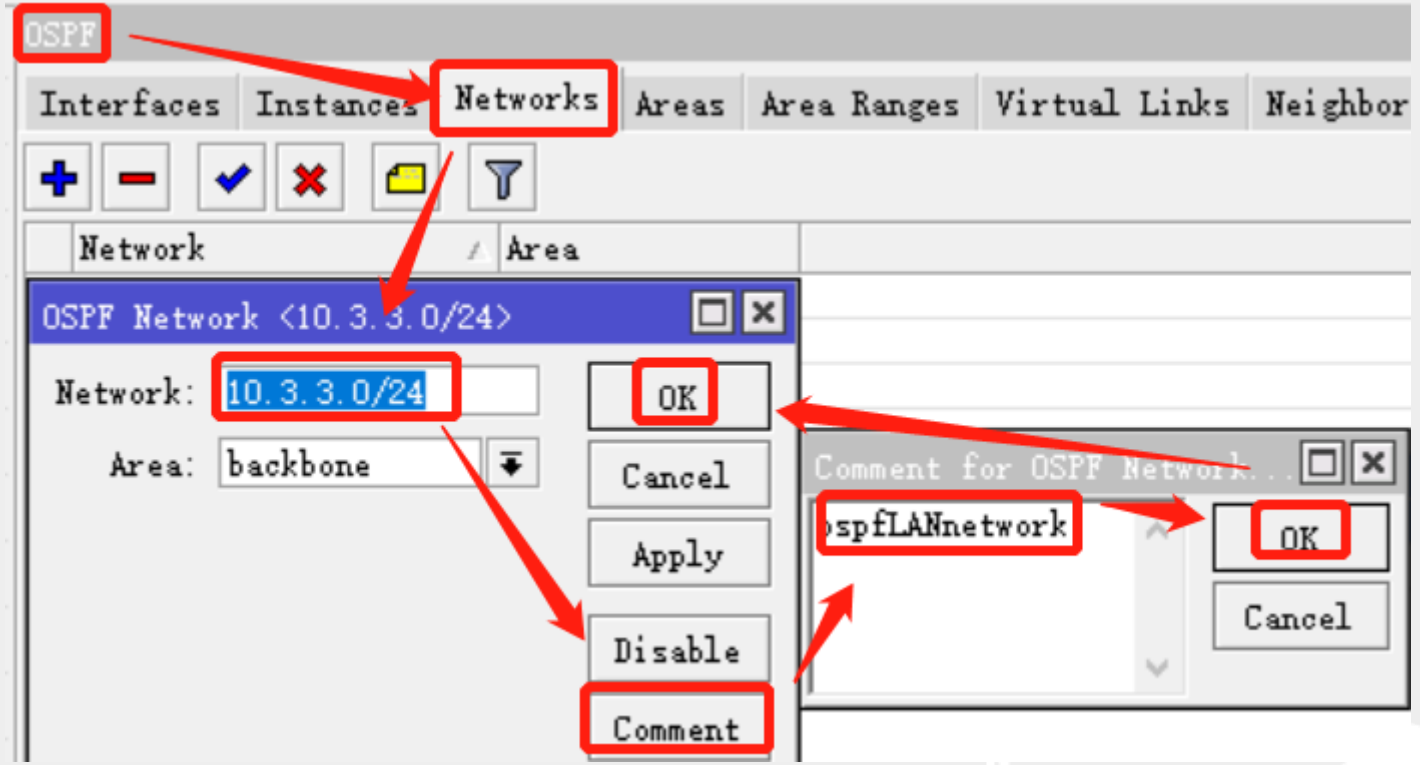
③ LAB 5– How To Configure OSPF In Branch RouterOS Device

Step 5.2 – Configure OSPF Lan Network In Branch Router Device



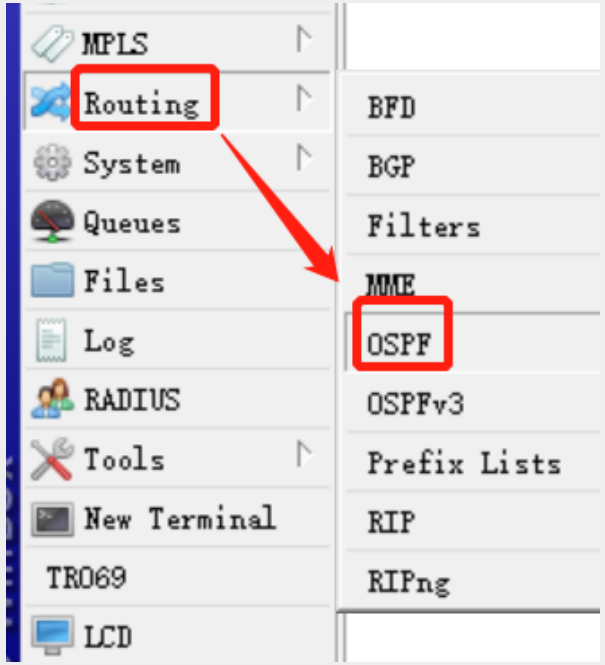
③ LAB 5– How To Configure OSPF In Branch RouterOS Device

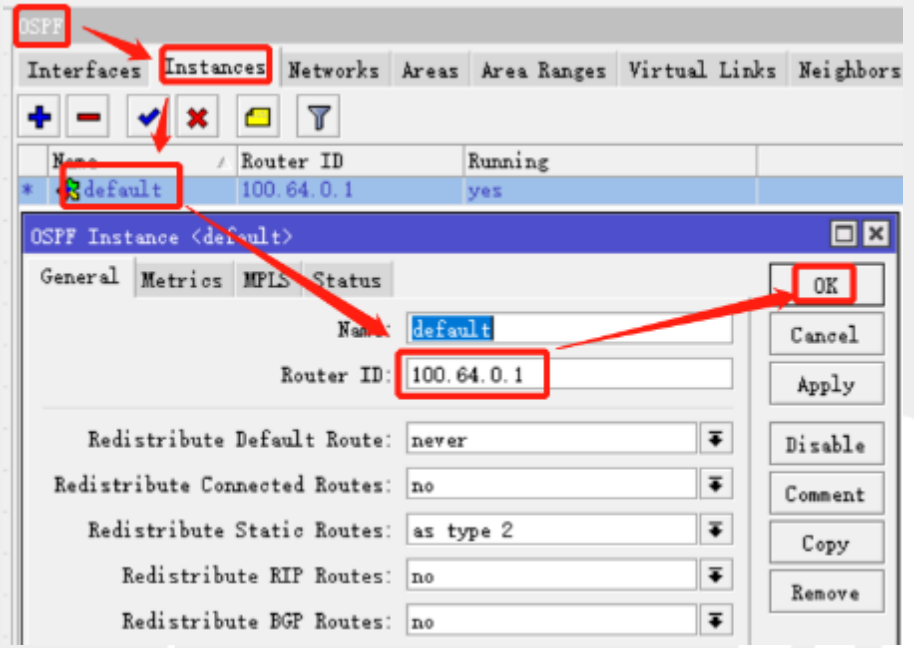
Step 5.3 – Configure OSPF VPN Network In Branch Router Device



③ LAB 6– How To Configure OSPF In HQ RouterOS Device

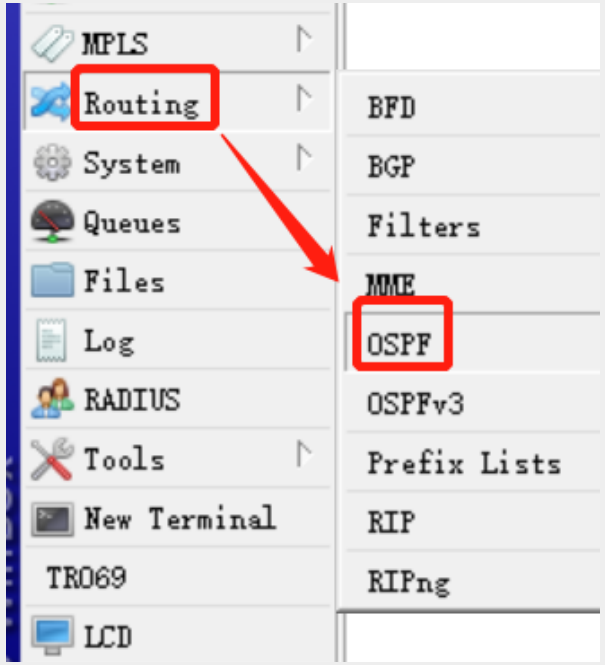
Step 6.1 – Configure OSPF Router-ID In HQ Primary Router Device

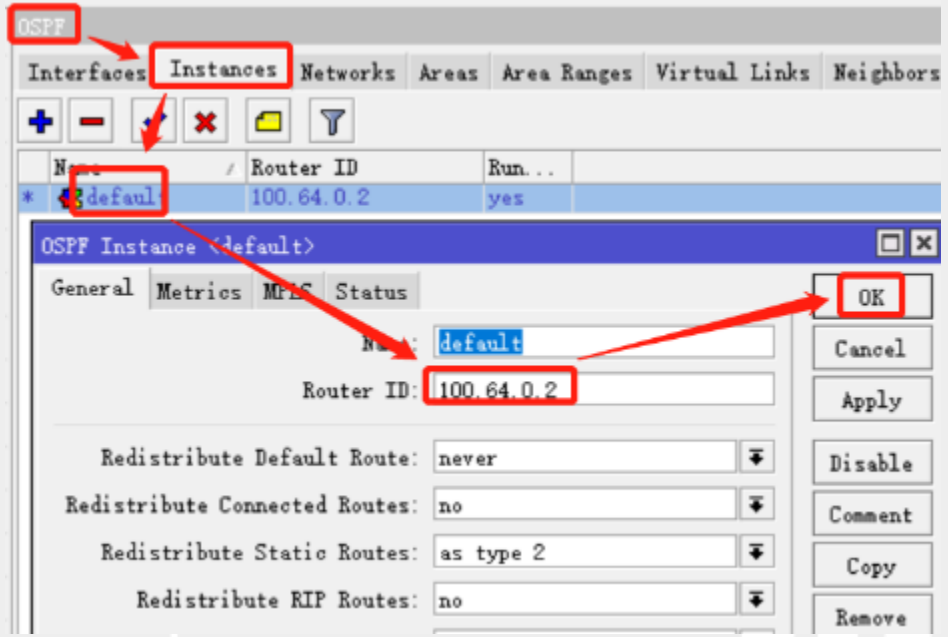




③ LAB 6– How To Configure OSPF In HQ RouterOS Device

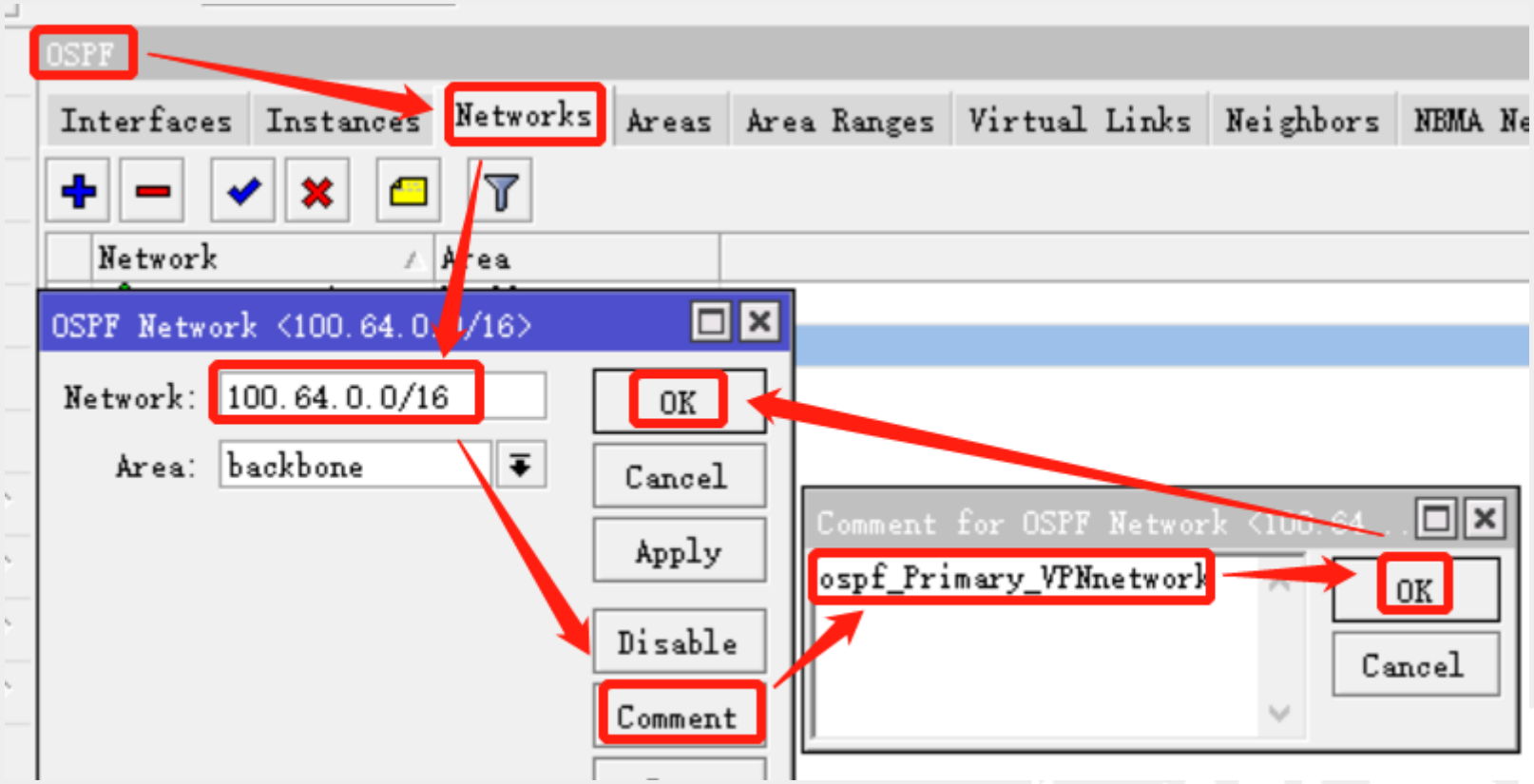
Step 6.2 – Configure OSPF Router-ID In HQ Backup Router Device





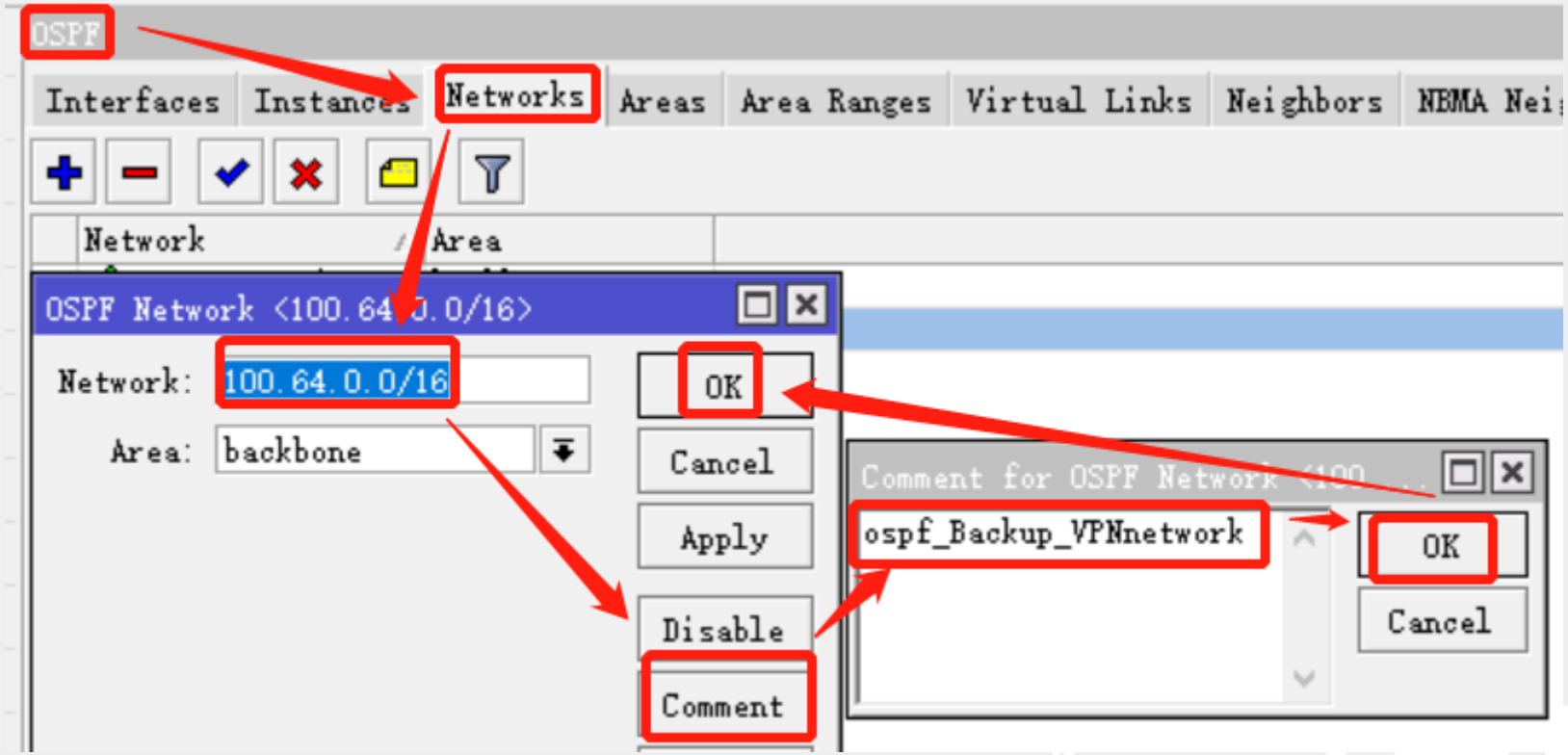
③ LAB 6– How To Configure OSPF In HQ RouterOS Device

Step 6.3 – Configure OSPF VPN Network In HQ Primary Router Device



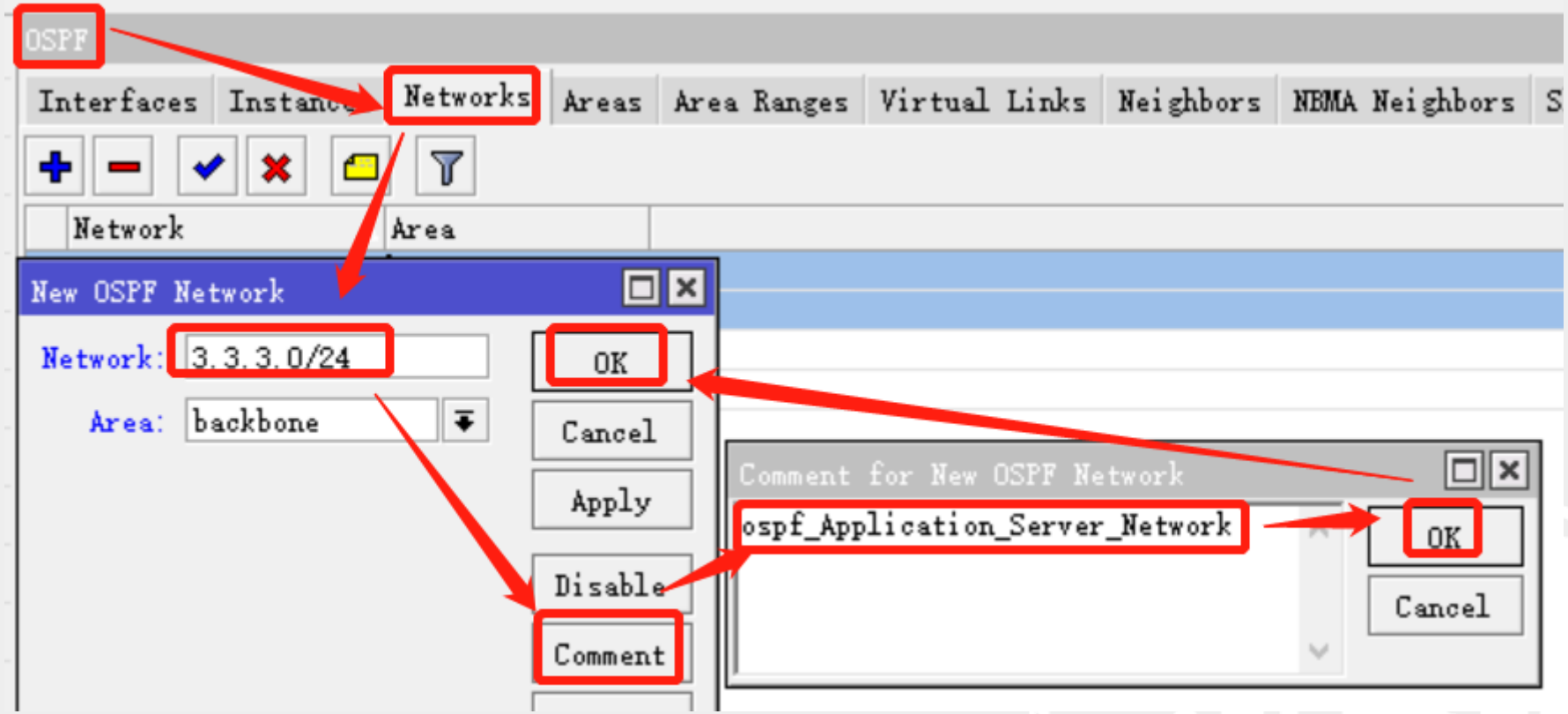
③ LAB 6– How To Configure OSPF In Branch RouterOS Device

Step 6.4 – Configure OSPF VPN Network In HQ Backup Router Device



③ LAB 6– How To Configure OSPF In HQ RouterOS Device

Step 6.5 – Configure OSPF VPN Network In HQ Primary and Backup Router Device

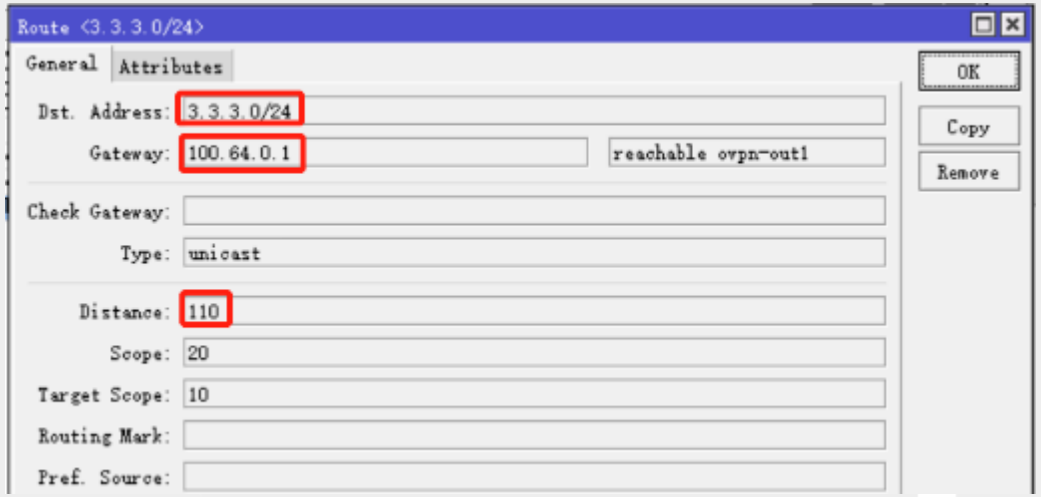


③ LAB 7– Test Line Connectivity-To Primary line

Step 7.1 - Branch ping HQ application device IP: 3.3.3.3/32

```
[admin@Office] > ping 3.3.3.3
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 3.3.3.3                                    56  64 6ms
    1 3.3.3.3                                    56  64 6ms
    2 3.3.3.3                                    56  64 6ms
    3 3.3.3.3                                    56  64 6ms
    4 3.3.3.3                                    56  64 6ms
    5 3.3.3.3                                    56  64 6ms
    6 3.3.3.3                                    56  64 6ms
    sent=7 received=7 packet-loss=0% min-rtt=6ms avg-rtt=6ms max-rtt=6ms
```

```
[admin@Office] > tool traceroute src-address=10.3.3.1 3.3.3.3
 # ADDRESS                          LOSS SENT    LAST     AVG    BEST   WORST
 1 3.3.3.3                           0%    3   6.2ms     6.2     6.2     6.3
-- [Q quit|D dump|C-z pause]
```

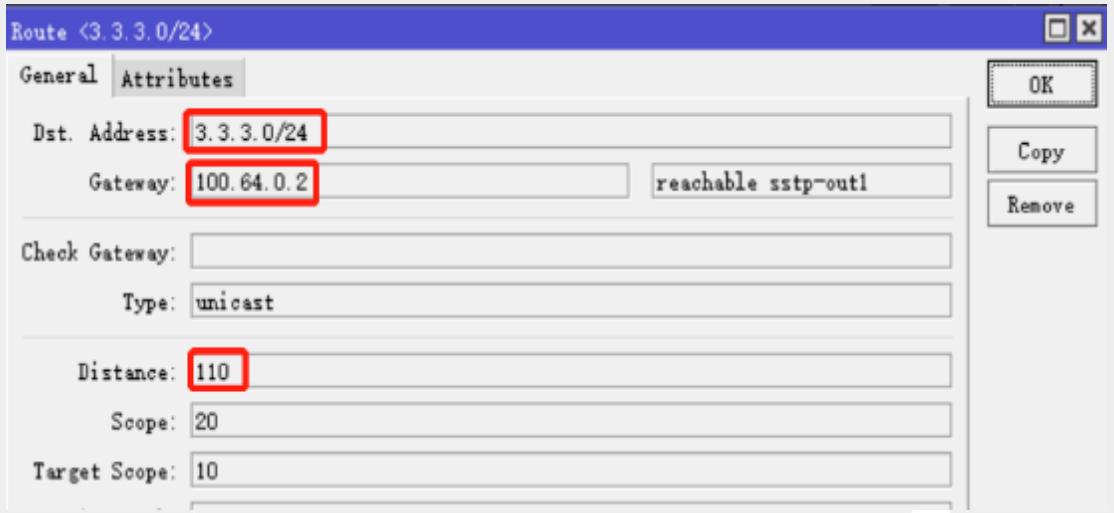


③ LAB 7– Test Line Connectivity-To Backup Line

Step 7.2 - Branch ping HQ application device IP: 3.3.3.3/32

```
[admin@Office] > ping 3.3.3.3
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 3.3.3.3                                    56  64 7ms
    1 3.3.3.3                                    56  64 7ms
    2 3.3.3.3                                    56  64 7ms
    3 3.3.3.3                                    56  64 7ms
    4 3.3.3.3                                    56  64 7ms
    5 3.3.3.3                                    56  64 7ms
    sent=6 received=6 packet-loss=0% min-rtt=7ms avg-rtt=7ms max-rtt=7ms
```

```
[admin@Office] > tool traceroute src-address=10.3.3.1 3.3.3.3
 # ADDRESS                          LOSS SENT    LAST     AVG    BEST   WORST
 1 3.3.3.3                           0%    3   6.2ms     6.2     6.2     6.3
-- [Q quit|D dump|C-z pause]
```



④ Summary

By switching the VPN connection between the primary and backup lines, Branch automatically switches the routes to ensure the normal operation of the production service of the enterprise.

Moreover, for the enterprise, the switching of the primary and backup lines is completely transparent, and the service availability is guaranteed for the enterprise.

Key learning content:

1. How do the two networks of the enterprise establish a VPN with the HQ?
2. How to run OSPF routing protocol between two VPN dial-up lines and the HQ

Note:

The points of knowledge used include:

1. manually create a VPN connection
2. configure OSPF

Questions?

Thank you

zhangwei@189csp.cn
WeChat ID：lovebantianqishi
My Company Website: http://www.189csp.com