Mikrotik TTT

Selective Failover & Intentional Service Segmentation

Using MikroTik RouterOS v7

Date: 11/27/2025

Instructor: Aaron Gustafson

Website: ByteMeNetworks.com

Course Level: MTCRE – MikroTik Certified Routing Engineer
Session Length: 1 Hour (Lecture + Lab)

This Module Tested on rOS 7.20.4

Intro
(And instruction following exercise)

MikroTik Trainer Nov 2025

WhatsApp group

Who am I?

- **Former Owner, Computers N' Stuff LLC (2008–2025)**

Retired from day-to-day operations on March 1, 2025
Self-Host and internal design made CNS more agile and affective

- **Current Owner, ByteMe Networks, LLC**

Focused on networking, ISP services, and technical consulting

- **Education**

A.A.S. in Cisco Network Administration (2012)

- **MikroTik Background**

– Using MikroTik since ~2016 (started with RB750Gr3)
– MikroTik Certified since 2018

- **Primary Specialty**

Network Administration & Infrastructure Design

And Drinking Whiskey ☺

What we will cover

- Real-world need for selective multi-WAN failover
- RouterOS v7 policy routing concepts (Mangle Vs Routing Rules)
- Building routing tables and routing rules
- Creating business-critical vs. non-critical VLAN paths
- Implementing selective failover logic
- Hands-on lab: full configuration + failover test

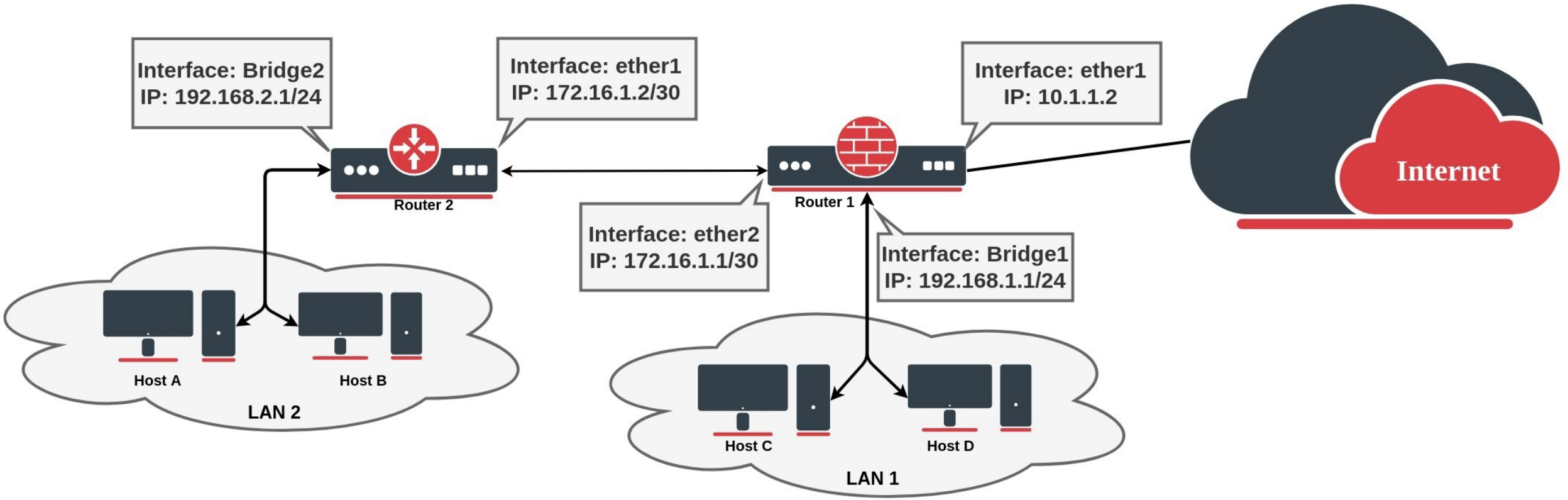
IP Routing

From the MikroTik Wiki and MTCNA – Quick Routing Refresher

Routing is the process of choosing the best path across networks to deliver packets from one host to another.

Always remember: **the most specific route wins.**
For example, a **/32 route** will be preferred over a **/24 route** because it provides a more precise match.

IP Routing

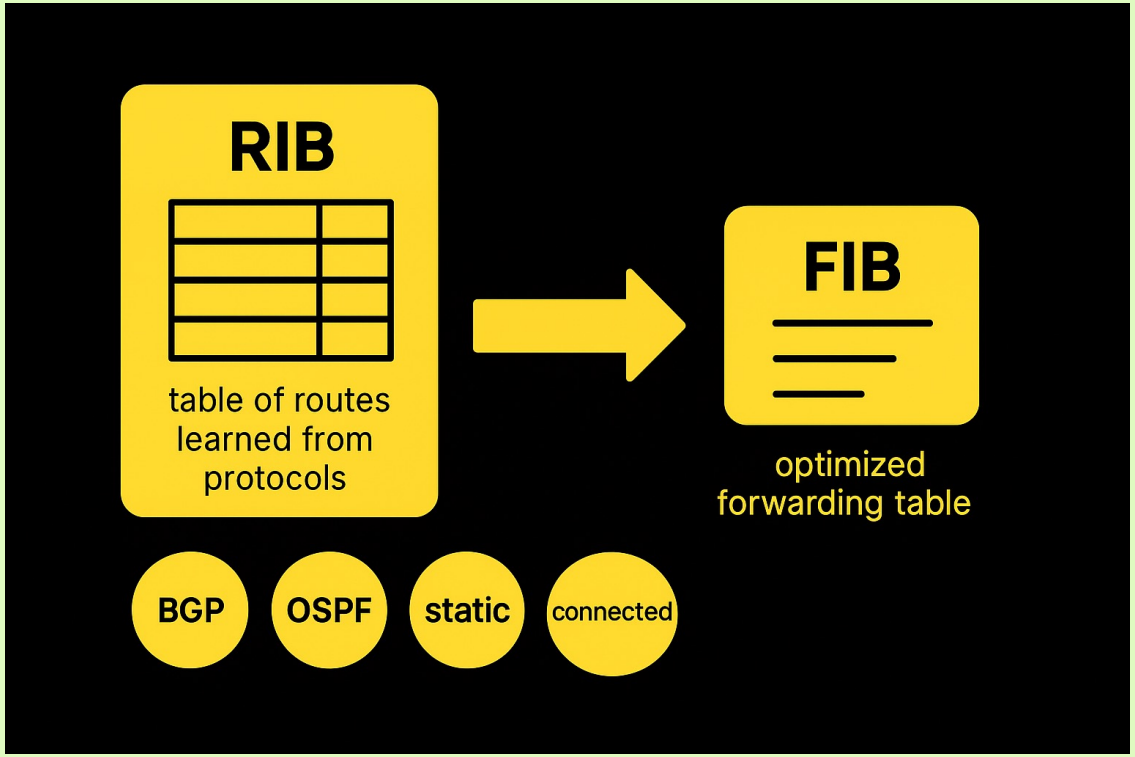

Interface: Bridge2
IP: 192.168.2.1/24
Interface: ether1
IP: 172.16.1.2/30
Interface: ether1
IP: 10.1.1.2
Internet
Router 2
Router 1
Interface: ether2
IP: 172.16.1.1/30
Interface: Bridge1
IP: 192.168.1.1/24
Host A
Host B
LAN 2
Host C
Host D
LAN 1

FIB and RIB

RouterOS routing information consists of two main parts:

FIB (Forwarding Information Base), is used to make packet forwarding decisions. It contains a copy of the necessary routing information.

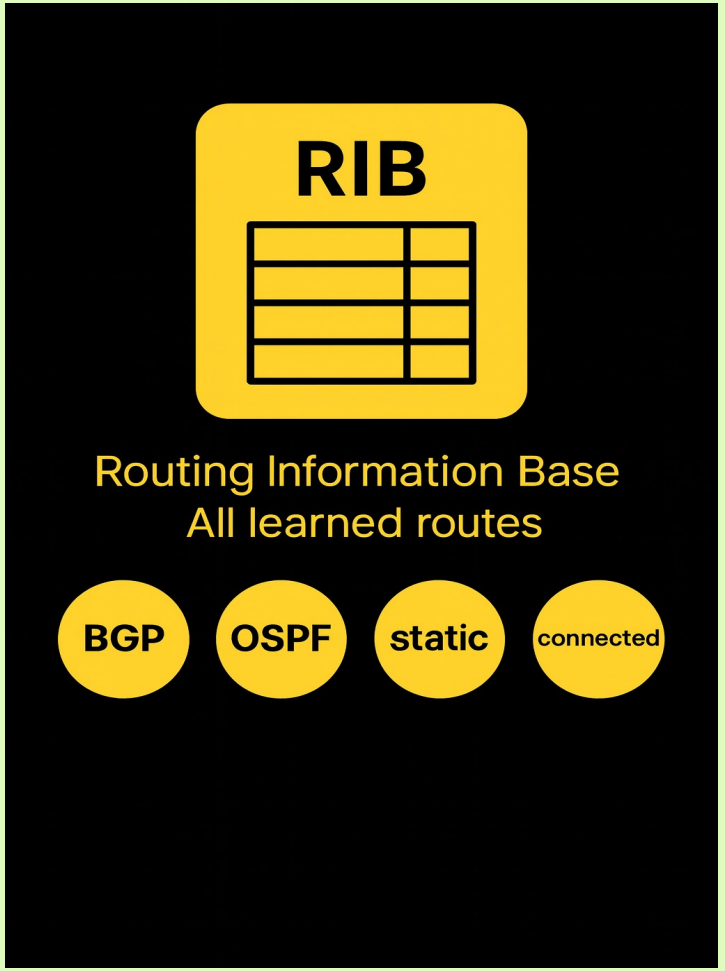
RIB (Routing Information Base) contains all learned prefixes from routing protocols (connected, static, BGP, RIP, OSPF).



RIB

Routing Information Base is a database that lists entries for particular network destinations and their *gateways* (address of the next device along the path or simply *next-hop*). One such entry in the routing table is called a *route*.

A *hop* occurs when a packet is passed from one network segment to another. By default, all routes are organized in one "main" routing table. It is possible to make more than one routing table which we will discuss further in this module.



FIB

FIB uses the following information from the packet to determine its destination:

- source address
- destination address
- source interface
- routing mark

Possible routing decisions are:

- receive packet locally
- discard the packet (either silently or by sending an ICMP message to the sender of the packet)
- send the packet to a specific IP address on a specific interface

Which statement best describes the difference between the Routing Inforwation Base (RIB) and the Forwarding Information Base (FIB)?

A The RIB makes forwarding decisions, while the FIB stores all learned routes from routing protocols.

B The RIB stores all available routes, while the FIB contains only the best, usable routes for actual packet forwarding.

C The FIB stores backup routes, while the RIB stores only active routes.

D The RIB forwards packets based on source address only, while the FIB uses destination address only.

Which statement best describes the difference between the Routing Inforwation Base (RIB) and the Forwarding Information Base (FIB)?

A The RIB makes forwarding decisions, while the FIB stores all learned routes from routing protocols.

B The RIB stores all available routes, while the FIB contains only the best, usable routes for actual packet forwarding.

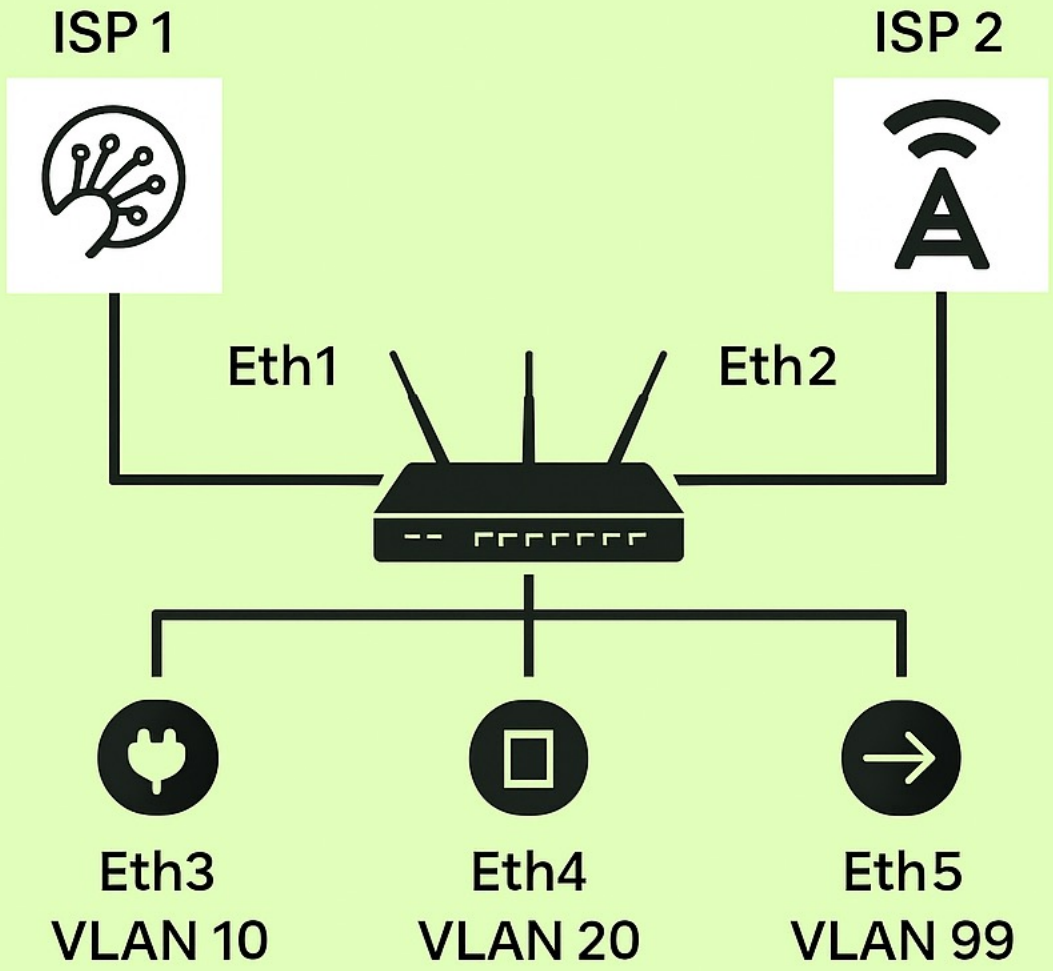
C The FIB stores backup routes, while the RIB stores only active routes.

D The RIB forwards packets based on source address only, while the FIB uses destination address only

Why Selective Failover Matters

- Businesses (At least in the US) often have **two WAN connections**
  - ISP1: Primary (Fiber/Coax)
  - ISP2: Backup (LTE)
- Not all traffic should fail over
  - **Business-critical devices** must stay online
  - **Guest Wi-Fi / non-essential services** can be dropped
- Preserves **limited LTE bandwidth** for priority operations
- Used widely in retail and hospitality
  - Example: **Chick-fil-A (Quick Service Restaurant)** POS networks fail over; guest Wi-Fi does not to allow Card Processing
  - Can sometimes save money when dealing with per-usage billing for backup circuits

LAB Topology



Policy Goals

Office WiFi (VLAN10) → Use ISP1 → Fail over to ISP2

Office Wired (VLAN20) → Use ISP1 → Fail over to ISP2

Guest WiFi (VLAN99) → Use ISP1 → *Do not* fail over
(Intentionally loses Internet during outage)

to_isp1	Primary Fiber (ISP1) + Failover to ISP2
guest_isp1	Guest-only → ISP1 only (no fallback)

Initialization

Go to TTT.ByteMeNetworks.com and open both Base Config and Solutions

Factory Reset your router with no-default config and winbox into your router

Copy and paste the Base Config Text into CLI

Password after config will be admin/admin

TIP: Make a backup using Terminal “export file=backup show-sensitive”

Configuration

1. Create Routing Tables

- `to_isp1`
- `guest_isp1`

/routing table
add name=to_isp1 fib
add name=guest_isp1 fib

TIP: When working on a remote MikroTik using Winbox, always use **Safe Mode**.
Turn Safe Mode **on**, make your changes, and then turn it **off and back on again at each checkpoint**.
This creates a “save point,” so if you lose connection, the router will **automatically roll back** to the last Safe Mode save instead of locking you out.

Configuration

2. Add Default Routes per Table

- ISP1 primary (distance 1)
- ISP2 backup (distance 2)
- Guest table ONLY includes ISP1

```
/ip route
add dst-address=0.0.0.0/0 gateway=192.168.1.1 routing-table=to_isp1 distance=1 check-gateway=ping
add dst-address=0.0.0.0/0 gateway=192.168.2.1 routing-table=to_isp1 distance=2 check-gateway=ping
add dst-address=0.0.0.0/0 gateway=192.168.1.1 routing-table=guest_isp1 distance=1 check-gateway=ping
```

Configuration

3. Add Routing Rules

- VLAN10 → `to_isp1`
- VLAN20 → `to_isp1`
- VLAN99 → `guest_isp1` (lookup-only-in-table)

/routing rule
add src-address=192.168.10.0/24 action=lookup-only-in-table table=to_isp1
add src-address=192.168.20.0/24 action=lookup-only-in-table table=to_isp1
add src-address=192.168.99.0/24 action=lookup-only-in-table table=guest_isp1

Configuration

4. Test ISP 1 functional

- Ping from each VLAN
- Simulate ISP1 failure
- Observe selective failover behavior

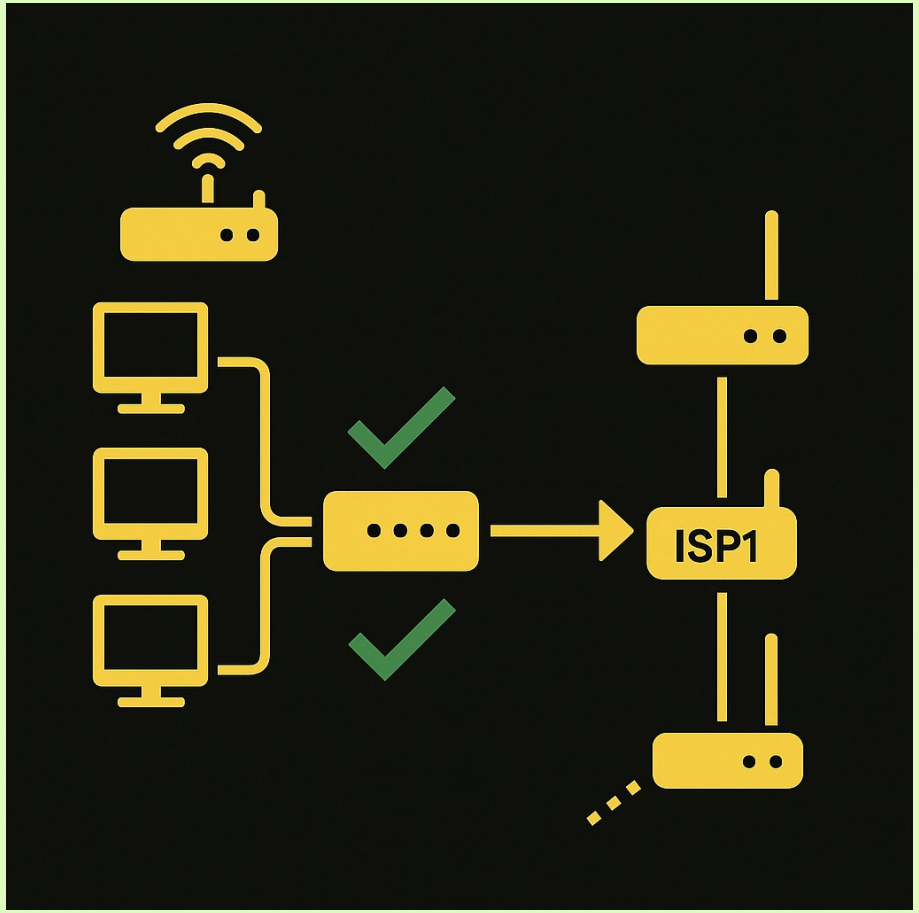
- From Ether 3 Ping 172.26.2.1
- From Ether 4 Ping 172.26.2.1
- From Ether 5 Ping 172.26.2.1

Testing

From all VLANs, test:
ping 172.26.2.1

Expected:
✔ All VLANs reach **172.26.2.1** via ISP1
✔ Guest VLAN works normally
✔ No traffic uses 192.168.2.1 yet

Optional traceroute (if needed):
traceroute 172.26.2.1.



Configuration

5. Test ISP 1 failure

- From Ether 3 Ping 172.26.2.1 – should work
- From Ether 4 Ping 172.26.2.1 – should work
- From Ether 5 Ping 172.26.2.1 – SHOULD NOT WORK

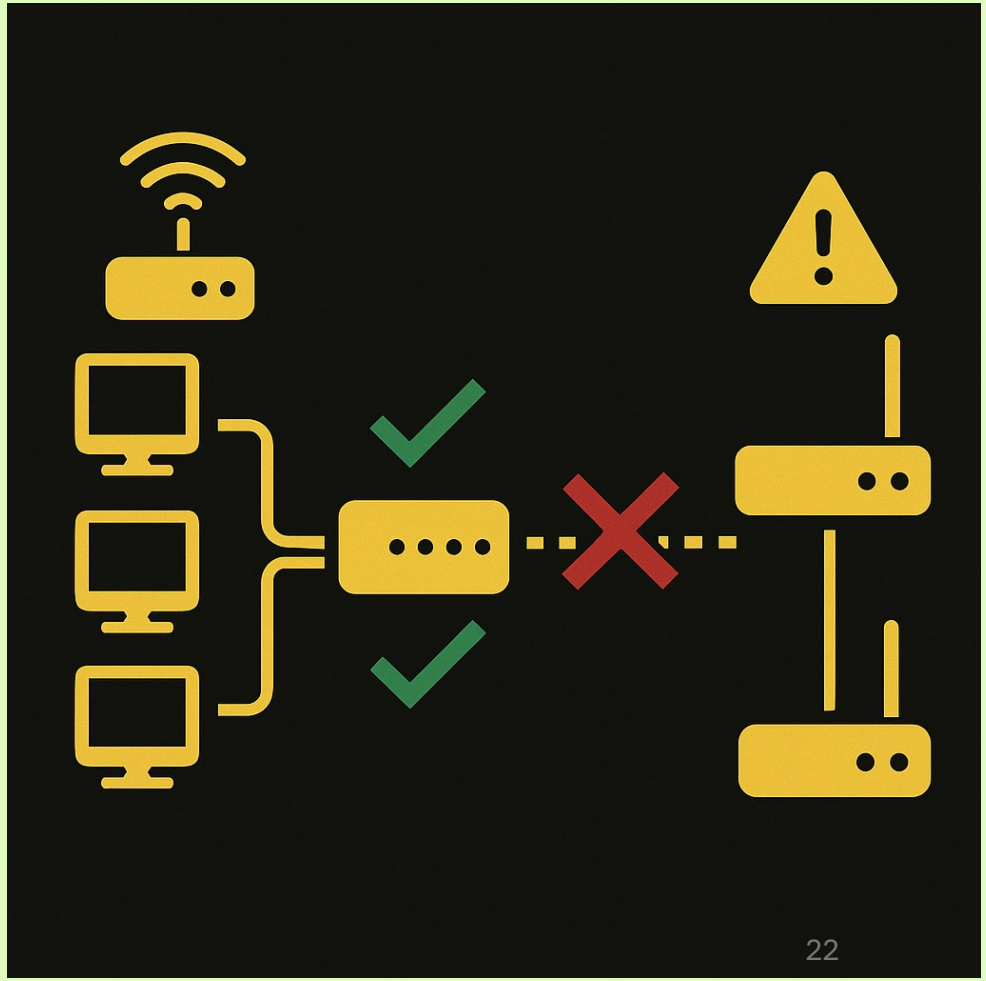
Testing

Simulate ISP1 Failure

Business VLANs (10 & 20):
ping 172.26.2.1
Expected:
✓ Should reach **172.26.2.1** (failover to ISP2)

Guest VLAN (99):
ping 172.26.2.1

Expected:
✗ Should **not** get a reply
✗ Should **not** have a route to ISP2



Summary

What You Learned Today

- How RouterOS v7 handles **Policy-Based Routing (PBR)**
- Creating and managing **multiple routing tables**
- Assigning **VLANs to specific routing tables** using routing rules
- Using **lookup-only-in-table** to enforce strict path isolation
- Building **selective WAN failover** between two upstreams
- Verifying routing behavior with targeted tests (e.g., ping **172.26.2.1**)

Real-World Use Cases

- Retail networks: **POS continuity** and **guest WiFi isolation**
- Branch sites using **LTE / satellite** as secondary WAN
- MSP environments requiring **customer or service-tier segmentation**
- Reducing usage on **metered or high-cost backup links**

Summary

Closing Notes
This entire configuration works on any MikroTik running RouterOS v7+.
The design scales easily—add more VLANs or WANs without changing the core logic.
You now have a reusable template for real-world selective failover deployments.

Branding Tip
Use CNAMEs to mask the default MikroTik DDNS and present a branded domain:
serial.mynetname.com → customer.ByteMeNetworks.com
Great for VPNs, camera access, and keeping your company name front-and-center.

Security Tip
The MikroTik default config is only a starting point—it's **not secure**.
Build your own standardized, hardened default configuration to maintain consistent security across every deployment.

Contact Info

Download a copy of this Presentation at TTT.ByteMeNetworks.com

E-mail: Aaron@ByteMeNetworks.com
Office Number: +1 254 845 6012

Access Tip:
Use **Address Lists** and **FQDNs** for your home or corporate routers so you always have a reliable way to reach remote devices.
Example: point **home.bytemenetworks.com** (CNAME) to your MikroTik DDNS name (**serial.mynetname.com**) to avoid getting locked out if the IP changes.

On remote Routers:
/Ip firewall address-list add address=home.bytemenetworks.com comment=Home.bytemenetworks.com list="Exempt IP Addresses"
/Ip Firewall Filter add action=accept chain=input comment="Allow Exempt IP Addresses" src-address-list="Exempt IP Addresses"