

WELCOME TO MUM INDIA 2018

TARA CONSULTANTS PVT LTD



www.ispmart.com



Agenda

How to Implement large Scalable Network with Mikrotik

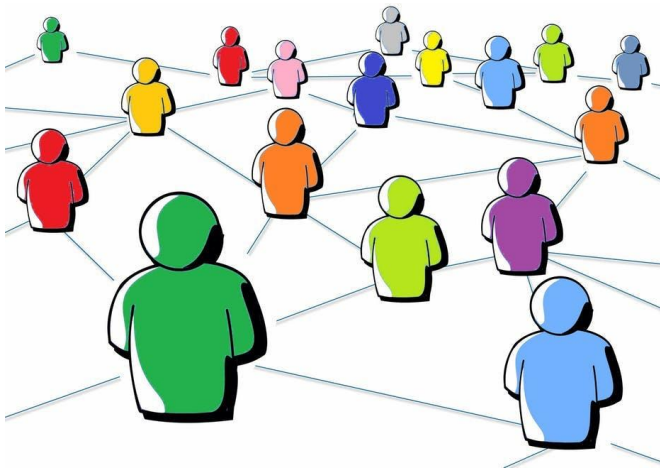
- What is network
- What is large network
 - Static Routing v/s Dynamic Routing
- Topology
- MPLS and Its Advantage
- Configuration Example
- Some Smart Configurations for ISP benefits
- Recent Vulnerabilities and their Solutions
- Save your back with some small configurations

By Vikas Gupta



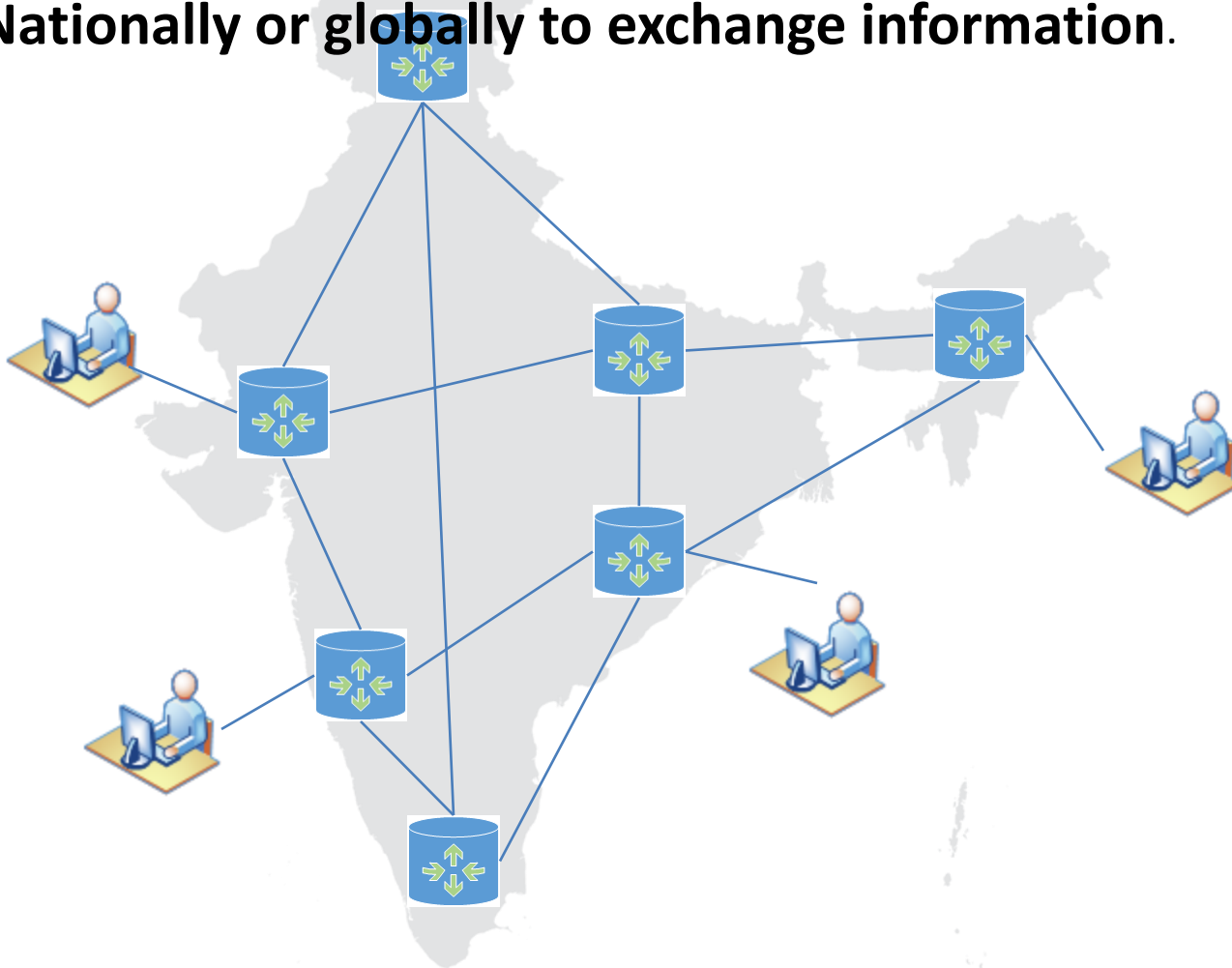
What is Network ?

To interact/communicate with others to exchange information and develop professional or social contacts.

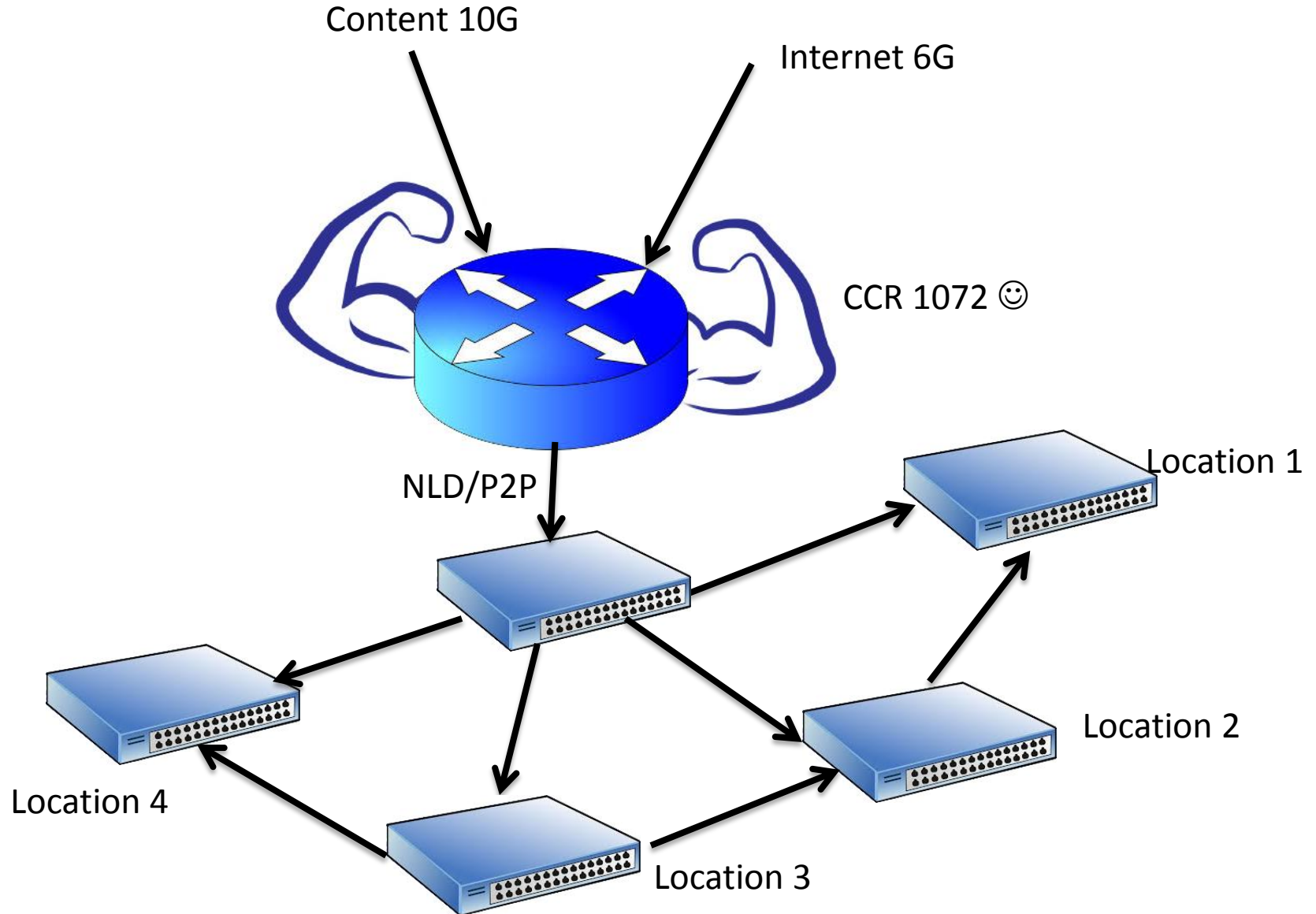


What is ISP Network ?

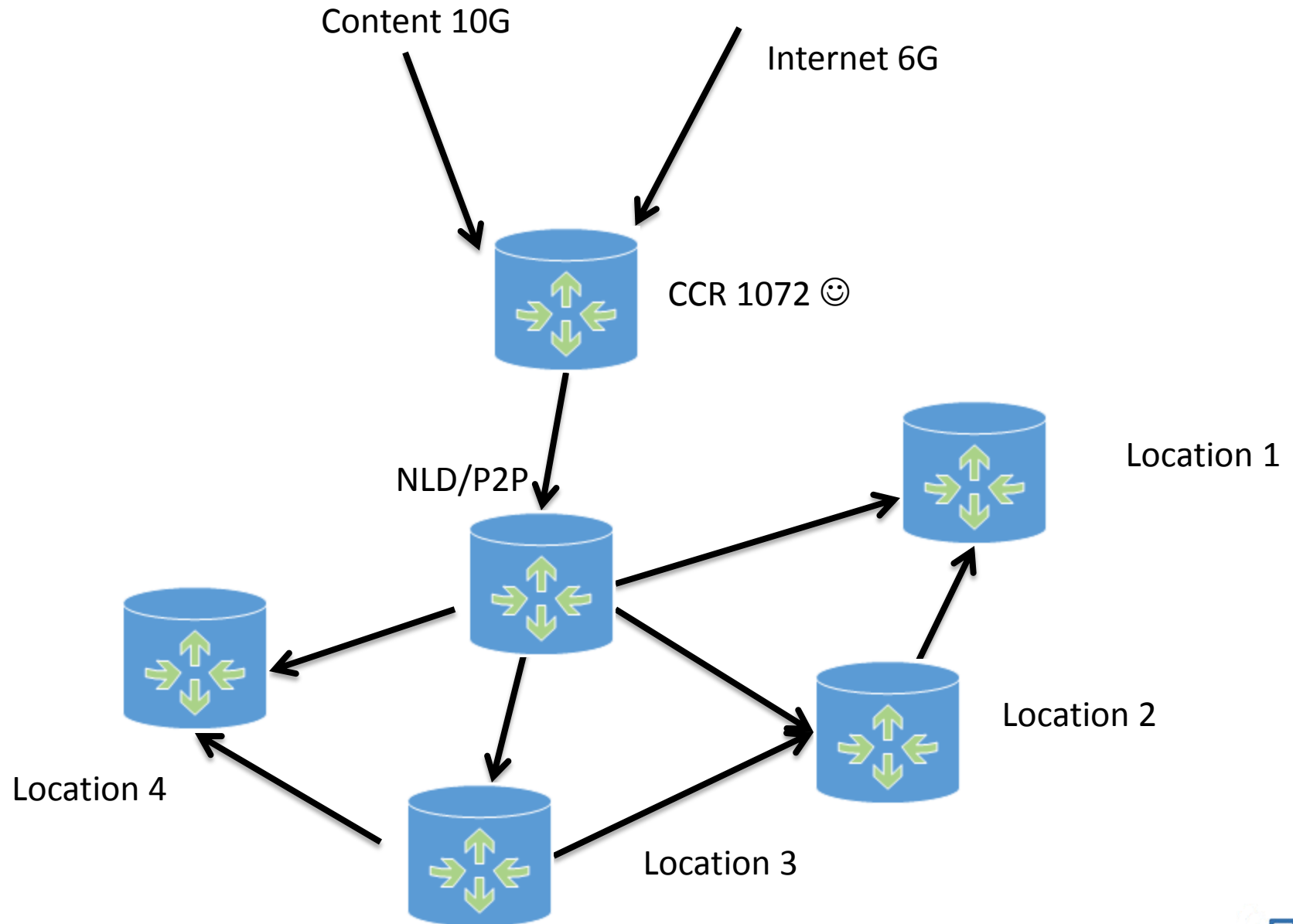
ISP Network is a group of multiple routers which connect users Nationally or globally to exchange information.



What is large and scalable network



What is Large Scalable Network



Static v/s Dynamic Routing

Static Routing	Dynamic Routing
Preferred for Small Setup	Preferred for large setup
Not Fault Tolerant	Fault Tolerant
Less Overhead on CPU	More Overhead on CPU
Manual Routing Information Update	Auto Update
Granular control on how traffic is routed	dynamically choose a different (or better) route

MPLS and Its Usage

What is MPLS?

Multiprotocol Label Switching (MPLS) is a type of data-carrying technique for high-performance telecommunications networks. MPLS directs data from one network node to the next based on short path labels rather than long network addresses, avoiding complex lookups in a routing table.

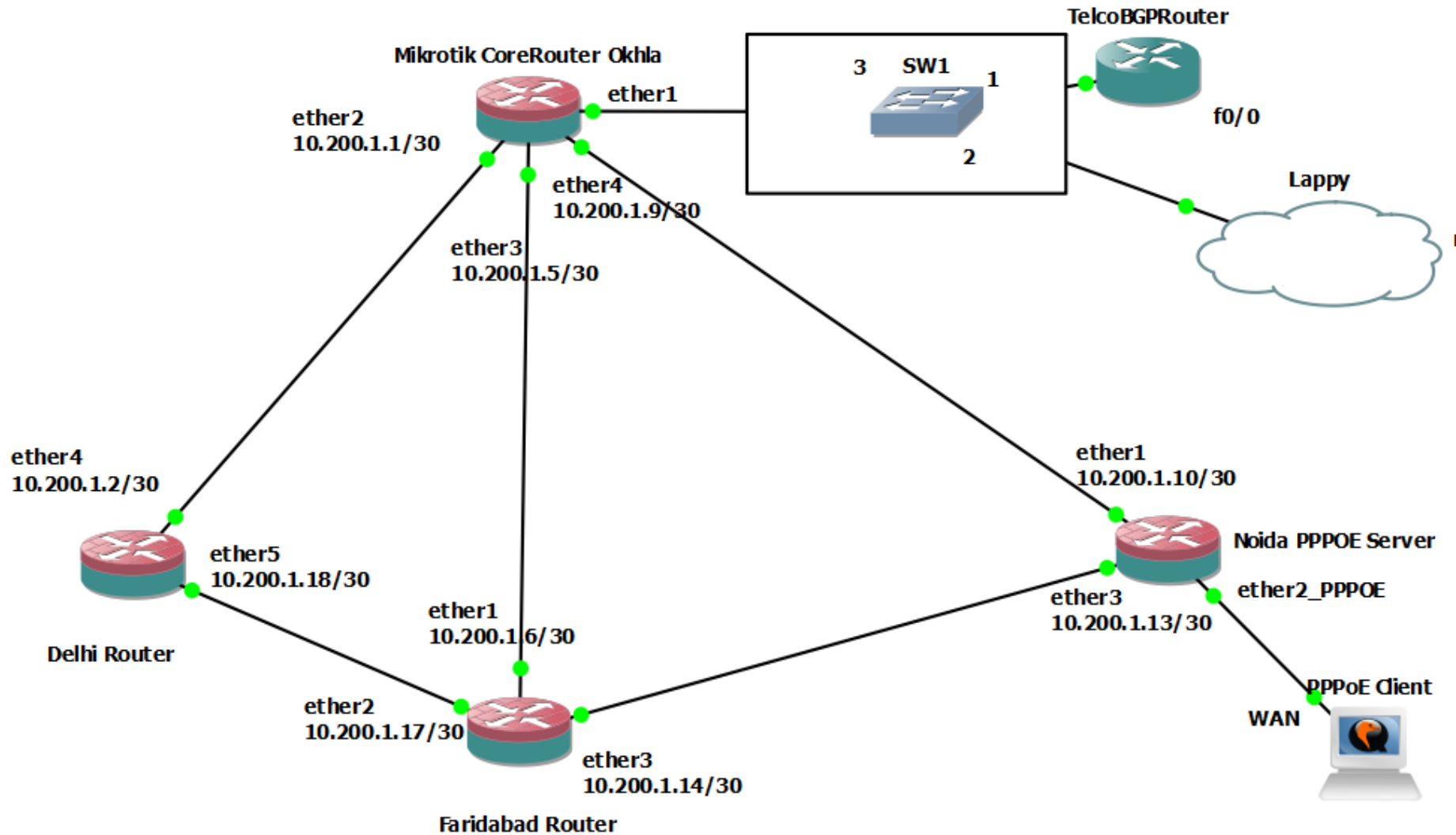
WHY MPLS ?

Did you ever order something online from a distant retailer and then track the package as it makes strange and seemingly illogical stops all over the country. That's similar to the way IP routing on the Internet works. When an internet router receives an IP packet, that packet carries no information beyond a destination IP address. There is no instruction on how that packet should get to its destination or how it should be treated along the way.

Each router has to make an independent forwarding decision for each packet based solely on the packet's network-layer header. Thus, every time a packet arrives at a router, the router has to "think through" where to send the packet next. The router does this by referring to complex routing tables.

The process is repeated at each hop along the route until the packet eventually reaches its destination. All of those hops and all of those individual routing decisions result in poor performance for time-sensitive applications like video-conferencing or voice over IP (VoIP).

Lets try one Topology and Configuration



Some Smart Configurations for ISP Benefits

- Donot use public IPs on your distribution routers/Edge Routers
- Allot Public IPs only to customer end device only
- Forward static public route only on private IP

•Recent Vulnerabilities in Mikrotik

[Mikrotik](#) » [RouterOS](#) : Security Vulnerabilities

CVSS Scores Greater Than: [0](#) [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#)

Sort Results By : [CVE Number Descending](#) [CVE Number Ascending](#) [CVSS Score Descending](#) [Number Of Exploits Descending](#)

[Copy Results](#) [Download Results](#)

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity
1	CVE-2018-7445	119		Exec Code Overflow	2018-03-19	2018-04-24	10.0	None	Remote	Low
A buffer overflow was found in the MikroTik RouterOS SMB service when processing NetBIOS session request messages. Remote attackers with access to execution on the system. The overflow occurs before authentication takes place, so it is possible for an unauthenticated remote attacker to exploit it. All versions 6.41.3/6.42rc27 are vulnerable.										
2	CVE-2017-8338	399			2017-05-18	2017-06-01	7.8	None	Remote	Low
A vulnerability in MikroTik Version 6.38.5 could allow an unauthenticated remote attacker to exhaust all available CPU via a flood of UDP packets on port affected router from accepting new connections; all devices will be disconnected from the router and all logs removed automatically.										
3	CVE-2017-7285	400			2017-03-29	2017-04-10	7.8	None	Remote	Low
A vulnerability in the network stack of MikroTik Version 6.38.5 released 2017-03-09 could allow an unauthenticated remote attacker to exhaust all available router from accepting new TCP connections.										
4	CVE-2017-6297	254			2017-02-27	2017-03-15	4.3	None	Remote	Medium
The L2TP Client in MikroTik RouterOS versions 6.83.3 and 6.37.4 does not enable IPsec encryption after a reboot, which allows man-in-the-middle attack access to networks on the L2TP server by monitoring the packets for the transmitted data and obtaining the L2TP secret.										
5	CVE-2015-2350	352		CSRF	2015-03-19	2015-09-24	6.8	None	Remote	Medium
Cross-site request forgery (CSRF) vulnerability in MikroTik RouterOS 5.0 and earlier allows remote attackers to hijack the authentication of administrator via a request in the status page to /cfg.										
6	CVE-2012-6050	16	1	DoS	2012-11-26	2017-08-28	6.4	None	Remote	Low
The winbox service in MikroTik RouterOS 5.15 and earlier allows remote attackers to cause a denial of service (CPU consumption), read the router version download the router's DLLs or plugins, as demonstrated by roteros.dll.										

Total number of vulnerabilities : 6 Page : 1 (This Page)

- Save your self with some small configurations**

IP Service>

Change port of known services or disable them if not usable like Telnet, FTP, SSH, API, API_SSL

IP Socks>Disable It

IP DNS >Don't enable it on your Border or any router until unless you haven't protected it from Outside access

IP Firewall Raw >

Block unused Static Ips

IP Firewall Raw/Filter >

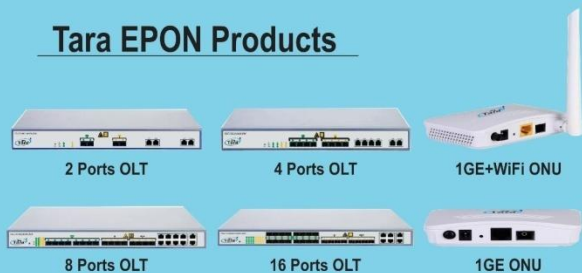
Block Port Scanning

Block ICMP of your Border Router

https://mum.mikrotik.com/presentations/IN16/presentation_3611_1474890637.pdf

Questions ?

Tara EPON Products



Fiber Accessories



Our Strength

- ★ Manufacturing EPON OLT/ONU. ★
- ★ Triple Play/Quad Play Solutions. ★
- ★ WISP infrastructure. ★
- ★ ISP Solutions. ★
- ★ Point to Point Solutions. ★
- ★ Point to Multi Point Solutions. ★
- ★ Routing Solutions. ★
- ★ Surveillance Solutions. ★
- ★ FTTx Solutions. ★
- ★★ After Sale Support ★★

Tara GPON Products



Switches



SIP Products

(Session Initiation Protocol)



Brands which we deals



Contact Details:

307,08,09 Osian Building-12, Nehru Place, New Delhi-110019
Tel : 011-65170029, 46570272, 46570273, Mob : +91-9811686026, 9205137250, 9210898452
E-mail: sales@tcplonline.com, gamma@tcplonline.com, bharat@tcplonline.com
Web: www.ispmart.com/www.tarafiber.com

Thank You for Listening 😊

TARA CONSULTANTS PVT LTD

307, OSIAN BUILDING,
12, NEHRU PLACE,
NEW DELHI-110019

TEL: 011-46570273

Ph : +91-9311686026, +91-9811686026

FAX:011-26448917

www.tcplonline.com

www.ispmart.com

