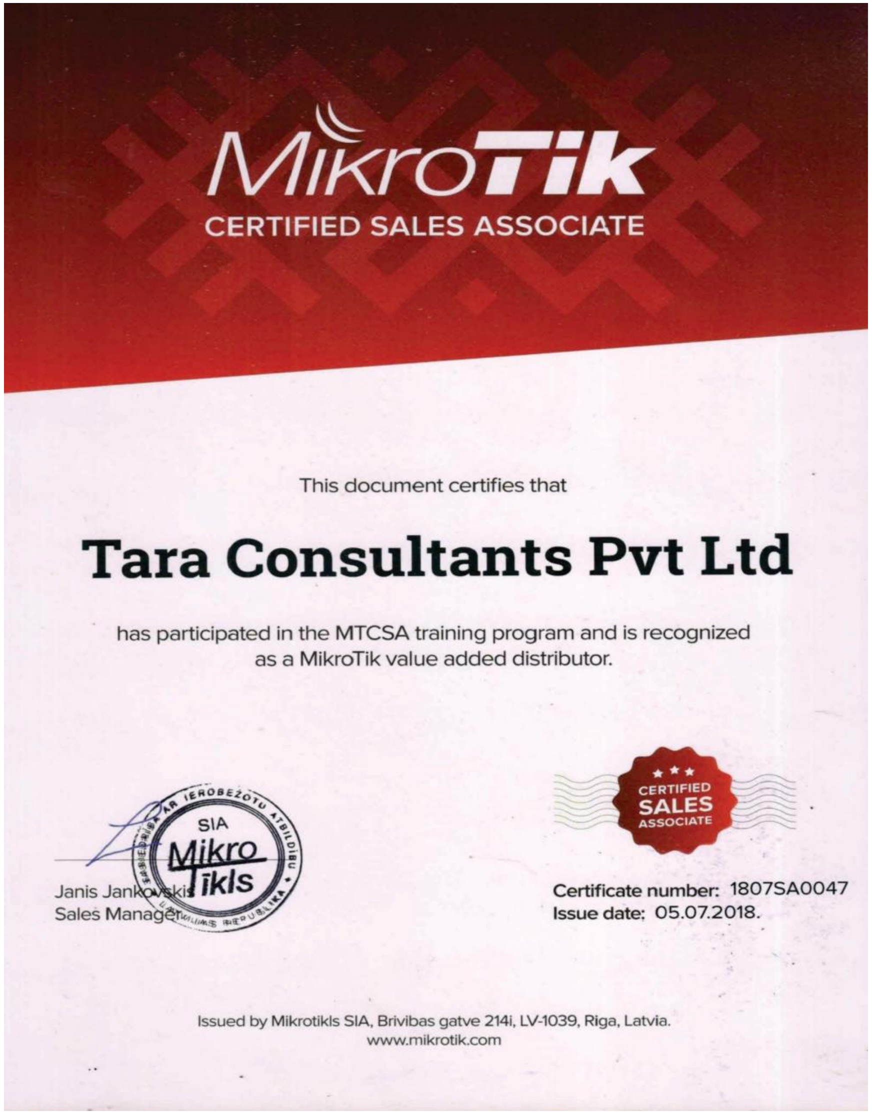
WELCOME TO MUM INDIA 2018

TARA CONSULTANTS PVT LTD

tcpl
online

www.ispmart.com

WELCOME TO MUM INDIA 2018



MikroTik

CERTIFIED SALES ASSOCIATE

This document certifies that

Tara Consultants Pvt Ltd

has participated in the MTCSA training program and is recognized as a MikroTik value added distributor.

SABIEDRĪBA AR IEROBEŽOTU ATBILDĪBU
SIA
Mikro Tikls
LATVIJAS REPUBLIKA

Janis Jankovskis
Sales Manager

CERTIFIED
SALES
ASSOCIATE

Certificate number: 1807SA0047
Issue date: 05.07.2018.

Issued by Mikrotikls SIA, Brivibas gatve 214i, LV-1039, Riga, Latvia.
www.mikrotik.com

tcpl
online

Agenda

How to Implement large Scalable Network with Mikrotik

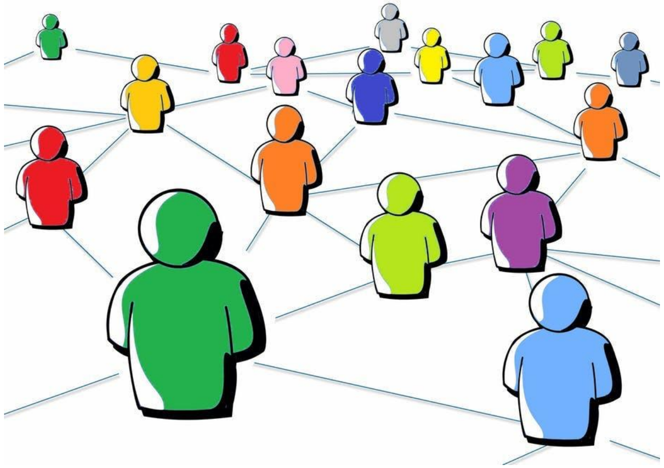
- What is network
- What is large network
  - Static Routing v/s Dynamic Routing
  - Topology
  - MPLS and Its Advantage
  - Configuration Example
  - Some Smart Configurations for ISP benefits
  - Recent Vulnerabilities and their Solutions
  - Save your back with some small configurations

By Vikas Gupta

Powered by MikroTik

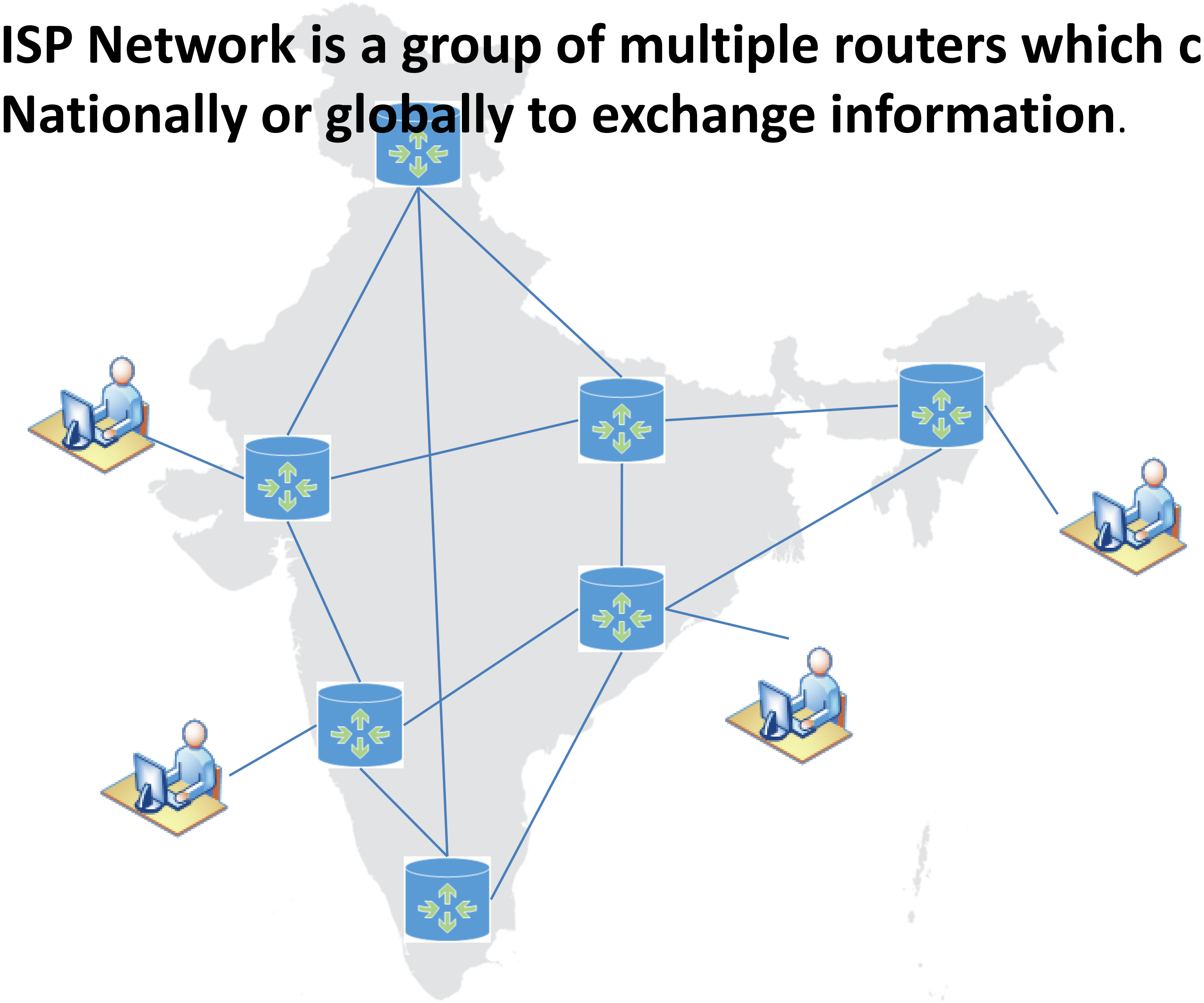
What is Network ?

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

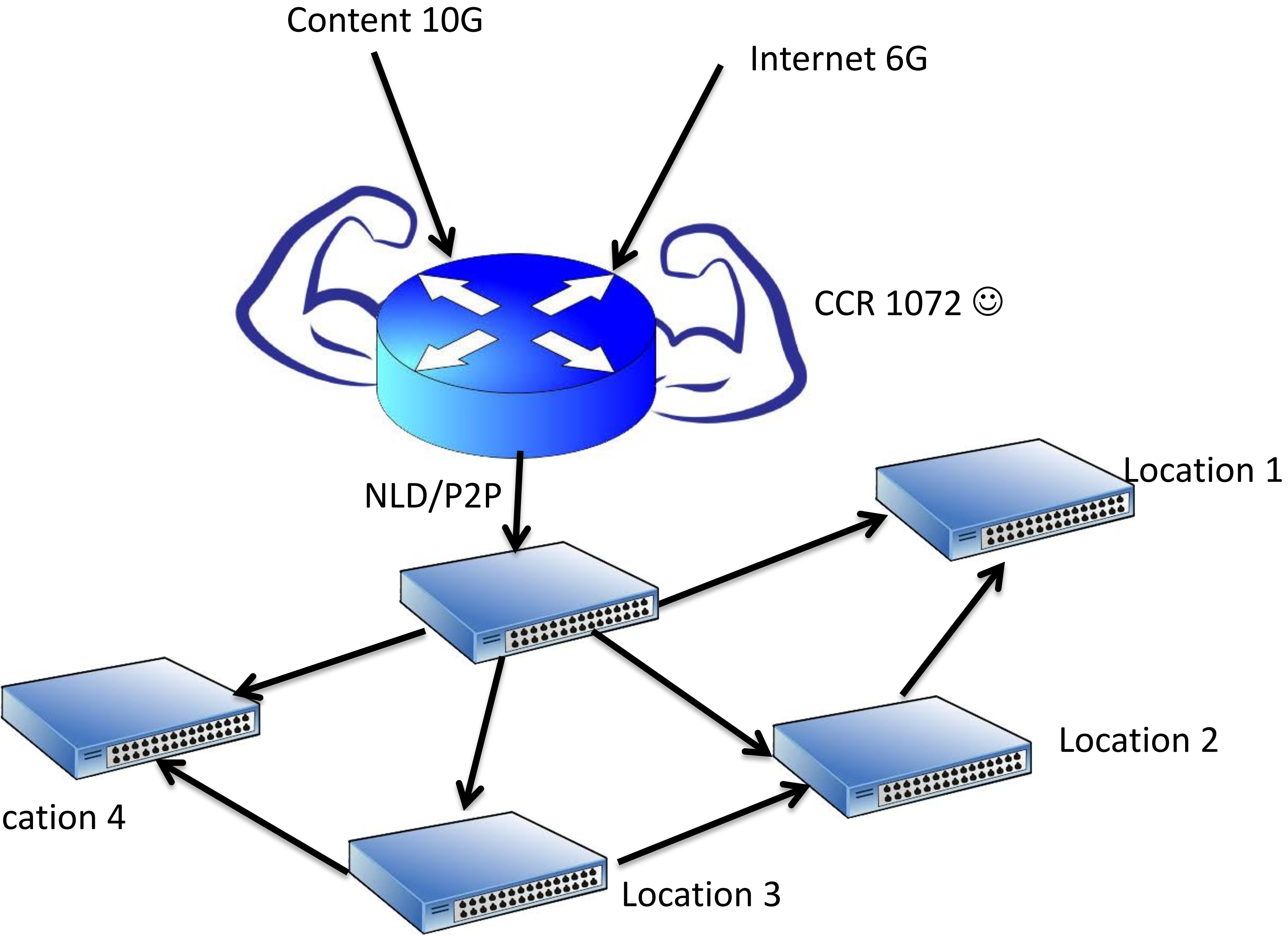


What is ISP Network ?

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



What is large and scalable network



Content 10G

Internet 6G

CCR 1072 ☺

NLD/P2P

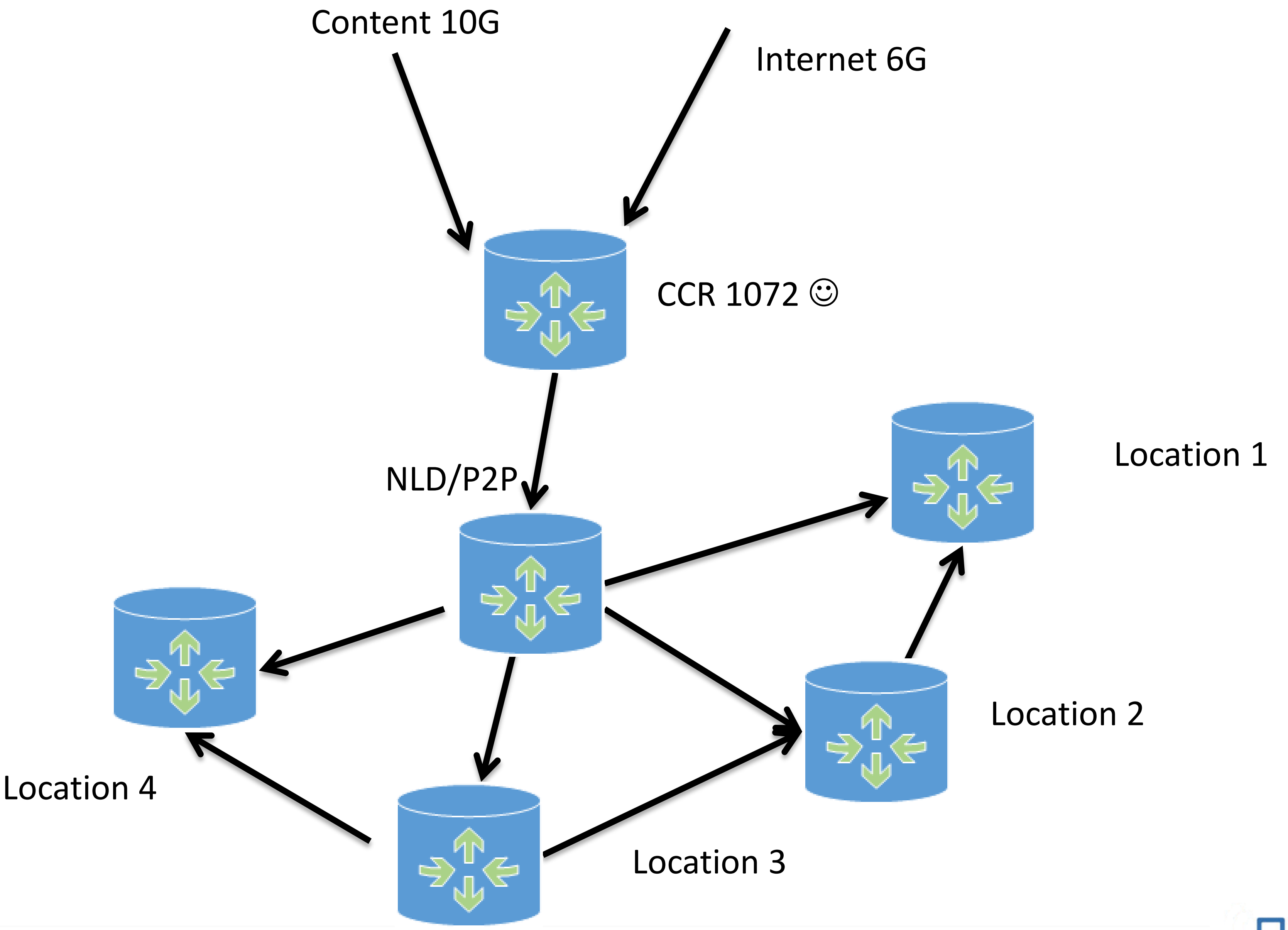
Location 1

Location 2

Location 3

Location 4

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.

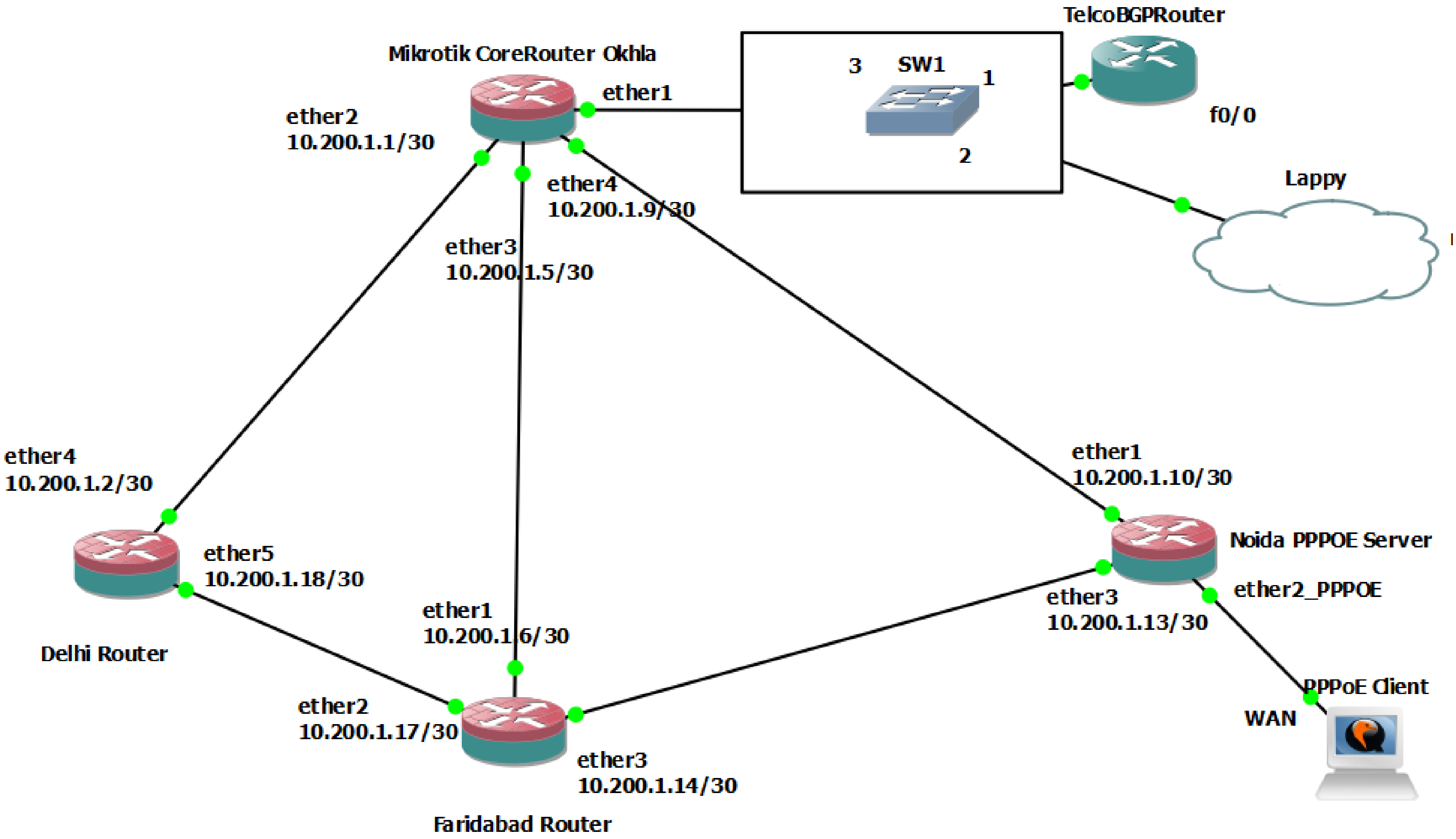
WHY MPLS ?

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



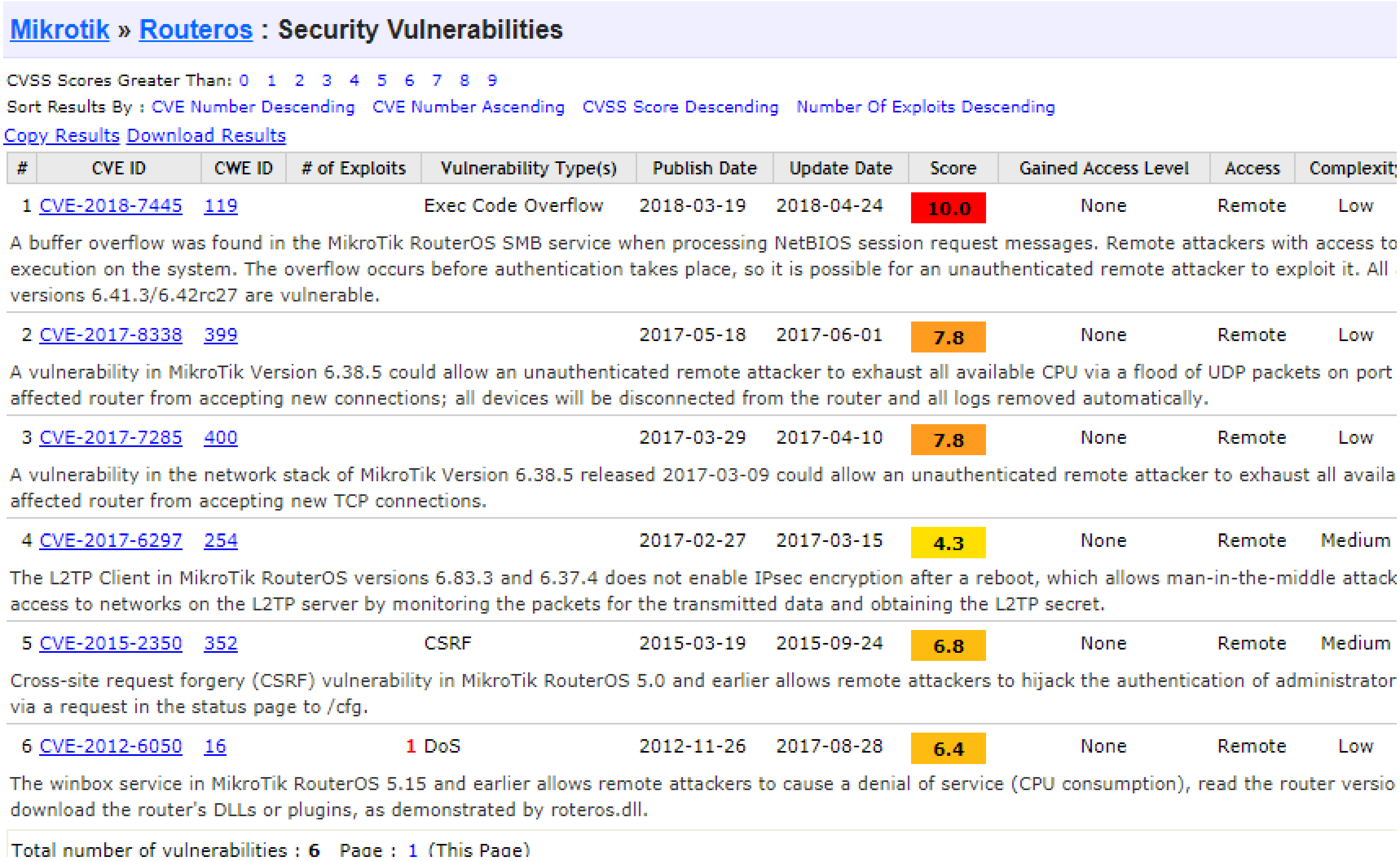
Some Smart Configurations for ISP Benefits

- 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

<table>
<tr><th>#</th><th>CVE ID</th><th>CWE ID</th><th># of Exploits</th><th>Vulnerability Type(s)</th><th>Publish Date</th><th>Update Date</th><th>Score</th><th>Gained Access Level</th><th>Access</th><th>Complexit</th></tr>
<tr><td>1</td><td>CVE-2018-7445</td><td>119</td><td></td><td>Exec Code Overflow</td><td>2018-03-19</td><td>2018-04-24</td><td>10.0</td><td>None</td><td>Remote</td><td>Low</td></tr>
<tr><td colspan="11">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.</td></tr>
<tr><td>2</td><td>CVE-2017-8338</td><td>399</td><td></td><td></td><td>2017-05-18</td><td>2017-06-01</td><td>7.8</td><td>None</td><td>Remote</td><td>Low</td></tr>
<tr><td colspan="11">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.</td></tr>
<tr><td>3</td><td>CVE-2017-7285</td><td>400</td><td></td><td></td><td>2017-03-29</td><td>2017-04-10</td><td>7.8</td><td>None</td><td>Remote</td><td>Low</td></tr>
<tr><td colspan="11">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 availa affected router from accepting new TCP connections.</td></tr>
<tr><td>4</td><td>CVE-2017-6297</td><td>254</td><td></td><td></td><td>2017-02-27</td><td>2017-03-15</td><td>4.3</td><td>None</td><td>Remote</td><td>Medium</td></tr>
<tr><td colspan="11">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.</td></tr>
<tr><td>5</td><td>CVE-2015-2350</td><td>352</td><td></td><td>CSRF</td><td>2015-03-19</td><td>2015-09-24</td><td>6.8</td><td>None</td><td>Remote</td><td>Medium</td></tr>
<tr><td colspan="11">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.</td></tr>
<tr><td>6</td><td>CVE-2012-6050</td><td>16</td><td>1</td><td>DoS</td><td>2012-11-26</td><td>2017-08-28</td><td>6.4</td><td>None</td><td>Remote</td><td>Low</td></tr>
<tr><td colspan="11">The winbox service in MikroTik RouterOS 5.15 and earlier allows remote attackers to cause a denial of service (CPU consumption), read the router versio download the router's DLLs or plugins, as demonstrated by roteros.dll.</td></tr>
</table>

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™
(An ISO 9001 : 2015 Certified Company)

Tara Consultants Pvt. Ltd.

Most trusted name in fiber Optics.

Tara EPON Products

2 Ports OLT

4 Ports OLT

1GE+WiFi ONU

8 Ports OLT

16 Ports OLT

1GE ONU

Fiber Accessories

FTTH Drop Cable Stripper

Fiber Stripper

Fiber Cutter

Fast Connector

Fiber Adapters

Face Plate TY-GOM-A

Splitter with steel Tube type
1x2/1x4/1x8/1x16/1x32

PLC Splitter Cassette 1x4

PLC Splitter Cassette 1x8

PLC Splitter Cassette 1x16

PLC Splitter Cassette 1x32

Ty-GF14-6J

Ty-GF16-8E

Ty-GF06-16P

Ty-GF21-16P

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

1GE+1FE+1POTS+1CATV+WiFi

GPON PON Module

1GE+1FE+1POTS+WiFi

Tara 1GE GPON ONT

Tara 8 Port GPON OLT

1GE XPON ONU

Switches

N1-9802w

N1-9208W

Tara Reverse PoE
Switch

Tara Reverse PoE Switc
1G input

Edgecore
ECS2110-26T

Edgecore
ECS2100-10T

Edgecore
ECS4120-28F

Edgecore
ECS2100-28T

Edgecore
ECS4120-28FV2

SIP Products
(Session Initiation Protocol)

Video Door Phone
GDS 3710

VOIP Phone
GXP1610/1615

SIP Server
UCM6202/6204

SIP Server
UCM6510

Brands which we deals

TARA FIBER, HUAWEI, NPort, Edge-core NETWORKS, GRANDSTREAM CONNECTING THE WORLD, CISCO, ZTE, MikroTik, UBIQUITI NETWORKS, D-Link Building Networks for People, Tenda, TP-LINK The Reliable Choice

MAKE IN INDIA

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

MUM INDIA 2018

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

tcpl
online