

WELCOME TO MUM INDIA 2016

TARA CONSULTANTS PVT LTD



www.ispmart.com



About Us

We **Tara Consultants Pvt Ltd**, Offer The Best of Latest technological Product, Solutions and Services at the most competitive prices to increase productivity, quality of work conditions in automation and improve the quality of life by offering meaningful, effective and efficient solutions, Gadgets. Gizmos and Life changing Products and pursue with other core activities such as Networking Products, Audio-Visual Product, Imports, Project Consultancy. Timely delivery and High Quality Service are the integral part of TCPL philosophy for ensuring client satisfaction retention and continuation.

Agenda

How to protect ISP network from various Attacks

- Who is ISP
- ISP Layer
- ISP Identified by
- What are Network attacks
- DDoS-DoS
- Port Scanner
- Syn Flooding
- Brute Force Attack
- Smurf Attack
- Blocking Regular Ports
- How to protect with RouterOS
- Live Simulation

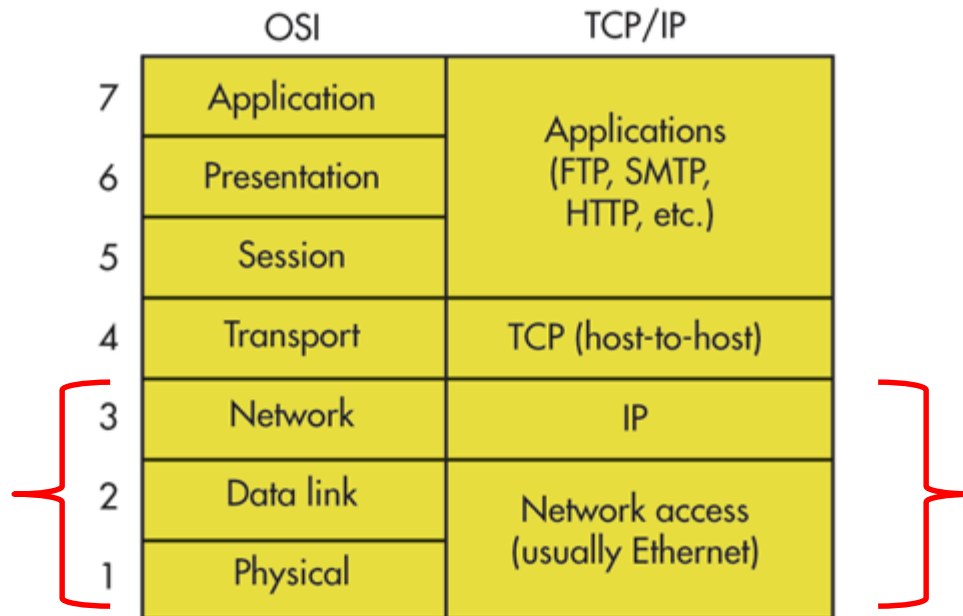


By Vikas Kumar Gupta

Who is ISP ?

Internet Service Provider, who provides access to Internet over Public or Private IP.

ISP Layer



•ISP Identified by

 IP Address Lookup



•What are Network attacks

Network **attack** is any attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset.

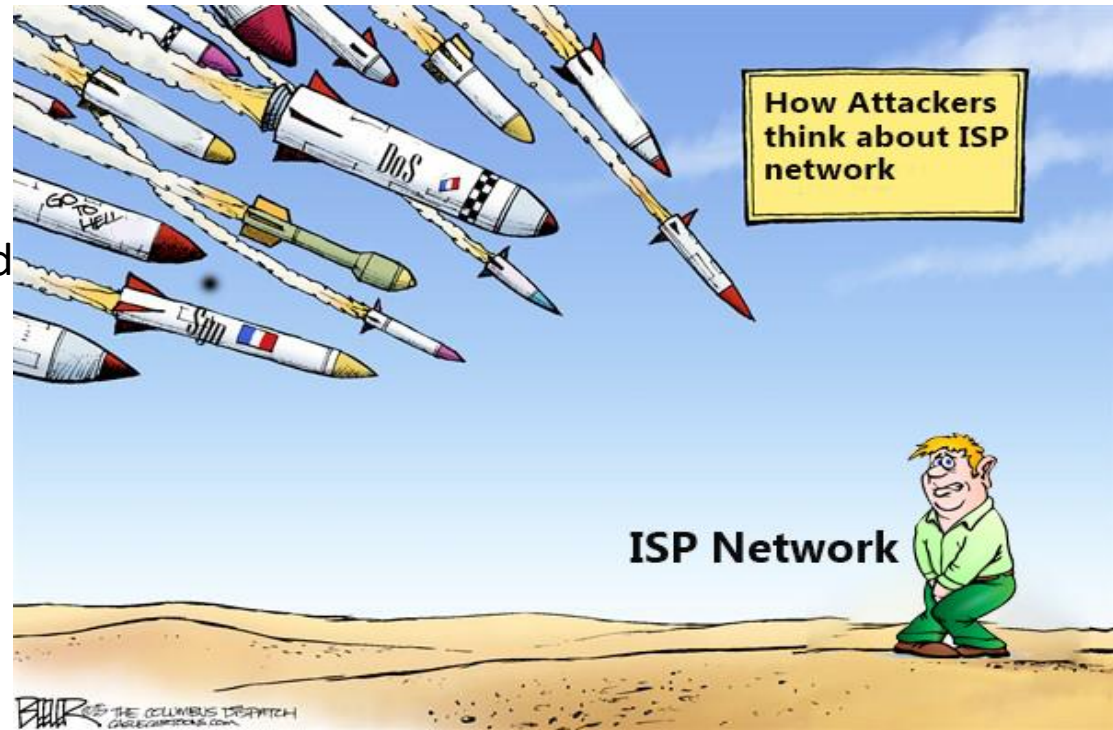
Passive Attacks : Wiretapping, Port Scanning

Active Attacks. Denial-of-service attack, SYN Flooding

Brute Force Attack

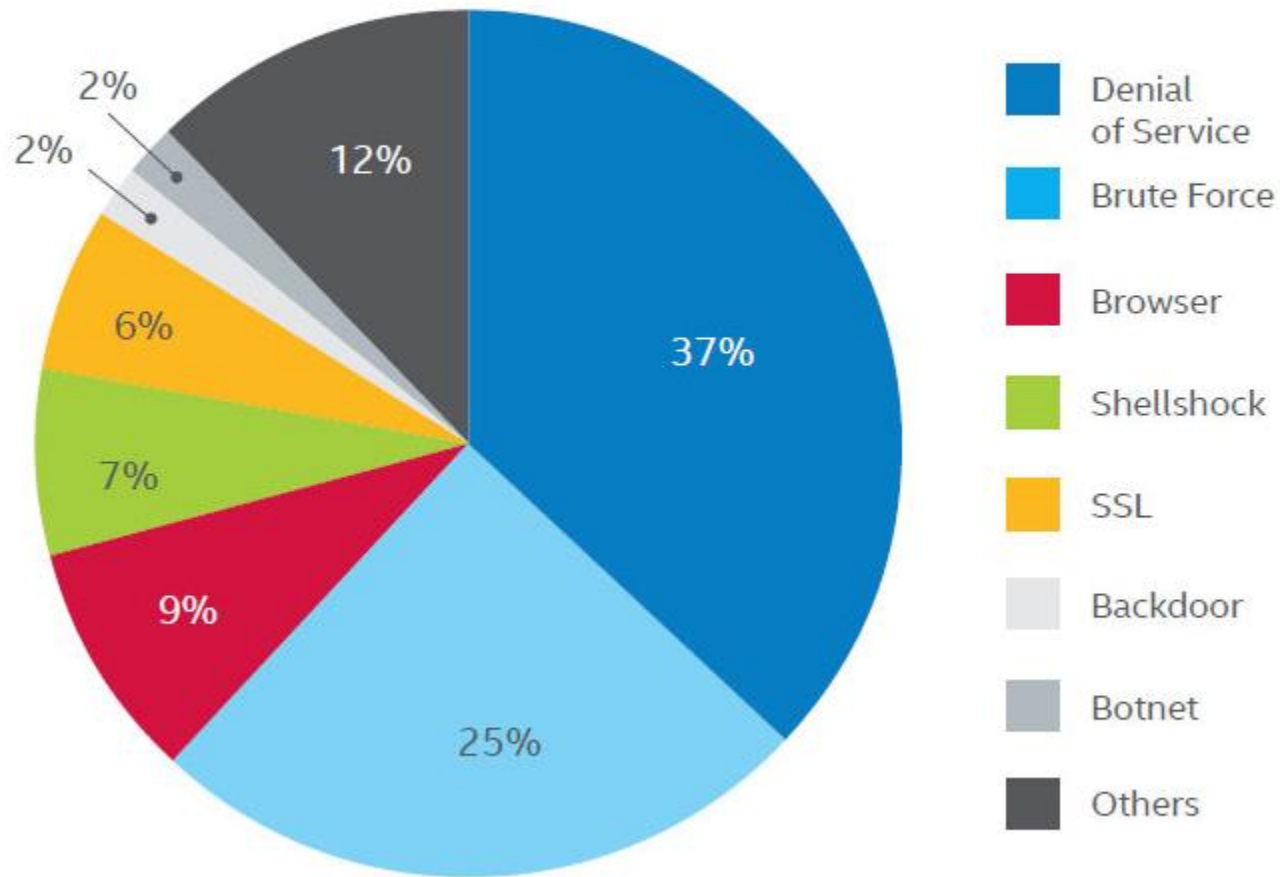
Smurf Attack

As per Survey, 10-30% of Internet Bandwidth get wasted Due to network attacks.



•Case Study on Top Network Attacks

Top Network Attacks



Source: McAfee Labs, 2015.

- **DDoS-Distributed Denial of Service**

- A **distributed denial-of-service (DDoS)** attack occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers/Router.

- **DoS-Denial of Service**

- **Denial-of-service (DoS)** attack is an attempt to make a machine or network resource unavailable to its intended users, such as to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet.

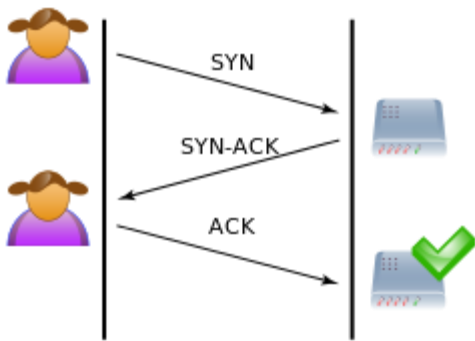


•Port Scanner

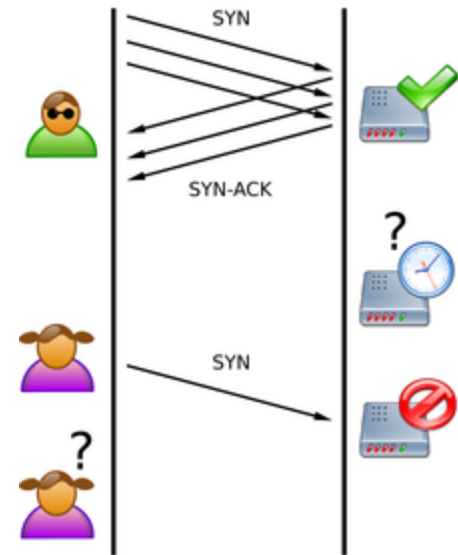
Port scanning is a method of getting list of opened and listening ports, which gives idea to hackers or attackers about vulnerability of network

•Syn Flooding

A **SYN flood** is a form of denial-of-service attack in which an attacker sends a succession of **SYN** requests to a target's system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic.



A normal connection between a user and a server. The three-way handshake is correctly performed



SYN Flood. The attacker sends several packets but does not send the "ACK" back to the server. The connections are hence half-opened and consuming server resources. Neeraj, a legitimate user, tries to connect but the server refuses to open a connection resulting in a denial of service.

•Brute Force Attack

Brute-force attack consists of an attacker trying many passwords or passphrases with the hope of eventually guessing correctly. The attacker systematically checks all possible passwords and passphrases until the correct one is found. Alternatively, the attacker can attempt to guess the key.

•Smurf Attack



The **Smurf Attack** is a distributed denial-of-service **attack** in which large numbers of Internet Control Message Protocol (ICMP) packets with the intended victim's spoofed source IP are broadcast to a computer network using an IP Broadcast address.

Searching Flooding source with Mikrotik

The screenshot shows the Mikrotik WinBox interface. On the left, the 'interface <ether1>' configuration window is open, with the 'Torch' button highlighted by a red arrow. The 'Torch (Running)' window is also open, displaying a list of traffic entries and their statistics.

Torch (Running) - Basic

- Interface: ether1
- Entry Timeout: 00:00:03 s

Collect

- Src. Address
- Dst. Address
- MAC Protocol
- Protocol
- Src. Address6
- Dst. Address6
- Port
- VLAN Id

Filters

- Src. Address: 0.0.0.0/0
- Dst. Address: 0.0.0.0/0
- Src. Address6: ::/0
- Dst. Address6: ::/0
- MAC Protocol: all
- Protocol: any
- Port: any
- VLAN Id: any

| Et... | Prot... | Src. | Dst. | VLAN Id | Tx Rate | Rx Rate | Tx Pack... | Rx Pack... |
|-------------------|---------|-----------------------------|------------------------------|---------|-----------|-----------|------------|------------|
| 800 (ip) 1 (ic... | | 10.0.1.127 | 192.168.85.10 | | 0 bps | 75.7 kbps | 0 | 128 |
| 800 (ip) 6 (tcp) | | 10.0.0.7:1433 (ms-sql-s) | 10.0.1.112:2070 | | 0 bps | 67.7 kbps | 0 | 7 |
| 800 (ip) 1 (ic... | | 10.0.0.77 | 192.168.85.10 | | 0 bps | 37.8 kbps | 0 | 64 |
| 800 (ip) 17 (...) | | 216.58.197.69:443 (https) | 192.168.89.11:57448 | | 10.6 kbps | 29.0 kbps | 5 | 6 |
| 800 (ip) 17 (...) | | 74.125.68.132:443 (https) | 192.168.89.11:59138 | | 15.4 kbps | 23.8 kbps | 3 | 3 |
| 800 (ip) 6 (tcp) | | 74.125.68.132:443 (https) | 192.168.89.11:54083 | | 3.2 kbps | 14.8 kbps | 3 | 4 |
| 800 (ip) 6 (tcp) | | 74.125.68.95:443 (https) | 192.168.89.11:54086 | | 3.6 kbps | 12.8 kbps | 4 | 4 |
| 800 (ip) 6 (tcp) | | 122.252.237.68:443 (https) | 10.0.2.254:3351 | | 0 bps | 11.6 kbps | 0 | 1 |
| 800 (ip) 6 (tcp) | | 74.125.68.95:443 (https) | 192.168.89.11:54082 | | 2.4 kbps | 11.5 kbps | 3 | 3 |
| 800 (ip) 17 (...) | | 216.58.197.78:443 (https) | 192.168.89.11:61845 | | 4.3 kbps | 10.0 kbps | 1 | 2 |
| 806 (...) | | 0.0.0.0 | 0.0.0.0 | | 336 bps | 6.7 kbps | 1 | 14 |
| 800 (ip) 6 (tcp) | | 74.125.68.108:587 | 192.168.89.19:54375 | | 2.5 kbps | 4.9 kbps | 3 | 5 |
| 800 (ip) 6 (tcp) | | 74.125.68.108:587 | 192.168.89.19:54376 | | 2.5 kbps | 4.9 kbps | 3 | 5 |
| 800 (ip) 6 (tcp) | | 216.58.197.78:443 (https) | 192.168.89.11:54084 | | 7.5 kbps | 4.1 kbps | 4 | 4 |
| 800 (ip) 17 (...) | | 192.168.1.1:67 (bootps) | 255.255.255.255:68 (boot... | | 0 bps | 2.1 kbps | 0 | 0 |
| 800 (ip) 6 (tcp) | | 216.58.197.78:443 (https) | 192.168.89.11:54081 | | 512 bps | 2.1 kbps | 1 | 2 |
| 800 (ip) 6 (tcp) | | 74.125.68.108:587 | 192.168.89.19:54378 | | 1008 bps | 1832 bps | 2 | 2 |
| 800 (ip) 17 (...) | | 10.0.2.74:137 (netbios-ns) | 10.255.255.255:137 (netbi... | | 0 bps | 1717 bps | 0 | 2 |
| 800 (ip) 17 (...) | | 10.0.2.125:137 (netbios-ns) | 10.255.255.255:137 (netbi... | | 0 bps | 1472 bps | 0 | 2 |
| 800 (ip) 17 (...) | | 0.0.0.0:68 (bootpc) | 255.255.255.255:67 (boot... | | 0 bps | 1424 bps | 0 | 0 |
| 800 (ip) 17 (...) | | 10.0.0.6:67 (bootps) | 255.255.255.255:68 (boot... | | 0 bps | 1368 bps | 0 | 0 |
| 800 (ip) 17 (...) | | 10.0.0.65:38849 | 239.255.255.250:1900 | | 0 bps | 1336 bps | 0 | 1 |
| 800 (ip) 17 (...) | | 10.0.1.37:137 (netbios-ns) | 10.255.255.255:137 (netbi... | | 0 bps | 1226 bps | 0 | 1 |
| 800 (ip) 17 (...) | | 10.0.1.104:137 (netbios-ns) | 10.255.255.255:137 (netbi... | | 0 bps | 1226 bps | 0 | 1 |
| 800 (ip) 17 (...) | | 10.0.2.74:55671 | 239.255.255.250:1900 | | 0 bps | 1152 bps | 0 | 0 |
| 800 (ip) 17 (...) | | 10.0.2.112:137 (netbios-ns) | 10.255.255.255:137 (netbi... | | 0 bps | 981 bps | 0 | 1 |

Summary: 122 items, Total Tx: 170.4 kbps, Total Rx: 375.8 kbps, Total Tx Packet: 226, Total Rx Packet: 293

How to protect from Attacks with RouterOS

•Blocking Vulnerable Ports

| Protocol | Port Number | Protocol | Port Number |
|------------|----------------------|-------------|-----------------------------|
| Both | 7(Echo, WOL) | TCP | 2869(uPnP) |
| Both | 9(Discard) | UDP | 4500(IPSEC) |
| Both | 13(Daytime) | Both | 389(LDAP) |
| Both | 17(Skun trojan) | Both | 445(Virus, Mail) |
| Both | 19(CGP) | UDP | 500(IKE) |
| TCP | 113(Authentication) | UDP | 520(RIP, Backdoor) |
| UDP | 123(NTP) | TCP | 1002(Net Meeting) |
| TCP | 135(RPC, Virus) | TCP | 1024-1030(Virus and Others) |
| Both | 137(Net Bios) | TCP | 1433(Virus, SQL) |
| Both | 138(Net Bios, Virus) | TCP | 1444(Threats) |
| TCP | 139(Net Bios, Virus) | TCP | 25(SMTP) |
| UDP | 1701(L2tP) | UDP | 53(DNS) |
| TCP | 1720(H323) | Both | 8080(Webproxy) |
| TCP | 1723(PPtP) | UDP | 80(DDOS) |

Source : https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers
<http://www.speedguide.net/>

Note : These ports are not meant to threats everytime, but sometimes.

- **Blocking ports with RouterOS**

```
/ip firewall filter
```

```
add action=drop chain=input dst-port=111 protocol=tcp in-interface=<LAN/WAN>  
add action=drop chain=input dst-port=119 protocol=udp in-interface=<LAN/WAN>
```

```
/ip firewall raw
```

```
add action=drop chain=prerouting dst-port=111 protocol=tcp in-interface=<LAN/WAN>  
add action=drop chain=prerouting dst-port=119 protocol=udp in-interface=<LAN/WAN>
```

Mikrotik Filters vs RAW(New Package)

| Filters | Raw |
|---------------------------|--------------------------|
| Input/Output/Forward | Prerouting/Output |
| Data flow to, from | Entering, Originated |
| Conntrack, Higher CPU | No Conntrack, Lesser CPU |
| L7 Matcher | No L7 Matcher |
| Connection Type Definable | NA |
| NA | DOS attack mitigation. |

•Saving from Attack

SSH Brute Force Attack

```
/ip firewall Filter
add action=drop chain=input comment="Drop SSH brute forcers" dst-port=22
  protocol=tcp src-address-list=ssh_blacklist
add action=add-src-to-address-list address-list=ssh_blacklist \
  address-list-timeout=1w3d chain=input connection-state=new dst-port=22 \
  protocol=tcp src-address-list=ssh_stage3
add action=add-src-to-address-list address-list=ssh_stage3 \
  address-list-timeout=1m chain=input connection-state=new dst-port=22 \
  protocol=tcp src-address-list=ssh_stage2
add action=add-src-to-address-list address-list=ssh_stage2 \
  address-list-timeout=1m chain=input connection-state=new dst-port=22 \
  protocol=tcp src-address-list=ssh_stage1
add action=add-src-to-address-list address-list=ssh_stage1 \
  address-list-timeout=1m chain=input connection-state=new dst-port=22 \
  protocol=tcp
```

Source : <http://wiki.mikrotik.com/wiki/Manual:IP/Firewall/Filter>

Syn Flooding/ ICMP Attack

/ip firewall Filter

```
add chain=icmp comment="Limited Ping Flood" icmp-options=0 limit=5,5 \  
    protocol=icmp  
add chain=icmp icmp-options=3:3 limit=5,5 protocol=icmp  
add chain=icmp icmp-options=3:4 limit=5,5 protocol=icmp  
add chain=icmp icmp-options=8 limit=5,5 protocol=icmp  
add chain=icmp icmp-options=11 limit=5,5 protocol=icmp  
add action=drop chain=icmp protocol=icmp
```


Stopping Port Scanner

/ip firewall Filter

```
add action=add-src-to-address-list address-list="port scanners" \  
    address-list-timeout=2w chain=input comment="Port Scanners to list" \  
    protocol=tcp psd=21,3s,3,1  
add action=add-src-to-address-list address-list="port scanners" \  
    address-list-timeout=2w chain=input protocol=tcp tcp-flags=\  
    fin,!syn,!rst,!psh,!ack,!urg  
add action=add-src-to-address-list address-list="port scanners" \  
    address-list-timeout=2w chain=input protocol=tcp tcp-flags=fin,syn  
add action=add-src-to-address-list address-list="port scanners" \  
    address-list-timeout=2w chain=input protocol=tcp tcp-flags=syn,rst  
add action=add-src-to-address-list address-list="port scanners" \  
    address-list-timeout=2w chain=input protocol=tcp tcp-flags=\br/>    fin,psh,urg,!syn,!rst,!ack  
add action=add-src-to-address-list address-list="port scanners" \  
    address-list-timeout=2w chain=input protocol=tcp tcp-flags=\br/>    fin,syn,rst,psh,ack,urg  
add action=add-src-to-address-list address-list="port scanners" \  
    address-list-timeout=2w chain=input protocol=tcp tcp-flags=\br/>    !fin,!syn,!rst,!psh,!ack,!urg  
add action=drop chain=input src-address-list="port scanners"
```

DDoS Attack

/ip firewall Filter

```
add action=add-src-to-address-list address-list=blocked-addr \  
    address-list-timeout=1d chain=input connection-limit=100,32 protocol=tcp \  
add action=tarpit chain=input connection-limit=3,32 protocol=tcp \  
    src-address-list=blocked-addr \  
add action=jump chain=forward connection-state=new jump-target=detect-ddos \  
add action=return chain=detect-ddos dst-limit=32,32,src-and-dst-addresses/10s \  
add action=add-dst-to-address-list address-list=ddosed address-list-timeout=\  
    1d chain=detect-ddos \  
add action=add-src-to-address-list address-list=ddoser address-list-timeout=\  
    1d10m chain=detect-ddos \  
add action=drop chain=forward connection-state=new dst-address-list=ddosed \  
    src-address-list=ddoser
```

Block Bogon IPs

```
/ip firewall filter
```

```
add action=drop chain=forward comment="Block Bogus IP Address" src-address=\
  0.0.0.0/8
```

```
add action=drop chain=forward dst-address=0.0.0.0/8
```

```
add action=drop chain=forward src-address=127.0.0.0/8
```

```
add action=drop chain=forward dst-address=127.0.0.0/8
```

```
add action=drop chain=forward src-address=224.0.0.0/3
```

```
add action=drop chain=forward dst-address=224.0.0.0/3
```

Questions ?

GPON ONU module

Product specifications

Details

- Product code SFPONU
- Data Rate 1244Mb/s downstream and 2488Mb/s upstream
- Connector Small form factor pluggable, simplex SC
- Format MSA SFP



EPON OLT

- Chassis based OLT (Expandable -12 Port)
- GEAPON OLT slots with 1: 64 splitting ratio at most
- Support 256 ONU maximally
- Maximum Transmission distance: 20 km
- Suitable for small FTTX networking access
- Full gigabit link speed forward
- 4 uplink SFP ports



EPON ONT (SFU)

- 1 G
- Receiver Wavelength:- 1490nm
- Receiving Sensitivity:- $< -25\text{dBm}$
- Working Temperature:- $-20\sim+60$



ONU

- Fiber Port:- 1 EPON Interface, SC single-mode
- single-fiber, Downstream rate 1.25Gbps,
- Upstream rate 1.25Gbps
- Wavelength:- Tx 1310 nm, Rx 1490 nm
- Fiber Interface:- SC/PC



Thank You for Listening 😊

TARA CONSULTANTS PVT LTD

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

[TEL: 011-46570273](tel:011-46570273)

Ph : +91-9311686026, +91-9811686026

FAX:011-26448917

www.tcplonline.com

www.ispmart.com

