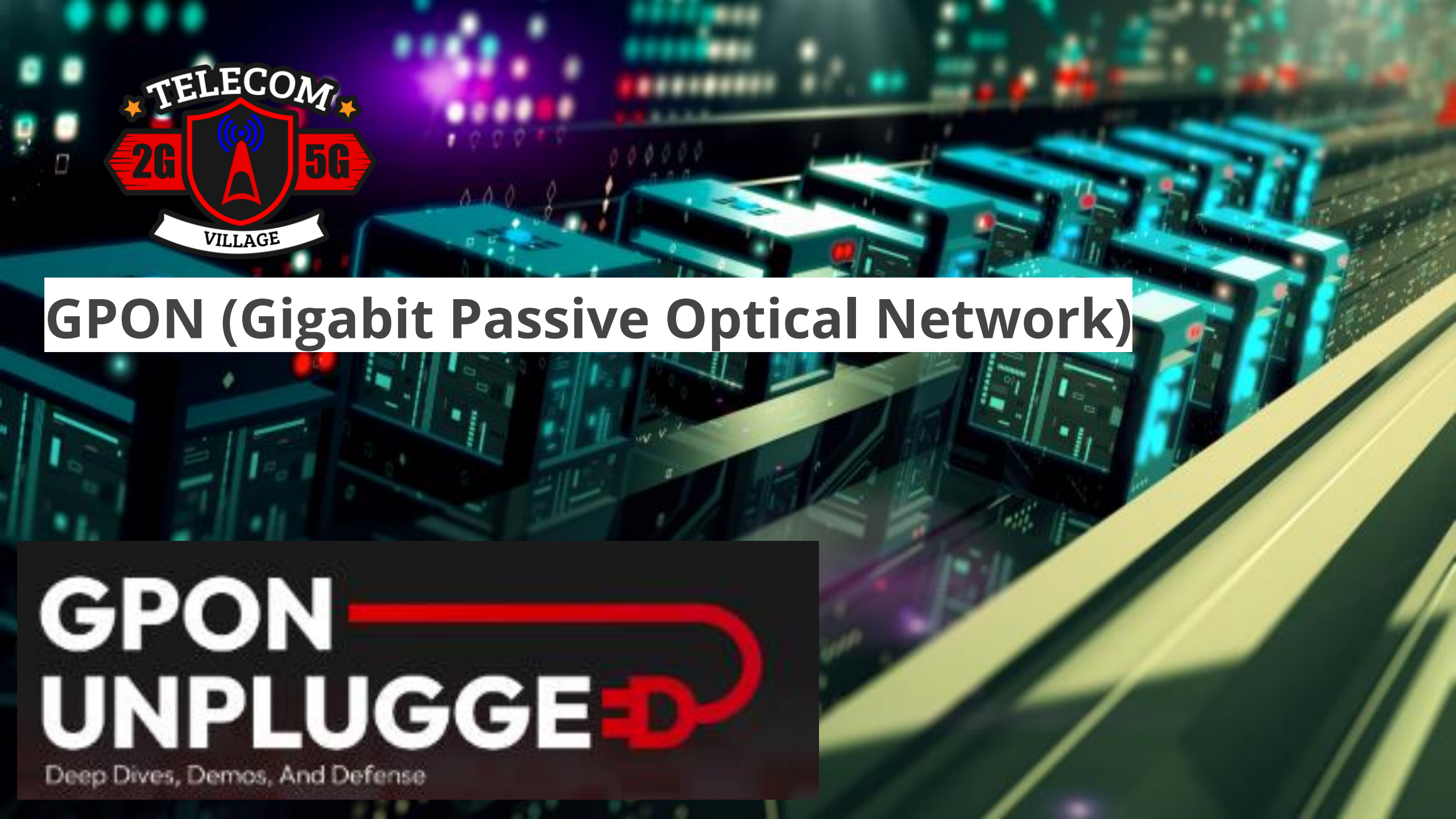
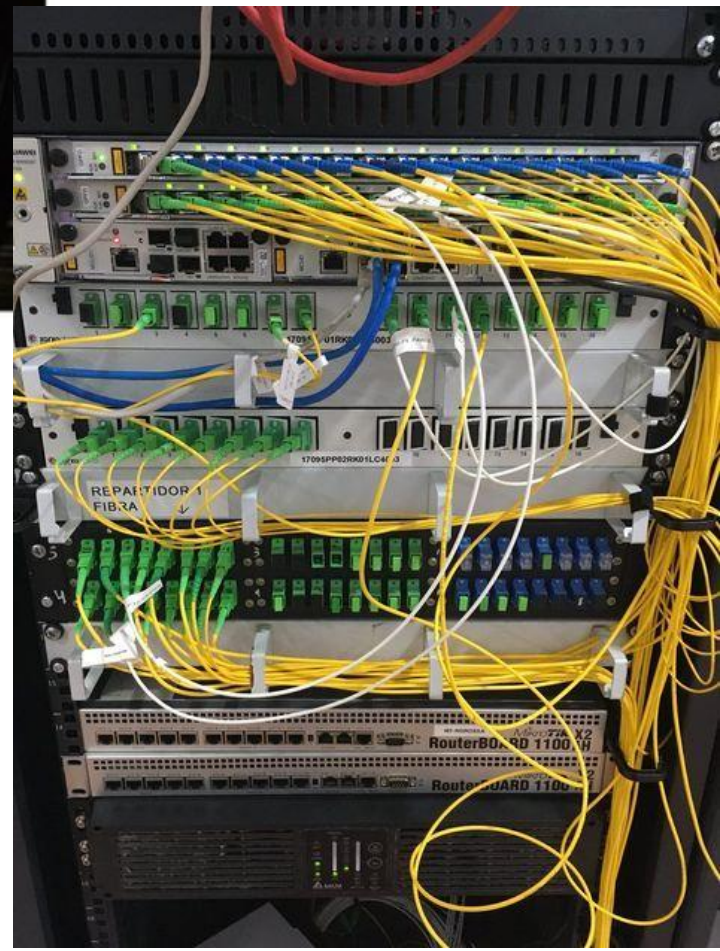


GPON (Gigabit Passive Optical Network)

Content

- Fundamental
- Introduction of GPONS
- Component of GPON
- Encryption
- Breaking Telecom network into part
- Telecom Threat Modeling

GPON (Gigabit Passive Optical Network)



FTTX- Fiber to X

Fiber to the Home or simply FTTH is a technology that uses optical fiber directly from the central point to the residential premises FTTx (fiber to the x) is a collective term that is used to describe various types of broadband network architectures. The “x” stands for a particular object. It could be a home, a cabinet or any end-user premise. As a result,

- **Fiber to the Home (FTTH),**
- **Fiber to the Building (FTTB),**
- **Fiber to the Premises (FTTP)**
- **Fiber to the Curb (FTTC).**

FTTx has many benefits related to speed and capacity. Other advantages include higher transmission rates and lower energy consumption. FTTx network takes fiber closer to the end-user, which helps in leveraging the latest construction, connection and transmission techniques.

The two typical technologies used in this method are Ethernet Passive Optical Network (EPON) & Gigabit-capable Passive Optical Networks (GPON).

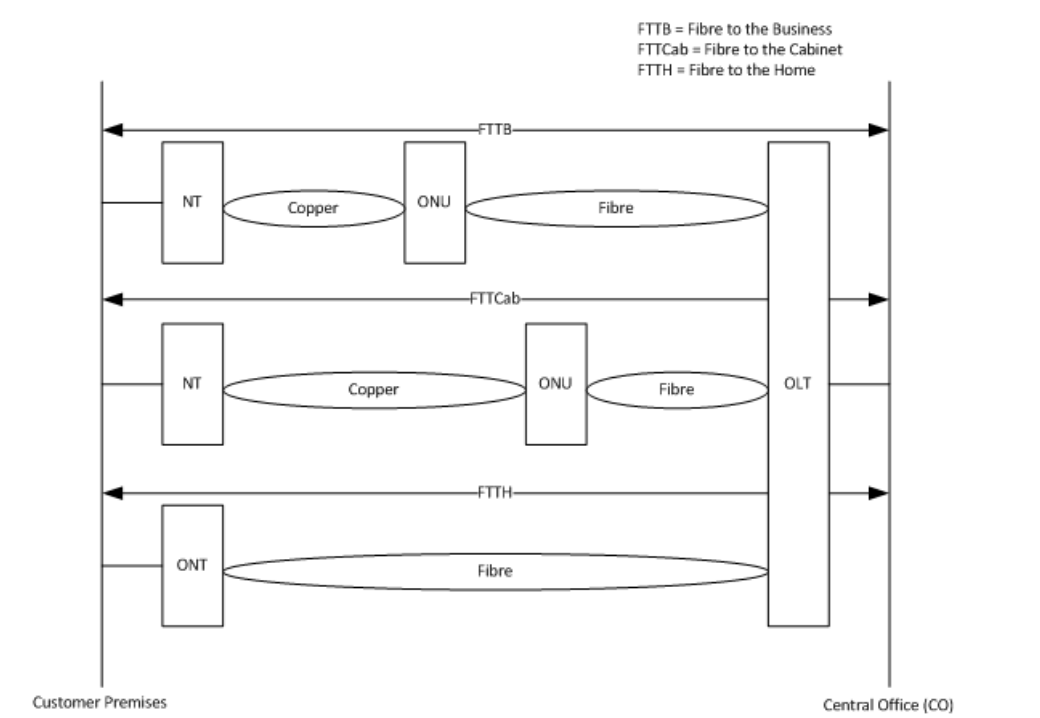
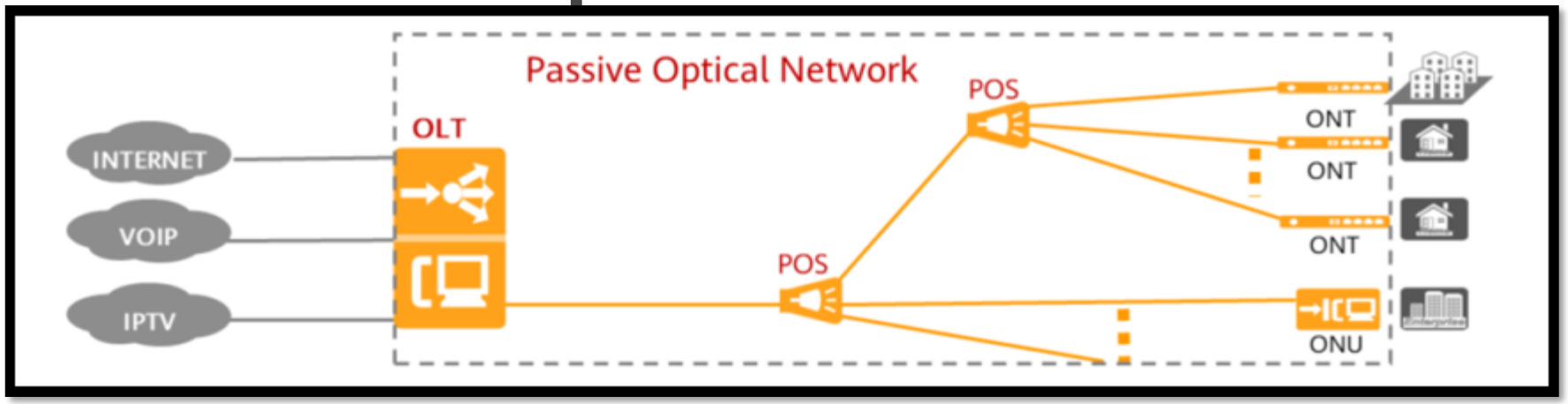


Figure 1. FTTx Network Architecture

Terminology

- **Gigabit-capable Passive Optical Network (GPON**) - Standard for passive optical networks (PON) published by the ITU-T.
- **Optical Distribution Network (ODN)** - The physical fibre and optical devices that distribute signals to users in a telecommunications network. The ODN is composed of passive optical components (POS), such as optical fibers, and one or more passive optical splitters.
- **Optical Network Termination (ONT) /Optical Network Units (ONU)** - Connects end-user devices (desktop, phones, and so on) into the GPON network. Provides the optical to electrical signal conversion. ONTs also provide AES encryption via ONT key.
- **Splitters** - Used to aggregate or multiplex fiber optic signals to a single upstream fiber optical cable. Usually 1:32 ratio.
- **Optical Line Terminal (OLT)** - Device that aggregates all optical signals from ONTs into a single multiplexed beam of light which is then converted into an electrical signal, formatted to Ethernet packet type standards for Layer 2 or Layer 3 forwarding.
- **Wavelength-Division Multiplexing (WDM)** - Wavelength-division multiplexing (WDM) is a technology that multiplexes a number of optical carrier signals onto a single optical fiber that uses different wavelengths (that is, colors) of laser light.
- **GEM GPON encapsulation method (GEM)** - A data frame transport scheme used in gigabit capable passive optical network (GPON) systems that is connection-oriented and that supports fragmentation of the user data frames into variable-sized transmission fragments
- **Fiber to the X (FTTX)** - FTTX is a generalization for several configurations of fiber deployment, arranged into two groups: FTTP/FTTH/FTTB (Fiber laid all the way to the premises/home/building) and FTTC/N (fiber laid to the cabinet/node, with copper wires to complete the connection).
- **T-CONT/TCONT** - Transmission Container
- **OMCC** - Optical Network Unit Management and Control Channel
- **OMCI** - Optical Network Unit Management and Control Interface
- **PCBd** - Physical Control Block downstream
- **TDM** - Time Division Multiplexing
- **TDMA** - Time Division Multiple Access

PON - Passive Optical Network



- PON: a point-to-multipoint (P2MP) passive optical network : A PON consists of an optical line terminal (OLT), an optical network unit/ optic al network Terminal (ONU/ONT), and an optical distribution network (ODN). An optical distribution network (ODN) consists of a passive optical splitt er (POS) and optical fibers.

- GPON: Gigabit-Capable Passive Optical Network : GPON is a leading standard of Passive Optical Network (PON) – a type of point-to-multipoin t network technology that delivers broadband access to the end user via fiber optic cable. Gigabit' in GPON denotes the maximum speed it provides which is typically 2.488 Gbps downstream and 1.244 Gbps upstream. GPOn use Active and passive components

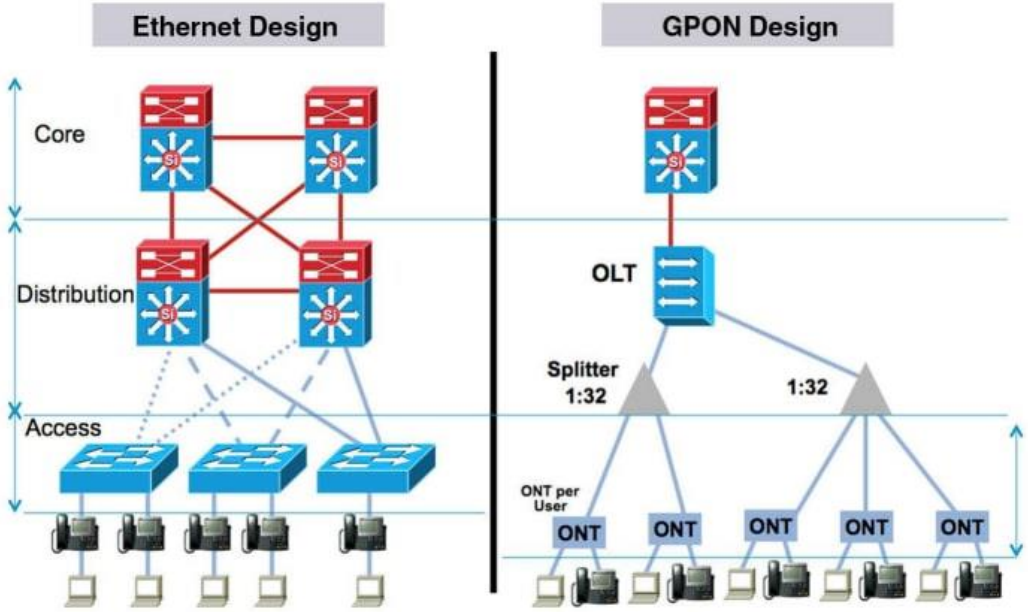
  - GPON use for 3 play service
  - Use VLAN base network for separating 3 play service
  - Downstream encrypted with AES
  - GPON evolution: same Infrastructure can support new standards such:

    XG-PON(10Gbps-2.5Gbps), XGS-PON, TWDM-PON (10Gbps-10Gbps)

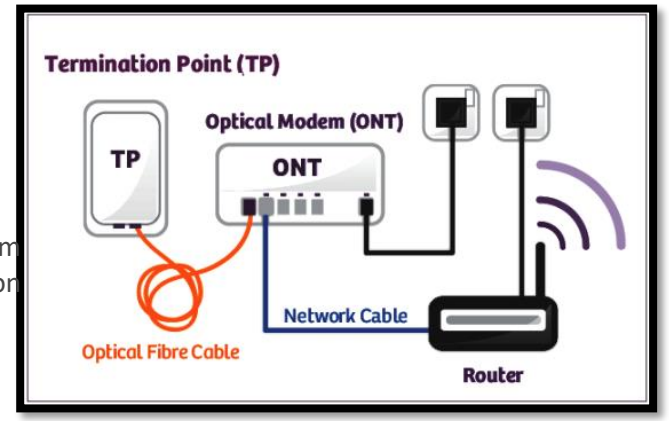
– 2.48 Gbps downstream (1490 nm)
– 1.24 Gbps upstream (1310 nm)
– Serve Remote Bldgs Up to 20Km

- GPON adopts Wavelength Division Multiplexing (WDM) technology, facilitating bi-directional communication over a single fiber.
- To separate upstream/downstream signals of multiple users over a single fibre, GPON adopts two multiplexing mechanism:
  - In downstream direction, data packets are transmitted in a broadcast manner;
  - In upstream direction, data packets are transmitted in a TDMA manner

- **EPON** technology, which is similar to GPON, but uses Ethernet protocols instead of GEM. It provides lower latency and higher data rates than GPON, but has a limited maximum distance of 20 km;
- **XGPON** technology which is same as GPON, but offers higher data rate and is capable to deliver 10G symmetrical data rate (downstream and upstream);
- **BPON (Broadband PON)** is commonly offered at 622 Mbps downstream and 155 Mbps upstream. Its ATM structure and bandwidth limits make it less than ideal for video. Development has stopped on BPON. BPON networks will over time be converted to EPON or GPON. There are approximately 2 million BPON users worldwide..
- **APON (ATM Passive Optical Network)** first Passive optical network standard. It was used for business applications, and based on ATM.
- **GE-PON (Gigabit Ethernet PON)** has a higher installed volume than all other PON technologies combined. EPON is found widely in Asia.



GPON adopts two signal multiplexing mechanisms – for downstream and upstream separate technology. In downstream direction (i.e. from Optical Line Terminal to the users), data packets are transmitted in an broadcast manner, with AES encryption to prevent eavesdropping or adjacent channels. But in the upstream direction (i.e. from users to OLT), data packets are transmitted in a TDMA manner.



Components of GPON

Optical Line Terminal

The OLT can be termed as the network manager of the Gigabit Passive Optical Network. Its role is to send and receive video, data and voice optical signals to and from the ONT at the receiver's end. OLT sends downstream optical signals at 1550 nm for video and 1490 nm for voice and data, whereas it receives upstream optical signals at 1310 nm. This prevents interference. The ***GPON OLT*** is present at the service provider's end, i.e., typically at a data center. Similar to a GPON ONT, OLT also converts received optical signals into electrical signals. It is connected to the ***optical splitter*** via backbone cabling.

Optical Fiber Splitter

The optical fiber splitter is a passive component that enables a single ***fiber optic*** cable to be split into multiple single strands of optic fiber that branch out and connect to individual ***Optical Network Terminals*** at end user premises. A GPON splitter often has a specified split ratio that could be 1:64, 1:32, 1:16, 1:8, 1:4, depending upon the number of outputs required. Such a splitter can be used for centralized splitting where the signals are split to, say, 64 end users, or for cascade splitting where the splitter is connected to other splitters down the line for a more branched out network.

Optical Network Terminal

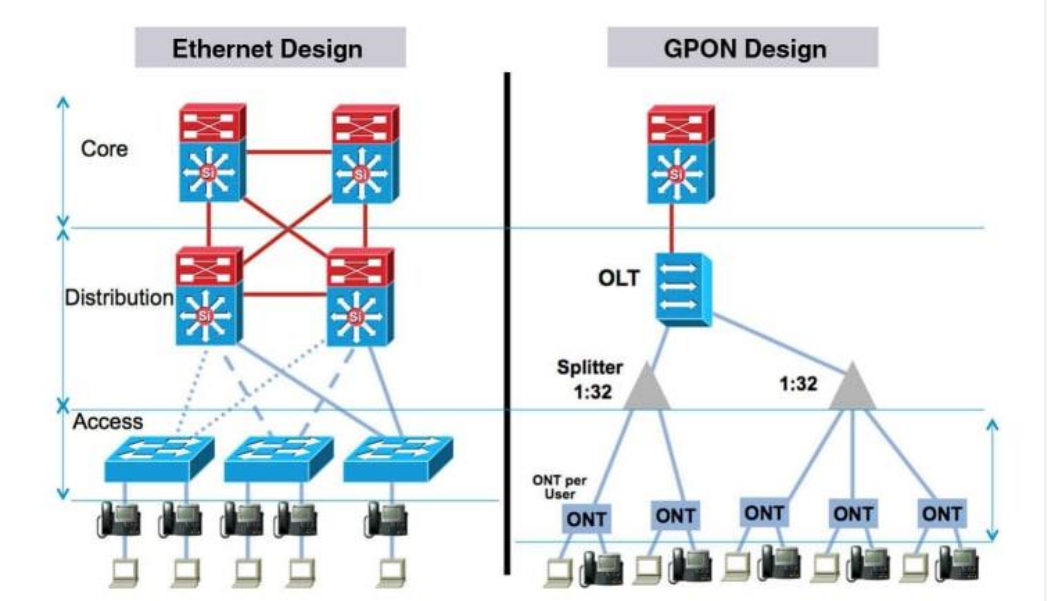
The user end-point of GPON is the ONT, i.e., the Optical Network Terminal. It is a specialised modem for converting optical signals into electrical signals at the premises of the end-user. Thus, it enables broadband access for equipment like WiFi, TVs, desktops, etc. An ONT also sends aggregated and optimised data from the end user back to the OLT.

Transmitting Media

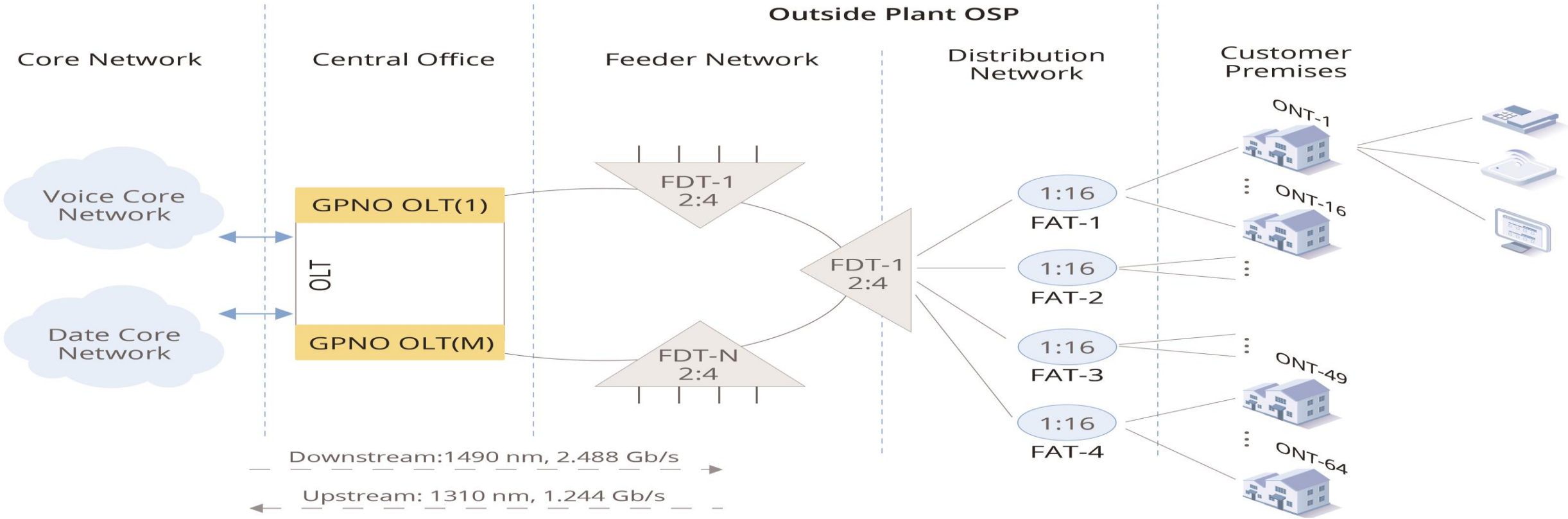
The transmitting media consists of the physical, passive hardware in the form of cabling and various components that is used along the GPON infrastructure. This includes copper cables, patch cords for fiber optics, splitters, adapter panels, connectors, etc. Transmitting media plays a huge role in determining and optimising optical signal loss adequately.

MUX and **DEMUX**

The service **MUX** and **DEMUX** function connects the Customer devices to PON side. The Optical Network Terminal (ONT) is designed for single subscriber use, while the ONU (Optical Networking Unit) is designed for multiple subscriber use. The splitters allow the PON to be shared by up to 128 ONTs or ONUs.



GPON	XG-GPON	XGS-PON	NG-PON2
Downstream	Downstream	Downstream	Downstream
2,5 Gbit/s	10 Gbit/s	10 Gbit/s	40 Gbit/s
Upstream	Upstream	Upstream	Upstream
1,25 Gbit/s	2,5 Gbit/s	10 Gbit/s	10 Gbit/s



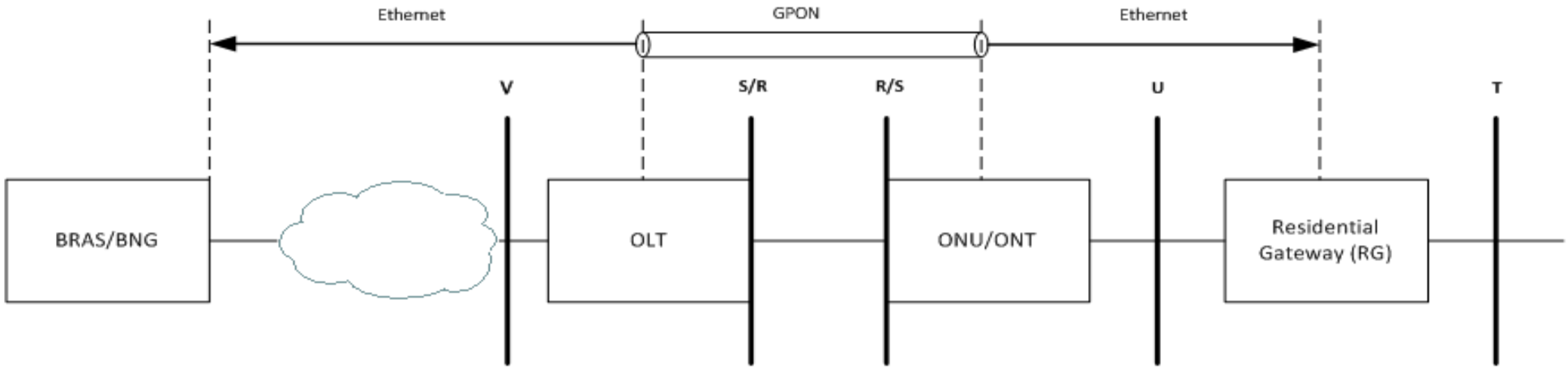
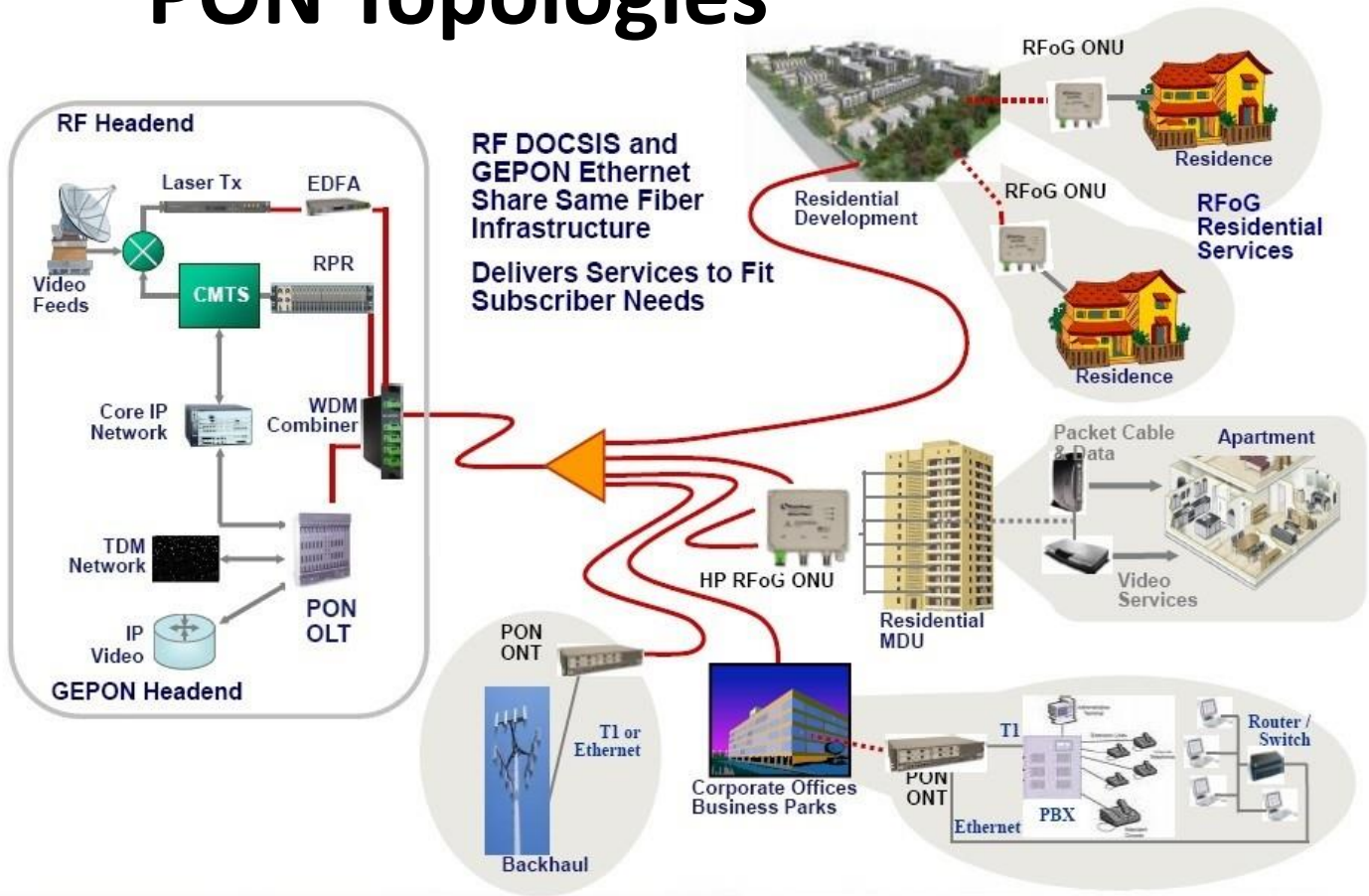
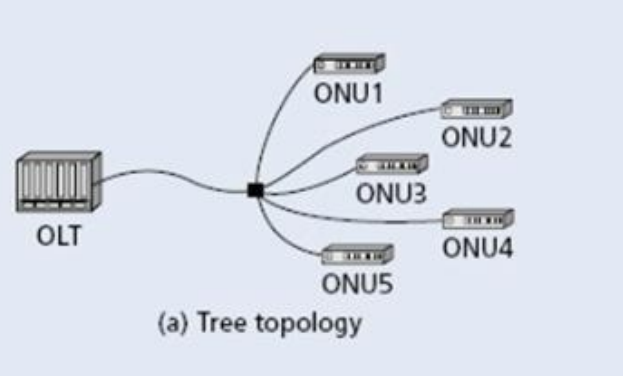


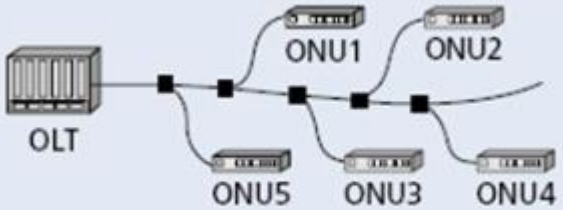
Figure 1. GPON to Ethernet Adaptation

PON Topologies

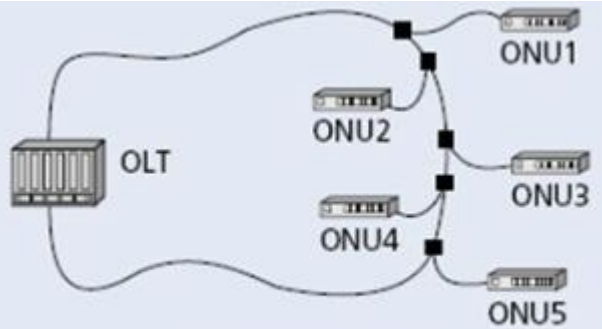




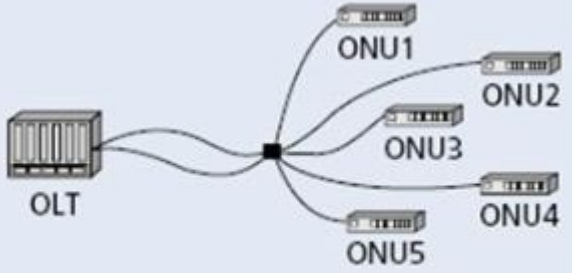
(a) Tree topology



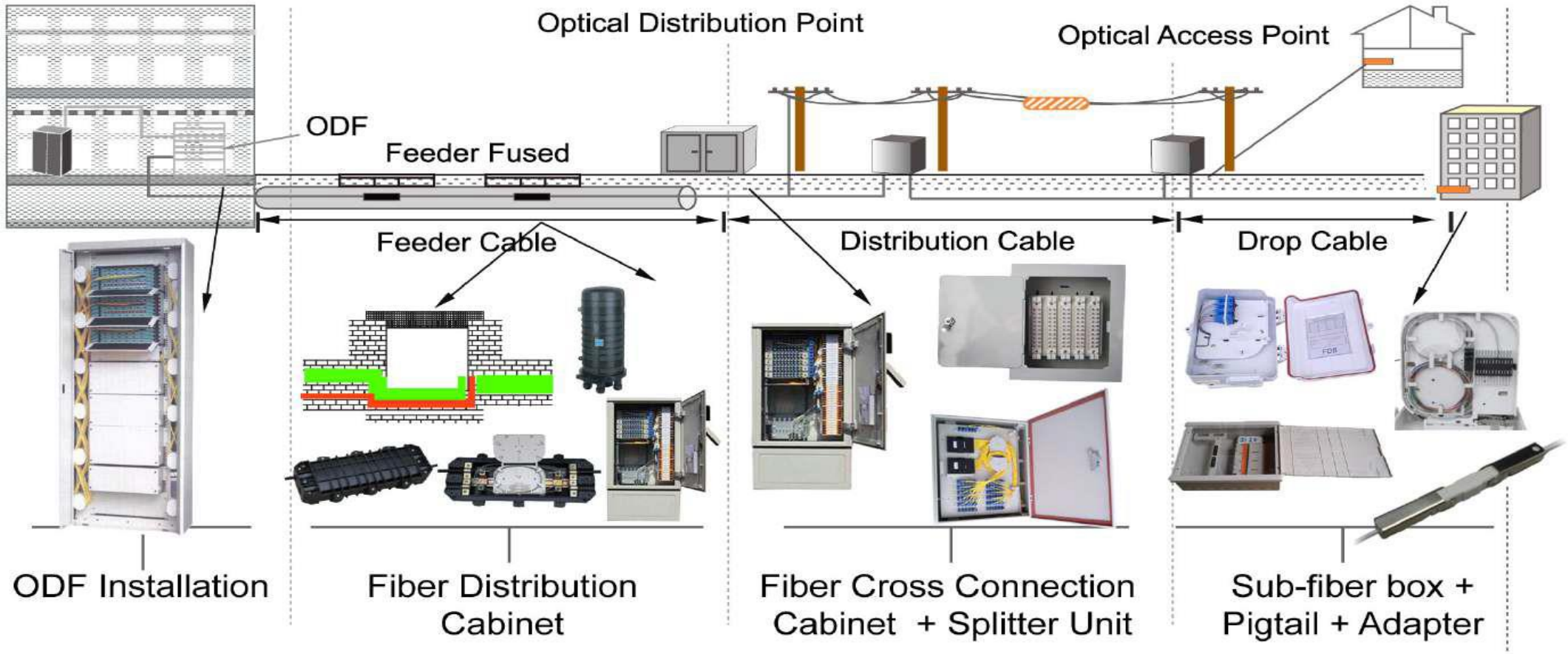
(b) Bus topology



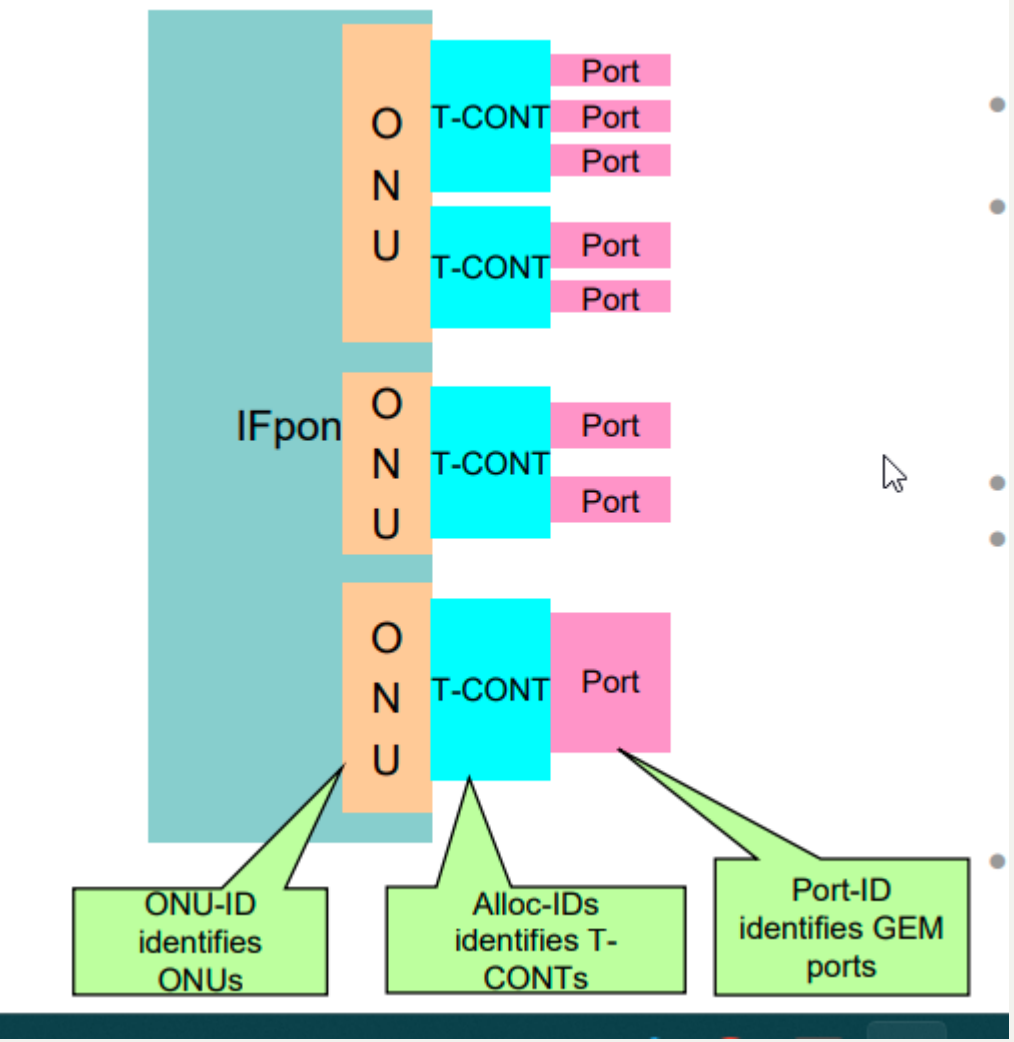
(c) Ring topology



(d) Tree with redundant trunk



Architecture of Optical Access Network



GPON Encapsulation Method (GEM) :It is the data transport scheme in the specified GPON transmission convergence layer. GEM provides a connection-oriented, variable-length framing mechanism for transport of data services over the passive optical network (PON). GEM is designed to be independent of the type of the service node interface at the OLT as well as the types of UNI interfaces at the ONUs.

T-CONT: Transmission Containers is a kind of buffer that carries services. It is mainly used to transmit upstream data units. T-CONT is introduced to realize the dynamic bandwidth assignment of the upstream bandwidth, so as to enhance the utilization of the line

IF pon: GPON interface. Based on the mapping scheme, service traffic is carried to different GEM ports and then to different T-CONTs.

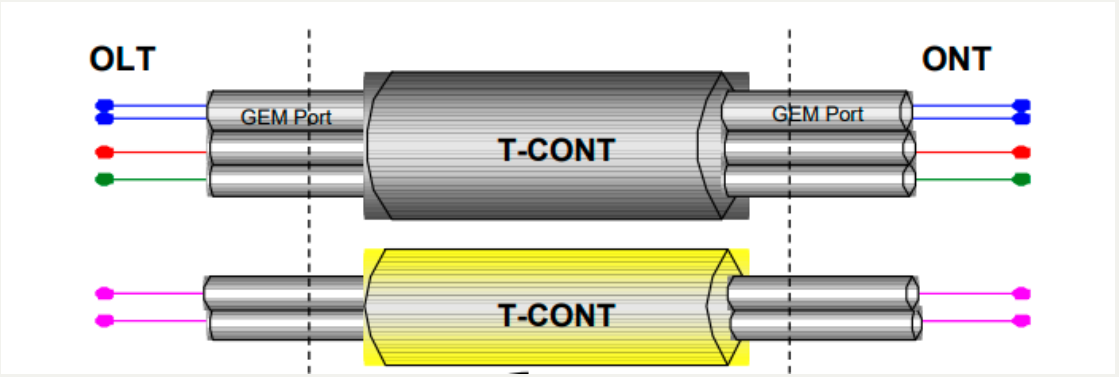
Each GEM Port is identified by a port ID uniquely. The Port ID ranges from 0 to 4095. It is allocated by the OLT i.e a GEM port can only be used by a single ONU/ONT per PON interface on the OLT.

Each T-CONT is identified by the ALLOC_ID uniquely. The ALLOC_ID ranges from 0 to 4095. It is allocated by OLT i.e. a T-CONT can only be used by one ONU/ONT per PON interface on the OLT.

There are 2 types of GEM Channels:

- Downstream-only GEM Channels - These channels are used to transmit downstream broadcast/multicast traffic from OLT to all ONTs. The ONTs identify traffic meant for them based on GEM Port ID.

- Bi-directional GEM Channels - These channels are used for upstream and downstream traffic between the OLT and the ONT. The frames are transmitted from the OLT into the GPON interface and are forwarded only on the U interface of the ONT on which that GEM Port has been assigned.

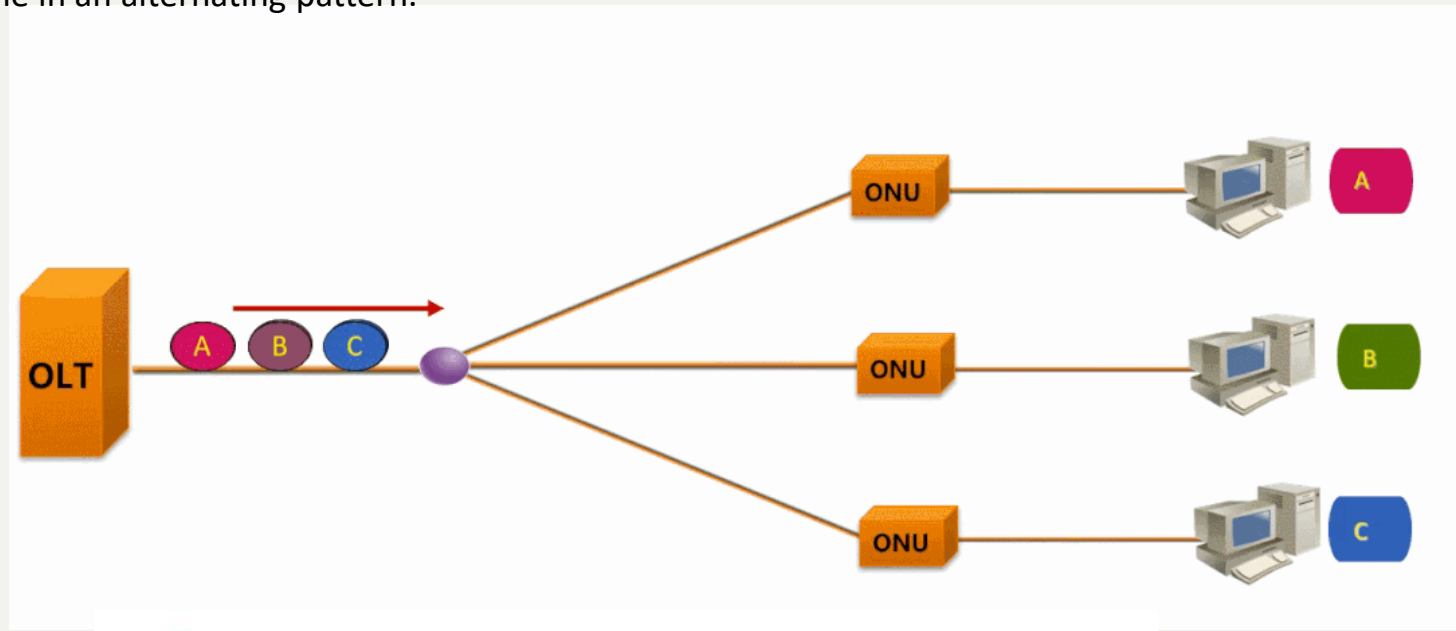


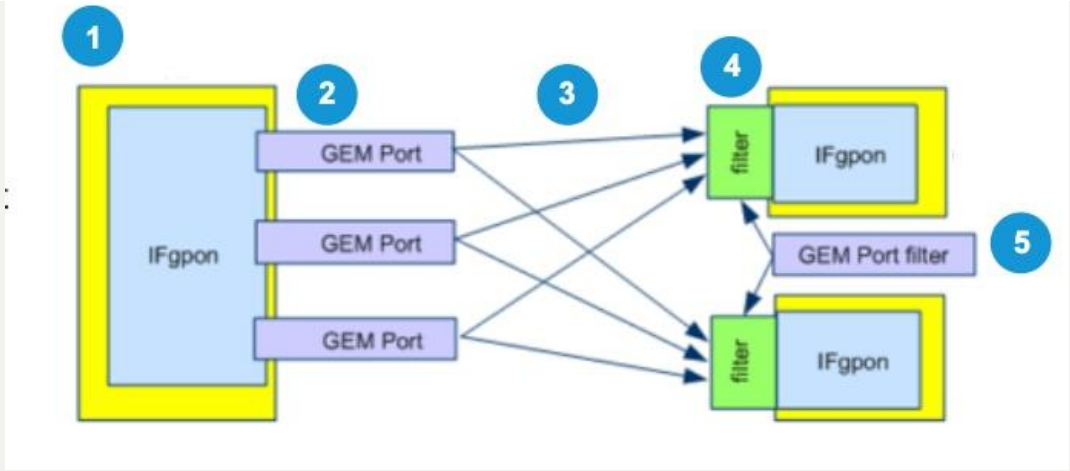
Data Multiplexing

Packet Walk in GPON

Downstream Packet Walk

Time Division Multiplexing (TDM) for downstream – It is a technique of transmitting and receiving separate signals over a common signal path. For this, it uses synchronized switches at each end of the transmission line; resultantly, each signal appears on the line only a fraction of time in an alternating pattern.



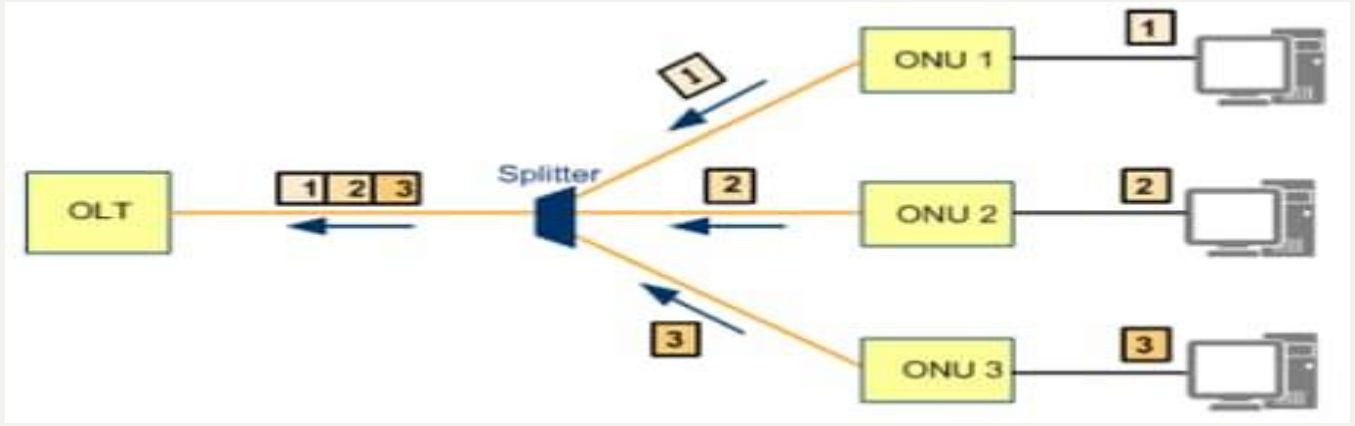


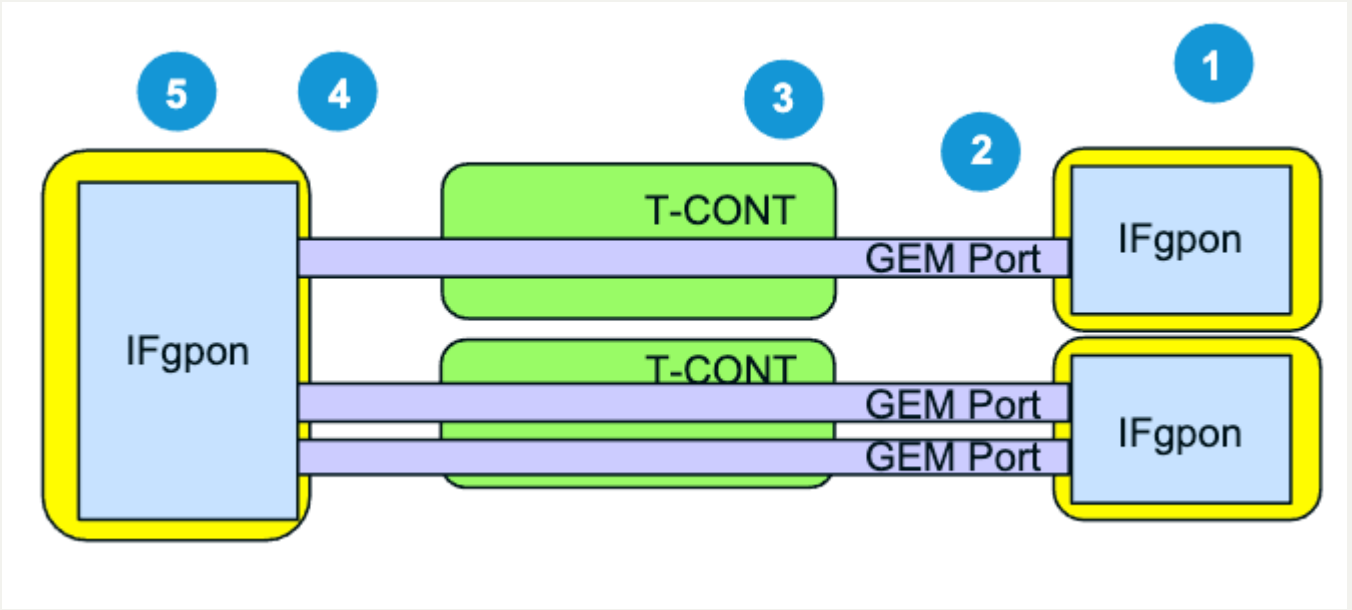
- Downstream packets are forwarded as broadcasts, with the same data sent to all the same ONU/ONT with different data identified by the GEM port ID.
- Downstream continuous mode operation - Even where there is no user traffic passed through GPON, there is a constant signal, except when the laser is administratively turned off.
- OLT sends Ethernet frames from Uplink ports to the GPON service processing module based on configured rules to the PON ports.
- GPON service processing module then encapsulates the Ethernet frames into GEM port data packets for downstream transmission.
- GPON transmission convergence (GTC) frames that contain GEM PDUs are broadcast to all ONT/ONUs connected to the GPON port.
- ONT/ONU filters the received data based on the GEM port ID contained in the GEM PDU header and retains the data only significant to the GEM ports on this ONT/ONU.
- ONT decapsulates the data and sends the Ethernet frames to the end users via service ports.

Packet Walk in GPON

Up stream Packet Walk

Time Division Multiple Access () for upstream – This technique facilitates many users to share the same frequency channel by dividing the signal into different time slots.

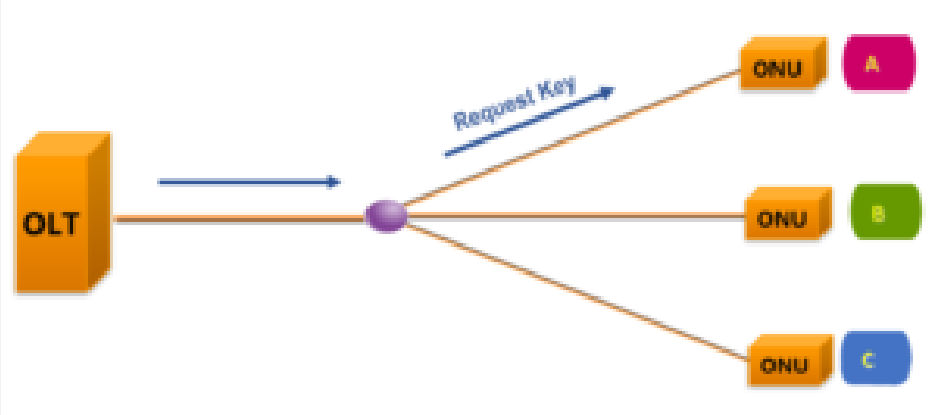


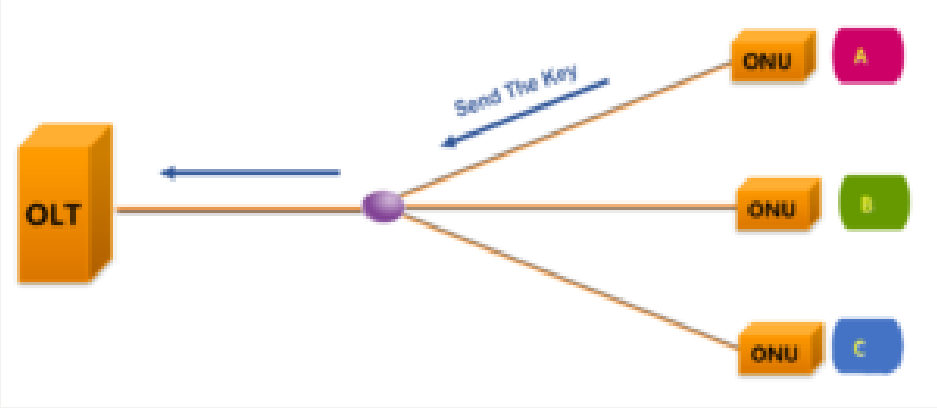


- ONT/ONU send Ethernet frames to GEM ports based on configured rules that map service ports and GEM ports.
- GEM ports encapsulate the Ethernet frames into GEM PDUs and add these PDUs to TCONT queues based on rules that map GEM ports and TCONT queues.
- TCONT queues use time slots based on DBA, then transmit upstream GEM PDUs to the OLT.
- OLT decapsulates the GEM PDU, the original Ethernet frame is now seen.
- OLT sends the Ethernet frames from a specified uplink port based on rules that map service ports and uplink ports.

Encryption Key Generation

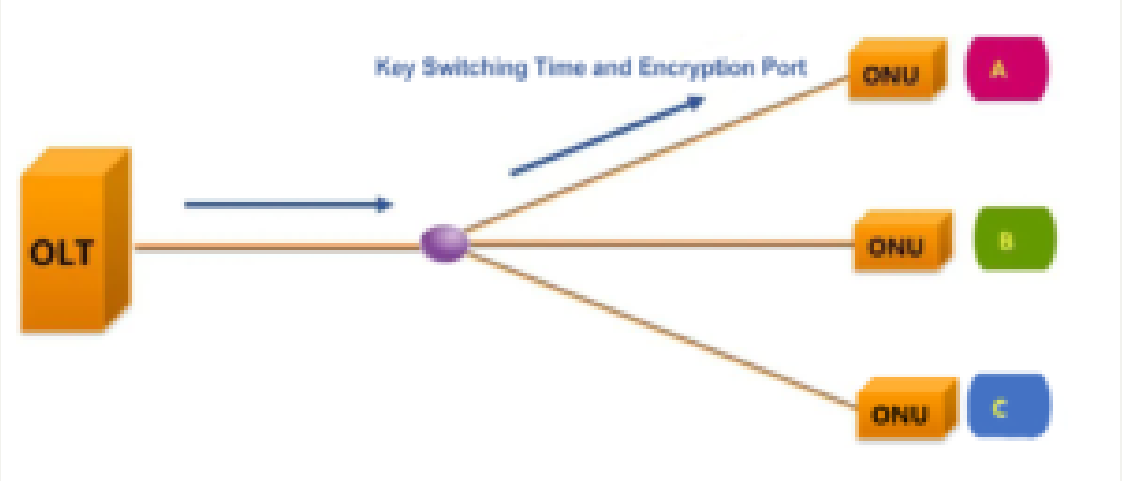
Request Key: The OLT requests the key from the ONU.





The ONU responds and sends the generated new key to the OLT in two parts, and repeats it three times.

After the OLT receives the new key, it starts the key switch and notifies the ONU of the frame number using the new key through the relevant command, also three times.

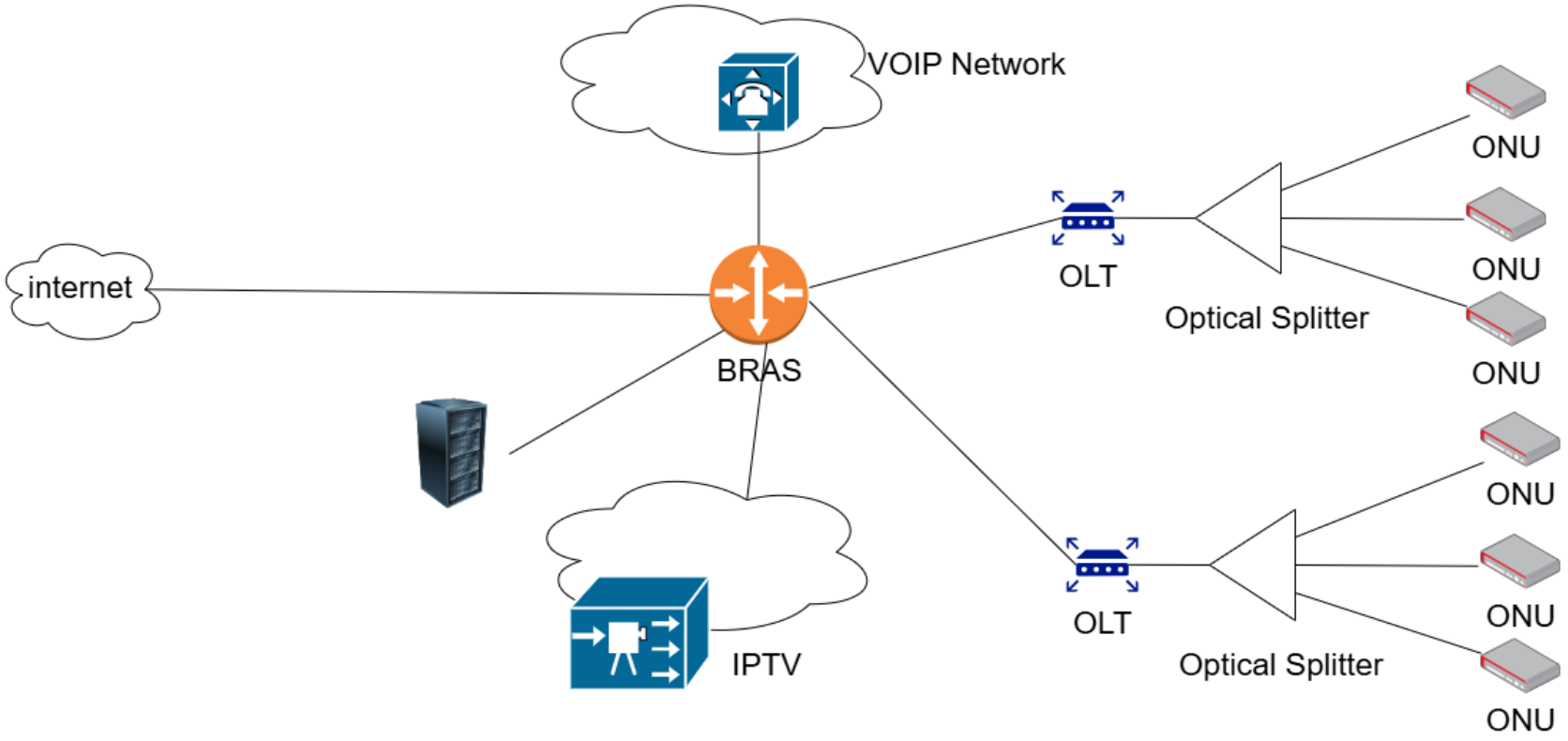


As we know, the downstream transmission of GPON is broadcast, that is, the PON port on the OLT side encapsulates the data sent to the ONU by the GEM frame and sends it to all ONUs in broadcast. All ONUs can receive the same data. Only the GEM PORT ID is used to filter its own data (the GEM PORT ID of different ONUs under the same PON PORT is different).

GPON Security

- One inherent advantage of fiber-optic networks like GPON over copper-based networks is that fiber is inherently more secure due to its nature. It's challenging to tap into a fiber line without causing noticeable disruption or attenuation (decrease in signal strength).
- GPON uses Advanced Encryption Standard (AES) encryption to secure the data transmitted between the Optical Line Terminal (OLT) and the Optical Network Unit (ONU) or Terminal (ONT). The encryption ensures that even if someone were to tap into the fiber, interpreting the data would be a challenge.
- During the initial setup or when a new ONU/ONT is added to the network, a process called "ranging" takes place. The OLT identifies the distance and timing of the ONU/ONT. Additionally, the ONU/ONT must provide a valid Serial Number and Password to be authenticated by the OLT. This process helps in ensuring only legitimate devices are connected to the network.
- In GPON, the downstream direction (from OLT to ONU/ONTs) is broadcast, meaning that the data is sent to all ONUs. However, due to the encryption mentioned earlier, only the intended ONU can decrypt and process the data meant for it.
- GPON networks can be segmented to isolate different user groups or services. By creating separate Virtual Local Area Networks (VLANs), service providers can enhance network security by preventing unauthorized access between different user groups and limiting the potential impact of security breaches.
- GPON technology's reliance on fiber optics provides inherent security benefits. Unlike traditional copper-based networks, fiber optics are immune to electromagnetic interference and more difficult to tap for unauthorized access, enhancing the overall security of the network.
- The upstream direction (from ONU/ONT to OLT) uses Time Division Multiple Access (TDMA). Each ONU is assigned specific timeslots during which they can transmit data, ensuring that ONUs don't access the medium simultaneously.
- To prevent malicious ONUs from joining the network, GPON has mechanisms to identify and block rogue devices. Proper management and monitoring of the OLT can help in identifying suspicious activities or devices.

HOW ISP Create Network



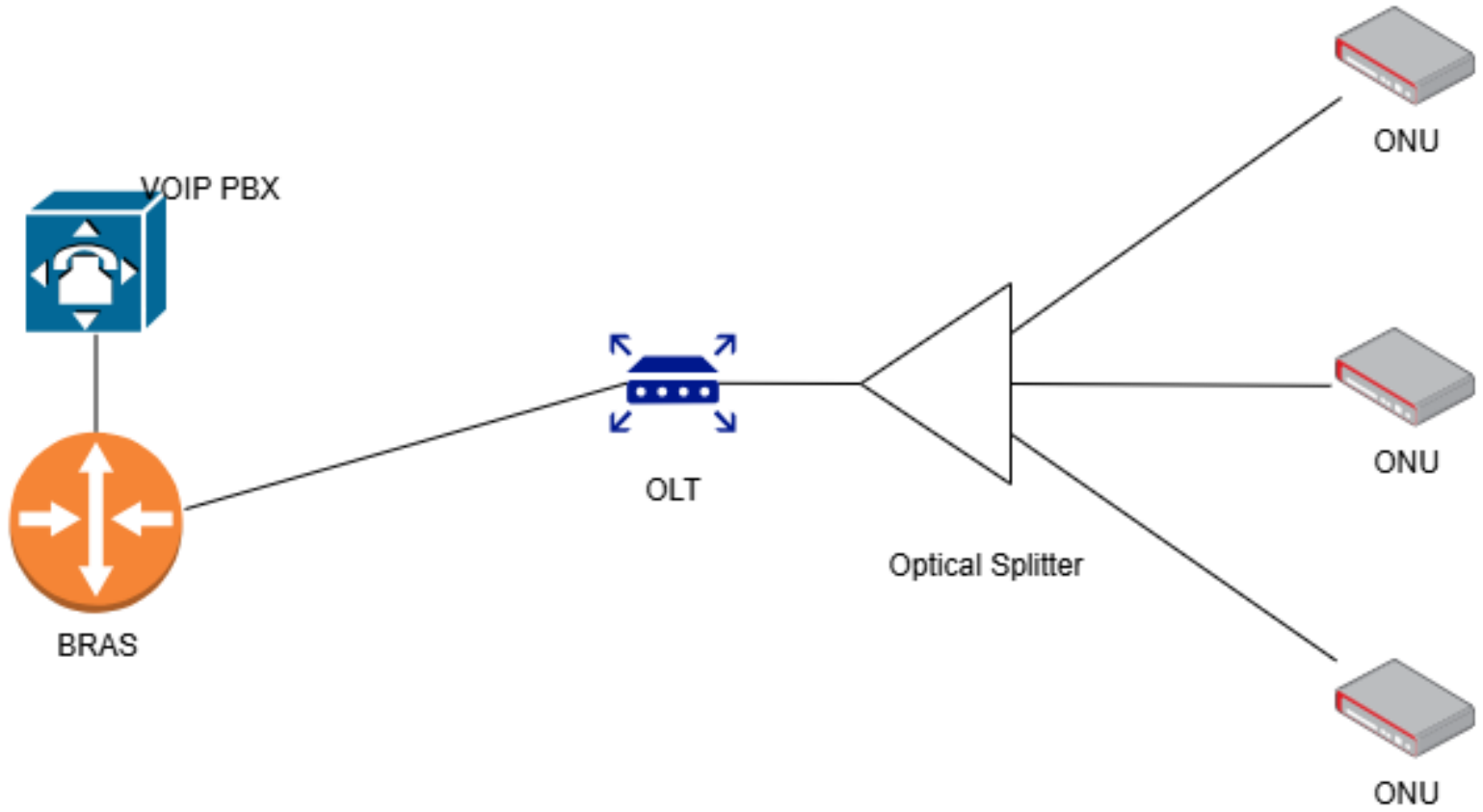
Technology Used

- ONT
  - Multi Vendor ONT
- OLT
  - Multi Vendor OLT
- BRAS
  - BRAS Server (usually Mikrotik) for PPPoE
- VOIP
  - Commercial IMS
- Radius Server
  - For Billing Purpose
- IPTV
  - Commercial IPTV Vendors

Services Available

- For Internet
- For VOIP
- IPTV

OUR GPON Network (SIMPLE ISP Setup)



Services Available

- For Internet
  - PPPOE
- For VOIP
  - IPoE
- BRAS Server
  - VYOS
- VOIP PBX
  - Asterisk

Attacking GPON

Attacking ONT/ONU

- First Entry Point for an attacker
- Gain Access to ONT
  - Easy
- Look into parameters that allow you to JUMP different networks

Simple Trick : Do Traceroute and NMAP for /16 Subnet

- C:\Users\Matrix-Shell>tracert 4.2.2.2

- Tracing route to b.resolvers.level3.net [4.2.2.2]
- over a maximum of 30 hops:

- 1 18 ms 9 ms 11 ms 10.18.0.1
- 2 3 ms 2 ms 6 ms 10.13.138.13
- 3 * * * Request timed out.
- 4 * * * Request timed out.

Try VLAN Jumping/Hopping

- There are multiple VLAN in these network
- Try Jumping VLAN from ONT/ONU
- Try bridge mode for direct L2 Access

Rest all is Standard IT penetration Testing