TRANSMISSION PROBLEMS!

Rajeshwar Singh
Operation Manager, NSN, Patna, India

Abstract
Today communication is a basic need of everyone and different types of transmission systems (PDH, SDH, and SONET) are used with different types of media i.e. copper cable, co-axial cable and fiber cable. This paper gives the brief idea of what are the problems occur in transmission? How to recognize it? How to solve the problem? And what are the preventive measures to be taken.

Keywords: Link Down, Link flapping, CRC Errors/Link Error, Latency/Slow browsing, Packet Drops

I. Introduction
In this paper I am going to discuss each and every problem step by step in brief.
1. What are the different types of problems faced by the customer?
2. How we can detect the problem?
3. How we are going to solve the problem?
4. What are the precautions taken to control the customer problems?
5. And finally I'd like to say some of the most equipments and instruments which are using in transmission section.

I. Problems faced by the customer
- Link Down
- Link flapping
- CRC Errors/Link Error
- Latency/Slow browsing
- Packet Drops

II. Link Down
This is the Most and frequent problem faced by the customer. The customer can identify the problem on his link by identifying alarm on the MODEM or ROUTER, there is an absence of data flow on the link, and the router shows the protocols are down.

Why the link goes down?
Here is the task where we have to concentrate! For this I am giving several steps to identify the problem. Please go through the steps carefully.

After lodging the complaint by customer the following steps should follow:

- 1. Check for alarms on the link by using NMS (Network Management System) /EMS (Element Management System) on monitoring system.
There are three cases! 1. If there are no alarms on the link, but customer complaint that the link is down, then ask him to give reset to the modem. If the link came up after resetting the modem then the modem was hang-up at that moment. 2. Even the link doesn’t come up after resetting the modem check for alarms in-service monitoring (this will not break the circuit). 3. The last case is direct alarms observed on the Monitoring terminal.

These are the Alarms generally observed on Monitoring system:

![Figure 1](above figure shows different types of alarms. Here I am concentrating to say why this alarms are occur if)
we know once about this then the problem can easily resolved.

1. The first and major alarm is **LOS** (Loss of Signal) what is this?

### III. LOS

This alarm Occurs in the following cases!

i) If there is no signal at the Physical interface (This is due to the fiber/Cable is not connected to the equipment).

ii) The power level is less than the threshold level of receiver sensitivity (For ex. Approx. – 24 db for ECI XDM and -38 db for ECI u-LAN, this depends on vendor to vendor).

iii) If the Equipment is failed, switched off or hang-up.

- When we observe the **LOS** in our monitoring equipment 99% the problem is in our Data Centre premises only.
- This alarm (**LOS**) will be clear by using checking whether the cable is properly connected or not? Threshold power is ok or not? Equipment is faulty or what?
- This **LOS** state will clear only when two consecutive frame structures in **SDH** will receive and no new **LOS** signal will appear. We will discuss about **SDH** and the alarms generated in corresponding section.
- Next one is the MAJOR and Frequent alarm **AIS** (Alarm indicating Signal).

### IV. AIS

This alarm is generated due to failure of signal at the exchange which is prior to our exchange (like TTML, MTNL, and BSNL etc. which are the local service providers).

- When **LOS** occurred at prior exchange, these exchanges (local service provider) will transmits all one’s to the next or down stream exchanges which indicates that the signal was failed.
- Even though if the signal is present, and if there was an error in receiving of Multiplex section or Regeneration section of **SDH**, then the exchange generates MS-AIS or RS-AIS.
- I am going to explain diagrammatically how the alarms will generate.

Note:

- Green line indicates path is ok.
- Red line indicates faulty in the path.

---

- Let there is a fiber cut in between customer premises and BSO. Then **LOS** is appeared at the BSO exchange and the equipment at BSO receives no signal it injects all ones in to the down stream which indicate **AIS** for all the down stream exchanges like VSNL, and d/e exchanges.

- The above two diagrams clearly explains how **LOS** is effects the down stream
- We are already familiar why these **AIS** will occur? Here we are going to discuss about where the exact location of problem and how to find out it? (Because **LOS** will transmit AIS alarm to the entire downstream and we can’t able to find at which place the **LOS** appears if more than one exchanges are present prior to us).
• The above problem is solving us by segment wise testing.
• What is Segment wise testing?
• This is the primary test used to find where the exact location of the problem in the transmission path.
• How this test was carried out? Let’s go step-by-step.
  • **Step 1.** Ask the customer. Whether the customer Modem is switched off or not? If the modem is switched off it will inject LOS to nearest BSO and the BSO will inject AIS to entire down stream.
  • **Step 2.** If customer modem is ok then take the loop from customer modem and check on the meter whether we are getting the loop or not? Or ask the customer to check the loop by providing the loop towards customer.

There are two things to be reminded while taking the loop from the customer.
• If the customer having two modems, one is at BSO premises and another one is at his office, ask him to give the local loop back which gives the loop towards VSNL side and if customer having only one modem asks him to give the remote loop back.
• If customer loop is un-getting, take the loop from nearest BSO and check the same. If you get the BSO loop , then the problem is in b/w customer and BSO, if more than one exchange is present in b/w you and customer then take loop from each exchange if you are not get the loop from prior exchange which is shown in the following fig.

  By this we can easily identify where the exact problem is?
  • If you are getting AIS from distend end do the loop test as same as before.
  • **There are certain types of AIS are there!**
    1. MS-AIS (Multiplex section Alarm indicating signal)
    2. AU-AIS (Administrative Unit Alarm indicating signal)
    3. TU-AIS (Tributary unit Alarm indicating signal)
    4. RS-AIS (Regeneration section Alarm indicating signal)

**MS-AIS** occurs when the overhead byte contains all binary ones then this alarm is raised. The overhead contains all ones only when there is LOS or frame synchronization etc.

**LSS:** Loss of sequence synchronization. This will occur when the frame structure is not synchronized with test set up. This is overcome by choosing the correct framing like famed / unframed CRC ON or OFF correct PRBS and etc.

**REI:** Remote Error indication. This alarm is returned to the transmitting node that an error block has been detected at the receiving node.

**RDI:** Remote Defect Indication. This is the signal returned to the transmitting equipment upon detecting a Loss of signal, Loss of frame or AIS defect.
**RFI:** Remote Failure indication, this alarm persists beyond maximum time Allocated to the transmission system protection mechanism.

**Unequipped:** This alarm is raised when there is no equipment connected to the link this is two types: HP-unequipped and LP-unequipped.

---

**V. Link Flapping / Erroring**

Why the links will flap/Erroring?

1. There is no proper physical connection (loose connection) b/w the equipments (like modem to router, passport to router etc according to customer requirement)
2. There is no proper termination at DAC port (exact punching) at DDF/MDF of BSO or our location
3. Ageing of equipments
4. Less transmitting power injects errors into the link
   - The Erroring is mainly due to copper connectivity at customer premises (if and only if our transmitting is optical or else problem at our premises also).

---

**VI. Latency/Slow browsing/Packet Drops**

What is Latency?

- Latency is the round trip delay of the circuit from end to end.
- How to measure it?
- Take the loop from customer measure the delay on the tester (like ANT-20), and take the loop from counter part and measure the delay, by combing both the delays we get overall delay.
- Why customer face the latency:
  1. The first and main reason customer can face the latency due to change in the routing of path (due to path Erroring, link breakage etc) i.e. change over path from main to protection.
  2. The latency is increased due to the equipment hang-up.
  3. The customer may face the latency due to over limit utilization of the link (i.e. if customer takes 2 Mb link and if uses more than that, or customer may open more applications at a time on the same link.)

---

**VII. Packet Drops**

Packet drops are occur due to the over size utilization of the link, if the customer trying to access more than the allocated size the packets coming into the router or equipment get on bombarded and collapsed at last. So the customer can face packet drops.

- What we will do?
- Ask customer about link utilization suggest him to utilize the link below the allocated
size only, and then this problem will easily resolved.

VIII. Conclusion
We have seen different problems in transmission media and its solutions in the above discussion. After study this paper you will easily identify the problem and solve it to give good performance by the link.

REFERENCES