Network Design Considerations in Telemetry Systems

Andy Grebe and Wayne Klein
Apogee Labs, Inc.

ABSTRACT

In today's world, computer networking has become common place both in industry as well as home, however all networks are not the same! The Telemetry world, like with many industries, has critical design considerations that need to be evaluated when you begin a new system or just adding on to a current infrastructure.

This paper is intended to outline needed considerations when planning or implementing a network design in Telemetry Systems. These applications can range from sensor data transport through High Definition/High Speed Video applications.

KEY WORDS

TM:	Telemetry
Networks:	A system of computers/processors inter-connected.
LAN:	Local Area Network
WAN:	Wide Area Network
Ethernet:	Standard LAN access method.
TCP/IP:	Transmission Control Protocol/Internet Protocol Standard protocol for transmitting data over networks and Internet Protocol.
UDP/IP:	User Datagram Protocol/Internet Protocol

OVERVIEW

Whether transmitting PCM serial data running at 20 Mbps, or high definition(HD) video at a few hundred megabits, the network topology must be considered before blindly sending this data across the network. When setting up these networks one must consider the following areas:

- Topology
  - How will the network equipment backbone be connected (range from "Point to Point" to a "WAN")?
  - Distances of connected equipment?
- Protocol

- Transport speeds
  - Is there a “real-time” requirement?

TYPICAL NETWORK DESIGNS/TOPOLOGIES

Most company's network designs are similar, a computer connected to a LAN which is connected to a WAN. This WAN can either be the companies WAN before it reaches the Internet, or it may be the Internet.

The most reliable and easy to configure, would be a point to point setup (Using a copper crossover cable)(See Diagram 1).

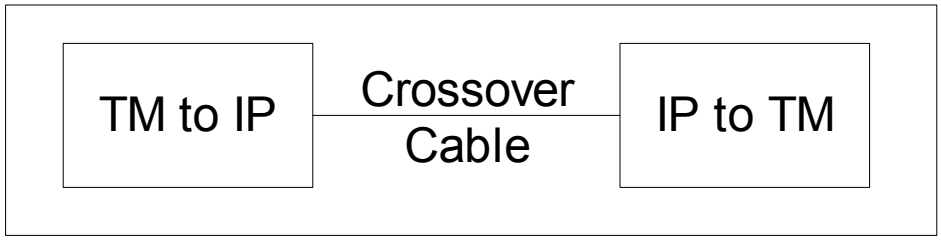


Diagram 1

The crossover cable uses a standard twisted-pair Ethernet cable directly from one network device to another. This simple approach is very reliable and easy to fix if there is an issue. This type of setup is typically used in a lab environment to verify a network connection/output. The issue here is the fact that it does not promote long distance transmissions. A single cable, whether cat 5e or cat 6, can only run up to 100 meters. The two common methods to increasing the distance between any two network devices is either a network repeater, or converting the media to fiber. Both methods can be used in this and the following network design examples.

The next easiest network design is attaching two TM to IP devices on the same LAN (or subnet)(See Diagram 2).

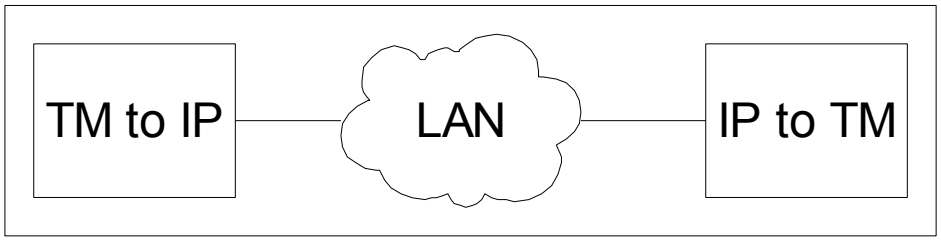


Diagram 2

When dealing with low data rates, i.e. 20% of the slowest link that you “pass through” in the LAN or less, this method will work 90% of the time. Attempting to use more than 20% of the

bandwidth on a company network could result in a saturation of the network thus causing data drop outs and increased latency in packet delivery. There are multiple reasons for dropped packets:

1) Other network users can be downloading information from the Internet
2) Some may be transmitting large files to one another
3) Downloading or uploading emails
4) Backing up data to a central server
5) etc...

The dropped packets can be seen especially if the unit's data is crossing multiple subnets. The main issue here may be that a network is organized in a star formation (See Diagram 3). This requires that all data be sent through a single switch or router. The single switch or router may receive data at a bandwidth higher than it's own, as it is handling all data on the network. Instead either a full or partial mesh network (See Diagram 3 below) should be implemented. This will remove most of the other network traffic from the network path between the two nodes.

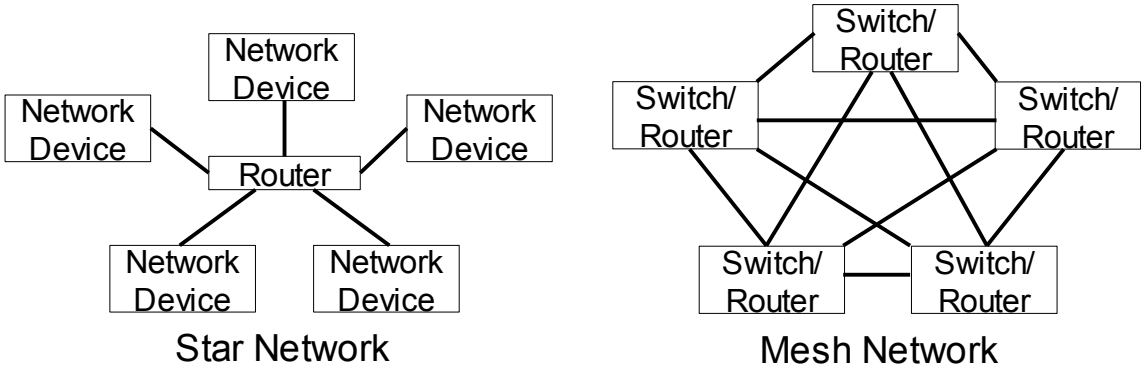
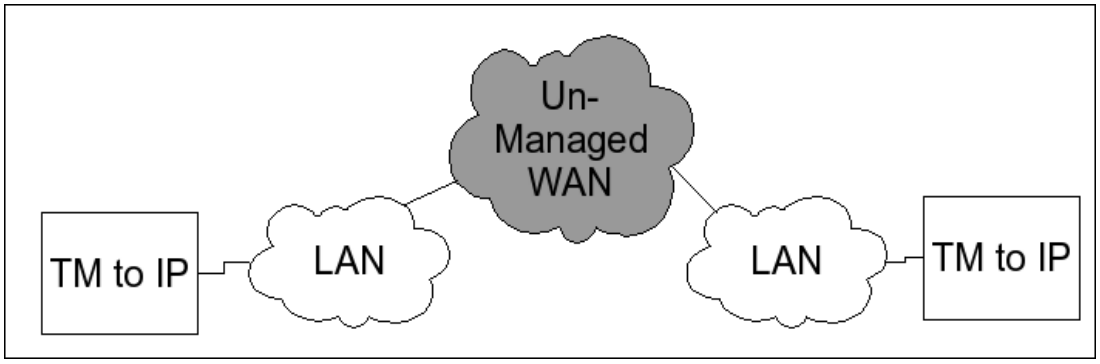


Diagram 3

The least deterministic of the network designs includes an unmanaged WAN. This is most easily envisioned as the Internet.



From point A to point B, once the IP packets leave the LAN, it is unknown what routes the data will take. The most influential factors in an unmanaged WAN are non-guaranteed bandwidth and jitter in the network latency due to other IP traffic. Most services give a maximum rate of uploading and downloading packets to and from the Internet. This rate is not guaranteed at all times, unless specified by the provider. This is a nightmare to real time transmissions, as the receiver may experience underflows.

Moving up in the complexity, we introduce a "Managed" WAN (See Diagram 4). The "Managed" WAN is usually a WAN at an organization that requires reliable, fast, controlled, and safe data between to two communication points, such as a DOD base. Please note that multiple managed WANs can co-exist as part of a larger WAN design.

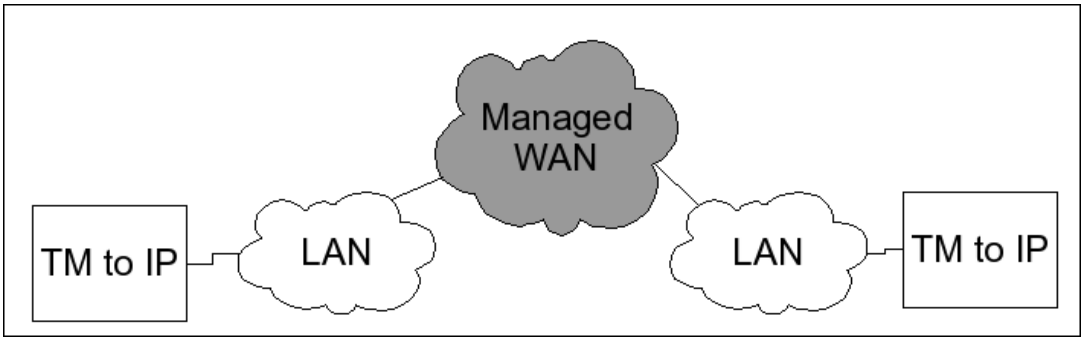


Diagram 4

The LANs in this case are usually contained within a building. The reason the WAN is considered "Managed", is that the company has control over the setup and the bandwidths between LANs. For instance, if there are LANs A, B and C and a test is going to be run between network appliance NAA and NAC, being on LAN A and C, respectively, the IT department would configure the network so that NAA and NAC would be given the desired transmit and receive bandwidth through the respective LANs and also through the WAN. This method can better guarantee bandwidth and can provide an environment better suited for real-time TM over IP applications.

SPEED, SPEED, SPEED

When dealing with real-time transmissions, the speed at which data enters the TM to IP devices and leaves the IP to TM device is most important. Although many Telemetry applications can easily reside on a 10 or 100 megabit network (Network design/traffic dependent) many new infrastructures are going to 1 Gig and above to allow for growth and increased needs in applications like video.

Once the topology is selected, the Protocol, MTU and equipment are the next steps to increasing speed and lowering latency.

The two most prevalent protocols currently used are TCP/IP and UDP/IP. TCP/IP is a protocol designed to get data from the source to the destination without errors. It does this with ACKs, NACKs, CRC checks, retransmissions and other means which are too in depth to cover in this paper. The drawback of using TCP/IP, is that it increases system latency, whether the network is running perfectly or not. This is due to all of the methods it uses to ensure the data has no errors once it reaches the destination. UDP/IP is a connectionless (no hand-shaking), fire and forget protocol, which does use CRC checks to at least ensure that if the packet has received errors on the network, it will not be given to the end program. The benefit of using UDP/IP is that it requires less CPU cycles, less bandwidth on the network and has a lower packet to payload ratio.

For low latency and high bandwidth, UDP/IP is the preferred method. UDP/IP can be used on loopback, crossover cable, LAN and perhaps even the managed WAN networks. When used on the LAN and managed WAN networks, the physical link should be checked for any hardware faults between the two ends of the link. The RCC is currently defining a protocol for TM over IP. This proposal uses UDP/IP as its standard protocol for handling data on the network. The reasoning is that most networks which attempt real-time TM over IP either already use guaranteed bandwidth, or are simple networks with a limited number of data streams. TCP/IP is preferred on the LAN and managed or unmanaged WAN networks, if every bit of data is required at the receiver. Please note, for "mission critical" data that needs to be recorded it is always recommended to store the data closest to the point of data collection in the network (i.e. Ground Station) .

The MTU stands for Maximum Transmission Unit. In most cases, the larger the MTU, the higher the effective bandwidth will be and the lower the latency will be. In the fast Ethernet, or 10/100 Mbps, the MTU is usually at 1,500 bytes. When configuring a network which uses fast Ethernet, verify that all paths can use a MTU size of 1500. Gigabit networks can use a MTU of 9,000 bytes, otherwise known as jumbo frames. While at first it may seem that 9,000 byte frames may add latency to the system, a 9,000 byte frame across a gigabit network takes the same amount of time as a 900 byte frame on a fast Ethernet network. So use a 9,000 MTU size on gigabit networks. It is only the MAXIMUM transmission size, not the required transmission size, so it is still possible to use smaller frames on this network.

An important element of the network design is the equipment used in the network, such as the switches, routers, and cables. In a network where real-time data will be transmitted, hubs should not be used. Hubs are similar to switches, but are half-duplex, thus reducing the total transmit time and receive bandwidth of the network. Hubs also transmit packets which come in one port to the rest of the ports, resulting in collisions and over congestion of the network. Collisions and over congestion can severely degrade the overall network performance. In UDP/IP this will lead to lost packets and in TCP/IP this will lead to retransmissions, which in turn leads to lower available bandwidth and higher latencies.

Switches are usually full duplex links which send data only to the destination, thus minimizing or eliminating the number of collisions. When selecting a switch, care must be taken to decide

what features are needed for the network which is being designed. We recommend using a managed switch, in LANs/WANs, allowing user control of the network for times when guaranteed bandwidth is required. If a switch is used to connect a remote site via a managed WAN, then an unmanaged switch could be used, as the remote network is only used for transmission of data to the main TM buildings. The main benefit for using an unmanaged switch is that it can be a magnitude less expensive than a managed switch.

Routers are similar to switches, with the exception that they add a gateway to another LAN or WAN. The same care must be taken when selecting a router as when selecting a switch. Another possible choice when choosing routers and switches is that the media can be changed. If copper is used in the LAN, it can be changed to a type of fiber before being sent across the network. This has multiple benefits, fiber has guaranteed bandwidth, giving more reliability to the network and it can also be used to partially upgrade to an Ethernet network while leaving some older fiber lines when running at lower rates.

When copper is used to transfer the data across the network, even though cat 5e can be used for both fast and gigabit networks, cat 6 cable should be used. Cat 6 cable shields the data better than cat 5e, and as a result, it can run data across faster. A simple test in the lab had shown an increase of 25 Mbps across a gigabit network just by changing a few cables from cat 5e to cat 6 cables. This is enough bandwidth to handle a few extra visually perfect MPEG2/MPEG4 encoded video streams!!

CONCLUSION

Not all network setups are equal, but then not all networks are setup to handle the same type of users/data. When dealing with real-time data, the simpler the network, the easier it will be to ensure data will arrive at higher bandwidths and lower latency. The more users on a network, the less likely the data will flow across the network smoothly. The basic rule for protocols is UDP/IP for simpler and managed networks and TCP/IP for more complex and unmanaged networks. For both types of networks, use the MTU size to minimize the number of IP packets on the net, as this will increase effective bandwidth. It is recommended not use hubs, unless a case can be made that they are required for the conditions of the data or testing, but to use managed switches. Finally, when using copper cables, always select the newest when trying to achieve high bandwidths and low latency, whether it is cat 6, 7 or another by the time this paper is being read.