A dB Levels White Paper

Dallas, TX USA
214-257-8823
www.dblevels.com

Methods for Verification of Network Timing and Synchronization Links

By Daniel B. Burch

July 2009

Contents

Introduction

Guidelines for Network Synchronization and Timing have been adequately chronicled for Network Planners and Engineers; however, there has been a void in materials and procedures to guide local site technicians and maintenance engineers regarding testing of BITS clock input and output links, and troubleshooting of synchronization and timing-related problems in general.

Problem Statement

Telecommunications site technicians are tasked with maintaining a wide array and vintage of Network Elements, including TDM voice switches, Fiber Optic transmission equipment, Channel Banks, Add-Drop Multiplexers and IP-based routers, gateways, switches and management systems. For the entire Network to be properly synchronized, nearly all of these devices require connections to the Building Integrated Timing Supply (BITS).

Equipment installations for local office and field locations were based on prevailing procedures of the day, resulting in a myriad of possible connection arrangements, test access points and cabling conventions. Overall Synchronization Planning was thwarted by failure to properly connect all related Network Elements, fueled by installations which did not follow strict standards.

Most locations adhered to some level of Synchronization Planning, so the Network was generally stable for long periods of time. Historically, site technicians rarely needed to work on BITS, so they possess little, if any knowledge or understanding of neither the local BITS system nor its relevance to network troubles. However, as Network transmission rates and channel capacities have risen, so also have outages related to Network Synchronization.

The implementation of Sync Status Messaging (SSM) on T1 and E1 timing links greatly increased reliability and complexity of Synchronization Planning and testing.

SSM provides a means for Network Elements downstream from the BITS to be aware of the traceability of the timing signal with a hierarchal system of coded messages. Transmitted “out-of-band” on E1 and the Facility Data Link for T1, SSM allows Network Elements to follow an automatic, pre-determined process for selecting the timing source of the highest reference; thereby eliminating outages due to timing failures.

Network Time Protocol (NTP) is now also widely implemented across carrier networks, supported by little, if any procedure for turn-up and maintenance testing.

Currently, site technicians lack:

1. Test equipment to properly evaluate BITS output signals, including readout of critical SSM codes for T1 and E1 signals.
2. Procedures for testing BITS and NTP output links.
3. Training to quickly identify Network Timing and Synchronization problems.

Previous Options

The common fall-back method has been to closely monitor alarms in the BITS equipment at the System Level, with hopes that individual timing output troubles could be detected at the higher level. However, this is often not the case.

Modern GPS-based Network Synchronization Systems do provide alarm monitoring to determine overall system operation, quality and usefulness of the GPS signal, status of antenna cables and antenna operation, and a limited number of output-related faults such as shorted output cables.

Troubleshooting methods were generally directed from a distant Network Operations Center (NOC), with the local site technician performing “eyes and ears” function for the NOC engineer. Cards could be swapped, LEDs viewed for activity, etc. However, at some point the NOC engineer must direct the site technician to perform physical maintenance activity such as cable testing, tracing and Network Element connection verification. At this point the local technician was very limited in availability of tools and training.

Recommended Solution

The solution is to provide telecommunications site technicians with tools and information (procedures) to identify, troubleshoot and correct Network Synchronization and Timing troubles.

This must include practical examples for completion of required tasks, analysis flowcharts, and simplified overview of the concepts of Network Timing and Synchronization.

This white paper provides directions for connection of laptop PCs, Network Sniffers and analysis of NTP links; and also use of a timing test set, analysis of test results, corrective measures and installation guidelines for the three most widely-used BITS timing link types worldwide:

1. T1 with or without SSM
2. E1 with or without SSM
3. CC (Composite Clock)

Benefit 1

This white paper will equip telecommunications site technicians to quickly evaluate the quality and usefulness of BITS timing signals, with instructions for testing all the way to the Network Element; and advanced troubleshooting of NTP-related troubles.

This will result in significant reduction in restoral times for timing-related outages, and reduction of costly repeated/chronic trouble reports.

Benefit 2

This white paper can be used to, or serve as a guideline for establishing routine maintenance procedures that can reduce or eliminate potential timing-related failures before they occur by introducing a method for remote, long-term monitoring of critical timing circuits.

Benefit 3

Lastly, this white paper will provide a framework for testing of new Synchronization Plans as they are implemented, ensuring that the design objectives have been achieved in practice (installation), including recognition of “timing loops” which prove fatal to Network Operations.

Implementation

To achieve the deliverables in this white paper, the end user company must acknowledge the identified deficiencies, provide minimal to moderate funding of required test equipment, review existing practice and procedure relating to BITS testing at the local site, and finally, condense and distribute the procedures herein, inserting any additional safeguards required by your company.

Such additions may include escalation procedures, authorizations for performing routine maintenance, and safety procedures for wrist-strap grounding where required.

This paper is not intended to supplant existing practice and procedure but can, with permissions, supplement or be incorporated into formal company documentation.

Summary

Since deregulation of AT&T in the 1980’s, telecommunications networks have become interconnected islands of technology, with no supreme arbiter to insure all the rules are obeyed. As these interconnections span the globe, carriers of all sizes can now impact overall network performance and reliability. It is critical that every carrier develop a Synchronization Plan which fits well with the rest of the world, ensuring reliable, self-healing transmission paths.

A key component then, is to properly equip and train telecommunications site technicians to adequately maintain timing and synchronization links at the local level. If not, services will be unreliable and noisy, calls will be dropped, Internet connections will slow, and HDTV images will be irregularly pixilated, ruining the quality so heavily touted by broadband connections.

Attachment 1- Methods for Verification of Network Timing and Synchronization Links - Rev. 1.1 - July 2009

dB levels

Table of Contents

Overview Section

Introduction to Timing & Synchronization including NTP and SSM

Troubleshooting Section - Timing and Synchronization Links

Troubleshooting Network Time Protocol

Troubleshooting Composite Clock (CC) Network Synchronization links

Troubleshooting T1/E1 synchronization links including SSM

Measuring Slips across BITS Outputs and Network Elements

Commissioning Testing of Newly-Installed BITS Systems

Manufacturing/Vendor Testing of Network Elements

List of Flow Charts

List of Tables

List of Figures

List of Figures, continued…

List of Figures, continued…

References

[1.4] Stefano Bregni, *Synchronization of Digital Telecommunications Networks*, Wiley Press, 2002 ISBN 0-71-61550-1, Chapter 4, Page 137.
[1.5] CXR Larus, “Getting it Right” M.Ritz Preso
[1.7] Stefano Bregni, *Synchronization of Digital Telecommunications Networks*, Wiley Press, 2002 ISBN 0-71-61550-1, Chapter 4, Page 185.
[1.71] David Mills, *Computer Network Time Synchronization: The Network Time Protocol*, CRC Press, 2006, Chapter 1, Pages 3, 4.
[1.8], [1.9], [2.3], [2.4] Microsoft Corp., Windows Vista
[1.92] CXR Larus, “QoS Measurements in PWE”
[1.93] CXR Larus, StarClock 6850 Grandmaster GPS/NTP/PTP Clock file photo
[1.94] CXR Larus, StarClock Tiempo 6400 Users Manual
[1.95] CXR Larus, “Getting it Right” M.Ritz Preso
[1.96] CXR Larus, “Getting it Right” M.Ritz Preso
[1.97], [2.0], [2.1] CXR Larus, Applications Note AN-96A RevA, 21 May 2001: GPS Antenna Installation for Larus Timing Systems
[1.98] CXR Larus, file photo
[1.99] CXR Larus, lightning damage file photo
[2.2] CXR Larus, Starclock 200E Users Manual
[2.5] WireShark Network Protocol Analyzer Ver 1.0.7 © 1998-2009 Gerald Combs
[2.6] Guisys Corp., Gb310-RITS Intelligent Timing Test Set, all photos and Menus used with permission
[2.7] Stefano Bregni, *Synchronization of Digital Telecommunications Networks*, Wiley Press, 2002 ISBN 0-71-61550-1, Chapter 4, Page 182, 183.
[2.8] CXR Larus, StarClock 6800 Edge GPS/NTP/PTP Clock file Photo

Resources

BOOKS:

- *Computer Network Time Synchronization: The Network Time Protocol*, David L. Mills, CRC Press 2006, ISBN: 0-8493-5805-1
- *Synchronization of Digital Telecommunications Networks*, Stefano Bregni, Wiley Press, 2002 ISBN 0-71-61550-1

TIMING/SYNC EQUIPMENT, JOB AIDES, TUTORIALS, ETC.:

- CXR Larus Corp, 894 Faulstich Ct., San Jose, CA USA 95112 408-573-2700 www.cxrlarus.com

CC/T1/E1TIMING TEST SET:

- Guisys Corp., 40W320 LaFox, St. Charles, IL USA 60175 630-672-8540 www.guisys.com GbB310-RITS Intelligent Timing Test Set

NETWORK SNIFFER (free versions available for PC)

- WIRESHARK Network Protocol Analyzer Ver. 1.0.7 (freeware) ©1998-2009 Gerald Combs www.wireshark.org

TECHNICIAN TESTING AIDES – VIRTUAL HELP DESK

- dB Levels, Inc. www.dblevels.com

1.0 The term *Timing* has historically been associated with Time-Division Multiplexed (TDM) Networks where a Building Integrated Timing Supply (BITS) utilized T1, E1, Composite Clock or other links to synchronize Network Elements. A technician might express, "I've got a *Timing* problem in my office." Or, "I need to run external *Timing* to that Channel Bank." Strictly speaking, this is not *Timing;* it is *Synchronization*.

Timing is a method for providing a reliable reference of exactly what time it is *right now*. For example, the answer might be that it's 10:23:00 or, twenty-three minutes past ten o'clock AM. Note that we still don't know what time zone we are referencing (EST, CST, PST, etc.) This is more commonly referred to as a *Time-Stamp*, signifying an exact moment in time. One of the most widely deployed protocols for time-stamping is called *Network Time Protocol* or *NTP* for short. When you think of *Timing*, think *Time-Stamps*. *Synchronization*, then, is a means for using a frequency reference to stabilize transmission equipment across a single or multiple locations.

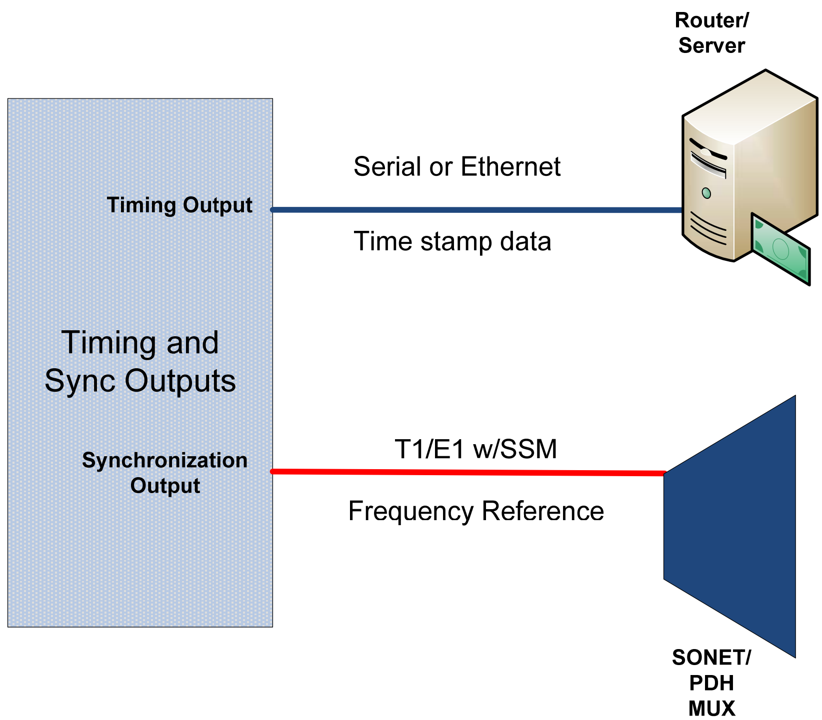


Fig. 1
Timing vs. Synchronization

In some cases, Network Elements require connections for both Timing *and* Synchronization. For example, a Voice-over-IP Gateway needs to be synchronized on the TDM side, yet requires Network Time Protocol (NTP) for accurate time-stamping on the IP side. Likewise, a SONET/PDH Node may require Synchronization for network traffic and NTP for accurate time-stamping of events like alarms or status changes.

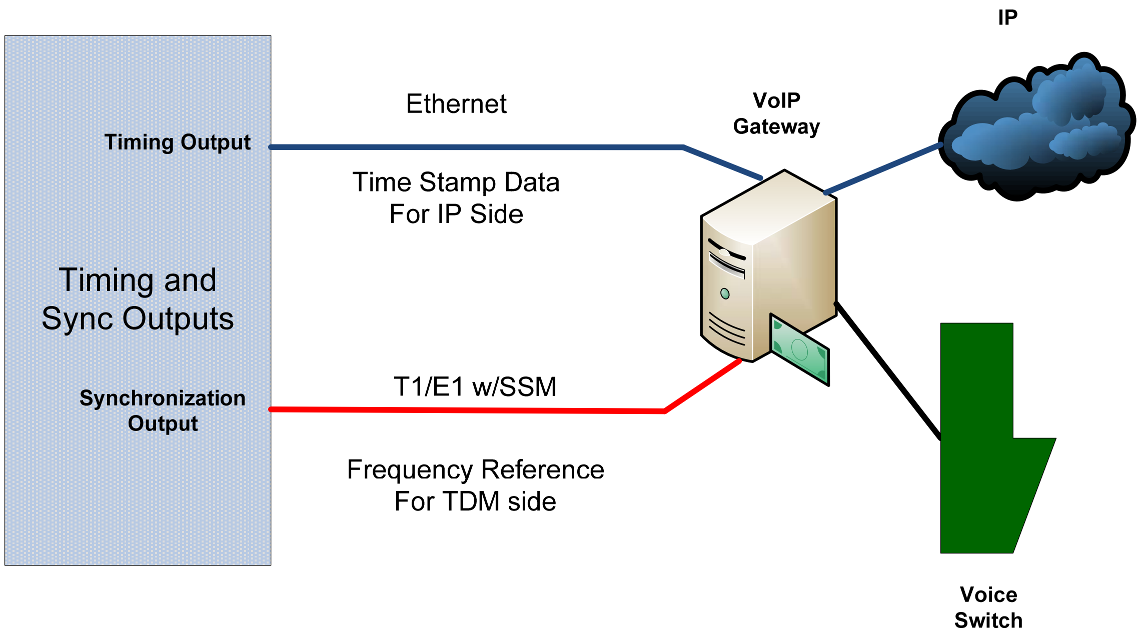


Fig. 2
Timing & Synchronization
Of Same Network Element

1.1 Allow this analogy to illustrate the difference between *Timing* and *Synchronization*: If I ask you "What time is it?", I'd expect you to look at your watch and tell me the time, not hand me a metronome so we could stay on beat with musical instruments. In fact, if I really am concerned about the time you gave me; perhaps I'll check several other sources and compare the time displays, arriving at some logical answer. I will use all references available to determine exactly what I believe is the correct time. While that is the premise behind NTP, let's first examine legacy *Synchronization* methods.

1.2 The Need for Synchronization in Networks

Modern technician lingo blurs the line between several aspects of *Network Synchronization*. In practice, it is normal for the following terms to be interchanged by technicians for the same meaning: *Timing, BITS, Clocking, and Synchronization*. While the engineering purist objects to this, we will delight technicians worldwide by not making a big deal out of it with exception of the sections relating to IP-based *Network Time Protocol (NTP).*

The introduction of Pulse Code Modulation (PCM) and digital transmission systems into the telephone network resulted in improved quality and efficiencies for transmitting voice and data. A single PCM link worked just fine, as the digital signals were governed by clocks built into the PCM Channel Banks.

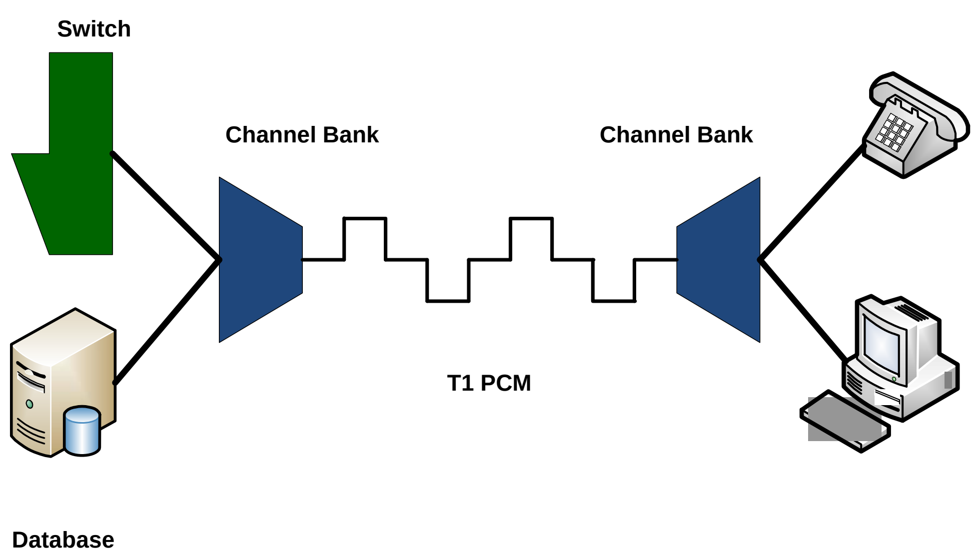


Fig. 3
Single PCM link

However, when end-to-end connections traversed two or more PCM links, subtle deviations in the Channel Bank clocks allowed frame slips, causing audible clicks in the voice traffic and occasional interruption or slowness of data connections.

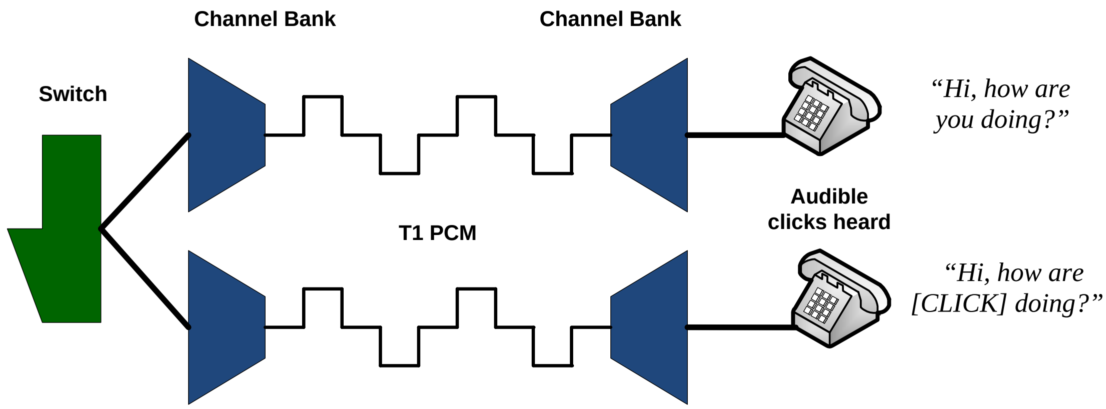


Fig. 4
Multiple PCM links

The solution was to connect all Channel Banks with a common frequency reference, synchronizing the internal Channel Bank clocks. There were actually two clock signals in the Channel Bank- 64kbps and 8kbps, called BIT and BYTE, respectively. These clock signals are utilized to convert analog voice signals into a PCM data stream, aligning the encoders and "Framers" which drive the T1 output signals. Since it was impractical to wire BIT and BYTE clock leads from the Building Integrated Timing Supply (BITS), a composite signal was developed, allowing a single link between BITS and Channel Bank. The composite signal consisted of 64kbps stream with a purposeful error every 8kb, and is called Composite Clock (CC).

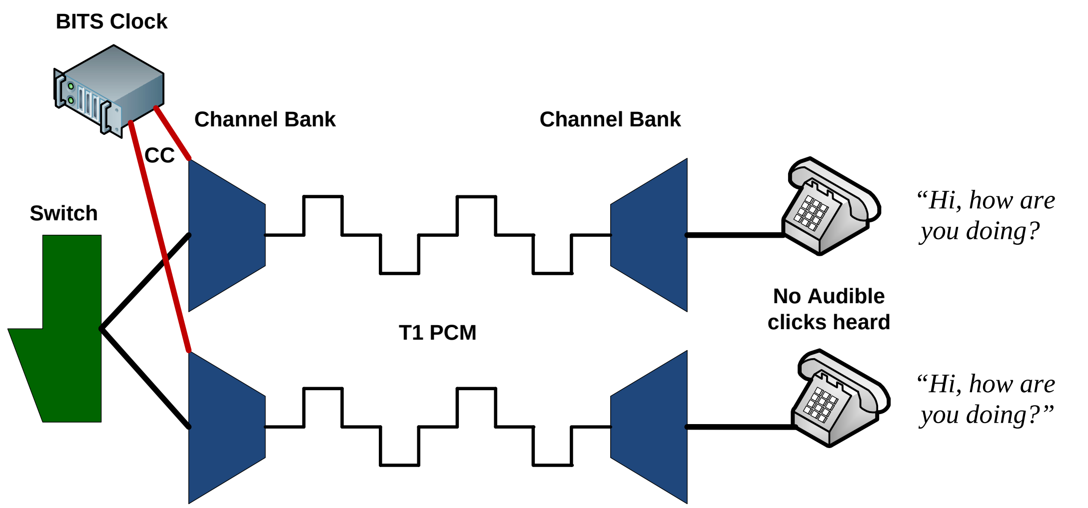


Fig. 5
Multiple synchronized PCM links

1.3 How Network Synchronization is achieved

By connecting one end of the Channel Bank to a common frequency reference (External Timing), the far end Channel Bank could be configured to derive synchronization from the incoming T1 pulses (Loop Timing also called Line Timing), resulting in synchronization of both Channel Banks.

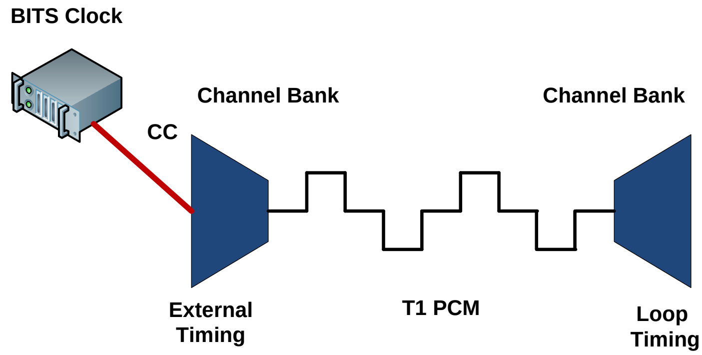


Fig. 6
External and Loop Timing

Of course, if both ends of the PCM span had clock sources that were on par with each other, then you could connect the Channel Banks at each end to their respective BITS as shown below.

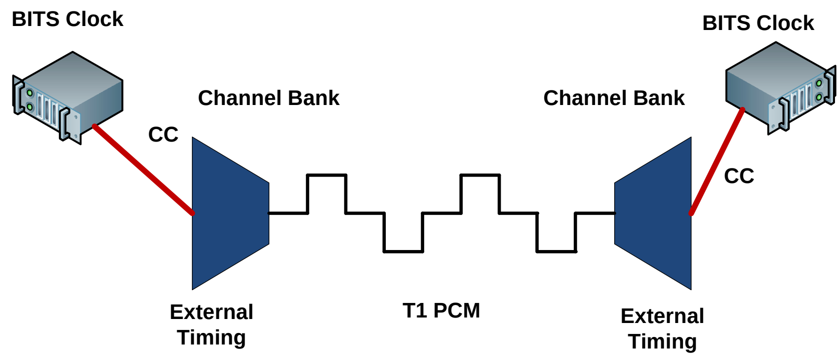


Fig. 7
External Timing only

To insure the Building Integrated Timing Supply (BITS) in each office are in sync with one another, a higher-order signal is required for all BITS systems to reference equally. In the USA, this signal is derived from satellites in the Global Positioning System (GPS).

1.4 Synchronization Signal Stratum Levels

Prior to adoption of GPS for synchronization of BITS systems, earlier attempts to provide network synchronization followed a hierarchical model as shown in Figure 8. A Cesium Beam oscillator provided precision frequency output, and the synchronizing signal cascaded downward through the tiers of switching centers. Stratum Level 1 was the most pure signal available, so as the signal passed through each level (switch, transport, etc.), it was of lesser quality (more jitter, etc.). Therefore, by the time the signal reached the End Office (the switching office closest to customers), it was Stratum 4 in quality.

In short, the higher the Stratum Level (1 is highest quality), the higher the level of stability as compared to the ideal. Therefore, as the Stratum levels decrease (1 is best, 2 is lesser quality, 4 is much lesser quality), so then do variances in stability. Think of it this way- the higher the Stratum Level designation/number (i.e.: 4), the more frame slips will occur in the transmission equipment. What does this matter? Table 1 below provides a glimpse.

Remember, Stratum 1 is as good as it gets, followed by lesser quality Stratum 2, lesser still quality Stratum 3, and much lesser quality Stratum 4. This is like your golf score- lower numbers are the goal.

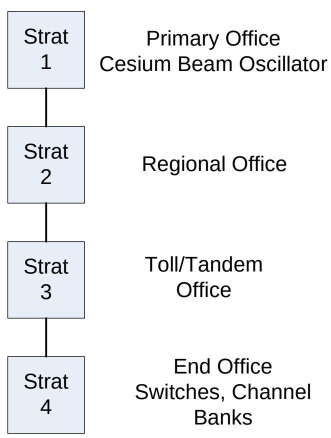


Fig. 8
Stratum Levels- by office

SERVICE	EFFECT of SLIPS
Voice-compressed	A slip will cause a click
Facsimile	A slip can wipe out several lines
Modem	A slip can cause several seconds of dropout
Compressed video or Video Conferencing	A slip can wipe out several lines. More slips can freeze frames for several seconds
Encrypted data protocol	Slips will reduce transmission throughput. Loss of key
Packet data	Loss of packets, resulting in degraded throughput and re-transmission delays
SS7 Networks	Errored data

Table 1
Effects of Frame Slips [1.4]

Since GPS-based BITS systems are widely deployed, End Office locations now enjoy the same Stratum Level as peer and Primary Offices. However, Network Synchronization does not end at the local Central Office/End Office.

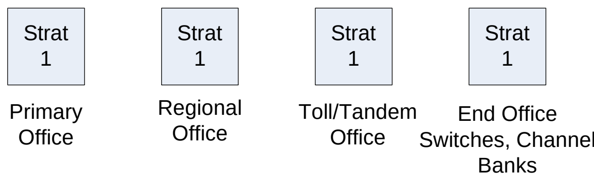


Fig. 9
Stratum Levels on Par

Network Synchronization Includes the Customer Loop
As new services and bandwidth requirements increased, T1 and fiber optic transmission systems were extended to customer locations. The customer, in turn, connected terminal equipment of equal complexity, often subscribing to service from multiple carriers. In many cases, ring-based, self-healing fiber optic networks deliver optimal reliability in the customer loop. Therefore, transmission systems beyond the local End Office must be included in Synchronization Planning.

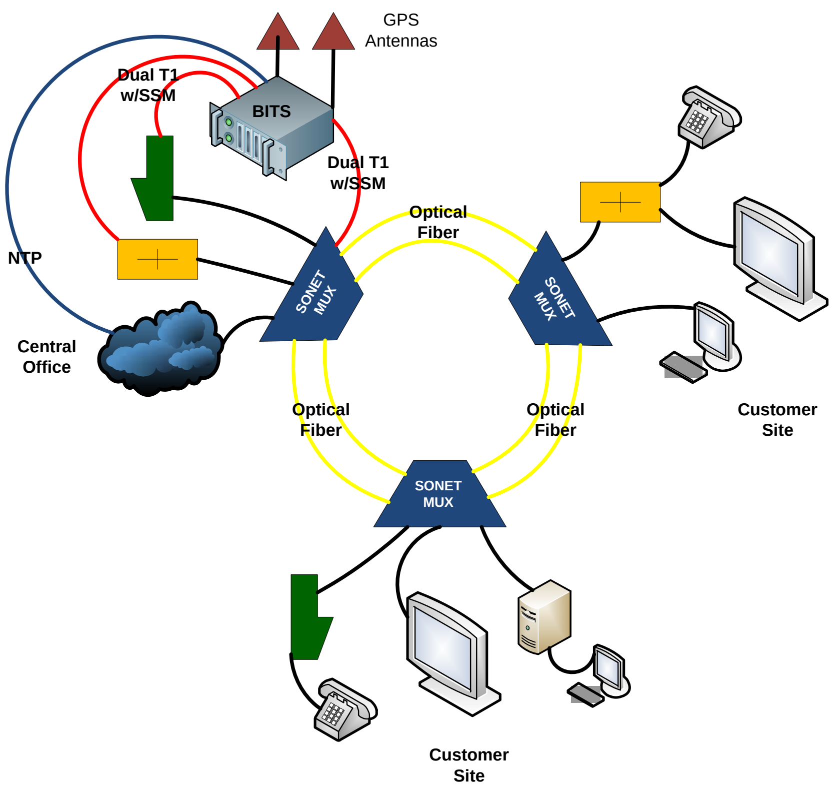


Fig. 10
Sync of Customer Loops

1.5 Anatomy of a BITS Clock

This overview will equip the reader with concepts of a Building Integrated Timing Supply (BITS) system. Though BITS systems vary in complexity, they really perform several simple tasks. Here's a block drawing of a basic system:

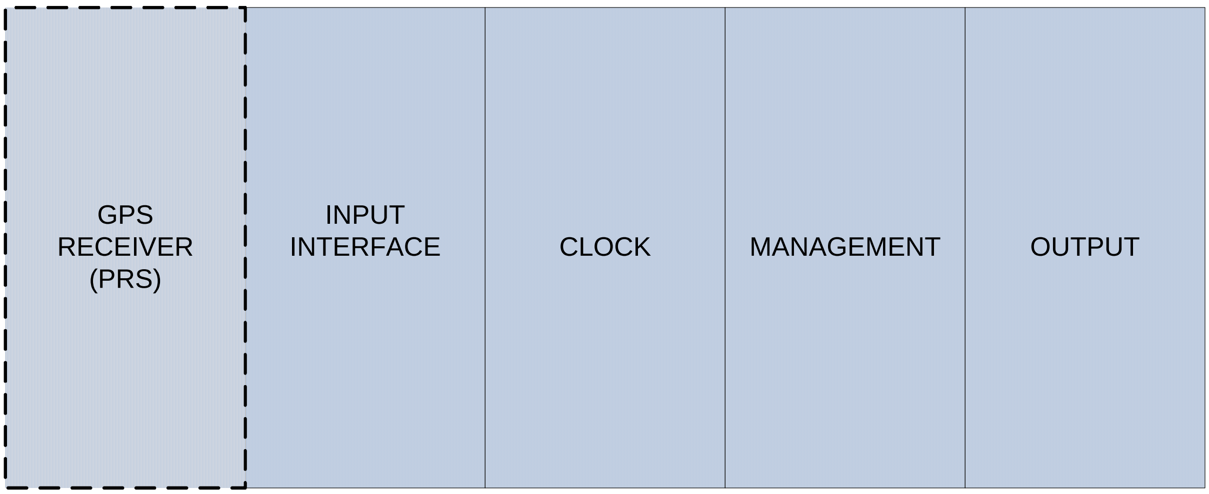


Fig. 11
Basic BITS Clock

1.5.1 The *GPS RECEIVER* section contains one or two identical receiver units that provide power to the active GPS antenna, decode signals from multiple GPS satellites, and convert the data into reference signals and time stamps that will be distributed by various output ports. The decoded GPS data and signals are first presented to the *INPUT INTERFACE* for further processing.

There are two configurations for BITS systems: those with integrated *GPS RECEIVERS*; those with separate *GPS RECEIVERS*. Since even separated *GPS RECEIVERS* are usually mounted atop the BITS shelf, we will consider them as a whole. The reason they are separate in large systems is that several distribution shelves may make use of the same *GPS RECEIVERS*. The separate *GPS RECEIVERS* may also be labeled *Primary Reference Source (PRS)*, as the literally are the primary source of Stratum 1 for the office. Some *PRS* systems also contain their own holdover oscillator(s), apart from what may be in the BITS shelf.

1.5.2 The *INPUT INTERFACE* allows several types of signals to "drive" the system, including single or dual GPS, T1, E1 or Composite Clock (CC) and 5MHz or 10MHz from another BITS system or Stratum 1 source. However, other than GPS, all other input signals must be traceable to (originate from) a Stratum 1 source or equiv.

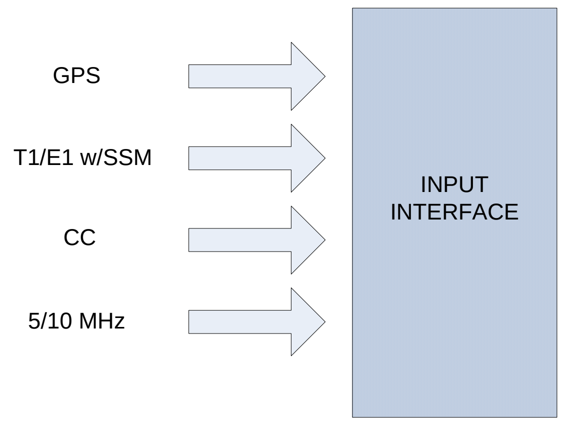


Fig. 12
BITS Clock
Input Interface

1.5.3 The *INPUT INTERFACE*, *CLOCK* and *MANAGEMENT* sections all work together to determine the best available reference for maintaining stable outputs, with a default "pecking order". The priority list assumes: GPS is reliable and the external T1/E1 or other signal is from reliable source. While you may change the list in software, typical default is:

1st PRIORITY	GPS
2nd PRIORITY	External Signal
3rd PRIORITY	Internal Holdover Oscillator
4th PRIORITY	Free Run

Table 2
BITS Input Priority [1.5]

Therefore, if a GPS signal is present, that is first priority and is Stratum 1. If GPS fails, the external input may be considered the next best source. This depends on a couple considerations. Over a period of hours/days, the BITS system will compare the External Signal with the GPS reference. If the signal is of sufficient quality, the system will maintain it in the priority list. Additionally, if the signal is a T1 or E1 with SSM, the system can immediately determine the traceability to a BITS source. This will be explained in detail in the next section.

1.5.4 If neither GPS nor External Signal is acceptable, the system will fall back to HOLDOVER. Holdover quality is based on the type of Holdover Oscillator installed in the system. If the GPS or External Signal is not restored within the range of the Holdover Oscillator, the system will degrade to FREE RUN condition. This is to say the output signals are likely at or below Stratum 4 and troubles at the local office are likely. Even though the system is in FREE RUN, at least all the outputs of the same BITS system are pretty close in quality. However, that creates additional problems when SONET equipment is used, as SONET elements contain an internal Stratum 3 clock which may be better than the FREE RUN BITS signals supplied. Again, you will soon discover how the use of SSM can aide in such situations.

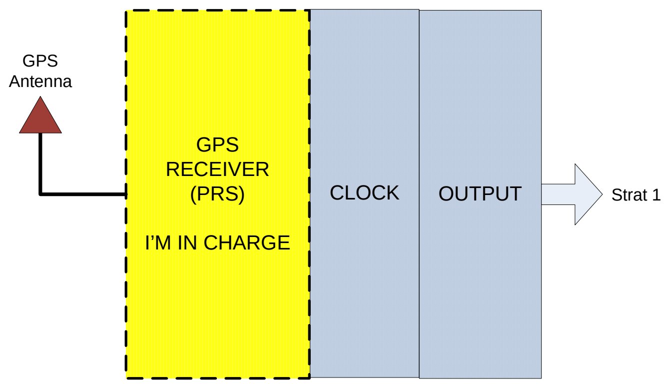


Fig. 13
Output with good GPS/Inputs

The *CLOCK* section contains the backup oscillators which can "Holdover" the quality of the BITS outputs over time. For example, if you lost both GPS and the external signal, the Holdover Oscillation would maintain as near Stratum 1 as possible. A Rubidium oscillator can hold outputs to Stratum 2 or 2e (almost Stratum 1, but not quite), while oven-controlled crystal oscillator can hold outputs to Stratum 3 or 3e (almost Stratum 2).

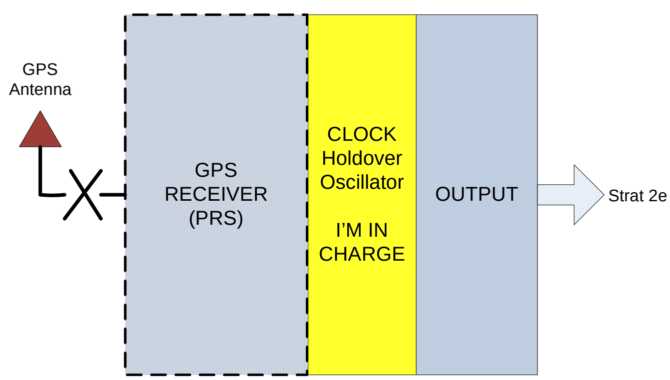


Fig. 14
Output with failed GPS/Inputs

There is a big difference in cost between rubidium and crystal oscillators, so some logic behind which is best for you:

If your system contains two GPS receivers, then you have one layer of redundancy. In other words, both GPS receivers, antennas or antenna cables would have to fail before any of the holdover oscillators would be utilized.

However, if both GPS receivers failed, a rubidium oscillator would "Holdover" at just less than Stratum 1 for several weeks unit you could repair the receiver, antenna or cabling. A crystal oscillator would "Holdover" several days, but at a lower Stratum level than rubidium. Therefore, rubidium buys you longer holdover at higher quality than crystal oscillators.

Some companies equip BITS systems with two of every critical component- two antennas, two receivers, two oscillators, two output ports per connected element. This is called *Full Redundancy*. However, before the second oscillator would be used, both receivers and the primary oscillator would have to fail, so in some cases, it may be appropriate to have a primary rubidium and secondary crystal holdover oscillator. It is highly unlikely (but not impossible) that the secondary oscillator would ever have to carry the day. The decisions for the number and type of receivers and oscillators are governed by your company guidelines and may vary by site.

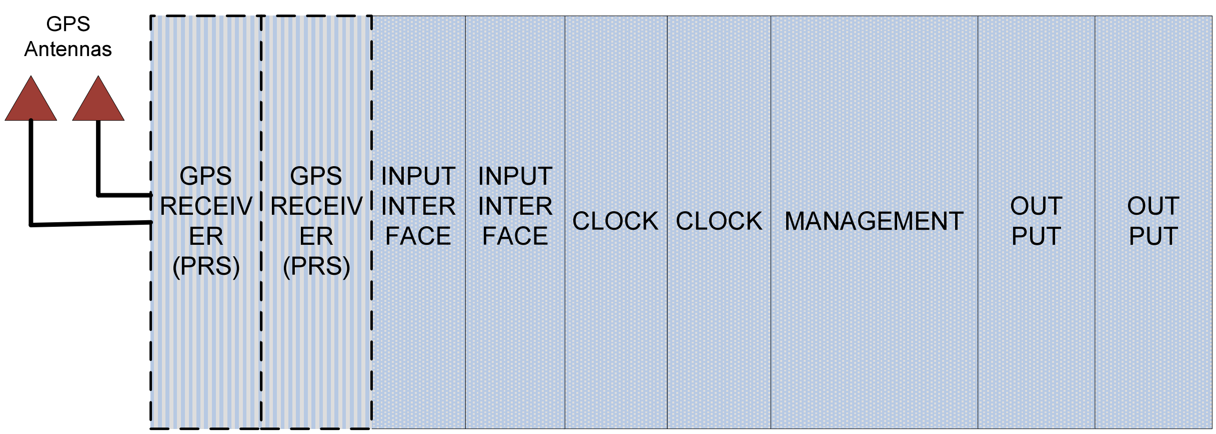


Fig. 15
Redundant BITS System

1.5.5 The *MANAGEMENT* section of a BITS system is pretty self-evident. That is, it allows communications via Serial and/or Ethernet ports, offers configuration menus, manages and displays (sends) alarms and generally keeps track of the rest of the system.

The *MANAGEMENT* section provides a means for performing simple or exhaustive diagnostics on the BITS system. The most commonly used commands analyze the integrity of the antenna circuit for proper operation; display the number of GPS satellites "seen" and the value of the received signals for timing purposes; the length of time the system has remained at Stratum 1; and other critical issues like condition and status of holdover oscillators.

1.5.6 Finally, the *OUTPUT* section provides physical access for connecting jumpers or cables to each connected Network Element. The outputs generally have been wire-wrap pins, but a variety of modular connector types are in use, including individual female RJ45 or BNC connectors.

There is a very wide variety of output types, including T1, E1, Composite Clock (CC), 5/10MHz, 2.048 MHz square wave, RS422/1.5MHz, RS422/8KHz, 1PPS, IRIG-B, NTP, PTP and more! How do you know which output is right for each Network Element? Consult the user's manual!

There are four ways to connect Network Equipment to the BITS system: *Unprotected, Protected Port, Protected Full, and Timing Insertion.*

1.5.6.1 *Unprotected Mode* means that the Network Element has only one Sync Input connector (Channel Bank for example), and does not warrant redundant card protection. In this case, an output card, sync cable or Sync Input failure would result in sync loss to the Network Element. While this was standard practice over the years, many companies now demand at least *Protected Port Mode.*

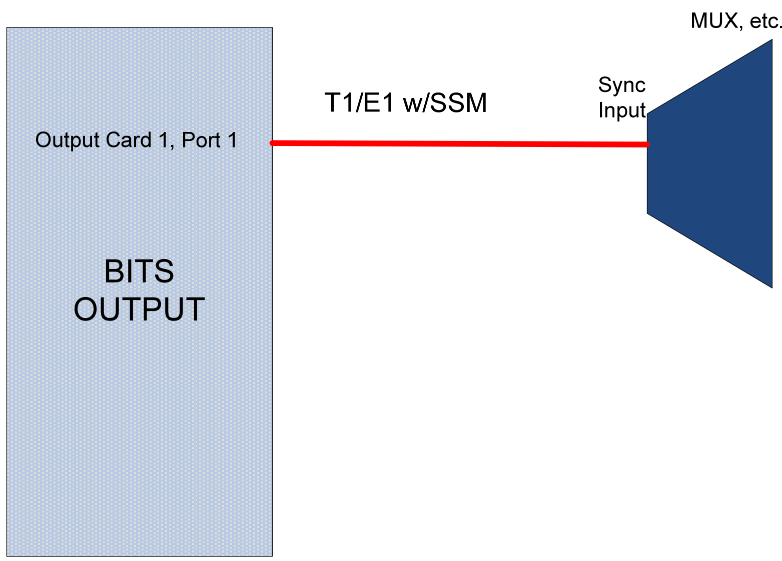


Fig. 16
Unprotected Mode

1.5.6.2 As stated above, most companies require single input Network Elements to be protected at least at the card level. This means the primary output is coupled (internally or via a "Y" cable) to an output of the same type on an adjacent output card. The outputs work as a pair, with one working and the other in standby mode. In event of failure, the secondary card is quickly activated so that sync is maintained to the Network Element. NOTE- generally, protected card arrangements must be configured in the BITS shelf with specific outputs assigned. Some systems do offer automatic protection of cards without the need for "Y" cables. Consult User's Manuals. Also, make sure the selected outputs are configured prior to connecting any "Y" cables, or you will be shorting live outputs together which may result in card damage. This is called *Protected Port Mode*.

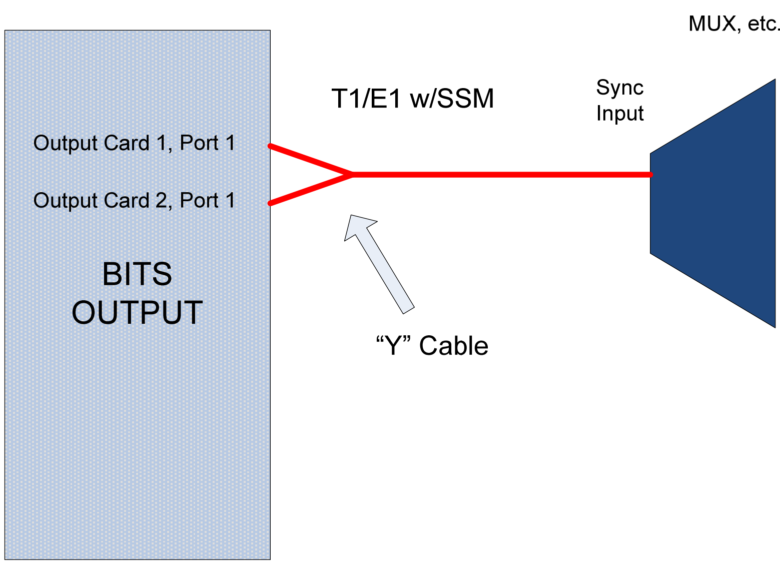


Fig. 17
Protected Port Mode

1.5.6.3 In *Protected Full Mode*, the Network Element will have two Sync Input connectors (example: Input A & Input B or Input 1 & Input 2). These may be wire-wrap or RJ-type connectors. The BITS outputs are taken from adjacent output cards, but the ports are not set up as *Protected Port*. Rather, the Network Element has two independent sync links so that in event a BITS card or cable fails, the second sync input is unaffected. In this case, both BITS links are active all the time. This is the most preferred method for connecting Network Elements to a BITS system.

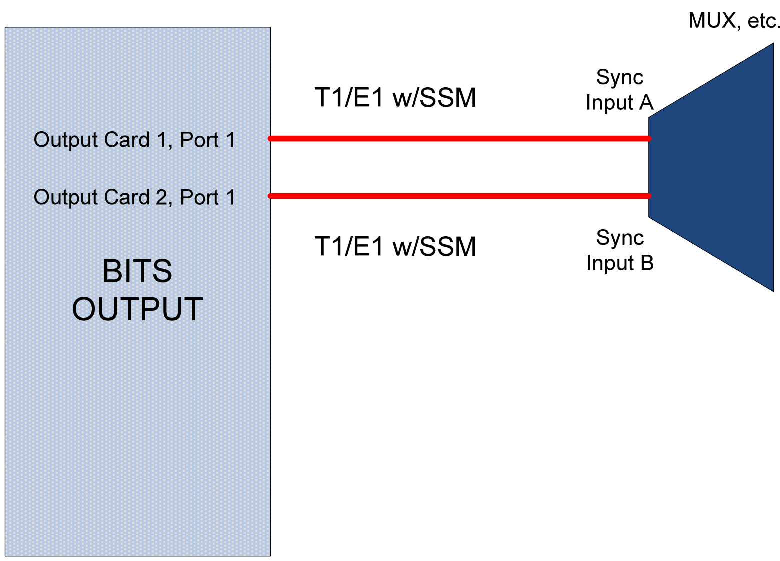


Fig. 18
Protected Full Mode

1.5.6.4 *Timing Insertion Mode* allows Network Equipment that has no external sync port (no extra pins used just for sync input) to be brought into the same level of synchronization as adjacent Network Elements that have dedicated BITS connections.

Basically, the traffic-bearing T1/E1 to the Network Element is looped through the BITS system, where the traffic-bearing T1/E1 is "re-timed". Therefore, the T1/E1 bearer traffic is maintained, but the Network Element is now synchronized with all other Network Elements connected directly to BITS.

To the Engineering purist, "re-timer" is a misnomer; however, it is the accepted term for this mode of synchronization. The more correct term "re-synchronizer" is just too clumsy.

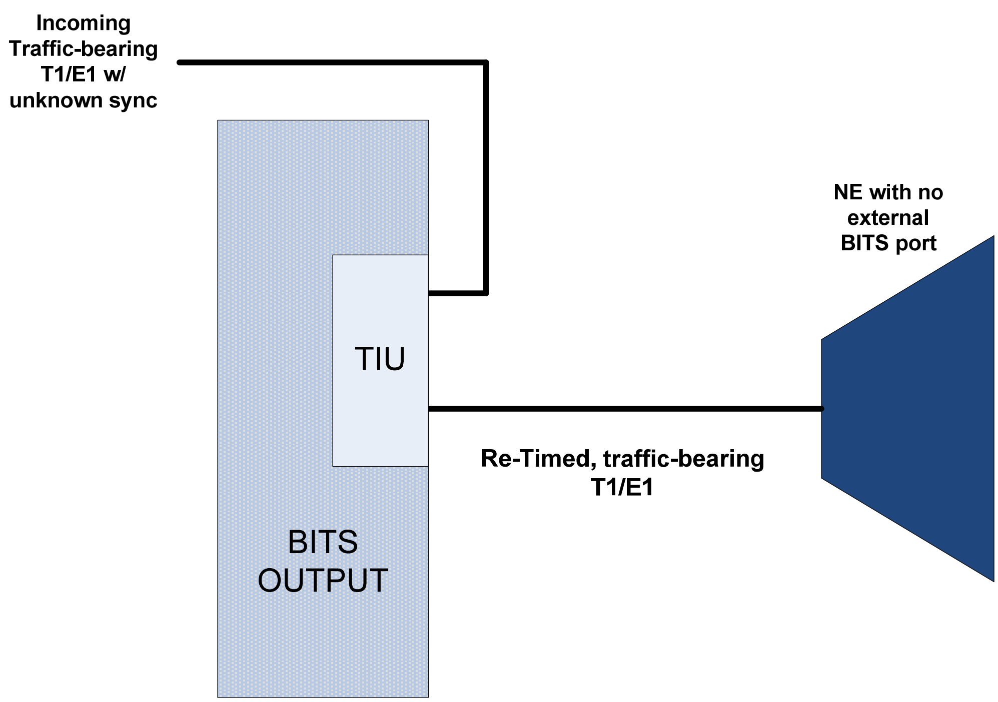


Fig. 19
Re-timer Mode
w/Timing Insertion Unit

1.6 BITS Distribution Shelves

In larger office locations, a single Primary Reference Source (PRS) may provide Stratum 1 links to one or more BITS Distribution shelves. Recall an earlier discussion that there are two configurations for BITS systems: those with integrated *GPS Receivers*; those with separate *GPS Receivers*.

Systems without GPS Receivers are referred to as *BITS Distribution Shelves*. There is no need to install multiple sets of PRS in the same site, so a large building can be surveyed, placing *BITS Distribution Shelves* at strategic locations. For example, *BITS Distributions Shelves* may be installed on each floor of a multi-story building, or at distant ends of a large floorplan. This will be determined by the number and type of BITS outputs required, and the distance from the BITS shelf to the connected Network Elements. This will be reviewed in greater detail in the section "**BITS Installation Considerations**".

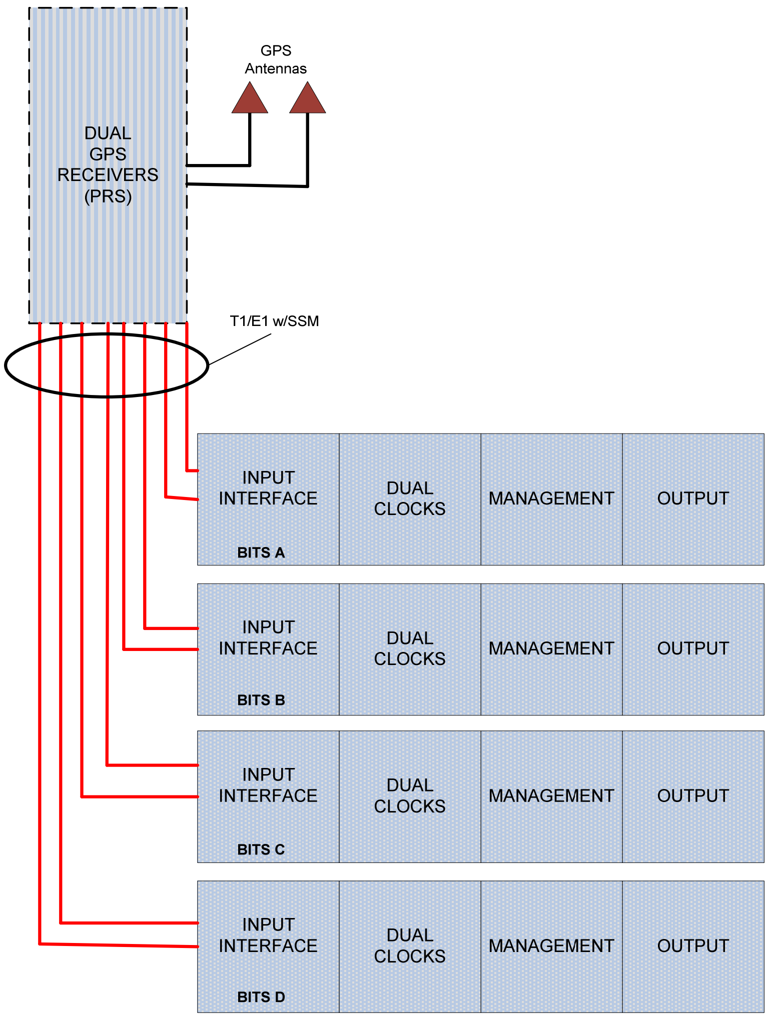


Fig. 20
PRS Serving Multiple
BITS Distribution Shelves

1.7 Sync Status Messaging

Sync Status Messaging (SSM) provides a means for Network Elements downstream from the BITS system to be alerted the Stratum Level of the timing signal. With a system of coded messages transmitted "out-of-band" on a T1 ESF or E1 signal, SSM allows Network Elements to follow an automatic, pre-determined process for selecting the timing source of the highest Stratum Level; thereby eliminating outages due to timing failures. For T1-ESF, the Facility Data Link carriers the SSM codes as shown below.

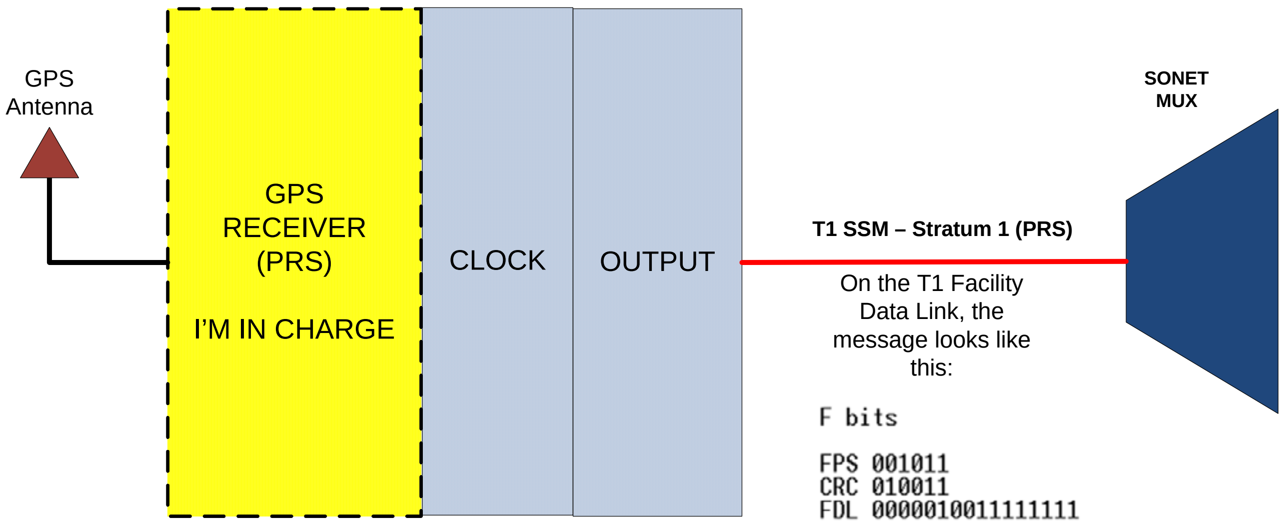


Fig. 21
SSM Message on T1

For SSM to be useful, connected Network Elements must be configured with instructions for actions to be taken in event of degradation of the SSM code. For example, a normal SSM message of Stratum 1 (PRS) indicates the T1 or E1 signal is traceable back to a Stratum 1 source. While the SSM is not a guarantee of signal quality, it can be used to automatically alert connected Network Equipment if the BITS knowingly becomes degraded.

1.7.1 SSM is especially useful in maintaining sync in SONET/PDH rings. The illustration below shows how SSM helps nodes on a ring network make changes to where each node picks timing off the network. With SSM, the ring is able to automatically reconfigure, maintaining synchronization with no technician interaction, offering ample time for repair of the original fault condition.

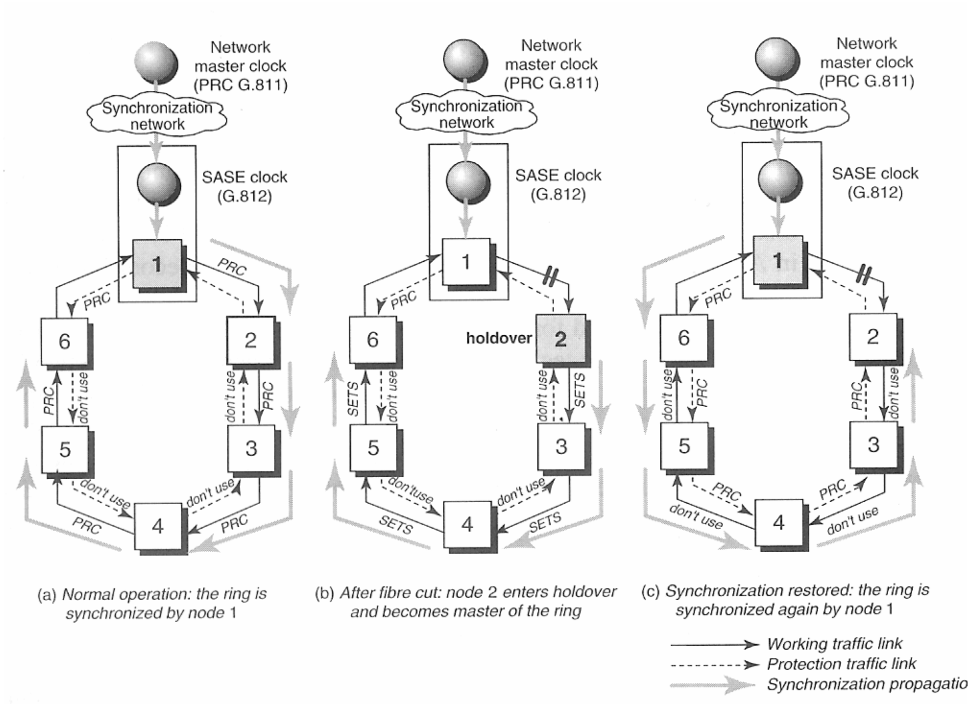


Fig. 22
SSM Messages on SONET/PDH Ring [1.7]

Use of SSM can significantly impact the planning of Network Synchronization, but is fully chronicled in other industry literature. Check **REFERENCES** Section for more information.
The **TROUBLESHOOTING** section will advise site technicians how to "read" SSM in the network.

Again, it is worth noting the SSM does not guaranty signal quality, but does identify traceability. If a T1/E1 signal carries an SSM, then at least it can be traced back to a BITS source at some point. If not, the SSM will say "Don't Use me".

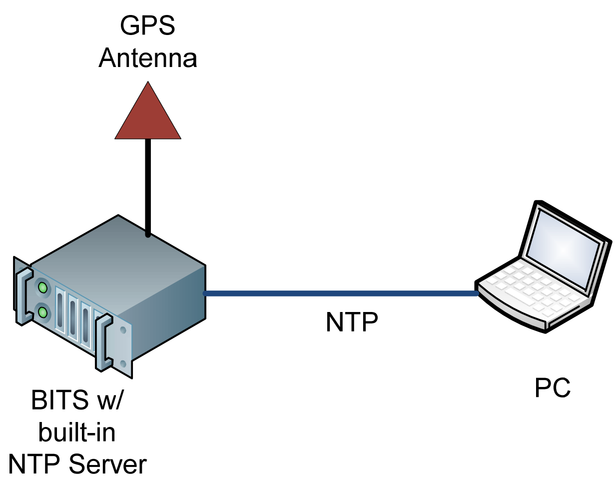
SSM codes are standardized worldwide, so if equipped with a proper Timing Test Set such as the Guisys Model GbB310-RITS, technicians can clearly read the SSM associated with T1 and E1 BITS links. The Gb310-RITS can also evaluate the quality and performance of the T1/E1 BITS link, as well as Composite Clock (CC) BITS links. This will be thoroughly explored in the **TROUBLESHOOTING** section.

1.8 NTP and IP-type Outputs

As discussed earlier, TDM networks traditionally required only T1, E1, Composite Clock (CC) or similar synchronization links to Network Elements. However, it is also useful if some sort of reliable *Time-Stamp* signal could be connected, as this would become very useful when correlating alarm conditions across multiple Network Elements. If the Network Element internal administrative clocks run free, over time they will be a wide spread of accuracy between Network Elements. Alarm events would appear to have occurred at different points in time.

The current preferred method for distributing *Time-Stamps* is the *Network Time Protocol* (NTP). Utilization of NTP requires a host server, and a remote client. In the example shown below, a PC is connected via Ethernet to a NTP server resident in a BITS system. While this explanation is an oversimplification of NTP protocol, the process works like this: PC or remote Network Element sends NTP query to the server with a transmit *Time-Stamp*; server responds with multiple *Time-Stamps.* The query/response contains information elements that allow the client to calculate round-trip delay of the messages, adjusting for the difference and yielding high accuracy as to actual time within milliseconds. The PC repeats this process for as many times as necessary to establish the initial setting, updating at specific periods (once/hour, once/day, once/week based on settings).

If more than one NTP server exists, the NTP client can reference both hosts, further increasing accuracy of the end result. However, for most applications, a single server is adequate.



PC to Server> “What time is it? I asked this question at xx:xx:xx:xx”
Server to PC> “Time is xx:xx:xx:xx; you asked this question xx:xx:xx:xx ago.”
PC to Server> “What time is it? I asked this question at xx:xx:xx:xx”
Server to PC> “Time is xx:xx:xx:xx; you asked this question xx:xx:xx:xx ago.”
PC to Server> “What time is it? I asked this question at xx:xx:xx:xx”
Server to PC> “Time is xx:xx:xx:xx; you asked this question xx:xx:xx:xx ago.”
PC to Server> “What time is it? I asked this question at xx:xx:xx:xx”
Server to PC> “Time is xx:xx:xx:xx; you asked this question xx:xx:xx:xx ago.”
PC to Server> “What time is it? I asked this question at xx:xx:xx:xx”
Server to PC> “Time is xx:xx:xx:xx; you asked this question xx:xx:xx:xx ago.”

Fig. 23
NTP Client-Server Query/Response [1.71]

1.8.1 To better understand NTP, consider the clock in your personal computer. Every PC contains an on-board clock which plods along on its own. This is not an extremely accurate timekeeper, so you may have noticed that over weeks or months the PC clock needs adjusted. Look down into the bottom right corner of your PC screen and observe the time display. If you have several PCs, the time is likely to vary by several minutes or more.

However, modern PCs now contain a small program which utilizes *Network Time Protocol* (NTP) for short which can constantly update the PC internal clock. However, for this program to work properly, the PC must be connected to the Internet at least once per week so it can poll one of several *NTP Servers.* If you double-click the time display, a window will appear titled "Date and Time Properties". Depending on the vintage of your PC (WIN2K and previous are doubtful), you should see three tabs; one allows you to adjust the time and date; a second let's you select the proper time zone; and the third should be labeled "Internet Time".

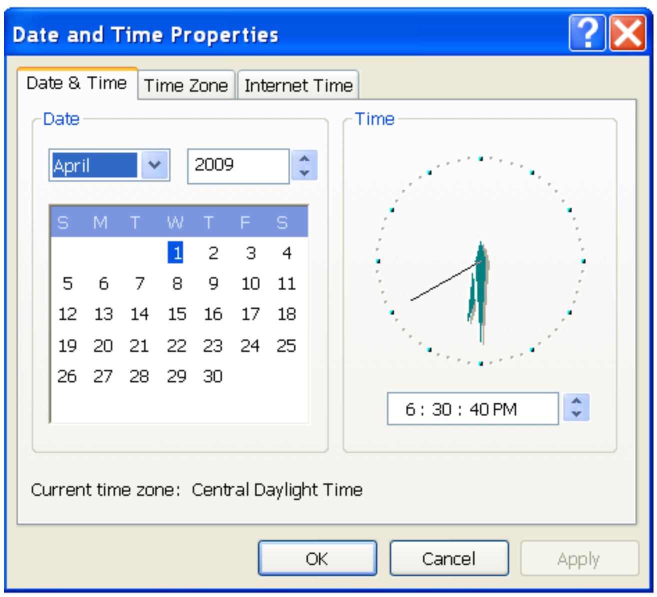


Fig. 24
Windows NTP Setup [1.8]

1.8.2 Click on the Internet Time tab and you can select from a number of sites in a drop-down window the NTP server of choice. In this example, the NTP server maintained by the US National Institute of Standards and Technology is selected. Therefore, at regular intervals (typically once/week), the PC sends an NTP query message to the NTP server, requesting a Time-Stamp. If successful, a message in middle of screen advises the exact time of the update, and also displays the date/time for the next scheduled query. In this case, the PC was updated @ 6:33 PM local time on 4/1/2009, and the next scheduled update will occur at 6:30 PM local time on 4/8/2009. Note you must check the box to automatically synchronize, or you will have to manually click UPDATE NOW at regular intervals of your own choosing.

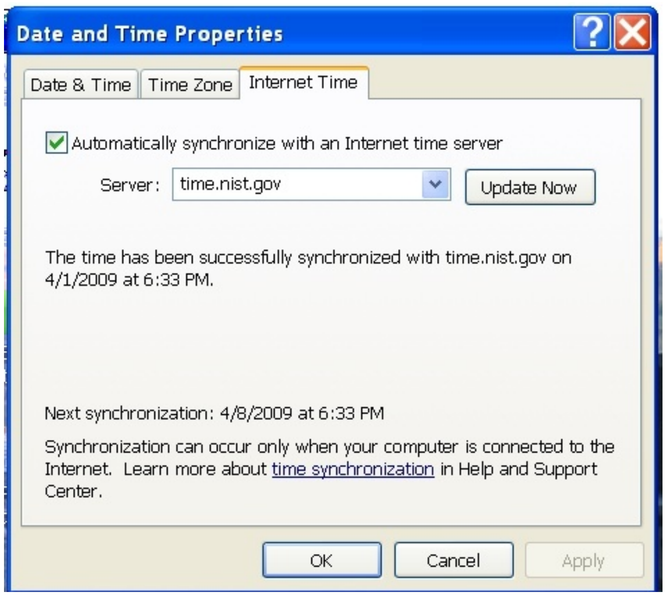


Fig. 25
Configuring Windows Client to
Source a NIST NTP Server [1.9]

It is notable that NTP has been around for a very long time, but has only recently been more widely adopted, deployed and utilized. Over the past several years, Network Providers have grown to rely heavily on NTP for time management of all critical network elements, including call processor records for billing systems, network management devices including routers, Ethernet switches and the management side of all switching and transmission systems.

1.8.3 Need for Reliable Time-Stamps

While you may consider the PC clock to be a mild convenience, consider the benefits of maintaining accuracy of the local clock. Many clients (PC programs) make use of the time stamp for events such as email, bank transactions, stock purchases, ebay activity, etc. Also, Windows uses the clock to maintain files, updates, events so that if needed, critical information can be retrieved to restore from a PC crash. It really is best if you keep the clock current.

1.8.3.1 The use of NTP has grown way beyond simple timekeeping for administrative and maintenance purposes. Reliable *Time-Stamps* form the basis for numerous Network Utilization and Performance measuring tools. Customers now demand some form of proof for network performance, such as availability, throughput and latency. Accurate *Time-Stamps* are the key to delivering real-time reports for network performance. In the drawing below, BITS systems (Tiempo) are used to supply T1 and NTP to appropriate *Pseudo-Wire Emulation* (PWE) Network Elements. PWE is the method for transporting TDM signals like T1 across a packet network.

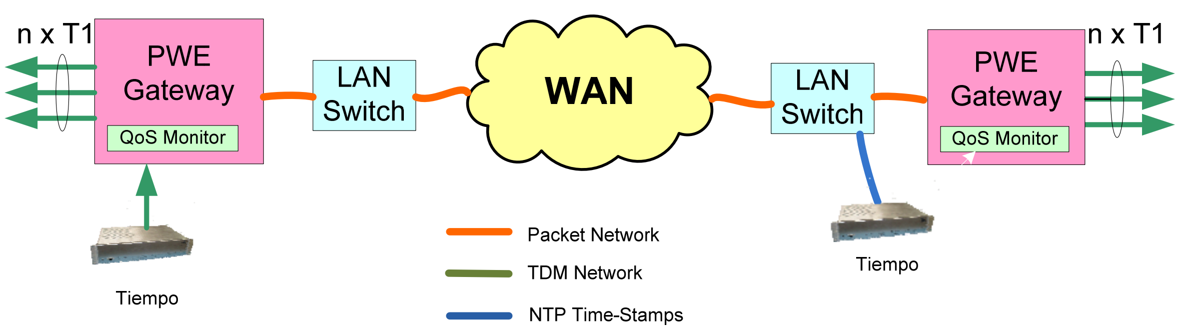


Fig. 26
Maintaining QoS for PWE [1.92]

1.8.4 There are two basic NTP implementations: SNTP and NTP. If you are going to install a single server in a small network (less than 50 or so clients), *Simple Network Time Protocol (SNTP)* will work fine. However, if your plan is larger, serving hundreds of clients (PCs, Network Elements, etc.), then you may need full NTP. Full NTP has many expanded capabilities for discovering adjacent NTP servers, configuration preferences such as ability to serve as a primary or secondary time source, and more. These are fully chronicled elsewhere; check **RESOURSES** section for more info.

In the illustration below, the BITS system contains a SNTP Server function, providing *Time-Stamps* to multiple Network Elements and PCs at the site. It is possible to utilize a NTP server over several "HOPS", however this should be limited to less than 6 HOPS for critical applications.

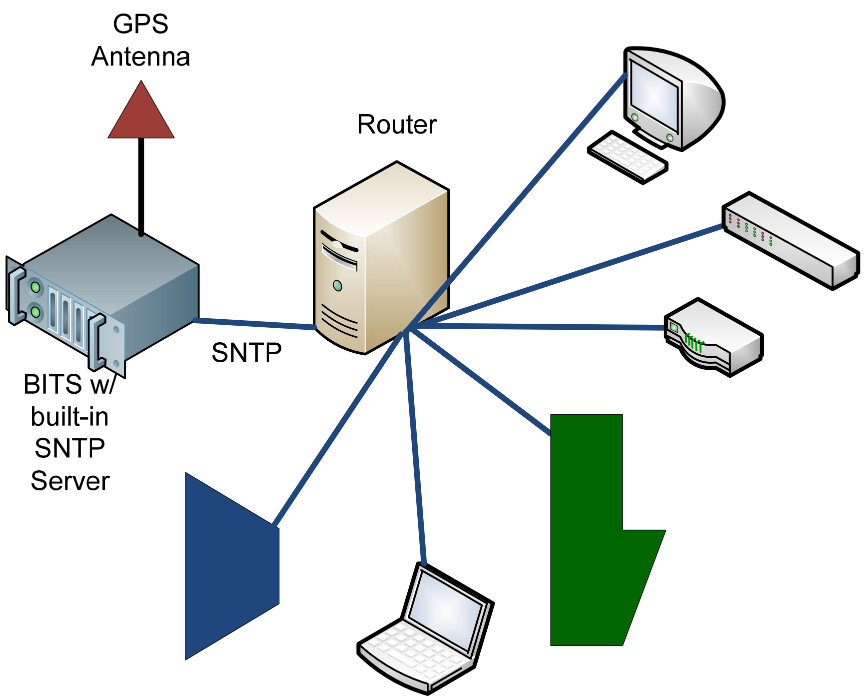


Fig. 27
BITS w/Built-In NTP Server

NTP is most accurate when multiple NTP servers are deployed. One or two servers will source back to GPS, and the remaining servers will poll each other. This mesh configuration creates an extremely stable time reference system which may achieve nanosecond accuracy, with redundancies to eliminate network outages.

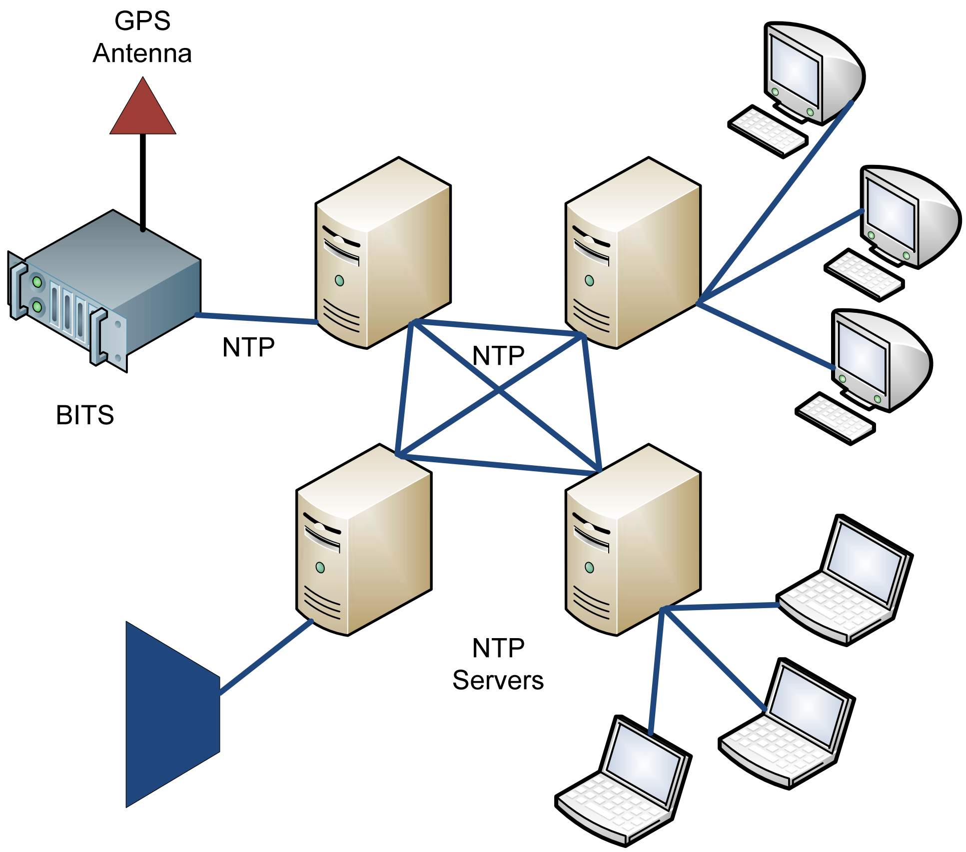


Fig. 28
Multiple NTP Servers

1.8.5 TDM Sync from an IP-Based Network

NTP may also be utilized to provide T1, E1 or other signals to locations where it is not possible or convenient to install an exterior GPS antenna. First, you must establish a site that will be GPS-based and install a BITS system with NTP capabilities. This will be termed a *Grandmaster Clock*. At one or more remote sites, a "very small footprint" Edge Client/Edge BITS device accepts the NTP feed over Ethernet connection, and converts the precision information into stable BITS outputs such as T1, E1, 1Pulse-Per-Second or 5/10MHz.

The benefit of this arrangement is that the Grandmaster Clock is only moderately priced, but the Edge Client devices are usually priced under $2,000. Therefore, one Grandmaster can provide Stratum-quality synchronization signals to a dozen or more end locations served only by your internal Ethernet network.

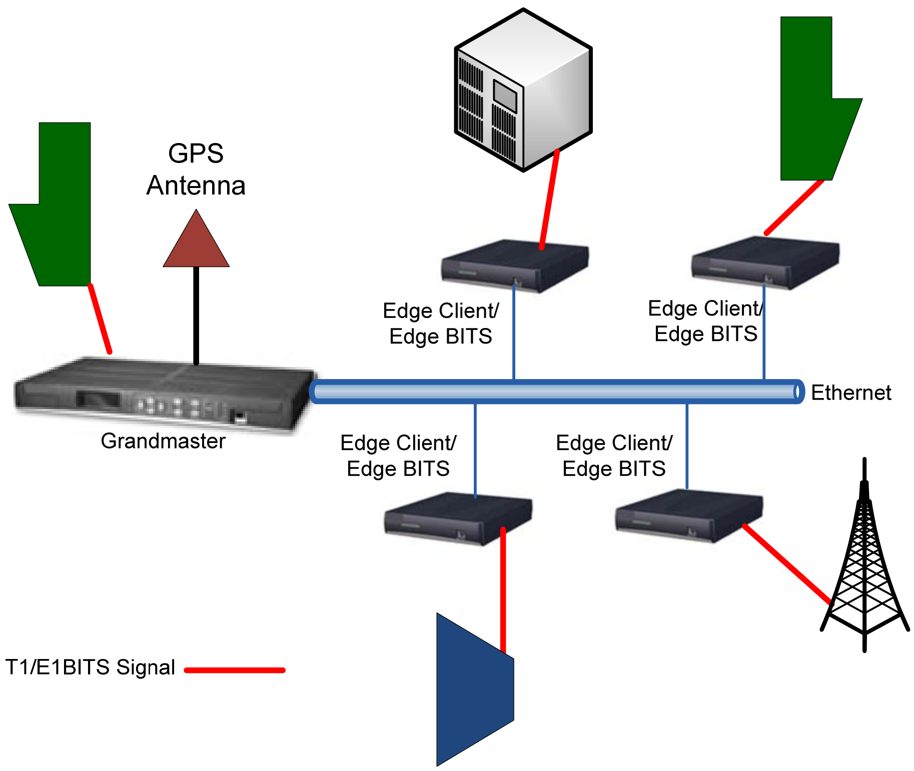


Fig. 29
NTP-to-BITS
via Ethernet [1.93]

1.8.6 Additional Packet-Based Timing

While NTP has been employed over two decades and more widely adopted in recent years, another emerging protocol is shouldering its way to the front of the line. IEEE 1588 v2 (PTP) is nearing completion and already deployed in some form. As with any cutting-edge technology, 1588 "Precision Time Protocol" continues to be refined and improved based on real-world results.

The decision of which time protocol to use will be based on the current and future design of you IP network. NTP may be utilized in almost any network configuration that meets minimal guidelines. However, 1588 requires some additional network topologies and performance enhancements already are in place, such as QoS. Therefore, significant improvements may be required for existing networks. However, when developing a new network, such issues will likely be mute. Timing and Synchronization vendors will gladly assist in reviewing your needs.

If the predominance of your output requirements are Synchronization based (T1/E1, CC, etc.), then the best solution is to add NTP capability to a new or existing BITS system. However, if the majority of your needs are on the IP side, purchasing a GPS-based NTP server is best. Most commercial NTP servers also have a limited number of Synchronization outputs as well, so today you can have both in a single package.

Below is the rear view of a modern combination BITS/NTP system available in ANSI or ETSI versions that may be equipped with single or dual GPS Receivers, up to 2 external inputs, single or dual Rubidium, crystal or mix of Rubidium/crystal holdover oscillators and 64 outputs that can be programmed by port, allowing you to "skinny down" or "fatten up" as needed. The system also offers IP connections for SNMP management and up to two ports of SNTP, and IEEE 1588 v2, all at only 2 Rack Units (RU). Just a few years ago, this same capability would have consumed 10 RU. The SNTP option for this system sells for under US $800. Today there is no reason to buy separate elements for providing Synchronization and Timing outputs.

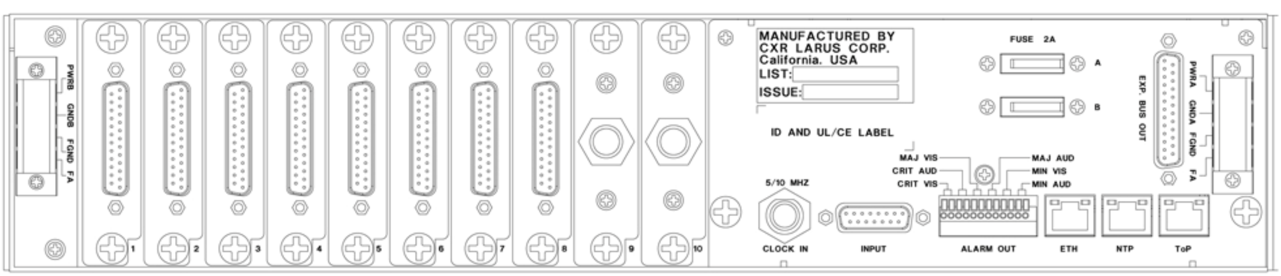


Fig. 30
Modern Combination
BITS/NTP System [1.94]

1.9 BITS Installation Considerations
This section provides an overview of basic considerations for typical BITS system installation at a site. The need for BITS at a location should be driven by Network Planners utilizing an instrument called a *Synchronization Plan* or *Sync Plan*, for short.

1.9.1 The *Sync Plan* should be the guiding reference tool for all BITS installations; decisioning of the BITS type, size and redundancy; connecting of Network Elements; and management/troubleshooting directives.

Routine maintenance of BITS output links does not require access to the *Sync Plan*. Failed output cards or cables, improper output configuration and basic BITS system analysis are pretty logical tasks. If Lightning damages one of the antennas; replace the antenna. If an Output card fails; replace output card. However, persistent, unexplained troubles require a closer look at the entire synchronization strategy. Frequent dropped calls, sporadic errors in 56/64kbps DDS and/or T1/E1circuits, bearer traffic issues on ISDN channels, SS7 failures, unexplained trunk failures and frequent multiple alarms are all indicators that synchronization problems exist.

1.9.2 When contacted for technical support on difficult synchronization troubles, experts will always want a look at the *Sync Plan*. You have to know where synchronization starts (originates) and where it ends (what's connected). It is crucial that *Timing Loops* be identified and corrected, or the entire network will collapse upon a GPS failure. A *Timing Loop* occurs when a BITS system is in some way referencing an input signal that is directly or indirectly derived from one of its own outputs.

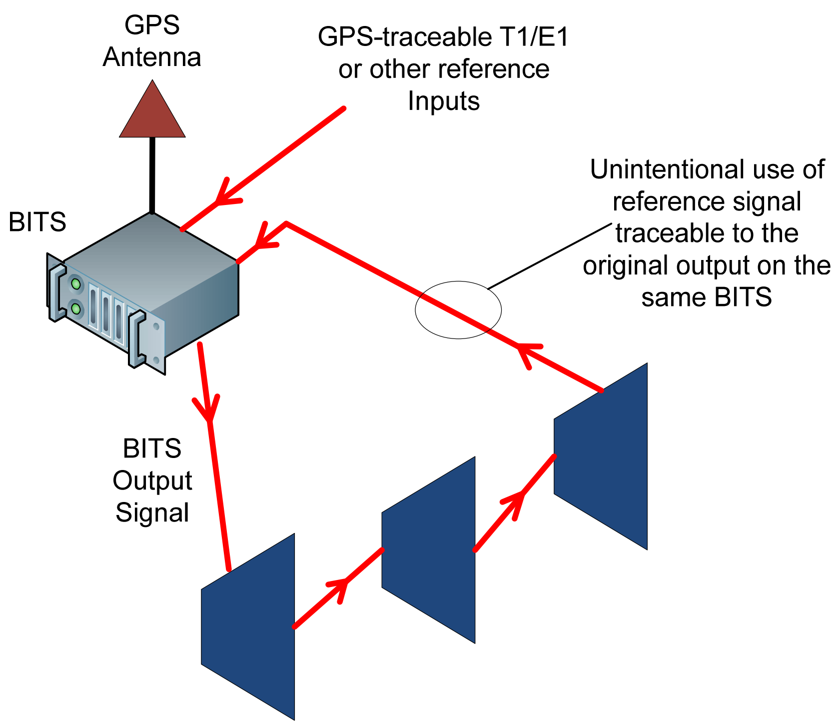


Fig. 31
Timing Loop

1.9.3 What and How Many?
As previously discussed, any BITS installation should be driven by specific dictates of the *Synchronization Plan* (*Sync Plan*). If the office is small with fewer than 64 Network Elements to be connected, a *Site Survey* will provide the details from which a *Sync Plan* may be developed.

1.9.4 A basic site survey consists of an audit of all Network Elements (NEs), determination of the type of synchronization signals required by each NE, availability of suitable power and ventilation, location and suitability of existing grounding scheme for the lightning arrestors, and access to a clear sky view on the outside of the building. From this survey, the Sync Plan will identify the size, type and number of BITS systems required for the site, including redundancy requirements.

Network Element	Type Input Required	Number of Inputs	Additional Input Requirements	Number of Additional Inputs	Distance to BITS
Alcatel Channel Bank	CC	1			30 ft
Alcatel Channel Bank	CC	1			120 ft
Cisco SONET	T1 w/SSM	2	NTP	1	84 ft
5ESS	T1	2			140 ft
Fujitsu DSLAM	CC	2	NTP	1	420 ft
Brand X MUX	LINE-T1	*			35 ft

Fig. 32
BITS Site Survey- NEs

Once the audit of Network Elements is completed, it is a simple thing to tally up the number of required outputs by type. Note in the example above, one Network Element (Brand X MUX) has no external sync input, so will have to be *Line Timed* on the traffic bearing T1. This can be accomplished via a *Timing Insertion Unit* where the traffic bearing T1 is looped into and out of the BITS system.

In most small offices, all Network Elements will be within allowable distance limits from the BITS system. Larger offices, especially with multi-floor buildings will require up to several *BITS Distribution Shelves*. The *BITS Distribution Shelves* have to be engineered so that the allowable output cable distances can be met without violating the distance limits between the *BITS Distribution Shelf* and *Primary Reference Source* locations. These distance limits will be fully explored below.

Redundancy requirements vary and based on each companies synchronization philosophy. Larger companies usually opt for dual antennas, antenna cables, GPS receivers, and holdover oscillators, employing Protected Card or Protected Full output redundancy. For companies with SONET/PDH networks, placement of several non-redundant clocks around the ring may eliminate the need for fully redundant systems at each site.

1.9.5 Historically, redundancy was thought of as ordering two of each critical component within the system proper. However, due to shrinking system footprints, a new concept has emerged called "*Shelf Redundancy*". With *Shelf Redundancy*, you order a non-redundant system times 2, meaning you mount identical systems together, achieving 100% redundancy down to the backplane. You still have two antennas, GPS receivers, holdover oscillators and outputs, they are just associated with completely separate shelves. This arrangement is frequently lower cost that a fully-loaded single-shelf redundant system, as newer technology offers significant improvements in "cost per port" as compared with older "hardened" designs.

1.9.6 Where?
Planning and installing a BITS system into an office is a daunting task. The two prime considerations relate to the distance from a proposed equipment rack (bay) location to the majority of Network Elements to be connected; and the distance from the bay to an outdoor location where GPS antennas will be mounted.

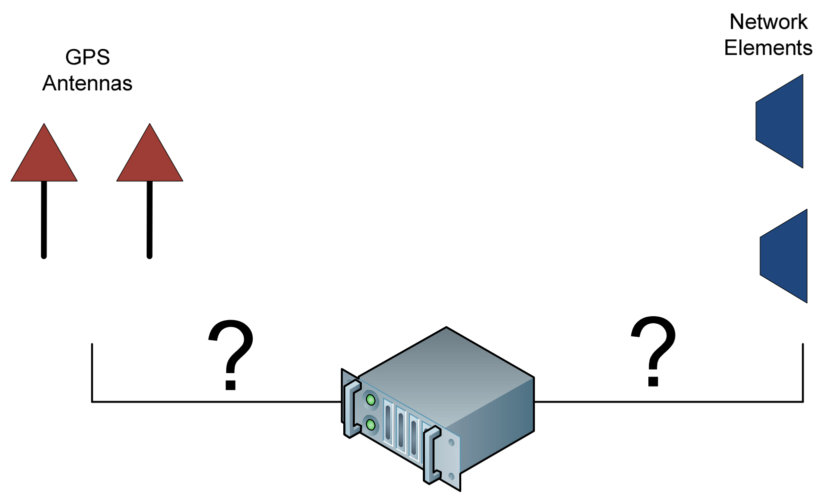
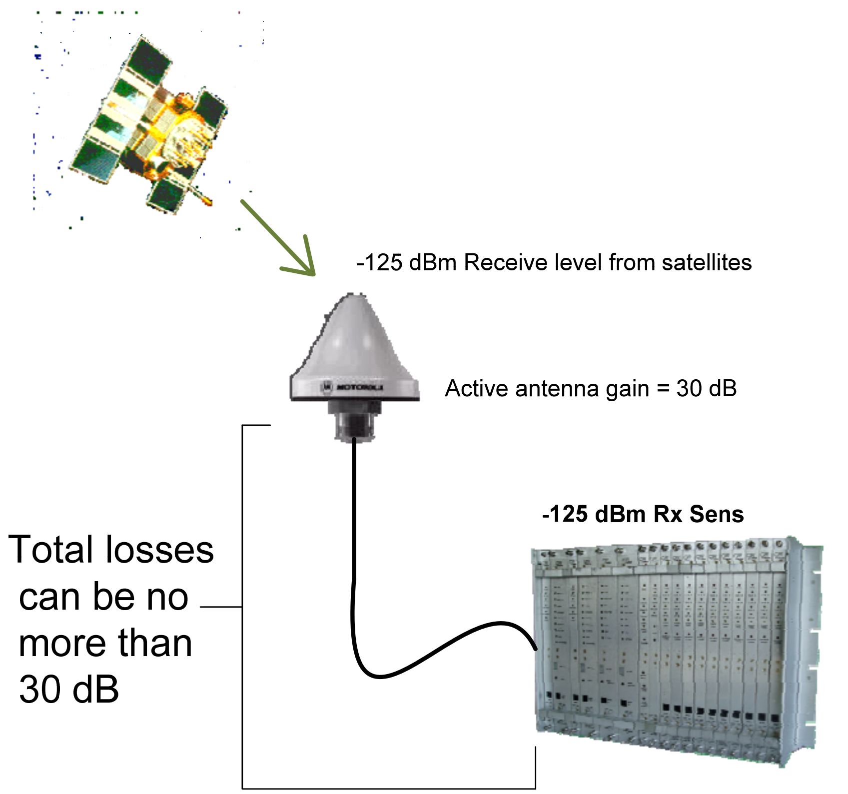


Fig. 33
BITS Location Planning

The most labor-intensive tasks associated with installation of a BITS system relate to: installing antenna and antenna cabling; running cables between BITS outputs and Network Elements. Of the two, antenna installation can be the most difficult, so we will examine these issues first.

1.9.7 GPS signals arrive at the antenna in the neighborhood of -125dBm, which also happens to be near the upper range of sensitivity for GPS Receivers. Most commercial GPS antennas feature 30dB of gain; therefore the loss budget for antenna cabling is also around 30dB. Antenna line loss varies by the size, type and gauge of the cable. For example, coaxial RG-58U cabling burns through most of the 30dB loss budget (with margin) at around 100 feet. This incorporates losses associated with connectors and insertion loss of the Lightning Arrestor and connections. Therefore, antenna runs longer than approximately 100 feet require lower loss cabling such as RG-213U, LMR-400 or LMR-600 based on distance requirements. Alternative schemes are available that utilize fiber optic cabling or frequency conversion units which allow longer runs of RG-58U (up to 1,500 feet).



Cable Type	20 dB Loss*	28 dB Loss*
RG58	70 feet	100 feet
RG213	170 feet	240 feet
Belden 9913	250 feet	350 feet
LMR400	350 feet	490 feet
LMR600	450 feet	630 feet
LMR1700	1,000 feet	1,400 feet

Fig. 34
Antenna Loss Budget [1.95]

The larger size LMR cables can get quite expensive, requiring special tools and skill for installing connectors. At some point there is a cost advantage to installing a down/up converter which will allow cheaper RG-58U cable runs of up to 1,500 feet.

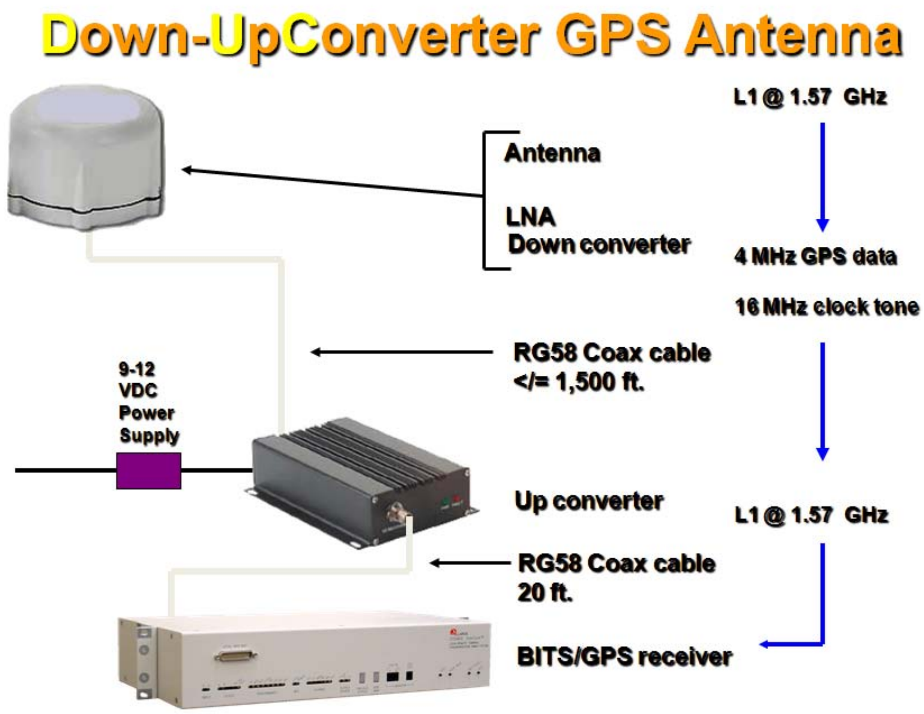


Fig. 35
Down/Up Converter [1.96]

Since longer antenna runs tend to be pricy, some companies economize by installing a single antenna, splitting the signal at the receiver. However, this is extremely unwise, as the antenna is the most likely element to fail over time. One lightning strike would immediately force the BITS system into holdover mode.

Think about it; why would you spend the extra money to install two GPS Receivers, two holdover oscillators and use redundant outputs, yet bet the farm on just one antenna? If the system is to be fully redundant, install one antenna for each GPS Receiver.

1.9.8 Antenna Siting

The most critical step in BITS installations is careful selection of the antenna site. If you get this wrong, the BITS clock will be plagued by intermittent troubles for the life of the system. While it is imperative to adhere strictly to the antenna cable loss budgets, this will be for naught if the antenna is located in the presence of interfering signals or blocked from a clear view of the sky.

Basically, the antennas need to be installed with no less than 30 feet of separation. In fact, use the most separation your cable length will allow. The extra length could save one of the antennas in event of a lightning strike, tree limb, or vandalism (shotgun blast, etc.). Locating antennas away from public view is highly desirable.

The antennas should not be the highest object on the roofline. Rather, they should have a clear view of the sky with an angle of at least 45 degrees, and also a view of the distant horizon if possible. Use of conduits is suggested, mostly to protect the cable from deterioration. Avoid tree branches, radio transmission antennas and low placement on high vertical walls.

Fig. 36
Typical Antenna Installations [1.97]

1.9.9 RF Interference and Metal Surfaces

It is not recommended to locate the antennas near broad metallic surfaces as shown below. The metal can potentially act as a reflector for interfering signals and also be a magnet for lightning strikes. This installation looks beautiful, but should be relocated.

Fig. 37
Avoid Metal Surfaces [1.98]

Do not install GPS antennas near transmitting antennas or high-power antenna feed lines. RF leakage and direct radiation can wipe out or intermittently interfere with the GPS signals, which are at -125dB. Take note of any radiating elements and also beware of "line of sight" path violations where the GPS antenna is placed in the radiating pattern (RF path) of nearby antennas.

If the loss budget is respected, the antennas free of interfering signals and away from broad metal surfaces, and the lightning arrestors properly connected, the BITS clock can provide decades of worry-free service. However, if you break the rules, be prepared for intermittent problems and lots of nighttime work tours.

1.9.10 Antenna Lightning Protection

As previously discussed, the antenna element is the most likely point of failure in a BITS system (excluding configuration errors). It should go without saying that any element that breaches the office walls should be adequately protected from delivering harmful voltages into the equipment room. Failure to do so routinely results in failures as shown below, which can cost upwards of $8,000 to repair.

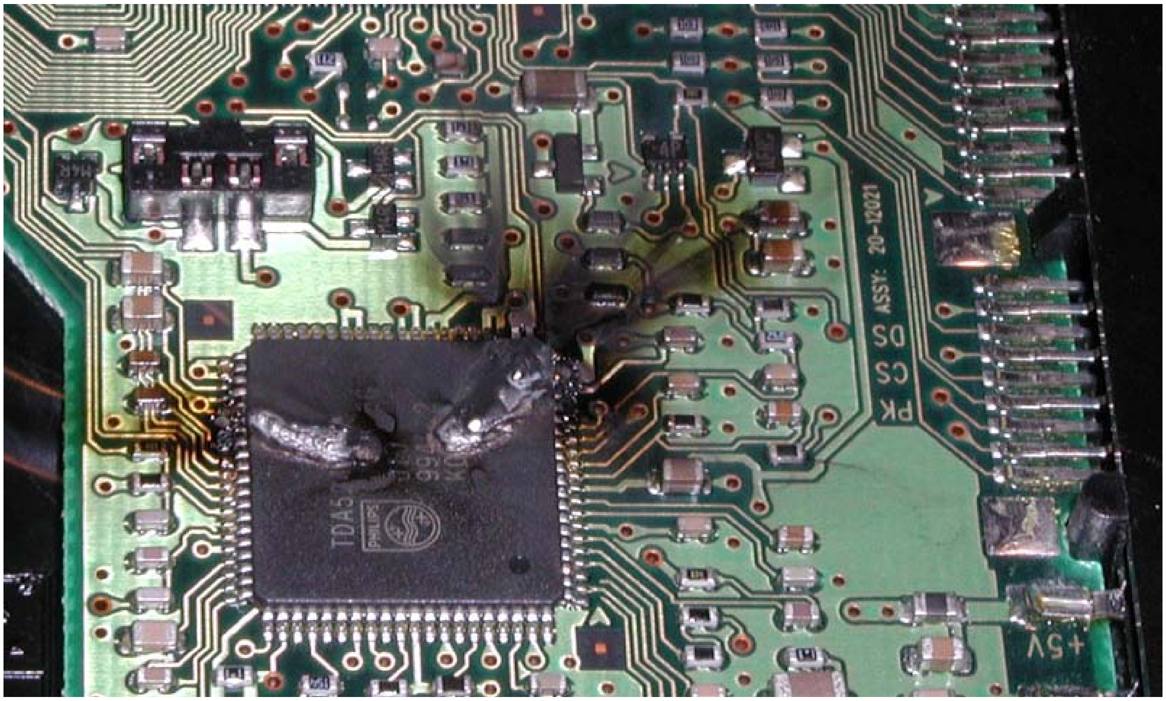


Fig. 38
Result of Inadequate Lightning Protection [1.99]

For active GPS antennas, special protection devices allow normal operation and isolation from ground except the duration of a lightning strike. The isolation and protection elements activate and, if not damaged or destroyed, faithfully return to the previous state.

It is critical to observe the manufacturers recommended installation procedure for lightning protection hardware. Failure to do so could actually increase the chance of permanent damage to the BITS system.

In addition to the manufacturer's instructions, local building codes must also be understood and applied. The subject of grounding is very important and each site likely is equipped with appropriate grounding systems. The building engineer should be consulted to locate the most appropriate grounding connection point for the antenna lightning arrestors. If not appropriately installed, these connections could introduce hazardous and destructive transient voltages into equipment ground circuits. The point is you cannot merely grab any nearby ground; lightning protection grounds are usually routed directly to the main ground buss away from normal equipment grounds. Below is a typical lightning arrestor arrangement. Note the Isolation Ground Adapter which actively ground the shield during a strike.

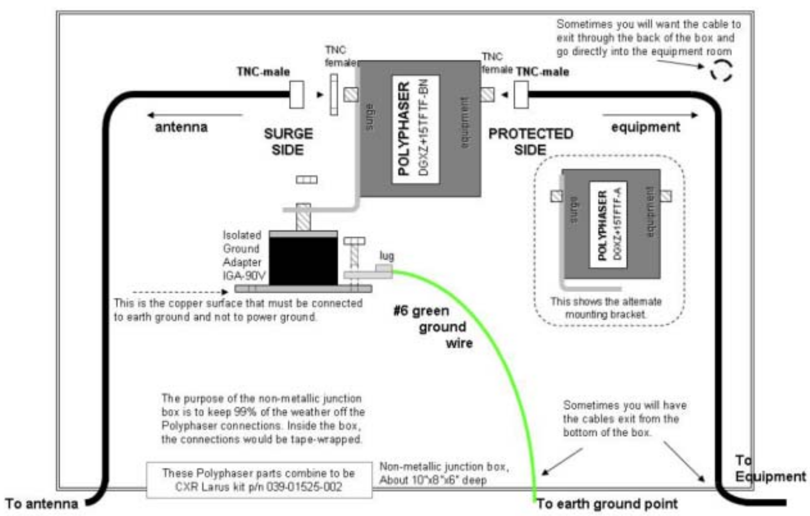


Fig. 39
Lightning Protection Connections [2.0]

1.9.11 Indoors or Outdoors?

Obviously the antennas are placed in an outdoor environment, but what about the lightning protection kit? Experts are split on two approaches: install protection right at the point the antenna cable penetrates the building (outside); install protection at the nearest point the antenna cable enters the building (inside). Both concepts are radically opposed, yet both agree that the point of entry or the wall through which the antenna cable passes is the right spot. This stops the lightning surge from traversing all the way into the equipment room. This will, or course, be governed by local ordinance (codes) and company policy.

Fig. 40
Inside vs. Outside [2.1]

1.9.12 BITS Output Cabling

This section will explore the process for connecting Network Elements to the BITS outputs. Recall our earlier discussion that the *Sync Plan* should drive all requirements for connecting Network Elements, provisioning links and ensuring no *Timing Loops* are constructed. The *Sync Plan* should also yield an assignment record that instructs provisioning out each output, designation of protected paths, and CLLI code or other identifying code for the connected equipment. Some BITS systems offer internal port assignment logs to maintain on-site records. However, this information must be routinely updated or reliability will suffer as the network undergoes rearrangements.

For troubleshooting efforts, nothing is more important than a record of output assignments on a per-card basis.

As previously discussed, each output type carries a set of requirements for staying within the useful range of proper operation. While the main qualifier is cable length, this can be greatly impacted by the size, type and gauge of cabling used to connect the Network Elements. Assuming proper cables installed, typical distance limits are shown below.

Output Type	Distance Limit
T1	130 feet
E1	100 feet
CC- Composite Clock	1,500 feet
2.048 MHz Square Wave	100 feet
RS422- 1.5 MHz	130 feet
RS422- 8 KHz	1,500 feet
5/10 MHz	30 feet

Table 3
Output Limits

For T1/E1 connections, it is important to employ a suitable cable which is rated for T1/E1 signals. Inexpensive fine-gauge UTP will yield poor results. The suggested cable is two conductor twisted pair, shielded, 22-gauge solid copper with a *drain wire*. A drain wire is a bare, solid copper wire that is wrapped tightly against, but outside the shield. The wire connects to a grounding point at the Network Element to eliminate noise and signals which may be couple to the cable. In most cases, the drain wire is not attached at the BITS end, but is insulated with heat shrink tubing. Unless dictated by local code or company policy, it is not recommended that both ends be grounded, as this will result in a ground loop that may actually cause more noise to be coupled to the inner wires.

When it comes to selection of wire types, check the manufacturer's recommendations, as they likely have tested their equipment with many cable types and best positioned to provide this information. The distance limits shown above are for general planning and may vary based on the type of output cards installed. However, installing longer runs of cable than permitted will significantly degrade the signal, which could lead to intermittent operation.

For existing installations, this may pose a problem, as the existing wiring may have been in place for many years. In this case, use of a test set to measure the quality and usefulness of the signal is in order. This will be fully explained in the **TROUBLESHOOTING** section.

1.9.13 Connecting BITS to Network Elements

Multiple wiring schemes may be encountered when connecting cables to BITS systems. For many years, wire-wrap was the preferred method and many modern systems have maintained that feature. The production system shown below has rows of familiar wire-wrap pins for connecting up to 200 output cables.

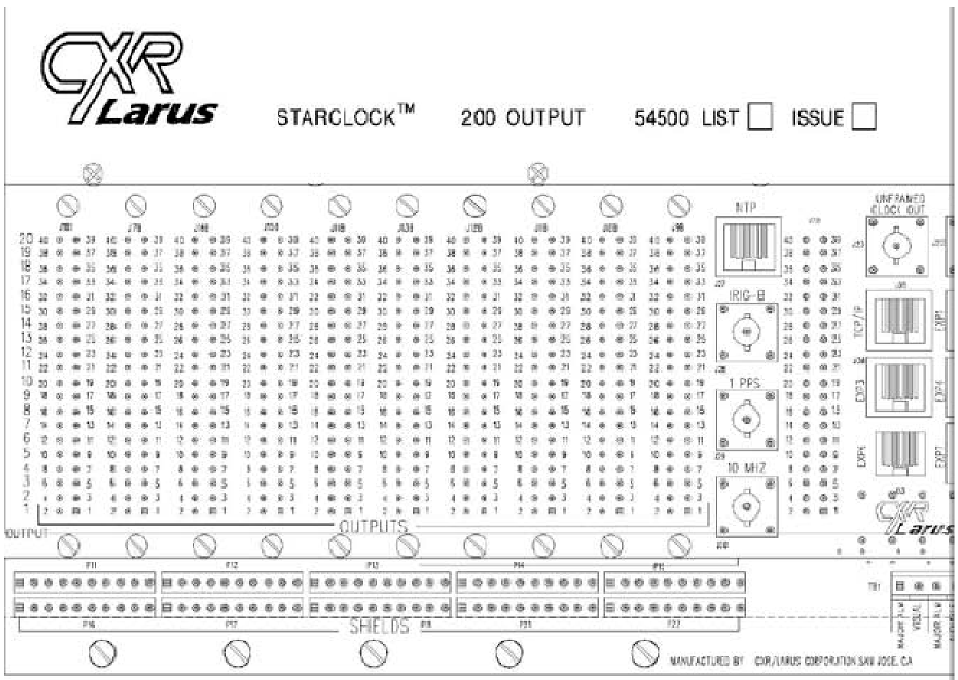


Fig. 41
Wire Wrap Directly
to BITS Shelf [2.2]

In addition to wire-wrap, some systems offer convenient connectors so that customers can install appropriate cables to test jacks or frame locations. One popular connector is a 25-pair variety commonly found in the Telco world. However, with appropriate adapter, you can also convert this connector to wire-wrap as shown below.

Fig. 42
Wire Wrap Adapter

1.9.14 To aide in troubleshooting efforts, many companies also wire BITS Outputs through test points such as Digital Signal Cross-connect (DSX) panels. The BITS Output circuit can quickly be monitored with a test set for repair efforts. As shown below, the BITS Output signal can be wired through the DSX panel so that Monitoring, Testing or Patching can be quickly achieved, greatly reducing troubleshooting time.

This process fully described in T**roubleshooting** section.

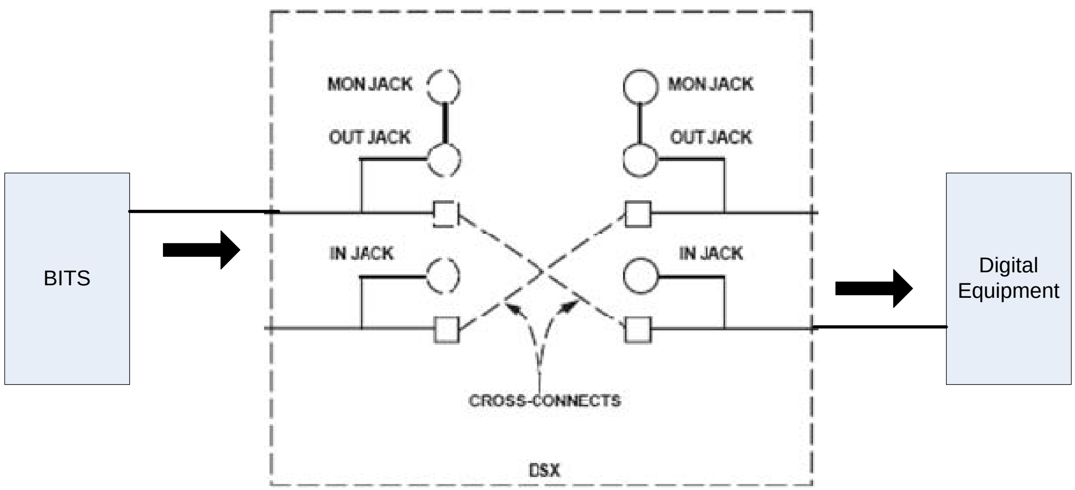


Fig. 43
DSX Panel Wiring Scheme

Two basic types of DSX Panels are prevalent: Bantam Jack and RJ45 Jack. Both types are shown below.

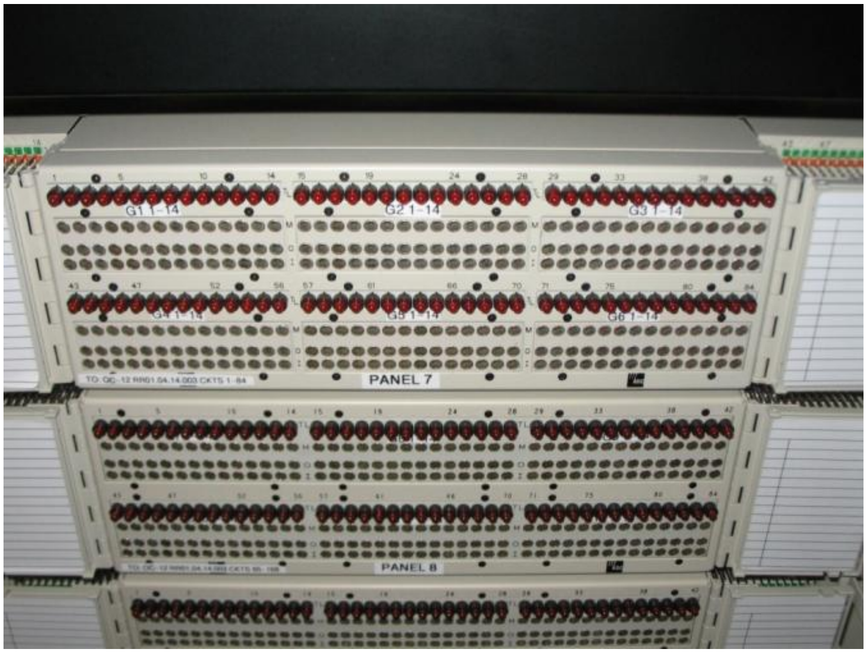
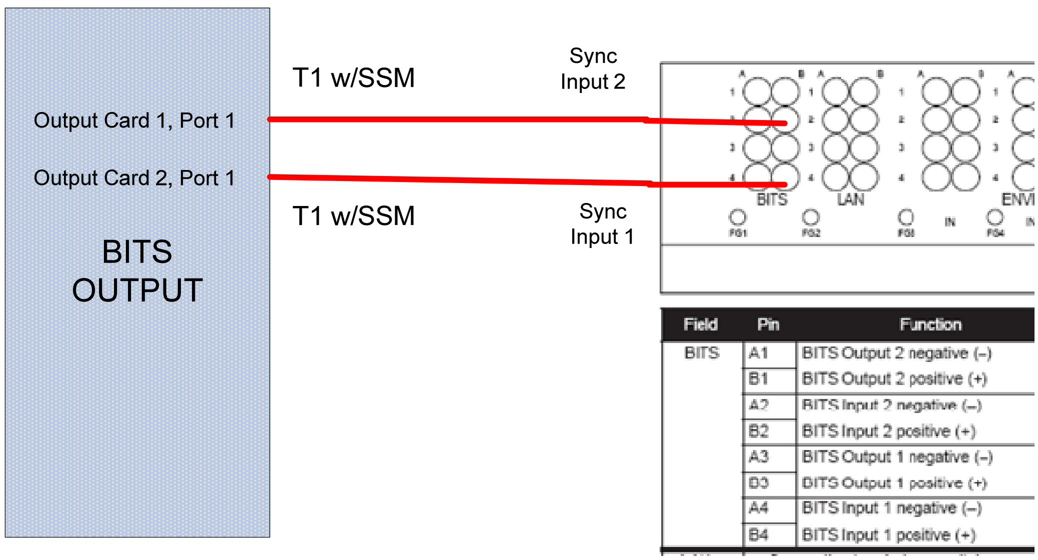


Fig. 44
DSX Panel with Bantam Jacks

Fig. 45
DSX Panel with RJ45 Jacks

1.9.15 The drawing below is typical for SONET/PDH transmission equipment connections. Note this Network Element has connections for two BITS inputs (BITS Input 1 & BITS Input 2) for Protected Full Mode operation. The BITS connection matrix is shown below the connecting pins. Review the matrix carefully. What pins would you naturally assume would be used? In this example, the primary BITS cable would tie down on pins A4 & B4 (BITS Input 1). The secondary BITS cable would tie down on pins A2 & B2.



Field	Pin	Function
BITS	A1	BITS Output 2 negative (–)
	B1	BITS Output 2 positive (+)
	A2	BITS Input 2 negative (–)
	B2	BITS Input 2 positive (+)
	A3	BITS Output 1 negative (–)
	B3	BITS Output 1 positive (+)
	A4	BITS Input 1 negative (–)
	B4	BITS Input 1 positive (+)

Fig. 46
SONET/PDH BITS Connections
Local End

In the above example, a SONET/PDH system is used to carry sync to a distant location (off-site), where the T1 sync signals (two T1 circuits extended from the local BITS) will serve as the inputs to the remote BITS shelf. No GPS Receivers were installed into the far end, the BITS is served by T1's only. Only T1 sync links are shown. They provide only sync and do not carry customer traffic.

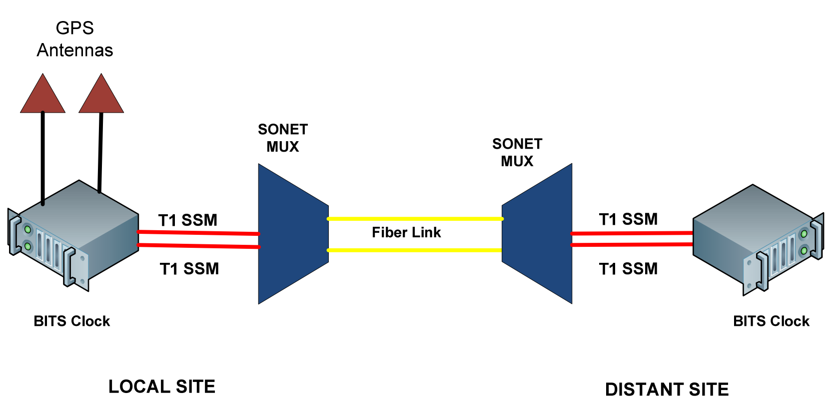
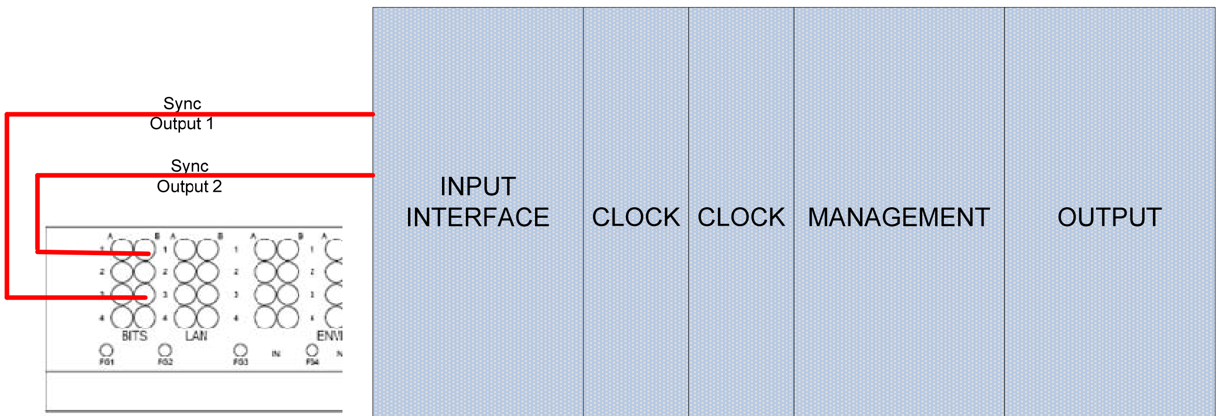


Fig. 47
Transport of BITS Signals

Note that pins A3 & B3 are labeled BITS Output, which would be utilized in cases where the SONET/PDH systems was used to “carry” BITS timing off-site to a distant location. In this case, the SONET/PDH node at the distant site could be used to provide BITS timing to other equipment at that location. At the distant site, BITS Output 1 would pass on the T1 sync signal that was connected to BITS Input 1 at the near end (where the SONET/PDH Node is connected directly to the BITS system). Likewise, pins A1 & B1 at the distant site would pass on (output) the T1 sync signal that was connected to pins A2 & B2 at the near end.



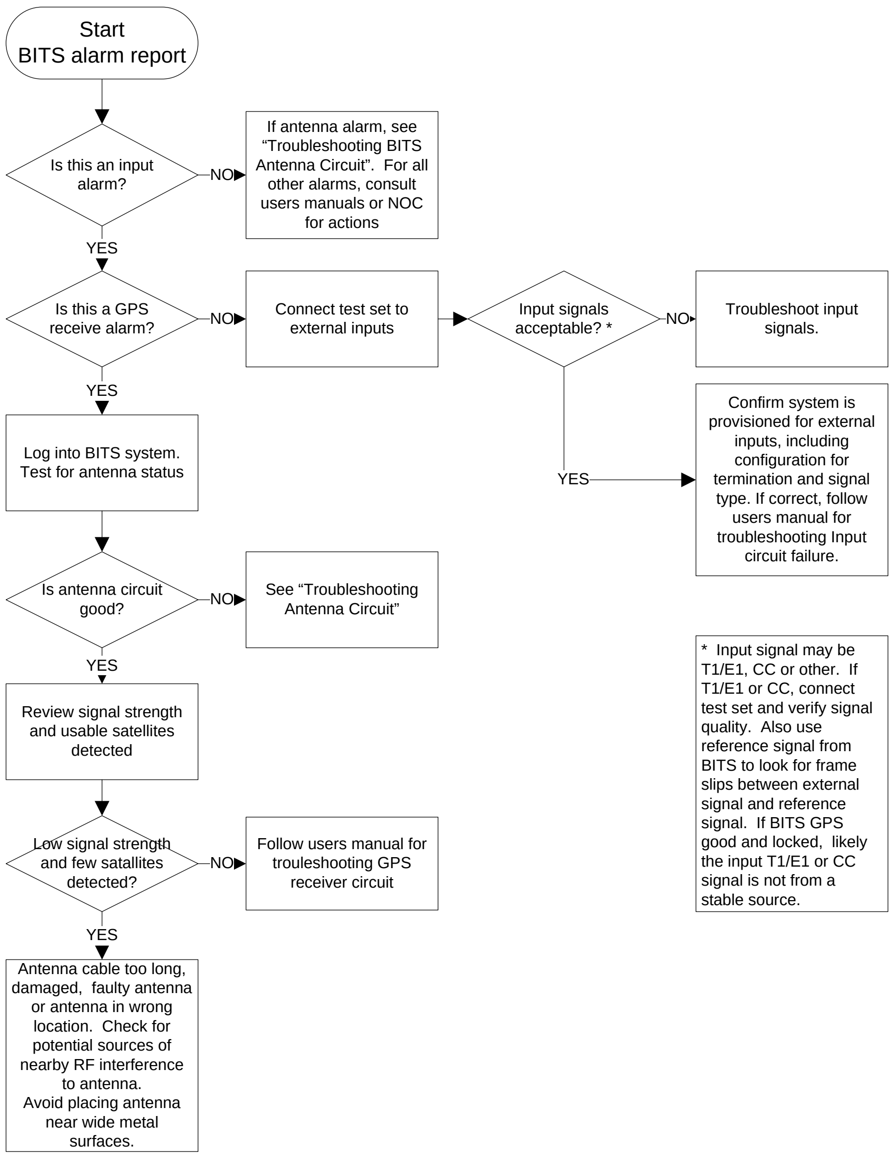
Field	Pin	Function
BITS	A1	BITS Output 2 negative (–)
	B1	BITS Output 2 positive (+)
	A2	BITS Input 2 negative (–)
	B2	BITS Input 2 positive (+)
	A3	BITS Output 1 negative (–)
	B3	BITS Output 1 positive (+)
	A4	BITS Input 1 negative (–)
	B4	BITS Input 1 positive (+)

Fig. 48
SONET/PDH BITS Connections
Distant End

The above example was purposefully selected, as it fully illustrates the need for careful review of the User’s Manual and Input/Output pins prior to connecting BITS cables to the Network Equipment. It is very easy to see the BITS label and assume pins A1 & B1 are the BITS input. However, that would be connecting a live BITS cable onto pins that themselves are outputting a live T1 signal. **NOTE- this example is one of them most common errors when connecting BITS cables to Network Elements.**

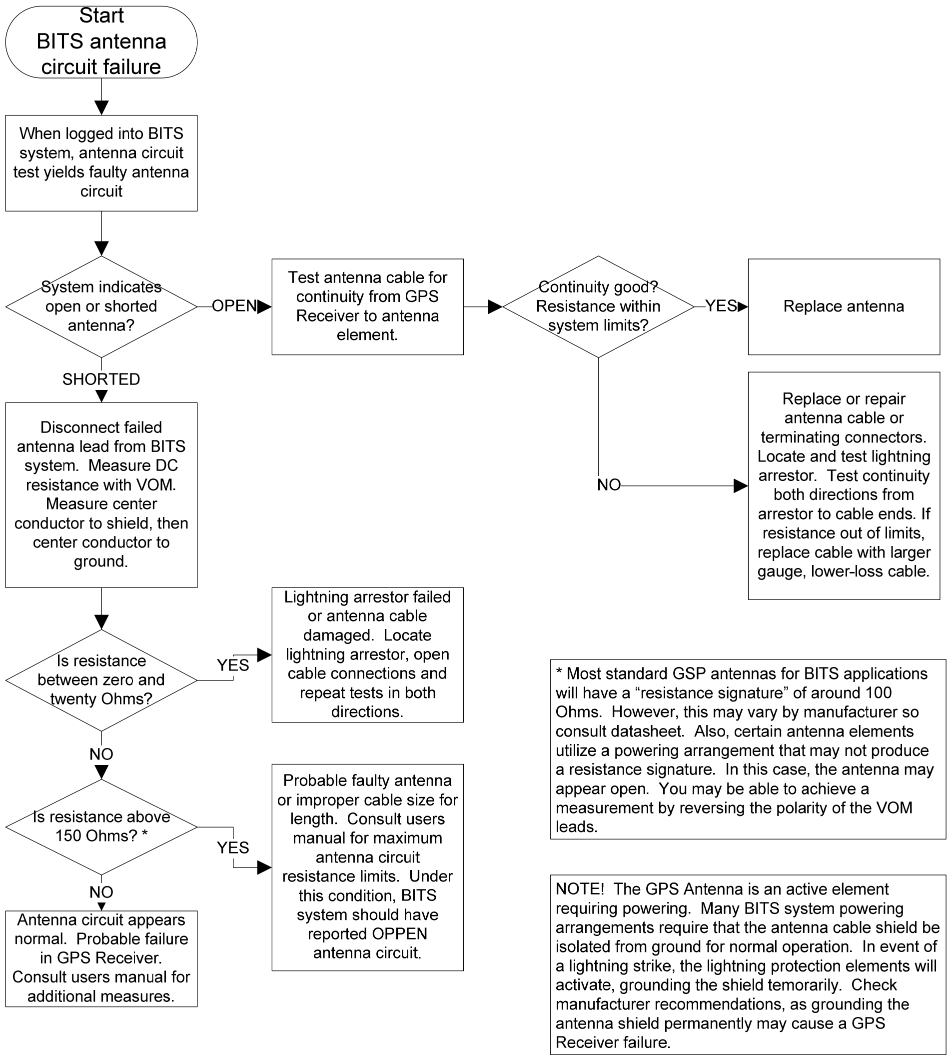
This concludes the Overview Section.

Troubleshooting BITS System Input Alarms



Flow Chart 1
BITS Input Signal Alarm

Troubleshooting BITS Antenna Circuit



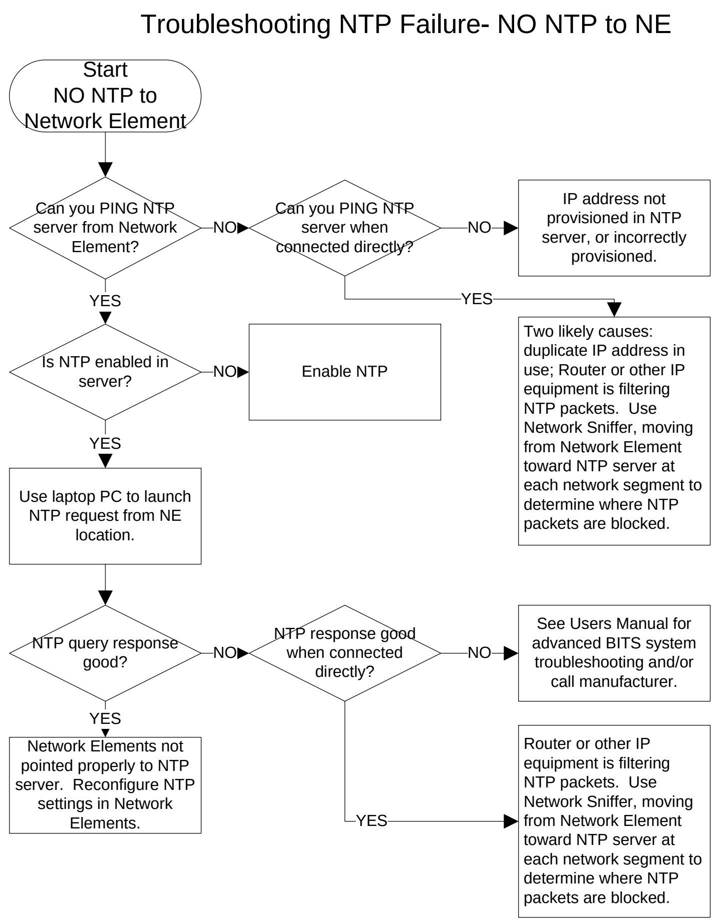
Flow Chart 2
BITS Antenna Circuit Failure

2.0 Troubleshooting Timing links (NTP over IPv4)

This section will provide instructions for troubleshooting *Network Time Protocol* (NTP) links. As discussed in the **Overview Section**, NTP provides accurate *Time Stamps* to any Network Element connected to an IP network. However, problems can be encountered during installation or anytime thereafter, so the following steps will identify and eliminate 95% of failures.

2.1 Scenario 1- NTP Failure to Network Elements

In this scenario, Network Elements are not receiving NTP updates. Flowchart items below are more fully explained in the next several pages.



Flow Chart 3
NTP Failure to Network Element

As shown in the Troubleshooting Flowchart above, there are two processes for testing NTP failures: PING Test Sequence; NTP Query Test sequence.

2.1.1 STEP 1- PING the NTP Server

Using a laptop PC, disconnect one Network Element and replicate the IP address (NOTE- this is service affecting and may require maintenance window). In below example, a VoIP Gateway address 192.168.1.100 was replicated in the laptop. As an alternative, you may configure the laptop with a new IP address (selected by the network administrator). NOTE- if no router is between you and the NTP Server, you must use an address on the same sub-net as the NTP Server address.

Open DOS window and at > prompt, enter: ping 192.168.1.50 (or the address of your NTP Server) then press Enter. If successful, results similar to Fig. 50. A good PING response does not guaranty NTP is working, but is the first step in determining if you can “see” the NTP server on the network.

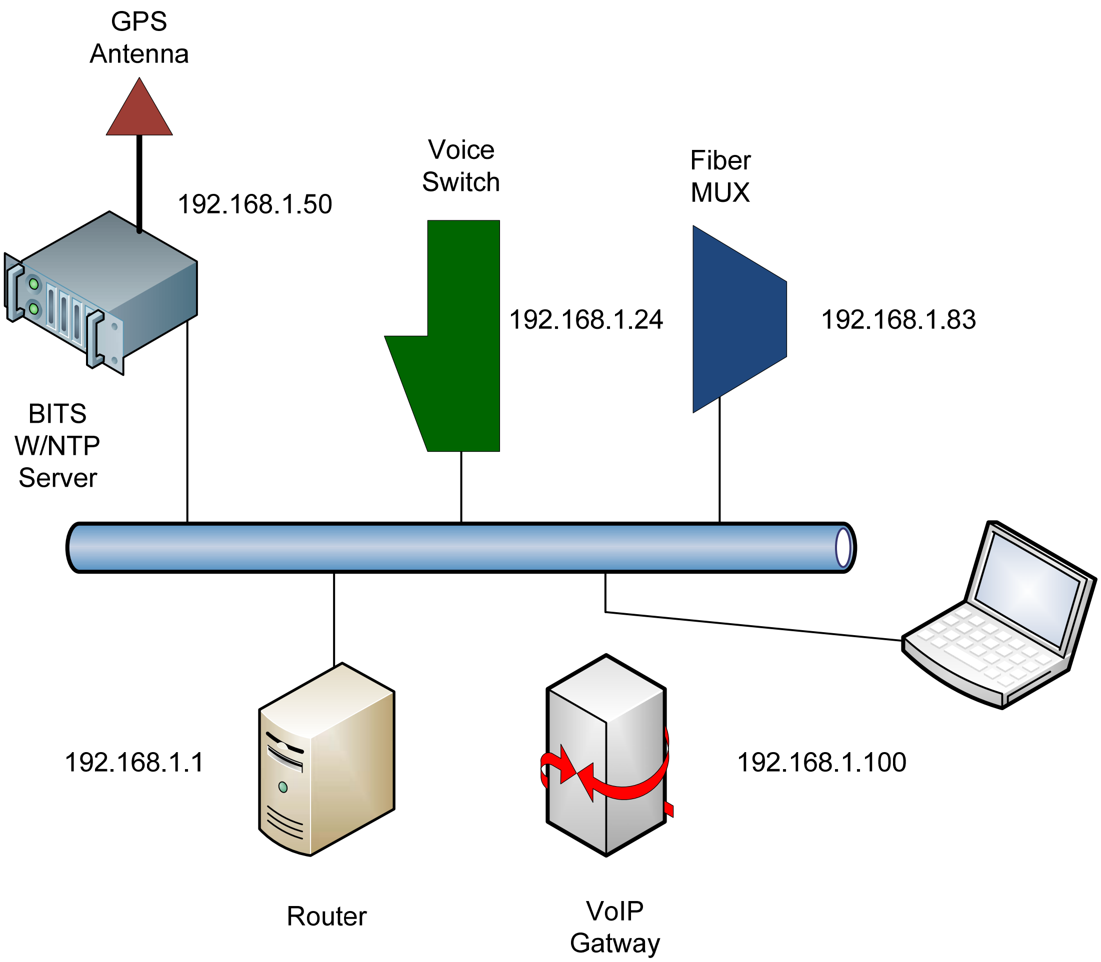


Fig. 49
PING the NTP Server

If PING successful, results will be similar to the screen below:

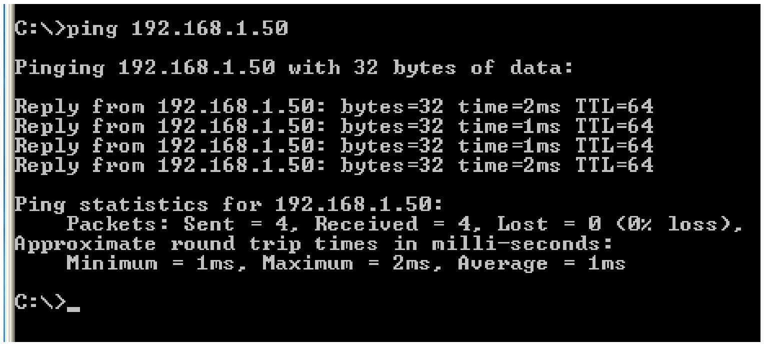


Fig. 50
Successful PING of NTP Server

If PING unsuccessful, results will be similar to the screen below:

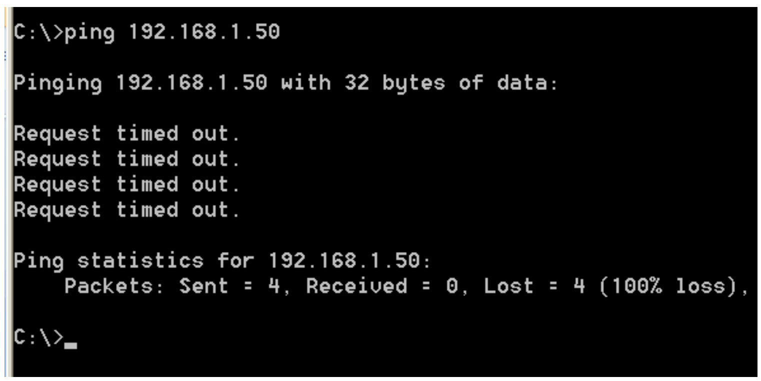


Fig. 51
Unsuccessful PING of NTP Server

2.1.1.1 If the remote PING was unsuccessful, connect the laptop PC directly to the NTP Server port. This may require a "SWAP Cable" with TX/RX transposed for older BITS Systems, but modern version Ethernet Transceivers should be able to sense and correct TX/RX if a straight-thru cable is used.

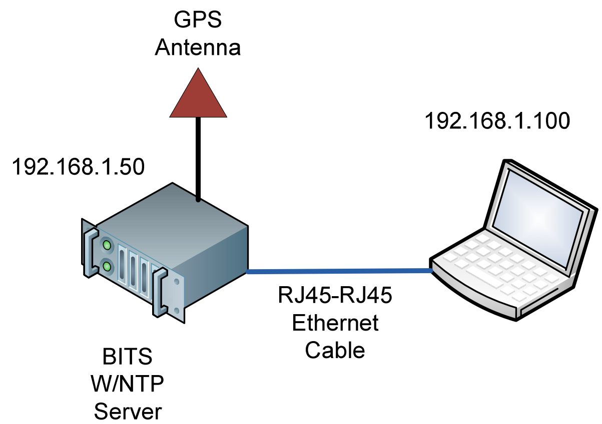


Fig. 52
Direct Connection to NTP Server

2.1.1.2 Be sure the laptop is configured on the same subnet as the NTP Server address. Set up the laptop as shown below:

1. **Click Start> Control Panel**
2. **Click Network Connections**
3. **Right Click Local Area Connection in use**
4. **Click Properties**
5. **Highlight Internet Protocol (TCP/IP)**
6. **Click Properties**
7. **Click Use the following IP address**
8. **Enter new test IP address**
9. **If directly connected to NTP Server,**
   use NTP Server address for Default gateway.
10. **Click OK**

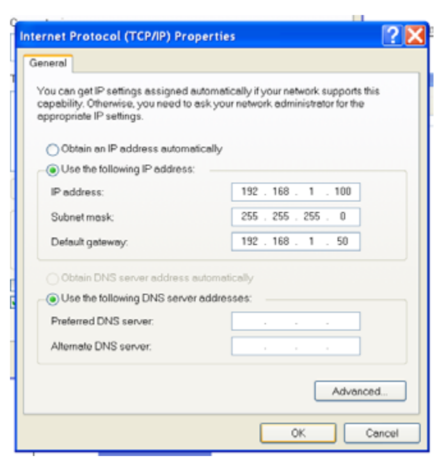


Fig. 53
Setting Test PPC IP Address [2.3]

2.1.1.3 If you can PING the NTP Server when connected directly, but cannot PING from a remote location, it is likely that the IP address is duplicated on the network, the IP address is invalid, there is an address subnet issue, or a router is blocking the address.

If you cannot PING the NTP Server even when directly connected, the NTP Server is not configured properly. If you desire to test the assigned NTP Server address, you may want to configure a 2nd laptop PC, using the NTP Server address (verify all settings with the network administrator, including the proper Default Gateway). Disconnect the Ethernet cable from the NTP Server port and connect it directly into the 2nd Laptop PC as shown below. This provides for a full test of all facilities up to the NTP Server. In other words, the 2nd Laptop shown below will be used only to determine if the assigned NTP Server address can be PING'd from the distant Test Laptop. If the 2nd Laptop PC can be PING'd, but not the NTP Server when using the same address settings, the trouble is in the NTP Server. NOTE- when configured with the same IP Address, only the 2nd Laptop or the NTP Server may be connected to the network, but not at the same time, as this would result in duplicate addressing.

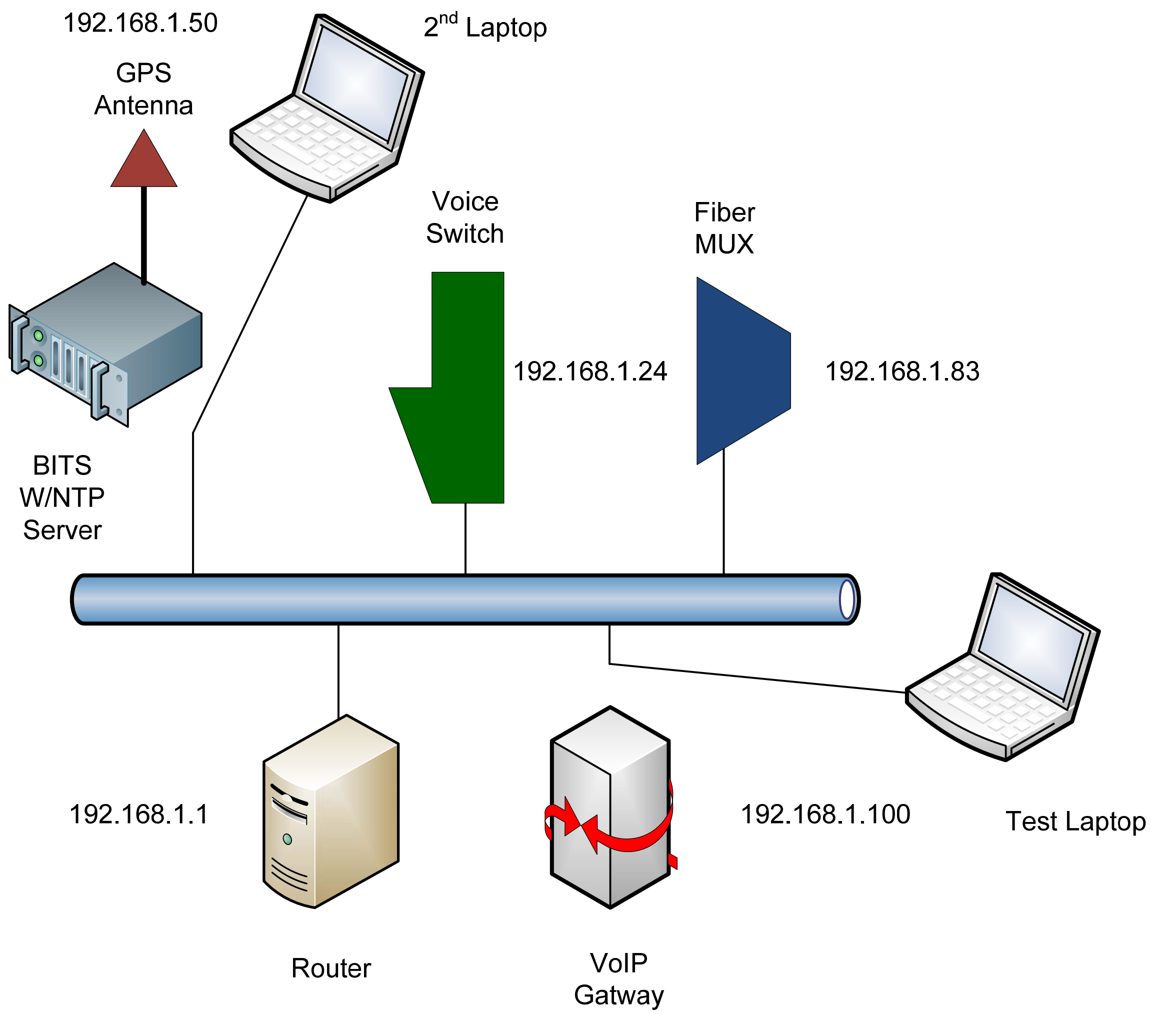


Fig. 54
Using laptop in lieu of
NTP Server for PING Test

2.1.2 STEP 2- Generate NTP Test Request

If the NTP Server PING test results are satisfactory (good response), the next step is to generate a NTP query with the Test Laptop. As explained in the **Introduction Section**, most modern PC's have NTP Clients onboard which may be used to test the NTP Server.

1. **Double-Click Clock in lower right-hand laptop display**
2. **Click 'Internet Time' tab**
3. **Enter NTP Server address**
4. **Click Update Now**

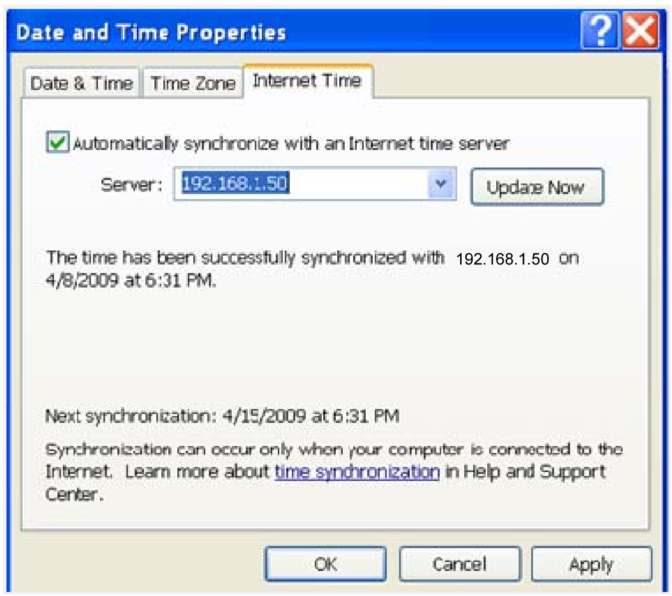


Fig. 55
Launch NTP Query from Test PC [2.4]

If NTP query successful, screen will update with new time and date of response. If NTP query unsuccessful, screen will not change. However, some Windows versions require the page be closed and reopened to display update success.

2.1.2.1 If the NTP query failed, yet the NTP Server responds to a PING, move the laptop PC to the NTP Server, repeating the setup as for the direct PING test, but launching the NTP query as shown above. If the NTP query is successful, use a Network Sniffer to sectionalize the Network, as NTP packets are being filtered at some point.

Most Networks have multiple subnets, routers and associated hardware. Therefore, you may have to move the Network Sniffer from the Test Laptop to other Network access points between the Test Laptop and NTP Server. Your goal is to locate the point at which a captured NTP Server query is blocked in one direction or the other.

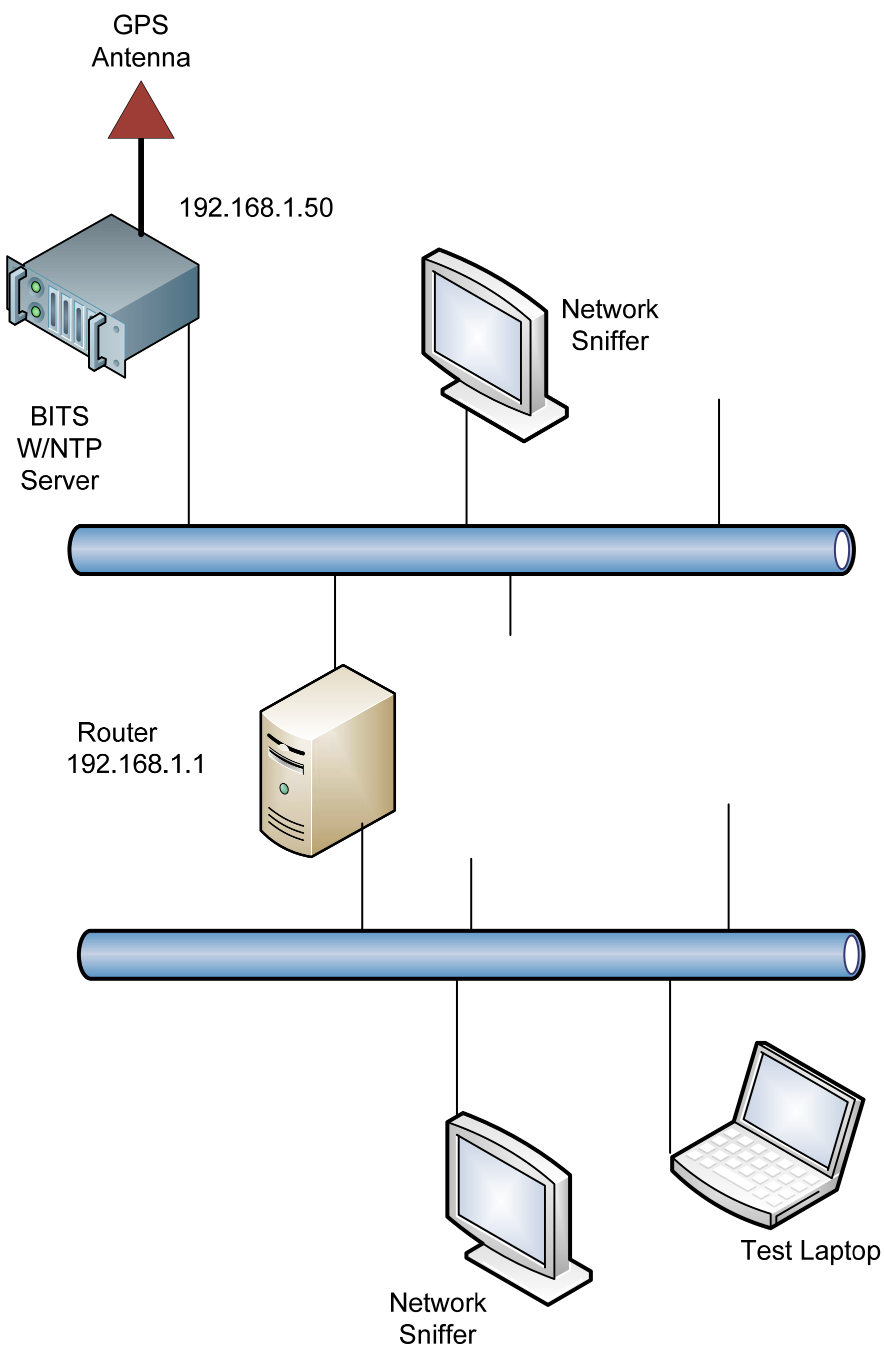


Fig. 56
Suggested Network Sniffer Locations

2.1.2.2 Below are results of a standard Network Sniffer output. Note the NTP query and response were both recorded at this test point as shown in Line Number 16 & 17. Below is the outbound NTP query (Line 16), which is expanded in the lower half of the display under the header Network Time Protocol:

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.100	192.168.1.255	NBNS	Name query NB WPAD.<00>
2	0.750028	192.168.1.100	192.168.1.255	NBNS	Name query NB WPAD.<00>
3	1.502622	192.168.1.100	192.168.1.1	DNS	Standard query A download.windowsupdate.com
4	2.500158	192.168.1.100	192.168.1.1	DNS	Standard query A download.windowsupdate.com
5	3.500185	192.168.1.100	192.168.1.1	DNS	Standard query A download.windowsupdate.com
6	5.312779	192.168.1.100	192.168.1.1	DNS	Standard query PTR 1.0.0.127.dnsbugtest.1.0.0.127.in-addr.arpa
7	5.500223	192.168.1.100	192.168.1.1	DNS	Standard query A download.windowsupdate.com
8	9.500337	192.168.1.100	192.168.1.1	DNS	Standard query A download.windowsupdate.com
9	16.506933	192.168.1.100	192.168.1.1	DNS	Standard query A wpad
10	17.500637	192.168.1.100	192.168.1.1	DNS	Standard query A wpad
11	18.500904	192.168.1.100	192.168.1.1	DNS	Standard query A wpad
12	20.500741	192.168.1.100	192.168.1.1	DNS	Standard query A wpad
13	24.500880	192.168.1.100	192.168.1.1	DNS	Standard query A wpad
14	28.110451	GemtekTe_56:7b:79	Broadcast	ARP	Who has 192.168.1.50? Tell 192.168.1.100
15	28.112282	CxrLarus_00:4a	GemtekTe_56:7b:79	ARP	192.168.1.50 is at 00:50:c2:68:d0:4a
16	28.112294	192.168.1.100	192.168.1.50	NTP	NTP symmetric active
17	28.113314	192.168.1.50	192.168.1.100	NTP	NTP symmetric passive
18	29.329294	192.168.1.100	192.168.1.1	DNS	Standard query PTR 1.0.0.127.dnsbugtest.1.0.0.127.in-addr.arpa

```
⊞ Frame 16 (90 bytes on wire, 90 bytes captured)
⊞ Ethernet II, Src: GemtekTe_56:7b:79 (00:90:4b:56:7b:79), Dst: CxrLarus_00:4a (00:50:c2:68:d0:4a)
⊞ Internet Protocol, Src: 192.168.1.100 (192.168.1.100), Dst: 192.168.1.50 (192.168.1.50)
⊞ User Datagram Protocol, Src Port: ntp (123), Dst Port: ntp (123)
⊟ Network Time Protocol
  ⊞ Flags: 0xd9
    Peer Clock Stratum: unspecified or unavailable (0)
    Peer Polling Interval: 10 (1024 sec)
    Peer Clock Precision: 0.015625 sec
    Root Delay:    0.0313 sec
    Root Dispersion:    12.0763 sec
    Reference Clock ID: NULL
    Reference Clock Update Time: Apr 13, 2009 22:25:27.7813 UTC
    Originate Time Stamp: NULL
    Receive Time Stamp: NULL
    Transmit Time Stamp: Apr 14, 2009 00:19:39.1675 UTC
```

Expanding the NTP query response (Line 17):

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.100	192.168.1.255	NBNS	Name query NB WPAD.<00>
2	0.750028	192.168.1.100	192.168.1.255	NBNS	Name query NB WPAD.<00>
3	1.502622	192.168.1.100	192.168.1.1	DNS	Standard query A download.windowsupdate.com
4	2.500158	192.168.1.100	192.168.1.1	DNS	Standard query A download.windowsupdate.com
5	3.500185	192.168.1.100	192.168.1.1	DNS	Standard query A download.windowsupdate.com
6	5.312779	192.168.1.100	192.168.1.1	DNS	Standard query PTR 1.0.0.127.dnsbugtest.1.0.0.127.in-addr.arpa
7	5.500223	192.168.1.100	192.168.1.1	DNS	Standard query A download.windowsupdate.com
8	9.500337	192.168.1.100	192.168.1.1	DNS	Standard query A download.windowsupdate.com
9	16.506933	192.168.1.100	192.168.1.1	DNS	Standard query A wpad
10	17.500637	192.168.1.100	192.168.1.1	DNS	Standard query A wpad
11	18.500904	192.168.1.100	192.168.1.1	DNS	Standard query A wpad
12	20.500741	192.168.1.100	192.168.1.1	DNS	Standard query A wpad
13	24.500880	192.168.1.100	192.168.1.1	DNS	Standard query A wpad
14	28.110451	GemtekTe_56:7b:79	Broadcast	ARP	Who has 192.168.1.50? Tell 192.168.1.100
15	28.112282	CxrLarus_00:4a	GemtekTe_56:7b:79	ARP	192.168.1.50 is at 00:50:c2:68:d0:4a
16	28.112294	192.168.1.100	192.168.1.50	NTP	NTP symmetric active
17	28.113314	192.168.1.50	192.168.1.100	NTP	NTP symmetric passive
18	29.329294	192.168.1.100	192.168.1.1	DNS	Standard query PTR 1.0.0.127.dnsbugtest.1.0.0.127.in-addr.arpa

```
⊞ Frame 17 (90 bytes on wire, 90 bytes captured)
⊞ Ethernet II, Src: CxrLarus_00:4a (00:50:c2:68:d0:4a), Dst: GemtekTe_56:7b:79 (00:90:4b:56:7b:79)
⊞ Internet Protocol, Src: 192.168.1.50 (192.168.1.50), Dst: 192.168.1.100 (192.168.1.100)
⊞ User Datagram Protocol, Src Port: ntp (123), Dst Port: ntp (123)
⊟ Network Time Protocol
  ⊞ Flags: 0x1a
    Peer Clock Stratum: primary reference (1)
    Peer Polling Interval: 10 (1024 sec)
    Peer Clock Precision: 0.000000 sec
    Root Delay:    0.0000 sec
    Root Dispersion:    0.0000 sec
    Reference Clock ID: Global Positioning Service
    Reference Clock Update Time: Apr 14, 2009 00:19:40.1139 UTC
    Originate Time Stamp: Apr 14, 2009 00:19:39.1675 UTC
    Receive Time Stamp: Apr 14, 2009 00:19:40.1139 UTC
    Transmit Time Stamp: Apr 14, 2009 00:19:40.1139 UTC
```

Fig. 57 & 58
NTP Query & Response [2.5]

The point of the preceding illustrations was that if the NTP query is never returned, the packets must be traced from source all the way to destination. Note the NTP query response contains Time Stamps which can aide also insure they are from your recent test packets.

The PING and NTP Query tests shown above are useful for ensuring NTP is passing through the IP Network. However, a couple other tests may help determine if an intermittent NTP failure exists, especially if two or more NTP Servers are connected to the IP Network.

2.1.2.3 Windows contains a program (w32tm) which is somewhat useful for ensuring a Network Element or PC can "reach" multiple NTP Servers, or provide Strip Chart readouts for multiple Time Delta requests. Our first example will display the delta between the host PC and two or more NTP servers.

2.1.2.4 In a DOS window, enter w32tm /monitor /computers:xxx.xxx.x.xx,xxx.xxx.x.xx then press Enter (use valid addresses for the xxx). Note there is a space preceding each / and a comma between the computer addresses. The result is a multiple output format which displays the round-trip delay to each PC or NTP Server, and delta of local clock to NTP clocks. Note the NTP clock also identifies its source (RefID).

```
C:\>w32tm /monitor /computers:192.43.244.18,72.18.205.156
192.43.244.18 [192.43.244.18]:
    ICMP: 49ms delay.
    NTP: +3.2513177s offset from local clock
        RefID: 'ACTS' [65.67.84.83]
72.18.205.156 [72.18.205.156]:
    ICMP: 49ms delay.
    NTP: +3.2618376s offset from local clock
        RefID: (unknown) [64.202.112.75]
```

Fig. 59
Test to Dual NTP Server

The default number of PCs/Servers that may be compared is 3, but if you append the command with /threads:<number> you can compare up to 50 systems. This may be a useful tool for comparing the internal clocks on multiple PC's on a Network to determine if they are all referencing the same NTP source. NOTE- not all NTP Servers may respond to this command-consult Users Manual.

2.1.2.4 The second w32tm format we will examine is useful for conducting a longer test of NTP command/responses. For example, this test may be appropriate when troubleshooting route-path with a Network Sniffer, as it can be launched in a mode which is repetitive, providing a larger number of examples for tracing.

In a DOS window, enter w32tm /stripchart /computer:192.168.1.50 /dataonly /samples:10 then press Enter. Note there is a space preceding each /. The result is strip chart readout of the delta between the NTP clock, and local PC clock. Since the NTP clock is more stable than the internal PC clock, this number may vary slightly +/- a few microseconds over time. The default sample rate is every 2 seconds, so if you set a long sample quantity of 50, the queries will continue for 100 seconds. This provides multiple NTP samples over time for observing the Network Sniffer results.

```
C:\>w32tm /stripchart /computer:192.168.1.50 /dataonly /samples:10
Tracking 192.168.1.50 [192.168.1.50].
Collecting 10 samples.
The current time is 4/13/2009 5:29:21 PM (local time).
17:29:21, +00.8686374s
17:29:23, +00.8575015s
17:29:25, +00.8576820s
17:29:27, +00.8572249s
17:29:29, +00.8576269s
17:29:31, +00.8571908s
17:29:33, +00.8570998s
17:29:35, +00.8567060s
17:29:37, +00.8565957s
17:29:39, +00.8564058s
```

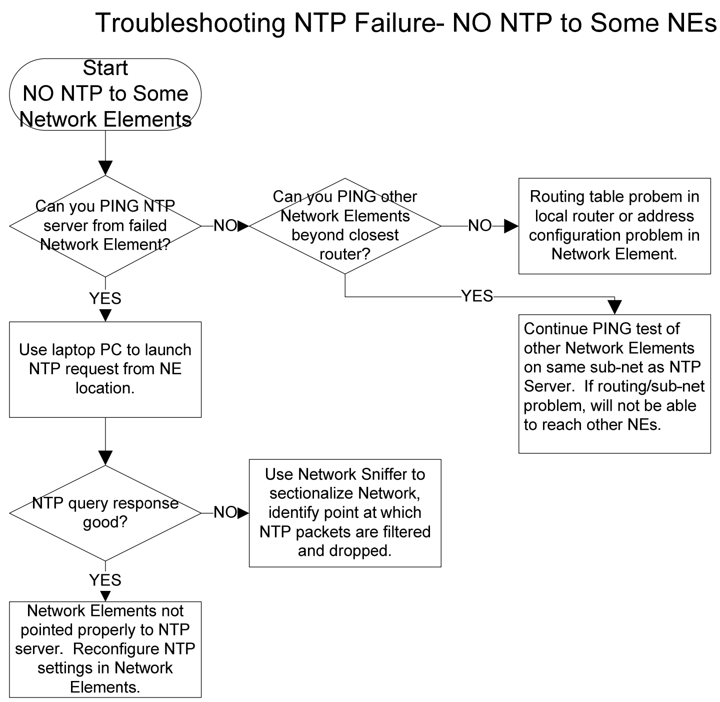
Fig. 60
Test for Delta to NTP
Server or PC Host

The results of this query can be analyzed in a couple ways: firstly, you want to see a good response every two seconds. If a query fails, the line will read- error**. Therefore, if you begin seeing successive or frequent errors, then perhaps a network element is dropping some of the packets. NOTE-not all NTP Servers respond to this command, consult Users Manual. This program is also useful for comparing delta between two PCs.

2.1.2.5 If you have no access to an NTP Server, you may use w32tm with the NIST NTP Server at 192.43.244.18, but they do limit the number of successive queries so results may vary. Other Internet-based NTP Servers are available, but also may limit use of some of the w32tm applications.

To review all w32tm components, at DOS prompt enter: w32tm /?

2.2.0 Scenario 2- NTP Failure to specific Elements
In this scenario, some, but not all Network Elements are receiving NTP updates. The same tests used previously- PING and NTP Query will be employed to diagnose this trouble.



Flow Chart 4
NTP Failure to Select NEs

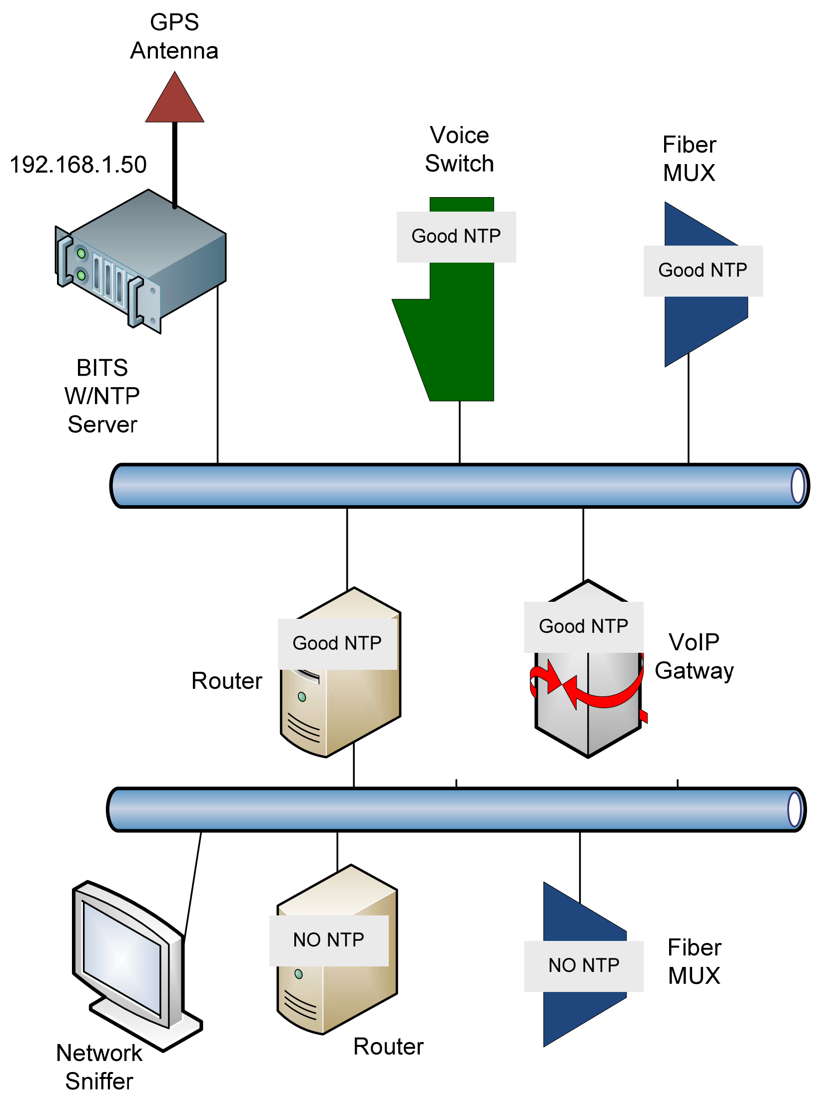


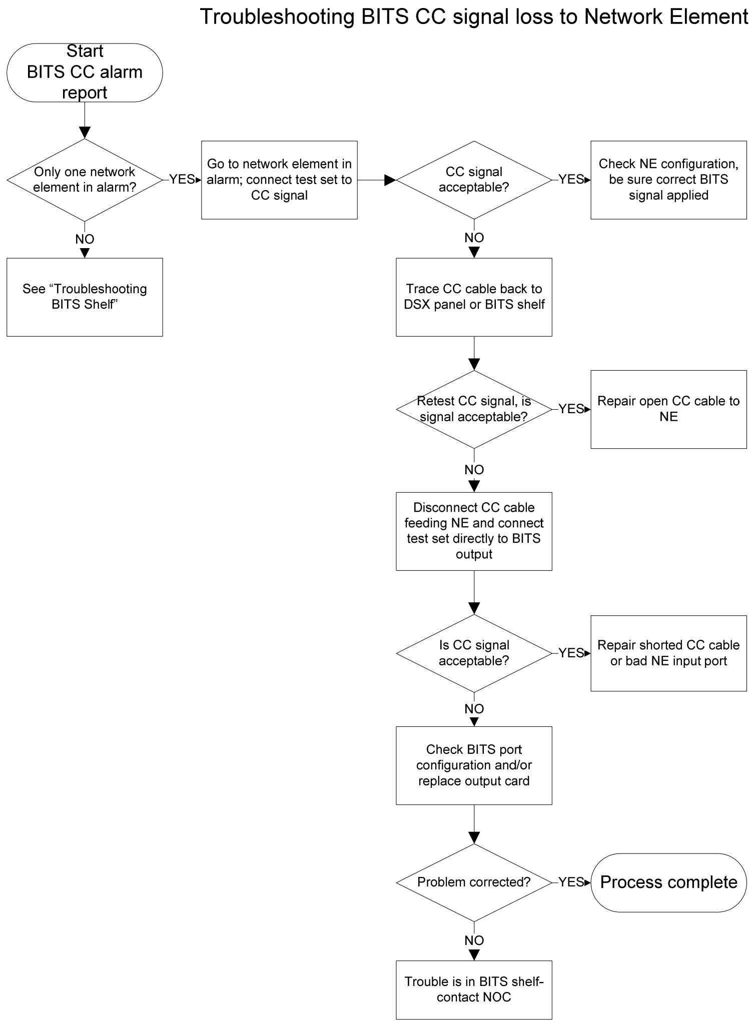
Fig. 61
Sectionalizing NTP Failures

2.2.1 As shown above, the Network topology must be carefully scrutinized to determine if an entire segment is isolated from NTP, or if the fault is restricted to only a few Network Elements. The best method for locating this fault is to employ the PING and NTP Query tests as discussed in Scenario 1, using a Network Sniffer to locate the point in which the NTP Packets are being filtered and dropped.

3.0 Troubleshooting Composite Clock (CC) Synchronization Links

The flowchart below provides the basic direction for responding to a BITS Composite Clock (CC) failure to an existing Network Element. This process is also useful for validating a new CC link connection. Detailed steps for this flowchart appear on the following pages.

3.0.1



Flow Chart 5
Troubleshooting CC

3.0.2 The BITS CC circuit will be tested at the following location(s):

- Test Point A- at the BITS card output connector or closest terminating point.
- Test Point B- at the DS0 DSX (or equiv, if present).
- Test Point C- at the Network Element Input connector.

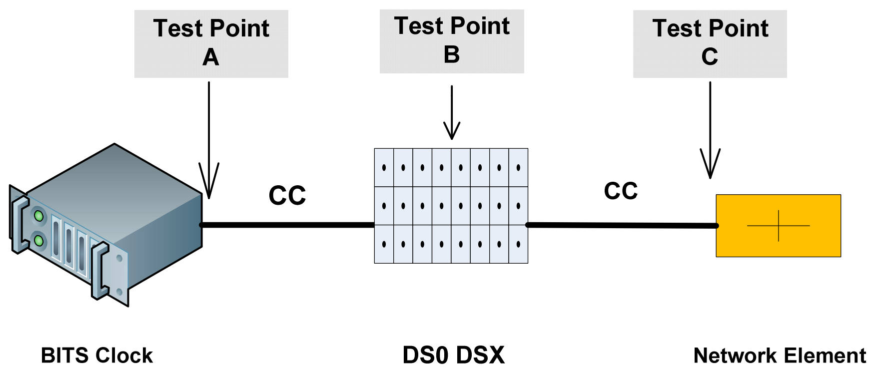


Fig. 62
CC Circuit Test Points

3.1.0 Step 1- Measure CC Signal at Testpoint C

3.1.0.1 Connect a GUISYS Model Gb310-RITS Intelligent Timing Test Set to the CC signal at the Network Element Sync Input connection. The Gb310-RITS is a portable, multi-purpose test set with special features for analyzing T1, E1 and CC BITS signals.

To power on instrument, lift power switch toward top.

After configuring test set, use the Single Circuit Testing Input- male Bantam jack. It is also suggested to connect a ground to the test instrument.

Configuration steps are shown below.

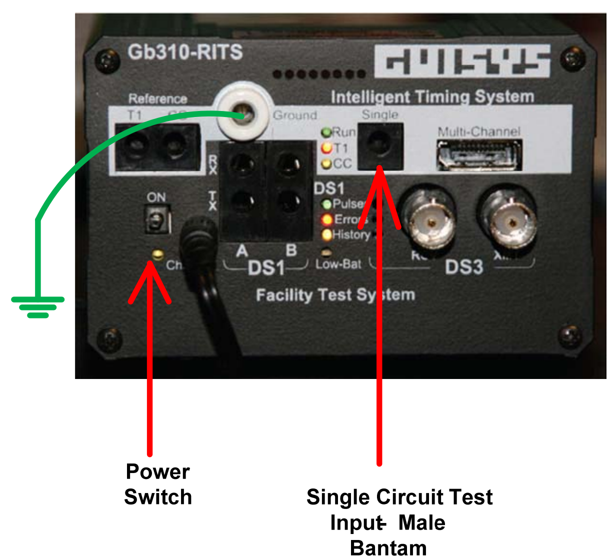
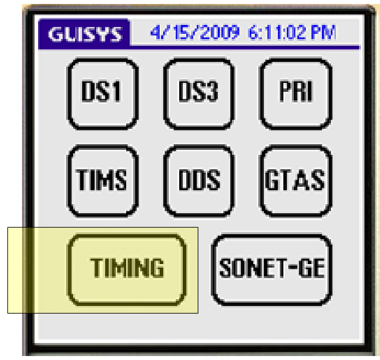
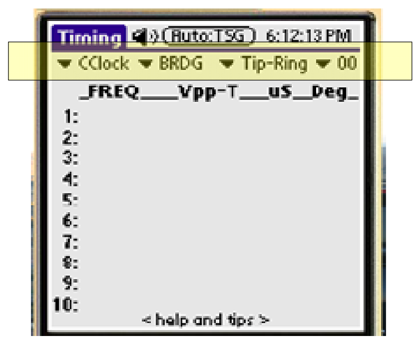


Fig. 63
Timing Test Set Access Jacks [2.6]

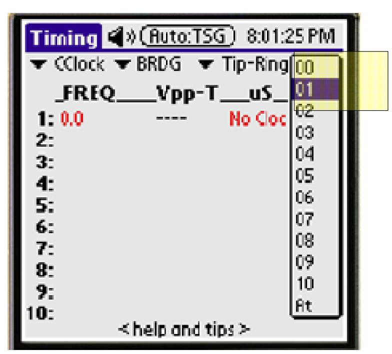
1..At Power-Up, tap TIMING from the touch-sensitive Main Menu area.



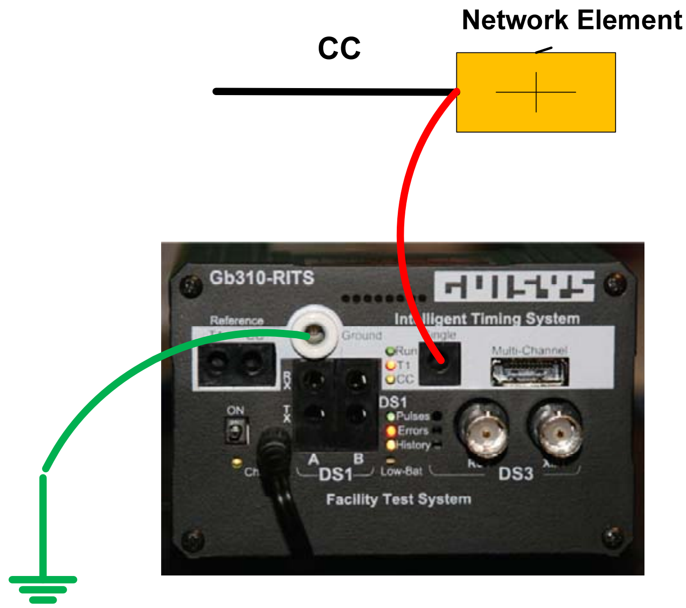
2..The default is Composite Clock, Bridged, Tip-Ring, Input 00. While the Gb310-RITS is capable of measuring up to 10 simultaneous inputs, we will view a single CC link.



3..Tap the dropdown menu beside 00 and select 01. This will start the test process and you may hear beeps.



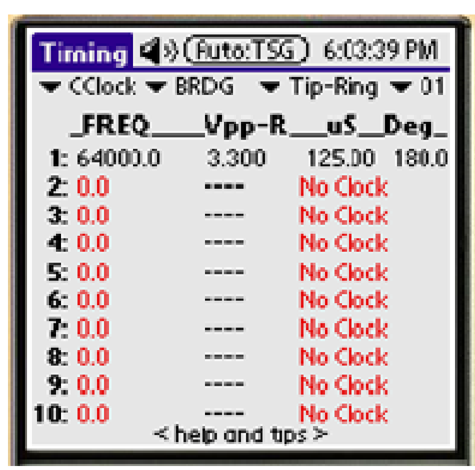
4.. Use Bantam-to-Alligator Cable to tap onto the CC cable connection. Insert Bantam plug into "Single" jack on Gb310-RITS as shown at right. Connect ground cable from Ground terminal of test set to signal ground.



GUISYS Model Gb310- RITS
Intelligent Timing Test Set

Fig. 64
Test Set Connection at NE
For CC Test

5..A good CC signal will display characters in BLACK as shown at right. The Gb310-RITS automatically measures all CC signal parameters, and a RED reading signifies a FAILURE.



3.1.0.2 NOTE ON TERMINATIONS!

The Gb310-RITS defaults to BRDG-GND Ref for testing CC signals. However, if the termination status is unknown for the Network Element(s), the test set may show RED initially. If a RED reading is obtained, switch to LIVE-No GND Ref and remove ground cable from test set. The following scenarios provide guidance on which termination setting is appropriate:

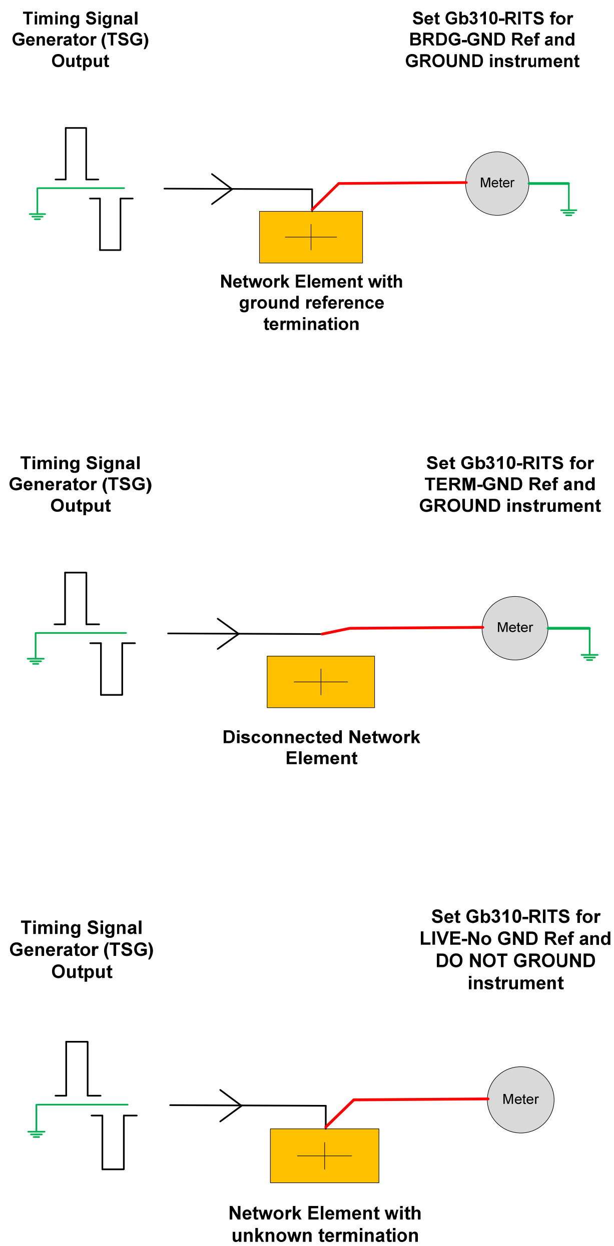


Fig. 65
Test Set Termination Options for CC Testing

To change the termination setting, just tap BRDG for a drop-down menu.

3.1.0.3 Results Analysis

The Gb310-RITS automatically performs analysis on the CC under test. All readings in BLACK are acceptable; all readings in RED are unacceptable. For the CC to be deemed acceptable, all readings must be BLACK. Any RED readings indicate a CC failure.

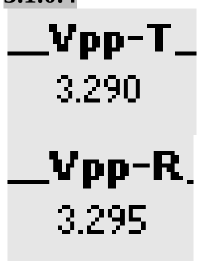
Frequency (Freq): This is a measure of the 64 KHz portion of the CC signal, with detection of the 8 KHz element. Both the 64 KHz and 8 KHz elements must be present for this to be acceptable.

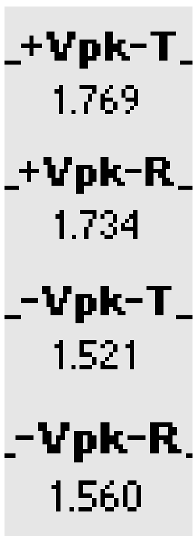
Voltage Peak-to-Peak-Tip or Ring (Vpp-T)- See box below.

MicroSecond (uS): This is a measure of the Tip and Ring of the CC link and will be around 125 uS when measuring Tip-Ring. This measurement, along with Degrees (Deg) will be further explored when measuring one CC signal against another CC reference signal.

Degrees (Deg): For Tip-Ring measures, this is the delay between Tip-Ring leading edges. When measuring one CC signal against another CC reference signal, this is the phase delta between the two signals.

3.1.0.4





If all readings on the initial screen are BLACK, you must also tap Vpp-T to view the reading for Vpp-R. Each time you tap the Vpp header, the reading will change to the next value, and each is described below:

Voltage Peak-to-Peak-Tip or Ring (Vpp-T)- This is a measure of the peak-to-peak CC signals references from the normalized Tip-to-Ring view. The acceptable range is 2.565 – 5.775 Volts.

Vpp-R- This is a measure of the peak-to-peak CC signals references from the normalized Ring-to-Tip view. The acceptable range is 2.565 – 5.775 Volts.

Under normal circumstances, Vpp-T and Vpp-R are the only readings of interest. However, if either Vpp-T or Vpp-R are RED, connect a ground cable to the Gb310-RITS and view the 4 additional values shown at left to see if any are RED. These are the base-to-peak readings and acceptable range for base-to-peak is 1.282 – 2.887 Volts.

Again, if all readings are BLACK, the signal is acceptable for use.

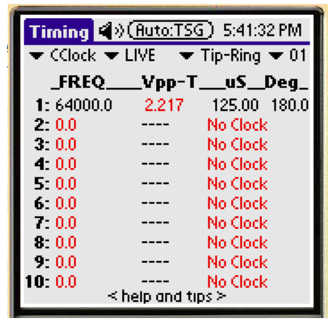
3.1.0.5 The likely causes of any RED readings are shown below:

RED Reading	Likely Cause	Additional Cause
Frequency (Freq)	Failing BITS Output Card	Noisy or extended length CC cable to NE
Voltages (Vpp-T, etc.)	Extended length, faulty CC cable or multiple termination on cable	Failing BITS Output Card
Delay (uS) (1)	Failing BITS Output Card	
Degrees (Deg) (1)	Failing BITS Output Card	
Delay (uS) (2)	Reference or CC not traceable to GPS	BITS Shelf settings/multiple BITS shelves
Degrees (Deg) (2)	Reference or CC not traceable to GPS	BITS Shelf settings/multiple BITS shelves

1- Tip-Ring Mode
2- Ref-CC Mode

Table 4
Analysis of CC Failures

At right is example of a failed CC link with a severely attenuated Signal level. Therefore, the Vpp (peak Tip Voltage) Displays in red. This CC cable was terminated onto multiple Network Elements in error. While a CC signal may be connected to multiple Network Elements, only a single NE may be in TERMINATE mode, all others are in BRIDGED mode Once the additional NEs terminations were corrected, the signal was acceptable.



Nearly all BITS CC failures are related to either the BITS Output card or the cable which extends CC to the Network Element. The Output card may be failing or merely needs configured properly. The cable may be too lengthy or exhibiting physical faults such as shorts or grounds. At any rate, the gB310-RITS can be used to sectionalize the fault condition.

If the CC signal passes all tests at Test Point C, the signal is usable for synchronization. If the Network Element does not sync on an acceptable CC signal, the NE requires configuration or hardware adjustments or replacement parts.

However, if any CC signal reading fails (displays red) at Test Point C, move on to Step 2.

3.2.0 Step 2- Measure CC Signal at Testpoint B

3.2.0.1 Connect a GUISYS Model Gb310-RITS Intelligent Timing Test Set to the CC signal at the DS0 DSX connection (or equiv. access point).

Configure the test set as per Step 1, and set Termination for LIVE- No GRD Ref.

Connect a Bantam-to-Bantam cable from the DS0 DSX OUT jack facing the BITS system into the Gb310-RITS as shown below. NOTE- this will open the CC circuit toward the Network Element, terminating the CC signal into the test set.

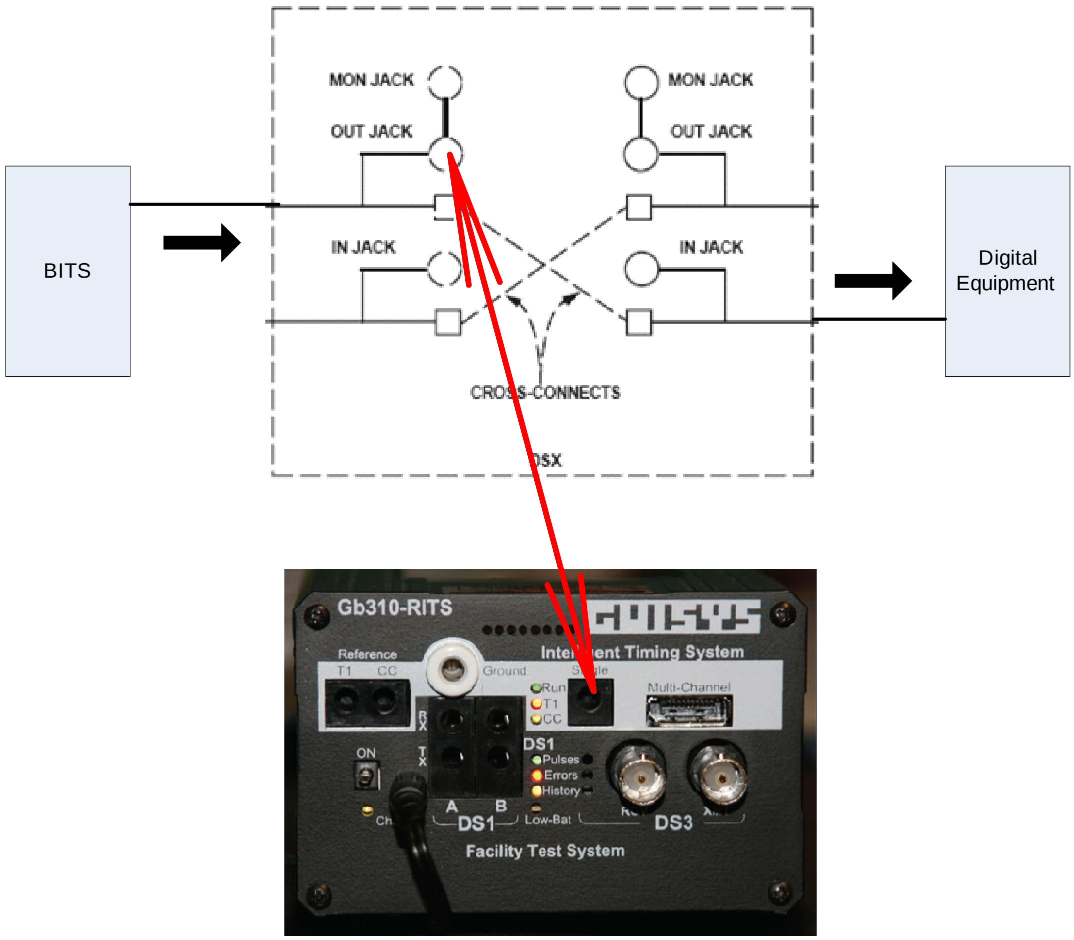


Fig. 66
Test Set Connection at DSX
For CC Test

If the CC signal passes all tests (all readings BLACK- be sure to review both Vpp-T and Vpp-R), the signal is usable for synchronization. If the CC signal is useable at the DS0 DSX toward the BITS system, but fails at the Network Element location, probable causes:

- Mis-wired DS0 DSX jacks
- Faulty cable between DS0 DSX and Network Element
- Multiple NE terminations on CC cable
- Distance to Network Element exceeds BITS system limits

3.2.0.2 Use Volt-Ohm Meter to measure CC cable between DS0 DSX and Network Element for physical faults such as opens, shorts or grounds. If continuity good and no physical faults, review allowable distance from BITS system to Network Element in BITS Users Manual. If CC cable connected to multiple NEs, remove one NE at a time to determine if one or more elements are shorted.

If CC signal fails tests at DS0 DSX (any readings display in red), move on to Step 3 on next page.

3.3.0 Step 3- Measure CC Signal at Testpoint A
3.3.0.1 Disconnect the cable to Network Element; connect a GUISYS Model Gb310-RITS Intelligent Timing Test Set directly to the CC signal at the BITS shelf or closest terminating point to the BITS shelf.

Configure the test set as per Step 1, and set Termination for LIVE- No GRD Ref.

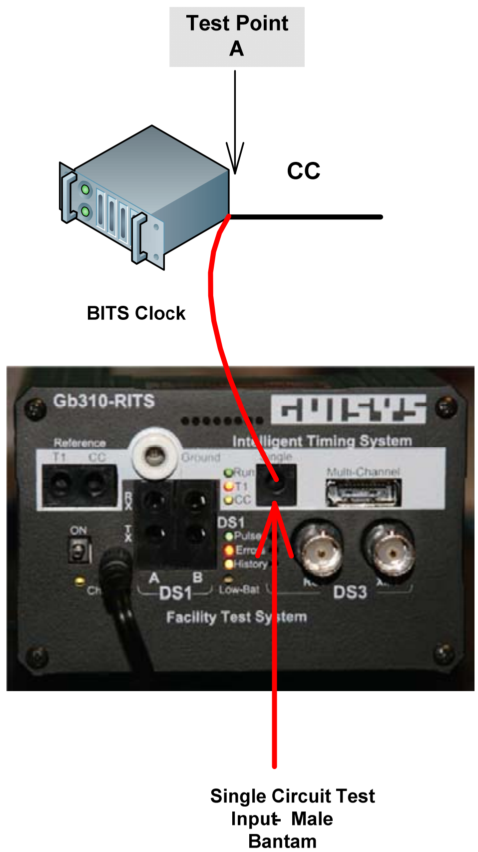


Fig. 67
Test Set Connection at BITS Shelf for CC Test

If the CC signal passes all tests (all readings BLACK- be sure to review both Vpp-T and Vpp-R), the signal is usable for synchronization. If the CC signal is useable at the BITS shelf Output, but fails at the DS0 DSX location, probable causes:

- Mis-wired DS0 DSX jacks
- Faulty cable between BITS shelf and DS0 DSX
- Distance to DS0 DSX exceeds BITS system limits

Use Volt-Ohm Meter to measure CC cable between BITS shelf Output and DS0 DSX for physical faults such as opens, shorts or grounds. If continuity good with no physical faults, review allowable distance from BITS system to DS0 DSX in BITS Users Manual. If CC signal fails tests at BITS shelf Output, Output Card is faulty or improperly configured. Call NOC or review Users Manual for troubleshooting Output Card.

3.4.0 Monitoring or testing multiple CC links simultaneously

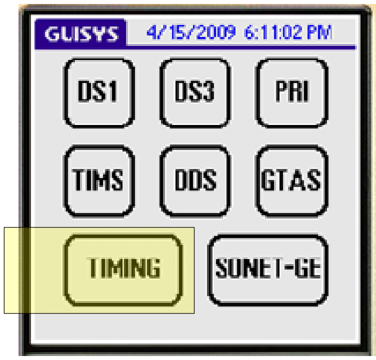
The GUISYS Model Gb310-RITS Intelligent Timing Test Set may also be used to monitor or test up to 10 CC links simultaneously. This is extremely useful for commissioning a new BITS system or long-term monitoring a site for intermittent failures.

To monitor multiple CC links, the GUISYS Model Gb310-RITS Intelligent Timing Test Set may be connected to an optional cable with various connector arrangements. Select the appropriate connector type and connect up to 10 CC links to the cable.

The Gb310-RITS can be configured to scan all 10 CC inputs continuously as shown on next page.

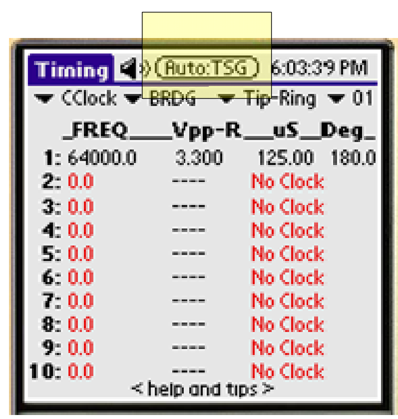
Fig. 68
Simultaneous Testing
up to 10 CC Signals

1..At Power-Up, tap TIMING from the touch-sensitive Main Menu area.

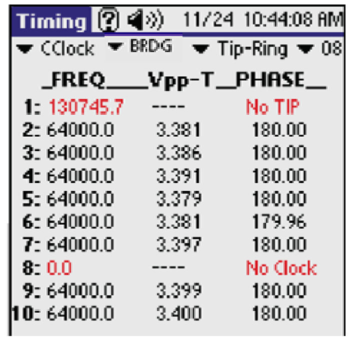


2..The default is Composite Clock, Bridged, Tip-Ring, Input 00. While the Gb310-RITS is capable of measuring up to 10 simultaneous inputs, we will view a single CC link.

3..Tap the icon at top of screen: Auto:TSG and the test set will automatically begin sequencing through each of the ten inputs.



The Gb310-RITS automatically scans all 10 links, performing analysis on the CC under test. All readings in BLACK are acceptable; all readings in RED are unacceptable. For the CC to be deemed acceptable, all readings must be BLACK. Any RED readings indicate a CC failure.



3.4.1 NOTE- This test may be performs locally, or the Gb310-RITS may be monitored via IP connection from a remote site.

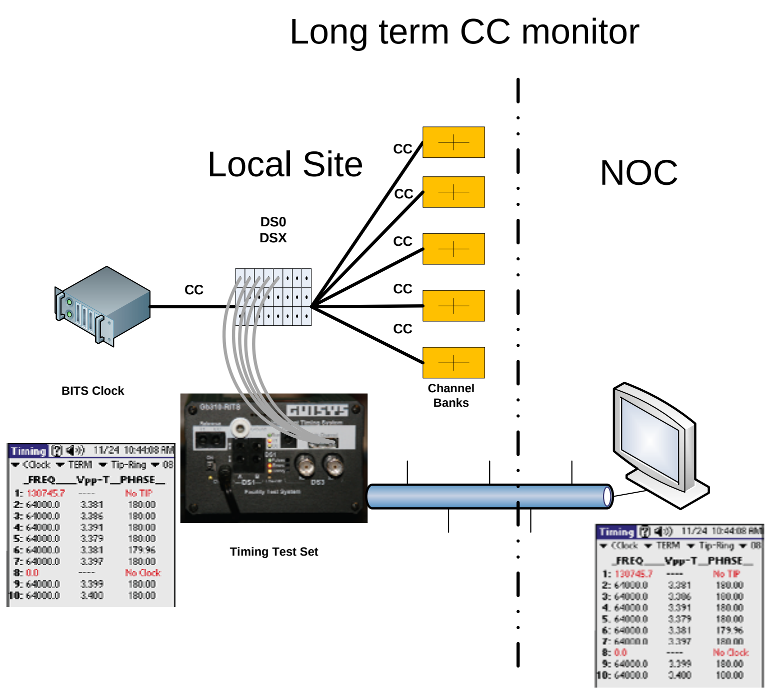
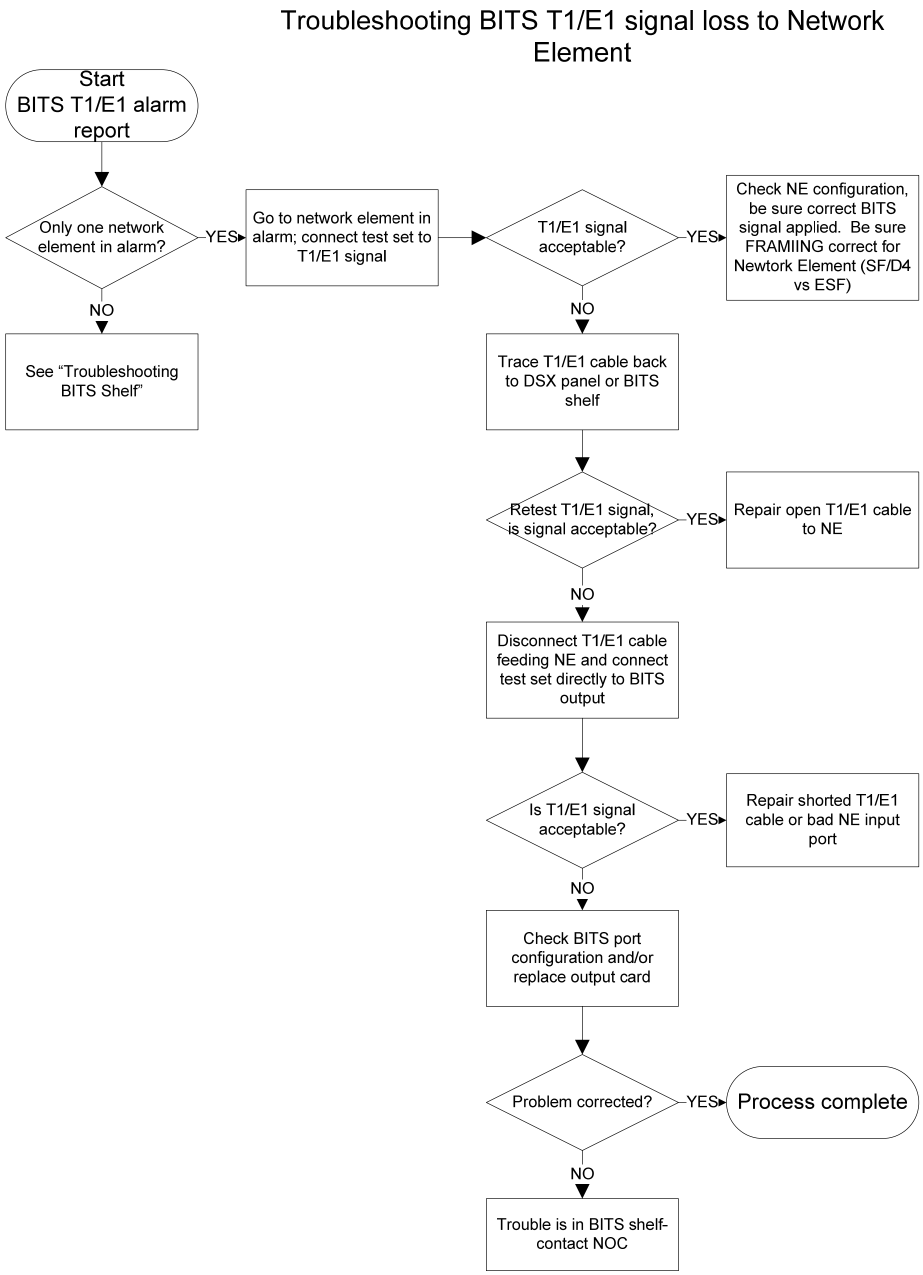


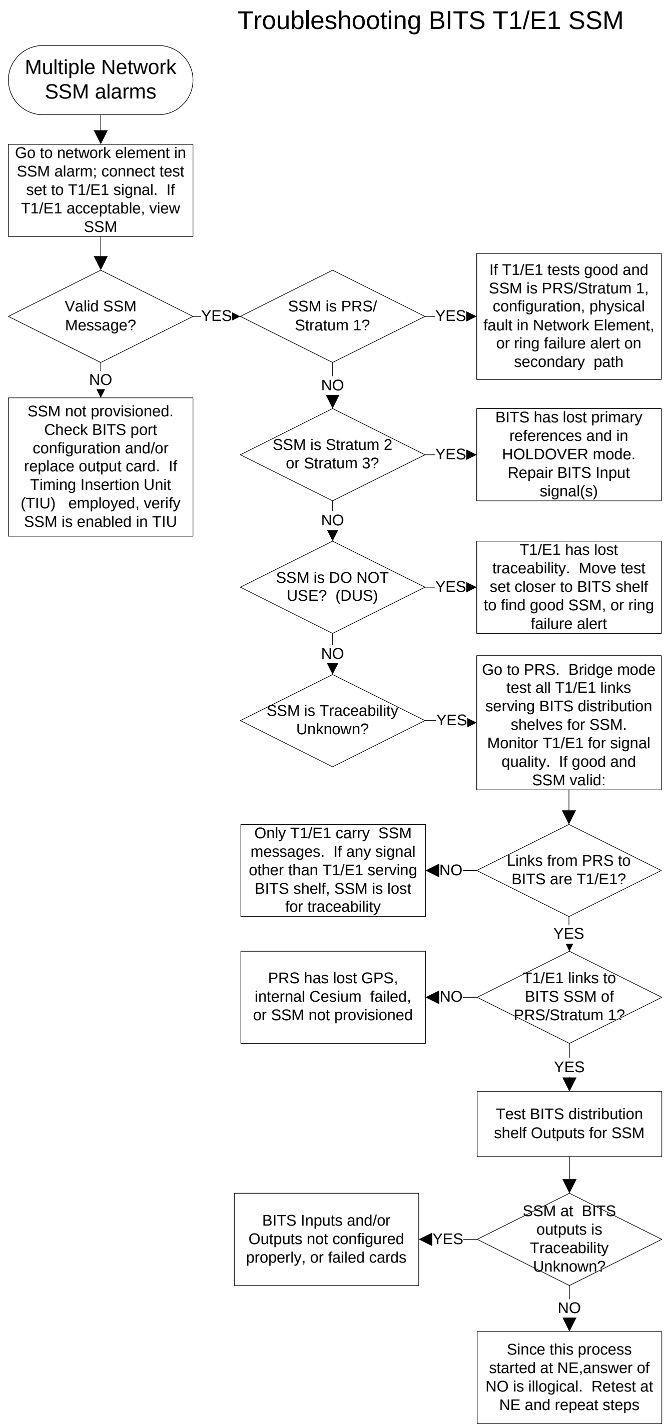
Fig. 69
Remote Monitoring of Multiple CC Signals

4.0 Troubleshooting T1/E1 Synchronization Links including SSM

4.0.1 The flowchart below provides the basic direction for responding to a T1/E1ailure to an existing Network Element. This process is also useful for validating a new T1/E1 link connection. Detailed steps for this flowchart appear on the following pages. The next page contains a flowchart for troubleshooting SSM problems on T1/E1 links.



Flow Chart 6
Unsuccessful PING of NTP Server



Flow Chart 7
Troubleshoot SSM on T1/E1

4.0.2 Troubleshooting T1 synchronization links including SSM

The BITS T1/E1 circuit will be tested at the following location(s): Test Point A- at the BITS card output connector or closest termination point; Test Point B- at the DS1 DSX (or equiv, if present); Test Point C- at the Network Element Input connector.

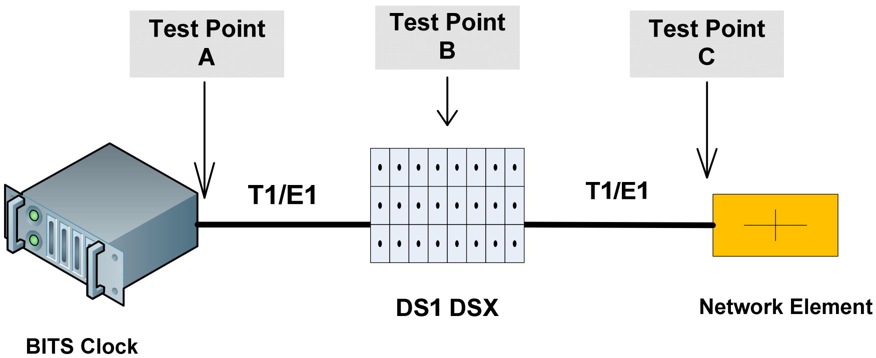


Fig. 70
Test Points for T1/E1 BITS Output Circuits

4.1.0 Step 1- Measure T1/E1 Signal at Testpoint C

Connect a GUISYS Model Gb310-RITS Intelligent Timing Test Set to the T1/E1 signal at the Network Element Sync Input connection. The Gb310-RITS is a portable, multi-purpose test set with special features for analyzing T1, E1 and CC BITS signals.

To power on instrument, lift power switch toward top.

After configuring test set, use the DS1 A RX Input- Bantam jack.

Configuration steps are shown below.

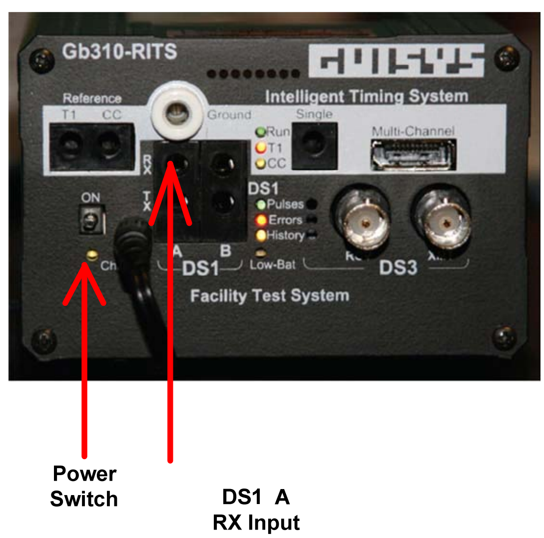
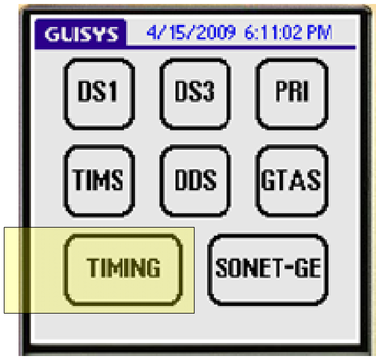
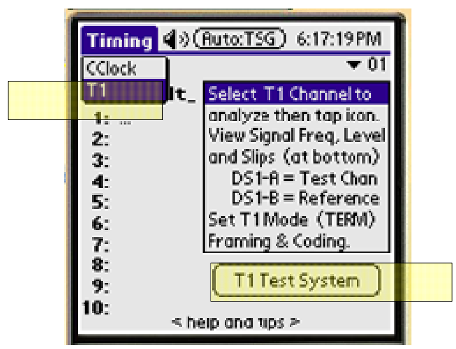


Fig. 71
Test Set Connections for T1/E1 Signals

1..At Power-Up, tap TIMING from the touch-sensitive Main Menu area.



2..The default is Composite Clock, but we will change this to T1 by tapping the dropdown menus beside CClock. Select T1 (or E1), then tap T1 TEST SYSTEM in lower portion of screen (or E1 TEST SYSTEM if selected). While the Gb310-RITS is capable of measuring up to 10 simultaneous inputs, we will view a single T1/E1 link.



3..Tap the dropdown menu beside DS1 MONITOR and select the appropriate termination based on the drawing on the next page.

4.1.1

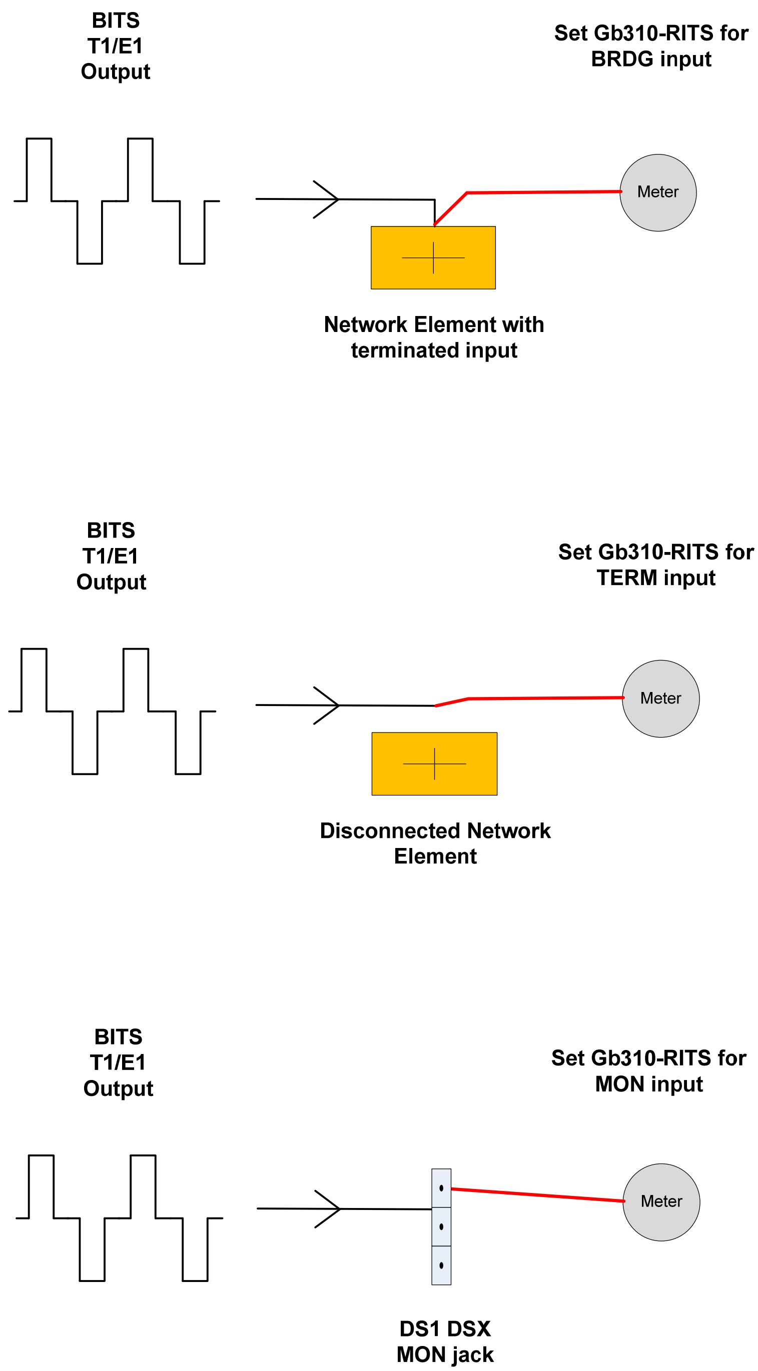
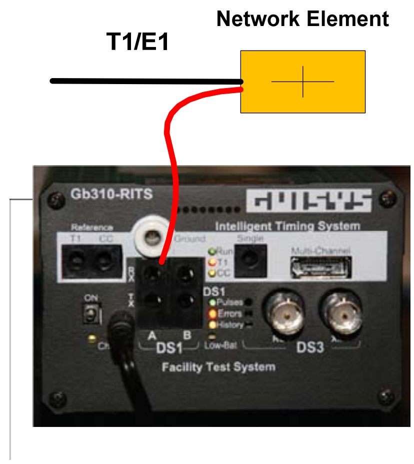


Fig. 72
Test Set Termination Options for T1/E1

4.1.2

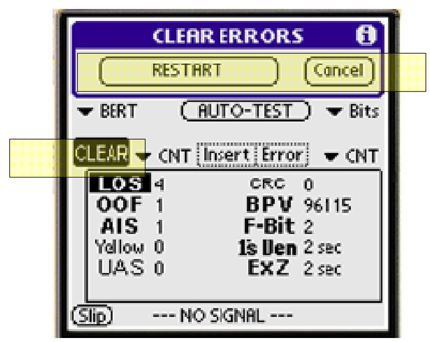


GUISYS Model Gb310- RITS
Intelligent Timing Test Set

4.. Use Bantam-to-Alligator Cable to tap onto the T1/E1connections. Insert Bantam plug into "DS1 A RX" jack on Gb310-RITS as shown at right. Be sure test set input set to BRDG.

Fig. 73
Test Set Connection at NE

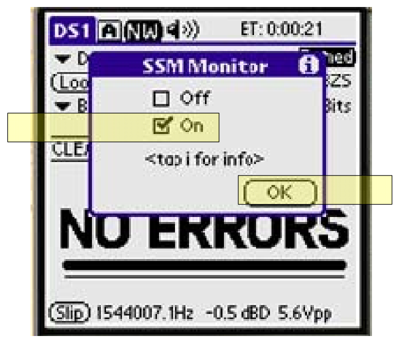
5.. Tap CLEAR, then tap RESTART to restart T1/E1 analysis.



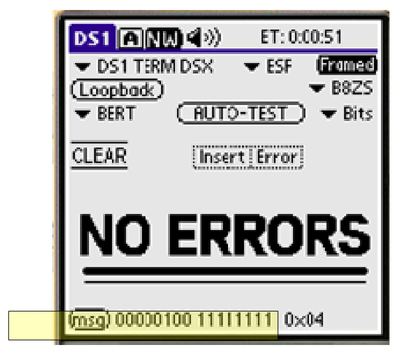
6.. If T1/E1 is in spec and acceptable for use, NO ERRORS appears on screen, with frequency and power level displayed at bottom of screen.

dB levels

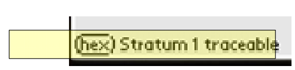
4.1.3



7..To view Sync Status Messages (SSM), tap the DS1 tab at top of screen to reveal the OPTIONS menu. Tap SSM MONITOR, check ON and OK.



8..The SSM is displayed in Binary/HEX at bottom of screen, but may also be viewed as text by tapping msg. When viewing text, switch to Binary/HEX by tapping hex.



4.1.3.1 While the Gb310-RITS automatically displays the SSM in text, advanced users may also desire to review the actual codes in binary or hex. The tables below identify the appropriate codes for each SSM.

The SSM status of a source signal depends on the classification of the source generator. For example, a device classified as a Primary Reference Source has a differing set of criteria as a BITS Clock with internal GPS Receivers relating to the change status for SSM.

Generally speaking, if a PRS or BITS Clock w/GPS Receiver is warmed up, it should be at Stratum 1. Therefore, for existing systems, your expectation should always be Stratum 1. However, the rules for SSM status change vary by class of elements, so consult the User's Guide to determine the appropriate SSM for each condition (loss of GPS, etc.). Many Synchronization devices perform better than the standard, so removing the GPS antenna on a system that is warmed will not cause an immediate change in SSM if the system can maintain Stratum 1 for a period without the GPS reference. Consult the User's manual or manufacturer to determine proper test sequences for all Synchronization elements.

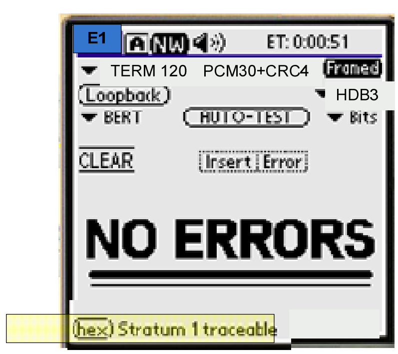
T1 Sync Status Message	DS1 Data Link/FDL (Binary)	DS1 Data Link/FDL (HEX)
Stratum 1 (PRS) Traceable	00000100 11111111	0x04
Sync Traceability Unknown (STU)	00001000 11111111	0x08
Stratum 2 Traceable	00001100 11111111	0x0C
Transit Node Clock	01111000 11111111	0x78
Stratum 3E Traceability	01111100 11111111	0x7C
Stratum 3 Traceable	00010000 11111111	0x10
Stratum 4 Traceable	00101000 11111111	0x28
Don't Use for Sync (DUS)	00110000 11111111	0x30

Table 5
SSM codes for T1[2.7]

E1 Sync Status Message	Sa Bit Message	
G.811 (PRS) Traceable	0010	
Sync Traceability Unknown	0000	
SSU-A Traceable	0100	
SSU-B Traceable	1000	
Synchronous Eq Timing Source	1011	
Don't Use for Sync (DUS)	1111	

Table 6
SSM Codes for E1[2.7]

The preceding examples showed T1. Below is a sample outputs for an E1 measurement:



4.2.0 Step 2- Measure T1/E1 Signal at Testpoint B
4.2.1 Connect a GUISYS Model Gb310-RITS Intelligent Timing Test Set to the T1/E1 signal at the DS0 DSX connection.

Configure the test set as per Step 1, and set Termination for TERM

Connect a Bantam-to-Bantam cable from the DS1 DSX OUT jack facing the BITS system into the Gb310-RITS "DS1 A RX" as shown below. NOTE- this will open the T1/E1 circuit toward the Network Element, terminating the T1/E1 signal into the test set.

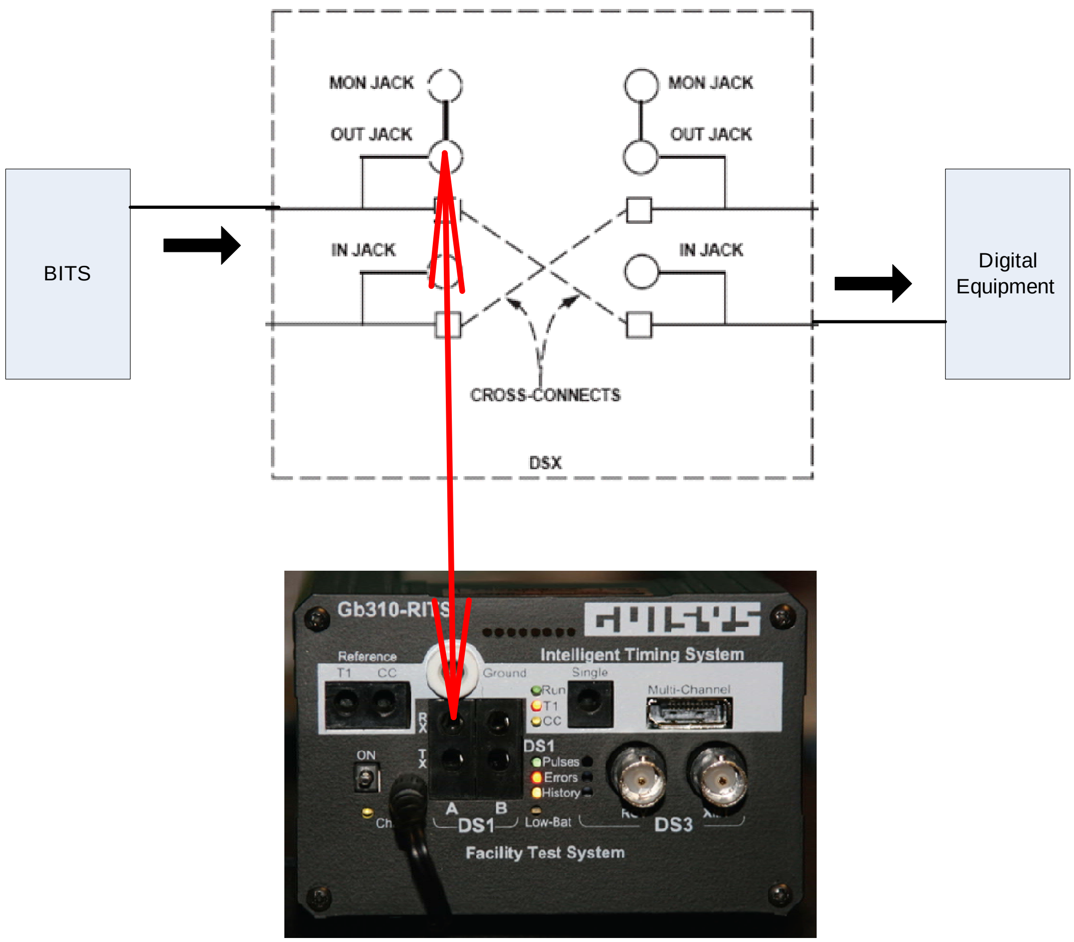


Fig. 74
Test Set Connections at DSX for T1/E1

For non-service-affecting testing, connect test cord to MON jack and set test set termination to MON.

If the T1/E1 signal passes all tests NO ERRORS displayed on screen, the signal is within specification. If the T1/E1 signal is useable at the DS1 DSX toward the BITS system, but fails at the Network Element location, probable causes:

- Mis-wired DS1 DSX jacks
- Faulty cable between DS1 DSX and Network Element
- Multiple NE terminations on T1/E1cable
- Distance to Network Element exceeds BITS system limits
- Improper T1/E1 cable type- see **OVERVIEW** section for more information.

Use Volt-Ohm Meter to measure T1/E1cable between DS0 DSX and Network Element for physical faults such as opens, shorts or grounds. If continuity good and no physical faults, review allowable distance from BITS system to Network Element in BITS Users Manual.

View SSM on T1/E1 link. If not proper Sync level, refer to **Troubleshooting SSM flow chart** for instructions.

If T1/E1 signal fails tests at DS1 DSX, move on to Step 3 on next page.

4.3.0 Step 3- Measure T1/E1 Signal at Testpoint A
4.3.1 Disconnect the cable to Network Element; connect a GUISYS Model Gb310-RITS Intelligent Timing Test Set "DS1 A RX" jack directly to the T1/E1 signal at the BITS shelf or closest terminating point to the BITS shelf.

Configure the test set as per Step 1, and set Termination for TERM

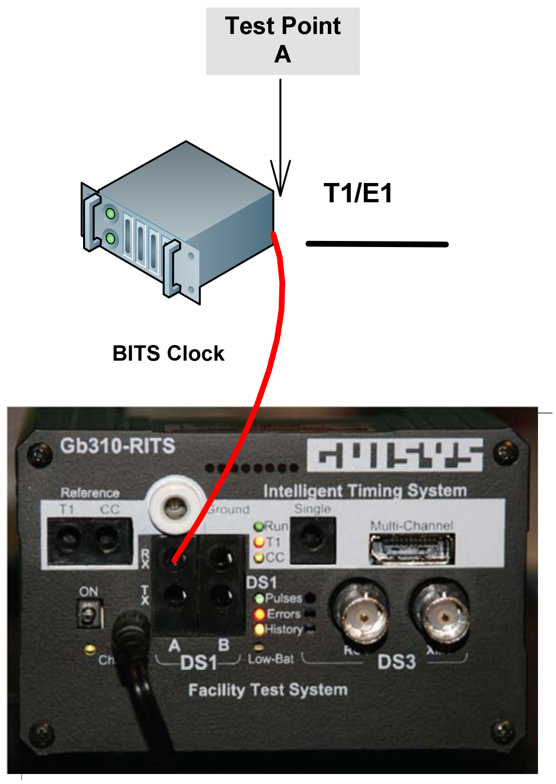


Fig. 75
Test Set Connection at BITS Shelf

If the T1/E1 signal passes all tests (screen reads NO ERRORS), the signal is within specification. If the T1/E1 signal is useable at the BITS shelf Output, but fails at the DS1 DSX location, probable causes:

- Mis-wired DS1 DSX jacks
- Faulty cable between BITS shelf and DS1 DSX
- Distance to DS1 DSX exceeds BITS system limits
- Improper T1/E1 cable type- see **OVERVIEW** section for more information.

Use Volt-Ohm Meter to measure T1/E1 cable between BITS shelf Output and DS1 DSX for physical faults such as opens, shorts or grounds. If continuity good with no physical faults, review allowable distance from BITS system to DS1 DSX in BITS Users Manual. If T1/E1 signal fails tests at BITS shelf Output, Output Card is faulty or improperly configured. Call NOC or review Users Manual for troubleshooting Output Card.

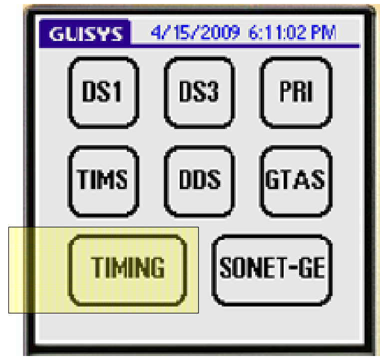
4.4.0 Monitoring or testing multiple T1/E1 links simultaneously
The GUISYS Model Gb310-RITS Intelligent Timing Test Set may also be used to monitor or test up to 10 T1/EE1 links simultaneously. This is extremely useful for commissioning a new BITS system or long-term monitoring a site for intermittent failures.

To monitor multiple T1/E1 links, the GUISYS Model Gb310-RITS Intelligent Timing Test Set may be connected to an optional cable with various connector arrangements. Select the appropriate connector type and connect up to 10 T1/E1 links to the cable.

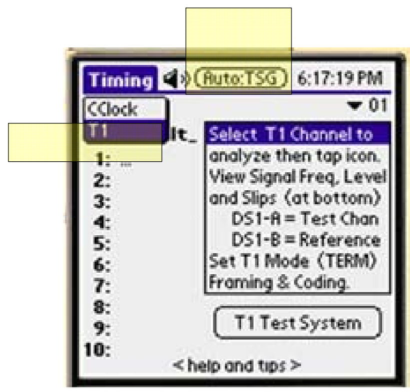
The Gb310-RITS can be configured to scan all 10 T1/E1 inputs continuously as shown on next page.

Fig. 76
Simultaneous Testing of Multiple T1/E1

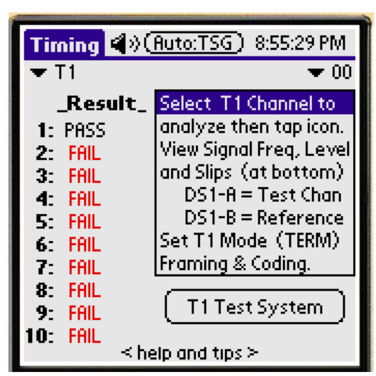
1.. At Power-Up, tap TIMING from the touch-sensitive Main Menu area.



2.. Tap CClock for dropdown menu, tap T1 to select T1. Make sure far right number is 00 (if 01, tap and change to 00).



3.. Tap the icon at top of screen: Auto:TSG and the test set will automatically begin sequencing through each of the ten inputs.



4.4.1 **The SSM and/or T1/E1 circuits may also be monitored remotely:**

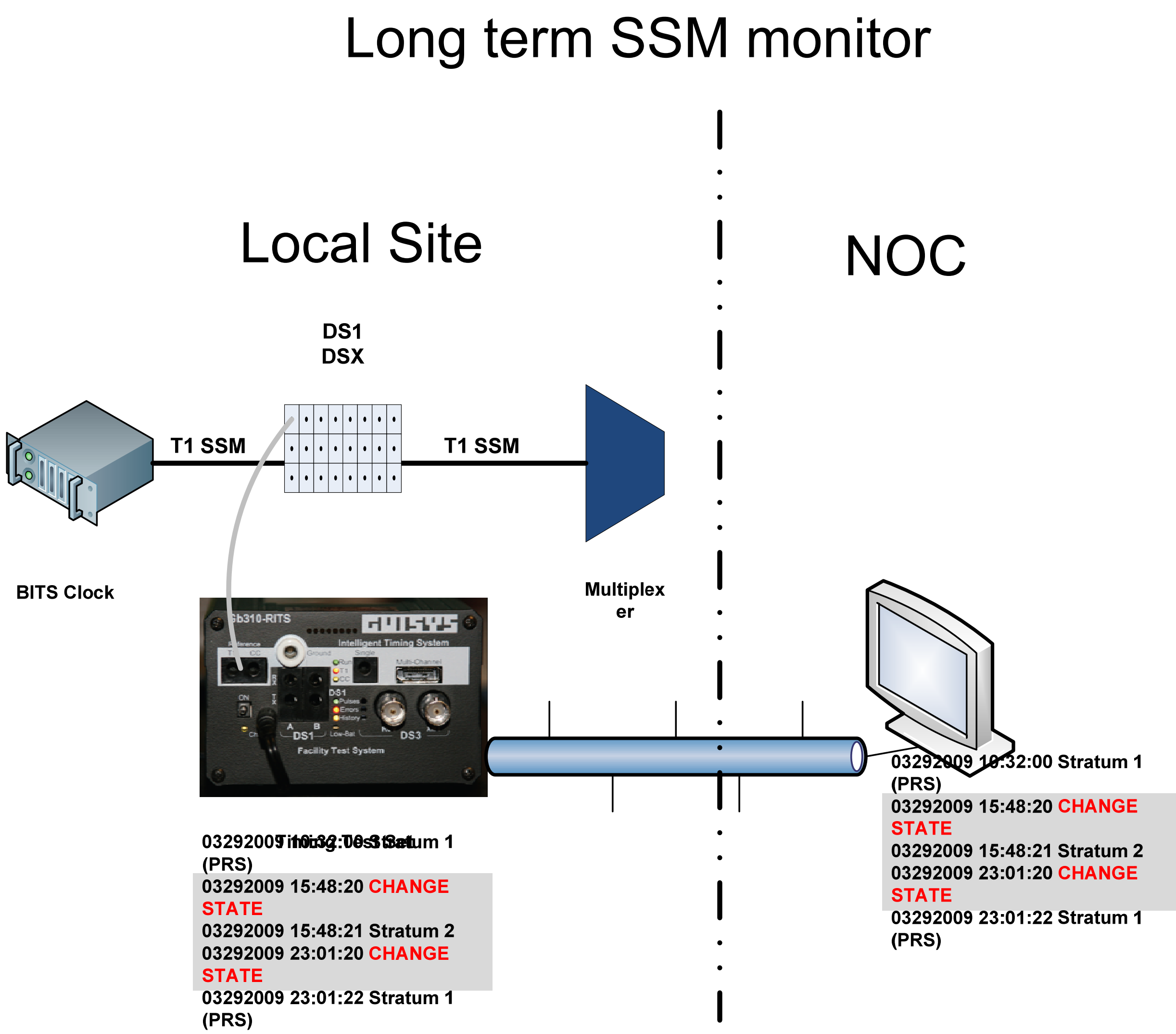


Fig. 77
Remote Monitoring of T1/E1 Signals

5.0 Measuring Slips across BITS Outputs and Network Elements

The preceding BITS Output measurements all dealt with a single or multiple signals viewed independently against the standard signal masks. However, even if the T1/E1 or Composite Clock (CC) signal meets the parametric measures, it must still be examined against a reference to determine if it is truly “in sync” with similar synchronization signals of the same type.

The **Introduction Section** examined the need for synchronization of Network Elements; timing slips are harmful to all transmission payloads. Therefore, several methods may be used to verify the stability of a timing signal:

- ***Reference against other signal from same BITS shelf***
- ***Reference against other signal not from the same BITS shelf***
- ***Reference against a temporary GPS source***
- ***Reference across the Network Element.***

5.1.0

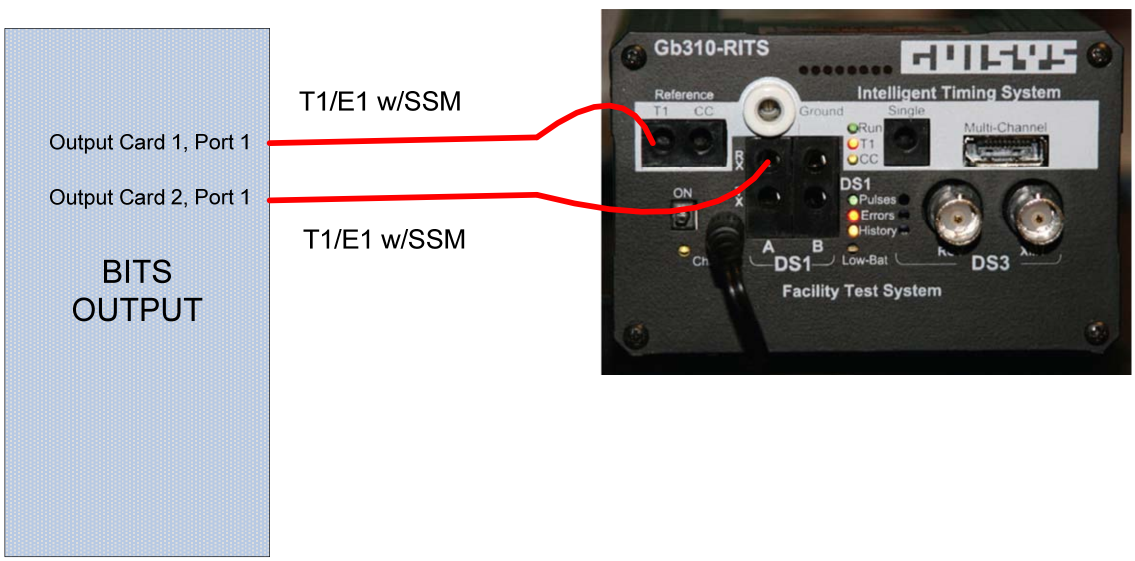
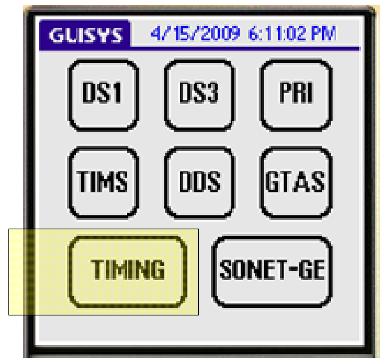


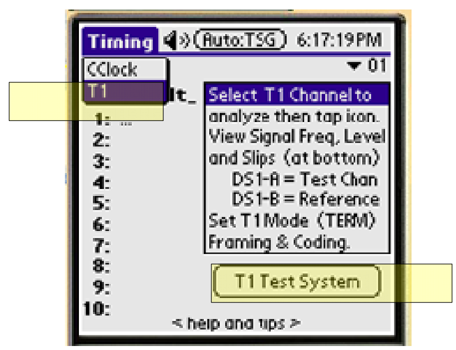
Fig. 78
Reference against other T1/E1
Signal from same BITS shelf

5.1.1

1..At Power-Up, tap TIMING from the touch-sensitive Main Menu area.



2..The default is Composite Clock, but we will change this to T1 by tapping the dropdown menus beside CClock. Select T1 (or E1), then tap T1 TEST SYSTEM in lower portion of screen (or E1 TEST SYSTEM if selected).



3..Tap the dropdown menu beside DS1 MONITOR and select the appropriate termination based on the drawing on the next page. After termination selected, tap Slip in lower left of screen.

NOTE- select proper termination from list below:

- If terminating a T1/E1 directly to the test set, select TERM
- If tapping onto a T1/E1 that is already terminated into a Network Element, select BRDG
- If plugging into a MON jack at DSX, select MON

The Gb310-RITS compares the input signal with the reference signal. If the signals are both stable, Slips will be zero (0) as shown at right above. If Slips present, BITS Output cards bad or not configured properly.

5.2.0

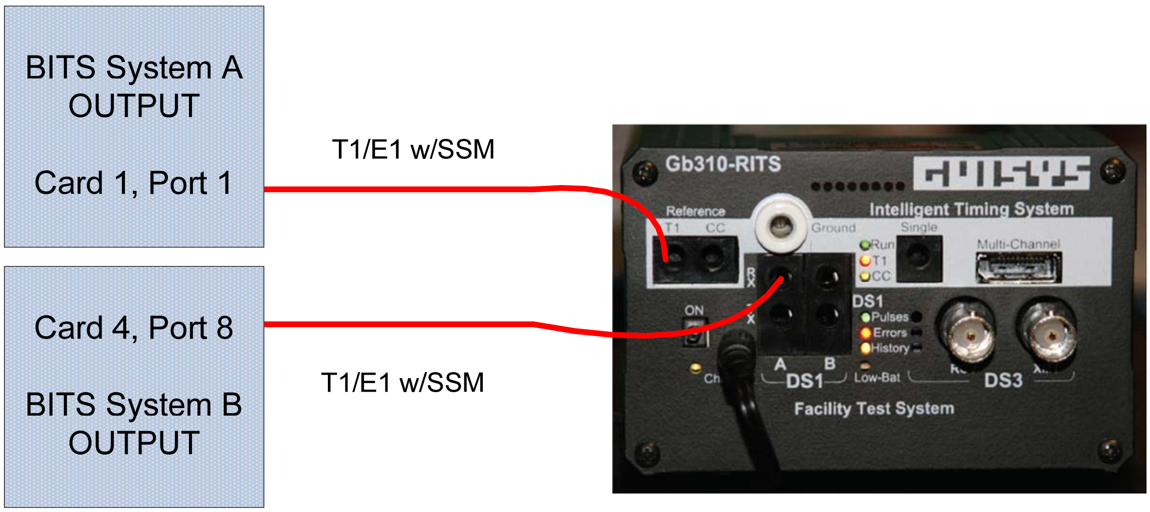
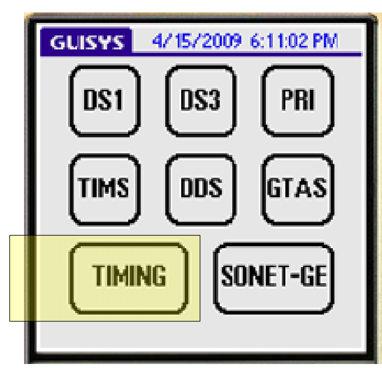


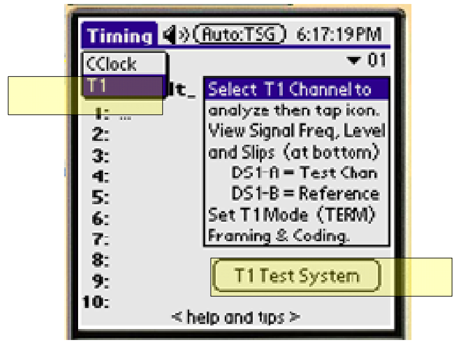
Fig. 79
Reference against other T1/E1
Signal NOT from same BITS shelf

5.2.1

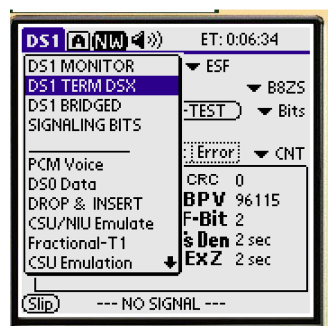
1..At Power-Up, tap TIMING from the touch-sensitive Main Menu area.



2..The default is Composite Clock, but we will change this to T1 by tapping the dropdown menus beside CClock. Select T1 (or E1), then tap T1 TEST SYSTEM in lower portion of screen (or E1 TEST SYSTEM if selected).

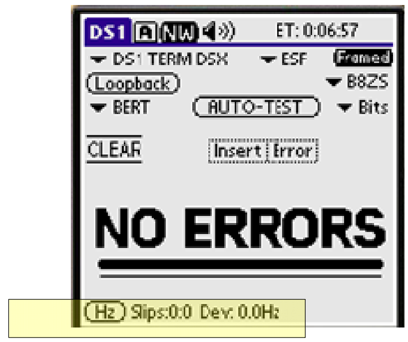


3..Tap the dropdown menu beside DS1 MONITOR and select the appropriate termination based on the drawing on the next page. After termination selected, tap Slip in lower left of screen.



NOTE- select proper termination from list below:

- If terminating a T1/E1 directly to the test set, select TERM
- If tapping onto a T1/E1 that is already terminated into a Network Element, select BRDG
- If plugging into a MON jack at DSX, select MON



The Gb310-RITS compares the input signal with the reference signal. If the signals are both stable, Slips will be zero (0) as shown at right above. If Slips present, trace BITS shelf Inputs to be sure both shelves are referenced to a PRS.

5.3.0

The setup shown below may be used to determine if the local BITS outputs are drifting. However, this setup is extremely useful when testing a T1/E1 signal with unknown origin of synchronization. For example, a small Central Office may be assumed to be "timed" by an incoming T1/E1 from a larger carrier. However, this is extremely risky and usually leads to future synchronization troubles. Use the setup below to measure the stability of any T1/E1 signal. You will quickly discover if the signal is traceable or if it is from a "free-run" source. This includes traffic-bearing T1/E1 circuits.

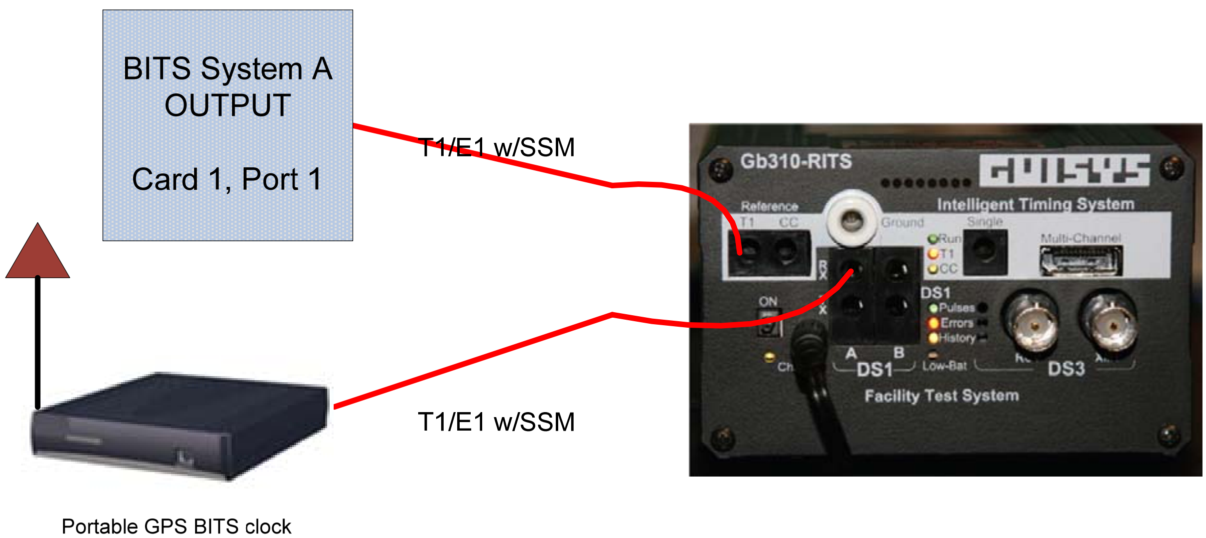
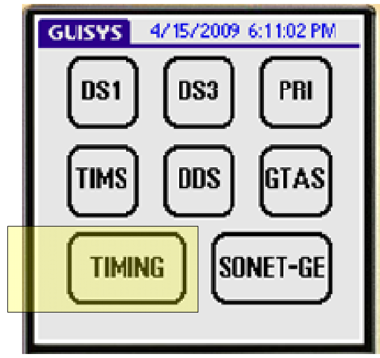


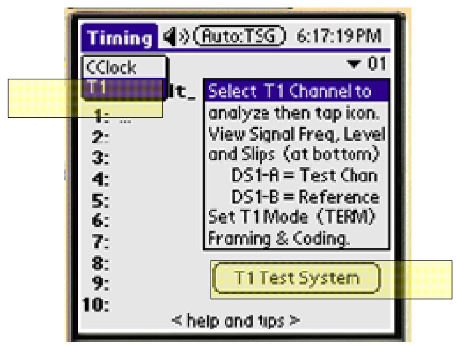
Fig. 80
Reference against a
Temporary GPS source [2.8]

5.3.1

1..At Power-Up, tap TIMING from the touch-sensitive Main Menu area.



2..The default is Composite Clock, but we will change this to T1 by tapping the dropdown menus beside CClock. Select T1 (or E1), then tap T1 TEST SYSTEM in lower portion of screen (or E1 TEST SYSTEM if selected).



3..Tap the dropdown menu beside DS1 MONITOR and select the appropriate termination based on the drawing on the next page. After termination selected, tap Slip in lower left of screen.

NOTE- select proper termination from list below:

- If terminating a T1/E1 directly to the test set, select TERM
- If tapping onto a T1/E1 that is already terminated into a Network Element, select BRDG
- If plugging into a MON jack at DSX, select MON

The Gb310-RITS compares the input signal with the reference signal. If the signals are both stable, Slips will be zero (0) as shown at right above.

If Slips present, troubleshoot PRS and BITS system per previous Troubleshooting Flowcharts.

5.4.0

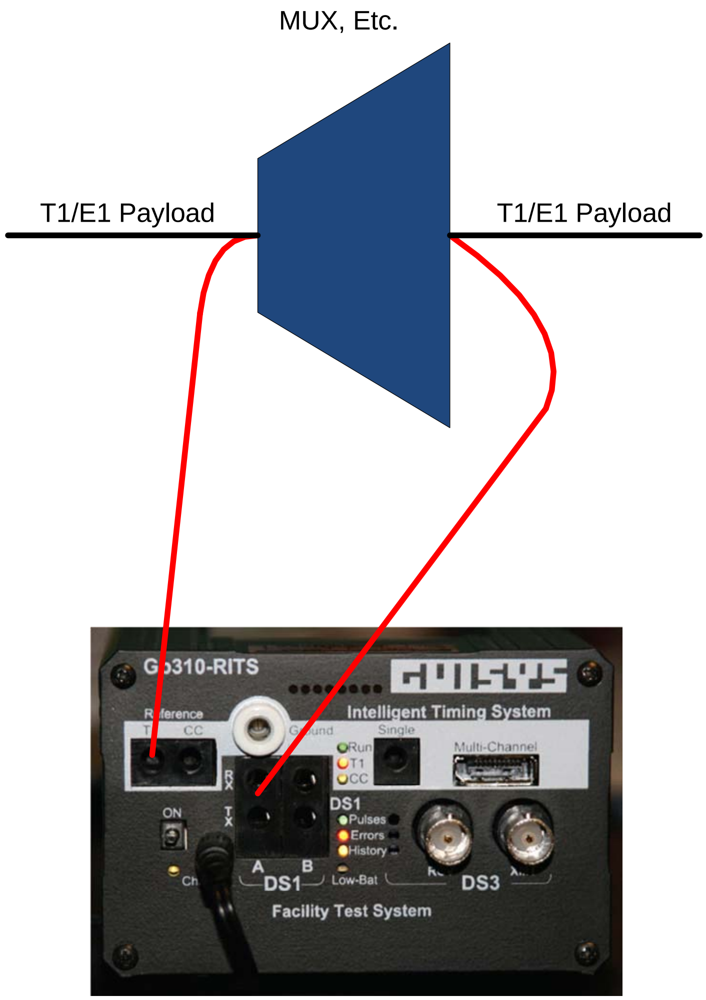
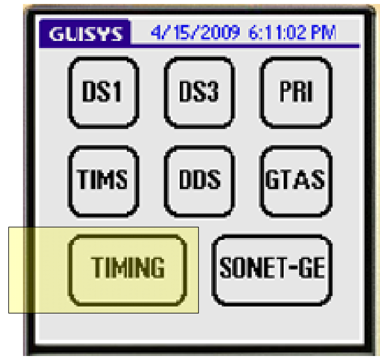


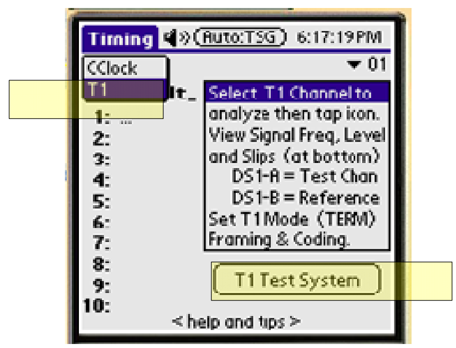
Fig. 81
Reference across a
Network Element

5.4.1

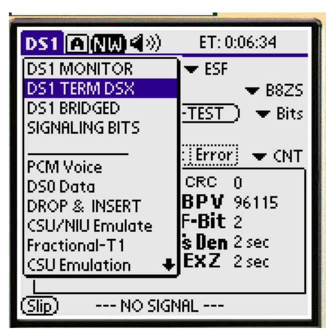
1..At Power-Up, tap TIMING from the touch-sensitive Main Menu area.



2..The default is Composite Clock, but we will change this to T1 by tapping the dropdown menus beside CClock. Select T1 (or E1), then tap T1 TEST SYSTEM in lower portion of screen (or E1 TEST SYSTEM if selected).

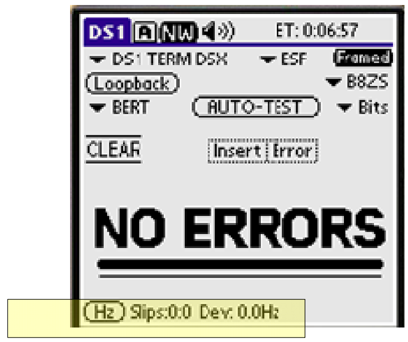


3..Tap the dropdown menu beside DS1 MONITOR and select the appropriate termination based on the drawing on the next page. After termination selected, tap Slip in lower left of screen.



NOTE- select proper termination from list below:

- If terminating a T1/E1 directly to the test set, select TERM
- If tapping onto a T1/E1 that is already terminated into a Network Element, select BRDG
- If plugging into a MON jack at DSX, select MON



The Gb310-RITS compares the input signal with the reference signal. If the signals are both stable, Slips will be zero (0) as shown at right above.

If Slips present, Network Element is not configured properly to maintain synchronization on output ports.

6.0 BITS System Turn-Up Testing

Once a PRS and BITS distribution system have been installed, several commissioning tests will insure the system is properly configured and equipped:

- ***PRS Output performance and SSM test***
- ***PRS loss of GPS SSM test***
- ***BITS Distribution Shelf Input test***
- ***BITS Distribution Shelf loss of Input test***
- ***BITS Timing Loop Test***
- ***BITS Distribution Output test***

Instructions for performing the above tests are included in each preceding section. The information below will provide a template for BITS System turn-up testing.

6.1 PRS Output performance, Loss of GPS and SSM tests

1. Connect a GUISYS Model Gb310-RITS Intelligent Timing Test Set to the T1/E1 signal at the PRS Output connector.
2. Confirm Output signal passes performance tests (NO ERRORS) on screen.
3. View SSM, insure Stratum 1 displayed.
4. Perform Steps 1 – 3 above for all PRS outputs.
5. Measure Slips from PRS Output Port 1 against all other PRS T1/E1 Output Ports. Insure zero (0) Slips.
6. Disconnect GPS Antenna(s), view SSM on Output Ports. Insure SSM changes from Stratum 1 to appropriate holdover value if PRS equipped with internal oscillator (Stratum 2/2E for Rubidium; Stratum 3/3E for Crystal). If no oscillator, insure SSM is "Traceability Unknown" or "Do Not Use for Synchronization".

6.2 BITS Distribution Shelf Input and loss of Input Tests

1. Connect a GUISYS Model Gb310-RITS Intelligent Timing Test Set to the T1/E1 or Composite Clock (CC) signals at the BITS Distribution Shelf Input connectors.
2. Confirm Input Signals pass performance tests: NO ERRORS on screen for T1/E1; all readings BLACK for CC.
3. Confirm T1/E1 Input signal SSM at Stratum 1. (CC does not have SSM).
4. Connect a GUISYS Model Gb310-RITS Intelligent Timing Test Set to the T1/E1 signals at the BITS Distribution Shelf Input connector, and disconnect T1/E1 signals feeding BITS Distribution Shelf. Observe SSM changes from Stratum 1to appropriate holdover value (Stratum 2/2E for Rubidium Holdover Oscillator; Stratum 3/3E for Crystal Holdover Oscillator).

6.3 BITS Timing Loop Test

1. Connect a GUISYS Model Gb310-RITS Intelligent Timing Test Set to the T1/E1 signals at the BITS Distribution Shelf Input connectors.
2. View SSM, insure Stratum 1.
3. Connect a 2nd GUISYS Model Gb310-RITS Intelligent Timing Test Set to a T1/E1 signal at the BITS Distribution Shelf Output connector.
4. Remove all Inputs to BITS Distribution Shelf. Observe SSM change at Output.
5. View T1/E1 signals that had been inputs to BITS Distribution Shelf, ensure they are still at Stratum 1. The SSM status changes of the BITS Outputs should have no effect on the SSM status of the BITS Input signals. If the BITS Input SSM changes follow the BITS Output SSM changes, a Timing Loop exists and must be corrected.

6.3.1 BITS Frame Slip Test

1. Connect a GUISYS Model Gb310-RITS Intelligent Timing Test Set to all Output Ports on the BITS Distribution Shelf. Record results for all outputs. If any output fails, determine if output is configured properly. NOTE- this can be quickly accomplished by utilizing an optional Multiple Input cable, as the Gb319-RITS can qualify up to ten (10) inputs simultaneously.
2. Perform Slip tests between at least one (1) port per card, per shelf. Correct any Slips prior to placing BITS into serve.

7.0 Manufacturing Tests

The Gb310-RITS Intelligent Timing Test Set can evaluate T1, E1 and Composite Clock (CC) signals, providing direct SSM readout. In the manufacturing community, this is useful for validating such output signals and ensuring proper SSM codes are being sent from the Network Element under test. Conversely, the Gb310-RITS can emulate (send) T1/E1 signals with variable SSM codes, allowing manufacturers to test Network Elements under simulated BITS degradation conditions.

Instructions for measuring BITS output signals and reading SSM codes are included previously in this publication. The following instructions describe setups for emulating SSM into Network Elements under test:

- ***Simple Test- Single Network Element***
- ***Advanced Test- Validating SSM in SONET/PDH Rings***

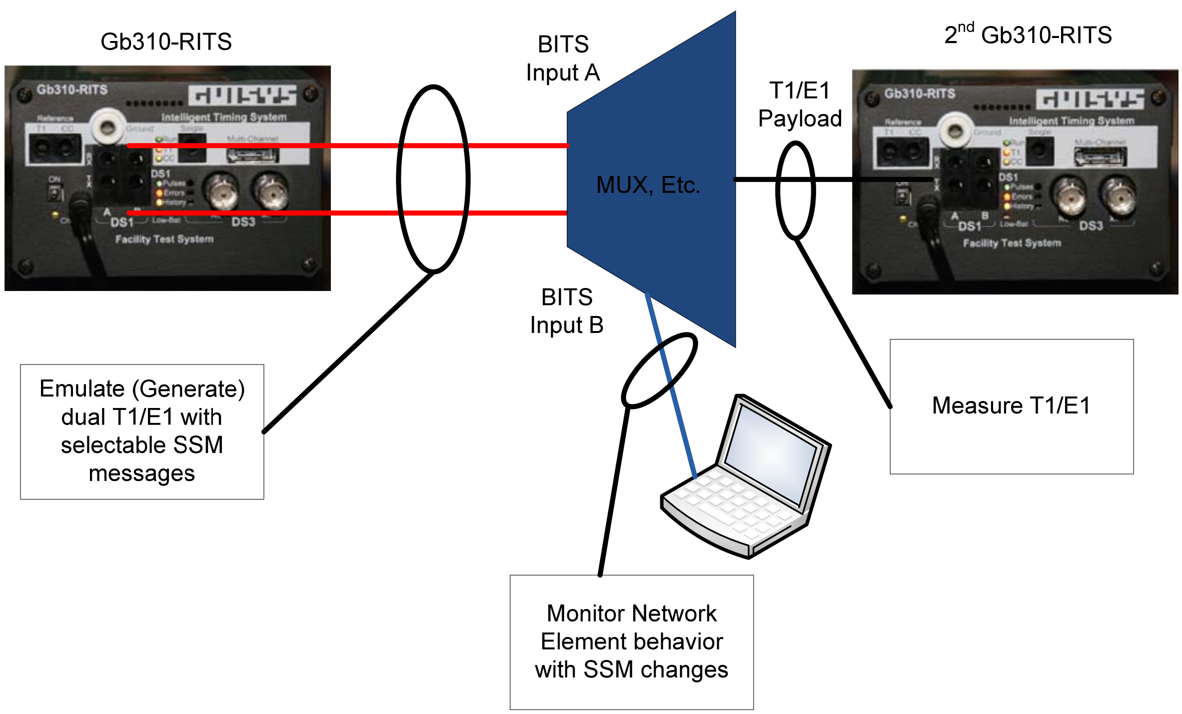


Fig. 82
Manipulating SSM for
Single Network Element

7.1 Figure 82 above depicts manipulation and techniques for measuring results as various SSM messages are transmitted. Fig. 83 below depicts the setup for manipulating SSM messages on a SONE/PDH ring network. At the outset, BITS Inputs A & B would both be set to Stratum 1. After allowing the network to normalize, BITS Input A would be changed to Do Not Use or any other code below Stratum 1. The Network Elements could all be polled to determine if they adjusted their timing to the BITS Input B on the opposite path.

7.2

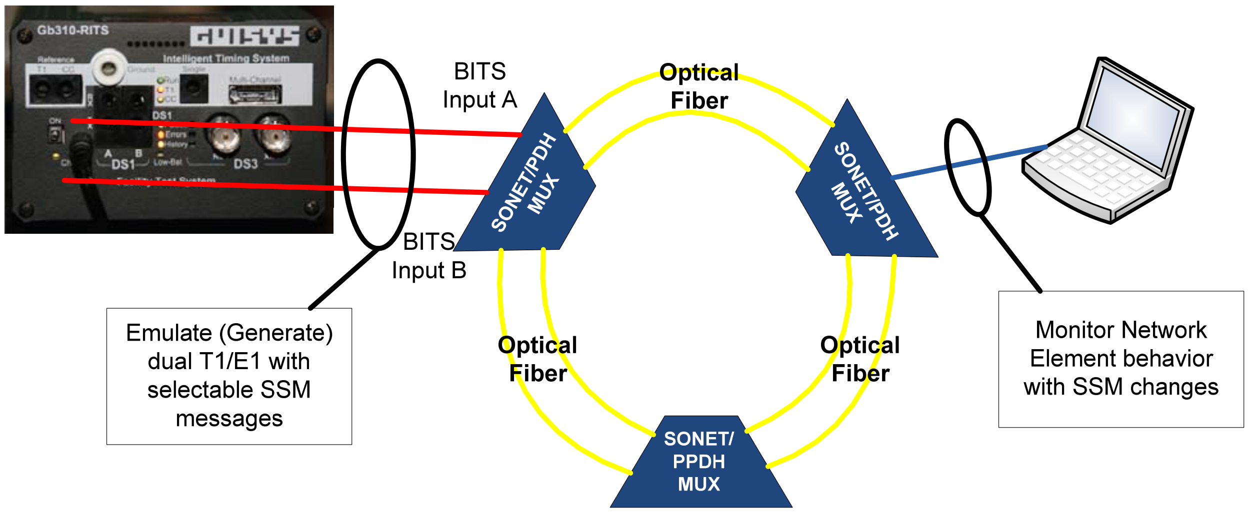


Fig. 83
Manipulating SSM for
Multiple Network Elements