INSTALLATION AND MAINTENANCE MANUAL
Tsunami FAMILY
FAST ETHERNET WIRELESS BRIDGES
December 2001

WESTERN
Multiplex

4. Troubleshooting

Also refer to Appendix E fold-out as an additional guide

Requirements for Full Duplex

For a network to support Full Duplex, both devices must support and be configured for Full Duplex. Full Duplex is intended to increase the speed of a direct link between two devices. i.e., between switches, or between an end-station and a switch. Switches support Full Duplex, hubs do not. Configuring an adapter for Full Duplex operation while connected to a hub or other half duplex device (NIC, etc.), can cause many network issues such as slowness, packet loss or station drop-offs.

What is Auto-Negotiation?

Auto-Negotiation is a protocol between devices where they negotiate highest common speed. Also known in the industry as NWAY. Since every frame is tested for speed and configuration, auto-negotiation takes away from the maximum bandwidth possible through a network. When possible, do not use auto-negotiation especially when the port configuration is known (e.g. 10 or 100Base, half or full duplex, etc.). Tsunami radios are especially sensitive and work best only with devices hard set to the radio's configuration (e.g. full duplex, 10BaseT) and NOT in auto-negotiation nor auto-sense.

What is the difference between 10 and 100BaseT (or F)?

These are fully different and mostly incompatible Ethernet communication. Ten (10)Base is any throughput speed from 1bps to 10Mbps, 100Base (also known as Fast Ethernet) is any throughput from 1bps to 100Mbps with the 10BaseT standard NOT capable of transmitting the full throughput of a 100Base device. Each has its own set of communication rules and need to be considered separately when communicating with either standard. Many hubs, switches and routers will auto-negotiate between these two speeds, but Tsunami radios (in order to maximize their throughput) do NOT auto-negotiate. Many throughput problems have been found when the computer's Ethernet NIC card is set to auto-negotiate when it should be set (through Network Properties) to NOT auto-negotiate. Although if the switch, router or NIC is set for auto-negotiation, the interface will function but the throughput speed can suffer considerably and high latency can result. All NICs & routers and most "managed" switches can be hard set or programmed to not auto-negotiate (both 10/100Base and full/half duplex) and is the desired set-up for maximum Ethernet throughput with any network especially those with wireless components.

Hub Vs Switch

All the devices connected to a hub are in the same collision domain. These devices share the bandwidth of the hub (10 Mbps for Ethernet or 100 Mbps for Fast Ethernet). By contrast, each port of a switch is actually the entrance to a separate collision domain with its own dedicated bandwidth. Each domain is either shared by other devices or dedicated to a single device. If many devices and the network is utilized over 25%, a switch is necessary to optimize Ethernet traffic. If economics allow, a programmable or managed switch is desirable for many reasons such as for the reasons above and that spanning tree can be easily accomplished if needed in a network.

Response time slower with switch than it was with a hub

Low volume on the network could cause a slowness in performance when a switch is introduced into an environment where a hub was used previously. There may not be enough traffic on the network to warrant a switch. When network utilization starts to reach 25 - 30%, the conditions are good for a switching product.

W E S T E R N
M u l t i p l e x

4.1   Regular Maintenance

The *Tsunami* radios do not require any regular maintenance, however, it is prudent to monitor the radio link at regular intervals to assure that the link conditions are not changing. When visiting a radio site for maintenance, the following items may be checked and their results recorded:

- ❖ RSL Voltage

- ❖ PWR Voltage

- ❖ Far-end RSL Voltage

- ❖ Alarm conditions

- ❖ Verify radio has adequate ventilation

- ❖ Verify security ID is set the same at each radio through NMS

If any alarm conditions exist, they should be recorded, and troubleshooting procedures from this Section of the manual should be followed.

4.2   Changing Frequency Plans

The *Tsunami* RF frequency selections are listed in Section 3.5. The near-end radio and the far-end radio must be corresponding (e.g. A1 / A2). The frequency of a given *Tsunami* terminal is set by the specific filter, the physical orientation of this assembly, and a setting within the CONFIG port (or NMS configuration instructions, Section 4.11). With respect to a given filter, the frequencies are fixed, because tuned RF filters are required for normal operation. Changing of the (pre-tuned) radio frequencies may be required when installing spares or for special situations, such as interference mitigation. This is accomplished by installing an alternate filter.

☞   It is not necessary to remove the cover assembly of the Tsunami

1. Remove any cables connected to the antenna connector on the diplexer (filter) and then remove the two screws that mount the filter to the *Tsunami* chassis.

2. Slowly remove the filter from the chassis being careful to not endanger the cables that are connected to the rear side of the filter.

3. Disconnect the two SMA connectors that are attached to the rear of the filter with a 5/16" open end wrench.

4. Select the new filter such that the frequency channel label on the filter corresponds to the desired frequency channel (or rotate filter if applicable – see note below).

5. Connect the two SMA connectors to the new or reoriented filter with the 5/16" open end wrench.

6. Slowly place the wired filter assembly so that it is flush with the rear panel.

7. Install the two screws that mount the filter to the rear panel.

8. Modify the operating frequency as described in the CONFIG menus (Section 4.11)

☞   *Single-band versions of this radio can be interchanged from A1 to A2 by changing (but not rotating) the installed filter. After filter is changed, the frequency settings within the configuration menu (NMS) must be changed to match the installed filter.*

Dual-band versions of this radio also can change channels, but the orientation of low-side or high-side transmit must be retained. That is, an A1 radio can only be changed into a B1 radio with a new filter, but not into an A2 or a B2. Likewise, the A2 radio can only be changed into a B2 radio with a new filter, but not into an A1 or B1. The diplexer filters can go on any radio and must be properly oriented. After filter is changed, the frequency setting within the configuration menu (NMS) must be changed to match the installed filter.

4.3   Using a Spare Terminal

For dual-band units, a spare of each band may be required. For single-band units, one spare *Tsunami* terminal will service both channel orientations. See Section 4.2 for changing frequencies of a spare radio.

Customers with several radios, or radios in critical operations are encouraged to purchase one or more spare radios of each model in their system. This will allow rapid restoration of radio service in the unlikely event of a radio failure.

4.4   Technical Support

Western Multiplex provides 24-hour telephone technical support for installed *Tsunami* radios. Customers are encouraged to troubleshoot the radio and link in accordance with the latter part of this section in this manual before contacting Western Multiplex. Western Multiplex also has a limited supply of *Tsunami* radios that can be loaned to out-of-service customers for installation while units are being repaired. Loaner supply is limited, and is only used for critical applications on a first-come, first-served basis.

Customer service #:   +1 408 542-5390

4.5   Repair Policy

The *Tsunami* terminal includes comprehensive alarm indicators designed to diagnose potential faults. Should a fault occur, it often may be resolved by operator adjustment.

Should a fault occur that cannot be resolved by operator adjustment and has been confirmed by looping terminals together on the bench (See Section 4.9), then the equipment should be returned to the factory for repair.

The *Tsunami* radio is a complex system not designed for user repair. Do not remove the cover or open any part of the *Tsunami* terminal. The complete *Tsunami* terminal should be sent back in its original packing material for factory repair.

Please contact the factory in advance of returning the product. You will be assigned a Return Material Authorization (RMA) number that authorizes your return. Units sent to the factory without an RMA number may be delayed in the processing of the repair. Be sure to include the following information:

❖   RMA number

❖   description of the problem

❖   your name and telephone number

❖   return shipping address

❖   urgency of repair

Please refer to the published Warranty policy for repair policy details.

Tsunami radios should be packaged in their original packing boxes for shipment whenever possible Western Multiplex can provide an empty box shipment to facilitate proper packaging. Regardless, proper and adequate packaging must be used for shipments to protect the radio(s) from damage. Western Multiplex can not be held responsible for any repairs due to inadequately packed materials. Damage caused by improper packing will likely result in higher repair costs and delays (refer to the Warranty section at the beginning of this manual).

INSTALLATION AND MAINTENANCE MANUAL
Tsunami FAMILY
FAST ETHERNET WIRELESS BRIDGES
December 2001

WESTERN
Multiplex

4.6 Front Panel Status LEDs

There are several front panel status LEDs on the *Tsunami* radio. These LEDs indicate conditions where either a hardware failure has occurred or the radio link is not optimum. In many cases, a combination of LEDs may be illuminated. The following sections describe the necessary troubleshooting procedures should any LED(s) indicate a problem during or after installation.

Radio Fail	Green = Radio hardware O.K. Red = Hardware failure detected
RF Link	Green = Error-free operation Yellow = Bit errors occurring Red = Excessive bit errors or radio link failure ***Flashing Red = Link security ID mismatch***
TXD	Green = 100BaseT data to be transmitted at near end present Yellow = 100BaseT port connected (no data present) Off = No 100BaseT connection detected
RXD	Green = 100BaseT data received from far end present Yellow = 100BaseT port connected (no data present) Off = No 100BaseT connection detected
COLL	Yellow = Collisions occurring on 100BaseT (half-duplex mode)
FAR END	Red = Alarm(s) present on the far-end radio**
NMS (10BaseT)	Green = Tx or Rx data present on the NMS interface Yellow = NMS interface connected (no data present) Off = No NMS interface connection detected
T1/E1 INPUT Note: there are two T1s on the 27720 Model and one E1 on the 27710-52 Model with the option to turn on another E1 via the browser configuration	Green = Alarm enabled and T1 connection detected Red = Alarm enabled and no T1 connection detected Yellow = Alarm disabled and T1 connection detected Off = Alarm disabled and no T1 connection detected

** Radio Fail, RF Link (yellow or red), T1/E1 output (yellow or red)

Table 4-A: Front panel LEDs (Models w/o ODUs)

Alarm and Status Indicators (Models with IDU and ODU)

IDU	Green = Indoor Unit OK Yellow = warning condition in IDU (over-temp and/or both fans failed) Red = All fans failed, over-temp (>55°C), or NMU/IDU communication failure
Cable	Green = ODU Cable OK Red = ODU Cable shorted
ODU	Green = Outdoor Unit OK Red = Over-temp (>60°C), IDU to ODU communication failure, DC power loss, or Outdoor Unit detected hardware failure Yellow = Over temperature alarm, exceeds 55 degrees C
RF Link	Green = Link established with BER <10E-6 Yellow = BER 10E-6 ; any bit errors due to FEC overload Red = BER >10E-3 or Loss of Sync **Blinking Red = link ID does not match with far end radio**
TXD	Red = Links have loss of signal, both 100BaseT and 100BaseFX connector Yellow = Main Ethernet port is okay, but collision detected within the last 5 seconds or set to half duplex Green = Main Ethernet port is okay and valid data is passing thru Off (Dark) = Main Ethernet port is okay, but no data passing thru
RXD	Red = Links have loss of signal, both 100BaseT and 100BaseFX connector Green = Main Ethernet port is okay and valid data is passing thru Off (Dark) = Main Ethernet port is okay, but no data passing thru
Far End	Red = Alarm(s) present on the far-end radio** Green = No far end alarm(s) detected
NMS (10/100BaseT)	Green = Tx or Rx data present on the NMS interface Off = No NMS data, interface connection detected
E1 (or T1) WAYSIDE INPUT	Green = Wayside connection detected on enabled channels (both waysides) or channel(s) disabled Red = Wayside(s) input channel(s) enabled (either of the waysides) but eith channel has a LOS detected Yellow = One or both channels in Loopback mode

** Radio Fail, RF Link (yellow or red), T1/E1 Input (yellow or red)

Table 4-B: Front panel LEDs (Models w/ ODUs)

INSTALLATION AND MAINTENANCE MANUAL
Tsunami FAMILY
FAST ETHERNET WIRELESS BRIDGES
December 2001

W E S T E R N
Multiplex

4.6.1 RF LINK Alarm

Function:

This LED indicates that the demodulator function is not synchronizing with the intended received signal.

Possible Causes:

- ❖ Severe path fading due to atmospheric conditions, usually accompanied by low RSL voltage reading

- ❖ Poor transmission line connections usually accompanied by low RSL voltage reading

- ❖ Antenna problems, misalignment, or path clearance usually accompanied by low RSL voltage reading

- ❖ Improper radio settings (e.g. frequency channel)

- ❖ Received signal level (RSL) is too strong

- ❖ Interference

- ❖ Far-End radio transmitter circuitry is faulty

- ❖ Near-End radio receiver circuitry is faulty

- ❖ Link security ID not the same for each radio

Recommended Actions:

Check the following at each end of the link:
- ❖ Verify that rear panel filters are opposite channel plans on each end (e.g. one is A1 and other is A2).
- ❖ Verify that radio frequency settings match each installed filter (in NMS menus).
- ❖ Verify that all connections between radios and antennas are secure and all devices between radios and antennas are rated for the radio frequency band (5.3/5.8 GHz).

Measure RSL by placing a voltmeter across RSL and GND test points. Compare this voltage to the Factory Test Data Sheet and estimate the RSL in dBm. Compare this to the RSL that was expected using path calculations (see Section 3.3.3). Press and hold the DISPLAY FAR END button and measure the far-end RSL (while continuing to hold the button) or on those models w/o FAR-END RSL on the front panel, use the built-in browser software to acquire the near and far end RSLs. Compare this/these RSL(s) to the Factory Test Data Sheet for the far-end radio and estimate the RSL in dBm. Again, compare this RSL to the expected RSL from the link budget calculations.

If RSL from both ends of the radio are approximately the same as each other, but lower than anticipated for this installation, then the likely cause of the BER alarm(s) is excessive losses between the radios. Excessive loss problems could include the transmission line at either end, all adapters, connectors, the antennas, the antenna alignment as well as the path itself (any obstructions or clearance problems). Antenna alignment, line-of-sight and path clearance should be verified; if this does not improve RSL, all devices between the radios and their antennas at both ends should be checked. Make sure all

transmission line, connectors and any other devices are properly rated for operation at the radio's frequency (5.3/5.8 GHz).

If only one end has low RSL, this could be caused by low transmit output power from the opposite end radio. Verify that the transmitter output power of the radio opposite to the low RSL receiver has been set in accordance to path calculations, or EIRP restrictions (where applicable). Power adjustment must be performed by professional installation personnel only. The PWR test point can be used and compared with the Factory Test Data Sheet, the front panel recessed potentiometer can be turned clockwise to increase power. If an RF power meter is available, this can be connected to the RF output of the radio for precision measurement. This test will also verify that the radio transmitter is working properly.

If one terminal (or both) has high RSL, this could be caused by a very short path or interference. To verify the possible presence of interference, remove DC power to the radio which is opposite to the one that is reading high RSL. Once power is removed, measure RSL on the remaining radio. If RSL voltage is lower than that which is listed for "Threshold" in the Factory Test Data Sheet, then an interfering signal is present. If interference is suspected, the easiest potential remedy is to swap frequency channels on both sides of the link. See Section 4.2 for details. Swap terminals at both ends of the link so that they are the opposite from their original installation. After both ends are moved, reconnect the radios and determine if the BER alarm is still active. If the BER alarm is still active, other frequency channels can be installed, or other interference countermeasures can be tried, in accordance with Section 4.8.

If all path related and data input problems have been pursued and the BER alarm is still active, the problem could be related to a radio failure. While radio failure is typically indicated by more severe alarm conditions, it is possible that one of the radios may be out of specification, and this could be the cause of the BER alarm. A back-to-back test will verify proper radio operation. See Section 4.9 for details. A threshold test on both radios along with a test to verify proper RF output power would be beneficial.

Perform a back-to-back test before returning any radio terminal to the factory for repair. A back-to-back test verifies radio operation. (See Section 4.9).

If the radios successfully pass their back-to-back testing, the problem is likely with the path or the connections between the radio and the antenna or interference. Before reinstalling the radios, be sure to set the output power to the appropriate level for the installation.

INSTALLATION AND MAINTENANCE MANUAL
Tsunami FAMILY
FAST ETHERNET WIRELESS BRIDGES
December 2001

WESTERN
Multiplex

4.6.2   RADIO FAIL Alarm

Function:

The RADIO FAIL alarm indicates a known problem with the radio hardware.

Possible Causes:

❖   Internal synthesizers are unlocked

❖   Internal digital circuits have failed

Recommended Actions:

1.   Remove power from the unit.

2.   Check to make sure power supply voltages are within specification.

3.   Even if the voltages were within specification, reapply power to the unit.

4.   If RADIO FAIL alarm clears, place the radio back into service.

5.   If RADIO FAIL alarm does not clear, perform a back-to-back test to verify radio operation, as described in Section 4.9.

6.   If RADIO FAIL alarm is still active in a back-to-back test, return the radio to the factory for repair (see Section 4.5).

4.6.3   FAR END Alarm

Function:

This LED indicates that there is an alarm condition present on the far-end radio. When the DISPLAY FAR END button is pressed (and held), the status LEDs indicate the alarm conditions of the far-end radio.

Possible Cause:

 ❖   One or more alarm condition(s) exist on the far-end radio

Recommended Actions:

1.   Press and hold the DISPLAY FAR END button and observe the LED status.

2.   Follow instructions for troubleshooting the far-end radio in accordance to the appropriate LEDs which are in alarm, as described in Section 4.6.1 through 4.6.4.

INSTALLATION AND MAINTENANCE MANUAL
Tsunami FAMILY
FAST ETHERNET WIRELESS BRIDGES
December 2001

WESTERN
Multiplex

4.7   Errors in the Data Stream

When the radio is in service, errors in the data stream may occur. This is usually known to the operator by either faulty data indications of downstream equipment or external bit error rate testing.

It is possible that no alarms appear on the front panel during normal operations, but there are errors present in the data stream. Some errors will not result in no alarm (such as bipolar violations, slow "dribbling" errors, improperly terminated connections or incorrect settings), but will be exhibited on downstream data processing equipment or during a BER test. In other cases, there may be data errors due to atmospheric conditions (fading), interference or other reasons, but not at a high enough error level to be indicated with the BER alarm LED. In the case of these types of errors, the following information can be helpful to troubleshoot the radio link.

Indications:

- ❖ During external BER test, test equipment indicates errors

- ❖ Downstream equipment (mux, channel bank, CODEC, router, etc.) indicates errors

Possible Causes:
- ❖ Path fading due to atmospheric conditions

- ❖ Poor transmission line connections

- ❖ Antenna problems, misalignment or path clearance

- ❖ Received signal level (RSL) is too strong

- ❖ Far-End radio transmitter circuitry is faulty

- ❖ Near-End radio receiver circuitry is faulty

- ❖ Interference

Recommended Actions:

1.   Verify 100BaseT wiring.

2.   Follow the instructions described in Section 4.6.1

4.8   Interference Countermeasures

The recommended interference countermeasures available to the *Tsunami* operator are as follows:

1.   Short Paths

The single most effective countermeasure against interference is to maintain "short path" length. This may be achieved by dividing long paths into multiple small paths by cascading hops. Intermediate repeaters may be formed using back-to-back *Tsunami* terminals and transmit output power reduced, if required.

By definition, "short path" is defined as a path where fades are extremely rare and signal levels vary by no more than ±3 dB during fades. This distance will vary with the RF frequency. Typically a "short path" is defined as any path length shorter than 5 miles at 5.3/5.8 GHz.

2.   Narrow Beam Antennas (high gain)

This is the next most effective countermeasure. Narrow beam antennas ensure that the transmitted power is sent in a single direction and this minimizes the possibility of causing interference inadvertently to other users. Narrow beam antennas also reject off-azimuth signals being received from potential sources of interference and have high gain which boosts desired receive levels and improves the carrier to interference ratio. When selecting narrow beam antennas, it is helpful to know that larger antennas generally outperform smaller antennas. Another important antenna specification is the front-to-back ratio which ensures rejection of unwanted signals from azimuth angles behind the antenna.

3.   Frequency Selection

This is another very effective countermeasure. The *Tsunami* radio offers several distinct non-overlapping frequency channel plans (see Sections 3.5 and 4.2) and the radio's RF filter is able to reject interference more than 10 MHz away from the receive frequency. Offset frequencies combined with other countermeasures may enable several receive channels to operate at a single hub site. Because of the limited spreading ratio used, frequency selection is more efficient than code selection for interference rejection when operating multiple *Tsunami* terminals at a single site. Interference can often be overcome by exchanging frequencies of both-ends of the radio link (e.g. change your A1 terminal to an A2 and change the other end from an A2 to an A1). Also, changing channel plans (e.g. from A to B) can be very effective. (See Section 4.2).

INSTALLATION AND MAINTENANCE MANUAL
Tsunami FAMILY
FAST ETHERNET WIRELESS BRIDGES
December 2001

W E S T E R N
M u l t i p l e x

4.   Antenna Polarization

Cross-polarized antennas can provide approximately 20 to 30 dB discrimination of unwanted signals. The actual discrimination will depend upon the antenna design and any rotation of polarization along the path, for example, due to reflections. Discrimination only exists between two orthogonal polarizations:

- vertical vs. horizontal or

- left-hand circular vs. right-hand circular

There is only 3 dB discrimination between circular and linear (vertical or horizontal) polarization.

Interference can sometimes be overcome by changing antenna polarization at both ends of the link.

5.   Transmit Power

The maximum level into the receiver is -30 dBm. Above this level, errors may occur in the receive data stream. Transmit output power should be reduced on very short paths to avoid overload.

6.   Equipment/Antenna Location

Occasionally, interference is caused by the radio or the antenna being too close to another similar transmitter. Moving the radio, the antennas, or the interfering equipment can reduce or eliminate interference.

Interference countermeasures rely to some extent on the measurement of the received interference level and frequency. Prior to turning up a new hop, a spectrum analyzer can be used to monitor the spectrum at each end to check for possible interfering signals. See Section 4.8.1 for more details.

4.8.1   Use of a Spectrum Analyzer to Evaluate Potential Interference

Connecting to the antenna and using "peak hold" on a spectrum analyzer, the spectrum across the receive frequency range of the radio can be swept and any signals being received at levels above the radio's specified threshold identified. If potential interfering signals are found, then the *Tsunami* frequency plan can be changed to avoid a receive channel which may contain significant interference (see Section 4.2).

For example, interference may be reduced by moving from the A1/A2 plan to the B1/B2 plan or by swapping terminals or RF filters so that A1 becomes A2.

Signals outside the receiver frequency range may be ignored: they will not cause interference.

If a spectrum analyzer is not available, the RSL voltage can be used to indicate the background noise and interference level within the receiver RF filter band when the far-end transmitter is turned off. With the far-end radio turned off, if an RSL voltage level measured is above the radio's threshold level, there is potentially interference in this frequency channel.

When using a spectrum analyzer for determining the presence of interference, very narrow resolution bandwidth settings must be used to detect signals down to the radio's threshold (approximately -80 dBm, depending on radio type).

INSTALLATION AND MAINTENANCE MANUAL
Tsunami FAMILY
FAST ETHERNET WIRELESS BRIDGES
December 2001

WESTERN
Multiplex

4.9　Back-to-Back Testing

Back-to-back testing, as shown in Figure 4-1, is an ideal method of testing the *Tsunami* radios. This testing eliminates link problems caused by auxiliary equipment, installation, or the radio path and isolates potential radio hardware problems. Back-to-back testing must be performed with both radios at the same location. The following test equipment is required:

❖　DC power source capable of supplying approximately 90 Watts (total) to the radios (or two AC adapters)

❖　One low-loss coaxial cable, N-to-N male

❖　One (or more) coaxial in-line calibrated fixed attenuators, 40 to 80 dB total attenuation

The following test equipment may also be useful to perform further testing of the *Tsunami* radio:

❖　BER tester

❖　Variable (60 dB range or more) RF attenuator (rated for the proper frequency, 2.4 or 5.8 GHz)

❖　RF power meter

Back-to-back testing must be performed to verify a radio problem
before returning any radio to the factory for repair.

When the equipment is connected as shown in Figure 4-1, both *Tsunami* radios should have no alarm conditions. If these conditions have been met, then it is likely that the *Tsunami* radio is operating in accordance to specifications. If errors or alarms occur during this test, verify that all DIP switch settings are properly set. If alarms or errors are still present, the radio is likely to be faulty.

If further troubleshooting is required, a variable RF attenuator can be inserted between the radios to fade down the path to determine that the threshold specification is being met. The threshold tests can be run in both directions to isolate the radio problem (if any). More information testing is provided in Section 4.10. An RF power meter can be used to individually test each radio's output power.
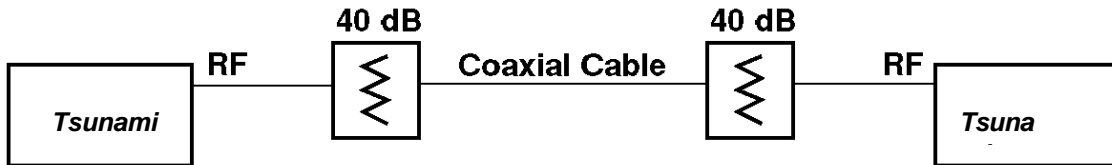
Figure 4-1: Back-to-Back Test Configuration

The Tsunami radios will be damaged if appropriate attenuation is not supplied between radios. You must provide a minimum of 40 dB and no more than 80 dB attenuation between the two radios.

INSTALLATION AND MAINTENANCE MANUAL
Tsunami FAMILY
FAST ETHERNET WIRELESS BRIDGES
December 2001

WESTERN
Multiplex

4.10   LINK Testing

Link testing is the preferred way to evaluate a radio link's performance. It can be performed from end-to-end or in link test mode (which tests both directions of the radio path). Figure 4-2 illustrates a typical test configuration (which may include the radio's path instead of in-line attenuators). Figure 4-2 illustrates a typical test configuration for end-to-end testing.

When performing testing, make sure of the following:

-    Disconnect all 100BaseT inputs and outputs to both radios.

-    Verify all configuration settings.

Link testing may be performed on the bench, with two terminals back to back, or over the radio path. Also, it may be performed from end-to-end (which requires two 100BaseT test sets over a link, the far-end unit slaved to the near-end unit's clock) or in loopback mode, as described in Section 4.9.

If link testing indicates an unacceptable level of errors, follow the instructions in Section 4.6.1. or perform a back-to-back test as described in Section 4.9.
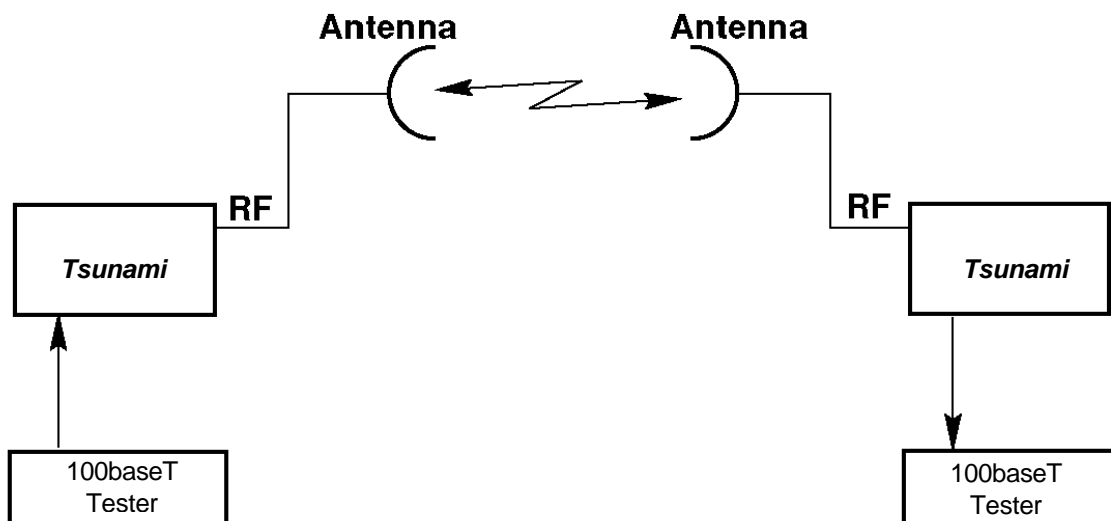
Figure 4-2: End-to-End Test Configuration

4.11   Network Management System (NMS)

The Tsunami 100BaseT radio platform provides multiple methods of managing the radio network:

1)   SNMP
2)   Browser (IE, Netscape, etc.) graphical user interface
3)   Software upgrade procedure
4)   TelNet (via VT100 session using Windows™ Hyperlink)

4.11.1   SNMP for the Tsunami 100Base-T 45 Mbps Radio

Use your favorite SNMP access software such as HP OpenView, SNMPc or equivelent.

What you will need: A Windows 95/98/NT laptop or workstation with Hyperterminal and an available COM port. A DB-9 F to DB-9 F crossover (pin 2 to 3, pin 3 to 2, pin 5 to 5) cable for the PC. A copy of the Tsunami 100 MIB. A workstation running an SNMP manager such as Castle Rock SNMPc or Ipswitch WhatsUp Gold. If in-band management is required a 10/100Base-T switch with at least 3 ports would be needed.

Install the MIB in the SNMP manager: Following the instructions provided with the software, load and compile the MIB file. The MIB contains all the traps and configuration variables for the SNMP agent and the radio.

Ethernet connections: All SNMP traffic including traps, set commands and get commands are sent and received through the 10Base-T NMS port. To backhaul the SNMP traffic over the radio link, the traffic from the 10Base-T NMS port must be multiplexed to the 100Base-T port using a 10/100Base-T switch with at least three ports, one for the payload, one for the 10Base-T NMS port, and one for the radio 100Base-T port. Make sure the duplex settings are correct. See **Problems** at the end of this document.

Connecting to the config port: The SNMP agent is set up through the radio's config port. Some settings are accessible only this way and not through the web browser. Connect the cable to the radio's config port and the PC's COM port. Start by launching Hyperterminal. You will be prompted to enter a name for the connection as shown:
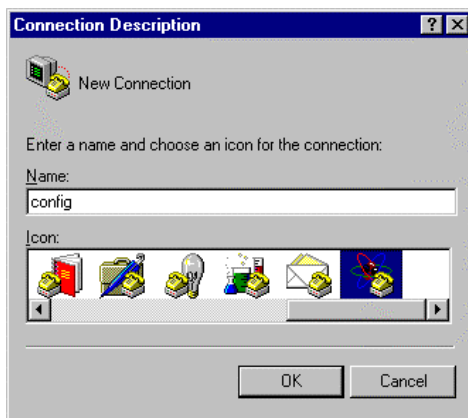
Choose a name and an icon for the connection and click the OK button.

INSTALLATION AND MAINTENANCE MANUAL
Tsunami FAMILY
FAST ETHERNET WIRELESS BRIDGES
December 2001

WESTERN
Multiplex

You will be asked for a phone number, etc. Go straight to "Connect Using:" and pick the COM port for your PC, then click the OK button.

You will then be prompted for the COM port properties. Enter the values shown below:
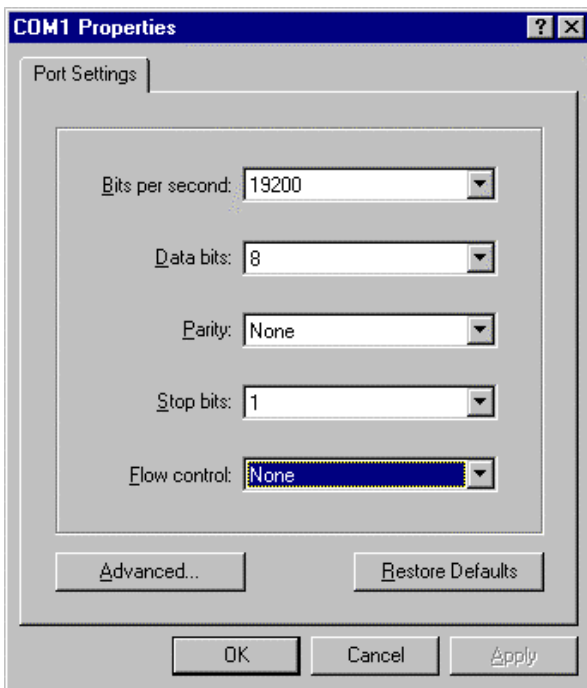
Click the OK button. You will then go to the HyperTerminal session screen.

The terminal emulation must be set to VT100. This can be done by clicking the Properties button on the toolbar in HyperTerminal or going to the File > Properties menu. The following screen will be displayed:
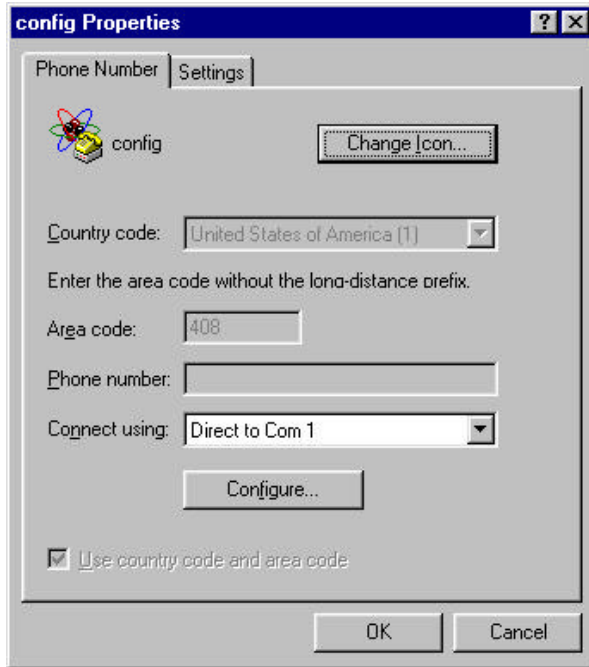
Click on the Settings tab to display the following:

INSTALLATION AND MAINTENANCE MANUAL
Tsunami FAMILY
FAST ETHERNET WIRELESS BRIDGES
December 2001

WESTERN
Multiplex
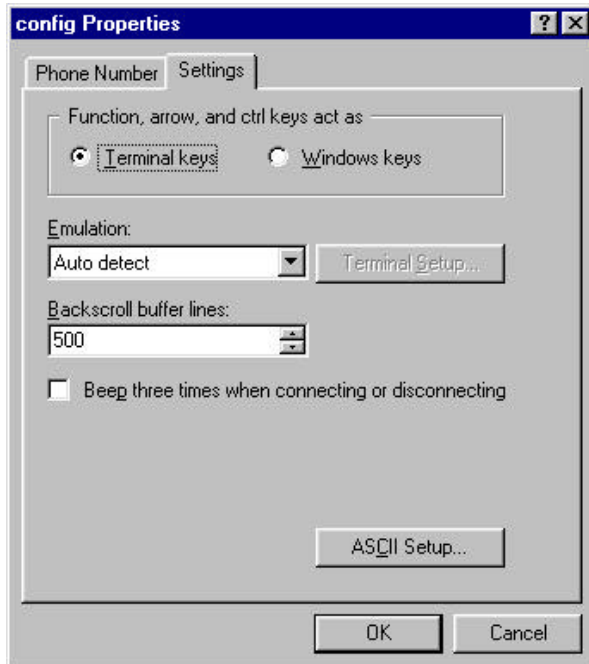
Choose VT100 from the Emulation drop down list.
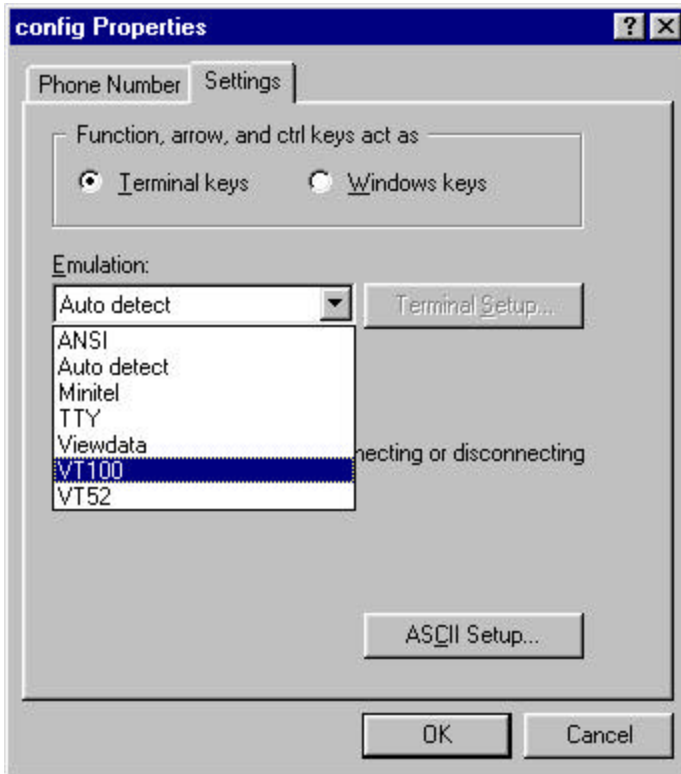
Now click the OK button. You will go back to the HyperTerminal session screen.

Type in <Enter> <Enter> (press the Enter key twice) to start the Login screen.

Config Port user interface: The config port has a simple user interface. Every screen has several fields and a command line at the bottom. Pressing the Tab key moves you between the fields in sequence. Pressing the Enter key always brings you back to the command line. To move to a specific field, type the number of the field in the command line and press the Enter key. When you have updated all the fields, press Enter to return to the command line and then type "accept" to implement the changes. You may also type "a" as a shortcut. Pressing the Control and J keys at the same time (<Ctrl><J>) will toggle through all the commands for that screen.

Loggin in: To log in Tab to the User Name field and type "manager" or "managers". Tab to the Password field and type "manager" (or managers) again. Tab to the command line and type "accept" or "a" and then press the Enter key.

```
nmu - HyperTerminal
File  Edit  View  Call  Transfer  Help



                         NMU   Login               11/22/2000 16:34


               1. User Name:        manager
               2. Password:




               Serial Number             0000000015af
               Login count               00















  Select option

                              normal-health(1):   NMU-000015af:ACCEPT

Connected 0:02:01    VT100    19200 8-N-1   SCROLL   CAPS   NUM   Capture   Print echo
```
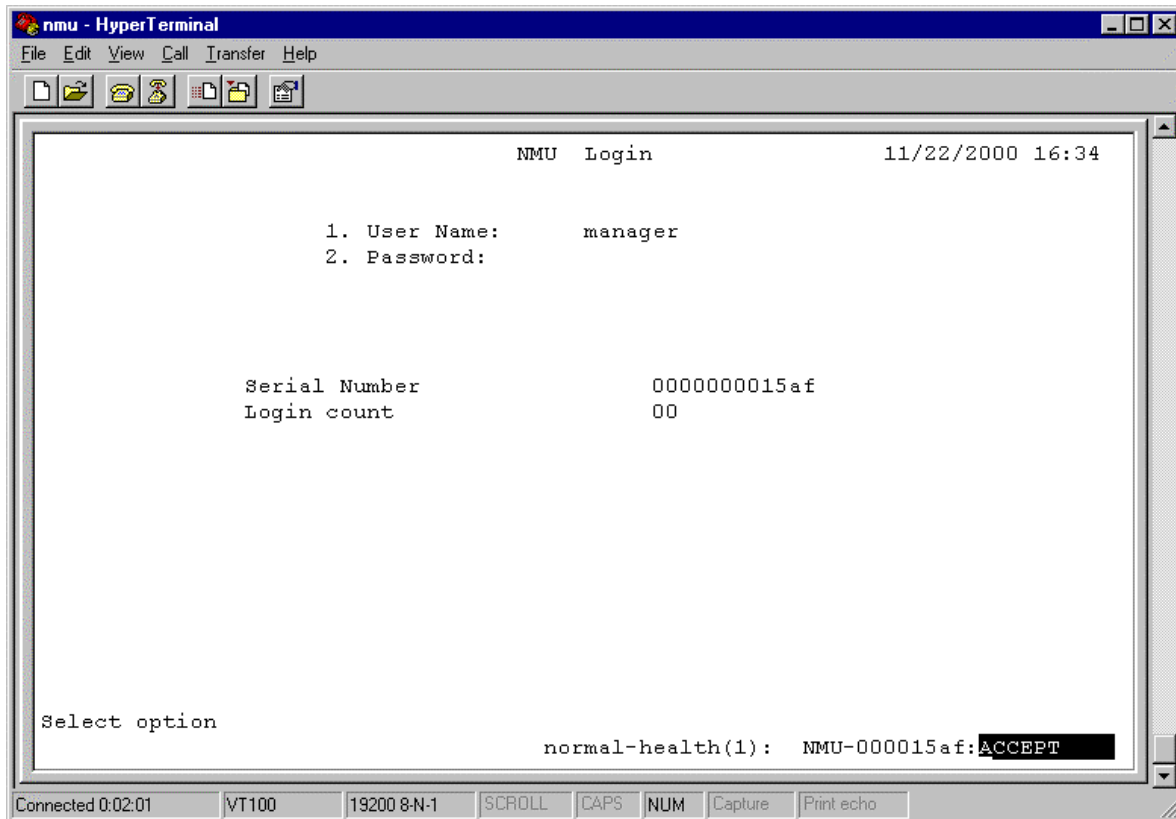
The following screen will then be presented:

INSTALLATION AND MAINTENANCE MANUAL
Tsunami FAMILY
FAST ETHERNET WIRELESS BRIDGES
December 2001

WESTERN
Multiplex
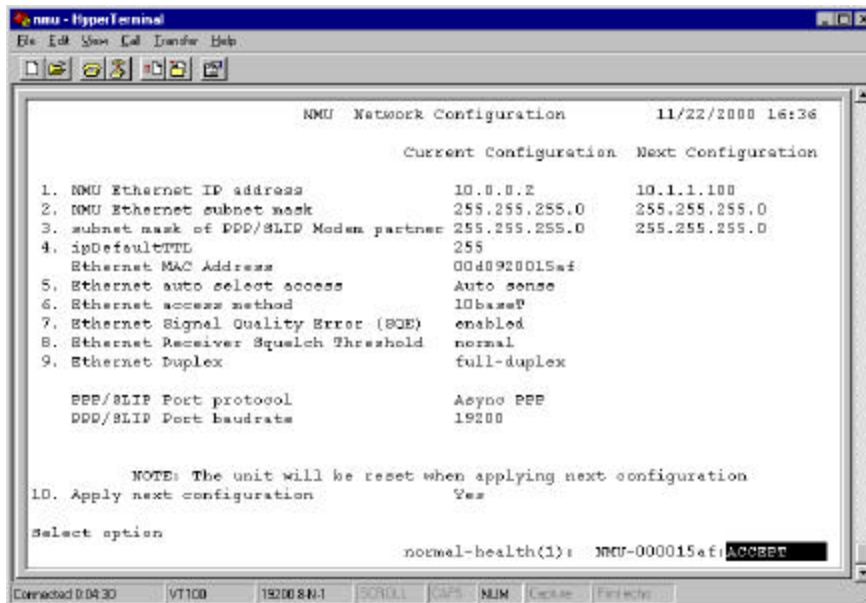
Main Menu: You should now see the Main Menu as shown below. To select an item, type the number in the command line and press the Enter key.
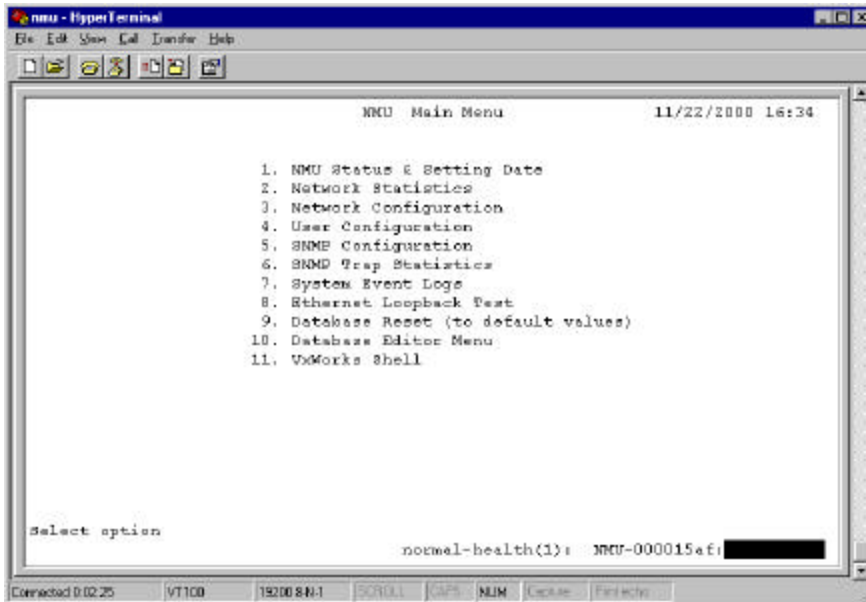
Network Configuration: To set the IP address select number 3, Network Configuration. The Network Configuration screen will appear as shown below. The IP address may also be set through the web browser interface of the radio.
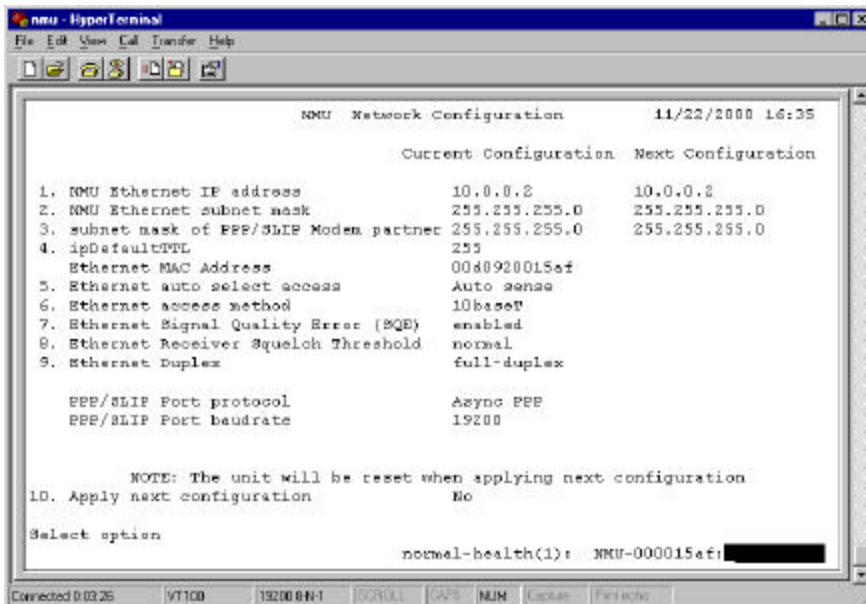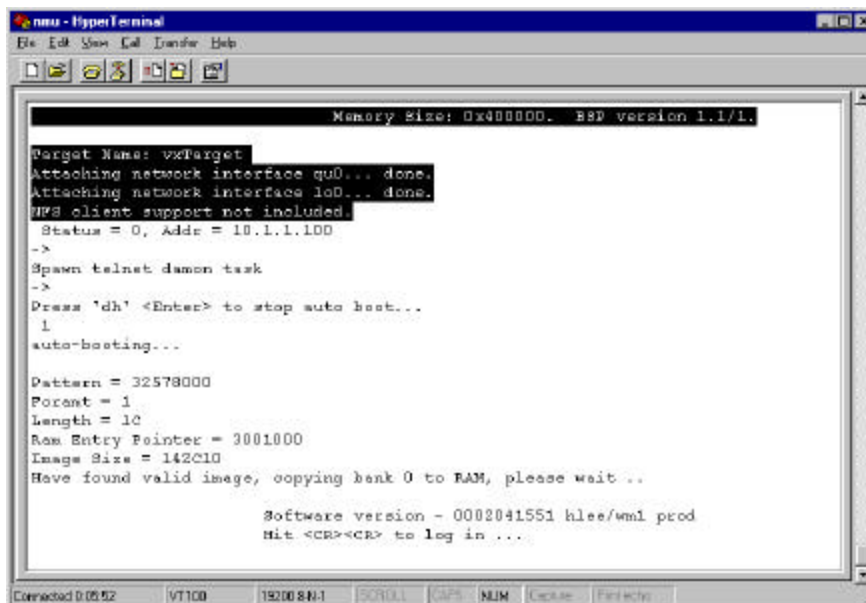
Setting the IP address: The SNMP agent must be rebooted to change the IP address. The IP address and subnet mask of the agent after the next reboot can be entered in fields 1 and 2. Enter the IP address and subnet mask as shown below. Entering Yes in field 10 will cause the SNMP agent to reboot, thereby applying the next configuration.

Reboot the SNMP agent: Typing "accept" and pressing the command line will cause the agent to reboot.
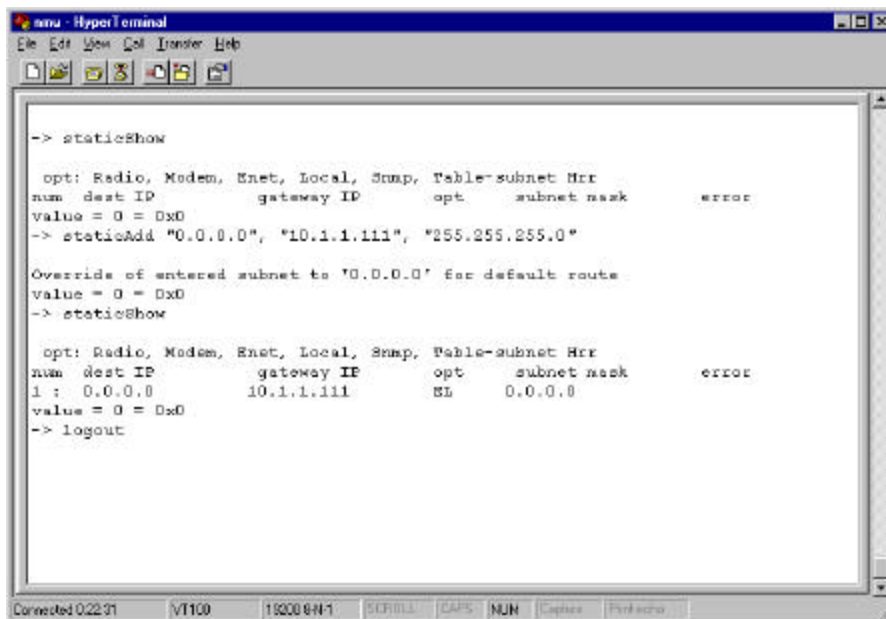
Go back to the Login screen: Press the Enter key twice to go back to the Login screen. Log in as before to get back to the Main Menu.

Setting the default gateway: If the workstation running the network management software is on a different IP subnet than the SNMP agent, a default gateway will need to be set. This must be done in the VxWorks shell. Instructions on how to do this are included in the Tsunami 100Base-T manual but are repeated here for convenience.

Go to the VxWorks shell by selecting item 11 from the Main Menu. The command prompt for VxWorks will be displayed. The default gateway is configured by adding a static route.

To display the static routing table, type in the command: staticShow as shown below. To add a static route, type in the command: staticAdd "0.0.0.0", <gateway IP address>, <subnet mask>. The IP address 0.0.0.0 represents the default route and causes all traffic that doesn't match the SNMP agent's subnet mask to be sent to the gateway IP address specified. Note that the gateway IP address and subnet mask should be in the same subnet specified above. If the gateway IP address is not in the same subnet as the SNMP agent, the command will fail and the static route will not be added. To verify that the route was added type staticShow again. To exit the VxWorks shell and go back to the menus type the command: logout.

Note that the static route is persistent. That is, it will remain in the routing table if the radio resets or the power is cycled.

Configuring SNMP Settings: Select item 5, SNMP Configuration from the Main Menu. The SNMP Configuration screen will appear as shown below.
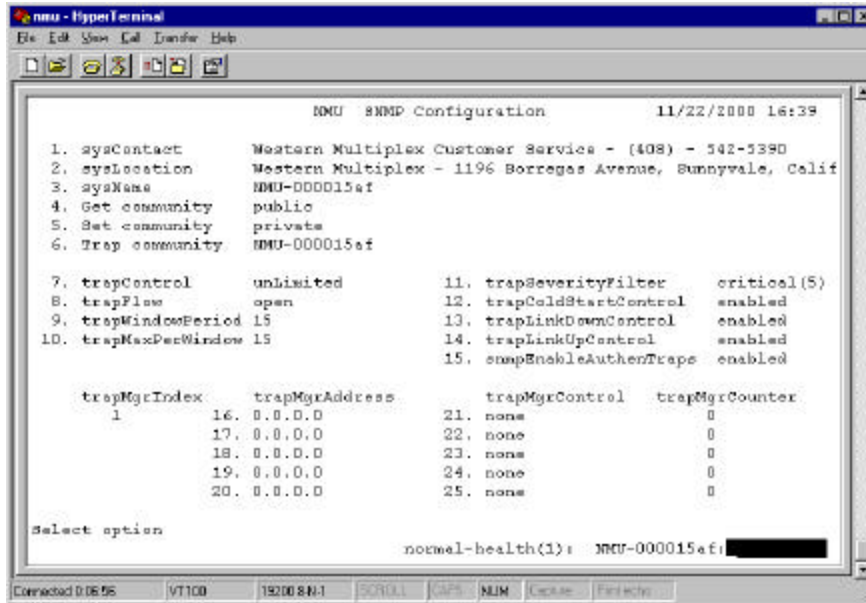
Items 1 to 3 are informational and may be set to the users preferences. The get and set community strings must match those in the SNMP manager software if you wish to retrieve and change radio settings by SNMP.

In order to receive all traps item 11, trapSeverityFilter should be changed to normal(1). This will allow all traps of normal severity and higher to be sent. The IP address of the workstation running the SNMP manager software is entered in field 16. Note that up to 5 IP addresses can receive traps. Field 21 sets which type of traps are sent to the IP address specified in field 16. This is usually set to "both" so that both standard traps as specified in the RFC's and enterprise traps specific to WMC's products are sent.
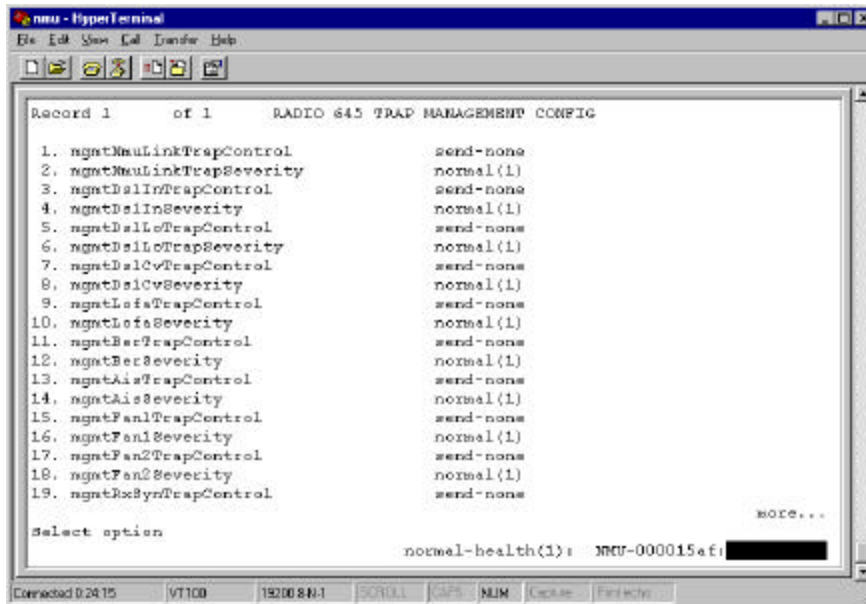
Enter the values applicable to your installation and type "accept" in the command line. Press the Enter key to implement the changes.

INSTALLATION AND MAINTENANCE MANUAL
Tsunami FAMILY
FAST ETHERNET WIRELESS BRIDGES
December 2001

WESTERN
Multiplex
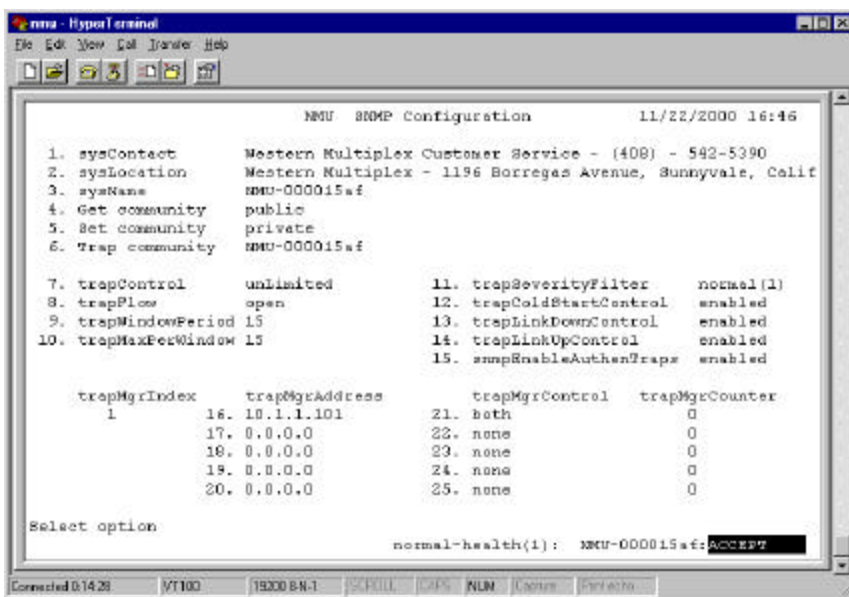
Enable the radio traps: Each of the 11 traps must be enabled individually. This is done from item 10 in the Main Menu, Database Editor Menu. The Database Editor displays mostly the same variables found in the other menus, only in a "flat" view rather than a "hierarchical" view. Some settings such as trap configurations are available only from this menu.
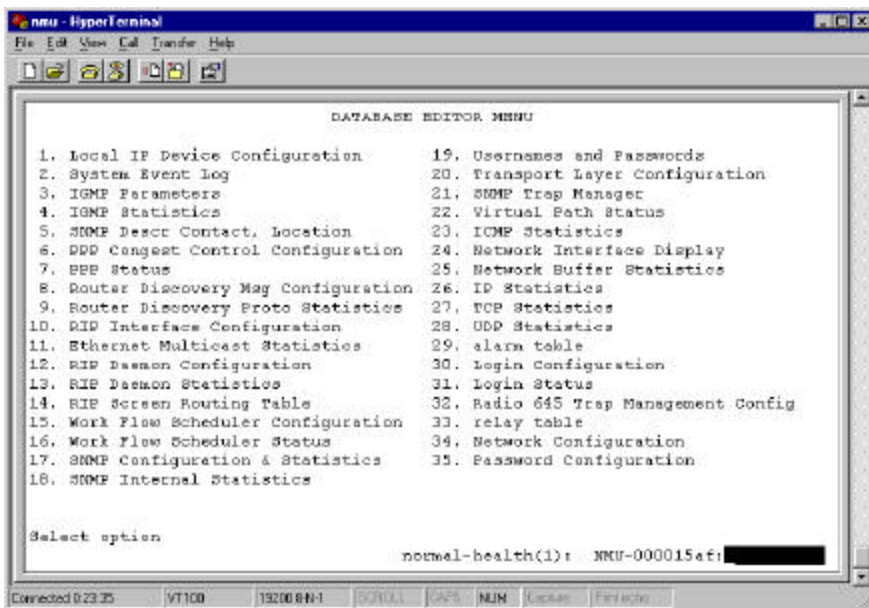
Select item 32, Radio 645 Trap Management Config from the Database Editor Menu. A list of traps and control settings will appear as shown:

Each trap has a trap control setting and a trap severity setting. The trap control setting determines if the trap is sent or not and if it is sent, whether it is sent on transition to alarm, transition to normal or on both transitions. Since it's useful to know both when an alarm condition appears and when it clears the trap control is usually set to send-both.

In some cases it's preferable to leave the trap disabled. Such is the case when the DS-1 is not in use. In that case, all the traps relevant to the DS-1 such as Ds1In and Ais would be left in the send-none state. Assuming the DS-1 is used, all traps would be set to the send-both state. Using the Tab key to move down the list and <Ctrl><J> to toggle the field settings each trap control variable can be set.

Each trap also has a trap severity control. Since trap severity can be set in most SNMP manager software on a global basis, there is no need to set each trap's severity radio by radio. It is more convenient to leave this setting at the default of normal and configure the SNMP manager software to assign the desired severity when the trap is received. These settings may also be remotely configured using SNMP set commands.

Note that the final field, trapHysteresis is not implemented and therefore has no effect on the unit's operation.

Going back to the command line, typing "accept" and pressing the Enter key will implement the desired changes.

```
nmu - HyperTerminal
File  Edit  View  Call  Transfer  Help

   3. mgmtDs1InTrapControl              send-none
   4. mgmtDs1InSeverity                 normal(1)
   5. mgmtDs1LoTrapControl              send-none
   6. mgmtDs1LoTrapSeverity             normal(1)
   7. mgmtDs1CvTrapControl              send-none
   8. mgmtDs1CvSeverity                 normal(1)
   9. mgmtLofaTrapControl               send-none
  10. mgmtLofaSeverity                  normal(1)
  11. mgmtBerTrapControl                send-none
  12. mgmtBerSeverity                   normal(1)
  13. mgmtAisTrapControl                send-none
  14. mgmtAisSeverity                   normal(1)
  15. mgmtFan1TrapControl               send-none
  16. mgmtFan1Severity                  normal(1)
  17. mgmtFan2TrapControl               send-none
  18. mgmtFan2Severity                  normal(1)
  19. mgmtRxSynTrapControl              send-none
  20. mgmtRxSynSeverity                 normal(1)
  21. mgmtTxSynTrapControl              send-none
  22. mgmtTxSynSeverity                 normal(1)
  23. mgmtTrapHysteresis                120

Select option
                             normal-health(1):   NMU-000015af:

Connected 0:26:26      VT100      19200 8-N-1    SCROLL  CAPS  NUM  Capture  Print echo
```

Problems:

1.   "I can't seem to get the config port to work" or "The config port was working before but now it doesn't" or "I press the <Enter> key twice but nothing happens."

To verify your PC settings and RS-232 cable bring up a HyperTerminal session with one end of the cable plugged into the PC com port and the other end unplugged. Using a piece of wire, short pins 2 and 3 together on the unplugged end of the cable. Make sure the HyperTerminal window is active and enter some characters from the keyboard. You should see the characters displayed in the HyperTerminal window. If you can't see the characters, make sure the com ports settings are correct and try a different cable.

Double check the HyperTerminal configuration settings and plug the cable back into the radio config port. If the characters displayed as described above and the HyperTerminal configurations are correct and the menu still doesn't display when you press the <Enter> key twice, the config port may already be "logged in". Once you are logged in to the config menu the config port stays logged in for the timeout period specified under main menu item 4, User Configuration. The default is 7200 seconds or 2 hours. If you unplug the cable or shut down HyperTerminal while you're still logged in and you restart the HyperTerminal session, it will appear that you have a blank screen that's not responding.

To get started again, press the <Tab> key a few times. If you were in a screen with multiple entry fields when you shut down, you will see the cursor move between those fields. Bring the cursor back to the command field on the lower right part of the screen and press the <H> key followed by the <Enter> key to go back to the main menu.

To log out of the config port go to the command field press the <H> key, then <Enter> to go to the main menu, then <O>, <Enter> to go to the login menu. From the command field in the login screen, press <D> then <Enter> to end the session. Pressing <Enter> twice will restart the session and bring up the login screen.

2.   "The web browser is really slow" or "Sometimes I can't log in to the web page".

Check the Ethernet duplex settings of the NMS port and the PC or switch connected to it. If the NMS port is set to full duplex and the device connected to it is set to half duplex or vice versa, the web browser will still work but it will be slow. Make sure that the duplex settings all match. The duplex setting for the NMS port can be set in the config port menu, under submenu 3, Network Configuration, item 9, Ethernet Duplex. Ignore item 5, Ethernet auto select access as it's an artifact from the original application the code was ported from and has no function.

4.11.2   Browser GUI

Use Internet Explorer™ or Netscape™ to access the radio by typing in its IP address. If you are setting up the radios for the first time, the default IP address is: 10.0.0.1 You will have to configure your computer to this domain first by setting its address to 10.0.0.2 and then changing the radio's IP to one within the domain of your network. After changing one radio's IP address (see Configuration tab) change the other radio's IP address also, but not to the same address of the previous radio. Reconfigure the IP address of your computer to it's original address and then restart the PC so it is now in the same domain as the radios.

The browser interface shows a "virtual" front panel of the radio that is addressed. To view the front panel of the associated far-end radio, click on the window that is located on the virtual front panel (see following illustrations). Illustrations on the next few pages of this manual provide details on all browser screens and operations.

4.11.3   In-band NMS Set-up

Use a 4-port (or larger) 10/100 switch (recommended as opposed to a hub that will also work) at each radio to operate the NMS in-band with the 100BaseT traffic. The NMS port can have a unique domain that is valid only with the PC that is being used for network management and system-wide operational status and will not interfere with 100BaseT traffic as the radio's MAC address plus its IP address are unique.

Radios are set at the factory to IP addr: 10.0.0.1. Temporally set your PCs domain (write down its present IP address) to a suggested setting of PC=10.0.0.5-the PC will force a re-boot. Re-boot the PC computer attached to the first radio's 10BaseT NMS port and log-in to radio NMS w/favorite browser (IE or Netscape) after log-in (manager:manager or managers:managers). Change the IP address (Configuration) to an unused one in your domain (if you want to also change the password at this time, do this first). Do the same with other radio (may have to reboot computer attached to this other 10.0.0.1 radio as the other's MAC address does not match the MAC/IP address the PC knows about). Set the IP address this radio to a different IP address in your normal operating domain. Set your PC back to its original domain (will force reboot again). This should allow for typical LAN operation. **Type http://10.0.0.1/index.htm to gain initial access.**

> *Note:*
> *Multicasting with in-band connection may cause collisions in the data stream.*

4.11.3.1   Models 27700 & 27710

Login Screen 1

Enter User Name and Password. If using for the
first time or the radio has been reset, use:
<u>Full User Rights:</u>
User Name: manager
Password: manager
<u>Limited User Rights:</u>
User Name: operator
Password: operator

It's advisable to change the password setting on
the administration (Admin) page to protect radio
settings, configuration and illegal entry into the
radio system.

Login Screen 2

With default Name and Password

Click on "Log On" to gain entry

To log in to the 100BaseT radio
(and the new 27710-52 w/E1 waysides)
use the eight (8) letter version of the
other model passwords:
manager: use 'managers'
operator: use 'operators'

WESTERN
Multiplex

Models 27700 and 27710

Device Screen

Tsunami model information

Configuration 1

The radio's characteristics can be modified from this page. The 'Current' column indicates current settings and the 'New' column the radio setting(s) that can be changed. Use the pull-down menus to select the new setting. Then, click on the Set button to invoke the setting.

In some cases it may be necessary to "refresh" the screen to see changes to settings.

Warning: the Tx/Rx Frequency can not be changed without also changing the physical diplexer.

Help Screen

At any time, on any page, clicking on Help will open a separate help window to facilitate operation of the Browser NMS.

Use the help page to provide details on the configuration settings.

Use the window close box to dispense with the help screen when finished.

Configuration 2

Scroll down to see the complete list of radio configuration settings.

Here is where the radio's IP setting can be modified from the default 10.0.0.1

On the Model 27710-52, this screen will offer the option of 'stealing' 2 more megabits from the Ethernet throughput to allow an additional E1 to be used for those sites needing 2xE1.

Note: To return to defaults, power up the radio while depressing the link test button.

Performance 1

Running data on the operation of the radio link.
To reset the historical data, click on History
Reset.

Note alarm bar between front panel depiction
and performance data.

Performance 2

New screen after resetting history.

Alarms

Both near-end and Far-end information on the running status of the link are displayed on this single page.

Administration

Change the default password (manager or operator) for subsequent entry into the browser NMS.

Click on set after changing the password.

If you forget the password, you must fully reset the radio by holding in the far-end button on the front of the radio while powering it up.

Contact Information

The E-mail and the URL links are active text if selected. Each will start your e-mail or browser when either is clicked on.

Link failure indication!

If the link is lost, the severely errored seconds will display the amount of time the link was not passing sufficient data.

In this example, the link had almost seven seconds of corrupt data since the last time the history had been reset (1271468 seconds or 353 hours or almost 15 days).

4.11.3.2   100 Mbps Models

Login Screen 1

Enter User Name and Password. If using for the
first time or the radio has been reset, use:
<u>Full User Rights:</u>
User Name: managers
Password: managers
<u>Limited User Rights:</u>
User Name: operators
Password: operators

It's advisable to change the password setting on
the administration (Admin) page to protect radio
settings, configuration and illegal entry into the
radio system.

Login Screen 2

With default Name and Password

Click on "Log On" to gain entry

To log in to the 100BaseT radio
(and the new 27710-52 w/E1 waysides)
use the eight (8) letter version of the
other model passwords:
manager: use 'managers'
operator: use 'operators'

Model 27720

Device Screen

Tsunami model information

To log in to the 100BaseT radio
(and the new 27710-52 w/E1 waysides)
use the eight (8) letter version of the
other model passwords:
manager: use 'managers'
operator: use 'operator'

Configuration 1

The radio's characteristics can be modified from
this page. The 'Current' column indicates current
settings and the 'New' column the radio
setting(s) that can be changed. Use the pull-
down menus to select the new setting. Then,
click on the Set button to invoke the setting.

In some cases it may be necessary to "refresh"
the screen to see changes to settings.

Warning: the Tx/Rx Frequency can not be
changed without also changing the physical
diplexer.

Note: Two T1s to configure

Help Screen

At any time, on any page, clicking on Help will open a separate help window to facilitate operation of the Browser NMS.

Use the help page to provide details on the configuration settings.

Use the window close box to dispense with the help screen when finished.

Configuration 2

Scroll down to see the complete list of radio configuration settings.

Here is where the radio's IP setting can be modified from the default 10.0.0.1

On the Model 27710-52, this screen will offer the option of 'stealing' 2 more megabits from the Ethernet throughput to allow an additional E1 to be used for those sites needing 2xE1.

Note: To return to defaults, power up the radio while depressing the link test button.

INSTALLATION AND MAINTENANCE MANUAL
Tsunami FAMILY
FAST ETHERNET WIRELESS BRIDGES
December 2001

WESTERN
Multiplex

Performance 1

Running data on the operation of the radio link.
To reset the historical data, click on History
Reset.

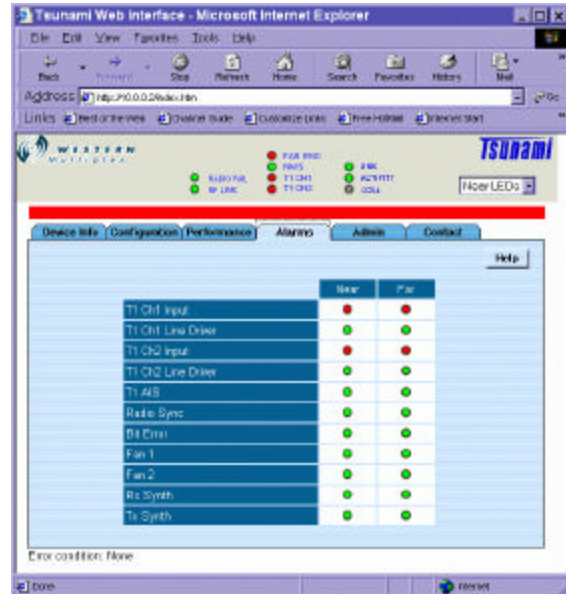Note alarm bar between front panel depiction
and performance data.

Performance 2

New screen after resetting history.

Alarms

Both near-end and Far-end information on the running status of the link are displayed on this single page.

Administration

Change the default password (manager or operator) for subsequent entry into the browser NMS.

Click on set after changing the password.

If you forget the password, you must fully reset the radio by holding in the far-end button on the front of the radio while powering it up.

Note: here is where you set your IP address, mask and any default gateway address.

INSTALLATION AND MAINTENANCE MANUAL
Tsunami FAMILY
FAST ETHERNET WIRELESS BRIDGES
December 2001

W E S T E R N
Multiplex

Contact Information

The E-mail and the URL links are active text if selected. Each will start your e-mail or browser when either is clicked on.

Link failure indication!

If the link is lost, the severely errored seconds will display the amount of time the link was not passing sufficient data.

In this example, the link had almost seven seconds of corrupt data since the last time the history had been reset (1271468 seconds or 353 hours or almost 15 days).
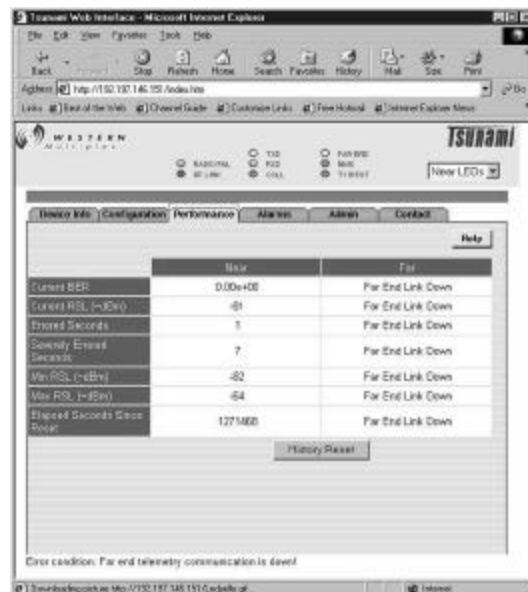
Model 28010

Device Screen

Tsunami model information

To log in to the 100BaseT radio
use the eight (8) letter version of the
other model passwords:
manager: use 'managers'
operator: use 'operator'

Alarms

Both near-end and Far-end information on the running status of the link are displayed on this single page.

Configuration

The radio's characteristics can be modified from this page. The 'Current' column indicates current settings and the 'New' column the radio setting(s) that can be changed. Use the pull-down menus to select the new setting. Then, click on the Set button to invoke the setting.

In some cases it may be necessary to "refresh" the screen to see changes to settings.

Warning: the Tx/Rx Frequency can not be changed without also changing the physical diplexer.

Note: Two E1s to configure (1, 2)

Performance

Running data on the operation of the radio link. To reset the historical data, click on History Reset.

Note alarm bar between front panel depiction and performance data.

Log Function

This menu details all alarm events that occur with this radio with a time stamp and severity level.

The filtering level can be set to determine what level and higher alarm levels are entered into the log table.

Contact Information

The E-mail and the URL links are active text if selected. Each will start your email or browser when either is clicked on.

INSTALLATION AND MAINTENANCE MANUAL
Tsunami FAMILY
FAST ETHERNET WIRELESS BRIDGES
December 2001

WESTERN
Multiplex

Administration

Change the default password for subsequent entry into the browser NMS.

Click on set after changing the password.

If you forget the password, you must fully reset the radio by holding in the far-end button on the front of the radio while powering it up.

Here is also where the date, time, IP address, subnet mask, default gateway and SNMP community information is located.

Help Screen

At any time, on any page, clicking on Help will open a separate help window to facilitate operation of the Browser NMS.

Use the help page to provide details on the configuration settings.

Use the window close box to dispense with the help screen when finished.
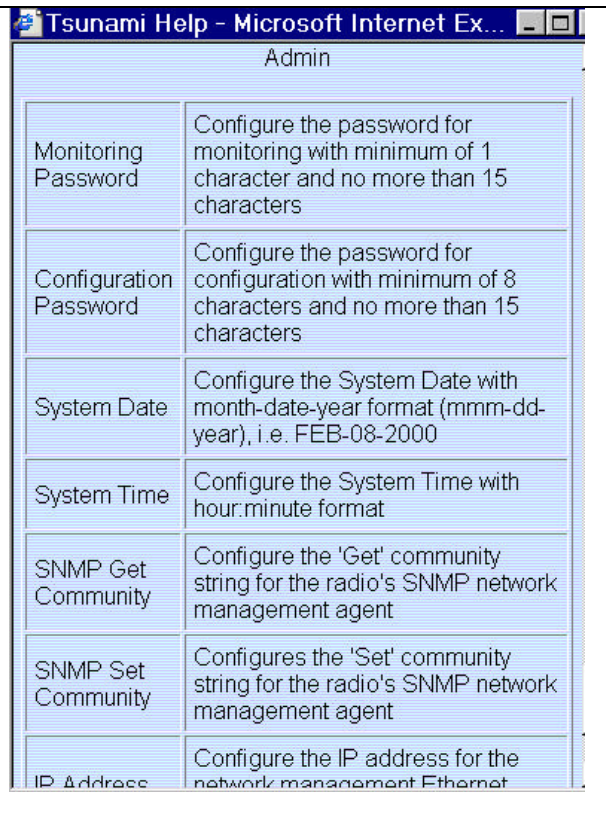
4.11.2   Tsunami Command Line Interface

This interface is available through the CONFIG port using HyperTerminal from MS WINDOWS. The user will need a mouse extender cable to connect to COM1 or COM2 of the computer to the CONFIG DB-9 DCE connector on the front panel.

This command line interface is the easiest way to change the IP address of the radio, as well as set up the default gateway address and setting the Community String. After the addresses have been changed and saved, the user can then access the NMS through the browser interface for all management features.

```
--------------------------------------------------------------------------
          Welcome to Tsunami 100-E1 Command Line Interface Menu

     NMU SW Version    --  1.0  ( Created Nov 28 2001, 13:31:35 )
     MAC address       --   00:08:d0:0e:0c:01
     IP address        --  10.10.3.39
     SubNetMask        --  255.0.0.0
     Default Gateway   --
     Set Community String --   private
     Get Community String --   public
     Current Time/Date    --   11-28-2001 13:57
--------------------------------------------------------------------------
                       User Online Command List

wmHelp(),  Shows system information and list of commands
getPerf(),  Snap Shot of the performance data
setIP(IpAdr), Sets IP address, example - setIP("10.10.5.37")
setMask(Netmask), Sets subnet Mask, example - setMask("255.0.0.0")
setGW(Gateway), Sets default Gateway example - setGW("10.10.5.10")
setSetComStr(ComStr), Sets SNMP set community string
setGetComStr(ComStr), Sets SNMP get community string
setPwd(oldPwd, newPwd), Sets adminstrator's password
--------------------------------------------------------------------------
Type <CR> to continue, Q<CR> to stop:
```

INSTALLATION AND MAINTENANCE MANUAL
Tsunami FAMILY
FAST ETHERNET WIRELESS BRIDGES
December 2001

WESTERN
Multiplex

If you use the Enter key or "CR," the following additional information is provided:

```
------------------------------------------------------------------
showAlarm(), Shows the alarm messgae
resetAlarm(), Resets the alarm log
setMainPort(speed, duplex), Sets the main Ethernet (TX) port
 parameter: speed: 1-auto, 2-100, 3-10; duplex: 1-Half, 2-Full
 example - setMainPort(1, 1)
getMainPort(), Gets the main TX port setting
setOduPwr(oduPower), Sets the ODU Power.
 example: setOduPwr(10)
getOduPwr(), Gets the ODU Power
setE1(channel, enable, ais, near-lpbk, far-lpbk), Sets the E1 channel
 parameter: channel: 1 or 2; all other parameters: 1-Enable, 2-Disable
 example - setE1(1, 1, 2, 2, 1)
getE1(channel), Gets the current E1 channel setting
 parameter: channel: 0 for all E1 channels, or select 1 or 2
 example - getE1(0)
resetPerf(), Resets the performance data
```

4.11.2.1 **NMS Help screen details:**

LEDs

Radio Fail	Green = Radio hardware O.K. Red = Hardware failure detected
RF Link	Green = Error-free operation Yellow = Bit errors occurring Red = Excessive bit errors or radio link failure
TXD	Green = 100BaseT data to transmit to far end present Yellow = 100BaseT port connected (no data present) Off = No 100BaseT connection detected
RXD	Green = 100BaseT data received from far end present Yellow = 100BaseT port connected (no data present) Off = No 100BaseT connection detected
COLL	Yellow = Collisions occurring on 100BaseT (half-duplex mode)
FAR END	Red = Alarm(s) present on the far-end radio**
NMS (10BaseT)	Green = Tx or Rx data present on the NMS interface Yellow = NMS interface connected (no data present) Off = No NMS interface connection detected
T1/E1 INPUT Note: there are two T1s on the model 27720 There is one full-time E1 on the model 27710-52 and one more can be added via radio configuration NMS.	Green = Alarm enabled and T1/E1 connection detected Red = Alarm enabled and no T1/E1 connection detected Yellow = Alarm disabled and T1/E1 connection detected Off = Alarm disabled and no T1/E1 connection detected

** Radio Fail, RF Link (yellow or red), T1 Input (yellow or red)

INSTALLATION AND MAINTENANCE MANUAL
Tsunami FAMILY
FAST ETHERNET WIRELESS BRIDGES
December 2001

WESTERN
Multiplex

Configuration (duplicated for Model 27720)

T1 Line Code	AMI/B8ZS setting for the T1 interface
T1 Line Build Out	T1 interface line length setting
T1 AIS @BER=10e-3	If selected, automatic injection of 1's into the T1 data stream during RF Link red alarm state
T1/E1 Input Alarm	If selected, activates alarm on loss of T1 signal
T1/E1 Near-end Radio Loopback	Activates loopback at the T1 input port of the near-end, towards the far-end of the link
T1/E1 Far-end Radio Loopback	Activates loopback at the T1 input port of the far-end, towards the near-end of the link
Orderwire Address	Orderwire telephone address (any 2 digit number 00-99)
Link Security Code	Security code set by user (any 6 bytes=12 characters) Valid characters are 0-9, A-F only (2 to the 48th codes) Note: Must match code on far-end radio to establish link Example: 3A45EBA27F65 or BDAF3976D2C5
Tx/Rx Frequency	Selects Tx and Rx frequencies – setting must match installed diplexer filter assembly – see manual for details
Ethernet Duplex	Selects half or full duplex for the 100BaseT interface
Learning Filter	Enables the ability to acquire and store IP addresses for efficient bridging operation (normally enabled)
Fiber Optic Interface	Enables the fiber 100BaseT interface
Device IP Address	Configure the IP address for the network management Ethernet interface
Device Subnet Mask	Configure the subnet mask for the network management Ethernet interface
SNMP Get Community	Configure the 'Get' community string for the radio's SNMP network management agent
SNMP Set Community	Configure the 'Set' community string for the radio's SNMP network management agent

Performance

Current BER	Current estimated RF link bit error rate
Current RSL (dBm)	Current estimated received signal level, in dBm
Errored Seconds	Number of seconds that incurred an error since the last reset of the "clear history" function. Indicates errored packets.
Severely Errored Seconds	Number of seconds that incurred errors in excess of BER=10e-6 since the last reset of the "clear history" function Usually indicates total loss of data/packets, not just errors
Min RSL (dBm)	Minimum estimated received signal level (in dBm) measured since the last reset of the "clear history" function
Max RSL (dBm)	Maximum estimated received signal level (in dBm) measured since the last reset of the "clear history" function
Elapsed Seconds Since Reset	Number of seconds since the last reset of the "clear history" function

Alarms

	IF GREEN	IF RED
T1/E1 Input	T1/E1 Input is present or T1/E1 input alarm is disabled	T1/E1 Input is NOT present and T1/E1 input alarm is enabled
T1 Code Violation	No T1 code violation error detected	T1 code violation error detected
T1 Line Driver	Line driver is adequate	Line driver is in fault condition
T1 AIS	NOT injecting all 1s	Injecting all 1s in data stream
Radio Sync	Radio link is synchronized	Radio link NOT established
Bit Error	Error-free operation	Bit Error Rate worse than 10e-7
Fan 1	Fan 1 is operating correctly	Fan 1 is NOT operating correctly
Fan 2	Fan 2 is operating correctly	Fan 2 is NOT operating correctly
Rx Synth	Receive synthesizer is locked	Receive synthesizer NOT locked
Tx Synth	Transmit synthesizer is locked	Transmit synthesizer NOT locked

Alarm and Status Indicators (models with IDU and ODU)

IDU	Green = Indoor Unit OK Yellow = warning condition in IDU (over-temp and/or both fans failed) Red = All fans failed, over-temp (>55°C), or NMU/IDU communication failure
Cable	Green = ODU Cable OK Red = ODU Cable shorted
ODU	Green = Outdoor Unit OK Red = Over-temp (>60°C), IDU to ODU communication failure, DC power loss, or Outdoor Unit detected hardware failure Yellow = Over temperature alarm, exceeds 55 degrees C
RF Link	Green = Link established with BER <10E-6 Yellow = BER 10E-6 ; any bit errors due to FEC overload Red = BER >10E-3 or Loss of Sync **Blinking Red = link ID does not match with far end radio**
TXD	Red = Links have loss of signal, both 100BaseT and 100BaseFX connector Yellow = Main Ethernet port is okay, but collision detected within the last 5 seconds or set to half duplex Green = Main Ethernet port is okay and valid data is passing thru Dark = Main Ethernet port is okay, but no data passing thru
RXD	Red = Links have loss of signal, both 100BaseT and 100BaseFX connector Green = Main Ethernet port is okay and valid data is passing thru Dark = Main Ethernet port is okay, but no data passing thru
Far End	Red = Alarm(s) present on the far-end radio** Green = No far end alarm(s) detected
NMS (10/100BaseT)	Green = Tx or Rx data present on the NMS interface Off = No NMS data, interface connection detected
E1 (or T1) WAYSIDE INPUT	Green = Wayside connection detected on enabled channels (both waysides) or channel(s) disabled Red = Wayside(s) input channel(s) enabled (either of the waysides) but eith channel has a LOS detected Yellow = One or both channels in Loopback mode

** Radio Fail, RF Link (yellow or red), T1/E1 Input (yellow or red)

4.11.4   Software Update Download Procedure

Software download procedure on Tsunami 100 (second release V 2.0):

1) Connect the host PC to the radio terminal through the NMS 10BaseT port.

2) Point the browser to the radio's Web page "http//xxx.xxx.xxx.xxx/upload.htm". (For factory default use 10.0.0.1 for the http: address)

3) Login as "manager" for name and password on the GUI prompt.

4) Follow the instructions on the screen.

   a) Enter the file name you want to upload, e.g. (a:ts_nmu.udl *software bianary image file*), or select the browse button and point to the proper location.

   b) While the file name is displayed on the screen, select the install button.

   c) It will display a status child window indicating it is erasing and writing to the *unused Bank*.. (Note the Bank # for ref.)

   d) After it is complete, you will see this message "File upload finished and system will reboot! Restart browser to logon again"

   e) Now, you can re-enter the upload GUI and insure the new uploaded Bank is valid and is the current Bank in use.

Memory Banks:

The radio has two banks of flash memory available, *Bank 0* and *Bank 1,* only one bank will be in use at a time. The radio will *automatically* utilize the new uploaded bank.

In addition, through the procedure, you can also manually select Bank 0 or Bank 1 by selecting the (switch) button. Switching between Banks is quick and you will need to re-start the browser. Also, to determine if a flash memory Bank has any software, you can read the Bank *status*. E.g. Valid or invalid, invalid indicating that it is an empty memory Bank.

INSTALLATION AND MAINTENANCE MANUAL
Tsunami FAMILY
FAST ETHERNET WIRELESS BRIDGES
December 2001

W E S T E R N
M u l t i p l e x
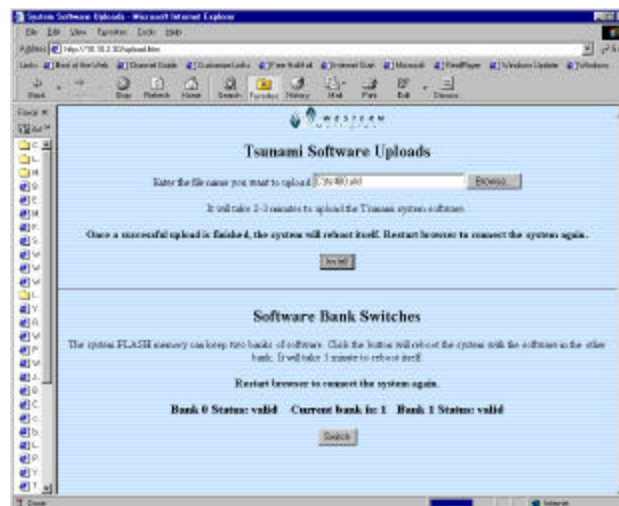
4.11.5   Serial Communication Mode

Use a standard session (i.e. Windows™ Hyperlink) to allow entry through the CONFIG port on the radio (program will emulate a VT100 monitor). Plug a null modem cable into the radio's CONFIGuration port.

Set the session to an unused COM port (e.g. COM1) and use 19,200 baud, 8 bits, No parity and One stop bit. Cable is two (2) DB-9F connectors with pins 2-3, 3-2 and 5-5 using 3 conductor wire.

To start a session (type what is within the single quotes and then the Enter key):

Hit the PC's CR/Enter key two (2) times after the radio has reinitialized

Type '1' and CR/Enter to enter the User Name and then Enter key (factory default=manager)

Type '2' and CR/Enter to enter the Password and then the Enter key (factory default=manager)

Type 'a' and Enter Key to accept the two entries - you should now see a menu list (a=accept)

Any time you wish to go back to a previous screen, type 'o' for out (if an 'o' does not exit from the page you working from, use 'logout' to exit).

There are many user changeable functions that may not be present in the browser such as setting the "Default Gateway" if the radio's NMS port is connected through a router.

As an example, the following steps can be used to check the radio's Network Status:

From the NMU Main Menu, type 3 and Enter.

Note the radio's IP address, subnet mask, MAC address and other radio parameters.

Example 2: Set a Default Gateway:

From the main menu (after logging in), type '11' to get to the VxWorks Shell prompt (->).

Type 'help' to get a list of all the advanced commands. Use the Enter key or 'Q' to complete.

From the -> prompt, type 'netHelp' to see a list of the network help commands
(Use Enter key or 'Q' to quit/stop).

From the -> prompt, type 'nmuHelp' to see a list of the nmu (Network Management Unit) commands
(Use Enter key or 'Q' to quit/stop).

From the -> prompt, type 'staticShow' to check to see if there is a current Default Gateway already set
(if set, you may want to write down the settings for future re-use).

Type 'staticAdd' to get to the Default Gateway setup command. Note the example.

Type 'help' to get the appropriate help details for the area you are accessing.

Follow the guidelines to set the Default Gateway command string:

> For example: staticAdd "0.0.0.0", "100.0.0.111", "255.255.255.0"

Check to confirm that the Default Gateway has been set properly by typing 'staticShow' again

When finished with the session, type 'o' or 'logout' until back to the Name-Password entry page you started from.

To print a complete list of available functions, type 'help' from a main menu screen and then print the page to your default printer connected to your PC.

Your Notes on the *Tsunami* Radio

5. Appendices

Appendix A - Digital Interface Specifications

1.   General Characteristics

100baseT (IEEE 802.3u) Fully compliant to Ethernet V.2

Pins:1=Tx+, 2=Tx-, 3=Rx+ & 6=Rx-

2.   Specifications

Transmission Medium	UTP
Signaling Technique	Manchester
Topology	Star
LAN Table	1,024 addresses (automatic learning and aging)
Filtering	15,000 pps
Data Rate	Up to throughput of particular radio model
Delay	2-5 frames
Buffer	4000 packets (200 kbytes)
Duplex	Full or half

Table A-1: Interconnection Specification

WESTERN *Multiplex*

Appendix B – 100BaseT and 10BaseT Connections

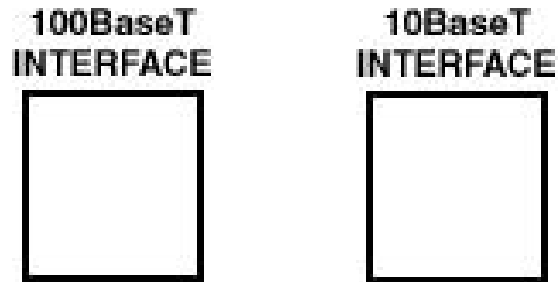**100BaseT INTERFACE**

10BaseT INTERFACE

Figure B-1: Fast Ethernet & Ethernet NMS Connectors

Pins:1=Tx+, 2=Tx-, 3=Rx+ & 6=Rx-

Appendix C – Networking Q&As

Q: What is Ethernet?

A: Ethernet is a type of network cabling and signaling specifications (OSI Model layers 1 [physical] and 2 [data link]) originally developed by Xerox in the late 1970. The IEEE's (Institute of Electrical and Electronics Engineers) used Ethernet Version 2 as the basis for the 802.3 CSMA/CD network standard.

Q: What is an 802.3 network?

A: That's IEEE-ish for Ethernet.

Q: What is CSMA/CD?

A: CSMA/CD is the media access control mechanism used by Ethernet and 802.3 networks; in other words, it determines how a packet of data is placed on the wire. CSMA/CD stands for "Carrier Sense Multiple Access, with Collision Detection". Before an Ethernet device puts a packet "on the wire", it listens to find if another device is already transmitting. Once the device finds the wire is clear, it starts sending the packet while also listening to hear if another device started sending at the same time (which is called a collision). Refer to the Q&A on collisions for more info about this phenomena.

Q: What is an OSI Model?

A: The Open Systems Interconnect (OSI) reference model is the ISO (International Standards Organization) structure for the "ideal" network architecture. This Model outlines seven areas, or layers, for the network. These layers are (from highest to lowest):

LAYER

7) Applications: Where the user applications software lies. Such issues as file access and transfer (FTP), virtual terminal emulation, Internet connections (HTTP), inter-process communication and the like are handled here.

6) Presentation: Differences in data representation are dealt with at this level. For example, UNIX-style line endings (CR only) might be converted to MS-DOS style (CRLF), or EBCIDIC to ASCII character sets.

5) Session: Communications between applications across a net-work is controlled at the session layer. Testing for out-of-sequence packets and handling two-way communication are handled here.

4) Transport: Makes sure the lower three layers are doing their job correctly, and provides a transparent, logical data stream between the end user and the network service s/he is using. This is the lower layer that provides local user services.

3) Network: This layer makes certain that a packet sent from one device to another actually gets there in a reasonable period of time. Routing and flow control are performed here. This is the lowest layer of the OSI model that can remain ignorant of

the physical network.

2) Data Link: This layer deals with getting data packets on and off the physical layer, error detection and correction and retransmission. This layer is generally broken into two sub-layers: The LLC (Logical Link Control) on the upper half, which does the error checking, and the MAC (Medium Access Control) on the lower half, which deals with getting the data on and off the physical layer (wire, fiber and Tsunami Wireless Bridges).

1) Physical: The nuts and bolts layer. Here is where the cable, fiber, radio, connector and signaling specifications are defined.

Q: What does an Ethernet packet look like?

A. See the information below, as described in the National Databook. The Ethernet packet preamble is normally generated by the chipset. Software is responsible for the destination address, source address, type, and data. The chips normally will append the frame check sequence.

```
+------------+
| | Preamble –
| 62 bits | A series of alternating 1's and 0's used by the
| | Ethernet receiver to acquire bit synchronization.
| |
+------------+
| | Start Of Frame Delimiter –
| 2 bits | Two consecutive 1 bits used to acquire byte
| | alignment.
+------------+
+------------+
| | Destination Ethernet Address –
| 6 bytes | Address of the intended receiver.
| | The broadcast address is all 1's.
+------------+
| | Source Ethernet Address –
| 6 bytes | The unique Ethernet address of the sending
| | station.
+------------+
| | Length or Type field –
| 2 bytes | For IEEE 802.3 this is the number of bytes of
| | data.
+------------+
| 46 bytes | Data –
| to | Short packets must be padded to 46 bytes.
| 1500 bytes |
+------------+
+------------+
| | Frame Check Sequence(CRC) –
| 4 bytes | The FCS is a 32 bit CRC calculated using
| | the AUTODIN II polynomial.
+------------+
```

The shortest packet is: 6 + 6 + 2 + 46 = 60 bytes The longest packet is: 6 + 6 + 2 + 1500 = 1514 bytes

Q: What is a MAC address?

A: It is the unique hexadecimal (numbering base 16) serial number assigned to each Ethernet network device to identify it on the network.. With Ethernet devices (as with most other network types), this address is permanently set at the time of manufacturer, though it can usually be changed through software (though this is generally a Very Bad Thing to do).

Q: Why must the MAC address to be unique?

A: Each communicating end device (not bridges) has a unique MAC address, so that it will be able to exclusively grab packets off the network meant for it. If MAC addresses are not unique, there is no way to distinguish between two devices. Devices on the network watch network traffic and look for their own MAC address in each packet to determine whether they should decode it or not. Special circumstances exist for broadcasting to every device.

Q: Is there a special numbering scheme for MAC addresses?

A: The MAC addresses are exactly 6 bytes in length, and are usually written in hexadecimal as 12:34:56:78:90:AB (the colons may be omitted, but generally make the address more readable). Each manufacturer of Ethernet devices applies for a certain range of MAC addresses they can use. The first three bytes of the address determine the manufacturer. RFC-1700 (available via FTP) lists some of the manufacturer-assigned MAC addresses. A more up-to-date listing of vendor MAC address assignments is available on ftp.lcs.mit.edu in pub/map/Ethernet-codes.

Q: What does CRC mean?

A: Cyclical Redundancy Check - A method of detecting errors in a message by performing a mathematical calculation on the bits in the message and then sending the results of the calculation along with the message. The receiving work-station performs the same calculation on the message data as it receives it and then checks the results against those transmitted at the end of the message. If the results don't match, the receiving end asks the sending end to send again.

Q: What do 10Base5, 10/100BaseT, 10Base2, etc mean?

A: These are the IEEE names for the different physical types of Ethernet. The "10" stands for maximum signaling speed: 10MHz. "Base" means Baseband. 10/100BaseT, where the T means twisted pair, and 10/100BaseF where the F means fiber (see the following Q&A for specifics). This actually comes from the IEEE committee number for that media. The "100" stands for maximum signaling speed: 100MHz.

In actual practice:

10Base2 Is a maximum of 10MHz Ethernet running over thin, 50 Ohm baseband coaxial cable. 10Base2 is also commonly referred to as thin-Ethernet or Cheapernet. 10Base5 is 10MHz Ethernet running over standard (thick) 50 Ohm baseband coaxial cabling. 10/100BaseF is Ethernet running over fiber-optic cabling. 10/100BaseT is Ethernet running over unshielded, twisted-pair cabling.

Q: What is UTP?

A: Twisted pair cables. UTP is for Unshielded, Twisted Pair, while STP is for Shielded, Twisted Pair. UTP is what's typically installed by phone companies (though this is often not of high enough quality for high- speed network use) and is what 10/100BaseT Ethernet runs over. UTP is graded according to its data carrying ability (e.g., Level 3, Level 4, Level 5). 10BaseT Ethernet requires at least Level 3 cable. Many sites now install only Level-5 UTP (CATegory 5), even though level 4 is more than sufficient for 10BaseT, because of the greater likelihood that emerging high-speed standards will require cable with better bandwidth capabilities. Fast Ethernet (100BaseT) must use CAT5!

Q: Are there any restrictions on how Ethernet is cabled?

A: Yes, there are many, and they vary according to the media used. First of all, there are distance limitations: 10/100BaseT generally accepted to have a maximum run of 100-150M, but is really based on signal loss in dB's (11.5db maximum loss source to destination). Then there are limitations on the number of repeaters and cable segments allowed between any two stations on the network.

The rule is, any possible path between two network devices on an unbridged/unrouted network cannot pass through more than 4 repeaters or hubs, nor more than 3 populated cable segments. 10/100BaseT and 10/100BaseF are star-wired, so there is no minimum distance requirement between devices, since devices cannot be connected serially. You can install up to the Ethernet maximum of 1024 stations per network with both 10/100BaseT and 10/100BaseF.

Q: When should I choose 10/100BaseT, 10/100BaseF (or others)?

A: The specific environment and application must be considered when selecting your media type. However, there are some general rules-of-thumb that you can consider:

Avoid using copper between buildings. The electrical disturbances caused by lightning, as well as naturally occurring differences in ground potential over distance, can very quickly and easily cause considerable damage to equipment and people. The use of fiber-optic cabling between buildings eliminates network cabling as a safety risk. There are also various wireless media available for inter-building links, such as laser, spread-spectrum RF and microwave.

10/100BaseT is the most flexible topology for LANs, and is generally the best choice for most network installations. 10/100BaseT hubs, or multi-hub concentrators, are typically installed in a central location to the user community, and inexpensive UTP cabling is run to each network device (which may be 100m, or 330ft, from the hub). The signaling technology is very reliable, even in somewhat noisy environments, and 10/100BaseT hubs will usually

INSTALLATION AND MAINTENANCE MANUAL
Tsunami FAMILY
FAST ETHERNET WIRELESS BRIDGES
December 2001

WESTERN
Multiplex

detect many network error conditions and automatically shut-down the offending port(s) without affecting the rest of the network (unless, of course, the offending port was your server, shared printer, or router to the rest of the world.

10/100BaseF, and its predecessor, FOIRL, are the only recommended topologies for inter-building links. However, they need not be limited to this role. 10/100BaseF can also be run to the desktop, though the cost is prohibitively high in all but the most specialized environments (generally, extremely noisy manufacturing facilities, or very security-conscious installations). More commonly, FOIRL (and now, 10/100BaseF) is used inside buildings and long distance wireless connections to form backbone networks.

Q: Is there an official "standard" punch down scheme for 10BaseT?

  A: Get a copy of EIA/TIA-568, it covers all of that sort of stuff: horizontal, vertical, connectors, patch cords, cross-connects, etc.

Q: Is it safe to run Unshield Twisted Pair next to power cable?

  A: According to EIA/TIA-569, the standard wiring practices for running data cabling and companion to the above referenced EIA/TIA-568, you should not run data cable parallel to power cables. However, in reality, this should not be a problem with networks such as 10/100BaseT. 10/100BaseT uses differential signaling to pick the data signals off the wire. Since any interference from nearby power lines will usually affect all pairs equally, anything that is not canceled-out by the twists in the UTP should be ignored by the receiving network interface.

Q: Can I connect the 10/100BaseT interface of two devices directly together, without using a hub?

  A: Yes, but not more than 2 devices, and you also need a special jumper cable between the two 10/100BaseT ports:

```
 RJ45 pin              RJ45 pin
 ======== ========
   1 <--[TX+]--------[RX+]--> 3
   2 <--[TX-]--------[RX-]--> 6
   3 <--[RX+]--------[TX+]--> 1
   6 <--[RX-]--------[TX-]--> 2
```

Q: What is a "segment"?

  A: A piece of network wire bounded by bridges, routers, repeaters or terminators.

Q: What is a "subnet?"

  A: Another overloaded term. It can mean, depending on the usage, a segment, a set of machines grouped together by a specific protocol feature (note that these machines do not have to be on the same segment, but they could be) or a big nylon thing used to capture enemy subs.

Q: What is a repeater?

A: A repeater acts on a purely electrical level to connect to segments. All it does is amplify and reshape (and, depending on the type, possibly retime) the analog waveform to extend network segment distances. It does not know anything about addresses or forwarding, thus it cannot be used to reduce traffic as a bridge can in the example above.

Q: What is a "switch?"

A: A switch connects Ethernet packets at the MAC address level (ISO Level 2, like Bridges). It divides a local area network (LAN) into multiple, separate *segments*. Each segment has it's own full Ethernet (or Fast Ethernet) bandwidth that does not compete with other segments for network transmission. The switch acts as a high-speed selective bridge between the individual segments. The switch, without interfering with any other segments, automatically forwards traffic that needs to go from one segment to another and blocks traffic that does not need to be sent through another segment. Always use a switch to maintain a high level of network operation over the choice of a hub. Switches come in both managed and unmanaged versions.

Q: What is a "hub?"

A: A hub is a common wiring point for star-topology networks, and is a common synonym for concentrator (though the latter generally has additional features or capabilities). 10/100BaseT and 10/100BaseF Ethernet and many proprietary network topologies use hubs to connect multiple cable runs in a star-wired network topology into a single network. Hubs have multiple ports to attach the different cable runs. Some hubs (such as 10/100BaseT) include electronics to regenerate and retime the signal between each hub port. Use a hub only when the network connections are very few, a switch is always a better choice for multiple network connections.

Q: What is a bridge?

A: A bridge will connect to distinct segments and transmit traffic between them. This allows you to extend the maximum size of the network while still not breaking the maximum wire length, attached device count, or number of repeaters for a network segment.

Q: What does a "learning bridge"?

A: A learning bridge monitors MAC (OSI layer 2) addresses on both sides of its connection and attempts to learn which addresses are on which side. It can then decide when it receives a packet whether it should cross the bridge or stay local (some packets may not need to cross the bridge because the source and destination addresses are both on one side). If the bridge receives a packet that it doesn't know the addresses of, it will forward it by default. IEEE's standard for a learning bridge is 802.1D.

Q: Is there a maximum number of bridges allowed on a network?

A: Per IEEE 802.1 (d), the maximum number of concatenated brides in a bridged LAN is 7.

This number is rather arbitrary, however, and is based on simulations of application performance with expected bridge delays.

In addition, the number assumes that all bridges are LOCAL (no remote WAN connections), and that the default Hold Time of 1 second is in place (this is the time after which a bridge will discard a frame it is holding). This prevents extra-late frame delivery. (i.e, a frame should never be delivered more than ~7 seconds after is it sent). The rule of thumb for wireless WAN bridged LANs is to limit the number of hops to 4.

Q: What is a router?

A: Routers work much like bridges, but they pay attention to the upper network layer protocols (OSI layer 3) rather than data link layer (OSI layer 2) protocols. A router will decide whether to forward a packet by looking at the protocol level addresses (for instance, TCP/IP addresses) rather than the MAC address. Because routers work at layer 3 of the OSI stack, it is possible for them to transfer packets between different media types (i.e., leased lines, Ethernet, token ring, X.25, Frame Relay and FDDI). Many routers can also function as bridges.

Q: So should I use a router or a bridge?

A: There is no absolute answer to this. Your network layout, type and amount of hosts and traffic, and other issues (both technical and non-technical) must be considered. Routing would always be preferable to bridging except that routers are slower and usually more expensive (due to the amount of processing required to look inside the physical packet and determine which interface that packet needs to get sent out), and that many applications use non-routable protocols.

Rules of thumb:

Bridges are usually good choices for small networks with few, if any, slow redundant links between destinations or for connecting distant LANs. Further, bridges may be your only choice for certain protocols, unless you have the means to encapsulate (tunnel) the un-routable protocol inside a routable protocol.

Routers are usually much better choices for larger networks, particularly where you want to have a relatively clean WAN backbone. Routers are better at protecting against protocol errors (such as broadcast storms) and bandwidth utilization. Since routers look deeper inside the data packet, they can also make forwarding decisions based on the upper-layer protocols.

Occasionally, a combination of the two devices are the best way to go. Bridges can be used to segment small networks that are geographically close to each other, between each other and the router to the rest of the WAN.

Q: Are there problems mixing Bridging & Routing?

A: Only if you plan on having bridged links in parallel with routed links. You need to be very careful about running bridges providing links in parallel to a router. Bridges may forward broadcast requests which will confuse the router there are lots of protocols you may not

think of filtering (e.g. ARP, Apple ARP over 802.3 etc. etc.). Also, DECnet routers have the same MAC address on all ports. This will probably cause the bridge to think it is seeing an Ethernet loop.

Q: Who makes the fastest/easiest/most advanced bridges or routers?

A: The IETF runs bench marks on a wide selection of wired/fiber bridges and routers. Network Computing runs bench marks for wireless routers (point-to-multipoint) and bridges (point-to-point).

Q: What does "IPG" mean?

A: The InterPacket Gap (more properly referred to as the InterFrame Gap, or IFG) is an enforced quiet time of 9.6 us between transmitted Ethernet frames.

Q: What means "promiscuous mode"?

A: Promiscuous mode is a condition where the network interface controller will pass all Ethernet frames, regardless of destination address, up to the higher level network layers. Normally the network controller will only pass up frames that have that device's destination address. However, when put in promiscuous mode, all frames are passed on up the network stack regardless of destination address. Promiscuous mode is usually used by network monitoring tools and transparent bridges.

Q: What is a collision?

A: A condition where two devices detect that the network is idle and end up trying to send packets at exactly the same time (within 1 round-trip delay). Since only one device can transmit at a time, both devices must back off and attempt to retransmit again.

The retransmission algorithm requires each device to wait a random amount of time, so the two are very likely to retry at different times, and thus the second one will sense that the network is busy and wait until the packet is finished. If the two devices retry at the same time (or almost the same time) they will collide again, and the process repeats until either the packet finally makes it onto the network without collisions, or 16 consecutive collision occur and the packet is aborted.

Q: What causes a collision?

A: See above. Ethernet is a CSMA/CD (Carrier Sense Multiple Access/ Collision Detect) system. It is possible to not sense carrier from a previous device and attempt to transmit anyway, or to have two devices attempt to transmit at the same time; in either case a collision results. Ethernet is particularly susceptible to performance loss from such problems when people ignore the "rules" for wiring Ethernet.

Q: How many collisions are too many?

A: This depends on your application and protocol. In many cases, collision rates of 50% will

INSTALLATION AND MAINTENANCE MANUAL
Tsunami FAMILY
FAST ETHERNET WIRELESS BRIDGES
December 2001

WESTERN
Multiplex

not cause a large decrease in perceived throughput. If your network is slowing down and you notice the percentage of collisions is on the high side, you may want try segmenting your network with either a bridge or router to see if performance improves.

Q: How do I reduce the number of collisions?

A: Disconnect devices from the network. Seriously, you need to cut- down on the number of devices on the network segment to affect the collision rate. This is usually accomplished by splitting the segment into two pieces and putting a bridge or router in between them.

Q: What is a late collision?

A: A late collision occurs when two devices transmit at the same time, but due to cabling errors (most commonly, excessive network segment length or repeaters between devices) neither detects a collision. The reason this happens is because the time to propagate the signal from one end of the network to another is longer than the time to put the entire packet on the network, so the two devices that cause the late collision never see that the other's sending until after it puts the entire packet on the network. late collisions are detected by the transmitter after the first "slot time" of 64 byte times. They are only detected during transmissions of packets longer than 64 bytes. It's detection is exactly the same as for a normal collision; it just happens "too late."

Typical causes of late collisions are segment cable lengths in excess of the maximum permitted for the cable type, faulty connectors or improper cabling, excessive numbers of repeaters between network devices, and defective Ethernet transceivers or controllers.

Another negative concerning late collisions is that they occur for small packets also, but cannot be detected by the transmitter. A network suffering a measurable rate of late collisions (on large packets) is also suffering lost small packets. The higher protocols do not cope well with such losses. Well, they cope, but at much reduced speed. A 1% packet loss is enough to reduce the speed of NFS by 90% with the default retransmission timers. That's a 10 times increase of the problem!

Finally, Ethernet controllers do not retransmit packets lost to late collisions.

Q: What is a jam?

A: When a workstation receives a collision, and it is transmitting, it puts out a jam so all other stations will see the collision also. When a repeater detects a collision on one port, it puts out a jam on all other ports, causing a collision to occur on those lines that are transmitting, and causing any non-transmitting stations to wait to transmit.

Q: What is a broadcast storm?

A: An overloaded term that describes an overloaded protocol. Basically it describes a condition where devices on the network are generating traffic that by its nature causes the generation of even more traffic. The inevitable result is a huge degradation of performance or complete loss of the network as the devices continue to generate more and more traffic. This can be related to the physical transmission or to very high level protocols.

Q: How do I recognize a broadcast storm?

A: That depends on what level it is occurring. Basically you have to be aware of the potential for it beforehand and be looking for it, because in a true broadcast storm you will probably be unable to access the network. This can change dramatically for a higher level protocol. NFS contention can result in a dramatic DROP in Ethernet traffic, yet no one will have access to resources.

Q: How can I prevent a broadcast storm?

A: Avoid protocols that are prone to it. Route (with routers) or Bridge (with wired/wireless bridges) when it is practical.

Q: What is *high* traffic on an Ethernet? 5%? 20%? 90%?

A: High traffic is when things start slowing down to the point they are no longer acceptable. There is not set percentage point, in other words. Usually start paying attention when it gets over 40-50%.

Q: Why do I see different throughput speeds?

A: Bridges (such as Tsunami) are ISO Layer 2 Data Link Layer (use MAC address for filtering) devices where they provide their full stated throughput. At level 2 (bridges) or 3 (routers) where hardware plays the major part, the most common tester is the SmartBits 200 product from NetCom Systems. At Application Layer 7, you will see less than 40% throughput from the maximum capacity measured w/SmartBits due to the increased protocol/software overhead at that level. Layer 7 can be tested with software such as Ganymede's Chariot or Qcheck product.

As an example: testing copper CAT5 cable with SmartBits will test 100% throughput (let's say you can send/rcv a full 10Mbps). At Layer 7 you will be transferring data at the 10Mbps rate, but only 4Mbps of user data will transfer (Ethernet has a high overhead of bytes added to each data packet each time you go up a layer). The advantage is the more complex overhead makes the data virtually resilient to corruption and minor errors (i.e. collisions), it's easy to reroute and can use inexpensive plug/play devices like hubs/switches instead of multiplexers as used in the telco industry (i.e. -51 T1 radios)

Western Multiplex tests at Layer 2 where bridges are defined. At layer 7 (Application Layer), you will see less than 40% or more depending on the other traffic that may be on the LAN as this layer is more dependent on the type of data being sent (it does not matter if it's wire, fiber or any Ethernet bridge -wired or wireless). Another way to look at it: the model 31145 12Mbps (10Mbps 10BaseT+T1/E1 wayside) bridge will test the same as a piece of CAT5 Ethernet cable.

Q: How can I test an Ethernet?

INSTALLATION AND MAINTENANCE MANUAL
Tsunami FAMILY
FAST ETHERNET WIRELESS BRIDGES
December 2001

WESTERN
Multiplex

A: This depends on what level you want to test. The most basic test (a.k.a., "the fire test") is to connect a pair of devices to the network and see if they can communicate with each other. If you want to test the electrical integrity of the wire (i.e., will it carry a signal properly), a TDR or cable scanner that incorporates TDR and other functions, would be the most comprehensive tool. If you need to test the performance or troubleshoot protocol transmission problems, you will need special and usually very expensive software, usually coupled with custom hardware, to capture, optionally filter, and analyze the network packets. Also, see the answer to the question above.

Q: What is a "TDR"?

A: A Time-Domain Reflectometer is a tool used to detect cable faults. This device operates by sending a brief signal pulse down the cable and looking for its reflection to bounce back. By analyzing the reflected pulse, it is possible to make judgments about the quality of the cable segment. More advanced units can not only detect and identify the nature of the problem, but give a reasonably accurate indication of the problem's location (distance from the point of the test). There is also a device known as an OTDR, which is an Optical Time-Domain Reflectometer for fiber-optic cables.

Q: What is a "BERT"?

A: Bit Error Rate Tester. This equipment is used to analyze the amount and types of errors that occur on a cable segment.

Q: What (free) tools are there to monitor/decode/etc an Ethernet?

A: There are many built into most DOS ,Unix and other operating systems. For example, the ping command can be used to determine if a given host is alive, and will also tell you the round trip transmission time. The command "ifconfig" will tell you the status of the network interfaces. "netstat" will summarize statistics for network usage.

DOS commands (through Windows DOS application) are:

ARP

Displays and modifies the IP-to-Physical address translation tables used by address resolution protocol (ARP).

ARP -a [inet_addr] [-N if_addr]

-a   Displays current ARP entries by interrogating the current protocol data. If inet_addr is specified, the IP and Physical addresses for only the specified computer are displayed. If more than one network interface uses ARP, entries for each ARP table are displayed.
-g   Same as -a.
   inet_addr   Specifies an internet address.
   -N if_addr   Displays the ARP entries for the network interface specified by if_addr.
-d   Deletes the host specified by inet_addr.
-s   Adds the host and associates the Internet address inet_addr with the Physical address eth_addr. The Physical address is given as 6 hexadecimal bytes

separated by hyphens. The entry is permanent.

eth_addr	Specifies a physical address.
if_addr	If present, this specifies the Internet address of the interface whose address translation table should be modified. If not present, the first applicable interface will be used.

Example:
> arp -s 157.55.85.212 00-aa-00-62-c6-09 .... Adds a static entry.
> arp -a .... Displays the arp table.

FTP

Transfers files to and from a computer running an FTP server service (sometimes called a daemon). FTP can be used interactively.

FTP [-v] [-d] [-i] [-n] [-g] [-s:filename] [-a] [-w:windowsize] [-A] [host]

-v	Suppresses display of remote server responses.
-n	Suppresses auto-login upon initial connection.
-i	Turns off interactive prompting during multiple file transfers.
-d	Enables debugging.
-g	Disables filename globbing (see GLOB command).
-s:filename	Specifies a text file containing FTP commands; the commands will automatically run after FTP starts.
-a	Use any local interface when binding data connection.
-A	login as anonymous.
-w:buffersize	Overrides the default transfer buffer size of 4096.
host	Specifies the host name or IP address of the remote host to connect to.

Notes:
 - mget and mput commands take y/n/q for yes/no/quit.
 - Use Control-C to abort commands.

NET CONFIG	Displays your current workgroup settings.
NET DIAG	Runs the Microsoft Network Diagnostics program to display diagnostic information about your network.
NET HELP	Provides information about commands and error messages.
NET INIT	Loads protocol and network-adapter drivers without binding them to Protocol Manager.
NET LOGOFF	Breaks the connection between your computer and the shared resources to which it is connected.
NET LOGON	Identifies you as a member of a workgroup.
NET PASSWORD	Changes your logon password.
NET PRINT	Displays information about print queues and controls print jobs.

W E S T E R N
Multiplex

NET START   Starts services.

NET STOP   Stops services.

NET TIME   Displays the time on or synchronizes your computer's clock with the clock
                 on a Microsoft Windows for Workgroups, Windows NT, Windows 95, or
                 NetWare time server.

NET USE   Connects to or disconnects from a shared resource or displays information
                 about connections.

NET VER   Displays the type and version number of the workgroup redirector you are
                 using.

NET VIEW   Displays a list of computers that share resources or a list of shared
                 resources on a specific computer.

For more information about a specific Microsoft NET command, type the command name
followed by /? (for example, NET VIEW /?).

PING

PING   [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS] [-r count] [-s count] [[-j host-list] | [-k
        host-list]] [-w timeout] destination-list

-t   Ping the specified host until stopped. To see statistics and continue - type
                 Control-Break; To stop - type Control-C.
-a   Resolve addresses to hostnames.
-n count   Number of echo requests to send.
-l size   Send buffer size.
-f   Set Don't Fragment flag in packet.
-i TTL   Time To Live.
-v TOS   Type Of Service.
-r count   Record route for count hops.
-s count   Timestamp for count hops.
-j host-list   Loose source route along host-list.
-k host-list   Strict source route along host-list.
-w timeout   Timeout in milliseconds to wait for each reply.

ROUTE

Manipulates network routing tables.

ROUTE [-f] [command [destination] [MASK netmask] [gateway] [METRIC metric]]

-f   Clears the routing tables of all gateway entries. If this is used in conjunction with
         one of the commands, the tables are cleared prior to running the command.

command   Must be one of four:
                 PRINT   Prints a route
                 ADD   Adds a route

DELETE   Deletes a route
CHANGE   Modifies an existing route

destination   Specifies the destination host.

MASK   Specifies that the next parameter is the 'netmask' value.

netmask   Specifies a subnet mask value to be associated with this route entry. If not specified, it defaults to 255.255.255.255.

gateway   Specifies gateway.

METRIC   Specifies that the next paramenter 'metric' is the cost for this destination

All symbolic names used for destination are looked up in the network database file NETWORKS. The symbolic names for gateway are looked up in the host name database file HOSTS.

If the command is PRINT or DELETE, wildcards may be used for the destination and gateway, or the gateway argument may be omitted.

Diagnostic Notes:
Invalid MASK generates an error, that is when (DEST & MASK) != DEST.
Example>   route ADD 157.0.0.0 MASK 155.0.0.0 157.55.80.1
          The route addition failed: 87

Examples:

> route   PRINT
> route   ADD 157.0.0.0   MASK 255.0.0.0   157.55.80.1   METRIC 3
           ^destination   ^mask   ^gateway   ^metric
> route   PRINT
> route   DELETE 157.0.0.0
> route   PRINT

SNMP

Starts SNMP agent

-close   Closes previously running instance of snmp
-help   Displays SNMP help dialog box

TELNET

Opens telnet window

TRACERT

TRACERT [-d] [-h maximum_hops] [-j host-list] [-w timeout] target_name

```
-d                      Do not resolve addresses to hostnames.
-h maximum_hops         Maximum number of hops to search for target.
-j host-list            Loose source route along host-list.
-w timeout              Wait timeout milliseconds for each reply.
```

WINIPCFG

Opens IP configuration window

/All - Display detailed information
/Batch - [filename] Write to file or .\winipcfg.out
/renew_all - Renew all adapters
/release_all - Release all adapters
/renew N - Renew adapter N
/release N - Release adapter N

Q: What books are good about Ethernet LAN's?

A: The IEEE 802.3 documents are considered the definitive source for information on Ethernet. However, these may not be suitable for all levels of users. Surprisingly, there are few good books specifically dealing with Ethernet LANs, but here are a few that you might find useful:

Local Area Networks, An introduction to the technology by John E. McNamara, published by Digital Press, 1985 165 pps. with index and glossary, $29.00 ISBN 0-932376-79-7, Digital Press part number EY-00051-DP.

Network Troubleshooting Guide by Digital Equipment Corporation, August 1990 Approx. 278 pps. with index and glossary, $95.00 Digital Press part number EK-339AB-GD-002.

These books and others are recommended in the network reading list, net-read.txt, from ftp.utexas.edu.

Q: Where can I get IEEE802.x docs online?

A: Not available online. IEEE documents can be ordered directly from the IEEE themselves. You can contact them at:

Institute of Electrical and Electronic Engineers 445 Hoes Lane P.O. Box 1331 Piscataway, NJ 08855-1331 U.S.A. (800) 678-IEEE

Q: Where can I get EIA/TIA docs online?

A: Not available online They can be ordered from:

Global Engineering 800-854-7179

Appendix D – Auxiliary Data Connectors

The following figures illustrate the pin structure for all auxiliary connections. All figures are oriented as a customer would view them, facing the connector. DC power connection information is found in Section 3.7 of the manual.
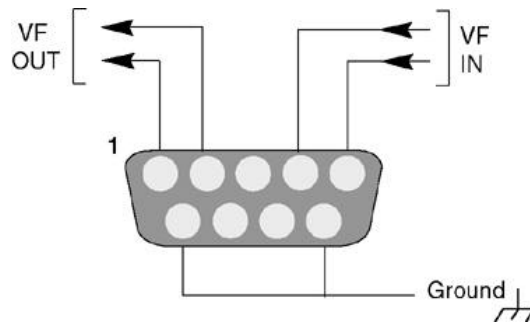
Figure D-1: VF Port Connection
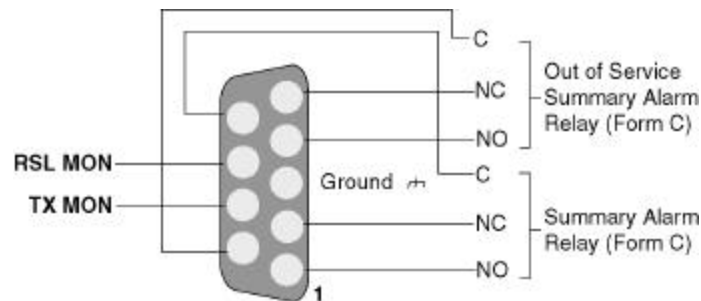
Figure D-2: Alarm Port Connections
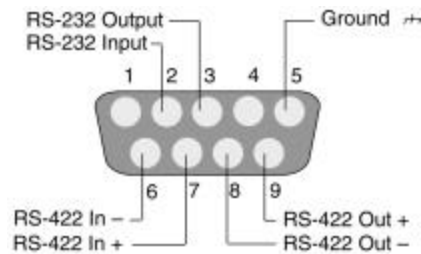
Figure D-3: Config(uration) Port 9-Pin D-Style Connector
Do NOT connect to RS-422 pins at any time.

INSTALLATION AND MAINTENANCE MANUAL
Tsunami FAMILY
FAST ETHERNET WIRELESS BRIDGES
December 2001

WESTERN
Multiplex
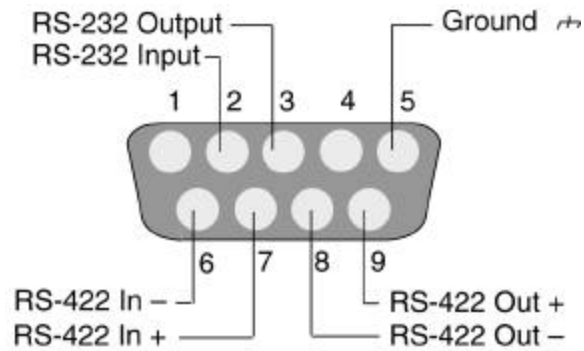
Figure D-4: AUX DATA Port 9-Pin D-Style Connector

Do NOT connect to RS-422 pins at any time.

Appendix E – Installation and Troubleshooting Guide

(Insert foldout after this page)

Your Notes on the *Tsunami* Radio

Index

W

For ISO Purposes -

Last Page of this Manual