Recommended Tools and Test Equipment

Table B-1 lists the basic tools and test equipment necessary to perform general maintenance and troubleshooting tasks on the Cisco uBR10012 router.

Table B-1 Recommended Tools and Test Equipment

Equipment	Description
Number 2 Phillips and flat-head screwdrivers	Small and medium-sized.
Voltage tester	Refer to the "Testing with Digital Multimeters and Cable Testers" section on page B-1.
Optical fiber test equipment	Refer to the "Testing with Digital Multimeters and Cable Testers" section on page B-1.
Cable testing equipment	Refer to the "Testing with Digital Multimeters and Cable Testers" section on page B-1.
ESD-preventive wrist or ankle strap with connection cord	—

The following sections describe advanced testing equipment to aid in complex problem isolation.

Testing with Digital Multimeters and Cable Testers

Use a digital multimeter to measure parameters such as AC and DC voltage, current, resistance, capacitance, cable continuity. Use cable testers, also, to verify physical connectivity.

Use cable testers (scanners) to check physical connectivity. Cable testers are available for shielded twisted pair (STP), unshielded twisted pair (UTP), 10BaseT, and coaxial and twinax cables. A given cable tester might be able to perform any of the following functions:

- Test and report on cable conditions, including near-end crosstalk (NEXT), attenuation, and noise.
- Perform time domain reflectometer (TDR), traffic monitoring, and wire map functions.
- Display Media Access Control (MAC) layer information about LAN traffic, provide statistics such as network utilization and packet error rates, and perform limited protocol testing (for example, TCP/IP tests such as ping).

Test fiber-optic cable both before installation (on-the-reel testing) and after installation. Continuity testing of the fiber requires either a visible light source or a reflectometer. Light sources capable of providing light at the three predominant wavelengths, 850 nanometers (nm), 1300 nm, and 1550 nm, are used with power meters that can measure the same wavelengths and test attenuation and return loss in the fiber.

Testing with TDRs and OTDRs

This section describes time domain reflectometers (TDRs) and optical time domain reflectometers (OTDRs), which are typically used to detect cable defects.

Testing with TDRs

Use time domain reflectometers to test for the following cable defects:

- Open and short circuits
- Crimps, kinks, and sharp bends
- Impedance mismatches
- Other defects

A TDR works by “bouncing” a signal off the end of the cable. Open circuits, short circuits and other problems reflect the signal back at different amplitudes, depending on the problem.

A TDR measures:

- the amount of time it takes for the signal to reflect
- The physical distance to a fault in the cable
- The length of a cable

Some TDRs can also calculate the propagation rate based on a configured cable length.

Testing with OTDRs

Use optical time domain reflectometers to:

- Locate fiber breaks
- Measure attenuation
- Measure the length of a fiber
- Measure splice or connector losses

An OTDR can be used to identify the “signature” of a particular installation, noting attenuation and splice losses. This baseline measurement can then be compared with future signatures if you suspect a problem in the system.

Testing with Breakout Boxes, Fox Boxes, and BERTs/BLERTs

Use breakout boxes, fox boxes, and bit/block error rate testers (BERTs/BLERTs) to measure the digital signals present at:

- PCs
- Printers
- Modems
- CSU/DSUs

These devices can monitor data line conditions, analyze and trap data, and diagnose problems common to data communication systems. Traffic from data terminal equipment (DTE) through data communications equipment (DCE) can be examined to:

- Isolate problems
- Identify bit patterns
- Ensure that the correct cabling is installed

These devices cannot test media signals such as Ethernet, Token Ring, or FDDI.

Testing with Network Monitors

Use network monitors to:

- Track packets crossing a network
- Provide an accurate picture of network activity at any moment
- Provide a historical record of network activity over a period of time

Network monitors do not decode the contents of frames. Monitors are useful for baselining, in which the activity on a network is sampled over a period of time to establish a normal performance profile, or baseline.

Monitors collect information such as packet sizes, the number of packets, error packets, overall usage of a connection, the number of hosts and their MAC addresses, and details about communications between hosts and other devices. This data can be used to:

- Create profiles of LAN traffic
- Locate traffic overloads
- Plan for network expansion
- Detect intruders
- Establish baseline performance
- Distribute traffic more efficiently

Testing with Network Analyzers

Use network analyzers (also called protocol analyzers) to decode protocol layers in a recorded frame and present the layers as readable abbreviations or summaries, detailing which layer is involved (physical, data link, and so forth) and the function each byte or byte content serves.

Most network analyzers can perform many of the following functions:

- Filter traffic that meets certain criteria so that, for example, all traffic to and from a particular device can be captured.
- Time-stamp captured data.
- Present protocol layers in an easily readable form.
- Generate frames and transmit them onto the network.
- Incorporate an “expert” system in which the analyzer uses a set of rules, combined with information about the network configuration and operation, to diagnose and solve, or offer potential solutions to, network problems.