

NetKnowledge Webinar



Router Troubleshooting: A Fast and Effective Approach



Presented by:

Scott Hogg, Principal Consultant

Rick Blum, Senior Manager, Strategic Marketing

scott.hogg@ins.com

rick.blum@ins.com

T h e k n o w l e d g e b e h i n d t h e n e t w o r k ®

International Network Services

- ◆ Vendor-independent consulting services
- ◆ IP network management software
- ◆ Build, secure and manage network infrastructure
- ◆ 30+ offices in North America and Europe
- ◆ 18,000+ engagements over 12 years
- ◆ Serve Fortune 1000 enterprises, service providers, and other network-centric organizations



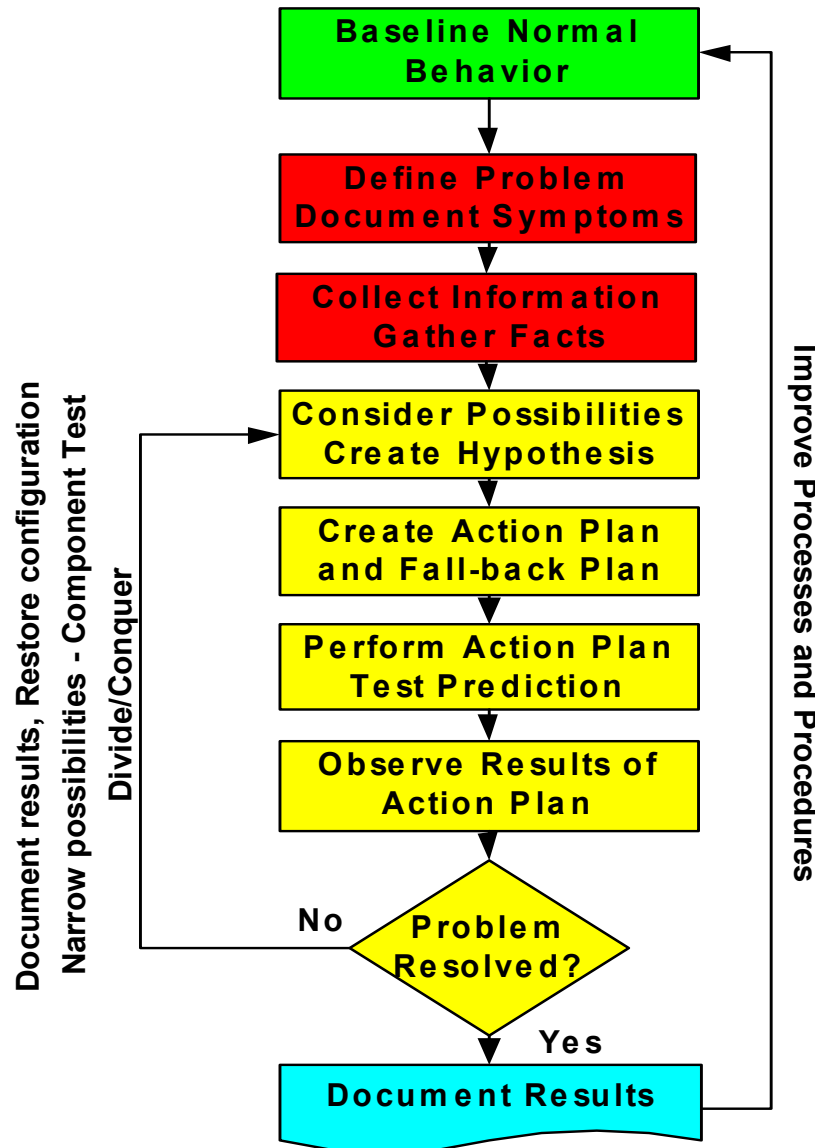
Cost of Network Downtime

- ◆ Can your company afford to be down for more than a few hours?
- ◆ What is the revenue lost per hour of downtime?
- ◆ Increased complexity means higher MTTR
- ◆ Improving troubleshooting skills directly impacts bottom line and reduces business risk

| Industry | Business Operation | Industry Range for Cost Per Hour | Average Cost Per Hour |
|----------------|--------------------|----------------------------------|-----------------------|
| Financial | Brokerage | \$5.6 - 7.3M | \$6.45M |
| Financial | Credit Card | \$2.2 - 3.1M | \$2.6M |
| Transportation | Airline | \$67 - 112K | \$89.5K |
| Transportation | Shipping | \$24 - 32K | \$8K |
| Retail | Catalog Sales | \$60 - 120K | \$90K |

Source: Dataquest

Scientific Method Troubleshooting

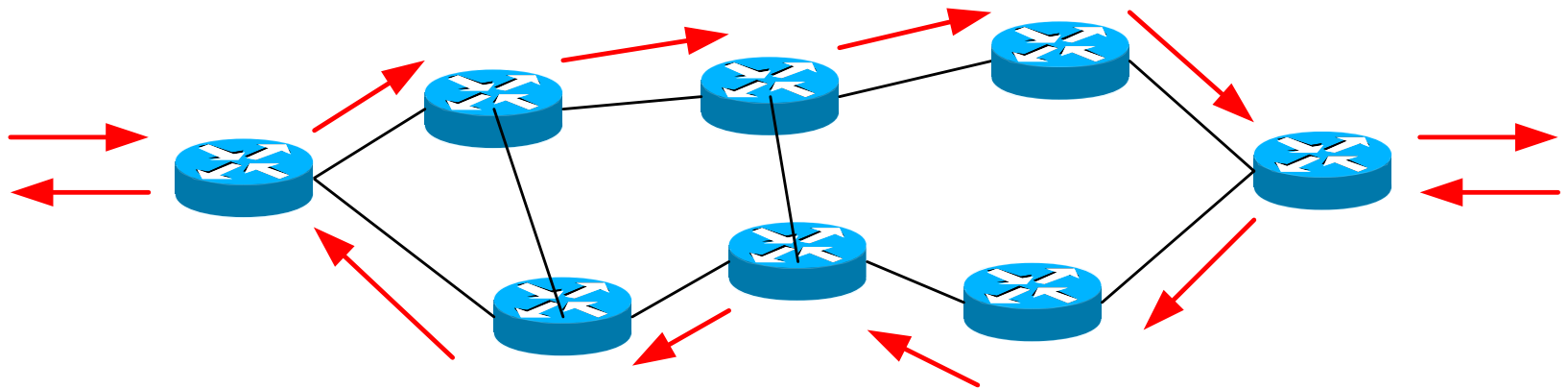


Start Gathering Information

- ◆ **Troubleshoot with the OSI model in mind**
 - *Use ARP tables to help verify Layer 2 connectivity*
 - *Remember to clear the ARP cache after IP or hardware changes*
- ◆ **Cisco Discovery Protocol (CDP)**
 - *Use CDP to help you map out the network*
 - *CDP can be used as another check between Layer 2/3*
- ◆ **Start at the edges of the network first**
 - *Check the TCP/IP stack of the host end-systems*
 - *Check the IP address and the default gateway*
 - *ifconfig, ipconfig, winipcfg, sh ip int, netstat -rn, route print*
- ◆ **Consider if DNS or DHCP are part of the problem**
 - *DNS can cause a global problem that appears like a routing problem*
 - *nslookup, host, dig, whois*

Troubleshoot in Both Directions

- ◆ Use troubleshooting tools in both directions
- ◆ Asymmetrical traffic paths can be indication of a misconfiguration
- ◆ Determine why are paths are different



End-to-End IP Connectivity

- ◆ **Ping checks basic connectivity; measures round-trip time**
 - *Ping yourself and then the default gateway (router)*
 - *Ping by name and by IP address (test DNS)*
 - *Ping both directions*
- ◆ **Traceroute uses UDP probes and checks ICMP responses one TTL hop at a time**
 - *The best utility for troubleshooting routing problems*
 - *Try traceroute both directions to test for asymmetry*
 - *Check last router to respond to the trace*
- ◆ **Telnet provides basic terminal emulation to a remote host**
 - *Telnet by name or by IP address – specify the TCP port number*
- ◆ **Try using extended ping, traceroute, and telnet parameters**
 - *Source IP, Loose/Strict/Record Route, Verbose, Fragmentation*

Gentle Router Debugging

- ◆ **Vendors have debug commands for every occasion**
- ◆ **Debug commands can be dangerous**
 - *Don't send debugs to console – 9600 baud*
 - *Sending output to vty is OK, syslog is preferred*
- ◆ **Open two Telnet/ssh sessions at a time**
 - *Be prepared to turn debugging off in one session*
- ◆ **Use filters on the debug output whenever possible**
 - *Access-list debug filtering*
 - *Interface debug filtering*
- ◆ **Use NTP for accurate timestamps**

TCP/IP Protocol Analysis

- ◆ # tcpdump host mercury and tcp port 23 -w outfile
- ◆ # snoop mercury and tcp port 23 -o outfile
- ◆ “debug ip packet [ACL#] [detail] [dump]”
 - *If displays “unroutable”, “show ip route”*
 - *If displays “encap failed”, check Layer 2*
- ◆ **Ethereal – conversion between capture formats**
- ◆ **Protocol analyzers**
 - *Numerous protocol decodes*
 - *H.323 – ASN.1 decode*
 - *Remote probe capabilities*
 - *Remote SPAN (RSPAN)*

Routing Table Problems



- ◆ Routing forwarding table and protocol table
- ◆ Inactive or flapping routes
- ◆ Check routing table and routing metrics for specific routes – check in both directions
- ◆ Clear out specific route or entire routing table and let it build back again – last resort
- ◆ Check route summarization and redistribution
- ◆ Administrative distance (believability/favorability)
- ◆ Equal-cost load balancing
- ◆ Asymmetrical routing
 - *Open jaw routes , Black hole routes, Gray hole routes*

Troubleshooting RIP



- ◆ Hop-by-hop updates get lost
- ◆ Check RIPv1 and RIPv2 compatibility
- ◆ Problems caused by summarization
 - *RIPv2's default behavior is to summarize at net boundaries – Use "no auto-summary"*
- ◆ Discontiguous subnet mask problems
- ◆ Redistribution into classless routing protocols
- ◆ Check if split-horizon enabled on interface
- ◆ View the RIP database or use debug commands
- ◆ Ripquery – tool written by Jeff Honig
- ◆ Convergence times may be longer than ever thought possible (~10 minutes)

Troubleshooting EIGRP

- ◆ Remember “no auto-summary”
- ◆ Check interface summary commands
- ◆ Tables: Routing, Topology, Neighbor
 - *“show ip eigrp neighbor”*
 - *“show ip eigrp topology”*
- ◆ Neighbor instability (multicast, hello/hold)
 - *Extended ping to 224.0.0.10*
- ◆ Use “eigrp log-neighbor-changes” for syslog analysis
- ◆ Troubleshooting Stuck-In-Active Routes
 - *Find the Active and the Stuck parts*
 - *Cause of active often easier to find, but the cause of stuck more important to find*
 - *Look for neighbors that have the “reply status flag (r)” set – keeps track of outstanding queries*
 - *“show ip eigrp topology active”*

Troubleshooting OSPF

- ◆ **Neighbor adjacencies**
 - *Understand state table for protocol*
 - *Hello/Dead timers must be equal on neighbors*
 - *Router authentication must match*
 - *Know which router is the DR/BDR*
 - *Use “ospf log-adjacency-changes” for syslog analysis*
- ◆ **OSPF metrics use 10^8 /Interface-bandwidth**
 - *Turn off “auto-cost-determination” and enter manually*
 - *Change “auto-cost reference-bandwidth”*
- ◆ **Use explicit mask on network statements**
- ◆ **Check redistribution with classful protocols**
 - *Summarization and discontinuous networks*
 - *External Type 1 versus External Type 2*
- ◆ **View routing table and OSPF database**
 - *What routes made it into forwarding table?*

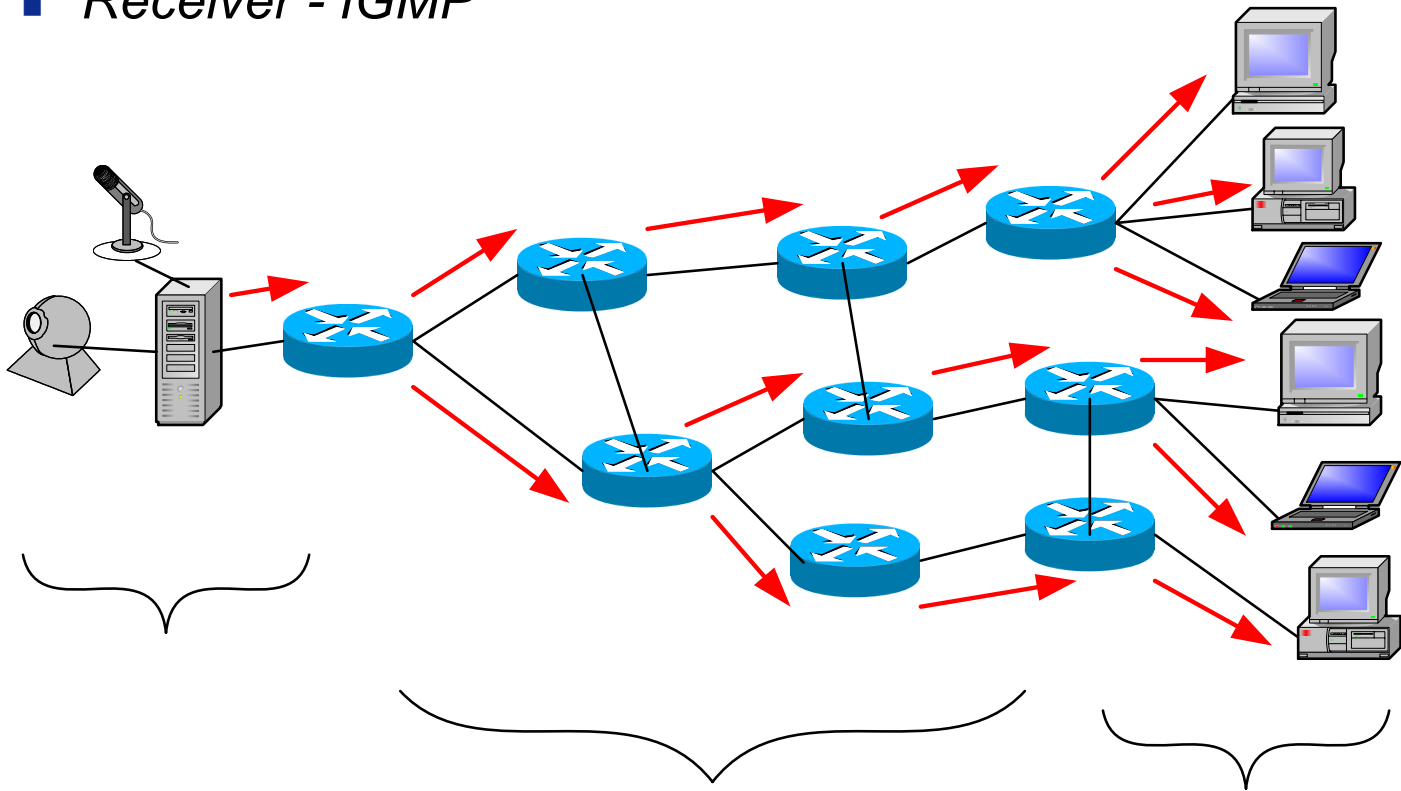
Troubleshooting BGP-4

- ◆ **BGP peering takes place on TCP port 179**
- ◆ **A stable IGP is required for a stable BGP network**
- ◆ **Neighbors should be in “Established” state**
 - *Reset peer – soft reconfiguration*
 - *BGP – exchanges just hello’s after initial peering*
- ◆ **Synchronization with IGP**
 - *Transit AS - use synchronization*
- ◆ **Check BGP table & decision algorithm**
 - *View routes in BGP table to see which ones make it into forwarding table*
 - *Know BGP’s attributes – well-known, mandatory, optional, transitive, non-transitive*
- ◆ **Route flap dampening**
 - *If you are dampened then you need to reset the peers*
 - *See if the table version number is incrementing rapidly as an indication of flapping*

Multicast Troubleshooting

◆ Troubleshoot IP Multicast in sections

- *Source Segment*
- *Rendezvous Point (PIM-SM)*
- *Receiver - IGMP*



PIM-SM Troubleshooting

- ◆ **Make sure all routers agree on the RP**
- ◆ **Set Shortest Path Tree (SPT) threshold to infinity to prevent SPT switchover**
- ◆ **Start from receiver and move toward source**
- ◆ **Check receiver's LAN and IGMP**
- ◆ **Check PIM DR and start moving toward RP via (*,G) following RPF**
- ◆ **Make sure the RP knows about the source**
- ◆ **Check all PIM routers along (S,G)**
- ◆ **Check source's LAN and IGMP**

Multicast Troubleshooting

- ◆ If receiver to source unsuccessful, troubleshoot from source to receiver
- ◆ Test with receiver on same segment as source – use hub/switch - test only the application
- ◆ Check source streaming format compatibility with receiver software
- ◆ Create low-speed streams
- ◆ Log into many routers and view multicast routing tables and PIM-SM states
- ◆ Enable IGMP snooping and enable mroute-caching to reduce CPU load on network elements
- ◆ Watch out for redundant links – can confuse RPF

Mcast Troubleshooting Tools

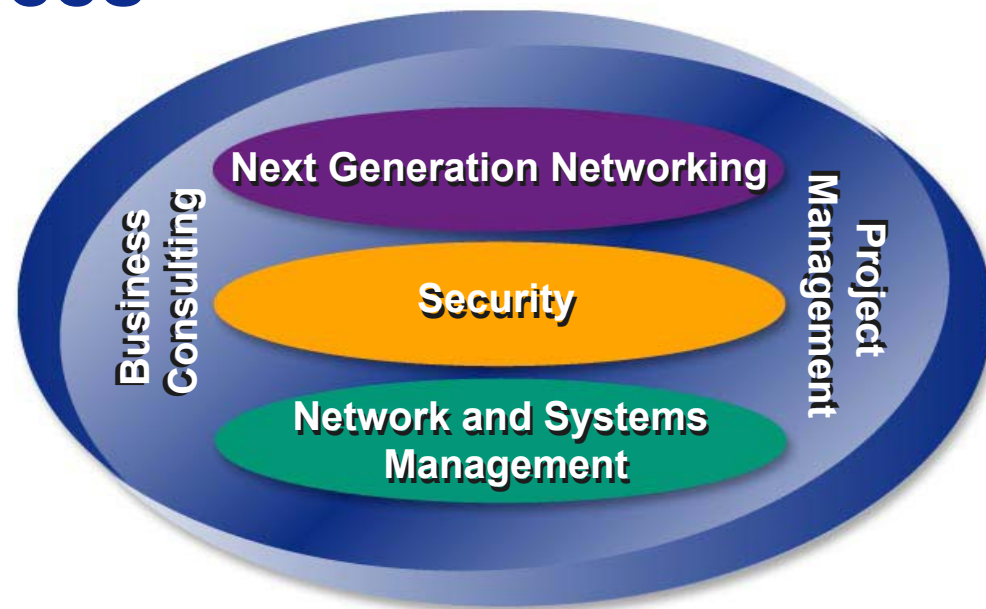
- ◆ “mrinto [hostname | address] [source-address | interface]”
- ◆ “mtrace source [destination] [group]”
- ◆ “mstat source [destination] [group]”
- ◆ **Multicast Routing Monitor (MRM)**
 - *Sends UDP/RTP test stream to 224.0.1.111*
 - *Set up a sender, a receiver, and a manager*
- ◆ **RTP and RTCP tools**
 - *RTPMon, rtping, rrtcp, and rqm*

The Bottom Line

- ◆ *Use a good methodology*
- ◆ *Document your baseline, actions, and results*
- ◆ *Leverage all tools to gather information*
- ◆ *Troubleshoot in both directions*
- ◆ *Use a protocol analyzer to help troubleshoot difficult problems*
- ◆ *Understand the protocols you are troubleshooting*

INS Network Infrastructure Consulting Services

- ◆ **Network Baseline Assessment**
- ◆ **Network Architecture Design**
- ◆ **Network Implementation**



Question and Answer

- ◆ Tell us what you think about this webinar

<http://www.ins.com/knowledge/surveys/feedback.asp>

- ◆ Upcoming webinars

- *Avoiding Network Outsourcing Pitfalls, A Roadmap for Enterprises and Service Providers*

- ◆ For more information

- *Call 1-888-767-2988 in the U.S., 44 (0) 1628 503000 in Europe, or 1-408-330-2700 worldwide*



Internet Resources

- ◆ **Cisco Technical Assistance Center (TAC) Troubleshooting Web Page** (accessible to Cisco clients)
 - <http://www.cisco.com/kobayashi/support/tac/troubleshoot.shtml>
- ◆ **Cisco-centric Open Source Initiative (COSI)**
 - <http://cosi-nms.sourceforge.net>
- ◆ **Cisco Switching Best Practices** (accessible to Cisco clients)
 - <http://www.cisco.com/warp/customer/473/103.html>
- ◆ **Cisco Troubleshooting Assistant** (accessible to Cisco clients)
 - http://www.cisco.com/kobayashi/support/tac/tsa/launch_tsa.html
- ◆ **Cisco Multicast Information**
 - <ftp://ftpeng.cisco.com/ipmulticast.html>
- ◆ **Cisco Google Group**
 - <http://groups.google.com/groups?group=comp.dcom.sys.cisco>
- ◆ **General Network Troubleshooting We site**
 - <http://www.networktroubleshooting.com/>

Network Troubleshooting Books

- ◆ **Network Troubleshooting Tools (O'Reilly System Administration) by Joseph D. Sloan** Publisher: O'Reilly & Associates; ISBN: 059600186X; (August 2001)
- ◆ **Network Analysis and Troubleshooting by J. Scott Haugdahl** Publisher: Addison-Wesley Pub Co; ISBN: 0201433192; 1st edition (January 15, 2000)
- ◆ **Troubleshooting IP Routing Protocols (CCIE Professional Development Series) by Faraz Shamim, Zaheer Aziz, Johnson Lui, Abe Martey** Publisher: Cisco Press; ISBN: 1587050196; 1st edition (May 7, 2002)
- ◆ **Cisco Internetwork Troubleshooting (The Cisco Press Certification and Training Series) by Laura Chappell (Editor), Dan Farkas, Thomas M. Kelly, Daniel Farkas (Editor)** Publisher: Cisco Press; ISBN: 1578700922; 1st edition (July 12, 1999)
- ◆ **Internetworking Troubleshooting Handbook (2nd Edition) by Cisco Systems Inc.** Publisher: Cisco Press; ISBN: 1587050056; 2nd edition (February 15, 2001)
- ◆ **Network Maintenance and Troubleshooting Guide by Neal Allen** Publisher: Cisco Press; ISBN: 158713800X; 1st edition (November 1, 2000)
- ◆ **Troubleshooting Campus Networks: Practical Analysis of Cisco and LAN Protocols by Priscilla Oppenheimer, Joseph Bardwell** Publisher: John Wiley & Sons; ISBN: 0471210137; 1 edition (July 19, 2002)
- ◆ **Cisco Router Troubleshooting Handbook by Peter Rybaczyk** Publisher: John Wiley & Sons; ISBN: 0764546473; (March 2000)
- ◆ **Troubleshooting TCP/IP by Mark A. Miller** Publisher: John Wiley & Sons; ISBN: 0764570129; Third Edition edition (July 1999)
- ◆ **Troubleshooting Internetworks: Tools, Techniques, and Protocols by Mark A. Miller** Publisher: Hungry Minds, Inc; ASIN: 1558512365; (December 1991)
- ◆ **Cisco Router Configuration and Troubleshooting (2nd Edition) by Mark Tripod** Publisher: New Riders Publishing; ISBN: 0735709998; 2nd edition (January 15, 2000)
- ◆ **Novell's Guide to Troubleshooting Tcp/Ip by Silvia Hagen, Stephanie Lewis** Publisher: John Wiley & Sons; ISBN: 0764545620; (September 1999)

Network Troubleshooting Books

- ◆ **Sams Teach Yourself Network Troubleshooting in 24 Hours by Janathan Feldman, Jonathan Feldman Publisher: Sams; ISBN: 0672314886; 1st edition (December 16, 1998)**
- ◆ **Troubleshooting, Maintaining & Repairing Networks by Stephen J. Bigelow Publisher: Osborne McGraw-Hill; ISBN: 0072222573; 1st edition (August 23, 2002)**
- ◆ **Troubleshooting Local Area Networks by Othmar Kyas, Thomas Heim Publisher: International Thomson Publishing; ISBN: 1850321221; (March 1996)**
- ◆ **Network Troubleshooting by Othmar Kyas Publisher: Agilent Technologies; ISBN: 0970333110; (April 2001)**
- ◆ **Network Optimization & Troubleshooting by Daniel J. Nassar Publisher: Prentice Hall Computer Pub; ISBN: 1562053078; 1st edition (January 15, 1994)**
- ◆ **Network Monitoring and Analysis: A Protocol Approach to Troubleshooting by Ed Wilson, James Naramore Publisher: Prentice Hall PTR; ISBN: 0130264954; 1st edition (February 15, 2000)**
- ◆ **Guide to Network Support and Troubleshooting by Greg Tomsho Publisher: Course Technology; ISBN: 061903551X; Bk&Cd-Rom edition (January 30, 2002)**
- ◆ **Ethernet Tips & Techniques: For Designing, Installing and Troubleshooting Your Ethernet Network by Byron Spinney Publisher: CMB Books; ASIN: 1878956434; 2nd edition (March 1995)**
- ◆ **Cisco Internetworking and Troubleshooting by Cormac S. Long Publisher: McGraw-Hill Professional Publishing; ISBN: 0071355987; (November 24, 1999)**
- ◆ **The Network Troubleshooting Handbook by Ed Taylor Publisher: McGraw-Hill; ASIN: 0071342281; 1st edition (January 25, 1999)**
- ◆ **Multiprotocol Network Design and Troubleshooting by Chris Brenton Publisher: Sybex; ASIN: 0782120822; 1st edition (January 15, 1997)**
- ◆ **Cisco Router Troubleshooting: A Solutions Handbook by Frank Fiore Publisher: Macmillan Technical Publishing; ASIN: 1578701090**

Glossary

- ◆ **ACL – Access Control List**
- ◆ **ARP – Address Resolution Protocol**
- ◆ **BGP-4 – Border Gateway Protocol Version 4**
- ◆ **CDP – Cisco Discovery Protocol**
- ◆ **DHCP – Dynamic Host Configuration Protocol**
- ◆ **DNS – Domain Name Service**
- ◆ **IGMP – Internet Group Multicast Protocol**
- ◆ **RIP – Routing Information Protocol**
- ◆ **OSPF – Open Shortest Path First**
- ◆ **MRM – Multicast Route Monitor**
- ◆ **MTTR – Mean Time To Repair**
- ◆ **PIM-SM – Protocol Independent Multicast – Sparse Mode**
- ◆ **RPF – Reverse Path Forwarding**
- ◆ **RTCP – Real-Time Transport Control Protocol**
- ◆ **RTP – Real-Time Transport Protocol**
- ◆ **TTL – Time To Live**