Fault tolerance paper essay

Business, Management

Fault Tolerance PaperNetwork Fault ToleranceFault Tolerant provides high levels of availability and reliability in network connections. Used with redundant network interface hardware, Fault Tolerant allows the user to maintain persistent sessions during a hardware failure or a routing outage or change.

Redundant network interface hardware is required to use this feature. It has been estimated that more than 80% of network downtime is spent looking for network problems, while less than 20% is spent actually fixing them. The need for accurate, timely root cause analysis and event correlation is therefore paramount. Although many vendors and products have attempted root cause analysis, very few actually deliver this capability. Some employ mathematical or systems models formed in the academy. Others are based on simple event filtering schemes.

All networks demand 24×7 reliability. In a work environment where one minute of downtime can mean tens of thousands of dollars in lost sales and productivity, you can’t afford to have a network failure. Although network topologies like FDDI and ATM offer fault-tolerant network connections, most networks are built on Ethernet and Fast Ethernet backbones, which do not. Fortunately, vendors are responding with innovative ways to add fault tolerance to these networks. The basic component in fault Tolerance is SNMP: The Simple Network Management Protocol (SNMP) allows you to manage a node running the SNMP Master agent. The SNMP supports the following features: MIB II and its SNMP derivatives (as specified in RFC 1213 and RFC

1215), including: Statistics countersIP and SNMP managementInterface managementInterface configurationMIB II SNMP version 1 traps or version 2 notificationsAdditional Management of Proprietary MIB itemsThe SNMP implementation fully supports GET and SET requests.

The SNMP implementation listens on port 161 for SNMP requests and on port 162 for SNMP traps. These are the ports recommended by RFC 1906. Master Agent and Sub-Agent ArchitectureSNMP support is provided by a run-time extensible SNMP agent. The extensible SNMP agent is partitioned into a master agent and multiple sub-agents. This allows: Users to be able to assign new Athena protocol binaries containing additional sub-agents without re-releasing the master agent or any other Athena/Access binary. SNMP support for protocol feature additions are accomplished by updating the protocol sub-agent without re-releasing the master agent. Users can dynamically add/delete protocol tasks at run-time.

The SNMP family of agents (master agent and sub-agents) are transparent to the Network Management Station. SNMP Community and Trap SupportThe following items are configurable: SNMP Community Table (read-create)Entry NumberCommunity Name (Configure a Community Name for each entry)Access Level (read-write) (Allow or dis-allow SNMP operations to modify configuration for the specified community)SNMP Community Address Table (read-create)Community Entry NumberAddress Entry Number (Configure up to two entries for the above specified Community)IP Address (Configure an IP address for this entry in the above specified Community)Trap Level (0-7) (A severity level filter for the above specified entry number). Trap Format (SNMPv1 Trap or SNMPv2 Notification)Trap Status (enable/disable Traps)Detailed Capability Description: SNMP supports the following capabilities: 1. MIB II2. Base Configuration (NMP)3. IP Public Mib Capabilities (as per MIB II)4.

IP Proprietary MIB5. Ethernet6. Frame Relay7. WAN RoutingSNMP Operations: SNMP itself is a simple request/response protocol. NMSs can send multiple requests without receiving a response.

Six SNMP operations are defined: Get — Allows the NMS to retrieve an object instance from the agent. GetNext — Allows the NMS to retrieve the next object instance from a table or list within an agent. In SNMPv1, when an NMS wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations. GetBulk — New for SNMPv2. The GetBulk operation was added to make it easier to acquire large amounts of related information without initiating repeated get-next operations. GetBulk was designed to virtually eliminate the need for GetNext operations. Set — Allows the NMS to set values for object instances within an agent.

Trap — Used by the agent to asynchronously Inform the NMS of some event. TheSNMPv2 trap message is designed to replace the SNMPv1 trap message. Inform — New for SNMPv2. The Inform operation was added to allow one NMS to send trap information to another. Components of Fault Tolerance:· Network Discovery· SNMP Devices Discovery· SNMP Devices Identification and viewing SNMP device properties· Polling functionality for gathering statistical data from any SNMP or RMON enabled device and store in a database.· Graphical representation of the data gathers from the polling module.· Retrieving data from the database for trend analysis.

· Trap receiver for receiving messages generated by the agent.· Trap log which will show the trap history. Key Vendors: 1. Cisco: Advantages: Multiplexing, the intelligent use of multiple controllers to handle hardware failures. Gateway Dæmon (GateD), supporting Open Shortest Path First (OSPF) and Routing Information Protocol (RIP) to handle router failures or routing changes. Multiplexing: Cisco IOS for S/390 actively samples network activity to detect network outages. This can happen when a channel error occurs or a network defect is discovered (in other words, bad cable or defective hub).

The Address Resolution Protocol (ARP) is used to dynamically map Internet (IP) and MAC (hardware) addresses. In addition, the SNMP agent of Cisco IOS for S/390 will send an “ interface down” trap to a network management station when either of the above conditions are met, Configuration for information on configuring the SNMP agent. GateD: Cisco IOS for S/390 uses the gateway dæmon (GateD) application to implement open systems interior and exterior routing protocols within the local network. With the use of GateD, Cisco IOS for S/390 functions as a router on the network and quickly detects changes in the routing environment and dynamically acts upon the information quickly enough to keep sessions from being interrupted or delayed.

This section describes what routing protocols are and provides information about the two routing protocols supported by GateD, OSPF and RIP. Limitations:· Cisco IOS for S/390 GateD/OSPF does not support multicast. NSC HYPERchannel interfaces only recognize hardware outages. A network outage may go unreported due to the Internet Protocol (IP) router built in to these network controllers. Accurate network outage determination is possible with link level controllers supporting CETI and 3172 protocols.

2. The EventWatch ModelImplementing an automated solution for fault management involves more than simply ensuring that network events get quickly processed and accurately correlated to their root causes. It also requires an adequate response to the events: the appropriate personnel must be notified, and records must be kept. EventWatch accomplishes this using a three-phase process that consists of: 1) Verification, 2) Correlation, 3) Notification.

In the verification phase, EventWatch eliminates transient network failures and authenticates that the reported down condition is genuine. In the correlation phase, EventWatch locates the root cause of the reported failure. During the notification phase, EventWatch notifies the appropriate support personnel that a particular device or interface has failed. References: 1. www. cisco. com2.

http://www. rlx.
com/downloads/pdf/softwareguides/windows/RLXWinSNMPTG.
pdf3. http://www.

develcon. com/Products/SNMP/SNMP. htm4. http://www. dpstele.
com/offer/snmp_implementation_guide. php5.