WINDOWS BASED EMBEDDED SYSTEMS

Abstract:

There are many computing systems where are failure (either malicious or arbitrary) of a device which is completely unacceptable. These networks will face security threads and suffer traditional hardware failure. Even though the dedicated efforts of hardware & software engineers have enable computing devices to become more are less reliable appliances.

As a substitution for these networks, embedded systems devices often perform critical functions and they need a method to accomplish functional survivability of essential computations in a hostel or volatile environment.

As the cost of both networking & producing powerful embedded devices drops, collections of these highly specialized and heterogeneous platforms will proliferate. The applications of embedded are very vast. The windows based embedded basically deals with the part of the transformation of the information from one part of the computer to another part in the computer software either though hardware or software. These windows based embedded also tells the various types of redundancy that can take place in the process of information exchange and also their brief view.

In this paper we are going to discuss about the details regarding the applications of embedded systems in the windows embedded.

Introduction:

An embedded system is one that has computer hardware with software embedded it as one of its most important component. It has three main components viz : hardware, main application software, real time operating systems(RTOS). Also, these have less power dissipation and consumption, tolerate extreme heat, high computing speed, and their need less space requirements than ordinary computer hardware. The approach identifies "*management of both design complexity & system heterogeneity as the key problem*".

An embedded real-time system possesses the characteristics of both an embedded system & a real-time system. A real-time system is one that must perform operations with in rigid timing constraints. Real time systems are further sub divided into hard real-time & soft real time. Hard real time means that a failure will of great consequences. An example of this is a real time system controlling a nuclear reactor. A soft real-time system must act with in timing constraints for its operation to be correct, although a timing failure in this kind of system is more of an annoyance. An example of this kind of is a bank's is a automate teller machine.

The real-time nature of the system depends on a clock interrupt, and consequently this interrupt has highest priority. Multiple tasks are used to acquire the data, process the data & write it to the display, & store the data. The first task is the highest priority; we must acquire data on the regular interval as closely as possible for an accurate usage profile. Processing of data & writing it to the display is of secondary importance. Storing the data is of the lowest priority because the data is queued until written.

ABOUT WINDOWS EMBEDDED:

The windows embedded division is delivering technology, end-to-end tools, and resources to build smarter, more useful, and productive 32-bit embedded devices. Windows embedded enables you to provide highly customized device designs on a flexible platform with easy-to-use development tools. Microsoft operating system technology has been deployed in the broadest and most demanding environments, and is at the forefront of providing the most solid foundation for the next generation of 32-bit devices

WINDOWS EMBEDDED OVERVIEW:

1. Enables powerful, scalable platforms for 32-bit connected devices that include advanced applications and services.

2. Accelerates device, take advantages of familiar programming model and a powerful set of development tools.

3. Provides with a broad, knowledgeable partner base and comprehensive technical resources

The process of transmission of data in the windows embedded is as follows

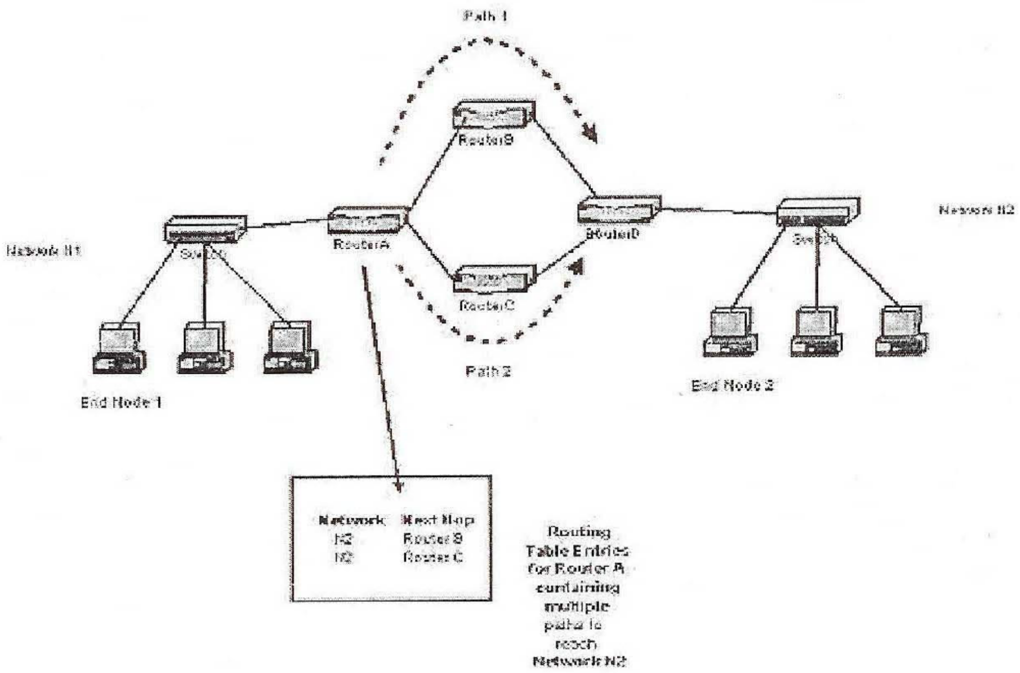
LOAD BALANCING:

Below we are going to take a detailed look at end-node and network redundancy. But, before doing that, let's look at the impact of load balancing.

A key consideration with redundancy is whether the alternate or redundant element (component, link or path) is used during normal operation. Consider a link-level redundancy scenario with two links –link 1 and link 2 – connecting two switches. During normal operation, packets may be sent only over link 1 while link 2 is in standby mode, waiting to take over if link 1 fails. This is an inefficient utilization of network resources since link 2 is idle during normal operations that are only 50% of link resources are being used.

An alternative is to use both link 1 & link 2 during normal operation so that one of the links takes over if the other fails. Also called the load-balancing approach, this scheme has two advantages: the capacity of connection between the two nodes has been doubled, since both links can be used for traffic between the nodes. The second advantage is that there is no designated primary or backup for redundancy, so the design is simpler.

With node-level redundancy, it is possible to use load balancing by sending the traffic to a different next hop so that it follows an alternate path to a destination. Consider figure 1 where the destination can be reached via two paths from router A. one is through router B and the other through router C.



Network	Next Hop
N2	Router B
N2	Router C

Figure 1: Network with multiple paths between routes.

In figure 1, paths to end node 2 through both routers B & C exists in router A's forwarding table. one approach to load balancing: a packet can be sent to router A if the IP addresses is odd and through router B if the address is even.

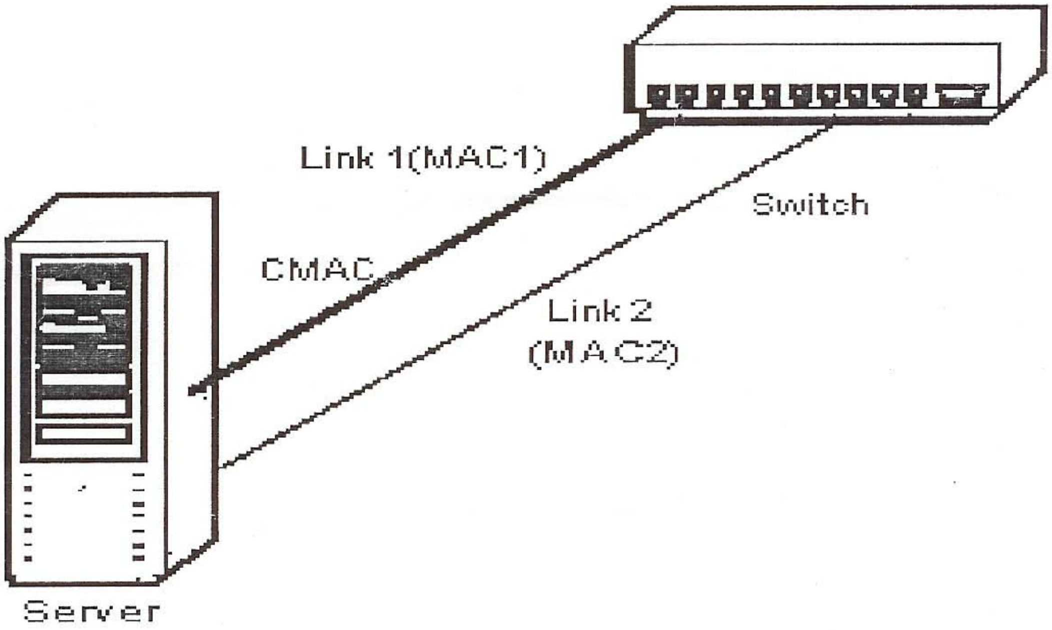
REDUNDANCY:

It means the various types of checking process that are going to be done in the process of manage transformation. The various types of redundancies applied in the networks are

END NODE REDUNDANCY:

Figure 2 shows an end-node attached via two separate links to the same switch. If one of the links or switch port fails, the data can be sent over the other port. To ensure that happens seamlessly, the most common technique is for the higher-layer software to be completely unaware of load balancing and switch over

In figure 2, assume that the redundancy is implemented without load balancing. Link 1 is the active link while link 2 is the standby link. Also assume that the media access control (MCA) addresses of the end node on these links are MAC1 and MCA2. Additionally, assume that the node has a "common" link MAC ress for all transmissions from the end node to other nodes. This MAC address (CMAC) will be used as a source MAC address for Ethernet frames originated by this end node designated other end nodes. Thus, this only MAC address known to the switches connected to the end node, as well as the operating system and the higher layer software.



The advantage of the above approach is that if one of the links fails, the network never leads to learn a new MAC address. The active link or preferred link transfers the packets while the backup link is in the hot standby mode.

Periodically the end node transmits keep- alive MAC frames on link 1 with source address as a MAC 1 and destination MAC address as MAC 2 then end node receives keep alive frame for link 2(forwarded by the switch) it knows that link 1 active (as is the connected port on the switch) and continues to keep link 2 in standby mode. If it does not receive a specified number of keep alive with in a certain period the end node causes link 2 to transition 2 active made at this time it sends a frame with source MAC as CMAC. So that the switch changes its address mapping table entry to indicate that CMAC is reachable via link 2.

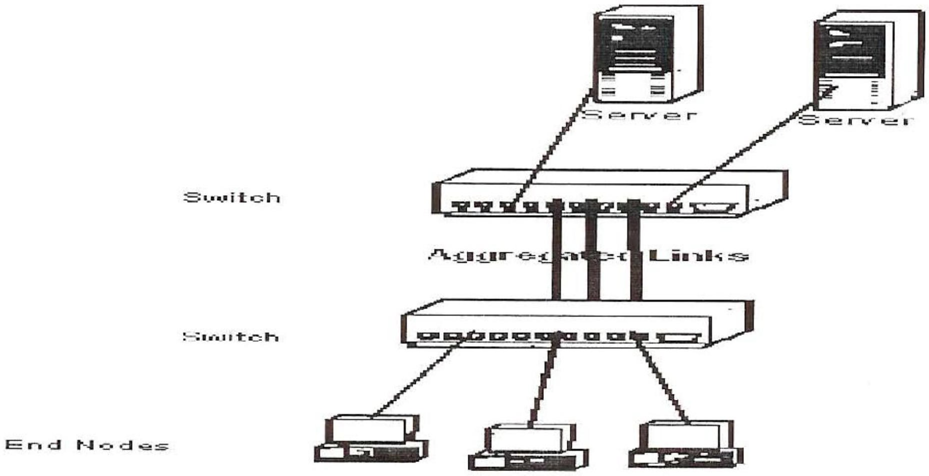
When the end node is connected to two separate switches, traffic in the switched back up link to the second switch, if either the link port, link or switch port fails the two switches are connected to each other so if the frames start arriving on port 2 of switch B, switch A will also learn of this connectivity via switch B, so traffic can continue without disruption. Note that load balancing is not possible/links are attached to separate switches.

NETWORK REDUNDANCY:

When considering network redundancy, we can evaluate redundancy from both a layer 2(Ethernet) and layer3 (IP routing and forwarding)perspective. The following sections discuss the various schemes used to implement layer2&layer3 network redundancy.

LINK AGGREGATION :

If load balancing is used in conjunction with link-level redundancy, it is typically via link aggregation (LA). Figure3 shows three links that appear as a single link to the switch so that the name Mac address can be used across all three links. A link aggregation processes on the end node and the switch provide the control signaling and packet ordering for the links so that the applications are unaware of the link aggregation if one of the link fails the other continuous to operate so that the aggregate link appears as a lower speed link now.



SWITCH AND LINK REDUNDANCY:

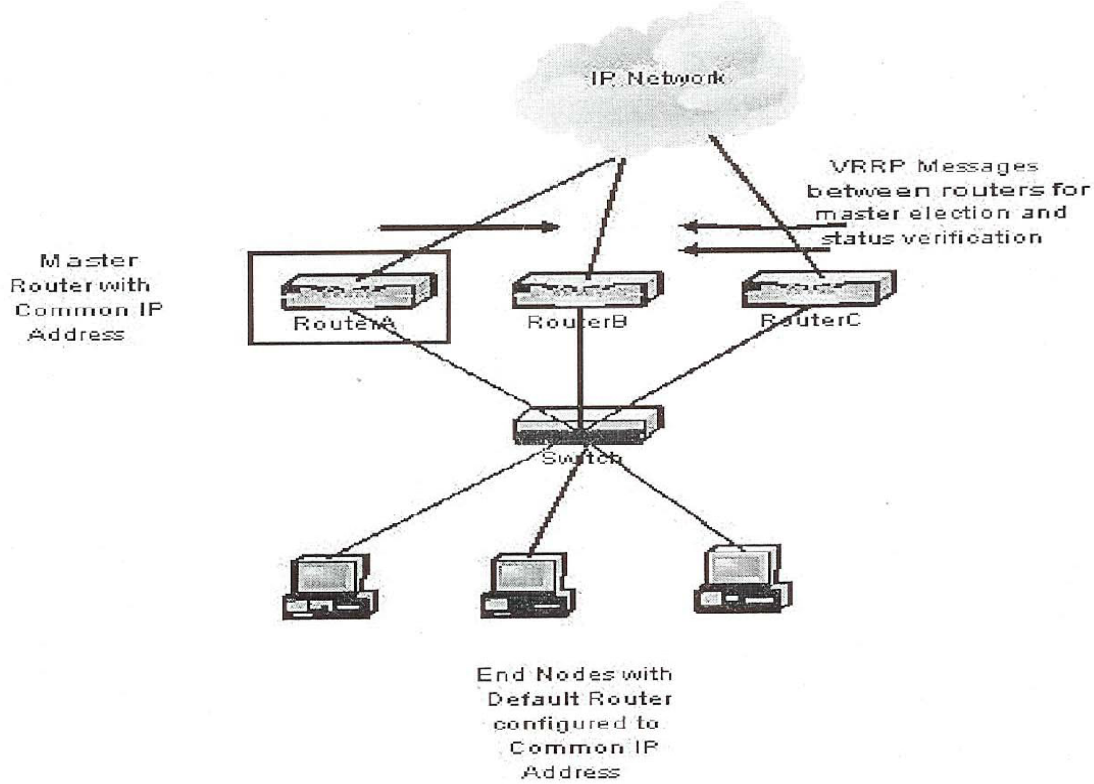
The most common scheme for network-level redundancy in Ethernet switches is by using multiple switches and/or multiple links between switches. When multiple switches operate in parallel, one switch can take over when the primary fails. However, due to the nature of MAC based learning and forwarding, this can cause bops. Thus, we need to disable one of the switches during "normal "operation and let it take over when the active switch fails.

VRRP:

End nodes are frequently configured with a default router, which they always use to communicate with nodes on other networks. This default router information can be provided via DHCP or static configuration. When end nodes need to communicate with end nodes outside their own network, they send the packets to the default router, which in turn forwards the packets towards the final destination.

The virtual router redundancy protocol (VRRP) helps nodes recovers from outage of default router in the transparent manner. VRRP specifies an election protocol that dynamically assigns the default router responsibility to a specific router(the master) among a group of routers. If the default router fails, one of the other routers in the group takes over with the same default router IP address/ MAC address so that end nodes see no disruption (figure4).

The common MAC address used by all the routers in the VRRP group is known as a virtual MAC address .since, the end nodes have the same IP address and(virtual) MAC address mapping, they will not notice that a back up has taken over from the master. VRRP can also provide load balancing functions, for example same router that acts as a back up for one group of nodes can be the master for another group.


IP Network
VRRP Messages between routers for master election and status verification
Master Router with Common IP Address
RouterA
RouterB
RouterC
Switch
End Nodes with Default Router configured to Common IP Address

ROUTER MULTIPATH:

Redundancy and resiliency are built into a Layer 3 network topology via the routing protocols. A protocol like RIP or OSPF recovers from a failure in network (a node or link going down) via a recalculation of routes to destinations that were previously reachable through the failed node or link. When the new routing tables are built up after this recalculation, forwarding of traffic can take place. Thus, packets will resume their flow between source and destination after this recovery.

To avoid disruption of forwarding while the recalculation is taking place, the layer 3 switches (i.e. router) can use an alternate forwarding path as shown in figure 1. This is the route through router C which shows up as an alternate route. The calculation would have been performed earlier by routing protocol and the information maintained in the routing table as alternate route. Most routing protocols do not permit to use of this alternate route during normal operation. An exception is OSPF, which permits equal cost multi path (ECMP) routing; for example forwarding of packets over multiple paths to the same destination as long as the paths have same costs.

WRAP UP:

Table 1 summarizes the various types of redundancy along with their key features.

No.	Redundancy type	Key Features	Load Balancing Considerations
1.	End node redundancy	Multiple adapters on host connecting to separate ports on the same switch or multiple switches.	May implement with higher layer awareness.
2.	Layer 2 network redundancy-link aggregation .	Implemented between network nodes aggregated links appear as a single link. Failure of any component link is not known to the application it only appears as a slower aggregated links.	Inherent path of implementation.
3.	Layer 2 network redundancy spanning tree protocol and multiple spanning tree protocol.	Implemented to avoid loops in the presence of redundant links/switches.	MSTP can ensure load balancing by providing
4.	Layer 3 network redundancy-VRRP.	Implemented between default routers on a LAN end nodes are not aware of the change to anew default router of since the IP and MAC address of the default router remains unchanged.	Can use different default routers for different sets of routers.
5.	Layer 3 network redundancy-router multipath.	Packets can take multiple path to destination based on intermediate router forwarding each router	Backup routes can be used for forwarding if they have the same cost as in ECMP.

		maintains more than one route to a destination so that packets can follow A backup route if primary route fails.	

This article focused on implementing redundancy in networks. End node redundancy is typically implemented on servers while link level and equipment level redundancy is used to build resilient networks. Backup networks nodes (e.g. in VRRP environments) and alternate paths(e.g. in RSTP,MSTP and OSPF environments) are some of the building blocks used to build redundancy in networks. Network operators can use the methods described here to ensure reliable end.

Applications: it has a very vast application in almost all fields.

- SATELLITE COMMUNICATION
- BIO-MEDICAL
- ARTIFICIAL INTELLIGENCE
- SCIENTIFIC RESEARCH
- DEVELOPMENT OF ROBOTS

References:

1. EMBEDDED SYSTEMS by RAJ KAMAL
2. IEEE by MAGAZINES
3. DIGIT MAGAZINE