Journal of Telecommunications System & Management

Graham, J Telecommun Syst Manage 2015, 4:1
DOI: 10.4172/2167-0919.1000120

Research Article Open Access

Applying High Availability Design and Parallel Redundancy Protocol (PRP) in Safety Critical Wide Area Networks

Mark Graham*

Harris Corporation, Government Communications Systems Division, Mission Critical Networks, 1025 West NASA Boulevard, Melbourne, Florida 32919, USA

Abstract

Networks which protect the safety of human lives place special emphasis on network availability and survivability. The nation's Air Traffic Control (ATC) and First Responder public safety networks used by police departments, fire and rescue, and emergency medical teams are examples of networks that require high availability and survivability. The term mission critical network is often used to describe the characteristics of networks which protect the safety of human lives. There is not a universally accepted standard definition of the term, but much literature on the subject typically identifies three salient characteristics:

- Highly Secure
- Highly Available
- Highly Survivable

Highly secure is an important characteristic and needed to design a safety critical network, but the focus of this paper is availability and survivability. It should be noted that mission critical safety networks are private networks and should not be confused with the public Internet simply because they use IP. A private network in itself does not constitute a mission critical network, but it is a significant characteristic of a mission critical network due to the security and performance benefits it supports. The security benefit is risk mitigation from external threats because only authorized internal users can access the network. The performance benefit is similar in that only authorized users have access to the network and their network usage does not have to compete for bandwidth with other external users.

Availability and Survivability are related, but they are not the same thing. Availability is simply a measure of the time the network is operating compared to the total time it should be operating. Availability is defined as Uptime divided by Uptime plus Downtime. This same reference defines Survivability as the capability of a system (or network in this case) to perform its mission recognizing that failures are going to occur. As will be explained later in this paper, survivability considers catastrophic events that cannot be easily predicted in an inherent availability model.

Specifically, this paper focuses on the availability and survivability of the Wide Area Network (WAN) terrestrial core backbone component of safety critical networks. Much literature on public safety networks for First Responders is devoted to the wireless radio networks including Land Mobile Radio (LMR), P.25 packet radio, cellular telephony and evolution towards broadband 4G Long Term Evolution (LTE) wireless networks. Air Traffic Control networks rely on other wireless forms of communication including narrow-band Air-to- Ground (aircraft to ground based controller) voice and data links in the Very High Frequency (VHF) spectrum. All of these wireless forms of communication rely on a terrestrial core backbone for backhauling and distributing information to the right place. The terrestrial core backbone is a foundational building block for other safety critical network components.

This paper also describes some of the differences between legacy Time Division Multiplexing (TDM) technology and modern Internet Protocol (IP) packet switched technology. Historically, networks such as the nation's Air Traffic Control (ATC) network have relied on point-to-point TDM technology.

Keywords: Availability; Survivability; Wide Area Network (WAN); Parallel Redundancy Protocol (PRP); Time Division Multiplexing (TDM); Dual core architecture

Introduction

Mission critical networks that provide voice, video and data communication services for safety critical applications require special consideration to ensure they are highly available and survivable. Most network systems and services desire a highly available network design because of the economic impact associated with lost revenue opportunity and the cost of doing business. Safety critical networks need to place special emphasis on availability and survivability of the network because not only is there an economic impact when the network fails, but there is also the risk of safety impact which could potentially affect human lives.

Modern networks use routing and switching architectures to improve flexibility and efficiency. Flexibility is improved through the ability to dynamically route network traffic over multiple paths to avoid failures and improve network throughput performance. These routed and switched networks are more adaptable and affordable compared to traditional TDM networks because they are built over a shared routing infrastructure. A shared routing infrastructure uses packet switching and statistical multiplexing to "share" network resources for all traffic. In contrast, a TDM network infrastructure separates network traffic into separate timeslots and dedicates the timeslots to specific users and traffic. The downside of a TDM implementation is

***Corresponding author:** Mark Graham, Harris Corporation, Government Communications Systems Division, Mission Critical Networks, 1025 West NASA Boulevard, Melbourne, Florida 32919, USA, Tel: 1-321-727-9100; E-mail: Mark.Graham@harris.com

Received February 04, 2015; **Accepted** July 27, 2015; **Published** July 29, 2015

Citation: Graham M (2015) Applying High Availability Design and Parallel Redundancy Protocol (PRP) in Safety Critical Wide Area Networks. J Telecommun Syst Manage 4: 120. doi:10.4172/2167-0919.1000120

that the dedicated timeslots are unused and wasted when the specific user or traffic which the timeslot is assigned is idle. A modern routed network overcomes this shortcoming of TDM networks with statistical multiplexing, but the improvement creates new vulnerabilities that did not have to be considered in a TDM network. In a point-to-point TDM network, physical equipment redundancy and physical circuit diversity are enough to overcome most types of network failures. In a modern routed network, the routing function is a logical function that can also fail. Logical routing failures are not common, but even infrequent failures cannot be tolerated in mission critical networks where public safety is at risk. These uncommon failures are characterized as "six sigma" events because of their infrequent occurrence. An example of six sigma event is a logical routing protocol phenomenon known as a black hole where packets are dropped and data is lost even though no apparent or obvious failure event has occurred. Although these events are rare, the sinister nature of them makes them difficult to be detected and repaired. And unlike point-to-point TDM circuits which effect only sites and services at each end of a circuit when failures occur, a shared routing network infrastructure problem can be widespread effecting multiple sites, services and applications.

Network survivability goes beyond traditional availability modelling to address the challenge of overcoming these unpredictable six sigma events. Parallel Redundancy Protocol (PRP) was designed for mission critical environments where high survivability is required. Initially designed for dual core Local Area Networks (LAN), PRP has been enhanced for dual core WAN environments and is part of the solution needed for providing a highly survivable WAN for public safety. A dual core network is exactly what the term implies, two separate core networks. The separation can be physical, logical or both. High availability requires the two networks to be physically diverse from one another with physically separate equipment and physically separate circuit paths. High survivability requires them to be logically diverse with separate routing domains. Furthermore, logically separate means the two networks cannot be interconnected with a routing protocol such as Border Gateway Protocol (BGP) because of the potential for routing anomalies from one network affecting the other. Note that more than two networks can be used for even greater survivability and this capability is currently being evaluated in the Critical Network labs of Harris Corporation. The dual core WAN implementation has already been evaluated and deployed and is in operation today.

This paper focuses on availability and survivability considerations, describing how PRP works in conjunction with a dual core network and how it has been enhanced to provide the needed survivability for mission critical public safety networks.

Modern networks being used and deployed for these safety critical services are based on shared routing infrastructures using Internet Protocol (IP) technology. The flexibility and economies of scale afforded by IP technology cannot be ignored even though they present new challenges to address for safety critical networks.

Furthermore, almost all researches and development activities in industry are focused on the more flexible and cost effective IP technologies as many TDM technologies are becoming obsolete. Technology obsolescence is a serious telecommunications infrastructure concern that will have to be addressed in coming years [1-3].

High Availability Design

Availability modelling is a proven science which has been adapted for networks and telecommunications. It uses Reliability engineering to calculate Mean Time between Failures (MTBF) and Mean Time to Repair (MTTR) parameter values and proven mathematical formulas to predict the expected availability of a network service.

There are multiple aspects to consider when designing a high availability network. These aspects are:

- Physically diverse and redundant equipment strings
- Protection switching and routing
- Circuit and fibre path diversity and redundancy

Physically redundant and diverse equipment strings as well as circuit and fibre path redundancy rely on proven mathematical formulas for serial and parallel components for calculating the service availability between a core node in the network to any other core node in the network. The ITU [4] defines availability as follows:

"Availability of an item to be in a state to perform a required function at a given instant of time or at any instant of time within a given time interval, assuming that the external resources, if required, are provided [4]".

In our model we use the ITU definition and further define the "state to perform a required function" the ability to provide communication service between core nodes in the network. Bit errors, excessive latency, bandwidth congestion and other forms of degraded signal transmission are not considered in these calculations. These degraded forms of communications are handled by "higher level" functions. By higher level we mean protocols and/or applications which detect degraded signals and correct them through other means such as re-transmissions or Forward Error Correction (FEC). Examples of failures considered in the availability model are failures that cause a complete loss of communication service such as nodal equipment failure and/or a fiber cut. The term service outage is often used to describe this condition.

For illustration, we use the ITU definition and define the interval of time we want to measure as one day (24 hours).

Since the item we want to perform the required function is the network we define the ability of the network to communicate to be Network Uptime and Availability is calculated as:

Availability=Network Uptime / Network

Uptime + Network Downtime

In other words, if the network is designed to operate 24 hours a day but it is only communicating 23 hours in a given day then the network availability for that day is 95.83% (23/24).

Note that in practice availability is usually measured over longer intervals (monthly and annually) providing a larger population sample of data points to use in the Availability calculation. Service Level Agreements (SLA) where a network service provider contracts to meet a certain availability threshold are based on these longer intervals [5].

When designing a network, the actual network uptime is unknown so the Availability of specific components is predicted using Mean Time Between Failure (MTBF) and Mean Time to Restore (MTTR) metrics also defined by the ITU. MTBF and MTTR are Reliability parameters [1]. When using these metrics, Availability is predicted by the following formula:

This formula is used to predict the availability of network nodal equipment and power subsystems, but we also need the ability to predict failures in the transmission medium. Metrics for calculating the MTBF and MTTR for the transmission medium is shown in the IEEE journal5 on page 101 with references to other Telcordia standards6 (formerly known as Bellcore). The key metrics identified are an expected failure rate of 4.39 failures per year per 1,000 miles of sheath. The predicted restoral rate for each one of these failures is 12 hours.

Once the Availability of the specific components is known, the actual availability for a specific network design using redundant and parallel equipment and circuit paths (also shown in reference 1) can be calculated using the formula below.

$A_{parallel}$=1 – ((1-A1) * (1-A2) * … (1-An))

Since there is more than one piece of equipment in a string the availability of each of the parallel components is combined using the following formula for serial components (also shown in reference 1):

A_{string}=Aserial-1 * Aserial-2 * Aparallel-1 *…An

As shown, the formulas for parallel and serial components can be repeated “n times” or as much as necessary to account for strings and sub-strings of equipment.

Protection switching and routing is also very important because there is a need to be able to switch to a redundant path when one path fails. The protection switch itself can be a single point of failure if it is not designed properly. An example of a properly designed protection switch is the Cisco Optical Network Server (model 15454) which is a Synchronous Optical Network (SONET) Add-Drop Multiplexer (ADM). Other well-known manufacturers of SONET ADMs are Alcatel-Lucent and Fujitsu. SONET ADM’s are proven reliable protection switches and have a long and successful track record.

Uni-directional Path Switched Ring (UPSR) SONET technology is preferred for high availability design because of its simpler design, but Bi-directional Line Switched Ring (BLSR) technology can also be used if necessary. UPSR rings are implemented with two fibers in a ring configuration [6]. One fibre transmits in the clockwise direction and the other transmits in the counter-clockwise direction. Each node in the ring is initialized to receive the signal on the fibre transmitting in the clockwise direction and when a failure is detected it switches to the other fibre transmitting in the counter-clockwise direction. The two fibre paths are referred to a “working” which is the active path in use, and “protect” which is the redundant path ready to be used when a failure occurs on the working path. This feature is often described as “self-healing” because it can withstand a fibre cut.

BLSR rings can be implemented with two fiber or four fibre configurations. Unlike the simpler UPSR implementation, each fibre can be configured to transmit in either direction. BLSR ring configurations offer capacity benefits to service providers (relative to UPSR implementations) because they do not need the entire ring to transmit between two nodes on the ring.

Modern core network backbone topologies are designed with mesh backbones. The term stems from the idea that multiple paths exist from one core node to other core nodes in the network backbone forming a mesh. A full mesh core backbone is where every core node has a direct connection to every other core node in the network as shown below (Figure 1).

A partial mesh backbone is when every core node is not directly connected to every other node. The figure above would become a partial mesh backbone if one or more of the connections in the figure above were removed with the caveat that all nodes remain connected, just not necessarily with direct connections.

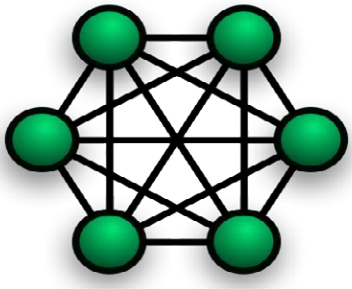


Figure 1: Full mesh core backbone.

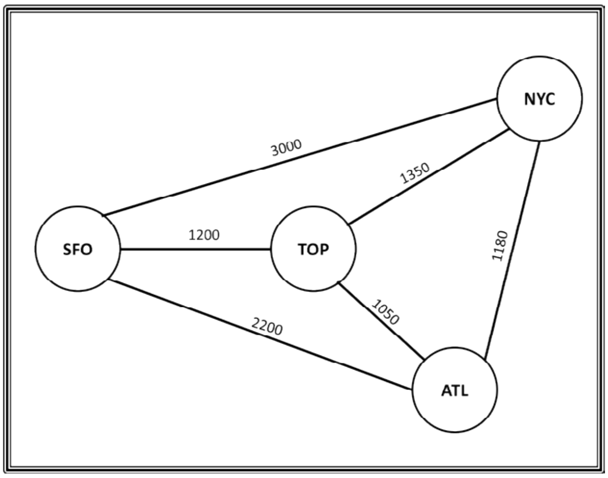


Figure 2: Simple fullmesh topology.

Mesh backbone technologies are also difficult to design to meet an availability objective. Over time methods and tools have been developed to solve this problem. In general, Telcordia standard metrics are used to estimate the expected number of failures on a circuit/fibre route. Fundamentally, the longer the route the lower the availability because of the higher probability that something will fail (e.g. equipment failure, fibre cut, etc.). The other problem is identifying the number of parallel and serial paths between any two end points in a mesh topology. For example, the simple full mesh topology shown below has five possible paths from every node to every other node (Figure 2).

The problem becomes much more complex in a large wide area network where tens of thousands of paths have to be evaluated. Tools which use Dijkstra’s algorithm10 have been developed to identify all of the possible paths as well as which ones overlap with one another.

Once all the possible routing paths are known, the predicted availability from each core node to every other core node can be calculated and predicted. The “NxN” matrix below shows the predicted availability from each core node in the Simple Full Mesh Topology shown above (Figure 3).

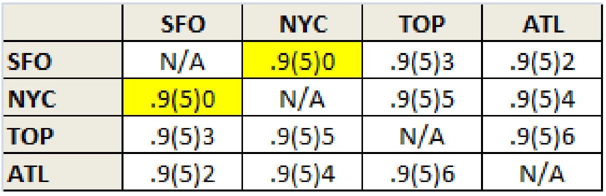
A shorthand notation is used in the matrix to improve readability. For example, the availability between the SFO and ATL node is shown as .9(5)2 which represents a predicted availability of 99.9992% (stated as five nines two). The availability calculation was based on the distances shown in the diagram using the metrics identified above [7]. The matrix shows the predicted availability for communication service between every core node pair, but it is common to be conservative and report the predicted availability of a given core node backbone using the lowest predicted availability in the matrix for a specific core node pair. In this example, we would predict the availability for any communication service over this simple full mesh core node backbone topology to be 99.999% (five nines zero) because it is the lowest predicted availability between any two core nodes as highlighted in the matrix (SFO to NYC).

Survivability

The other component needed for mission critical safety design is network survivability. Survivability is often confused with availability but it is quite different in that availability predicts failures using reliability engineering while survivability is concerned with the behaviour of the network when failures occur. Survivability also considers "accidents", or failures that cannot be predicted by an inherent availability model based on reliability parameters. Routing anomalies such as black holes are logical failures and occur less frequently than physical failures. Because of their infrequent occurrence they are not always addressed by network architects, but they can have widespread and devastating impact to routed networks and are unacceptable to mission critical networks where public safety is at stake.

The dual core architecture is a solution for overcoming these unpredictable six sigma events that cannot be predicted by traditional availability modelling. A dual core architecture uses two logically separate (separate routing domains with separate Autonomous System (AS) numbers) backbones. It preserves the flexibility that dynamic routing can provide along with the cost efficiencies of using a shared infrastructure. This is where Parallel Redundancy Protocol (PRP) technology comes into play, and in particular, the enhancements to PRP known as PRP-1+ which provide the ability to seamlessly use either one of the core networks in a dual core WAN architecture.

PRP was introduced as an industrial engineering standard for LANs by the International Electrotechnical Commission (IEC), an international standards body that develops and publishes standards for electrical, electronic and related technologies used in industry today. The original standard was published as IEC 62439-3 in 2010 and is often referred to as PRP-0. The standard was updated in July 2012 to be compatible with High-availability Seamless Redundancy (HSR) protocol. IEC 62439-3 (2012) has superseded IEC 62439-3 (2010) and is referred to as PRP-111 [8].



	SFO	NYC	TOP	ATL
SFO	N/A	.9(5)0	.9(5)3	.9(5)2
NYC	.9(5)0	N/A	.9(5)5	.9(5)4
TOP	.9(5)3	.9(5)5	N/A	.9(5)6
ATL	.9(5)2	.9(5)4	.9(5)6	N/A

Figure 3: "NxN" matrix.

PRP was motivated by the energy industry where automated power substations require a highly reliable operation with seamless failover. PRP-0 required separate parallel LANs of similar design12. PRP-1 improved upon the original PRP-0 by making it more flexible in its ability to deal with multi-protocol environments and more network topologies, especially ring topologies implemented using High-availability Seamless Redundancy (HSR). Harris Corporation enhanced the PRP-1 implementation so that it could operate in a WAN environment, hence the name PRP-1+.

How PRP Works

A functional diagram of dual core network architecture is shown below. The diagram shows two separate networks, Blue and Red, and a PRP Network Redundancy Box referred to as a Red Box on either side running PRP1+ (Figure 4).

Starting from the left side, the Ethernet frames entering the Red Box are duplicated and each packet is transmitted over the Red and Blue Core networks simultaneously to the Red Box on the right side. The Red Box on the right side uses a Discard Duplicate (DD) algorithm to identify duplicate packets and discard them when they are found. The operation is transparent to the user applications sending and receiving packets whereby the user is unaware which network (Red or Blue) is carrying the packets they receive.

How PRP was enhanced to work over a WAN

PRP was originally designed to work in a Local Area Network (LAN) and was limited to this environment. Limitations were due to the design of the Discard Duplicate algorithm which uses specific information in the Layer 2 frame to identify duplicates and discard them when they are found. Specifically, PRP uses the source Medium Access Control (MAC) address and a sequence identifier which PRP adds to a Redundancy Control Trailer (RCT) at the end of each frame when the sender duplicates a frame. With this approach, the PRP receiver stores the source MAC address and sequence identifier from the first frame it receives and passes the frame through. Each subsequent frame received is compared to these two fields and if they match the Discard Duplicate process will discard the duplicate frames it finds. Frame information is buffered for a specific duration of time so that the sequence number does not wrap; causing duplicate frames to erroneously be missed. Note that early PRP implementations required other fields for identifying duplicates (e.g. Lane Identifier) but PRP-1 eliminated the requirement

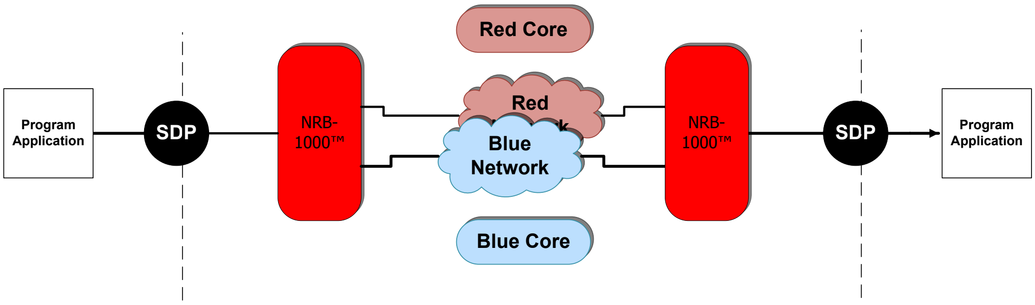


Figure 4: Red Box on either side running PRP1+.

of these fields in order to support improved flexibility in the types of networks where PRP can be used. PRP-1 simply provides guidance for how the Discard Duplicate algorithm should work instead of specifying the actual design.

PRP is ideal for a dual LAN architecture used in the energy industry for both its high reliability and seamless failover characteristics. When considered for use in a WAN environment, it did not seem applicable at first glance.

There were some technical challenges associated with getting PRP to work in the WAN environment. The first challenge was figuring out how to get the Discard Duplicate algorithm to work in the WAN environment. The reason is the key layer 2 data elements, source MAC address and layer 2 sequence number would not be retained as the layer 2 link level information is updated at every network node hop in a WAN. To overcome this, it was determined that the PRP receiver could determine if a frame contained Internet Protocol (IP) packets in the frame by the layer 2 protocol identifier field. Once it is known that the frame contains an IP packet, then fields in the layer 3 IP packet header that correspond to similar fields used by PRP at layer 2 could be used by the Discard Duplicate algorithm. In the IP packet header, the corresponding fields to use are the source IP packet address and packet Identification field which are similar to the frame sequence number field used by PRP. The structure of an IP packet is shown on the right.

Another challenge to overcome in the WAN environment was the relative difference in latency between the two networks. In a LAN environment, duplicate frames arriving on two separate networks will typically be microseconds apart. In a WAN environment this disparity of arriving duplicate packets on two separate WANs will be milliseconds apart so efficient buffering and processing techniques are required to identify and discard duplicates. Efficient buffering and processing is required because of the high data rates used in today's networks and the number of packets that will arrive on the two networks that have to be checked for duplicates (Figure 5).

For example, using the smallest packet size of a 46 octet IP packet

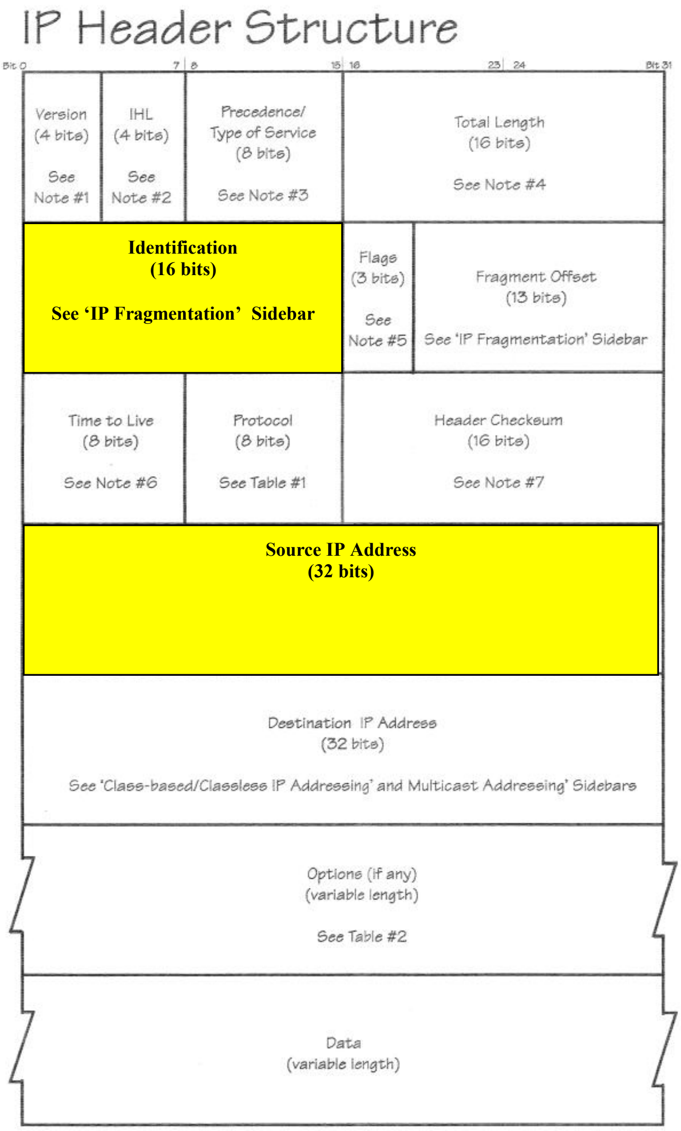

IP Header Structure
Bit 0
7
8
15
16
23
24
Bit 31
Version (4 bits) See Note #1
IHL (4 bits) See Note #2
Precedence/ Type of Service (8 bits) See Note #3
Total Length (16 bits) See Note #4
Identification (16 bits) See 'IP Fragmentation' Sidebar
Flags (3 bits) See Note #5
Fragment Offset (13 bits) See 'IP Fragmentation' Sidebar
Time to Live (8 bits) See Note #6
Protocol (8 bits) See Table #1
Header Checksum (16 bits) See Note #7
Source IP Address (32 bits)
Destination IP Address (32 bits) See 'Class-based/Classless IP Addressing' and Multicast Addressing' Sidebars
Options (if any) (variable length) See Table #2
Data (variable length)

Figure 5: IP header structure.

Preamble+SFD (start frame delimiter)	8 octets
Destination address	6 octets
Source address	6 octets
802.1Q tag (optional)	*4 octets*
Frame type	2 octets
Data	46 to 1500 octets
CRC	4 octets
IFG (Interframe Gap)	*12 octets*

Table 1: Characteristics for IEEE 802.1q Ethernet frames.

and a 1Gbps line rate requires approximately 1.488M packets per second that have to be examined for duplicates. This calculation takes into account the following characteristics for IEEE 802.1q Ethernet frames (Table 1):

The 46 octet layer 3 packet is encapsulated in the data field of the layer 2 Ethernet frame, and each packet will require 672 bit times as shown below:

- 46 octets + 8 octets Preamble and SFD + 12 octets of Destination and Source address + 2 octets of Frame type + 4 octets of CRC + 12 octets of IFG=84 octet packet times=84 * 8=672 bit times

At a line rate of 1Gbps, the number of packets that have to be examined is:

- 1Gbps / 672 bits per packet=1,488,095 p/s

It is also important to consider the possibility of the packet Identification field wrapping in the WAN environment. The Identification field is 16 bits in length and the analysis below shows that when using the small packet size of 46 octets at a line rate of 1Gbps the Identification Field could theoretically roll over in 44ms.

- 1,488,095 p/s= 1 packet every

.0000006720001 seconds=.672 us

- a 16 bit sequence number incrementing once per packet would roll over in

○ 65536 * .6720001 us=44.04 ms

If we relied strictly on the Identification field and the latency of arrival of one network relative to the other was greater than 44ms then the Discard Duplicate algorithm would not detect and discard all duplicate packets.

It should be pointed out that these are extreme conditions because most networks use larger size packets and the small size 46 octet packets are worst case. In other words, the problem is not as difficult with larger packet sizes because fewer packets are received in a given time interval and the number of packets that need to be checked by the Discard Duplicate algorithm becomes smaller. However, it does point out the need for efficient buffering and processing in the Discard Duplicate algorithm.

Although the probability of this wrapping phenomenon is mathematically small, the probability of its occurrence can be reduced by considering other fields in the IP packet when identifying and discarding duplicates. Considering and comparing other fields such as the Destination IP address, the Flags and Fragment Offset, and the Data field improve the robustness of the Discard Duplicate algorithm.

With these enhancements, PRP works in the WAN environment the same way it was designed to work in the LAN environment. Data is transmitted over both core networks by a sending Red Box to its destination where a receiving Red Box looks for duplicates. If one of the two networks were to fail for any reason, then the packet will make its way to the destination over the other network. In a routed IP network, this benefit is especially useful when unpredictable six sigma events such as a black hole occur.

Putting it All Together and the Benefits of PRP1+

Engineers have been running predicted availability models for years and the science and mathematics are well understood. The process involves breaking down components into serial and parallel paths and using proven formulas to calculate predicted availability based on MTBF and MTTR parameters. When designing a core network, availability is improved by creating parallel paths with physically separate equipment and circuit paths.

Automatic Protection Switching (APS) or dynamic routing is also required to use physically separate paths. It may seem the use of Red Boxes and PRP is all that is needed and can provide both physical and logical diversity as long as each core network is both physically and logically diverse. However, the robustness of the design can be improved if each one of the core networks is designed to be physically diverse within it. This design implies that high availability through physical diversity is achieved on each core network of the dual core network, and PRP is used to add the logical diversity feature. The benefit of this added robustness is that no single high availability design is perfect, and the added protection is warranted when it comes to public safety.

The physical diversity in the equipment and circuit paths is extremely important, but routed networks are also susceptible to logical failures and physical diversity alone is not enough to protect a mission critical safety infrastructure. Adding logical diversity to high availability architecture is known as survivability.

Survivability adds logical routing diversity to a network architecture by creating a logically separate routing domain. Route domain failures do not occur often, but when they do the impact can be devastating in that multiple sites and services are affected. Routing failures can be caused by unusual and unexpected equipment failures, deliberate cyber-attacks, or unintended human error. These types of failures are not anticipated by a typical availability model based on hardware component failure rates and/or fibre/copper cuts in the circuit paths. Although they do not occur often, widespread logical failures are unacceptable to mission safety critical services [9-12].

The principal survivability benefit of PRP is that it supports the use of both of the logically separate routing domains. And since PRP is a layer 2 switched protocol (as opposed to a layer 3 routing protocol) it has no reaction to routing anomalies that may occur in one of the two route domains. This point is significant because many dual core network architectures use routing protocols like Border Gateway Protocol (BGP) or multicast protocols to take advantage of the separate networks. However, a failure in routing can affect both networks with this type of design.

Another benefit of PRP is its seamless operation. PRP is similar in concept to Uni-directional Path Switched Ring (UPSR) technology which has been in use in the Synchronous Optical NETwork (SONET) world making disruptions in the network unnoticeable. This is especially important to latency and jitter sensitive services like mission critical voice. In a network that does not use a dual core architecture with PRP, a failure in either network will normally cause a momentary disruption while routing protocols figure out how to route around the failure. This phenomenon is known as route convergence and depends on many variables causing seconds (and possibly minutes) of disruption in a potentially critical voice stream. When human lives are at stake, a few seconds of disruption for such a critical service can be significant.

Related Work

Other concepts for enhancing PRP for IP networks were presented at the IEEE international conference in Cape Town in 2013 [13]. The IEEE reference addresses some of the differences between IPv4 and IPv6 packets where additional research is needed. This paper focuses on IPv4 and the capabilities described in this paper are proven and currently deployed in mission critical networks. More work is needed to address networks and applications that use IPv6. Harris Corporation is also working on PRP solutions for networks using IPv6.

Summary

Mission critical networks used to support safety critical applications require special design considerations for high availability performance and survivability.

High availability design uses proven reliability engineering with equipment redundancy and physical diversity routing of copper and circuit paths. Using proven mathematical formulas and parameters, a high availability objective can be accurately predicted and achieved.

Historically, in legacy point-to-point networks based on TDM technology, high availability design was all that was needed to meet the needs for mission critical safety networks. To take advantage of more flexible and more cost effective IP routed and switched networks, network survivability must also be addressed. Whereas availability addresses the physical aspects of the design, survivability addresses the logical aspects and six sigma events that are not anticipated by the availability model. Both components are needed for robust mission critical safety network architecture design.

The Dual Core network architecture is a proven highly available and highly survivable design and mitigates risks associated with unpredictable logical routing anomalies. Using Layer 2 PRP to connect logically separate core networks avoids the failures that can occur when the two networks are connected with Layer 3 routing protocols.

References

1. Murphy J, Morgan TW (2006) Availability, Reliability and Survivability: An Introduction and Some Contractual Implications. The Journal of Defense Software Engineering.
2. http://gcn.com/articles/2015/02/13/faa-fti-2.aspx
3. https://www.anpi.com/end-of-life-plans-for-tdm/
4. (2008) Recommendation ITU-T, Definition of Terms Related to Quality of Service E.800.
5. To M, Neusy P (1994) Unavailability Analysis of Long-haul Selected Areas in Communications 12: 100-109.
6. Kobayashi DS, Tesfaye M (1991) Availability of bi-directional line switched rings Rep.
7. http://www.sonet.com/EDU/upsr.htm
8. (2012) “Industrial communication networks - High availability automation networks - Part 3: Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR)” (3rdedn) IEC 62439.
9. http://www.sonet.com/EDU/blsr.htm
10. http://www.hill2dot0.com/wiki/index.php?title=4F-BLSR
11. Cormen TH, Leiserson CE, Rivest RL, Stein C (2001) Dijkstra’s algorithm. In: Introduction to Algorithms. MIT Press, Massachusetts, USA.
12. Weibel H (2011) Tutorial on Parallel Redundancy Protocol (PRP). Zurich University of Applied Sciences.
13. Rentschler M, Heine H (2013) The Parallel Redundancy Protocol for industrial IP networks. IEEE International Conference on Industrial Technology (ICIT).