



# **ProSoft Technology**

**Product Development Group**

Technical White Paper

## **Ethernet Broadcast Resiliency Policy**

November 01, 2007



## Your Feedback Please

We always want you to feel that you made the right decision to use our products. If you have suggestions, comments, compliments or complaints about the product, documentation or support, please write or call us.

### **ProSoft Technology**

1675 Chester Avenue, Fourth Floor

Bakersfield, CA 93301

+1 (661) 716-5100

+1 (661) 716-5101 (Fax)

<http://www.prosoft-technology.com>

Copyright © ProSoft Technology, Inc. 2000 - 2007. All Rights Reserved.

ProSoft Technology Ethernet Broadcast Resiliency Policy

November 01, 2007

PSFT...UM.07.11.01

ProSoft Technology®, ProLinx®, inRAx®, ProTalk® and RadioLinx® are Registered Trademarks of ProSoft Technology, Inc.

# Contents

Your Feedback Please .....	2
<b>1 ETHERNET BROADCAST RESILIENCY POLICY .....</b>	<b>5</b>
1.1 Datasheet Hardware specification update .....	5
1.1.1 Ethernet Port .....	5
<b>2 NOTES .....</b>	<b>7</b>
2.1 [1] Network Performance Baselineing by Daniel Nassar .....	7
2.1.1 Broadcast Storm Analysis .....	7
2.1.2 Using a Protocol Analyzer for a Broadcast Storm .....	8
2.2 [2] It's Alarming: Broadcast and Multicast Storms by Laura Chappell .....	8
2.2.1 SETTING THRESHOLDS FOR ALARMS .....	8
2.3 [3] Broadcast storm - Webopedia .....	9
2.4 [3] Building a Virtual Private Network by Meeta Gupta .....	9
2.5 [3] Networks Design and Management by Steven T. Karris.....	9
<b>3 REFERENCES .....</b>	<b>11</b>
3.1 Catalyst 2950 and Catalyst 2955 Switch Software Configuration Guide, 12.1(22)EA7 .....	11
3.2 Used Cisco: Broadcasts in Switched LAN Internetworks .....	12
3.2.1 Using Broadcasts with IP Networks.....	12
3.3 Broadcast radiation .....	12
3.3.1 From Wikipedia, the free encyclopedia .....	12
3.4 Additional References.....	14
<b>INDEX .....</b>	<b>15</b>



# 1 Ethernet Broadcast Resiliency Policy

## *In This Chapter*

- Datasheet Hardware specification update..... 5

It is considered as a general benchmark a broadcast sequence occurring at more than 500 (broadcast) frames per second is a storm event. Any broadcast activity beyond this amount is considered to be illegal. [1] (page 7) Most storms can be prevented with typical broadcast alarm thresholds set at about 100 broadcast frames per second. [2] (page 8)

ProSoft Technology normally incorporates Ethernet broadcast suppression (ARP) algorithms passing basic fault-tolerance tests in reference to illegal and excessive broadcast storm activity. The Ethernet broadcast storm endurance tests are run on a continuous basis thereby generating excessive traffic storm activity for multiple hours in excess of several thousand broadcast (ARP) frames-per-second.

ProSoft Technology requires limits on connected equipment with Ethernet functionality where improper network design or illegal [3] (page 9) broadcast traffic frequency and duration may exceed the upper limits of legitimate broadcast traffic. Further consequences in using such equipment on networks producing illegal broadcast storms beyond ProSoft Technology endurance tests may result in undesirable conditions, unexpected equipment behavior or system halting.

ProSoft Technology, Inc

Wallace Gastreich

Product Manager

## 1.1 Datasheet Hardware specification update

### **1.1.1 Ethernet Port**

Ethernet Broadcast Storm Resiliency =  $\leq 5000$  [ARP] frames-per-second and  $\leq 5$  minutes duration.



## 2 Notes

### *In This Chapter*

- [1] Network Performance Baseline by Daniel Nassar..... 7
- [2] It's Alarming: Broadcast and Multicast Storms by Laura Chappell..... 8
- [3] Broadcast storm - Webopedia..... 9
- [3] Building a Virtual Private Network by Meeta Gupta..... 9
- [3] Networks Design and Management by Steven T. Karris..... 9

### 2.1 [1] Network Performance Baseline by Daniel Nassar

#### **2.1.1 Broadcast Storm Analysis**

When encountering a broadcast storm in a network baseline session, an analyst can apply a specific technique to isolate the cause of the storm and the possible effect of the broadcast event on the internetwork.

A **broadcast storm** is a sequence of broadcast operations from a specific device or group of devices that occurs at a rapid frame-per-second rate that could cause network problems.

Network architecture, topology design, and layout configurations determine the network's tolerance level as it relates to frame-per-second broadcasts.

Consider, for example, a frame-per-second rate related to a broadcast storm generation of a specific protocol (Address Resolution Protocol [ARP], for example). Such generation, at more than 500 frames per second and on a continuing basis, is considered an abnormal protocol-sequencing event and can be extremely problematic.

### **2.1.2 Using a Protocol Analyzer for a Broadcast Storm**

Based on the network architecture, the protocols, and the node count on a site being studied, an analyst must determine what constitutes a broadcast storm. This requires the analyst to be quite familiar with the topology and types of protocols and applications being deployed. A general benchmark is that a broadcast sequence occurring from a single device or a group of devices, either rapidly or on an intermittent cycle at more than 500 frames per second, is a storm event. At the very least, the sequence should be investigated if it is occurring at 500 frames per second (relative to just a few devices and a specific protocol operation).

**Daniel J. Nassar** is president of LAN Scope Incorporated, a Havertown, Pennsylvania-area based international Network Baseline Consulting and Training firm. The firm specializes in emergency network troubleshooting, network baseline studies, application characterization and remote protocol analysis. Dan is personally active in the firm's training division, where he teaches courses on network baselining subjects.

As president of Eagle Eye Analysis Incorporated, another Pennsylvania-based network consulting firm, Dan evaluates industry products such as network analyzers or new networking devices such as switches and routers. Dan provides remote evaluation and writing services direct to industry manufacturers that includes documentation design for industry white paper reviews, training manual design, and overall product assessment.

Skilled in an extensive range of networking disciplines including network design, network implementation, troubleshooting, and network management, Dan is highly regarded throughout the industry as the global markets chief scientist in the area of network baseline evaluation and reporting.

## **2.2 [2] It's Alarming: Broadcast and Multicast Storms by Laura Chappell**

### **2.2.1 SETTING THRESHOLDS FOR ALARMS**

A broadcast or a multicast storm triggers a network analyzer alarm when the broadcast frames per second threshold has been exceeded. This threshold is usually configurable, and the default setting for most network analyzers is typically 100 broadcast frames per second.

**About Laura Chappell:** As the Sr. Protocol Analyst and founder of the Protocol Analysis Institute, Laura writes, lectures and advises on network troubleshooting, optimization, and security. She is an active member of HTCIA (High Technology Crime Investigation Association) and an IEEE Associate since 1990.

Ms. Chappell's clients include many Fortune 100 companies as well as local, national and international law enforcement and government institutions, as listed below:

- Cisco Systems
- Novell, Inc.
- IBM Corporation
- Bindview Corporation
- City of San Francisco, California
- State of New Mexico
- Federal Bureau of Investigation
- Helsana, Switzerland
- United States Navy
- United Bank of Switzerland
- High Technology Crime Investigation Association
- Swiss Re
- City of Plano, Texas
- Connected Classroom
- ...and many more

### 2.3 [3] Broadcast storm - Webopedia

A state in which a message that has been broadcast across a network results in even more responses, and each response results in still more responses in a snowball effect. A severe broadcast storm can block all other network traffic, resulting in a network meltdown. Broadcast storms can usually be prevented by carefully configuring a network to block **illegal** broadcast messages.

### 2.4 [3] Building a Virtual Private Network by Meeta Gupta

In Meeta's book, Building A Virtual Private Network, the author refers a broadcast storm as illegal; "Broadcast Storms can be effectively prevented by blocking illegal broadcast messages in the network"

**Meeta Gupta** has a master's degree in computer engineering. The topic of networking is her first love. She currently works at NIIT Ltd., where she designs, develops, and authors books on various subjects. She has co-authored books on TCP/IP, A+ Certification, ASP.NET, and PHP. She also has extensive experience in designing and developing ILTs. Besides writing, Meeta has conducted courses on C++, Sybase, Windows NT, Unix, and HTML for audiences ranging from students to corporate clients.

### 2.5 [3] Networks Design and Management by Steven T. Karris

In Steven's book, Networks Design and Management, the author refers to a broadcast storm as illegal; "Broadcast Storms can be minimized or eliminated by proper network design to block illegal broadcast messages"

**Steven Karris, M.S.E.E., P.E.**, earned a bachelor's degree in electrical engineering at Christian Brothers University, Memphis, Tennessee, and a master's degree in electrical engineering at Florida Institute of Technology, Melbourne, Florida. He is a registered professional engineer in California and Florida and has over 30 years of professional engineering experience in industry. In addition, he has over 25 years of teaching experience that he acquired at several educational institutions as an adjunct professor. He is currently with University of California-Berkeley Extension.



## 3 References

### *In This Chapter*

- Catalyst 2950 and Catalyst 2955 Switch Software Configuration Guide, 12.1(22)EA7 ..... 11
- Used Cisco: Broadcasts in Switched LAN Internetworks ..... 12
- Broadcast radiation ..... 12
- Additional References ..... 14

### 3.1 Catalyst 2950 and Catalyst 2955 Switch Software Configuration Guide, 12.1(22)EA7

Chapter: Understanding Storm Control.

Storm control prevents traffic on a LAN from being disrupted by a broadcast, multicast, or unicast storm on a port. A LAN storm occurs when packets flood the LAN, creating excessive traffic and degrading network performance. Errors in the protocol-stack implementation, mistakes in network configuration, or users issuing a denial-of-service attack can cause a storm.

Storm control is configured for the switch as a whole but operates on a per-port basis. By default, storm control is disabled.

Storm control uses rising and falling thresholds to block and then restore the forwarding of broadcast, unicast, or multicast packets. You can also set the switch to shut down the port when the rising threshold is reached.

Storm control uses one of these methods to measure traffic activity:

- Bandwidth based
- Traffic rate at which packets are received (in packets per second) (available only on non-Long-Reach Ethernet [LRE] Catalyst 2950 switches)

The thresholds can either be expressed as a percentage of the total available bandwidth that can be used by the broadcast, multicast, or unicast traffic, or as the rate at which the interface receives multicast, broadcast, or unicast traffic.

When a switch uses the bandwidth-based method, the rising threshold is the percentage of total available bandwidth associated with multicast, broadcast, or unicast traffic before forwarding is blocked. The falling threshold is the percentage of total available bandwidth below which the switch resumes normal forwarding. In general, the higher the level, the less effective the protection against broadcast storms.

---

## 3.2 Used Cisco: Broadcasts in Switched LAN Internetworks

### 3.2.1 Using Broadcasts with IP Networks

There are three sources of broadcasts and multicasts in IP networks:

- **Workstations**-An IP workstation broadcasts an Address Resolution Protocol (ARP) request every time it needs to locate a new IP address on the network. For example, the command telnet mumble.com translates into an IP address through a Domain Name System (DNS) search, and then an ARP request is broadcast to find the actual station. Generally, IP workstations cache 10 to 100 addresses for about two hours. The ARP rate for a typical workstation might be about 50 addresses every two hours or 0.007 ARPs per second. Thus, 2000 IP end stations produce about 14 ARPs per second.
- **Routers**-An IP router is any router or workstation that runs RIP. Some administrators configure all workstations to run RIP as a redundancy and reachability policy. Every 30 seconds, RIP uses broadcasts to retransmit the entire RIP routing table to other RIP routers. If 2000 workstations were configured to run RIP and if 50 packets were required to retransmit the routing table, the workstations would generate 3333 broadcasts per second. Most network administrators configure a small number of routers, usually five to 10, to run RIP. For a routing table that requires 50 packets to hold it, 10 RIP routers would generate about 16 broadcasts per second.
- **Multicast applications**-IP multicast applications can adversely affect the performance of large, scaled, switched networks. Although multicasting is an efficient way to send a stream of multimedia (video data) to many users on a shared-media hub, it affects every user on a flat switched network. A particular packet video application can generate a seven-megabyte (MB) stream of multicast data that, in a switched network, would be sent to every segment, resulting in severe congestion.

## 3.3 Broadcast radiation

### 3.3.1 From Wikipedia, the free encyclopedia

**Broadcast radiation** is the accumulation of broadcast and multicast traffic on a computer network.

The final stage of a broadcast radiation is called a **broadcast storm** and it is a state where new network connections cannot be established, and existing connections may be dropped, as the condition is now self-sustaining and magnifying.

Especially within a big broadcast domain a number of causes can generate a snowball effect chain reaction culminating with the broadcast storm with a severe negative impact on network latency.

### Causes

Most commonly the cause is a redundant switched topology where two or more links exist between two switches and as broadcasts and multicasts are forwarded by switches out every port except the port that received the traffic the two switches will broadcast each other's broadcasts creating a switching loop.

In some cases, a broadcast storm can be instigated for the purpose of a denial of service (DOS) using one of the magnification attacks smurf.c or fraggle.c, where smurf sends a large amount of ICMP Echo Requests ([ping](http://en.wikipedia.org/wiki/ping) (<http://en.wikipedia.org/wiki/ping>)) traffic to a broadcast address, with each ICMP Echo packet containing the spoof source address of the victim host.

When the spoofed packet arrives at the destination network, all hosts on the network reply to the spoofed address. The initial Echo Request is multiplied by the number of hosts on the network. This generates a storm of replies to the victim host tying up network bandwidth, using up CPU resources or possibly crashing the victim.

Sometimes, a broadcast storm may be caused by a network card malfunction result from disassociation of error packet.

In wireless networks a disassociation packet spoofed with the source to that of the AP and sent to the broadcast address can generate a disassociation broadcast DOS attack.

### Prevention

- Switching loops are largely addressed with STP, see Switching loop and Spanning tree protocol for more info. In [Metro Ethernet](http://en.wikipedia.org/wiki/metro_ethernet) ([http://en.wikipedia.org/wiki/metro\\_ethernet](http://en.wikipedia.org/wiki/metro_ethernet)) rings it is prevented using the Ethernet Automatic Protection System (EAPS) protocol.
- Filtering broadcasts by layer 3 equipment, typically routers (and even switches that employ advanced filtering called brouters).
- Physically segmenting the broadcast domains using routers (or logically with [VLANs](http://en.wikipedia.org/wiki/vlan) (<http://en.wikipedia.org/wiki/vlan>)) at Layer 3 in the same fashion switches decrease the size of collision domains at Layer 2.
- Routers and firewalls can be configured to detect and prevent maliciously inducted broadcast storms with the magnification attacks.

### Misinterpretations

- 1 A common misinterpretation is that routing loops have anything to do with broadcast storms. Working at Layer 3, routers (unlike layer 2 equipment) do not forward MAC-level broadcast traffic.
- 2 Another misinterpretation is that routers cannot forward broadcasts under special circumstances. Some routable protocols support the use of internetwork-level broadcasts, if the router is configured to forward them the broadcast domain segmentation is compromised.
- 3 Most commonly it is believed that only routers can impact the broadcast domain, or filter broadcasts, but as we have seen switches can blur the layer line and do that with VLANs and can do filtering (they still need a router for forwarding however).

- 4 A misinterpretation is that a broadcast can be responded with a broadcast. This is not true, however a broadcast can be issued to gather information needed to respond to an initially received broadcast, and in a redundant looped topology this second broadcast can reach the interface that sent the initial broadcast.

#### *MANET broadcast storms*

In a mobile ad-hoc network (MANET), route request (RREQ) packets are usually broadcast to discover new routes. These RREQ packets may cause broadcast storms and compete over the channel with data packets. One approach to alleviate the broadcast storm problem is to inhibit some hosts from rebroadcasting to reduce the redundancy, and thus contention and collision.

### 3.4 Additional References

- 1 Appendix E: Broadcasts in Switched LAN Internetworks [\[1\]](#) [\[2\]](#) PDF
- 2 Defense Against the DoS/DDoS Attacks on Cisco Routers [\[3\]](#) [\[4\]](#) PDF (56.2 KiB)
- 3 Disassociation Broadcast Attack Using ESSID Jack [\[5\]](#)
- 4 The Broadcast Storm Problem in a Mobile Ad Hoc Network [\[6\]](#) PDF (1.12 MiB)

Retrieved from "[http://en.wikipedia.org/wiki/Broadcast\\_radiation](http://en.wikipedia.org/wiki/Broadcast_radiation)"

## Index

### I

- [1] Network Performance Baseline by Daniel Nassar • 5, 7
- [2] It's Alarming Broadcast and Multicast Storms by Laura Chappell • 5, 8
- [3] Broadcast storm - Webopedia • 5, 9
- [3] Building a Virtual Private Network by Meeta Gupta • 9
- [3] Networks Design and Management by Steven T. Karris • 9

### A

Additional References • 14

### B

Broadcast radiation • 12  
Broadcast Storm Analysis • 7

### C

Catalyst 2950 and Catalyst 2955 Switch Software Configuration Guide, 12.1(22)EA7 • 11  
Causes • 13

### D

Datasheet Hardware specification update • 5

### E

Ethernet Broadcast Resiliency Policy • 5  
Ethernet Port • 5

### F

From Wikipedia, the free encyclopedia • 12

### M

MANET broadcast storms • 14  
Misinterpretations • 13

### N

Notes • 7

### P

Prevention • 13

### R

References • 11

### S

SETTING THRESHOLDS FOR ALARMS • 8

### U

Used Cisco Broadcasts in Switched LAN Internetworks • 12  
Using a Protocol Analyzer for a Broadcast Storm • 8  
Using Broadcasts with IP Networks • 12

### Y

Your Feedback Please • 2