Network Working Group
Request for Comments: 2644
Updates: 1812
BCP: 34
Category: Best Current Practice

D. Senie
Amaranth Networks Inc.

August 1999

Changing the Default for Directed Broadcasts in Routers

Status of this Memo

Copyright Notice

1. Introduction

Router Requirements [1] specifies that routers must receive and forward directed broadcasts. It also specifies that routers MUST have an option to disable this feature, and that this option MUST default to permit the receiving and forwarding of directed broadcasts. While directed broadcasts have uses, their use on the Internet backbone appears to be comprised entirely of malicious attacks on other networks.

Changing the required default for routers would help ensure new routers connected to the Internet do not add to the problems already present.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

2. Discussion

Damaging denial of service attacks led to the writing of [2] on Ingress Filtering. Many network providers and corporate networks have endorsed the use of these methods to ensure their networks are not the source of such attacks.

A recent trend in Smurf Attacks [3] is to target networks which permit directed broadcasts from outside their networks. By permitting directed broadcasts, these systems become "Smurf Amplifiers."

While the continued implementation of ingress filters remains the best way to limit these attacks, restricting directed broadcasts should also receive priority.

Network service providers and corporate network operators are urged to ensure their networks are not susceptible to directed broadcast packets originating outside their networks.

Mobile IP [4] had provisions for using directed broadcasts in a mobile node's use of dynamic agent discovery. While some implementations support this feature, it is unclear whether it is useful. Other methods of achieving the same result are documented in [5]. It may be worthwhile to consider removing the language on using directed broadcasts as Mobile IP progresses on the standards track.

3. Recommendation

Router Requirements [1] is updated as follows:

Section 4.2.2.11 (d) is replaced with:

> (d) { <Network-prefix>, -1 }
>
> Directed Broadcast - a broadcast directed to the specified network prefix. It MUST NOT be used as a source address. A router MAY originate Network Directed Broadcast packets. A router MAY have a configuration option to allow it to receive directed broadcast packets, however this option MUST be disabled by default, and thus the router MUST NOT receive Network Directed Broadcast packets unless specifically configured by the end user.

Section 5.3.5.2, second paragraph replaced with:

> A router MAY have an option to enable receiving network-prefix-directed broadcasts on an interface and MAY have an option to enable forwarding network-prefix-directed broadcasts. These options MUST default to blocking receipt and blocking forwarding of network-prefix-directed broadcasts.

4. Security Considerations

The goal of this document is to reduce the efficacy of certain types of denial of service attacks.

5. References

[1] Baker, F., "Requirements for IP Version 4 Routers", RFC 1812, June 1995.

[2] Ferguson, P. and D. Senie, "Ingress Filtering", RFC 2267, January 1998.

[3] See the pages by Craig Huegen at: http://www.quadrunner.com/~chuegen/smurf.txt, and the CERT advisory at: http://www.cert.org/advisories/CA-98.01.smurf.html

[4] Perkins, C., "IP Mobility Support", RFC 2002, October 1996.

[5] P. Calhoun, C. Perkins, "Mobile IP Dynamic Home Address Allocation Extensions", Work in Progress.

6. Acknowledgments

The author would like to thank Brandon Ross of Mindspring and Gabriel Montenegro of Sun for their input.

7. Author's Address

Daniel Senie
Amaranth Networks Inc.
324 Still River Road
Bolton, MA 01740

Phone: (978) 779-6813
EMail: dts@senie.com

8. Full Copyright Statement

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.