

IPv6 Operations
Internet-Draft
Expires: March 31, 2004

T. Chown
University of Southampton
Oct 2003

IPv6 Implications for TCP/UDP Port Scanning
draft-chown-v6ops-port-scanning-00

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of [Section 10 of RFC2026](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/lid-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on March 31, 2004.

Copyright Notice

Copyright (C) The Internet Society (2003). All Rights Reserved.

Abstract

The 128 bits of IPv6 address space is considerably bigger than the 32 bits of address space in IPv4. In particular, the IPv6 subnets to which hosts attach will by default have 64 bits of host address space. As a result, traditional methods of remote TCP or UDP port scanning to discover open or running services on a host will potentially become far less computationally feasible, due to the larger search space in the subnet. This document discusses that property of IPv6 subnets, and describes related issues for site administrators of IPv6 networks to consider.

Table of Contents

1.	Introduction	3
2.	Target Address Space for Port Scanning	4
2.1	IPv4	4
2.2	IPv6	4
2.3	Reducing the IPv6 Search Space	4
2.4	Dual-stack networks	4
3.	Alternatives for Attackers	5
4.	Recommendations for Site Administrators	6
4.1	Use of IPv6 Privacy Addresses	6
4.2	DHCPv6 Configuration	6
5.	Potential Standards Extensions	7
6.	Security Considerations	8
7.	Acknowledgements	9
	Normative References	10
	Author's Address	10
	Intellectual Property and Copyright Statements	11

1. Introduction

The 128 bits of IPv6 [\[1\]](#) address space is considerably bigger than the 32 bits of address space in IPv4. In particular, the IPv6 subnets to which hosts attach will by default have 64 bits of host address space. As a result, traditional methods of remote TCP or UDP port scanning to discover open or running services on a host will potentially become far less computationally feasible, due to the larger search space in the subnet. This document discusses that property of IPv6 subnets, and describes related issues for site administrators of IPv6 networks to consider.

It must be remembered that the defense of a network must not rely on the obscurity of the hosts on that network. Such a feature or property is only one measure in a set of measures that may be applied. However, with a growing usage of IPv6 devices in open networks likely, and security becoming more likely an issue for the end devices, such considerations should be given some weight where to implement appropriate measures is of little cost to the administrator.

Port scanning is quite a prevalent tactic from would-be attackers. The author observes that a typical university firewall will generate many Megabytes of log files on a daily basis purely from port scanning activity.

2. Target Address Space for Port Scanning

2.1 IPv4

A typical IPv4 subnet may have 8 bits reserved for host addressing. In such a case, a remote attacker need only probe at most 256 addresses to determine if a particular open service is running on a host in that subnet. At one probe per second, such a scan may take under 5 minutes to complete.

2.2 IPv6

A typical IPv6 subnet will have 64 bits reserved for host addressing. In such a case, a remote attacker needs to probe 2^{64} addresses to determine if a particular open service is running on a host in that subnet. At one probe per second, such a scan may take some 5 billion years to complete.

2.3 Reducing the IPv6 Search Space

The IPv6 host address space through which an attacker may search can be reduced in at least two ways. First, the attacker may rely on the administrator conveniently numbering their hosts [prefix]::1 upwards. Second, in the case of statelessly autoconfiguring [\[1\]](#) hosts, the host part of the address will take a well-known format that includes Ethernet vendor prefix and the "fffe" stuffing. For such hosts, if the Ethernet vendor is known, the search space may be reduced to 24 bits (with a one probe per second scan then taking 194 days).

2.4 Dual-stack networks

Full advantage of the increased IPv6 address space in terms of resilience to port scanning may not be gained until IPv6-only networks and devices become more commonplace, given that most IPv6 hosts are currently dual stack, with (more readily scannable) IPv4 connectivity also. However, many applications or services (e.g. new peer-to-peer applications) on the (dual stack) hosts may emerge that are only accessible over IPv6, and that thus can only be discovered by IPv6 port scanning.

3. Alternatives for Attackers

If IPv6 port-scanning becomes infeasible, attackers will need to find new methods to identify IPv6 addresses for subsequent port scanning. One such method would be the harvesting of IPv6 addresses, either in transit or from recorded logs such as web site logs. Another may be to inspect the Received from: or other header lines in archived email or Usenet news messages.

IPv6-enabled hosts on local subnets may still be discovered through probing the "all hosts" link local multicast address. This implies that if an attacker can compromise one remote host, they may then learn addresses of the hosts in the same subnet on the remote network.

In IPv6 networks, attackers may also switch to using more aggressive yet subtle methods of attack, e.g. by using worms or virii that may attach to or attack the new IPv6 applications (e.g. peer-to-peer messaging).

4. Recommendations for Site Administrators

There are some methods that site administrators can apply to make the task for IPv6 port scanning attackers harder. We describe such methods in this section.

4.1 Use of IPv6 Privacy Addresses

By using the IPv6 Privacy Extensions [[3](#)] the hosts in the network would only ever connect to external sites using their (temporary) privacy address. While an attacker may be able to port scan that address if they do so quickly upon observing the address, the threat or risk is reduced. An example implementation of [RFC3041](#) already deployed has privacy addresses active for one day, but such addresses reachable for seven days. Note that an [RFC3041](#) host may have a separate static global IPv6 address by which it can also be reached.

4.2 DHCPv6 Configuration

The administrator could configure DHCPv6 so that the first addresses allocated from the pool begin much higher in the address space than [prefix>::1.

5. Potential Standards Extensions

It may be worth considering a standards extension to DHCPv6 that in some way allows a "random" IPv6 host address part to be assigned to a host, that will then be used for that host to receive incoming communications (and upon which it would thus need to be port scanned by an attacker).

6. Security Considerations

There are no specific security considerations in this document outside of the topic of discussion itself.

7. Acknowledgements

Thanks are due to people in the 6NET project for discussion of this topic, including Pekka Savola (CSS/FUNET) and Christian Strauf (JOIN Project, University of Muenster).

Normative References

- [1] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", [RFC 2460](#), December 1998.
- [2] Thomson, S. and T. Narten, "IPv6 Stateless Address Autoconfiguration", [RFC 2462](#), December 1998.
- [3] Narten, T. and R. Draves, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", [RFC 3041](#), January 2001.

Author's Address

Tim Chown
University of Southampton

Southampton, Hampshire S017 1BJ
United Kingdom

EMail: tjc@ecs.soton.ac.uk

Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on the IETF's procedures with respect to rights in standards-track and standards-related documentation can be found in [BCP-11](#). Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementors or users of this specification can be obtained from the IETF Secretariat.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this standard. Please address the information to the IETF Executive Director.

Full Copyright Statement

Copyright (C) The Internet Society (2003). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assignees.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION

HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF
MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Acknowledgment

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