Network Working Group
Internet Draft

Steven M. Bellovin
AT&T Labs Research

Expiration Date: August 2003

February 2003

Access Control Prefix Router Advertisement Option for IPv6

draft-bellovin-ipv6-accessprefix-01.txt

Status of this Memo

Abstract

Some very low-end devices are expected to rely on address-based authentication, even though that is not a high-security mechanism. In particular, they may wish to permit access by "local" peers only, for some value of "local". This memo proposes a new Router Advertisement option to supply a list of privileged prefixes.

1. Introduction

Some very low-end devices may rely on address-based authentication, even though that is not a high-security mechanism [Bell89]. In particular, they may wish to permit access by "local" peers only, for some value of "local".

This desire was one of the rationales for site-local addresses [RFC2373]. But site-local addresses have a number of disadvantages. Though most are out of scope for this document, one is important: not only is "site" ill-defined, its instantiation in any given installation may not match the desired security property. For example, a university dormitory may wish to restrict access to its printers to residents, but the "site" may include the entire campus.

Explicitly-configured filters could accomplish the same thing, of course. But printers can be painful to configure via a limited menu interface; lower-end devices, such as Internet-connected light switches and toasters, are even harder to administer. An easy-to-administer autoconfigure mechanism is essential.

The solution is to have routers announce the proper access control prefix via an option in the Router Advertisement message [RFC2461]. Devices that care can interpret and obey this option.

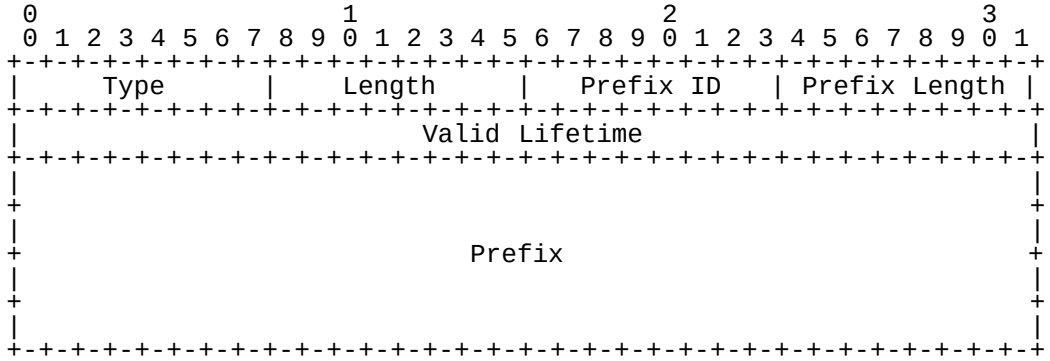
1.1. Terminology

The keywords MUST, MUST NOT, REQUIRED, SHALL, SHALL NOT, SHOULD, SHOULD NOT, RECOMMENDED, MAY, and OPTIONAL, when they appear in this document, are to be interpreted as described in [RFC2119].

2. Prefix Option

2.1. Syntax

The access control prefix option follows the format given in Section 4.6 of [RFC2461].



Type [To be assigned]

Length 3

Prefix ID The ID value for this prefix entry. A subsequent access control prefix option with the same ID replaces the older entry.

Prefix Length 8-bit unsigned integer. The number of leading bits in the Prefix that are valid. The value ranges from 0 to 128. Options with a prefix length greater than 128 MUST be ignored. A prefix length of 0 is a null entry, and is used to delete a prefix from the access control table.

Lifetime 32-bit unsigned integer, giving the valid lifetime of this prefix, in seconds. At the end of the validity interval, all access rights granted by this prefix MUST be deleted. A value of 0 indicates unlimited lifetime; this is NOT RECOMMENDED, because of the expense of subsequent revocation.

Prefix An IP address or a prefix of an IP address. The Prefix Length field contains the number of valid leading bits in the prefix. The bits in the prefix after the prefix length are reserved and MUST be initialized to zero by the sender and MUST be ignored by the receiver.

2.2. Router Behavior

A suitably-configured router MAY include one or more access control prefix announcements in its Router Advertisement messages. If more than one prefix is announced, communication is permitted with all such prefixes.

If possible, routers SHOULD send out the same, consistent set of prefixes in each message. If that is not possible (i.e., because of packet size limitations), additional Advertisement messages should be sent as soon as is possible, consistent with congestion control principles. Bear in mind that the typical target devices for this feature are low-end, and will have neither very much buffering nor the ability to service incoming packets quickly.

A router may revoke access to a prefix by sending a new advertisement with the same ID field but a 0 prefix length. (Lifetime does not apply to deleted prefixes.) This SHOULD be repeated at suitable intervals until the lifetime from the last valid advertisement has expired, plus some allowance for timer differences. The RECOMMENDED way to gently change an allowed prefix (such as during site renumbering) is by sending out a new advertisement with the new prefix and a new ID; the old prefix should be allowed to expire.

Per Section 6.2.7 of [RFC2461], routers SHOULD examine the access control prefix options in any received Router Advertisement messages. Any inconsistencies between the received value for any ID and what the router itself would send on that link SHOULD be logged to system or network management. Note that doing this helps find holes in the access control perimeter.

2.3. Device Behavior

A device MAY be configured to use access control based on prefix advertisements. If a device is configured in this fashion, it MUST listen for access control prefix announcements. Duplicate Address Detection messages -- i.e., Neighbor Solicitation messages that pass the validation criteria in [RFC2461], and have a source address of Unspecified MUST be accepted and processed normally, as described in [RFC2462]. Other incoming packets whose source address does not match one of the permitted prefixes MUST be discarded without further processing, even if they are acceptable via other security mechanisms. Devices MUST NOT send packets to any destination whose address does not match one of the allowed prefixes. Inbound or outbound packets dropped by these rules SHOULD be noted in the appropriate MIB or other auditing mechanism.

By default, devices MUST be preconfigured to think that they have received an advertisement for Prefix fe80::/10, lifetime unlimited. This is the link-local prefix; it must be allowed initially to permit devices to receive their initial access control configurations. Routers MAY NOT override this.

In their default configuration, devices MUST NOT accept packets from any non-link-local prefixes until they have received suitable advertisements. However, there MAY be a configuration option to permit acceptance of packets with the current link's prefix.

Access control prefix announcements apply only to the interface on which they are received. Multi-homed devices generally should receive such messages on each interface, with the obvious exception

of the local loopback interface.

Nothing in this specification prevents devices from using access control prefix announcements as a supplementary mechanism. In such configurations, the obligations to drop or block packets do not apply.

3. Open Issues

The biggest open issue is whether or not this option should exist. It is not a substitute for real security. Beyond that, we may wish to simplify it.

Should the lifetime field exist in this option? Note that the default router lifetime in [RFC2461] is explicitly described as not applying to options.

Should revocation exist? We clearly need either it or a lifetime.

What, if anything, should be done differently about tunneled links?

4. IANA Considerations

A new IPv6 Neighbor Discovery option type code must be assigned.

5. Security Considerations

This mechanism should not be confused with a real security mechanism, such as IPsec [RFC2041]. If at all possible, cryptographic security mechanisms should be used instead of this option.

Among the the threats are packets with forged source addresses. Routers may be able to filter packets that, based on their source address, cannot legally arrive on some interface; they SHOULD do so for any prefixes that have privileged access. But it is generally trivial for hosts on a LAN to forge the source address of some other, more trusted host on that LAN. Access control prefixes cannot defend against this sort of attack.

It's even possible to impersonate the advertising router. To guard against this, nodes implementing the access control prefix option MUST take special care to validate Router Advertisement options according to Section 6.1.2 of [RFC2461].

Remember that the entire concept of prefix-based access control is useful if and only if all attackers are coming from outside of the protected perimeter. An insider by definition has the right prefix, or could fake any other address prefix or suffix.

6. Changes Since -00

The "class" field has been deleted; it was too complex, and left room for too many errors. The ID field has been added; this provides a cleaner mechanism for adding or deleting allowed prefixes, especially during site renumbering. DAD messages are now explicitly permitted. Consistency between routers is now provided for.

7. References

[Bell89] "Security Problems in the TCP/IP Protocol Suite", S.M. Bellovin, Computer Communications Review 19:2, April 1989.

[RFC2119] "Key words for use in RFCs to Indicate Requirement Levels", S. Bradner. RFC 2119. March 1997.

[RFC2401] "Security Architecture for the Internet Protocol", S. Kent and R. Atkinson, RFC 2401, November 1998.

[RFC2373] "IP Version 6 Addressing Architecture. R. Hinden and S. Deering. RFC 2373. July 1998.

[RFC2461] "Neighbor Discovery for IP Version 6 (IPv6)", T. Narten, E. Nordmark, W. Simpson. RFC 2461. December 1998.

8. Author Information

Steven M. Bellovin
AT&T Labs Research
Shannon Laboratory
180 Park Avenue
Florham Park, NJ 07932
Phone: +1 973-360-8656
email: bellovin@acm.org