Network Working Group
Request for Comments: 4192
Updates: 2072
Category: Informational

F. Baker
Cisco Systems
E. Lear
Cisco Systems GmbH
R. Droms
Cisco Systems

September 2005

Procedures for Renumbering an IPv6 Network without a Flag Day

Status of This Memo

Copyright Notice

This document describes a procedure that can be used to renumber a network from one prefix to another. It uses IPv6's intrinsic ability to assign multiple addresses to a network interface to provide continuity of network service through a "make-before-break" transition, as well as addresses naming and configuration management issues. It also uses other IPv6 features to minimize the effort and time required to complete the transition from the old prefix to the new prefix.

Table of Contents

1. Introduction

The Prussian military theorist Carl von Clausewitz [Clausewitz] wrote, "Everything is very simple in war, but the simplest thing is difficult. These difficulties accumulate and produce a friction, which no man can imagine exactly who has not seen war.... So in war, through the influence of an 'infinity of petty circumstances' which cannot properly be described on paper, things disappoint us and we fall short of the mark". Operating a network is aptly compared to conducting a war. The difference is that the opponent has the futile expectation that homo ignoramus will behave intelligently.

A "flag day" is a procedure in which the network, or a part of it, is changed during a planned outage, or suddenly, causing an outage while the network recovers. Avoiding outages requires the network to be modified using what in mobility might be called a "make before break" procedure: the network is enabled to use a new prefix while the old one is still operational, operation is switched to that prefix, and then the old one is taken down.

This document addresses the key procedural issues in renumbering an IPv6 [RFC2460] network without a "flag day". The procedure is straightforward to describe, but operationally can be difficult to automate or execute due to issues of statically configured network state, which one might aptly describe as "an infinity of petty circumstances". As a result, in certain areas, this procedure is necessarily incomplete, as network environments vary widely and no one solution fits all. It points out a few of many areas where there are multiple approaches. This document updates [RFC2072]. This document also contains recommendations for application design and network management, which, if taken seriously, may avoid or minimize the impact of the issues.

1.1. Summary of the Renumbering Procedure

By "renumbering a network", we mean replacing the use of an existing (or "old") prefix throughout a network with a new prefix. Usually, both prefixes will be the same length. The procedures described in this document are, for the most part, equally applicable if the two prefixes are not the same length. During renumbering, sub-prefixes (or "link prefixes") from the old prefix, which have been assigned to links throughout the network, will be replaced by link prefixes from the new prefix. Interfaces on systems throughout the network will be configured with IPv6 addresses from the link prefixes of the new prefix, and any addresses from the old prefix in services like DNS [RFC1034][RFC1035] or configured into switches and routers and applications will be replaced by the appropriate addresses from the new prefix.

The renumbering procedure described in this document can be applied to part of a network as well as to an organization's entire network. In the case of a large organization, it may be advantageous to treat the network as a collection of smaller networks. Renumbering each of the smaller networks separately will make the process more manageable. The process described in this document is generally applicable to any network, whether it is an entire organization network or part of a larger network.

1.2. Terminology

DDNS: Dynamic DNS [RFC2136][RFC3007] updates can be secured through the use of SIG(0) [RFC4033][RFC4034][RFC4035][RFC2931] and TSIG [RFC2845].

DHCP prefix delegation: An extension to DHCP [RFC3315] to automate the assignment of a prefix, for example, from an ISP to a customer [RFC3633].

flag day: A transition that involves a planned service outage.

ingress/egress filters: Filters applied to a router interface connected to an external organization, such as an ISP, to exclude traffic with inappropriate IPv6 addresses.

link prefix: A prefix, usually a /64 [RFC3177], assigned to a link.

SLAC: StateLess Address AutoConfiguration [RFC2462].

1.3. Summary of What Must Be Changed

Addresses from the old prefix that are affected by renumbering will appear in a wide variety of places in the components in the renumbered network. The following list gives some of the places that may include prefixes or addresses that are affected by renumbering, and gives some guidance about how the work required during renumbering might be minimized:

- Link prefixes assigned to links. Each link in the network must be assigned a link prefix from the new prefix.
- IPv6 addresses assigned to interfaces on switches and routers. These addresses are typically assigned manually, as part of configuring switches and routers.
- Routing information propagated by switches and routers.
- Link prefixes advertised by switches and routers [RFC2461].
- Ingress/egress filters.
- ACLs and other embedded addresses on switches and routers.
- IPv6 addresses assigned to interfaces on hosts. Use of StateLess Address Autoconfiguration (SLAC) [RFC2462] or DHCP [RFC3315] can mitigate the impact of renumbering the interfaces on hosts.

- DNS entries. New AAAA and PTR records are added and old ones removed in several phases to reflect the change of prefix. Caching times are adjusted accordingly during these phases.

- IPv6 addresses and other configuration information provided by DHCP.

- IPv6 addresses embedded in configuration files, applications, and elsewhere. Finding everything that must be updated and automating the process may require significant effort, which is discussed in more detail in Section 3. This process must be tailored to the needs of each network.

1.4. Multihoming Issues

In addition to the considerations presented, the operational matters of multihoming may need to be addressed. Networks are generally renumbered for one of three reasons: the network itself is changing its addressing policy and must renumber to implement the new policy (for example, a company has been acquired and is changing addresses to those used by its new owner), an upstream provider has changed its prefixes and its customers are forced to do so at the same time, or a company is changing providers and must perforce use addresses assigned by the new provider. The third case is common.

When a company changes providers, it is common to institute an overlap period, during which it is served by both providers. By definition, the company is multihomed during such a period. Although this document is not about multihoming per se, problems can arise as a result of ingress filtering policies applied by the upstream provider or one of its upstream providers, so the user of this document also needs to be cognizant of these issues. This is discussed in detail, and approaches to dealing with it are described, in [RFC2827] and [RFC3704].

2. Detailed Review of Procedure

During the renumbering process, the network transitions through eight states. In the initial state, the network uses just the prefix that is to be replaced during the renumbering process. At the end of the process, the old prefix has been entirely replaced by the new prefix, and the network is using just the new prefix. To avoid a flag day transition, the new prefix is deployed first and the network reaches an intermediate state in which either prefix can be used. In this state, individual hosts can make the transition to using the new prefix as appropriate to avoid disruption of applications. Once all

of the hosts have made the transition to the new prefix, the network is reconfigured so that the old prefix is no longer used in the network.

In this discussion, we assume that an entire prefix is being replaced with another entire prefix. It may be that only part of a prefix is being changed, or that more than one prefix is being changed to a single joined prefix. In such cases, the basic principles apply, but will need to be modified to address the exact situation. This procedure should be seen as a skeleton of a more detailed procedure that has been tailored to a specific environment. Put simply, season to taste.

2.1. Initial Condition: Stable Using the Old Prefix

Initially, the network is using an old prefix in routing, device interface addresses, filtering, firewalls, and other systems. This is a stable configuration.

2.2. Preparation for the Renumbering Process

The first step is to obtain the new prefix and new reverse zone from the delegating authority. These delegations are performed using established procedures, from either an internal or external delegating authority.

Before any devices are reconfigured as a result of the renumbering event, each link in the network must be assigned a sub-prefix from the new prefix. While this assigned link prefix does not explicitly appear in the configuration of any specific switch, router, or host, the network administrator performing the renumbering procedure must make these link prefix assignments prior to beginning the procedure to guide the configuration of switches and routers, assignment of addresses to interfaces, and modifications to network services such as DNS and DHCP.

Prior to renumbering, various processes will need to be reconfigured to confirm bindings between names and addresses more frequently. In normal operation, DNS name translations and DHCP bindings are often given relatively long lifetimes to limit server load. In order to reduce transition time from old to new prefix, it may be necessary to reduce the time to live (TTL) associated with DNS records and increase the frequency with which DHCP clients contact the DHCP server. At the same time, a procedure must be developed through which other configuration parameters will be updated during the transition period when both prefixes are available.