MAP-E testing helps IPv6 carry IPv4 traffic

Niels Widger - January 18, 2019

Internet service providers (ISPs) are running out of public IPv4 addresses and want to move away from IPv4 in their internal network. Mapping of Address and Port with Encapsulation (MAP-E), an IPv6 transition mechanism for transporting IPv4 packets across an IPv6 network using IP encapsulation, lets ISPs provide IPv4 services without deploying a full dual-stack network. MAP-E saves money on network upgrades and speeds the migration to IPv6. MAP-E also helps relieve the issue of IPv4 address exhaustion by letting multiple CPE’s share the same public IPv4 address through a form of Carrier-Grade NAT (CGN).

This article discusses the mechanisms that MAP-E needs to function, explains the MAP-E configuration options and how they can be provisioned, and describes what you should test when developing a MAP-E implementation.

**MAP-E architecture**
IPv4 address sharing is a Carrier-Grade NAT (CGN) technique to allow sharing a single IPv4 address amongst multiple customer edge (CE) devices. MAP-E, defined in RFC 7597, enables this sharing by requiring each CE with the same IPv4 address to use different TCP/UDP ports. It is a mechanism to statelessly provide IPv4 connectivity via shared IPv4 addresses in an IPv6-only ISP network. DHCPv6 configuration options for MAP-E are defined in RFC 7598 to allow autoconfiguration of the use of MAP-E.

In MAP-E, IPv4 packets moving between the CE and the public IPv4 internet are encapsulated in IPv6 packets while transiting the IPv6-only ISP network. A MAP-enabled router inside the ISP network known as the MAP-E Border Relay (BR) receives MAP-E traffic from the CE and acts as the gateway between the ISP’s IPv6-only internal network and the public IPv4 internet. The IPv6-only internal network is known as the MAP domain. The IPv6 destination address for all outbound MAP-E traffic from the CE is set to the address of the BR.

The CE performs the normal Network Address and Port Translation (NAPT) processing on IPv4 packets prior to IPv6 encapsulation and after IPv6 decapsulation (Figure 1). NAPT maps private IPv4 addresses and UDP/TCP ports from the CE’s LAN clients onto the CE’s public IPv4 address. Thus, for outbound traffic, the CE rewrites the private source IPv4 address to be the CE’s public IPv4 address and rewrites the TCP/UDP source port from the list of available ports on the CE’s public IPv4 address. To do this, the CE maintains a table of NAPT bindings for all IPv4 traffic passing through the CE to its LAN clients.
Encapsulating IPv4 within a MAP domain

In MAP-E, multiple CE’s in a MAP domain share the same public IPv4 address. Each CE is assigned a Port Set Identifier (PSID) that determines the ports it’s allowed to use with its assigned public IPv4 address. Therefore, MAP-E requires that the CE’s NAPT implementation be aware of this additional restriction and only create NAPT bindings with port numbers on the public IPv4 address that are within the CE’s MAP-E port set.

Each CE is provisioned with a Basic Mapping Rule (BMR) and PSID offset, which can be provisioned via DHCPv6 options and must be the same for all CE’s within a MAP domain. The BMR contains a Rule IPv6 prefix, a Rule IPv4 prefix and a Rule Embedded Address bits (EA-bits) length. In addition to a BMR, each CE is assigned an End-user IPv6 prefix, most likely provisioned via DHCPv6 as an IA_PD prefix. The CE uses the End-user IPv6 prefix to determine its public IPv4 address and possibly its PSID, although this may be provisioned via DHCPv6 instead. As shown in Figure 2, the EA-bits of a CE’s End-user IPv6 prefix are the bits starting after the BMR Rule IPv6 prefix length, with the length being determined by the BMR EA-bit length.

A CE constructs its public IPv4 address by combining its BMR Rule IPv4 prefix with as many EA-bits as are required to create a complete 32-bit IPv4 address. If not already provisioned via DHCPv6, the remaining EA-bits are the CE’s PSID. The CE uses its public IPv4 address as the IPv4 source address for all MAP traffic. As shown in Figure 3, the CE constructs its full IPv6 address by combining its End-user IPv6 prefix with an interface ID that embeds its public IPv4 address and PSID. The CE then
uses this as the IPv6 source address for all MAP traffic.

![128-n-o-s bits](image1)

**Figure 3.** MAP-E CPE IPv6 interface identifier is 64 bits wide.

With this architecture, the BR in a MAP domain can statelessly process MAP traffic to and from MAP CE’s. On receiving a MAP packet from a CE, the BR first verifies that the IPv6 source address is within the BMR Rule IPv6 prefix of the MAP domain. Next, it extracts the public IPv4 address and PSID embedded in the interface ID of the source IPv6 address. It uses this information to verify that the source address of the encapsulated IPv4 packet is correct and that the UDP/TCP source port chosen by the CE is within its port set as determined by its PSID.

**Port sets**

**Using port sets**

As mentioned previously, every CE is configured with a PSID and PSID offset, which the CE uses to determine the range of ports it can use in combination with its public IPv4 address. The PSID offset places a boundary on the lowest port any CE in the MAP domain can use. If not otherwise configured, the PSID offset defaults to 6, which prevents CE’s in the MAP domain from using system ports below 1024. The length in bits of a CE’s PSID is variable and is dependent on how it was provisioned. If the CE received its PSID via the EA-bits of its End-user Prefix, the PSID length is the number of bits that were left over from the EA-bits after constructing its full public IPv4 address. If the CE received its PSID via DHCPv6, the PSID length is given in the DHCPv6 option.

A valid port for a CE is constructed by embedding its PSID bits into a 16-bit port number at an offset determined by the MAP domain’s PSID offset. Bits to the right of the PSID can take any value, while bits to the left of the PSID can take any value so long as they are not all zeros. The diagram in **Figure 4** shows this structure and illustrates how embedding the PSID bits into the port number creates ranges of non-contiguous ports for the CE to use.

![Ports in the CE port set](image2)

**Figure 4:** MAP-E CPE port layout where the leading (left) bits can’t be all zeros.
The size and number of port ranges in a CE’s port set is a product of both the PSID offset and the PSID bit length. Using the notation from Fig. 4, the number of ports in each range is \(2^m\) and the number of ranges is given by \((2^n) - 1\). The requirement that every CE sharing the same public IPv4 address use same PSID offset and PSID bit length ensures non-overlapping port sets. Thus, a MAP domain administrator has considerable control over the lowest starting port, the number of contiguous ports in each port range and the total number of port ranges in each CE’s port set. Finally, because the PSID is always in the same position for every port number, port validation by the BR can be done with a simple bitmask using a mask constructed from the PSID offset, PSID and PSID length values.

There are, of course, some tradeoffs a MAP-E administrator must make. There are only 65k ports per public address. While an administrator can have many CEs sharing a single public address, the more CEs that share that address, the number of ports per CE become smaller and less contiguous.

**Example**

For a concrete example, let’s assume a MAP CE is provisioned with a BMR Rule IPv6 prefix of 2001:db8:0000::/40, a BMR Rule IPv4 prefix of 192.0.2.0/24 (0xc0000200), a BMR EA-bit length of 16 and a PSID offset of 6, all via DHCPv6. The CE receives its End-user IPv6 prefix of 2001:db8:0012:3400::/56 via DHCPv6. Knowing that there must be 16 bits of EA-bits in its End-user IPv6 prefix after the BMR Rule IPv6 prefix, the CE extracts an EA-bits value of 0x1234 and uses it to compute its public IPv4 address and PSID. Because its BMR Rule IPv4 prefix has a length of 24 bits, the CE takes the most significant 8 bits (0x12) from the EA-bits to construct a full 32-bit public IPv4 address 192.0.2.18 (0xc0000212), which it will use as the source IPv4 address for all MAP traffic. The CE uses the 8 remaining EA-bits (0x34) for its PSID, resulting in a PSID of 52. The CE computes its MAP interface ID by combining its public IPv4 address and PSID resulting in an interface ID of ::0000:c000:0212:0034. Finally, the CE combines its End-user IPv6 prefix with the computed MAP interface ID resulting in the IPv6 source address it will use for all MAP traffic 2001:db8:0012:3400:0000:c000:0212:0034. See Figure 5.

Because the MAP domain is configured with a PSID offset of 6 and a PSID length of 8, no CE is allowed to use a port lower than 1024, each CE is allocated \(2^6 - 1 = 63\) port ranges and each port range contains \(2^2 = 4\) contiguous ports. In the case of the CE with PSID 52, its first two port ranges are 1232-1235 and 2256-2259. Its last two port ranges are 63696-63699 and 64720-64723.

**Testing**

When it comes to verifying the implementation of MAP-E on a CE device, there are several steps to take.
1. With a simulated MAP domain and BR, the first step is to validate that the CE correctly translates packets destined for the MAP domain, and those packets it receives from the MAP domain - correctly routing them to their intended destination (after also passing through NAPT).

2. Implementations should be tested that they correctly use the port ranges assigned (for both UDP and TCP). Negative testing is important here too, ensuring that the MAP-E stack does not use port ranges outside of those assigned, and rejects (doesn’t translate) packets with bad source addresses.

3. Since there’s a high likelihood of fragmentation for large packets, it’s important to test that the MAP-E stack handles packets that are fragmented, either inbound or outbound to the MAP domain.

4. Lastly, it’s important to test that any existing IPv4 applications still work through the MAP-E enabled CE. This includes lower level applications like Internet Control Message Protocol (ICMP), and end-user applications including DNS, HTTP, etc.

Conclusions

MAP-E is one of many different IPv6 transition mechanisms that have been developed over time, particularly for the broadband ISP industry, which have very particular needs when it comes to allowing IPv4 and IPv6 networks to work together. Though complex, it has benefits over some other tunneling or translation protocols, as the CE can be agnostic to the types of IPv4 packets being transferred, avoiding complicated and specific rules. There may come a time when such transition mechanisms are no longer necessary, but until then, protocol developers will continue to improve them for scalability and ease of deployment.

—Niels Widger is a Senior Developer at QA Cafe.

Related articles:

- IPv4 and IPv6 Addressing - Part 1: Overview of IP addressing
- IPv4 and IPv6 Addressing - Part 2: The network/host boundary and the IPv4 address
- IPv4 and IPv6 Addressing - Part 3: The IPv6 address
- IPv4 and IPv6 Addressing - Part 4: CIDR, VLSM & IPv6 addressing
- IPv6 testing: Tips you need to know
- IPv6-Only World On the Horizon
- Expanding the Embedded Universe: Migrating From IPv4 to IPv6
- North America is officially out of IPv4 web addresses — so what happens now?