IEN-156

Danny Cohen
U S C / I S I
September 7, 1980

CONTROLLED ROUTING IN THE CATENET ENVIRONMENT

This note suggests the use of Strict Source Routing, SSR, for gaining more control over the routes which are used for messages to traverse the catenet.

One of the cornerstones of the IN-philosophy is that users are completely separated from the low level transport issues such as routing.

While this is generally so, there are some real world situations where it is desired that users be given a way to influence the routing.

The ARPA Internet Protocol, IP, (see IEN-128), allows users to affect the routing decisions by using the source routing (SR) mechanism.

There are several reasons for users to influence the routing, rather than trusting the catenet to figure out the best route.

Some of these reasons are:

[A] Help the catenet find a destination otherwise unknown.

[B] Promoting the use of certain nets for reasons such as favorite tariff.

[C] Avoiding certain networks for reasons such as various sensativities.

The current source routing option of IP, as described in IEN-128 addresses mainly the first reason, [A], only.

In order to provide help to the catenet in figuring a route it allows the user to provide a sequence of addresses such that each of them is locally unique (hence unambiguous and known) where it is supposed to be interpreted. Obviously, this sequence must be continuous in the sense that at each address the next address in the sequence, must be known. The choice of route from each address to the next is left to the catenet to determine.

IP "assume"s that the given source route is a sequence of IP-addresses, each in the 32-bit format of 8/24 for the "NET-ID" followed by the "REST" which is typically a host address, including gateways.

However, this does not necessarily have to be so. If the NET-ID filed may include ESCAPE-CODES, as advocated in IEN-122, a much more powerful scheme may evolve.

The above scheme may be used in some clever way also for [B], the promotion of the use of certain nets. However, it does not provide an acceptable solution for [C], the avoidance of certain networks.

We argue that [C] is not a well formed requirement, and a tighter definition is required.

The reason for introducing the requirement to avoid certain networks is based on the classification of nets into friends and foes. If one knows about all networks, one could classify them all. But if some are unknown, they lack classification. In a controlled environment, where foes should be avoided, the unclassified nets must be avoided, too.

Hence, it is not enough to insist on avoiding the set of all known foe nets. One must insist, instead, on using only nets which are positively classified as friends.

Therefore, [C] should be changed from "avoiding known foes" into "using only well established friends".

Since the source routing technique which was described above does not tell the catenet how to route messages between the given addresses, it is possible for messages to be routed through foes while traversing a sequence of friendly addresses.

Hence, the above source routing technique is not adequate at all for [C], avoiding all foes.

In order to address this problem to following solution is proposed: Define a new variant of source routing, similar to the one described above, with the additional requirements that messages cross network boundaries only at the gateways specified in the source route.

If there is no DIRECT connection, meaning through a single network between two successive addresses in the source route, the message should be discarded rather and no attempt is made to reach the next address via another intermediate network (and gateways).

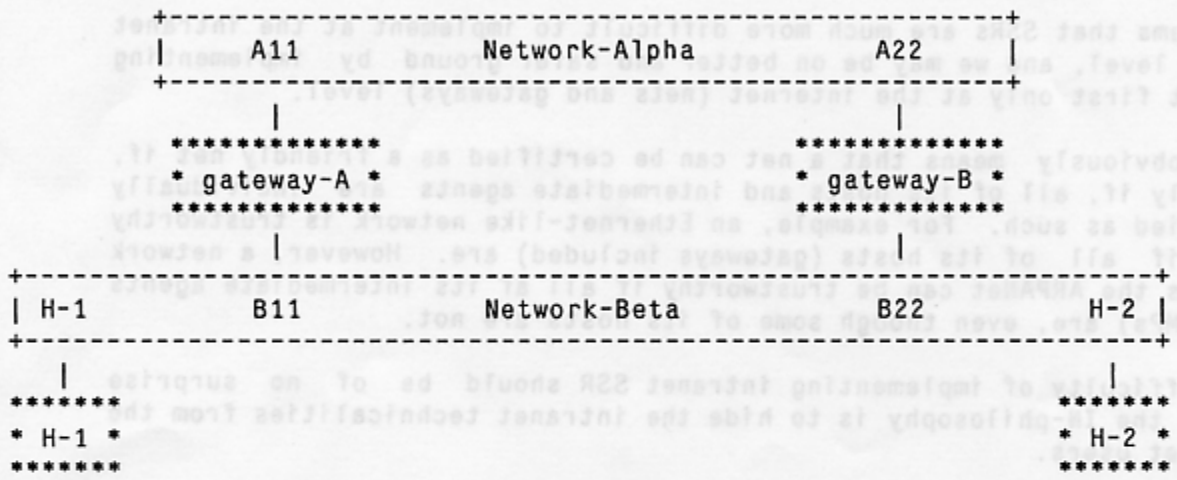
If this new option of Strict Source Routing, SSR, is adopted then it is up to the users to construct "safe" SSRs which include only networks and gateways which are positively identified as trustworthy friends and are known to have only gateways which are sure to handle the SSR properly.

The source routing which is not SSR may be referred to as an LSR (Loose SR).

One may view the LSR as "piecewise end-to-end" routing at the IP (gateways) level, as opposed to the SSR which is a kind of hop-by-hop routing at the same level.

The notion of a gateway being specified in a SSR has to be clarified. Gateway per se do not have IP addresses, but their interfaces to local networks do. Under SSR when the address Ni/Hj (Network/Host) is specified for a gateway, it is required to reach it through the network Ni even in the cases that other routes are available.

Consider the following example:



If the SSR specifies the address (Alpha/A11) followed by the address (Beta/B22) then the only accepatble route is to cross Gateway-A and then to traverse the Network-Beta to B22. It is not acceptable for the Gateway-A to recognize that (Beta/B22) is actually a gateway which is also on Network-Alpha and therefore to route through this network to (Alpha/A22) expecting the message to cross Gateway-B there.

Hence, H-1 can force his message to get to H-2 through the Network-Alpha by using the following SSR: (Beta/B11)-(Alpha/A22)-(Beta/H-2). If the Network-Alpha breaks between A11 and A22 this SSR will result in a communication failure, even though good routes through Network-Beta only are avilable, and might have been automatically used if LSR was used.

ON INTRANET SSR

It is possible to carry the foes and friends classification further from the nets (internet) level down into the hosts (intranet) level. One way to achieve that effect is by "teaching" the half-gateways which are in each host about SSRs.

However, in this case the definition of DIRECT connection has to be explicitly defined for each network. In the case of the ARPANET hosts cannot have this notions which is at the IMPs level. In the case of broadcast nets (such as satellite based, packets radios, Ethernet-like or ring-like nets) no connection is "direct enough" even though it has no intermediate agents along the way.

It seems that SSRs are much more difficult to implement at the intranet (host) level, and we may be on better and safer ground by implementing SSRs at first only at the internet (nets and gateways) level.

This obviously means that a net can be certified as a friendly net if, and only if, all of its hosts and intermediate agents are individually certified as such. For example, an Ethernet-like network is trustworthy only if all of its hosts (gateways included) are. However, a network such as the ARPANet can be trustworthy if all af its intermediate agents (the IMPs) are, even though some of its hosts are not.

The difficulty of implementing intranet SSR should be of no surprise since the IN-philosophy is to hide the intranet technicalities from the internet users.

CONCLUSION

A Strict Source Routing could be used by a set of "certified friendly" networks in order to avoid the transmission of certain datagrams through all the networks which are parts of the catenet but are not as trustworthy as others.