NAME

sr-ally – IP Alias resolution pairwise test

SYNOPSIS

sr-ally <first IP address or name> <second IP address or name>

DESCRIPTION

Ally is the tool that executes the IP identifier-based pairwise alias test to discover whether two IP addresses belong to interfaces on same machine. The source-address based test is also supported, and if undns is installed, name-based alias resolution is used when routers are unresponsive or unreachable. We describe each technique in turn, then present example output.

IP-identifier based alias resolution seeks evidence that the two IP addresses share a single IP-id counter. The IP identifier field is intended to make each packet unique so that it can be reassembled after fragmentation. It is commonly implemented as a counter, or not used at all, though some have made a case that it should be randomized. If packets generated by two different IP addresses have in-order IP identifiers, it is likely, but not certain, that those IP addresses are aliases. This is the technique developed in the Rocketfuel project.

Source-address based alias resolution relies on routers that use the outgoing interface address as the source of ICMP port unreachable messages. The source address to use is unspecified and up to the implementor, so sometimes this is not used. It is, however, the most accurate way to show that addresses are aliases.

Name-based alias resolution exploits the structure of DNS names in certain ISPs to determine whether addresses are aliases. The advantage is that DNS provides information about addresses that may not be responsive or routable for probe traffic. This method is only available with undns installed; it is used to parse DNS names.

The output of the script is either "ALIAS!", "NOT ALIAS.", or "UNKNOWN", followed by an explanation.

OUTPUT EXAMPLES

Some of these examples may still work when you read this. The explanation after the verdict is intended for debugging, not for parsing and use, so may change. This section is intended to document the types of responses you might observe.

> sr-ally 128.95.3.100 128.95.4.100
ALIAS! ally/ipid: 53416, 53417, 53422, 53423

These addresses are likely aliases by IP identifier. The identifiers received (following the colon) are nearby and in order. In general, ally/ipid should be verified later to ensure that it is not simply luck that caused the two counters to be equal.

> sr-ally 66.250.15.81 66.28.4.161
ALIAS! mercator/source address rate limited: 66.250.15.81->66.28.4.161 66.28.4.161->66.28.4.161

Both IP addresses returned port unreachable messages with the same source address. The common source address may not be either of the addresses. It is common for these routers to also rate-limit outgoing responses, which means the IP identifier test has less input. Rather than force more packets to show that the IP identifier test worked, we accept the source address approach. It is also possible for each IP address to send responses from the other to indicate an alias.

> sr-ally 198.107.150.52 140.142.150.24
ALIAS! ally/ipid; presumptive (second round had no responses): 8699, 8700

The first pair of packets both received responses, while the second did not. Ally claims these are aliases if they are within some small threshold. In general, it is worth re-running presumptive aliases, but in this case, they are very likely aliases as the IP identifiers are adjacent.

> sr-ally 205.171.21.121 205.171.21.150
ALIAS! name: atlcore02inet.qwest, otherwise two unresponsive: 205.171.21.121 and 205.171.21.150

Both addresses were unresponsive, but Undns saves the day, recognizing that both are named as belonging to a "core" router in Atlanta (atl) numbered "02".

> sr-ally 128.95.2.100 128.95.4.100
NOT ALIAS. quick (2): 37523, 56759

Tells that those addresses are not aliases because their IP identifiers are too different. Only two packets were used as an optimization. This is the most common response.

> sr-ally 154.54.10.110 154.54.2.198
NOT ALIAS. disparate ids: 56086, 56094, 56112, 56087

When addresses aren't immediately disproven by being too diverse in the first pair of packets, the second pair of packets may show them out of order.

> sr-ally 205.171.8.146 205.171.21.94
NOT ALIAS. name: atlcore01inet.qwest != atledge07inet.qwest and one unresponsive: 205.171.8.146

Because one of the two addresses was unresponsive, Undns was consulted. It's verdict was that the two are not aliases based on an understanding of Qwest's naming convention.

> sr-ally 128.83.10.14 205.171.8.250
UNKNOWN. two unresponsive: 128.83.10.14 and 205.171.8.250; undns failed: ser11-msfc-v708.gw.utexas.edu lacks unique fragments

Neither IP address returned any information. Undns is installed, but failed to yield an answer, as it has not been programmed with the naming convention of "utexas.edu" routers.

> sr-ally 38.118.132.98 205.171.8.146
UNKNOWN. one unresponsive: 205.171.8.146; undns failed: 38.118.132.98 host not found

One of the two IP addresses did not respond. Undns is installed, but doesn't work when either of the IP addresses lack DNS names.

> sr-ally 18.201.1.3 165.123.237.15
UNKNOWN. one unresponsive: 18.201.1.3; undns failed: RADOLE.LCS.MIT.EDU lacks unique fragments

One of the addresses was unresponsive. Although Undns knows a little about MIT's naming convention, this name is not recognized and is perhaps not a router.

EXIT STATUS

sr-ally exits 0 if the addresses are aliases, 1 if they are not, and 2 if unknown.

REMOTE EXECUTION

Different vantage points may increase the effectiveness of the source-address based test. Using them, however, prevents the use of undns. It is suggested that you run sr-ally locally as needed, or "require" it into your script.

BUGS

Send bug reports or suggestions to <bugs@scriptroute.org>.

I'd welcome an equation showing the likelihood of a false positive in ally/ipid related to how fast the IPID counter is moving, so that a confidence value can be provided using the IPID method.

AUTHOR

Neil Spring <nspring@cs.washington.edu>

SEE ALSO

sr-remotely.rb(1)