Needs

- IP spoofing counter measures that play well with existing infrastructure

- Packet forwarding is done on destination IP, with no concern for source, which permits IP spoofing. This faciliates numerous types of network attacks, such as Denial of Service and Man in the Middle. A forwarding protocol which either eliminates or gravely reduces the likelihood of spoofing effectively prevents these issues at the source.

-

1 Notes

- Currently techniques aim to traceback packet flows in order to identify the malicious source. Others try to protect the destination.

- Tags should not be changed often to avoid the overhead of relearning. But static tags present a possibility of theft. Perhaps, the tags could evolve over time, perhaps in every minute interval, with a set function being applied to them. This could mirror the use of unix intervals in the OTP schema used by google. Instead of [prefix, tag] being stored and indexed, it could be [prefix, raw$_t ag, mask].Eachtaggingrouterwouldusebitwiseoperationsonboththemaskandth$
$30s).Thiswouldensurethatifatagwascompromised, itwouldonlybevalidforashortduration.Onlywhena$
$maskbestolen.$