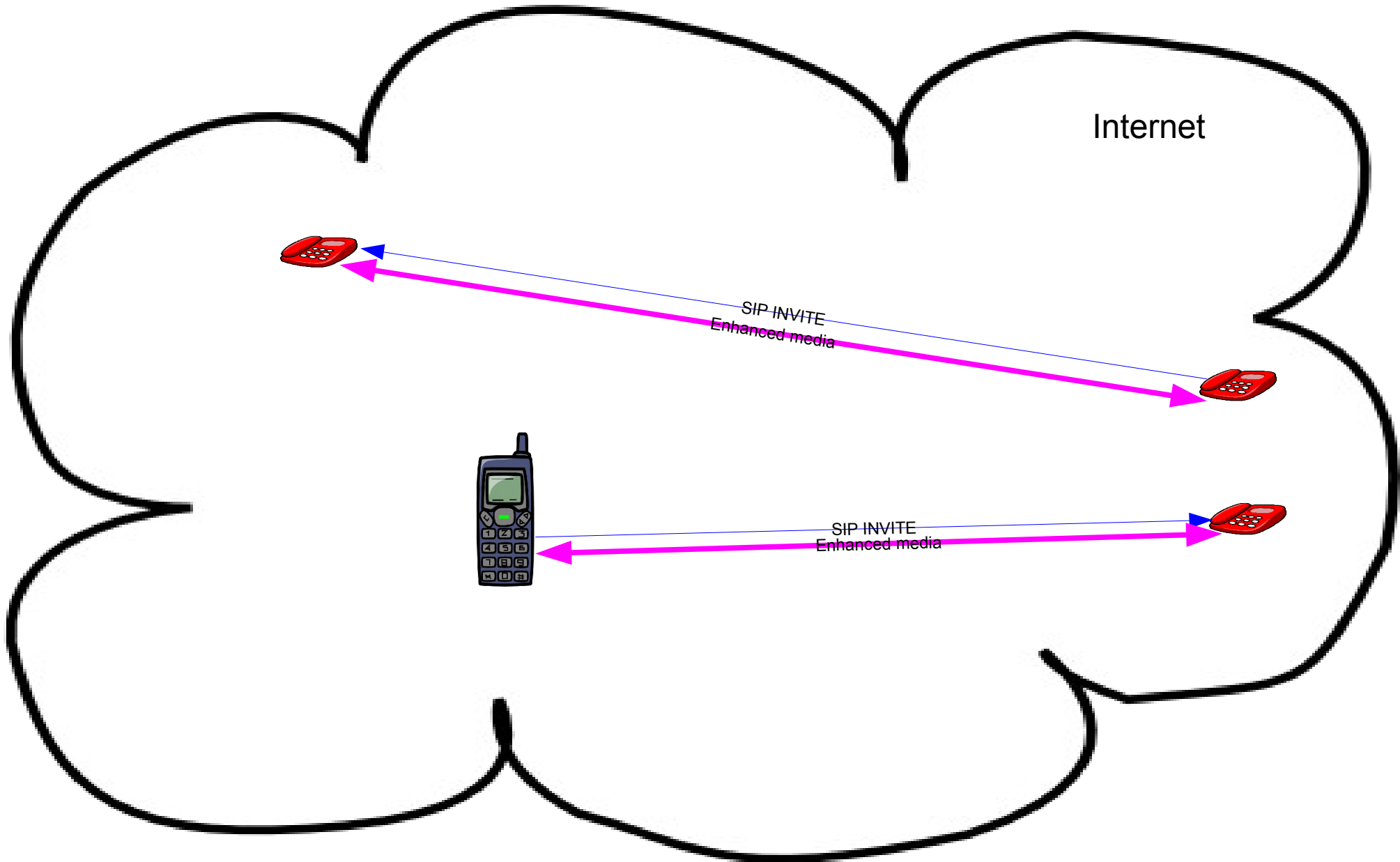
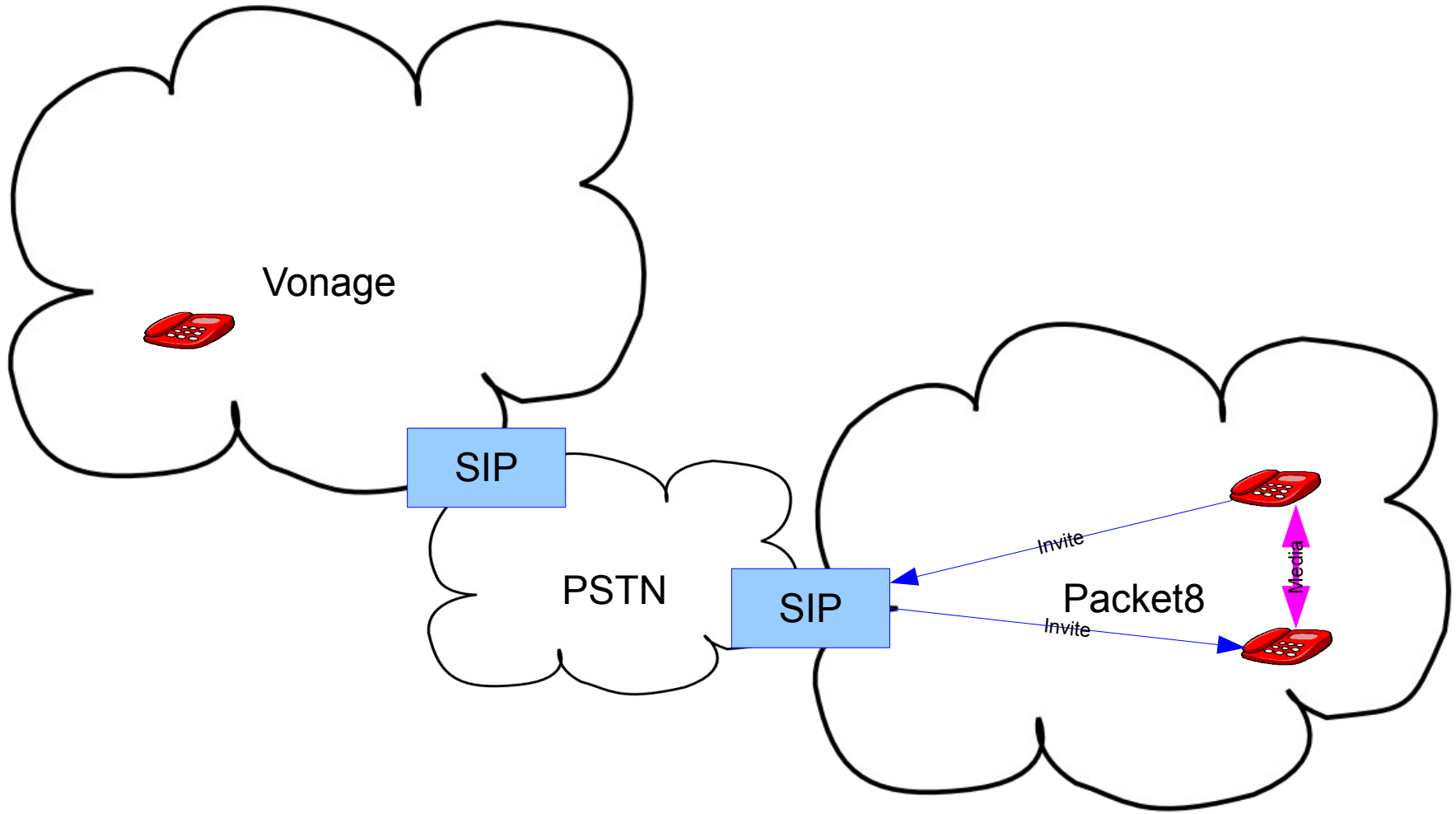
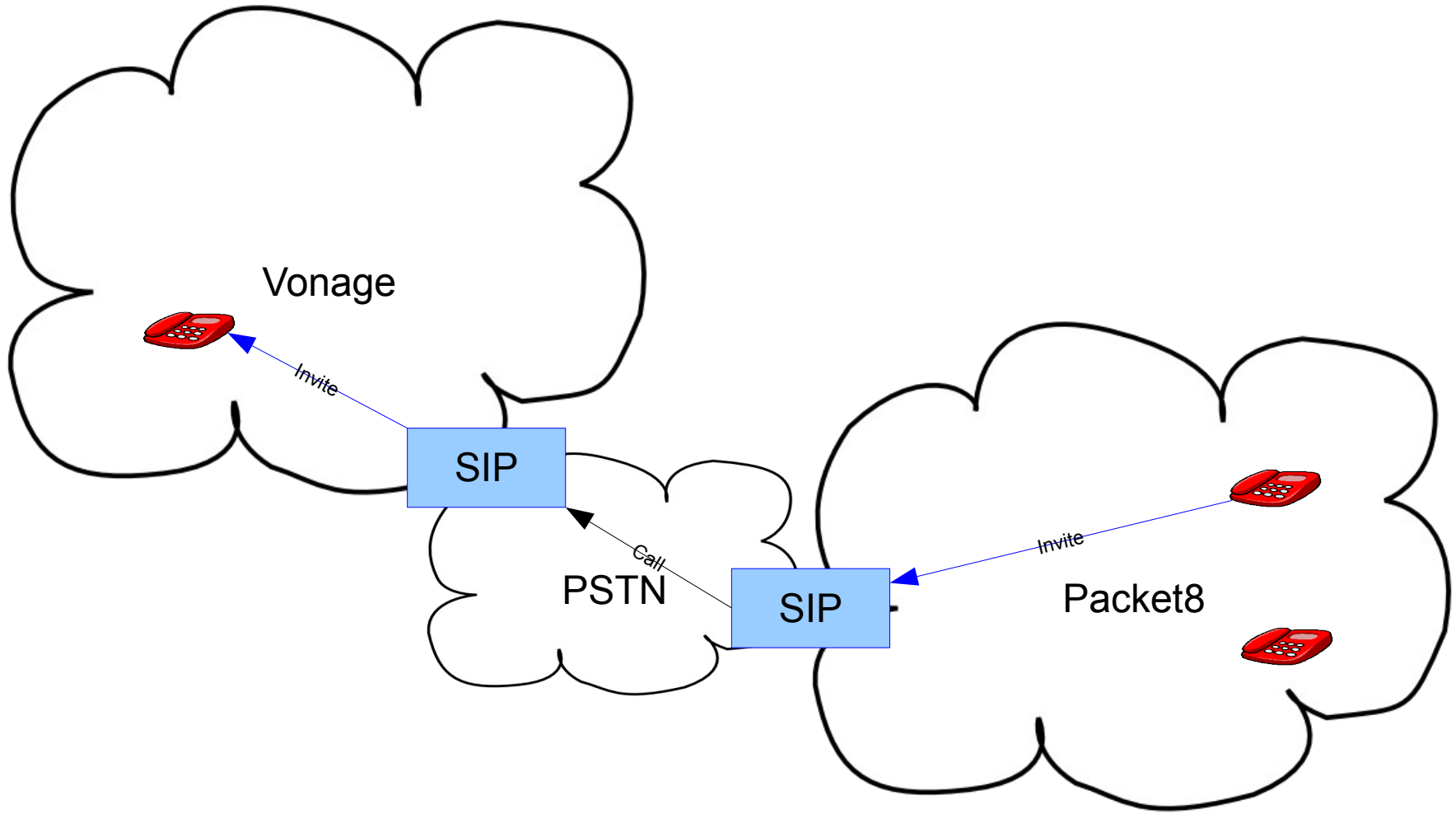


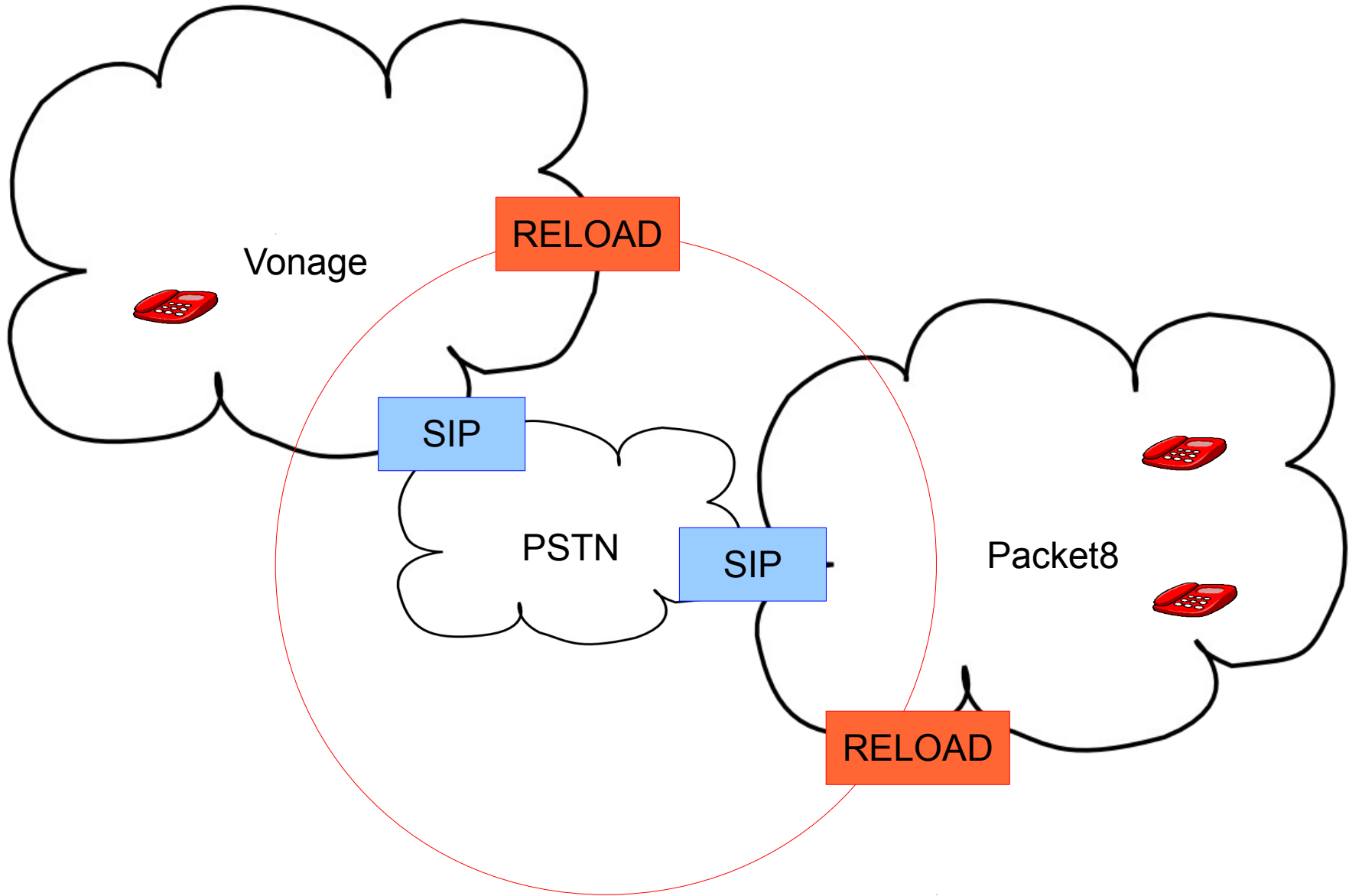
VIPR

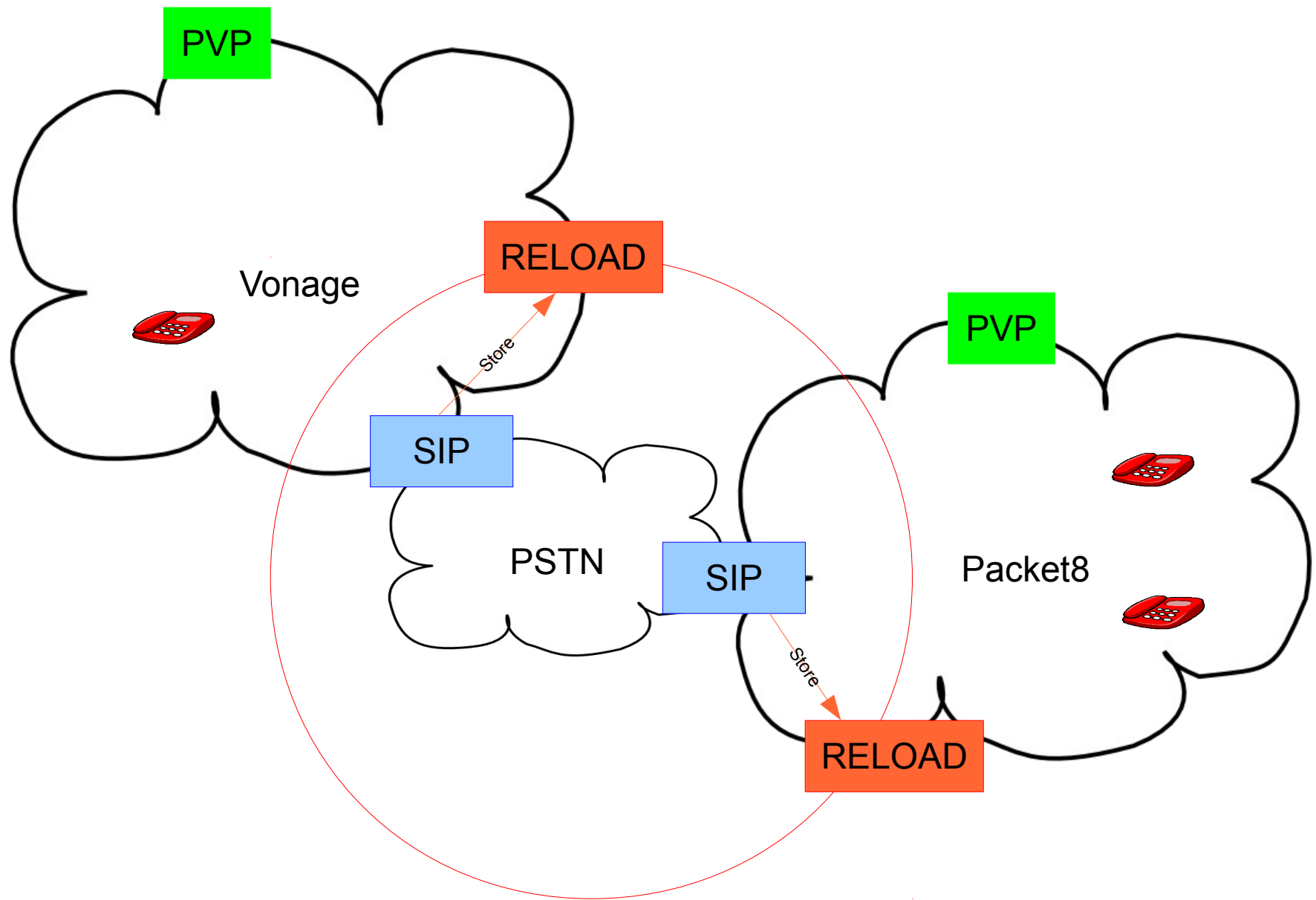
Marc Petit-Huguenin

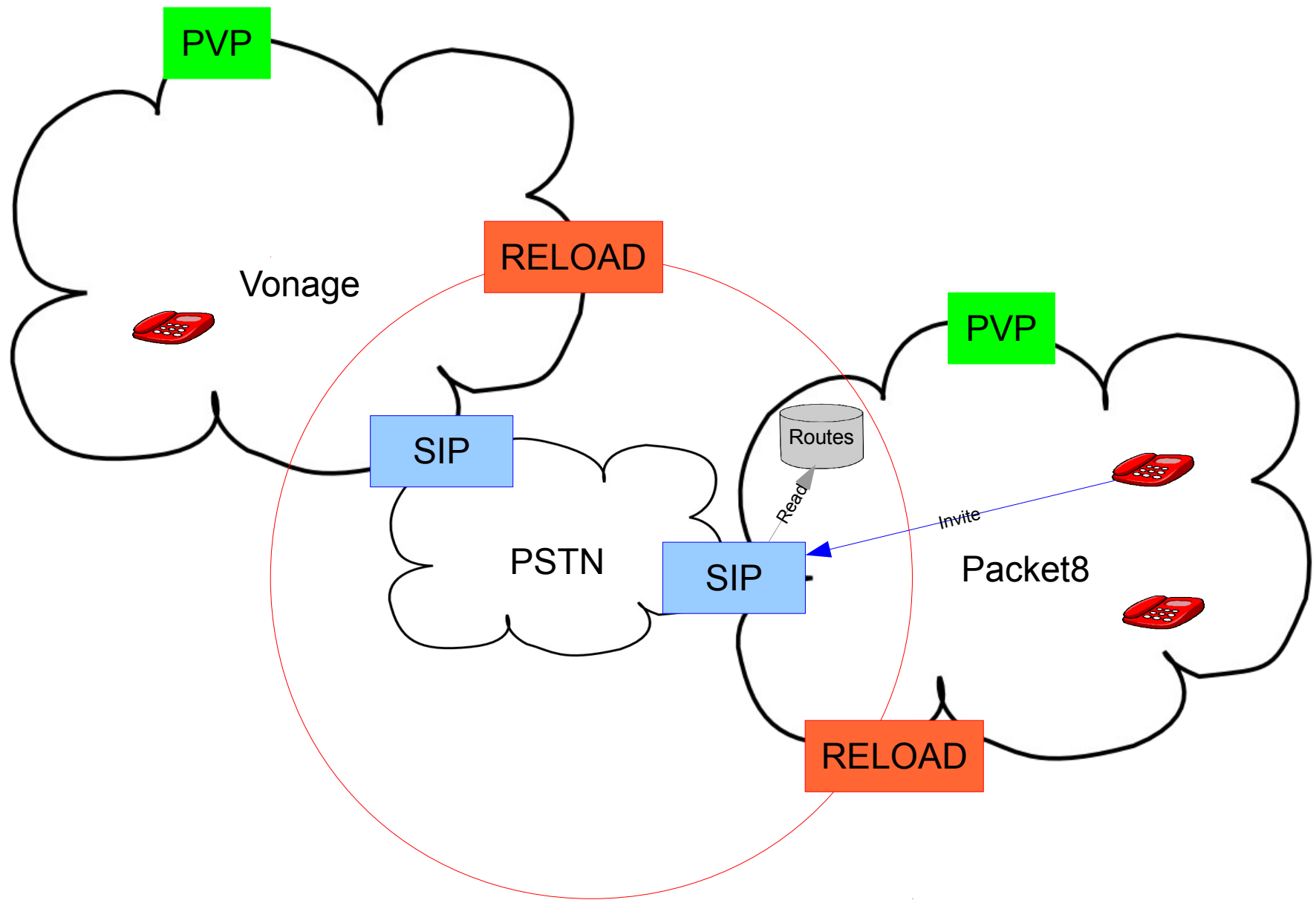


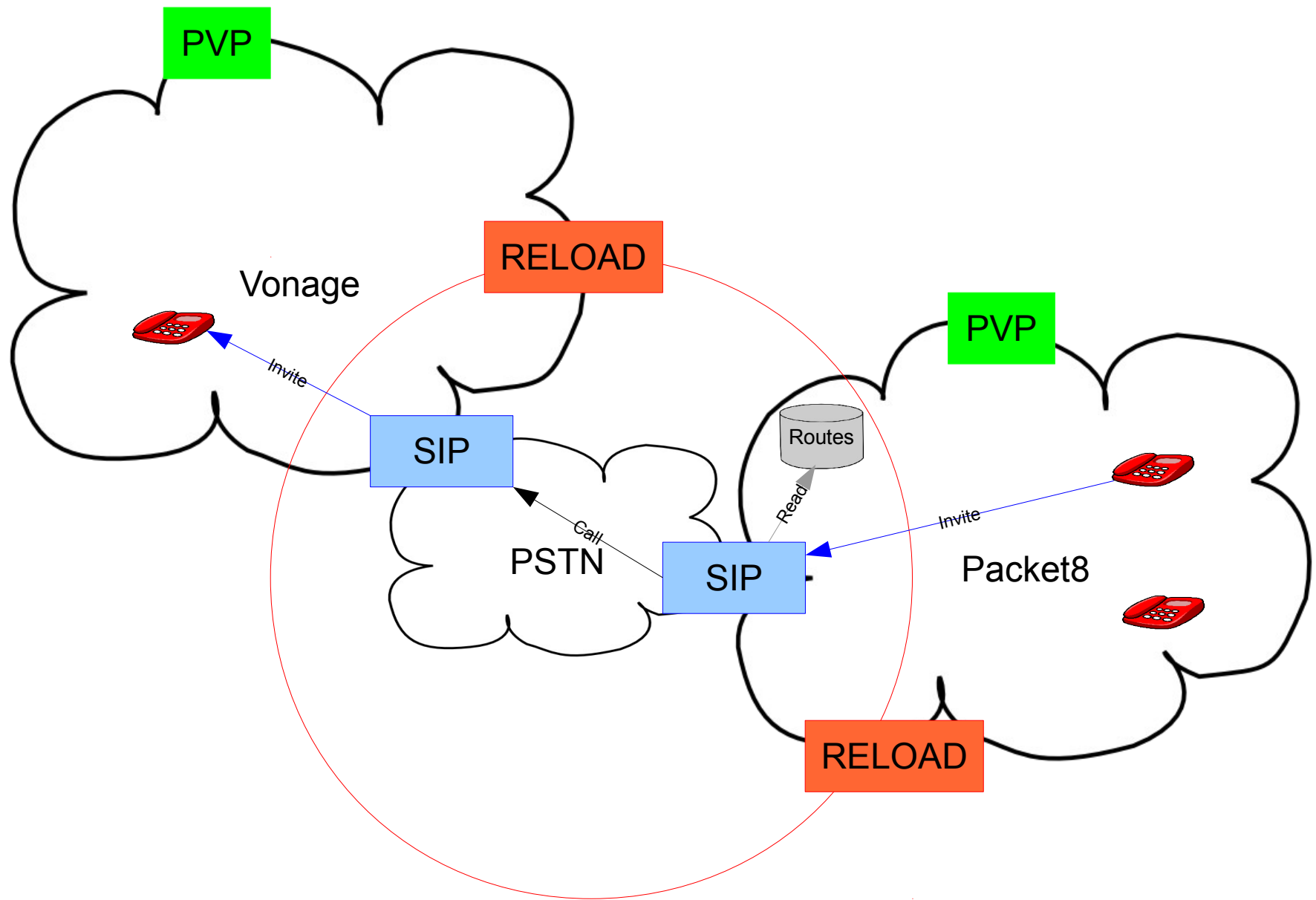


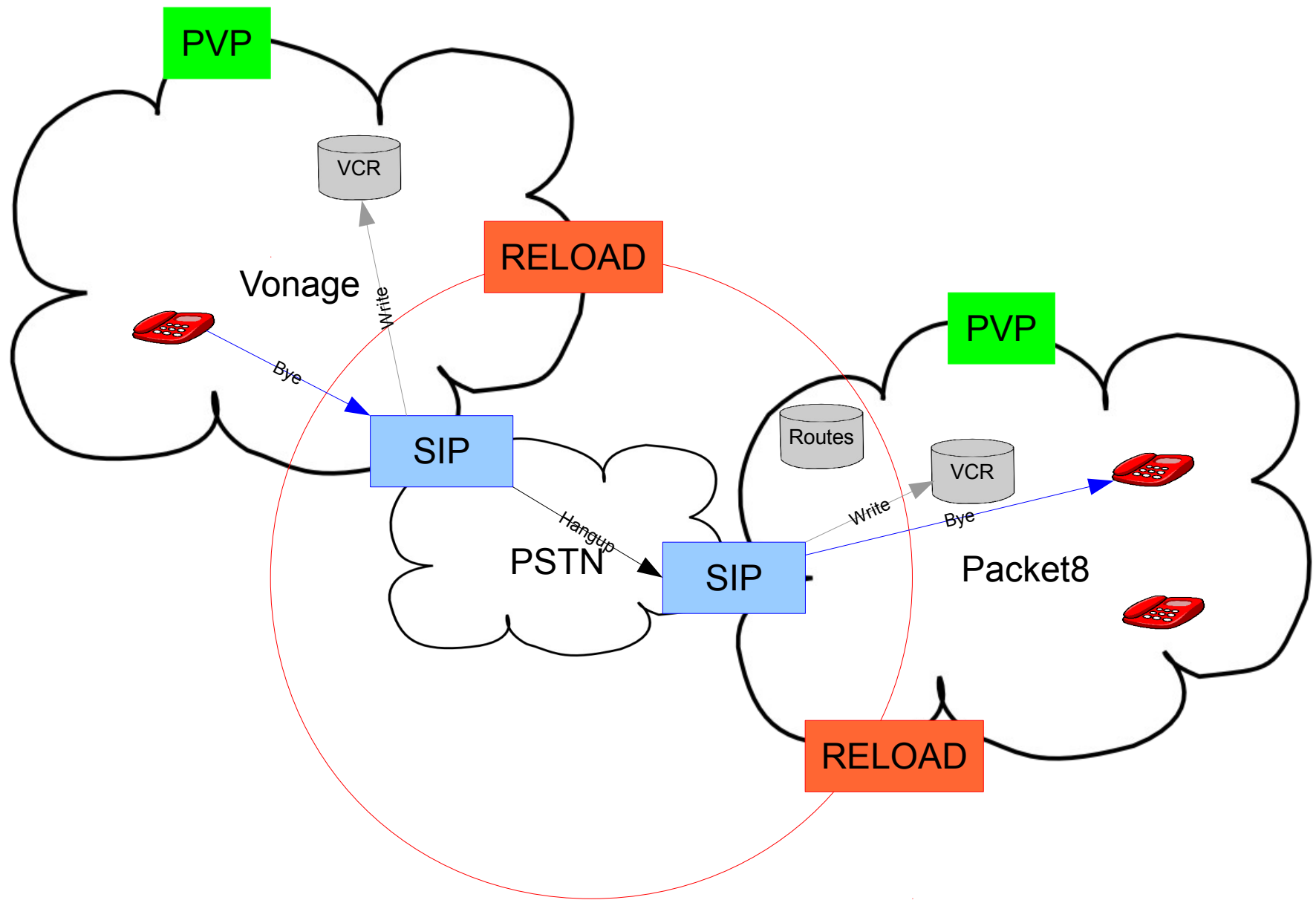


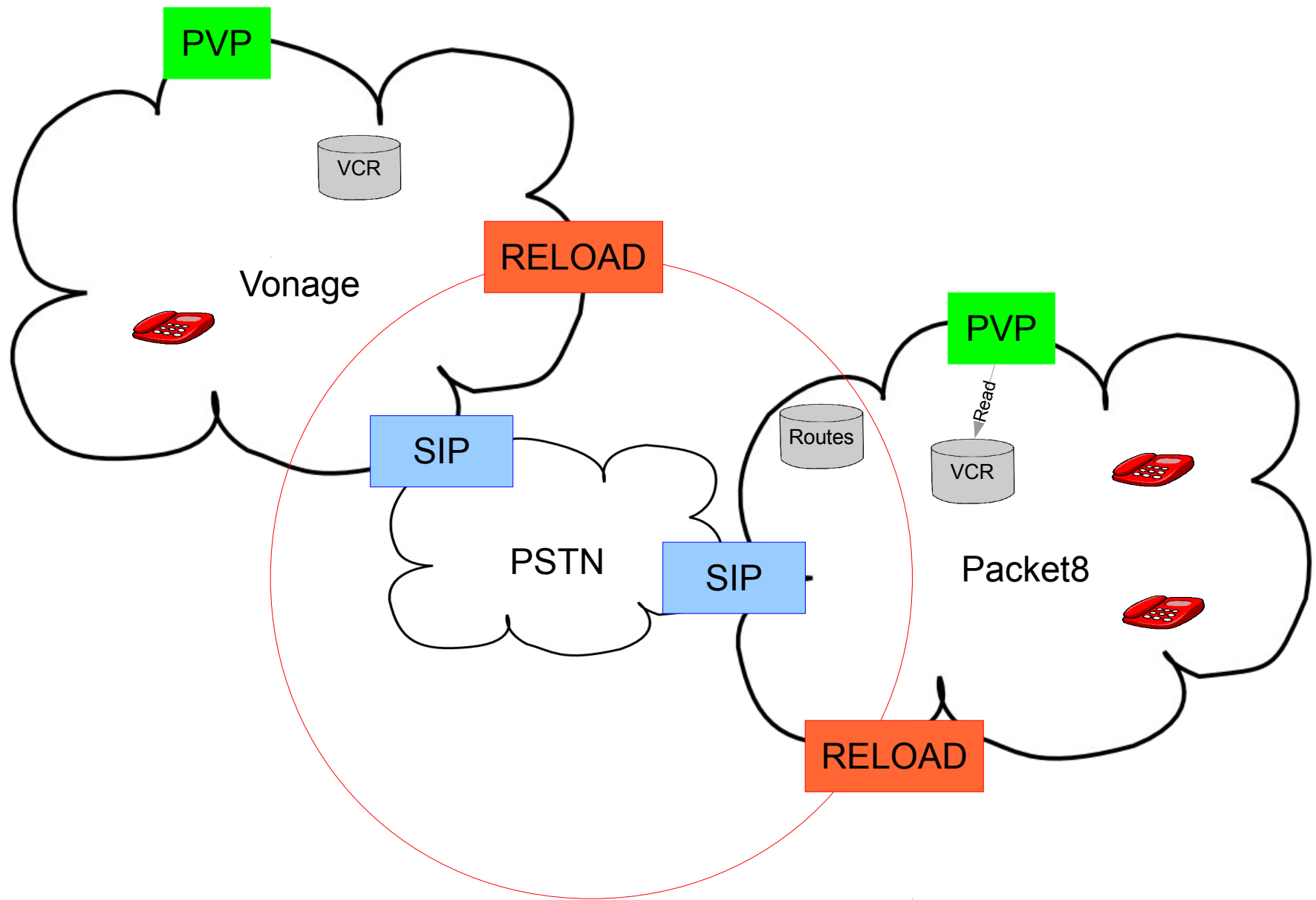


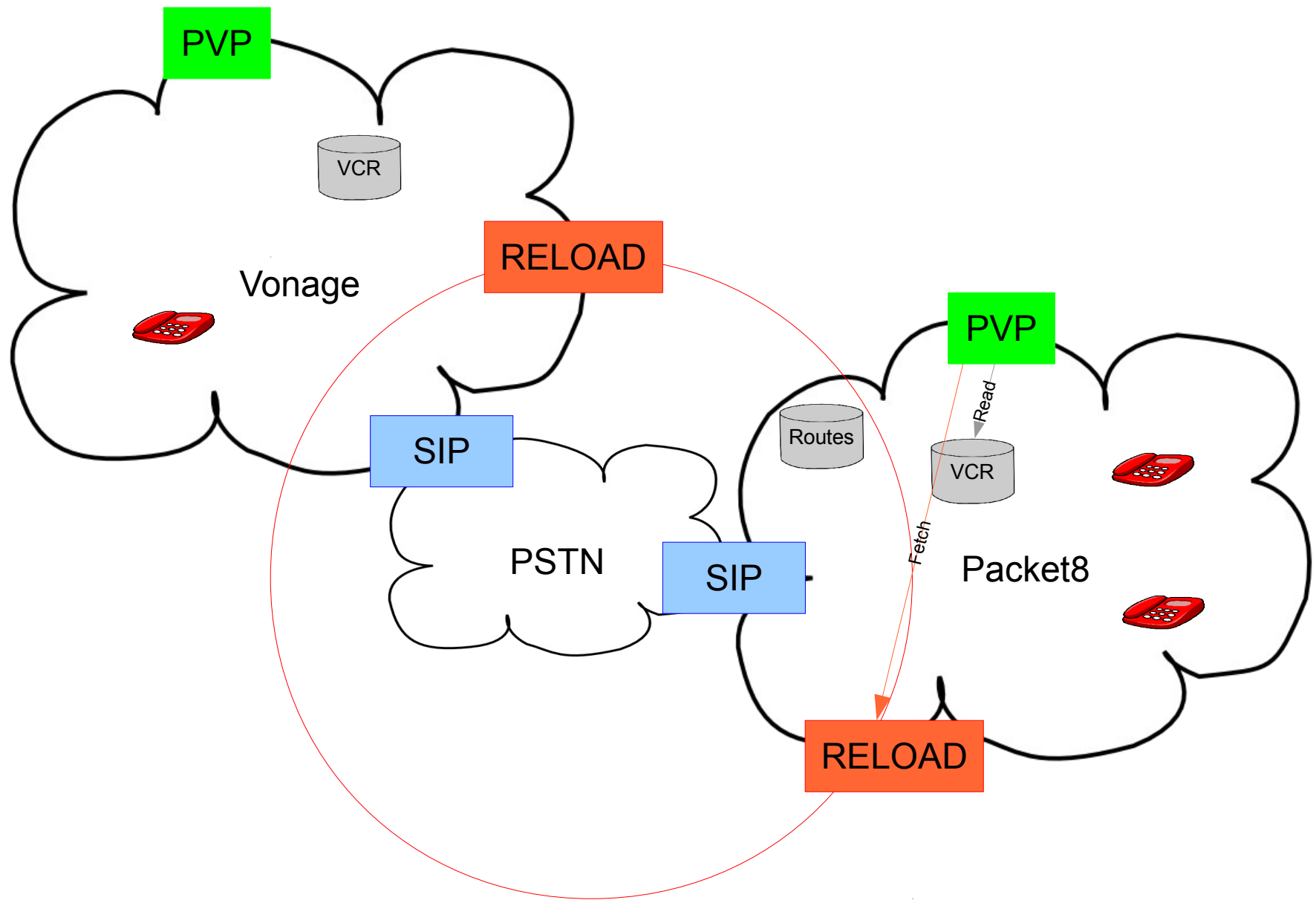


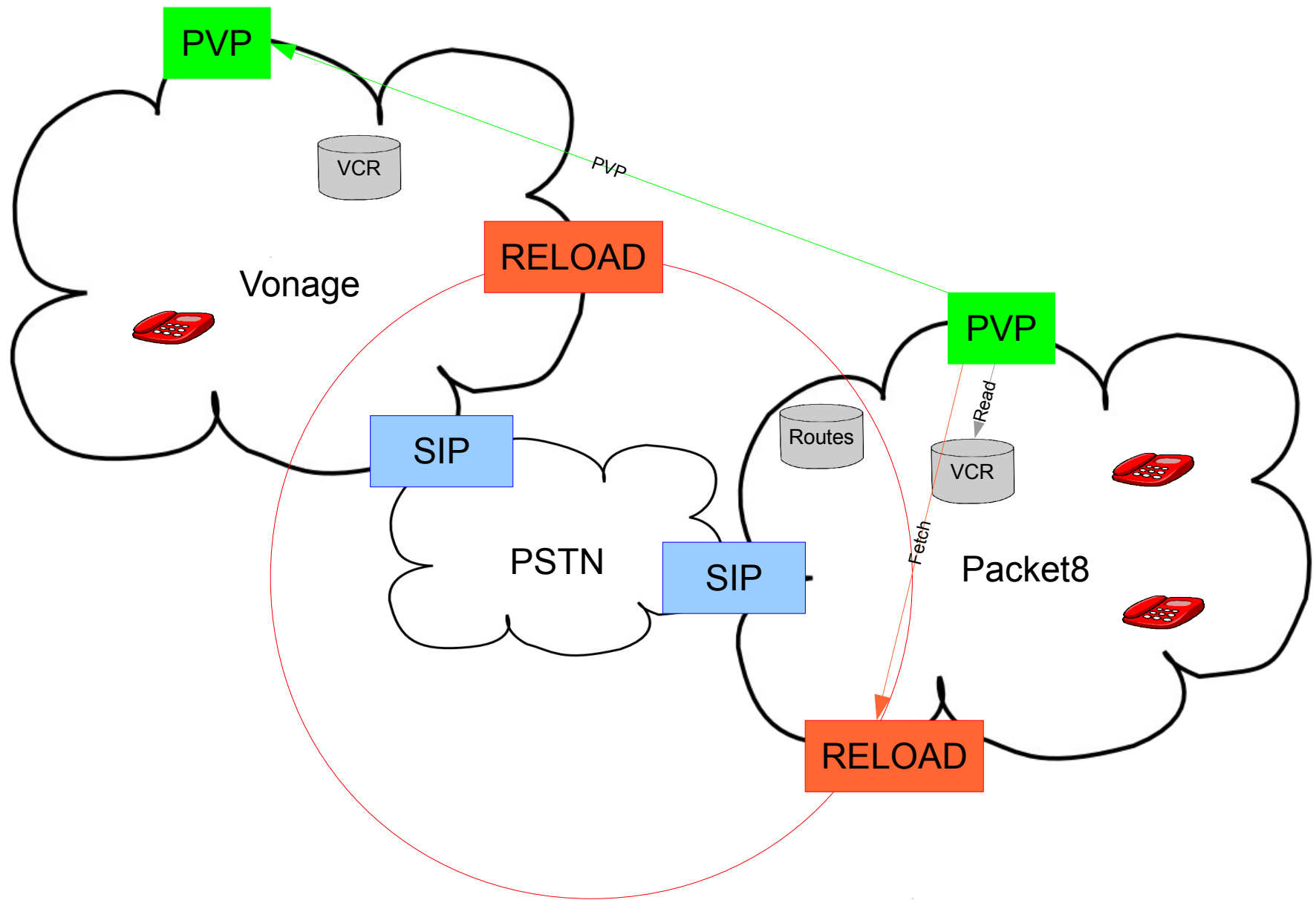


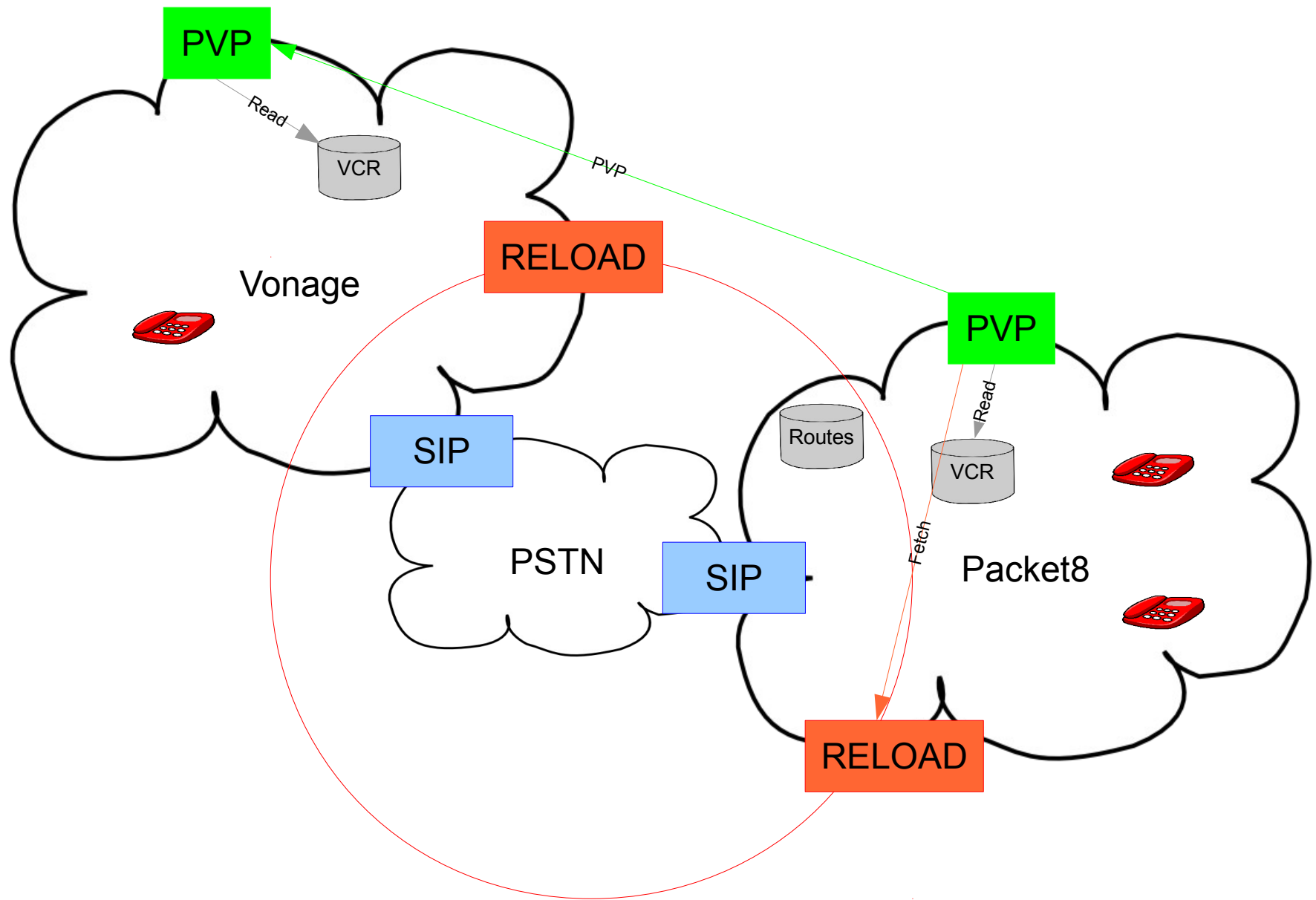


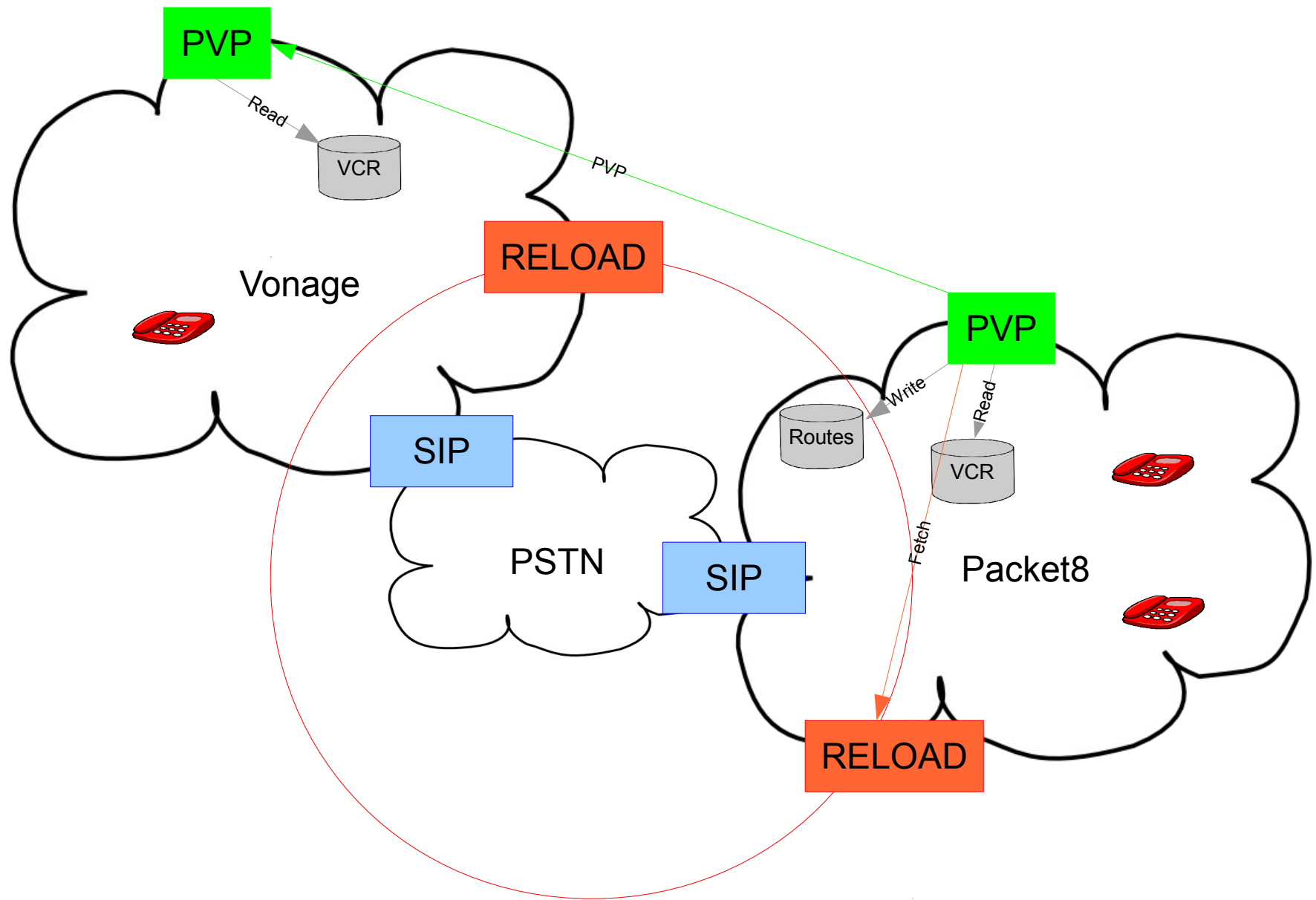


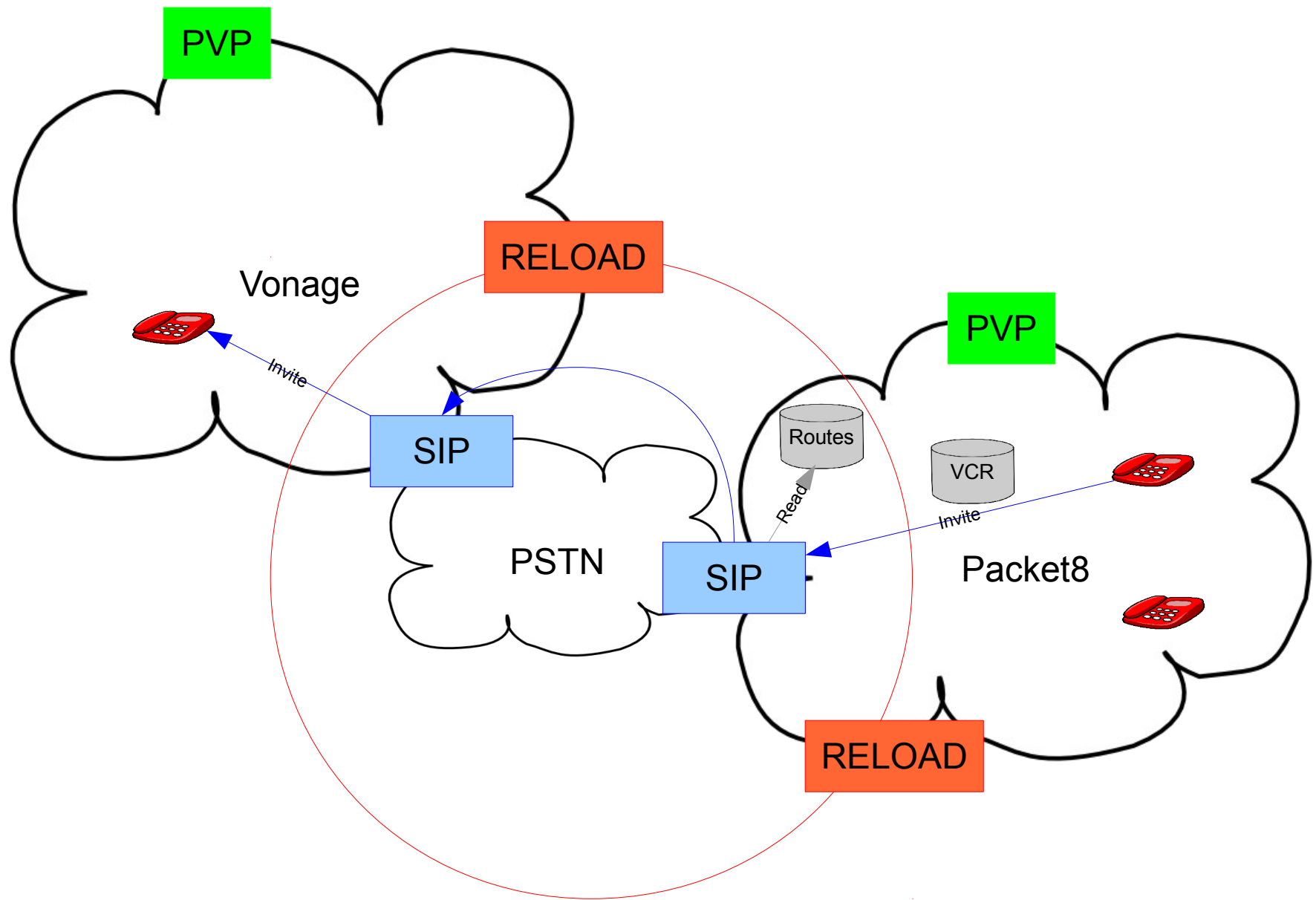


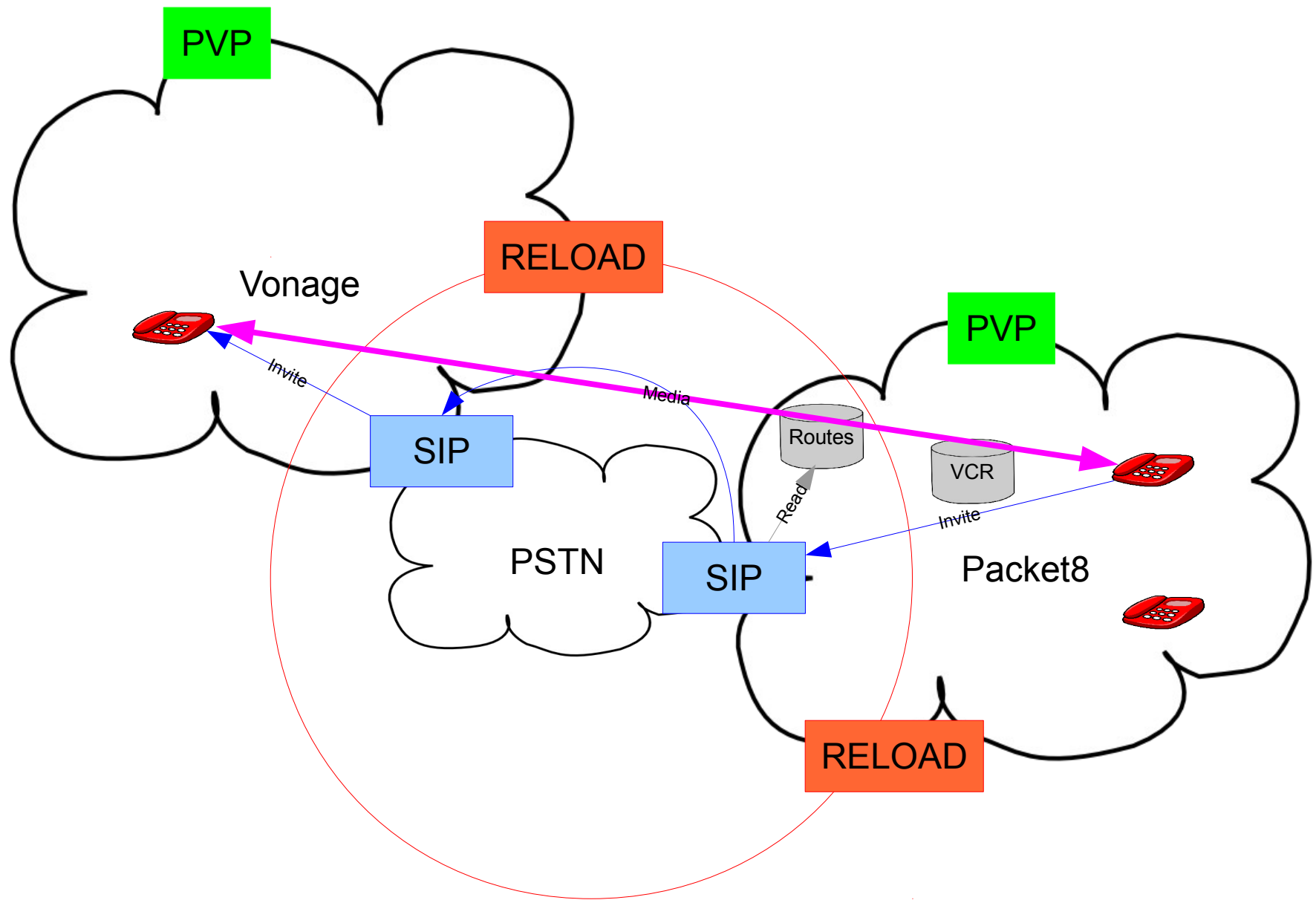






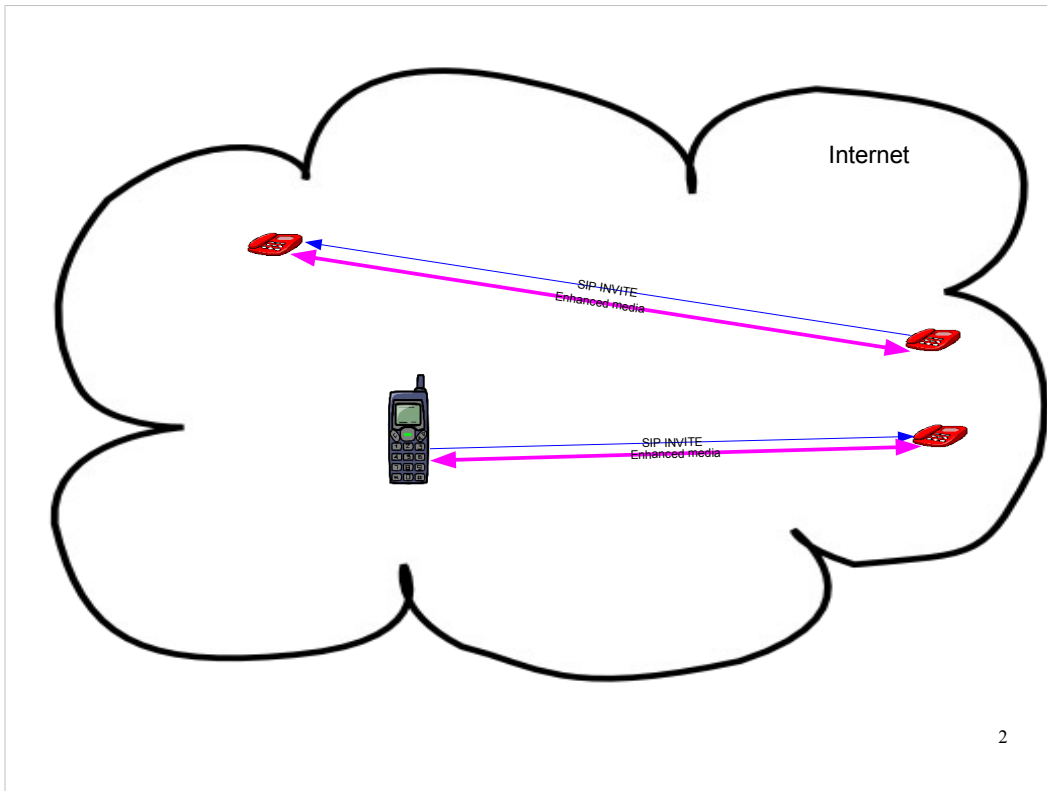






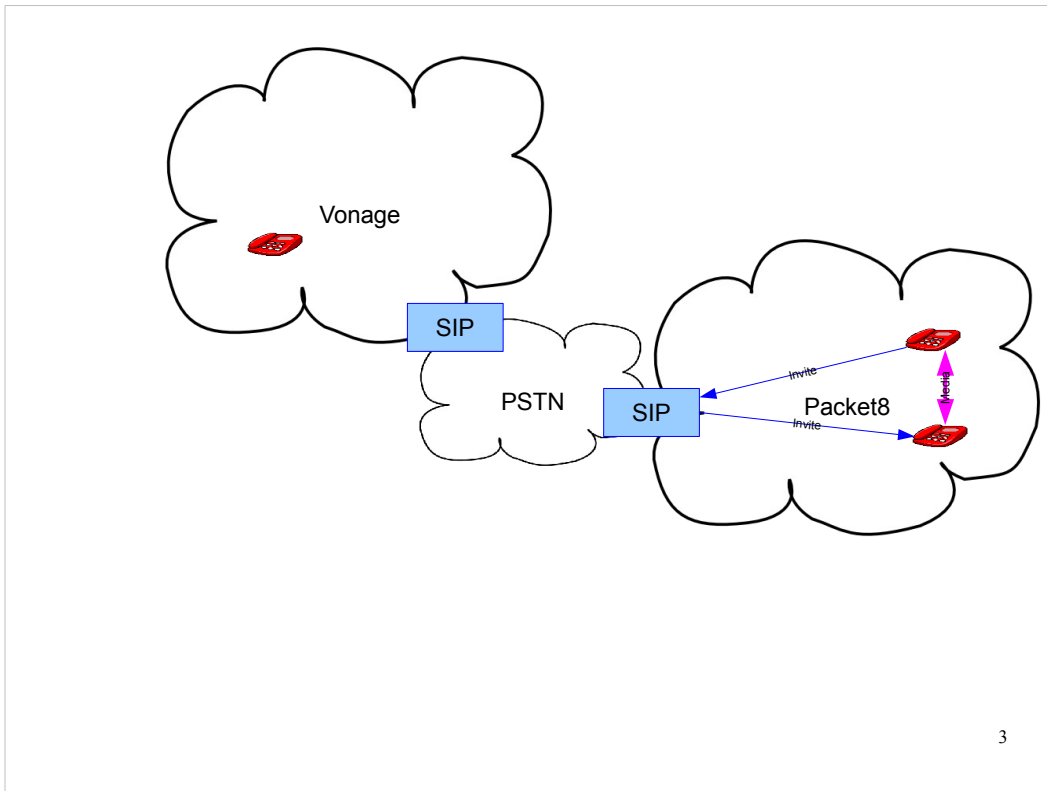
VIPR
Marc Petit-Huguenin

Copyright © 2010, 11 Stonyfish Inc.

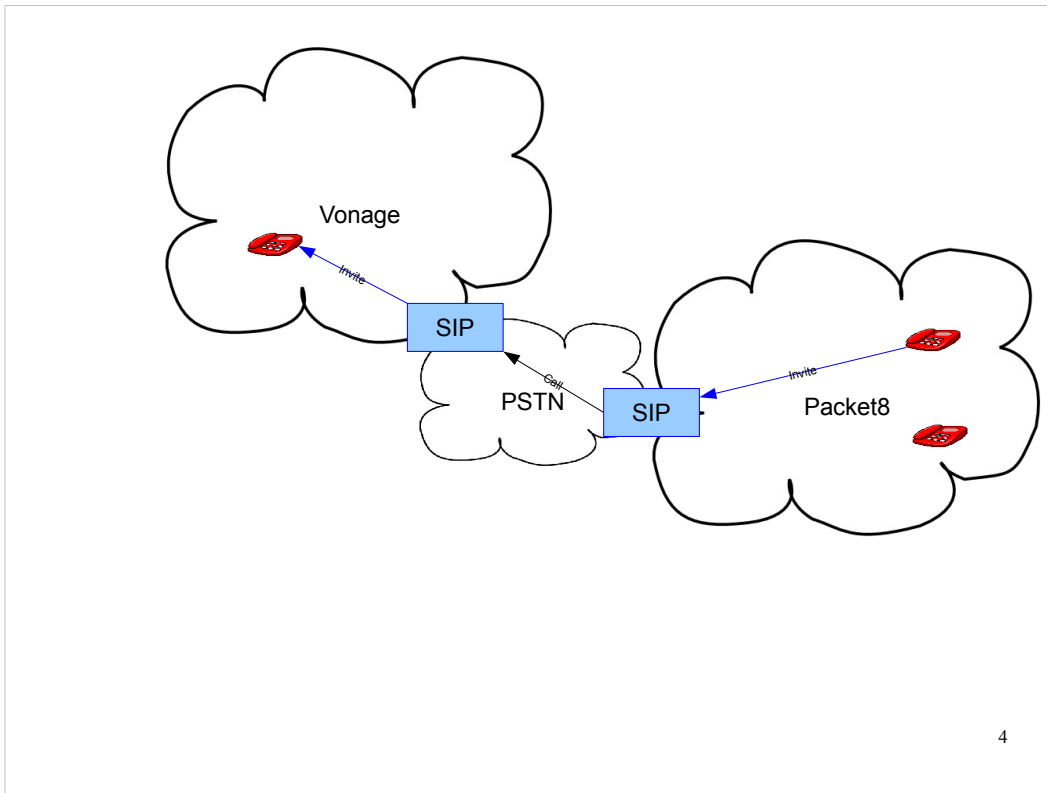


2

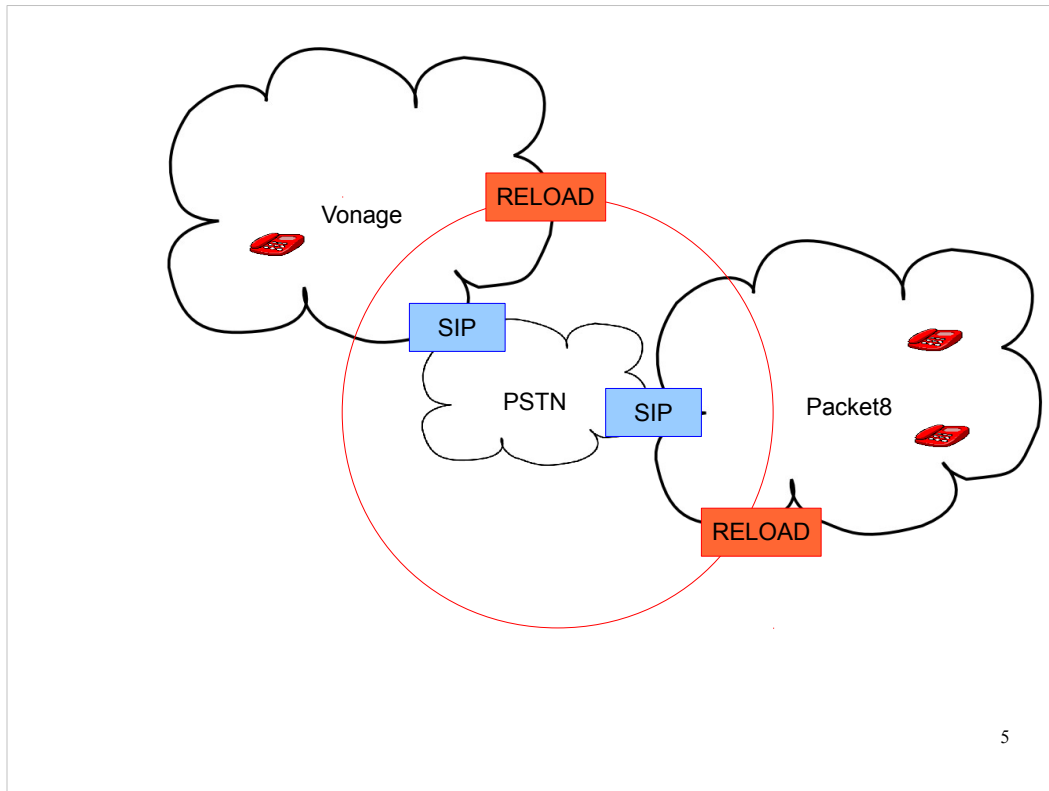
In a perfect world, VoIP would work the same way than emails, and everybody would be able to connect directly to everybody else, and using any possible media between the endpoints.



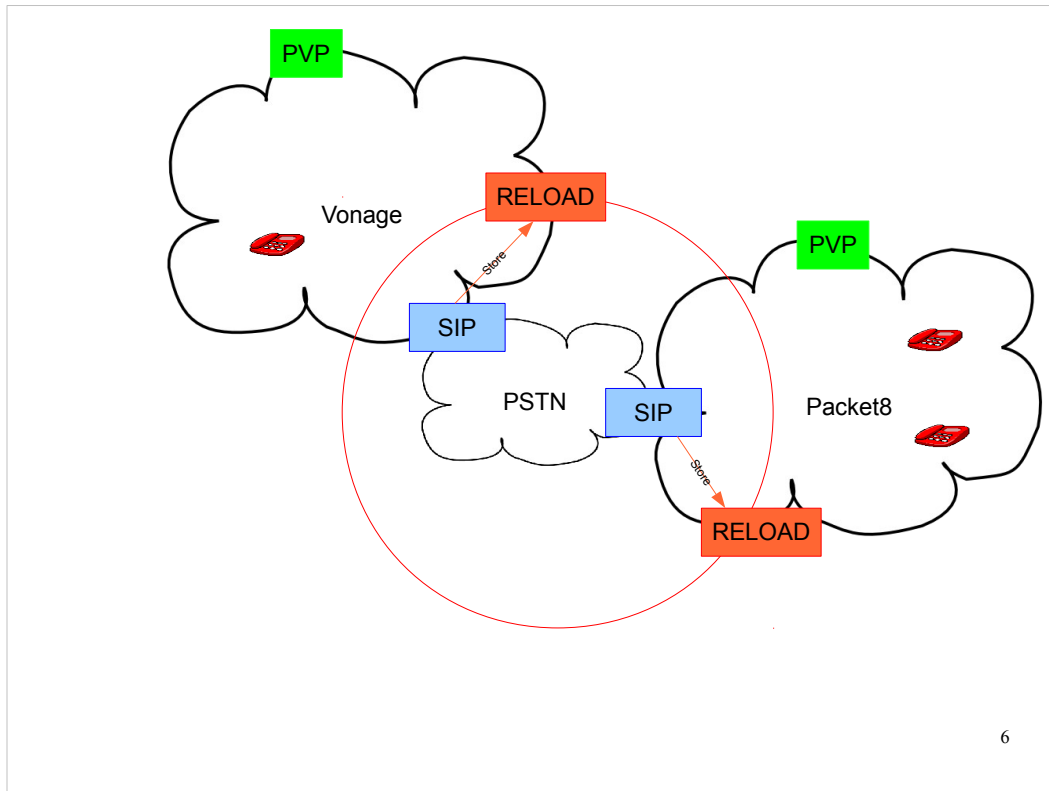
Unfortunately we do not live in such a world.
Endpoints are federated by VoIP providers, inside
which it is possible to use enhanced media.



But as soon as an endpoint in one VoIP provider wants to call an endpoint in a different provider, the call has to go through the PSTN, which limit the media available to narrowband voice.



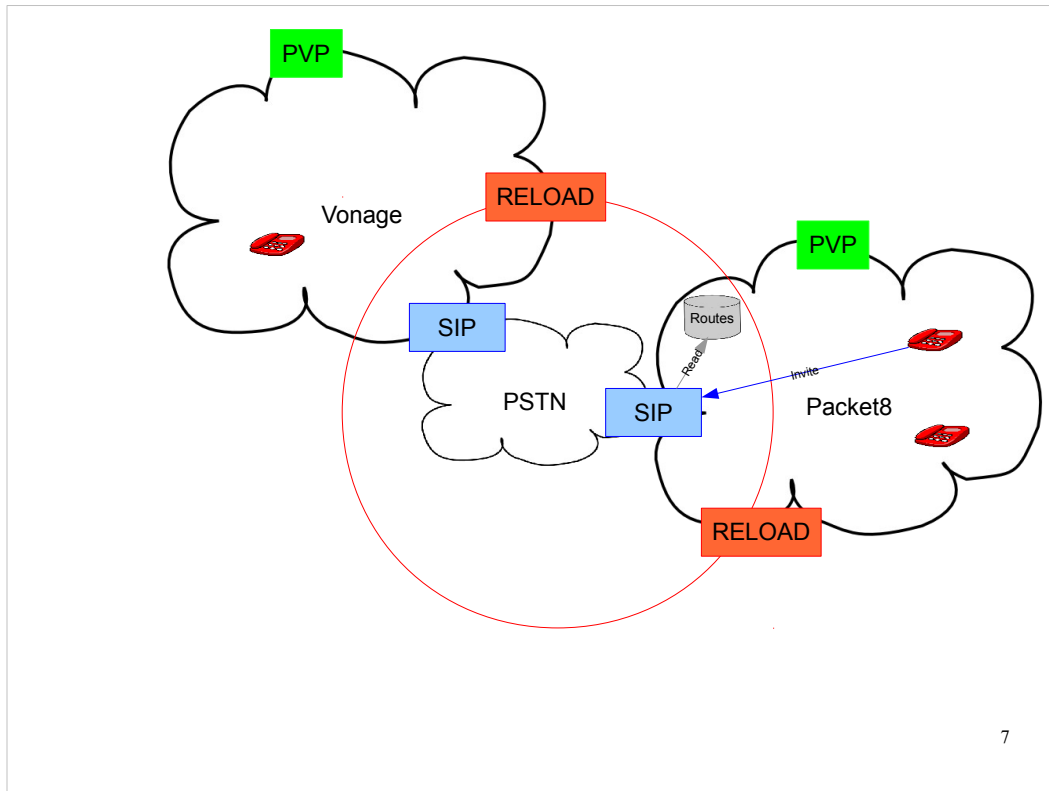
The first step of VIPR is to add a distributed database based on the RELOAD protocol. Each VoIP provider installs a number of RELOAD servers, proportional to the number of phone numbers in their domain. A set of RELOAD servers is known as an overlay, and is used to store and fetch pieces of data in a distributed, redundant and secure way.



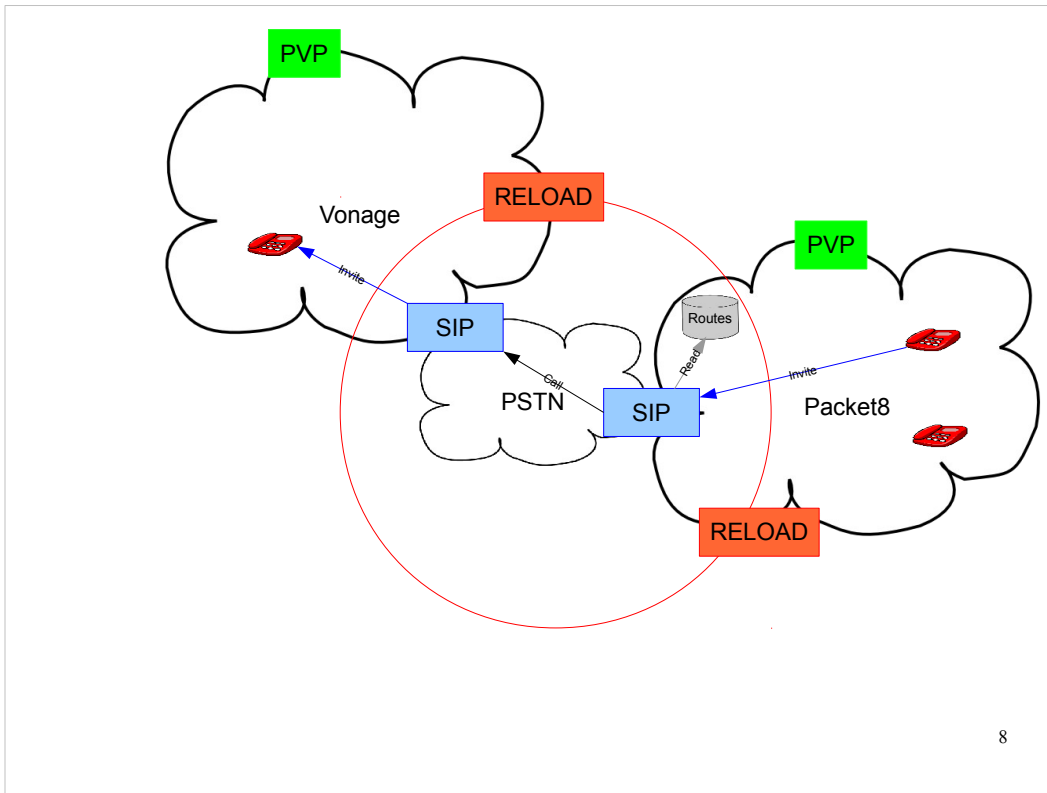
The SIP proxy of each VoIP provider stores in the VIPR overlay a mapping between each of the E.164 numbers it is responsible for and the indirect IP address and port of a PVP server.

These mappings are subsequently available to each client of the VIPR overlay for retrieval.

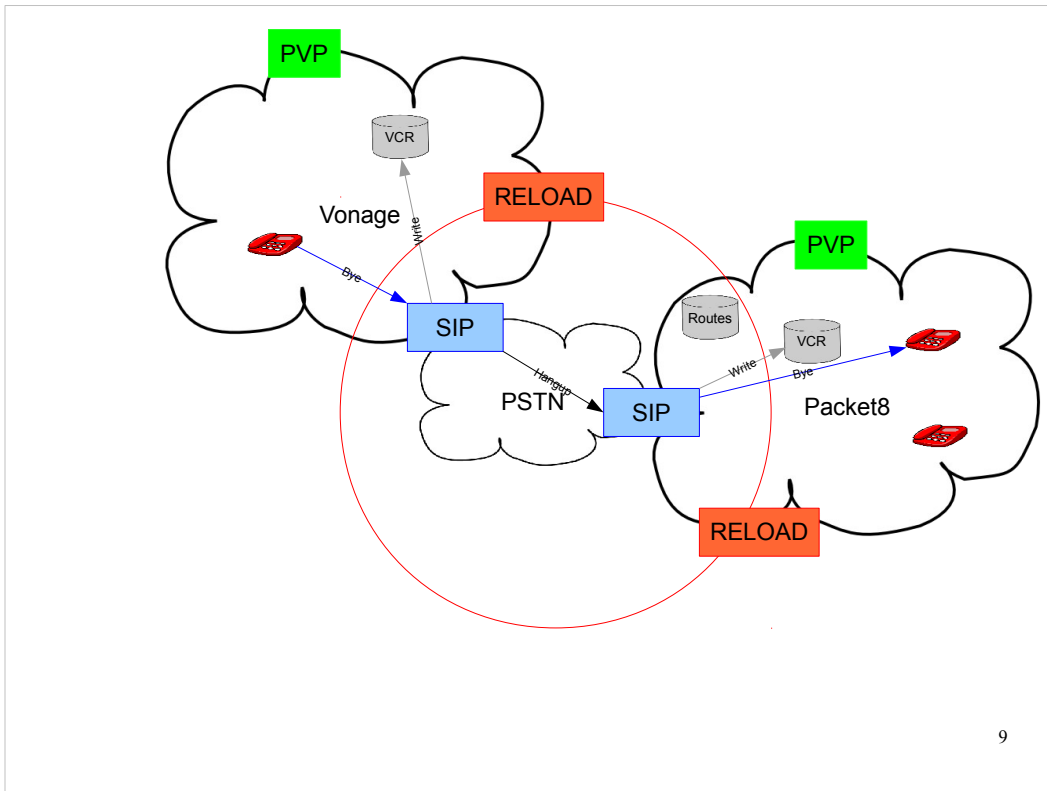
Note that more than one VoIP provider can store a mapping for a specific E.164 number. The PVP process will take care of finding who is really the owner of a specific number.



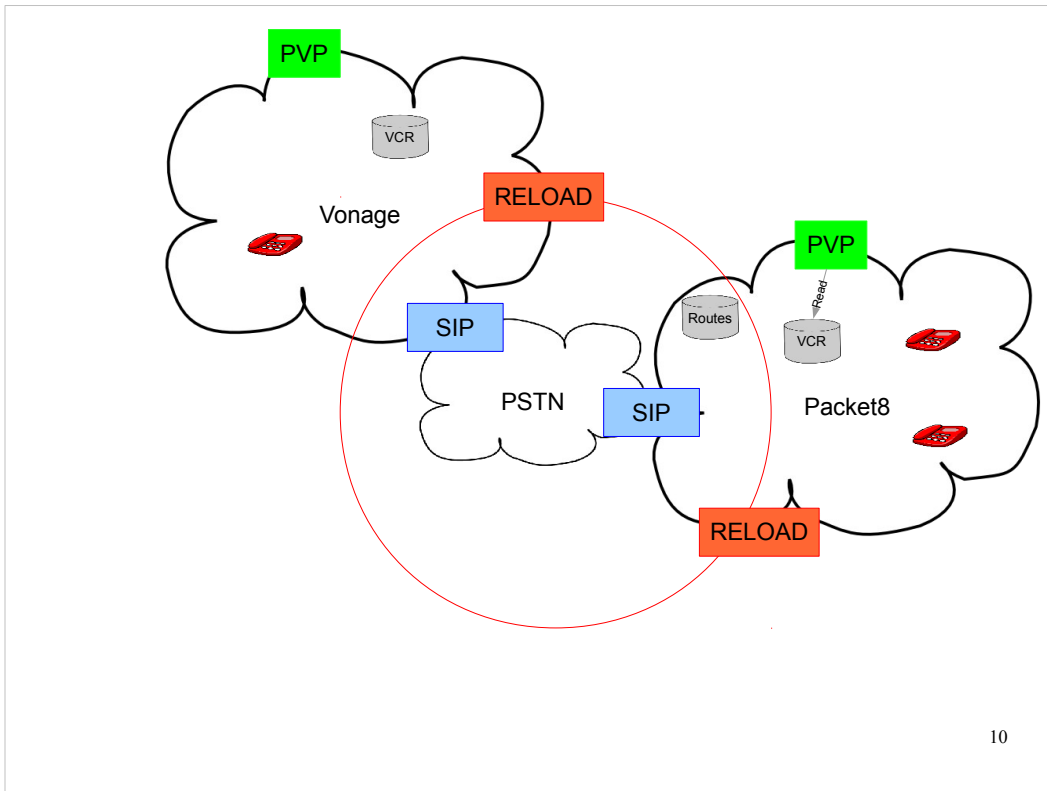
VIPR also manages a routes database, containing a list of SIP URIs, indexed by E.164 number. Each time the SIP proxy has to process an outgoing call, it first check if there is a route for the destination in the route database. Initially this database is empty.



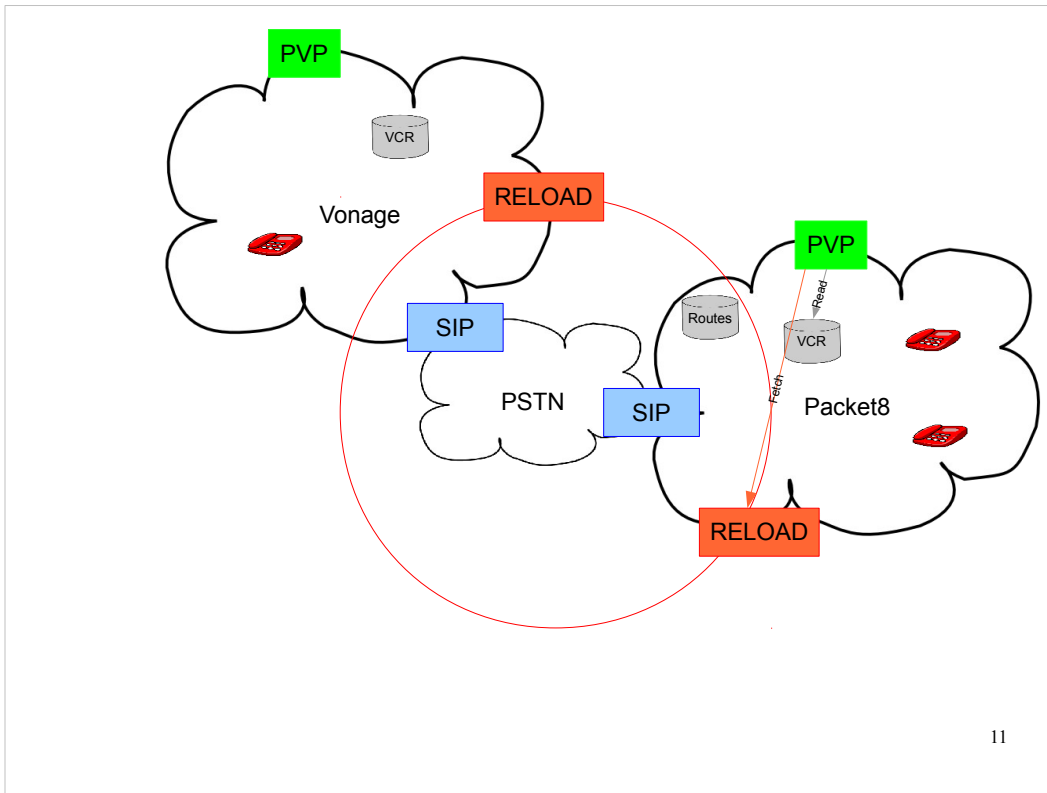
Because there is no route in the database the first time a call is made to an external destination, the SIP proxy will route the call through the PSTN, to its destination.



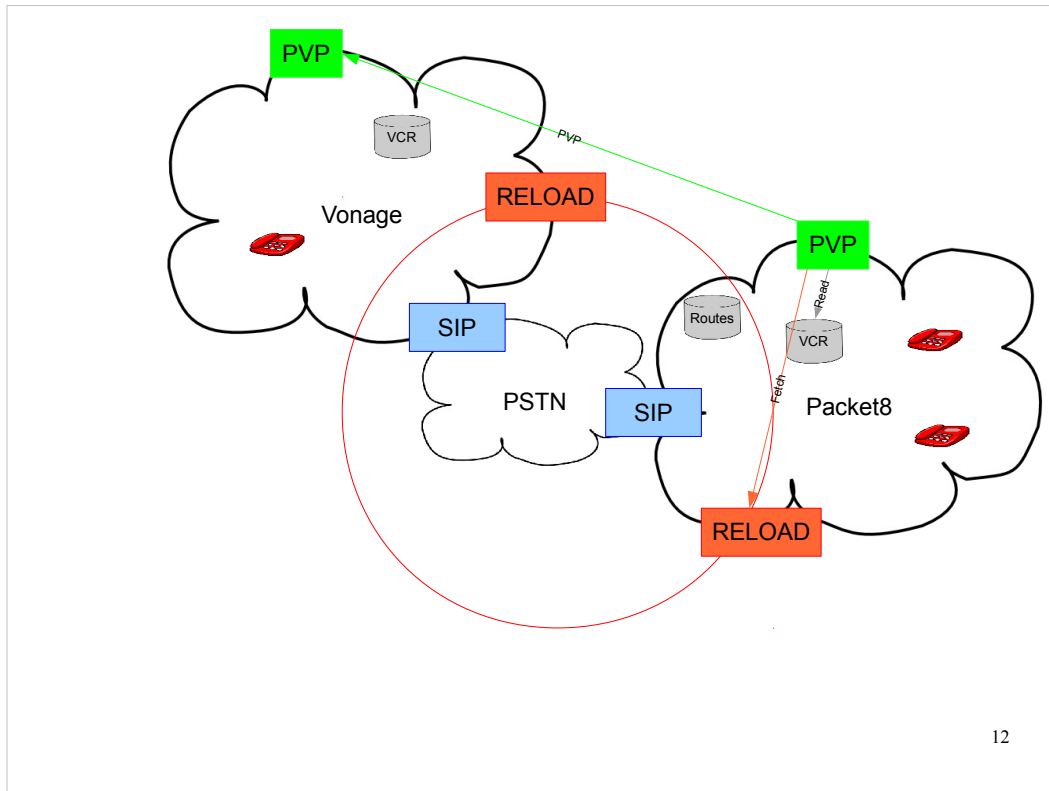
VIPR manages one additional database that contains VCRs (VIPR Call Record). This database contains one tuple for each calls made during the last 48 hours, each tuple containing the caller, callee, direction, start and stop time of one particular call. When the call ends, the SIP proxy on the caller side writes an originating VCR in the database, and the SIP proxy on the callee side writes a terminating VCR in the database.



After an outgoing VCR is written in the database, the PVP process wakes up and reads the VCR database.

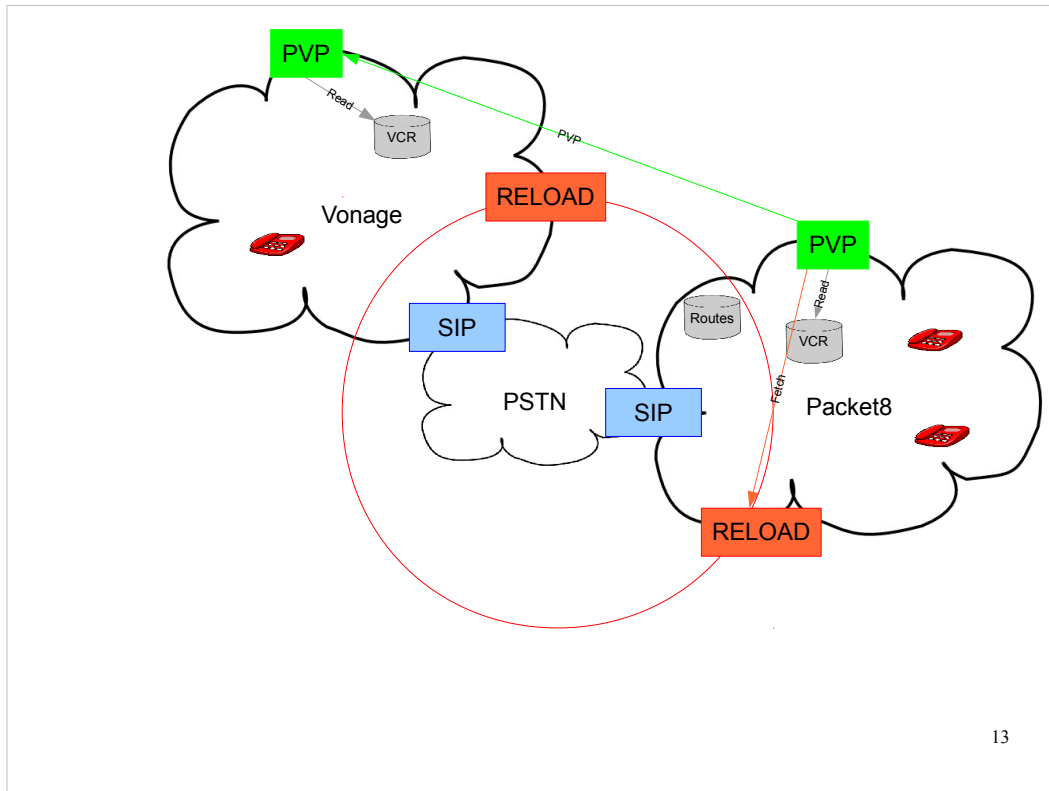


The PVP process first searches in the VIPR overlay if there is VoIP providers claiming ownership of the destination number from the originating VCR tuple. If not the tuple is silently removed from the database.

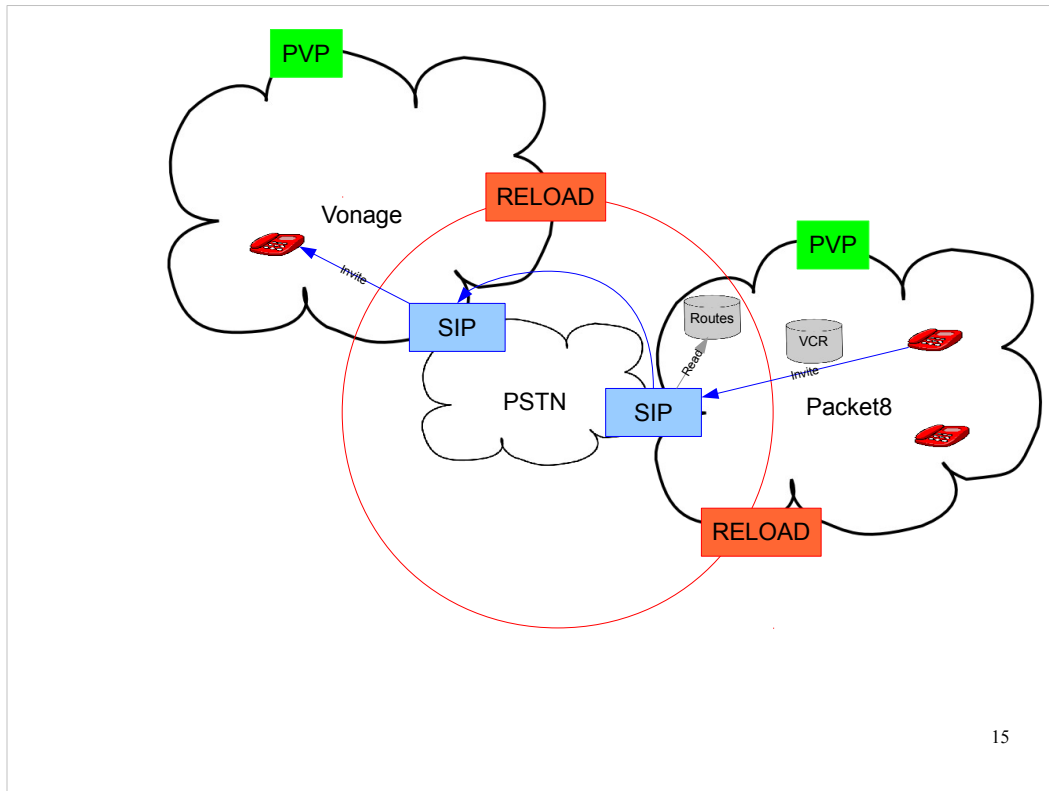


12

For each provider claiming ownership of the destination, the PVP process will try to establish a TCP connection with the IP address and port retrieved from the VIPR overlay. If this connection is successful, the PVP process will try to initiate a TLS connection using SRP (SRP uses login and password instead of the traditional X.509 certificates). The login used is the concatenation of the caller and callee numbers. The password is the concatenation of the start and stop times, rounded.

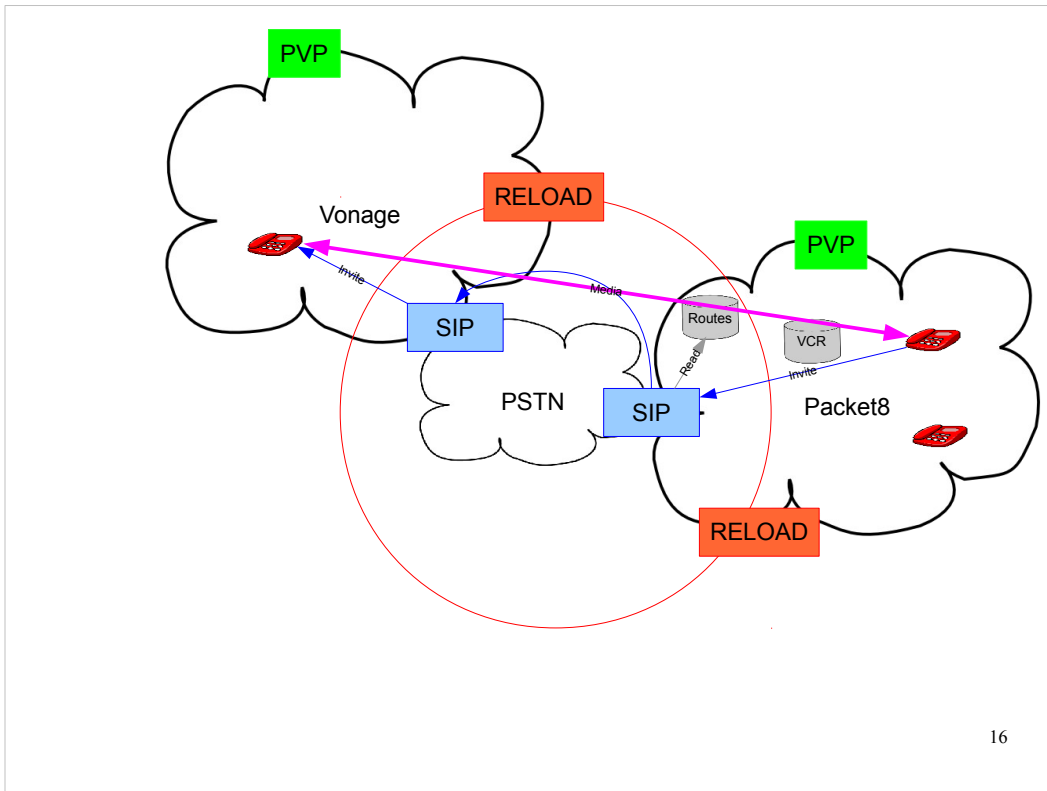


The PVP process on the remote side will receive the caller and callee numbers as login and will try to find a terminating VCR tuple in its database. If one is found, it will validate with the start and stop times (which are rounded to take care of network propagation delays).



15

On a subsequent call to the same destination, the SIP proxy will query the route database and found the SIP URI and ticket. The call will then be proxied using the SIP URI, attaching the ticket to the call. The SIP proxy receiving the call will first check that a ticket is attached to the call and that this ticket is valid and was signed by this provider. If it is not the case, then the call will be rejected – which would be the case if the call was spam. If the ticket validation succeeds, then the call is routed to its destination.



Because the call is now going over the Internet, the media is not limited to narrowband voice but can use a wideband audio codec, video and so on.