

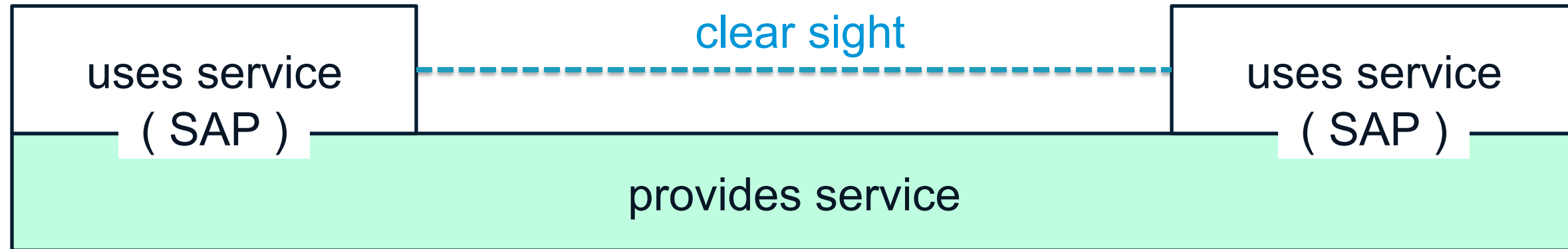
P802.1CB Layering Issues

Norman Finn
Cisco Systems

May 19, 2015

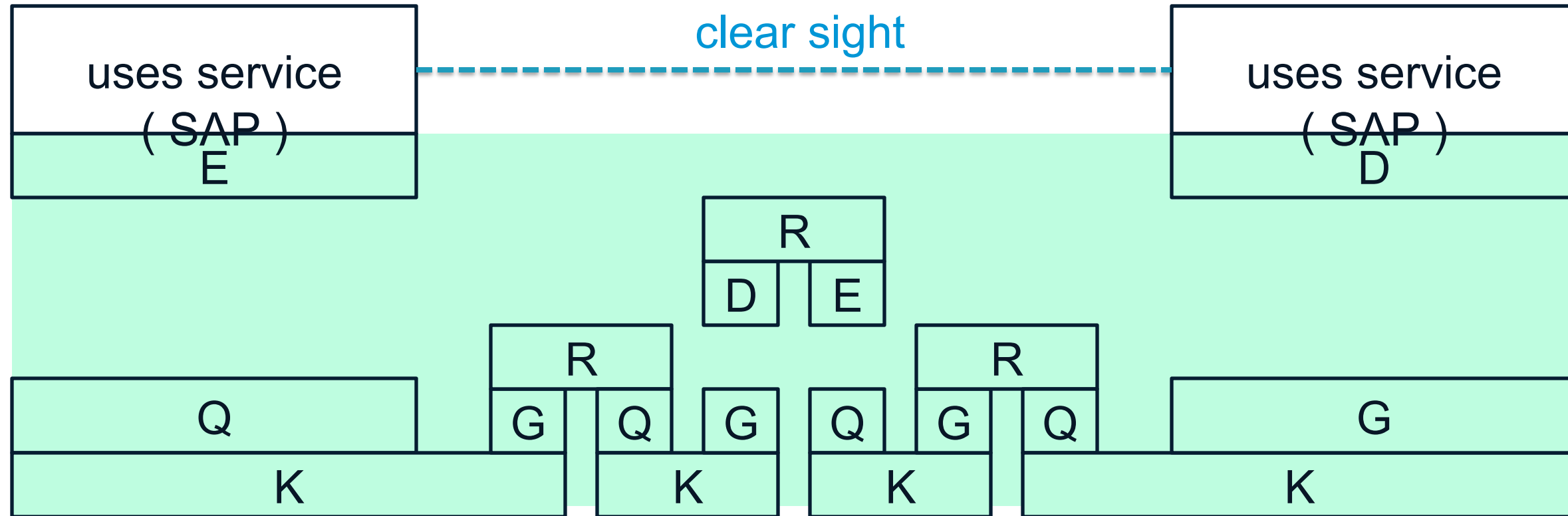


Fundamental layering



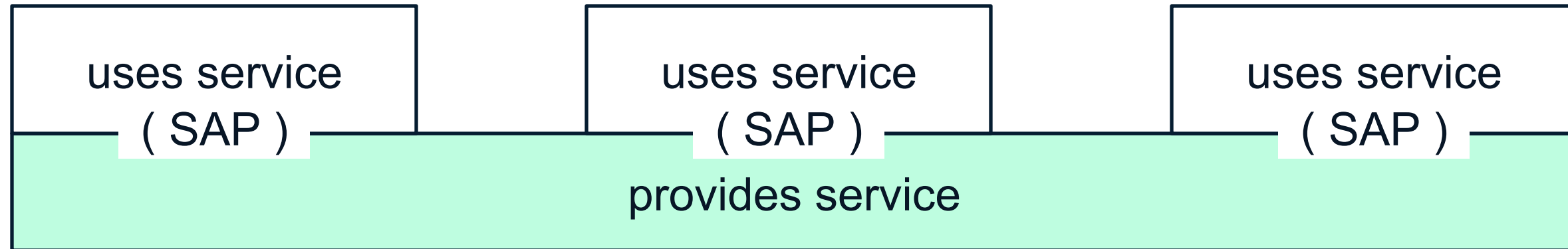
SAP == Service Access Point

Fundamental layering



- Service can be very complex, but that is invisible to the users of the service.
- Imagine MACsec (or something similar) hiding all of the details.

Fundamental layering



You CAN have multiple peers, of course.

Current diagram for ladder redundancy

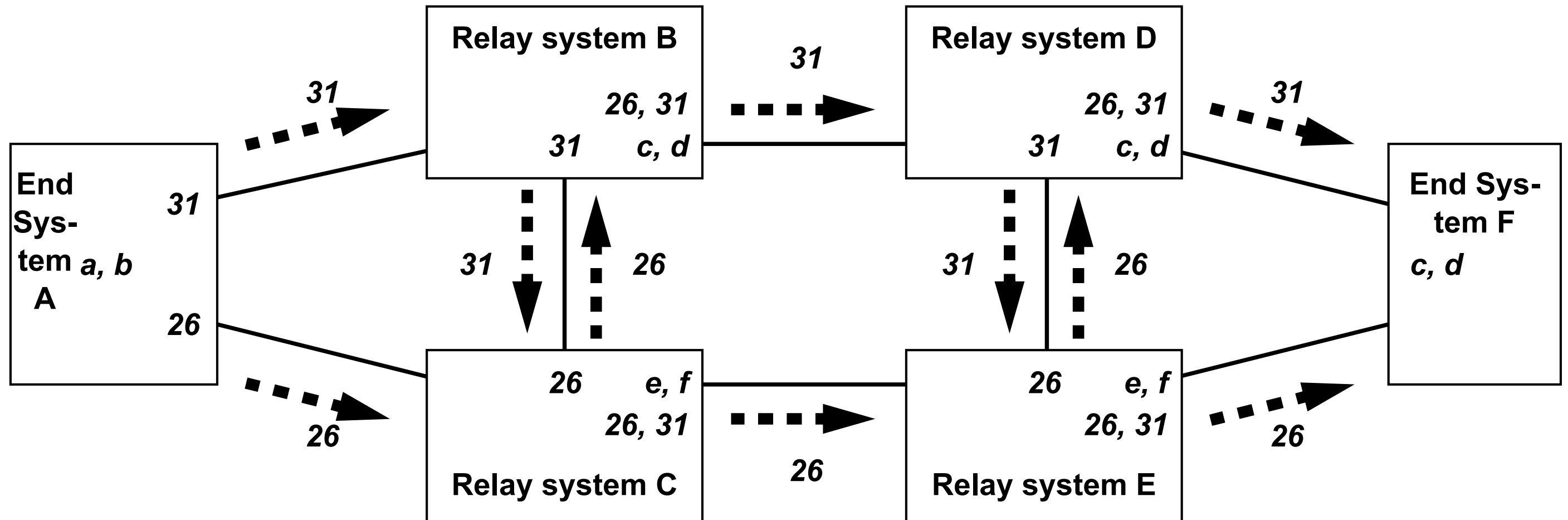


Figure F-6 Ladder Redundancy

Perhaps a better diagram for ladder redundancy

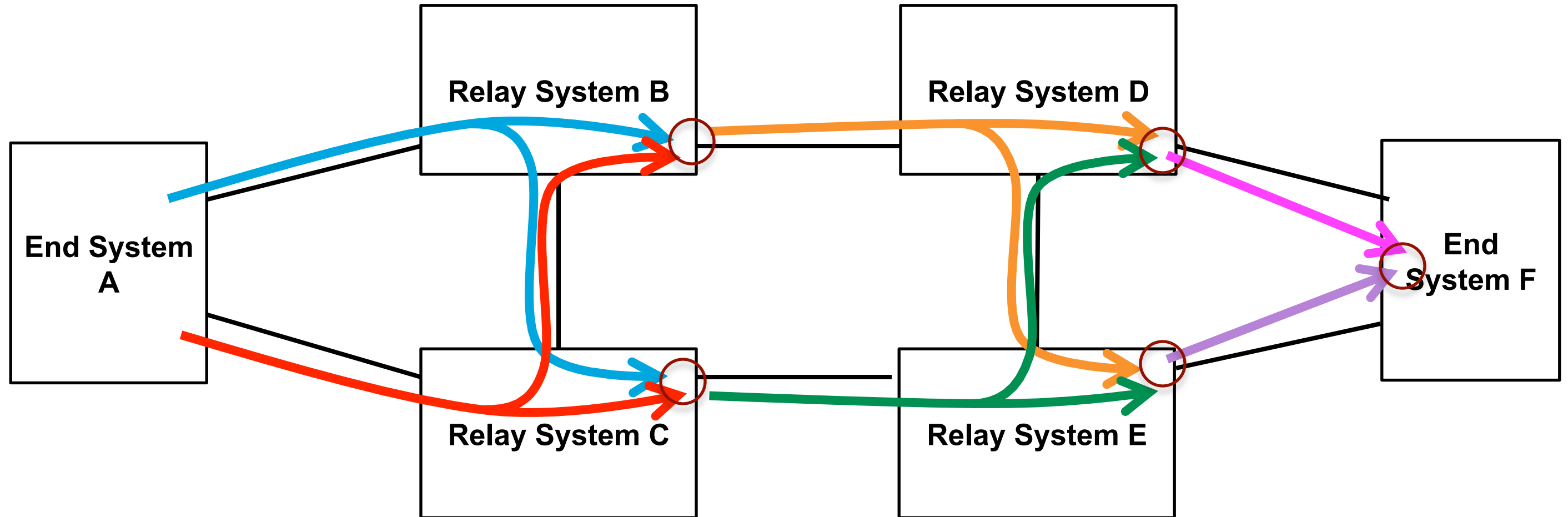
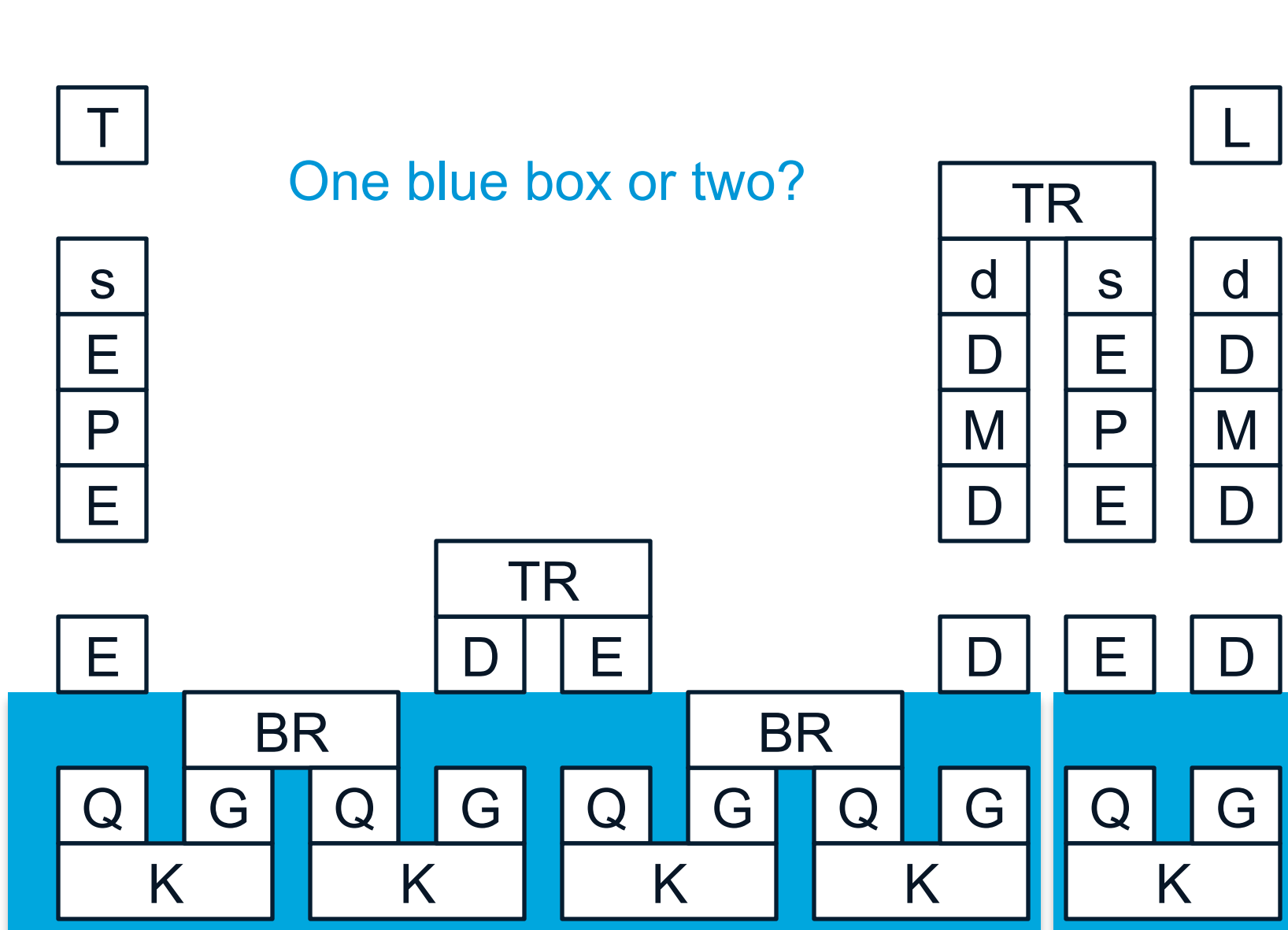


Figure F-6 Ladder Redundancy

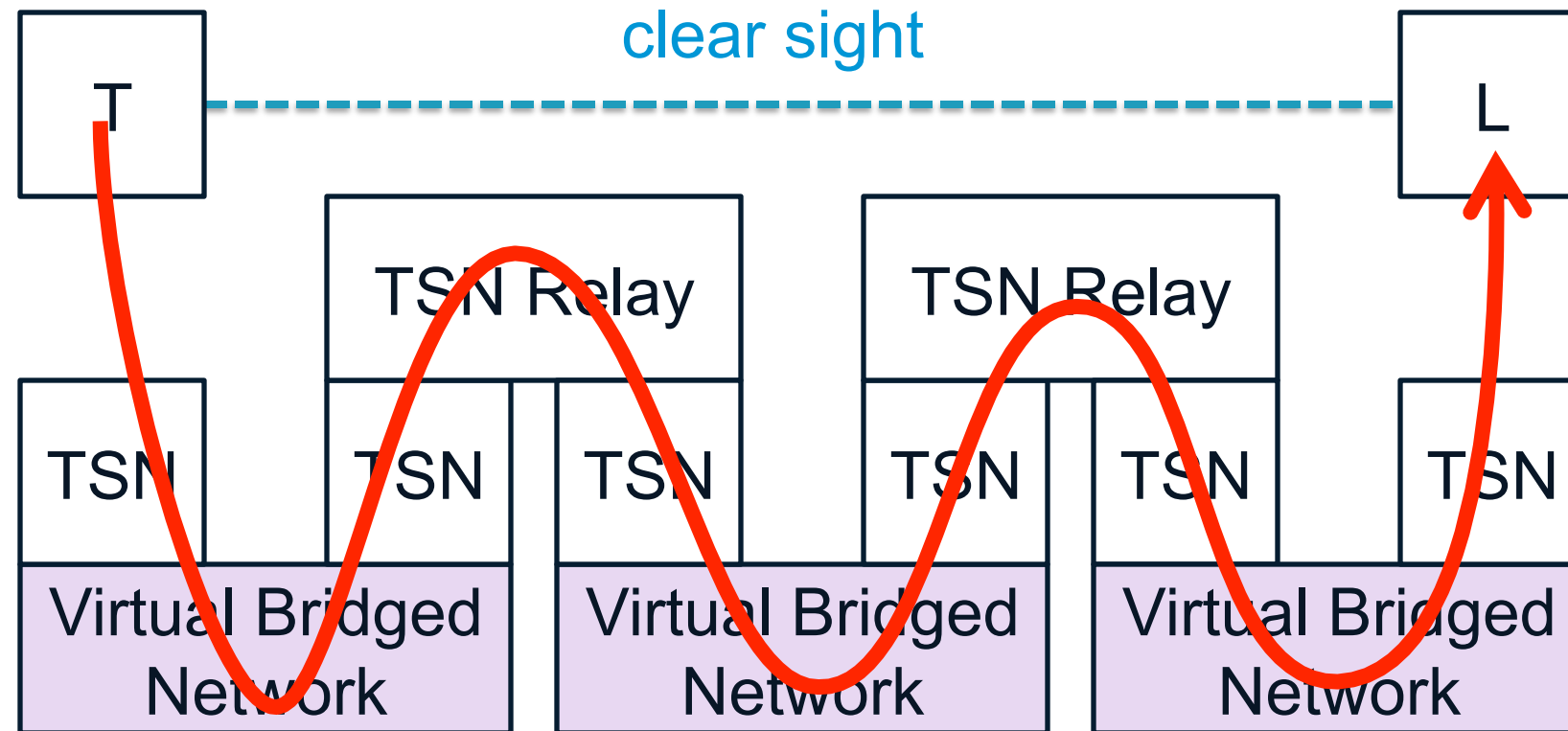
- We seem to agree that this is what we want to happen.

Model in P802.1CB D1.0



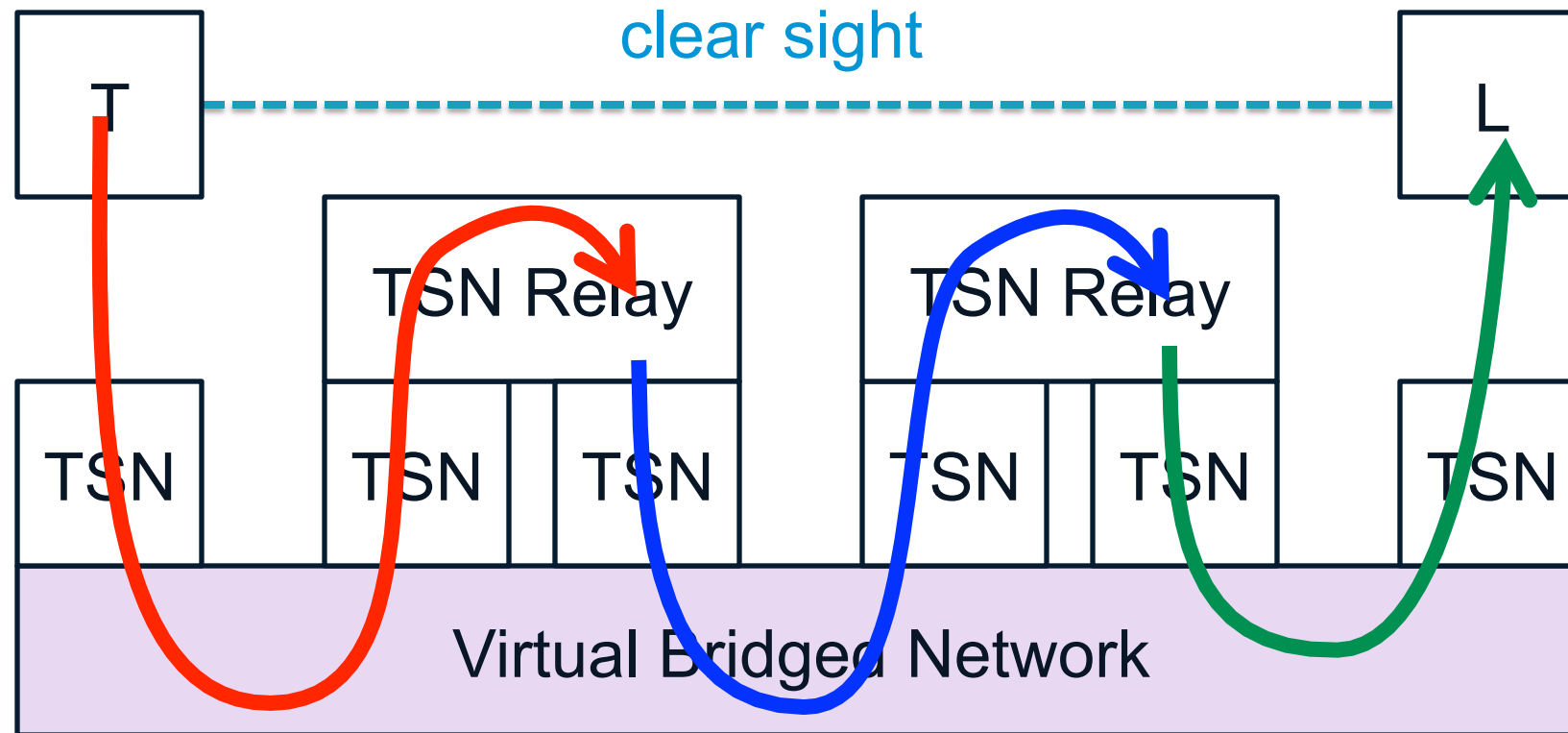
	KEY
T	Talker
L	Listener
s	seamless redundancy s erializer
d	seamless redundancy d iscarder
P	seamless redundancy sP litter
M	seamless redundancy M erger
E	E ncapsulate (maybe null)
D	D ecapsulate (maybe null)
Q	TSN Q ueuing/shaping
G	TSN input G ates
R	bridge/route/2-port R elay function
K	lin K (may be point-to-multipoint)

Routing among bridged networks example



- What we're doing, now, is either **chopping the network into pieces**, so the TSN relay is making (absolutely trivial – in left, out right) routing-type decisions . . .

Tunneling endpoints on one bridged LAN



- . . . or we're **double (triple) dipping** into the same bridged network, so we have to take steps (tunnels) to keep the various conversations separated.
(That is, we have to ensure that the blue center arrow doesn't go back to the Talker.)

P802.1CB D1.0

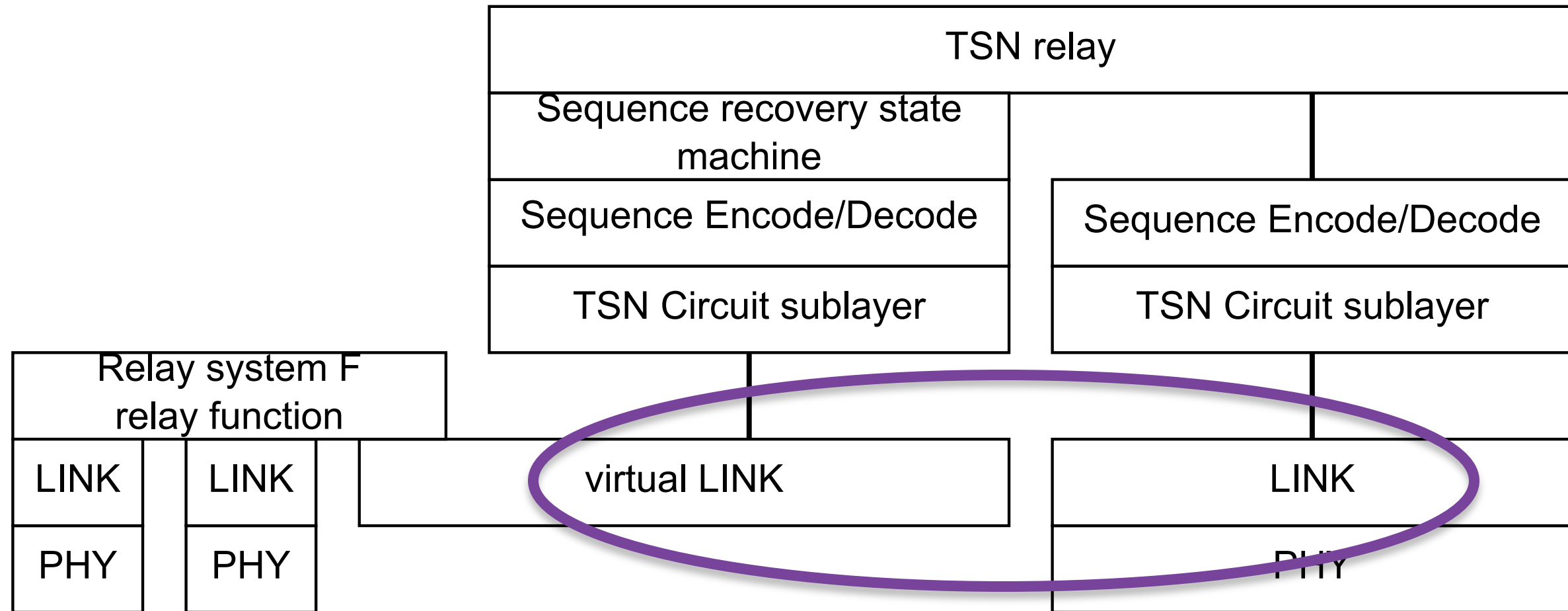
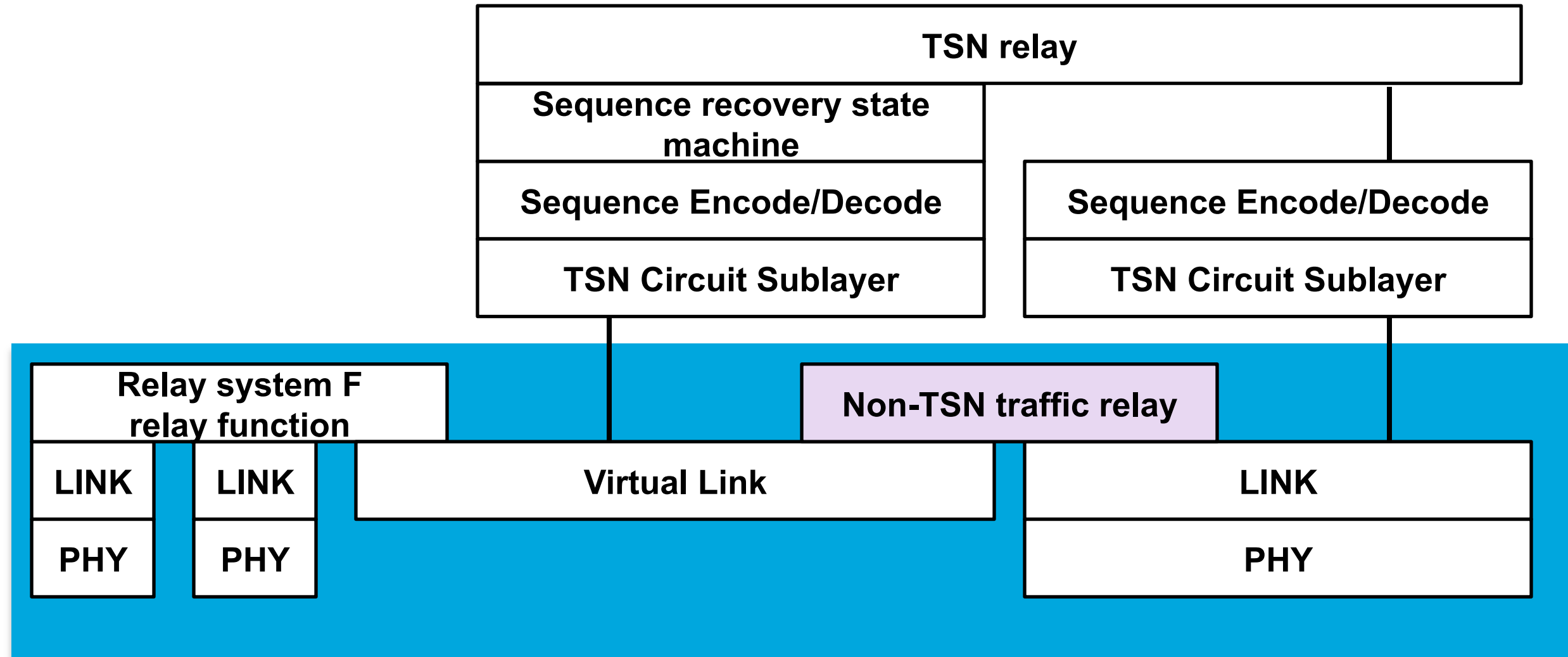


Figure F-4—Protocol stack for relay system F in Figure F-1

- **Problem:** Where is the **non-TSN traffic** in the “TSN relay”?

Where is the non-TSN traffic?



- **One answer:** A **Non-TSN relay** keeps the non-TSN traffic where it belongs.

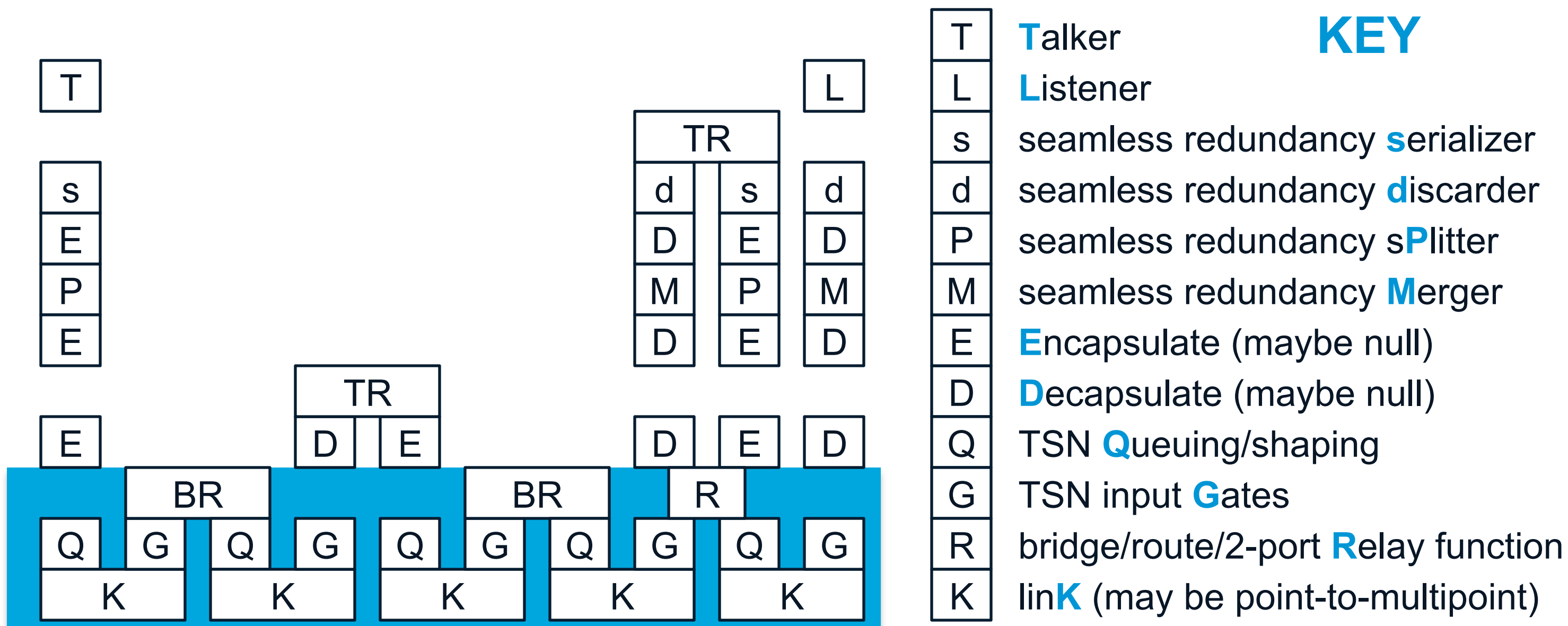
VLAN tags vs. CB tags

- **Norm's erroneous thinking:** With “proper layering,” P802.1CB can ignore whether it is dealing with bridges or routers.
- QUESTION: Suppose the network uses MAC-in-MAC-in-IPsec-in-VPN? A device near the center has to **unravel the whole stack to get to the CB-tag**, and thus tell whether this is TSN traffic or non-TSN traffic.
 - Obviously, the IPsec would make that impossible.
- QUESTION: What is the non-TSN relay?
 - **A TPMR?** I don't think we want the “Popeye arm” to intercept xx-0E LLDP PDUs!
 - **A TPMR?** What if the relay system is a router, and not a bridge? There is no equivalent of the TPMR in the routing world.

A possible “solution”

1. We define, as loosely as possible, the non-TSN relay.
2. We decode as much of the stack as necessary to identify our packets and deal with them.
3. We accept that this is a layer violation, in the same sense that we told IEEE 1588 that the transparent clock is a layer violation.
4. We change the source MAC address of the regenerated packet, and may well change the destination MAC address, also, in order to minimize the severity of the violation.

In other words, there is only one blue box



Summary

- I conclude that 802.1CB “violates proper layering” when applied to bridging and/or routing as they exist, today, and that changing the TSN Circuit at each discard point would make the violation less objectionable.
- This does not mean that P802.1CB is evil, and must be discarded.
- It does suggest that the idea of Seamless Redundancy has issues that will hinder its general applicability as a networking technique.
- An alternative formulation of Seamless Redundancy that overcomes these difficulties would be welcome.

Thank you.

