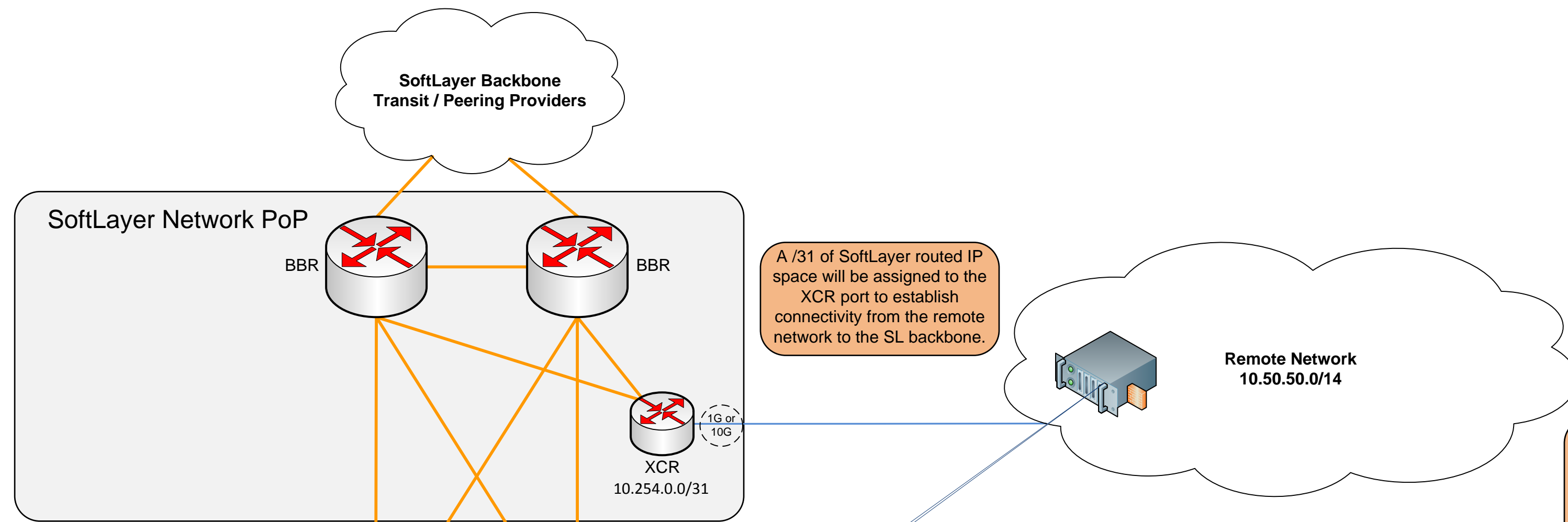


This diagram is meant to show how a customer can configure a Vyatta appliance and their hosts on the SoftLayer platform with IP space of their choosing (given it doesn't conflict with some specific ranges outlined below) on the private network and still connect to the SoftLayer services network. All IP's used in this diagram are example IP's and will be different upon deployment with the exception of the SoftLayer services network (10.0.0.0/14). **This solution is not officially supported by SoftLayer** however it has been validated as a solution that works given everything is configured properly. This solution requires that each host that has a customer provided IP bound to it and needs to communicate to the customer's remote network on that space, live in a VLAN associated with a Vyatta Gateway Appliance provided by SoftLayer. It also requires that a GRE or IPSEC tunnel be setup between an appliance on the remote network and the Vyatta Gateway Appliance that lives within their SoftLayer environment.

Naming Scheme	
Routers	
DAR	= distribution aggregation router
BBR	= backbone router
FCR	= frontend customer router
BCR	= backend customer router
MBR	= master backend router
VER	= VPN edge router
XCR	= Cross Connect router
XCS	= Cross Connect switch
Switches	
FCS	= frontend customer servers switch
BGS	= backend customer servers switch
FAS	= frontend racks aggregation switch
BAS	= backend racks aggregation switch
BMS	= backend management (PMI ports) switch
MSS	= master service switch
LBSW	= load balancer switch



A route will need to be configured on the GRE or IPSEC endpoint to push all traffic destined for the SoftLayer environment (10.20.20.1/24) out the GRE or IPSEC tunnel. All other traffic to remain on the customer network (10.50.50.0/14) should be pointed at the default gateway for the customer network.

