As 224.0.0.6 as used in ospfv2 for

As discussed by Teare (2010), one of the major changes introduced inOSPFv3 is thatthe protocol's header has been redesigned. The header is no longercomplex as compared to the header in OSPFv2. The header now includes aninstance ID field.

Routing in IPv6 is done on a per–interface basis not onper–subnet. Each IPv6 routing protocol is more concerned 16 about the link onwhich it is configured but not the subnet. The addition of the new instance IDfield to the protocol structure therefore makes it possible for several OSPFv3instances or addresses to be enabled on the same link. By default, instance IDis 0. When there is an additional instance, it is increased. Each OSPF instanceis assigned a separate instance ID. Also, instance ID has local link significance only.

This means thatbefore OSPFv3 routers can become neighbors, they must have identical instanceIDs. For example, if a router receives a packet whose instance ID is not thesame as its own instance ID, it simply discards the packet. Additionally, because the OSPFv3 header has been redesigned its hellopacketstructure has also been changed (Coltun et al, 2008). As discussed byTeare (2010), the changes made to the OSPFv3 include the following: In OSPFv3, the multicast addresses reserved for all SPF or link state routers and all designated routers are now FF02:: 5 and FF02:: 6 respectively; they are no longer 224. 0. 0. 5 and 224. 0.

0. 6 as used in OSPFv2 for IPv4. The packet header of OSPFv3 is not designed to include IPv6 addresses. Rather, IPv6 address is carried inside the payload of the link state update packet.

In OSPFv2, network LSAs carry IPv4 addresses but in OSPFv3, network LSAs do not include IPv6 addresses. To configure OSPFv3 on routers, the router ID must be enabled before routing can start. In OSPFv3, identification of the designated router and backup designated router is done with the router's ID; not with its IP address as in the case of OSPFv2. Also, another notable change for OSPFv3 is thesecurity mechanism it uses to protect its routing information.

In OSPFv2, Message Digest 5 is the main security technique used to 17 secure