Purpose of STP (C) 2016 Cisco and/or its affiliates. A Layer 2 loop can result in MAC address table 4.1 instability, link saturation, and high CPU utilization on switches and end-devices, resulting in the network becoming unusable. Spanning Tree Protocol (STP) is a loop-prevention network protocol that allows for redundancy while creating a loop-free Layer 2 topology. Cisco Confidential 5 Purpose of STP STP Recalculation STP compensates for a failure in the network by recalculating and opening up previously blocked ports. When multiple paths exist between two devices on an Ethernet network, and there is no spanning tree implementation on the switches, a Layer 2 loop occurs. Without STP enabled, Layer 2 loops can form, causing broadcast, multicast and unknown unicast frames to loop endlessly. o Spanning tree is enabled, by default, on Cisco switches to prevent Layer 2 loops from occurring. STP logically blocks physical loops in a Layer 2 network, preventing frames from circling the network forever. Layer 2 Ethernet does not include a mechanism to recognize and eliminate endlessly looping frames. Ethernet and Ethernet switches have no comparable mechanism for limiting the number of times a switch retransmits a Layer 2 frame. STP is based on an algorithm that creates a loop-free topology by selecting a single root bridge where all other switches determine a single least-cost path. Cisco Confidential 3 Purpose of STP Redundancy in Layer 2 Switched Networks ?Redundancy is an important part of the hierarchical design for eliminating single points of failure and preventing disruption of network services to users. However, redundant paths in a switched Ethernet network may cause both physical and logical Layer 2 loops. A loop in an Ethernet LAN can cause continued propagation of Ethernet frames until a link is disrupted and breaks the loop. Both IPv4 and IPv6 include a mechanism that limits the number of times a Layer 3 networking device can retransmit a packet. When a loop occurs, the MAC address table on a switch will constantly change with the updates from the broadcast frames, which results in MAC database instability. Broadcast storms can be caused by a hardware problem such as a faulty NIC or from a Layer 2 loop in the network. This topic covers the causes of loops in a Layer 2 network and briefly explains how spanning tree protocol works. Having alternate physical paths for data to traverse the network makes it possible for users to access network resources, despite path disruption. Cisco Confidential 4 Purpose of STP Spanning Tree Protocol ?Cisco Confidential 6 Purpose of STP Issues with Redundant Switch Links ?A router will decrement the TTL (Time to Live) in every IPv4 packet, and the Hop Limit field in every IPv6 packet. STP was developed specifically as a loop prevention mechanism for Layer 2 Ethernet. Cisco Confidential 7 Purpose of STP Layer 2 Loops ?Layer 2 multicasts are typically forwarded the same way as a broadcast by the switch. To prevent these issues from occurring in a redundant network, some type of spanning tree must be enabled on the switches. Cisco Confidential 9 Purpose of STP The Spanning Tree Algorithm ?Redundant networks require the addition of physical paths, but logical redundancy must also be part of the design. Ethernet LANs require a loop-free topology with a single path between any two devices. Path redundancy provides multiple network services by eliminating the possibility of a single point of failure. When these fields are decremented to 0, a router will drop the packet. This can cause high CPU utilization, which makes the switch unable to forward frames. An unknown unicast frame is when the switch does not have the destination MAC address in its MAC address table and must forward the frame out all ports, except the ingress port. Cisco Confidential 8 Purpose of STP Broadcast Storm ?A broadcast storm is an abnormally high number of

broadcasts overwhelming the network during a specific amount of time. Layer 2 broadcasts in a network, such as ARP Requests are very common. ICMPv6 Neighbor Discovery uses Layer 2 multicasts. A host caught in a Layer 2 loop is not accessible to other hosts on the network. Additionally, due to the constant changes in its MAC address table, the switch does not know out of which port to forward unicast frames.??????????????This can bring down a network ???????.quickly