Video - ARP Role in Remote Communication (3 min)

In this video, PC-A has an IP packet, source IP address itself at 192.168.1.110, and destination IP address 10.1.1.10, which is an IP address on a remote network. So the destination MAC address will be that of its default gateway, 192.168.1.1-- the router R1, in this case. PC-A checks its ARP cache for that IP address 192.168.1.1, and there's no entry with a MAC address. So it puts the packet on hold and creates an ARP request. The ARP request has the IP address of the router, 192.168.1.1, and the target MAC address is unknown. The destination MAC address of an ARP request is a broadcast, so it will be sent to the switch, and the switch will flood it out all ports except for the incoming port. PC-B receives the ARP request, compares its own IPv4 address against the target IPv4 address in the ARP request, and notices it is not a match, so it is not the intended target. PC-C receives the ARP request, compares its IPv4 address against the target IPv4 address, and it is not the intended target either. Router R1 receives the ARP request, compares its IPv4 address against the target IPv4 address, and it is indeed a match. It is the target of the ARP request. So router R1 will issue an ARP reply in response. It will include its own MAC address, 00-0D, along with its IPv4 address. The destination MAC address of the ARP reply is a unicast directed for PC-A. So it is a destination MAC address of 00-0A, so PC-A receives the ARP reply. PC-A, when it receives the ARP reply in response for its ARP request, sees the target IPv4 address and the target MAC address and adds that to its ARP cache. It now has the information it needs to forward the packet, which is on hold. So the destination MAC address is now going to be 00-0D, that of the router R1, its MAC address. And now PC-A can forward the frame on to router R1.