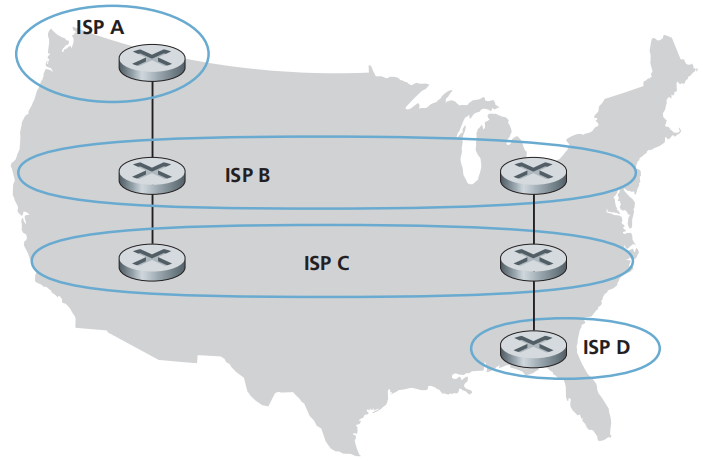
**P12.** Describe how loops in paths can be detected in BGP.

**Answer:**

BGP advertisements contain complete paths showing the AS’s the path passes through, and so a router can easily identify a loop because an AS will appear two or more times.

**P16.** Consider the following network. ISP B provides national backbone service to regional ISP A. ISP C provides national backbone service to regional ISP D. Each ISP consists of one AS. B and C peer with each other in two places using BGP. Consider traffic going from A to D. B would prefer to hand that traffic over to C on the West Coast (so that C would have to absorb the cost of carrying the traffic cross-country), while C would prefer to get the traffic via its East Coast peering point with B (so that B would have carried the traffic across the country). What BGP mechanism might C use, so that B would hand over A-to-D traffic at its East Coast peering point? To answer this question, you will need to dig into the BGP specification.



**Answer:**

ISP B provides backbone to the regional ISP A

-ISP C provides backbone to the regional ISP D

-Each ISP consists of one AS

-ISP B would like to hand over traffic of C through the West Coast

-The ISP C would like to receive traffic from B’s peering point via East Coast.

So,one way for C to force B to hand over all of B’s traffic onto D (on the east coast), is for C to ONLY

advertise its route to D via its east coast peering point with C.

ISP B provides backbone to the regional ISP A

-ISP C provides backbone to the regional ISP D

-Each ISP consists of one AS

-ISP B would like to hand over traffic of C through the West Coast

-The ISP C would like to receive traffic from B’s peering point via East Coast.

So,one way for C to force B to hand over all of B’s traffic onto D (on the east coast), is for C to ONLY

advertise its route to D via its east coast peering point with C.

ISP B provides backbone to the regional ISP A

-ISP C provides backbone to the regional ISP D

-Each ISP consists of one AS

-ISP B would like to hand over traffic of C through the West Coast

-The ISP C would like to receive traffic from B’s peering point via East Coast.

So,one way for C to force B to hand over all of B’s traffic onto D (on the east coast), is for C to ONLY

advertise its route to D via its east coast peering point with C.

ISP B provides backbone to the regional ISP A

-ISP C provides backbone to the regional ISP D

-Each ISP consists of one AS

-ISP B would like to hand over traffic of C through the West Coast

-The ISP C would like to receive traffic from B’s peering point via East Coast.

So,one way for C to force B to hand over all of B’s traffic onto D (on the east coast), is for C to ONLY

advertise its route to D via its east coast peering point with C.

-ISP B provides backbone to the regional ISP A

-ISP C provides backbone to the regional ISP D

-Each ISP consists of one AS

-ISP B would like to hand over traffic of C through the West Coast

-The ISP C would like to receive traffic from B’s peering point via East Coast.

So, one way for C to force B to hand over all of B’s traffic onto D (on the east coast), is for C to ONLY advertise its route to D via its east coast peering point with C.

**P20.** Suppose ASs X and Z are not directly connected but instead are connected by AS Y. Further suppose that X has a peering agreement with Y, and that Y has a peering agreement with Z. Finally, suppose that Z wants to transit all of Y’s traffic but does not want to transit X’s traffic. Does BGP allow Z to implement this policy?

**Answer:**

Yes, BGP allows AS Z to implement the policy to transit all of AS Y’s traffic but not AS X’s traffic by using AS path filtering. This filtering ensures that routes originating from AS X are not accepted by AS Z, thus effectively implementing the desired policy.

Given data:

The network contains Autonomous Systems AS X, AS Y and AS Z.

*BGP*means *Border Gateway Protocol*.  It is an Inter-AS routing protocol.

* It takes the subnet reachability data from neighboring AS.
* AS X has an agreement of peering with AS Y.
* AS Y has an agreement of peering with AS Z.
* This protocol permits AS Z to develop the policy.
* The *BGP* route trailers are held by each AS.
* AS Y should present AS X that, it has no path to Z.
* The system AS X is ignorant that AS Y has path to AS Z.
* AS X never forward the traffic.
* AS Z can transfer all of Y’s traffic.

**P22.** In Section 5.7, we saw that it was preferable to transport SNMP messages in unreliable UDP datagrams. Why do you think the designers of SNMP chose UDP rather than TCP as the transport protocol of choice for SNMP?

**Answer:**

The designers of SNMP chose UDP rather than TCP as the transport protocol for SNMP. The reason is that

SNMP protocol runs over the TCP then stops sending messages. If the network manager wants to send

SNMP messages, then the control of TCP back off the SNMP.

SNMP events such as links going down, or congestion happen when the network is under heavy load. If TCP was used there would be significant overhead in the resources necessary to establish and keep the connections alive.  
Also, TCPs congestion control would make the agents stop sending error messages, which is not the intended use of SNMP messages. UDP does not have this congestion control and sends messages regardless of the state of the network.

The choice of UDP for transporting SNMP messages was driven by the need for simplicity, low overhead, speed, efficiency, suitability for stateless communication, tolerance to occasional message loss, resource constraints of network devices, and scalability. These characteristics make UDP a fitting transport protocol for the quick, efficient, and straightforward message exchanges required by SNMP.