DATE: NO:

第9周 17

R1 路由算法在每个路由器中运行.
每一路由器作为独立实体实现自己控制面和数据平面.

R2. A logically central routing controller computes and distributes the forwarding tables to be used by each and every router.
Each router does not compute its forwarding table.
The control plane is implemented in a central server / multiple servers. ~~Date~~ The data plane is implemented in each router.

R3. Centralized routing algorithm: computes the least-cost path between a source and destination by using complete, global knowledge about the network. Calculation can be run at one site or replicated in the routing component of each router.
Distribute routing algorithm: calculate in an ~~迭~~ iterative, distributed ~~routing algorithm~~ manner by the routers.

R4. Link state algorithms: compute the ~~less~~ least-cost path using complete, global knowledge about the network.
Distance-vector routing: calculation is carried out in an ~~iterab~~ iterative, distributed manner.

R5. It takes a long time for a distance vector routing algorithm to ~~too~~ converge when there is a link cost increase.

R6. Yes. Each AS has administrative autonomy for routing within an AS.

R7 Policy: Among ASs, policy issues dominate.
Scale: different scale.
Performance: inter-AS routing concern less on quality. intra-AS focus on performance.

R8. False with OSPF, a router broadcasts its link-state information to all other routers in the AS to which it belongs.

R9 An area in an OSPF AS is refers to a set of routers, in which each router broadcast its link state to all other routers in the same set.

R10. Subnet: a portion of a larger network. doesn't contain a router. it's boundaris are defined by the router and host interface.
Prefix: the network portion of a CIDRized address.
written in the form a.b.c.d/x. A prefix covers one or more subnets.
BGP route: a prefix along with its attributes.

R11. ~~NEXT-HOP attribute usage:~~
AS-PATH: detect and prevent looping advertisement.
choose among multiple paths to the same prefix.
NEXT-HOP: indicates the IP address of the first router along an advertised path. to a given prefix.

R12 A tier-1 ISP may ~~not~~ not to carry ~~transit traffic~~ between two other ~~tier~~ tier-1 ISP.

R13. False.
only happen when receive path from other AS.

P3.

Step	N'	D(t), p(t)	D(u), p(u)	D(v), p(v)	D(w), p(w)	D(y), p(y)	D(z), p(z)
0	x	∞	∞	3, x	6, x	6, x	8, x
1	xv	7, v	6, v	3, x	6, x	6, x	8, x
2	xvu	7, v	6, v	3, x	6, x	6, x	8, x
3	xvuw	7, v	6, v	3, x	6, x	6, x	8, x
4	xvuwy	7, v	6, v	3, x	6, x	6, x	8, x
5							
6							

P5

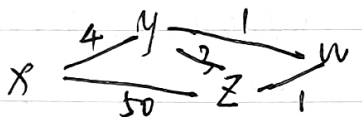
From \ Cost to	u	v	x	y	z
v	∞	∞	∞	∞	∞
x	∞	∞	∞	∞	∞
z	∞	6	2	∞	0

From \ Cost to	u	v	x	y	z
v	1	0	3	∞	6
x	∞	3	0	3	2
z	7	5	2	5	0

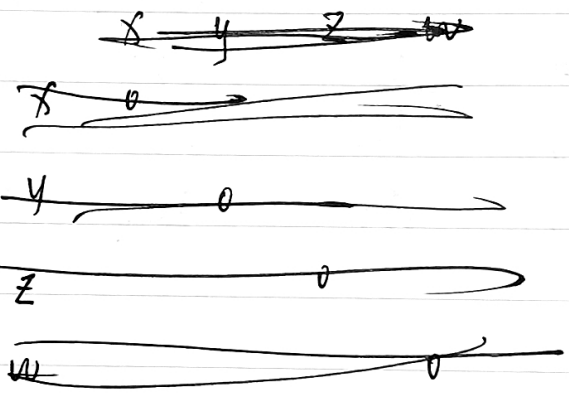
From \ Cost to	u	v	x	y	z
v	1	0	3	3	5
x	4	3	0	3	2
z	6	5	2	5	0

P9 NO. Decreasing link cost won't cause a loop.

P11



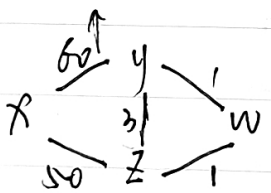
~~a. w inform z, $D_w(x)=\infty$.~~
~~inform y, D~~



a) z informs w, $D_z(x)=\infty$
informs y, $D_z(x)=6$

w informs z, $D_w(x)=5$
informs y, $D_w(x)=\infty$

y informs w, $D_y(x)=4$
informs z, $D_y(x)=4$

b) 

Yes.

c). cut the link between y and z.

P13. 不一定是最短路径. 会考虑各种因素. (e.g. 经济 / 政策原因).

DATE : NO .

P14. a) eBGP b) iBGP c) eBGP d) iBGP.

P15 a) I_1. 该接口到 1c 的成本最低

b) I_2. 两种路由都有相等路径长度. 从开始的路径有最近的下一跳的路由.

c). I_1. 基 I_1 开始有最短路径 AS-PATH.

DATE: NO

第9周 18

R14. 通信层通过OpenFlow等协议负责SDN控制器与受控网络设备之间的通信. SDN控制器控制远程SDN启用交换机、主机或其他设备的操作,并且设备将本地观察到的事件与控制器通信.
网络范围的状态管理层提供关于网络主机、链路、交换机和其他SDN控制设备的最新信息. 控制器还维护各种受控设备的流表和副本.
网络~~管理~~控制应用层代表SDN控制平面的大脑. 该层的应用程序使用SDN控制器提供的API来指定和控制网络设备中的数据平面.

R15. 在SDN的网络控制应用层实现一个新的路由协议. 因为这是一个路由协议决定源和目的地之间端到端的路径的层.

R16.
- 配置. 此消息允许控制查询和设置交换机的配置参数.
- 修改-状态. 添加/删除/修改交换机流表中的条目,设置开采端口属性.
- 阅读状态. 收集交换机中的流计消息和计数器值.
- 发送包
  指示为受控交换机在指定交换机.

R17 从受控设备到控制器的两种消息类型:
- 流删除消息
- 端口-状态消息.

从控制器到受控设备:
- 修改状态
- 读状态

DATE NO

R19 Echo reply (to ping), type 0, code 0
Destination network unreachable type 3 code 0
Destination host unreachable type 3 code 1
Source quench (congestion control), type 4 code 0

R20 ICMP warning message (type 11 code 0) and a destination port unreachable ICMP message (type 3 code 3)

R21 A managing server is an application, typically with human in the loop, running in a centralized network management station in a network operation center.
A managed device is a piece of network equipment that resides on a managed network.
A network management agent is a process running in a managed device that communicate with a managing server.
Management Information B collects the information associated with those managed objects in a managed network.

R22. Get Request is a message sent from a managing server to an agent to request the value of one or more MIB objects at the agent's managed device
SetRequest is a message used by a managing server to set the value of one or more MIB objects in a managed device.

DATE : NO :

R23

A SNMP trap message is generated as a response to an event happened on a managed device for which the device's managing server requires notification. It is used for notifying a managing server of an exceptional situation that has resulted in changes to MIB object values.

P21 Request response mode will generally have more overhead for several reasons. First, each piece of information received by the manager requires two messages: the poll and the response. Trapping generates only a single message to the sender. If the manager really only want to be notified when a condition occurs, polling has more overhead, since many of the polling messages may indicate that the wait-for condition has not yet occurred. Trapping generates a message only when the condition occurs.

Trapping will also immediately notify the manager when an event occurs. With polling, the manager needs will need to wait for half a polling cycle between when the event occurs and the manager discovers that the events has occurred.

If a trap message is lost, the managed device will not send another copy. If a poll massage, or its response is lost the manager would know these has been a lost message. Hence the manager could report, if needed.

DATE NO

>>. Often, the time when network management is most needed is in times of stress, when the network may be severely congested and packets are being lost. With SNMP running over TCP, TCP's congestion control would cause SNMP to back-off and stop sending messages at precisely the time when the network manager needs to send SNMP messages.