Service Level Agreements (SLA)

Customers have SLAs with their ISPs.

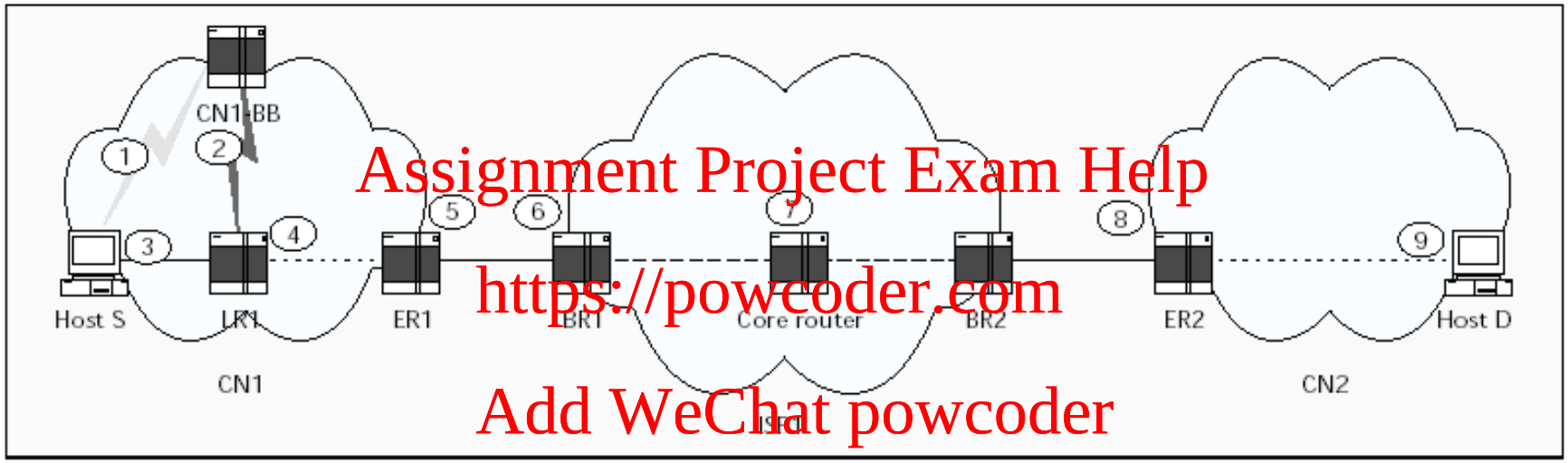
Assured Service

- SLAs specify the amount of bandwidth allocated for the customers
- SLAs for Assured Service are usually static, meaning customers can start data transmission whenever they want without signaling their ISPs

Premium Service

- SLAs specify desired peak bit rate for specific flow or aggregation of flows – customers responsible for not exceeding the peak rate
- ISP guarantees that contracted bandwidth will be available when traffic sent
- Dynamic SLAs allow customers to request premium service on demand (since premium service is expensive)
- Admission control is therefore needed for dynamic SLAs

Assured Service Delivery (with static SLA)

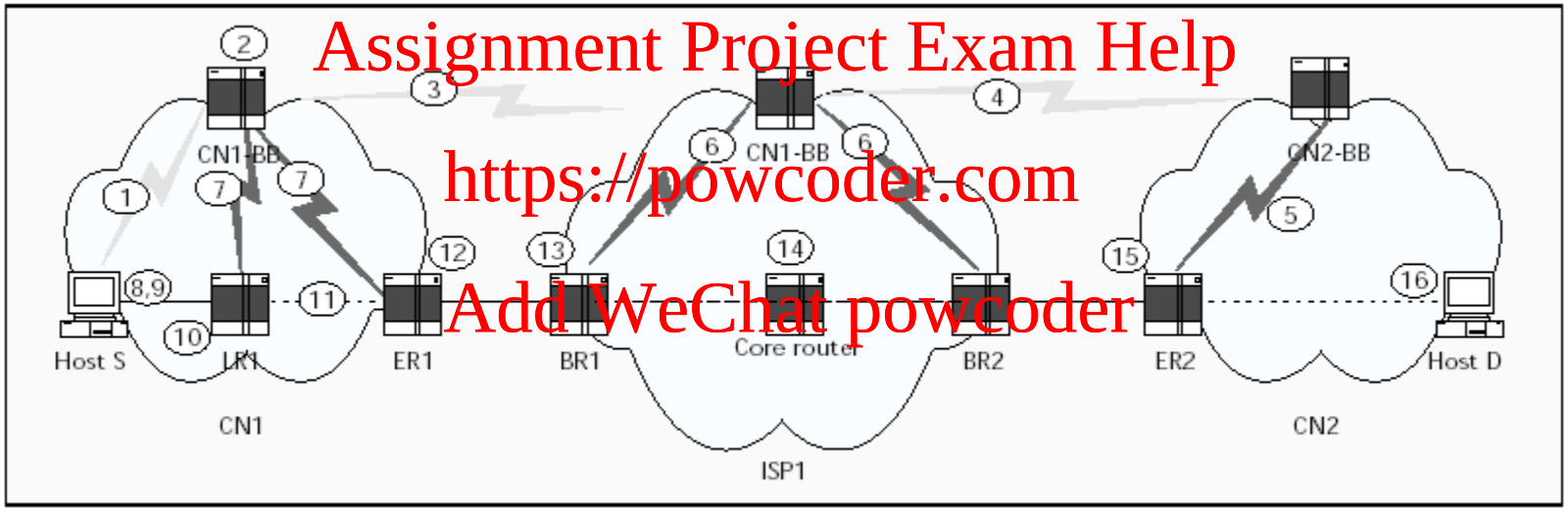


The delivery process of assured service with a static SLA.

Assured Service Delivery (with static SLA)

1. Host S sends RSVP message to local BB, CN1-BB requesting AS
2. If CN1-BB grants request – configures LR1so that it can mark packets
   - CN1-BB replies to host S; otherwise error msg sent to S
3. Host S sends packets to leaf router LR1
4. If LR1 configured to mark packets, it set DSCP of the packets
5. Every router from LR1 to ER1 does BA classification
   - Marked packets considered "in profile", others "out profile"
6. BR1 policies traffic
   - "out" traffic is out
   - If "in" traffic exceeds its bit rate, excess packets are considered "out"
7. All routers between BR1 and BR2 perform BA classification
8. ER2 performs same operation as BR1
9. Packets are eventually delivered to host D

Premium Service Delivery (with dynamic SLA)



The delivery process of premium service with a dynamic SLA.

Premium Service Delivery (with dynamic SLA)

Phase 1 – Signaling

1. Host S sends RSVP PATH msg to CN1-BB
2. CN1-BB makes admission control decision
   - If request denied, error msg send back to S
3. Request accepted by CN1-BB, sends PATH msg to ISP1-BB
4. ISP1-BB makes admission control decision
   - If request denied, error msg send back to CN1-BB, sender S notified
   - If request accepted, ISP1-BB sends PATH msg to CN2-BB
5. CN2-BB makes admission control decision
   - If request denied, error msg send back to ISP1-BB, sender S notified
   - If request accepted, CN2-BB uses LDAP or RSVP to set classification and policing rules on ER2
     - CN2-BB then sends RSVP RESV msg to ISP1-BB
6. ISP1-BB receives RESV message, configures classification and policing rules on BR1, and policing and reshaping rules on BR2
   - Sends RESV msg to CN1-BB
7. CN1-BB receives RESV message, sets classification and shaping rules on LR1 so that traffic is conformant, also sets policing and reshaping rules on ER1
   - Sends RESV msg to host S
8. Host S after receiving RESV message can start

Premium Service Delivery (with dynamic SLA)

Phase 1 – Signaling (continued)

1. Signaling process is different from that in IntServ/RSVP model
   - Sender requests resources, not the receiver
   - Request may be rejected when BB receives PATH msg
     - In IntServ, request is rejected on RESV msg
   - BB can aggregate multiple request and make single request to next BB
   - Each domain behaves like a single node (BB); core routers not involved
2. State information installed by BB on boundary routers is soft state

Premium Service Delivery (with dynamic SLA)

Phase 2 – Data Transmission

1. Host S sends packets to LR1
2. LR1 performs MF-classification and sets DSCP bits
3. Routers between LR1 and ER1 perform BA-classification
4. ER1 performs BA classification, reshapes traffic for aggregation of flows heading towards BR1
5. BR1 classifies and policies.
6. Routers between BR1 and BR2 perform BA classification. BR2 also reshapes traffic
7. ER2 classifies and policies traffic
8. Premium packets delivered to host D

MPLS and DiffServ

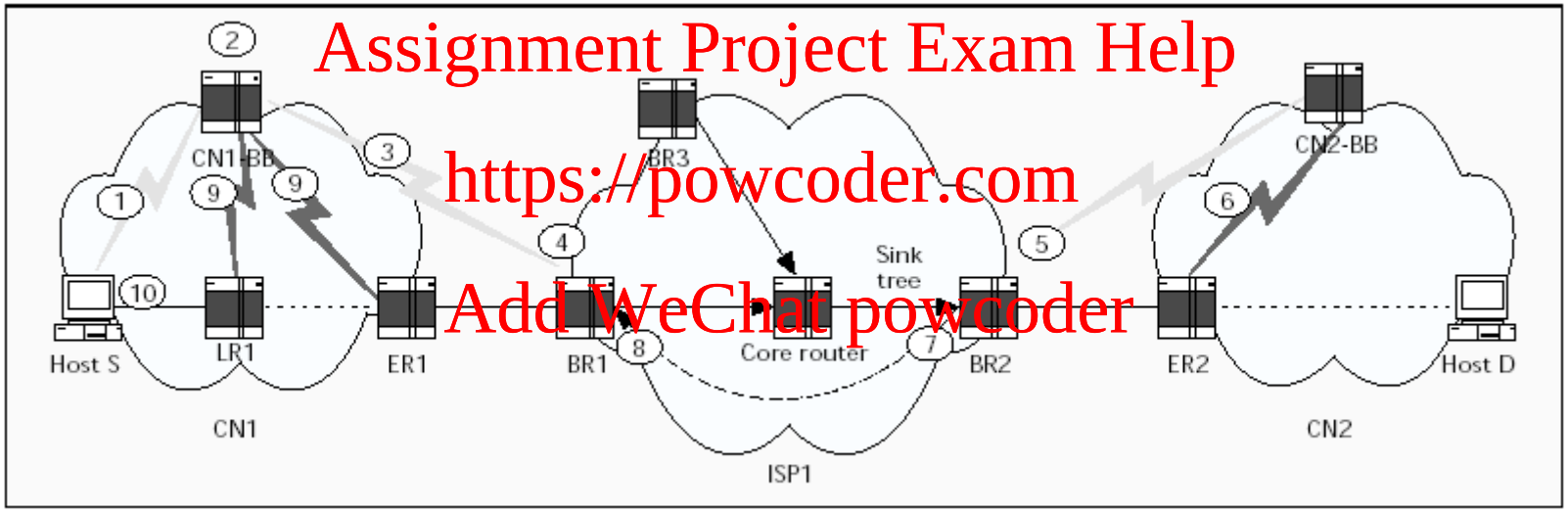
- At the Ingress of the ISP network, in addition to processing as in DS-field based architecture, MPLS is inserted into the packet.
- Core routers process packet based on its label and CoS field rather than DS field
- At Egress, MPLS header is removed

Whether a particular ISP's architecture is DS-field based or MPLS-based is transparent to other ISPs. Therefore the DS-field based and MPLS based architectures can easily interoperate

DS-field domain still needs a BB to allocate services and request resources when SLA is dynamic

MPLS based ISP networks may not need BB since LSPs are configured within ISPs and resource requests can be hidden from core routers. Admission control is done by ingress and egress routers

MPLS and DiffServ



The signaling process of dynamic premium service in an MPLS-based architecture.

MPLS and DiffServ

Signaling process for dynamic SLAs

1. Host S sends RSVP PATH msg to CN1-BB
2. CN1-BB makes admission control decision
   - If request denied, error msg send back to S
3. Request accepted by CN1-BB, sends PATH msg to BR1
4. BR1 decides if there are enough resources to send traffic to BR2
   - If request denied, error msg send back to CN1-BB, sender S notified
   - If request accepted, BR1 sends PATH msg through an LSP to BR2
5. BR2 sends PATH msg to CN2-BB
6. CN2-BB decides if its domain can support the traffic
   - If request denied, error msg send back to BR2, sender S notified
   - If request accepted, CN2-BB uses LDAP or RSVP to set classification and policing rules on ER2
     - CN2-BB then sends RSVP RESV msg to BR2
7. BR2 configures reshaping rules for traffic. It sends RESV msg through LSP to BR1
8. BR1 configures classification and policing rules for traffic. It sends RESV msg to CN1-BB
9. CN1-BB after receiving RESV message sets classification and reshaping rules on LR1 so that traffic is conformant; also reshaping rules on ER1
   - CN1-BB passes RESV msg to host S
10. Sender S starts transmitting data

References for these slides:

Xipeng Xiao and Lionel M. Ni, “Internet QoS: A Big Picture”, IEEE Network, 1999