NETWORK PROTOCOLS & SECURITY
23EC2210 R/A/E

Topic:

CONGESTION CONTROL

Session - 28

CONGESTION

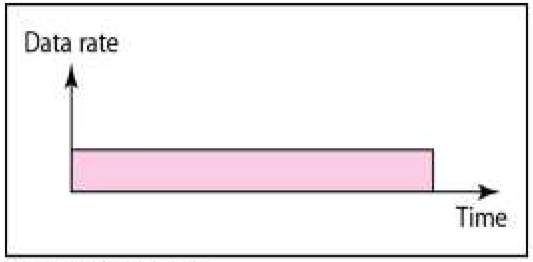
Data Traffic

- The main focus of congestion control and quality of service is data traffic.

- In congestion control we try to avoid traffic congestion.

- In quality of service, we try to create an appropriate environment for the traffic.

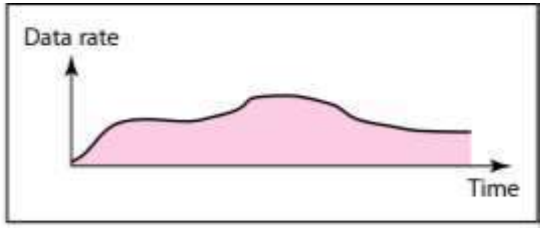
Three traffic profiles



a. Constant bit rate

Constant Bit Rate

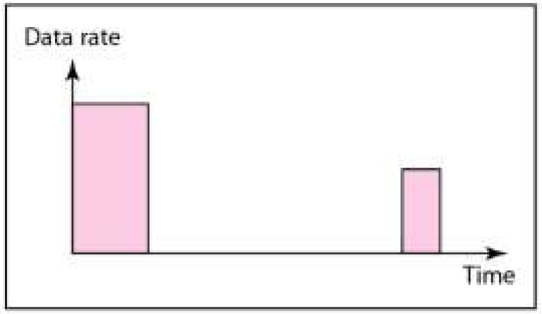
A constant-bit-rate (CBR), or a fixed-rate, traffic model has a data rate that does not change. In this type of flow, the average data rate and the peak data rate are the same. The network knows in advance how much bandwidth to allocate for this type of flow.



b. Variable bit rate

Variable Bit Rate

In the variable-bit-rate (VBR) category, the rate of the data flow changes in time. In this type of flow, the average data rate and the peak data rate are different.



c. Bursty

Bursty

In the **bursty data** category, the data rate changes suddenly in a very short time. It may jump from zero, for example, to 1 Mbps in a few microseconds and vice versa. Bursty traffic is one of the main causes of congestion in a network.

Congestion

- An important issue in a packet-switched network is congestion.

- Congestion in a network may occur *if the load on the network (the number of packets sent to the network) is greater than the capacity of the network (the number of packets a network can handle).*

- **Congestion control** refers to the mechanisms and techniques to control the congestion and keep the load below the capacity.

- Congestion happens in any system that involves waiting.

- Congestion cannot be completely avoided.

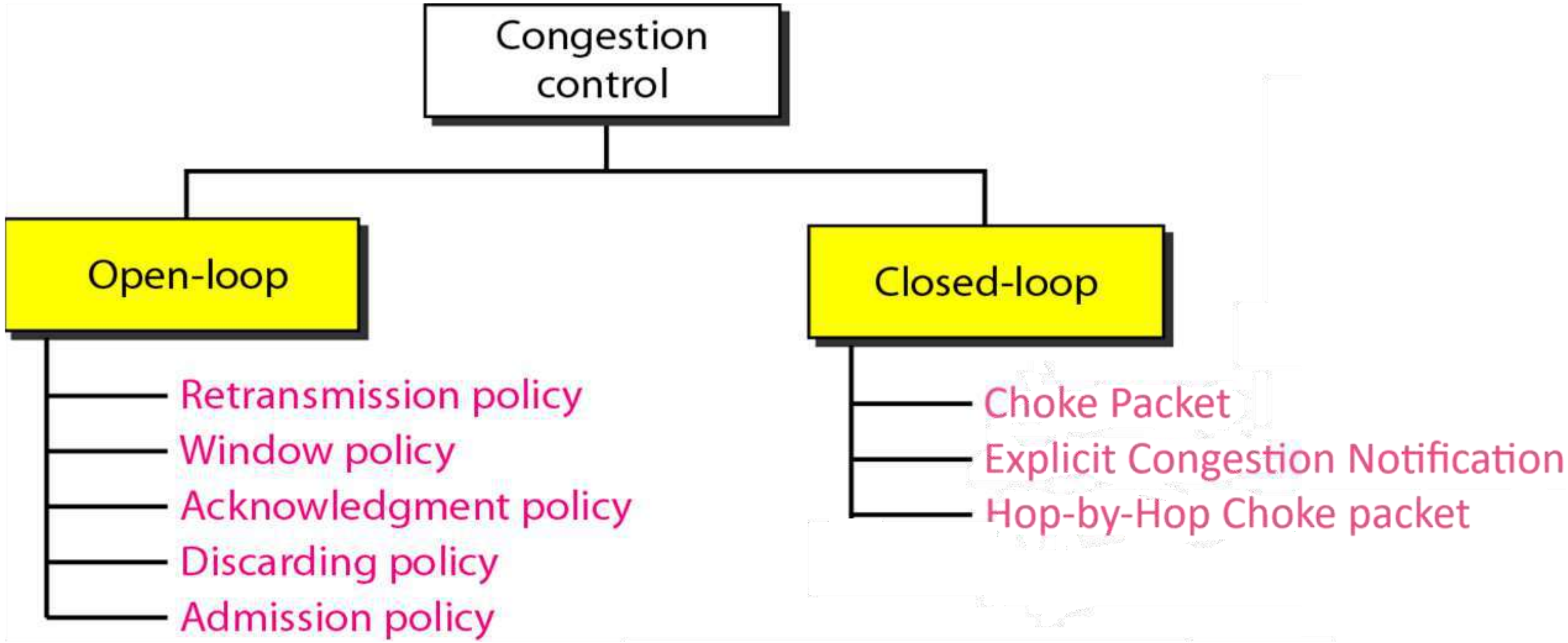
Congestion Control mechanisms

Congestion control refers to techniques and mechanisms that can either prevent congestion, before it happens, or remove congestion, after it has happened.

In general, we can divide congestion control mechanisms into two broad categories:

- **Open-loop congestion control**
- **Closed-loop congestion control.**

Congestion control categories



Policies adopted by open & closed loop congestion control

Open Loop Congestion Control

Open Loop Congestion Control

Open loop congestion control policies are applied to prevent congestion before it happens.

The congestion control is handled either by the source or the destination.

RETRANSMISSION POLICY

- If the sender feels that a sent packet is lost or corrupted, the packet needs to be retransmitted. This transmission may increase the congestion in the network.
- To prevent congestion, retransmission timers must be designed to prevent congestion and also able to optimize efficiency.

WINDOW POLICY

- The type of window at the sender's side may also affect the congestion. Several packets in the Go-back-n window are re-sent, although some packets may be received successfully at the receiver side. This duplication may increase the congestion in the network and make it worse.
- Therefore, Selective repeat window should be adopted as it sends the specific packet that may have been lost.

DISCARDING

- A good discarding policy adopted by the routers is that the routers may prevent congestion and at the same time partially discard the corrupted or less sensitive packets and also be able to maintain the quality of a message.
- In case of audio file transmission, routers can discard less sensitive packets to prevent congestion and also maintain the quality of the audio file.

ACKNOWLEDGMENT POLICY

- Since acknowledgements are also the part of the load in the network, the acknowledgment policy imposed by the receiver may also affect congestion. Several approaches can be used to prevent congestion related to acknowledgment.
- The receiver should send acknowledgement for N packets rather than sending acknowledgement for a single packet. The receiver should send an acknowledgment only if it has to send a packet(Piggybacking) or a timer expires.

ADMISSION POLICY

- In admission policy a mechanism should be used to prevent congestion. Switches in a flow should first check the resource requirement of a network flow before transmitting it further. If there is a chance of a congestion or there is a congestion in the network, router should deny establishing a virtual network connection to prevent further congestion

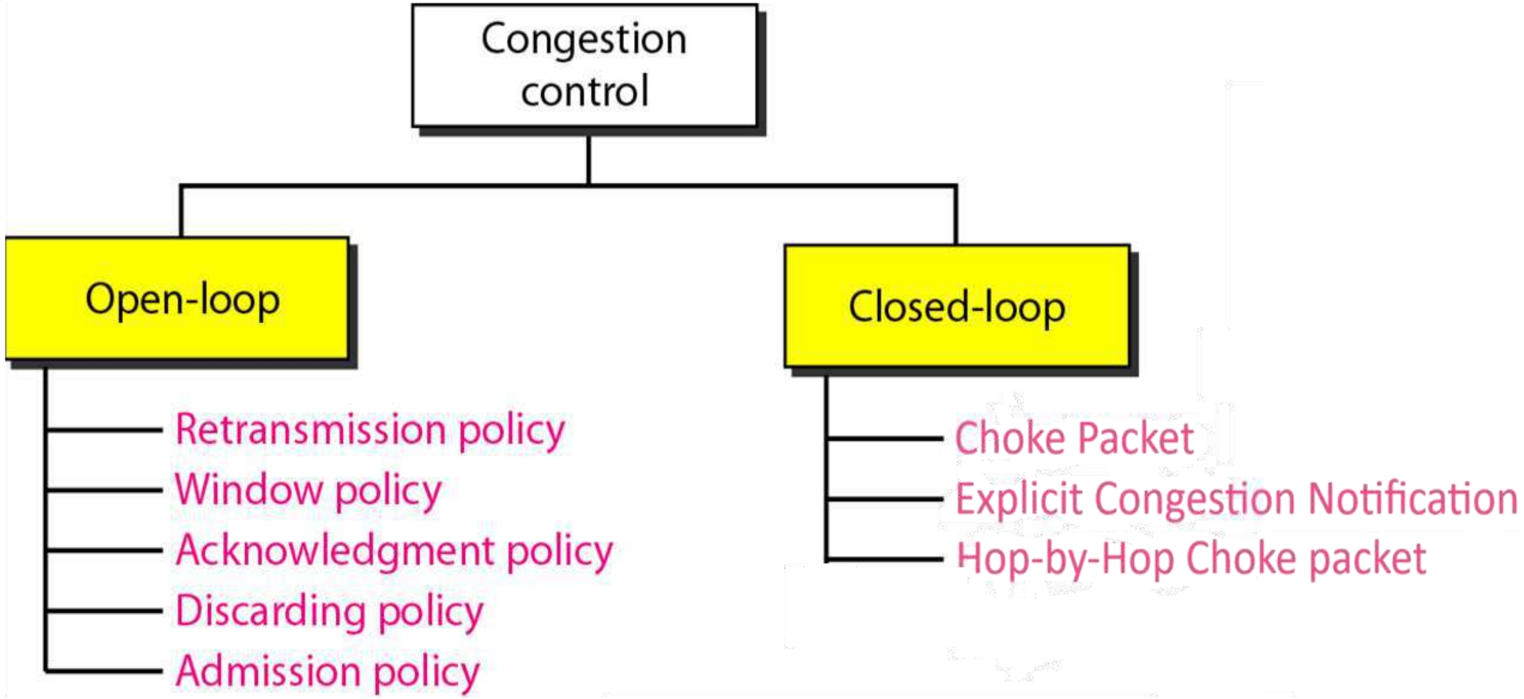
All the above policies are adopted to prevent congestion before it happens in the network

Closed Loop Congestion Control

Congestion control categories

- Closed loop congestion control techniques are used to treat or alleviate congestion after it happens.

- Several techniques are used by different protocols; some of them are listed here.



1. Choke Packets

- The most direct way to notify a sender of congestion is to tell it directly.

- In this approach, the router selects a congested packet and sends a **choke packet** back to the source host, giving it the destination found in the packet.

- When the source host gets the choke packet, it is required to reduce the traffic sent to the specified destination, for example, by 50%.

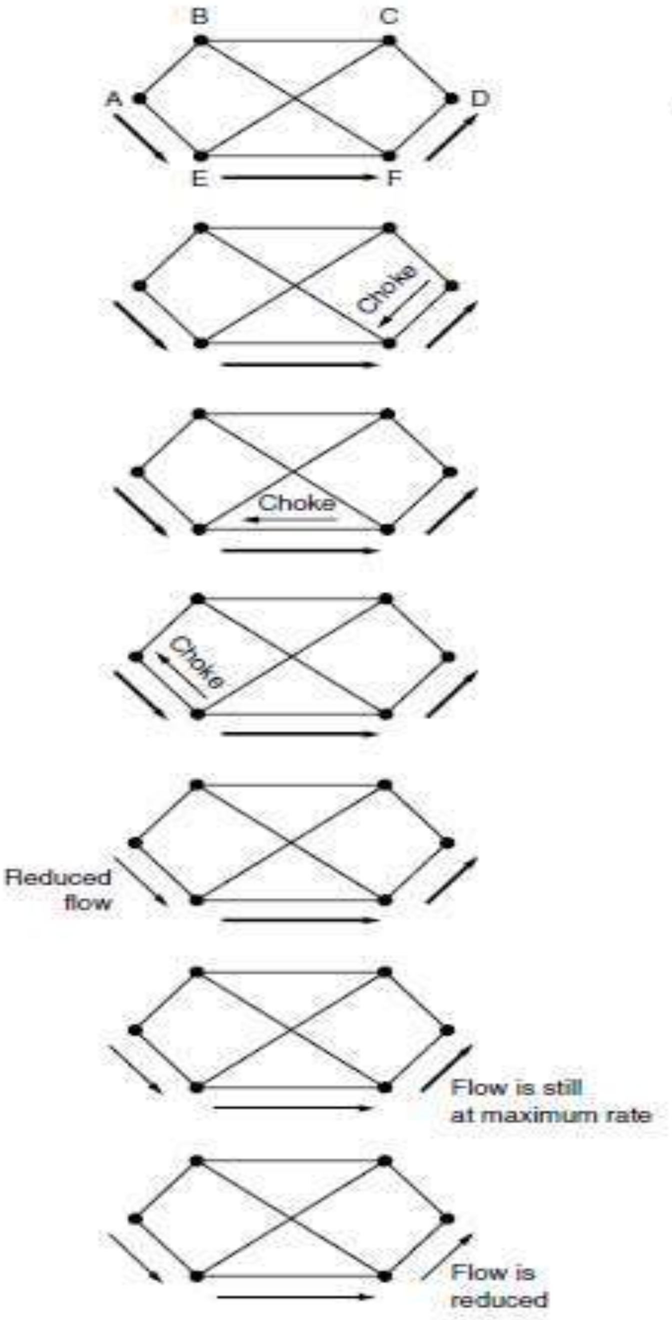


Figure A choke packet that affects only the source.

2.ECN (Explicit Congestion Notification)

- Used in internet.

- Instead of generating additional packets to warn of congestion, a router can tag any packet it forwards (by setting a bit in the packet's header) to signal that it is experiencing congestion.

- When the network delivers the packet, the destination can note that there is congestion and inform the sender when it sends a reply packet.

- The sender can then throttle its transmissi

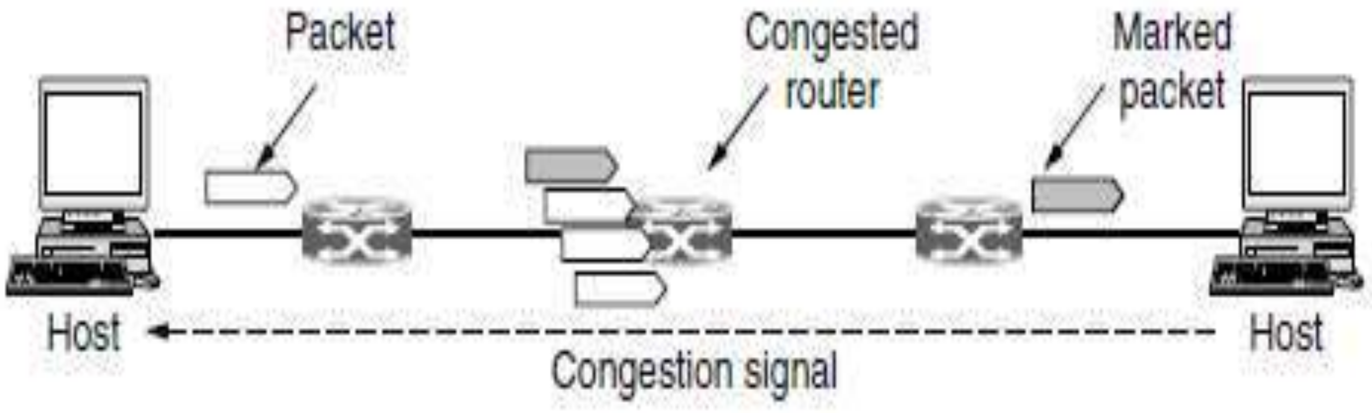


Figure 5-25. Explicit congestion notification

3.Hop-by-Hop Backpressure

- At high speeds or over long distances, many new packets may be transmitted after congestion has been signaled because of the delay before the signal takes effect.

- An ECN indication will take even longer because it is delivered via the destination.

- An alternative approach(Hop-by-Hop) is to have the choke packet take effect at every hop it passes through

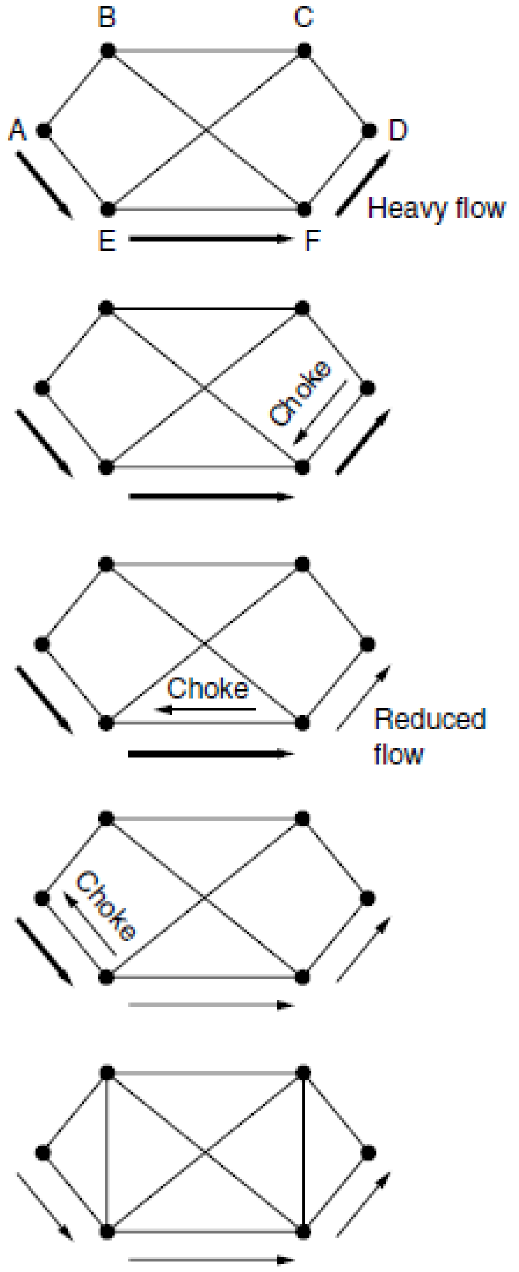


Figure. A choke packet that affects each hop it passes through

THANK YOU

KL
(DEEMED TO BE UNIVERSITY)

Team –Network Protocols and Security