Week5 Review Notes

ELEC0099: Introduce to Internet Protocol Networks 21/22

RUFENG DING

Contents

1 Multicast

eg. a TV station want to send **n** packets to **n** receivers.

what is multicast? The transmission of information to more than one destinations.

1. computer asks its router to join a group
2. router joins the multicast distribution tree

1.1 IGMP Internet Group Management Protocol

Multicast STEP-1

1. a computer want to join a multicast group using IGMP.
2. it sends an IGMP join message to its router.
3. **membership is dynamic** routers will periodically **poll** host in the network to verify if they are still in the group.
4. IGMP we put it as a integral part of IP.

1.2 Tree formation

Multicast STEP-2

1. it is the difficult part.
2. using Multicast Routing Protocol.

3. after join in they will reach the router and hosts in the network.
4. routers in a group's multicast tree have the group address in their Routing Tables.

DVMRP-Distance Vector Multicast Routing Protocol

1. all routers receive traffic for all groups.
2. routers not in group send **Prune** message up to the tree.
3. routers no-member-neighbours remove multicast entry.
4. repeated periodically.

MOSPF Multicast Extensions to OSPF

1. DVMRP generates lots of useless traffic(Prune).
2. OSPF have the information How to get to each node.
3. MOSPF use the information to multicast.
4. **Big Disadvantage** each router has to know all the group memberships.

PIM-SM - Protocol Independent Multicast - Sparse Mode

1. router do not know in advance what to do to join a group.
2. each group has a Rendez-Vons Point in advance.
3. router sends a unicast to RP and RP replies and the routers on this path are automatically part of the distribution tree.
4. Hosts wishing to multicast just send to the RP.

1.3 Muticast Extra Notes

1. Multicast address allocation needs independently. eg. MADCAP(RFC 2730).
2. original model : anybody can send message to a group. Reality: only specified sources can send.(security and scale)
3. IP multicast maps directly into Ethernet multicast. *If there is more than one member in a LAN, potentially only one packet is sent.*

1.4 Problems

1. each groups requires **state** (routing table entries) in every router in the path.
2. routers in the core of the Internet will require informations for every groups.
3. *difficult to be used for time shifted content.*
4. difficult to be achieve reliability and congestion control.
5. ISPs selling bandwidth. Multicast saves bandwidth.
6. Multicast today is only available in limited intra-domain deployments.

2 SDN software Defined Networking

2.1 define

- hardware only do packet forwarding.
- all control is done in software in a centralized manner.
- maybe far away in a cloud.

2.2 OpenFlow Protocol

Secure Channel connected to a controller via SSL.

Flow Table connected to PCs.

1. supports layer2/3/4 protocols
2. rule can be flexibly defined by combination of different matching fields
3. no rule match the packet is dropped or escalated.

Packet Escalation packet don't match any rules will be sent back to the controller. And, the controller will then calculates rule and send it back to router. Rules can be reset. This work well with TCP harder with UDP.

2.3 SDN Interface

1. Northbound Interface To applications.
2. Southbound Interface OpenFlow.
3. Eastbound Interface To Controllers in other domains.

2.4 Trends

1. P4
2. Network Function Virtualization

3 Queuing

- arrival rate and service rate.
- Most common Arrival Distribution : Possion
- Most common Servicing Distribution : Exponential

3.1 Kendal's notation ASCKND

- A : Arrival Process
- S : Service Time Distribution
- C : Numbers of Servers
- K : Numbers of places on the queue
- N : Population size
- D : Queue Discipline (FIFO)

Because Possion and Exponential is both Markovian we use M in the notation.
Typically we only use the first 3 parts.We assume the queue size is infinite.The Queue Discipline is FIFO. eg. M/M/1
in practice in computer networking : we use MM1 or more often MD1.
D stand for Deterministic because it is often a fixed rate.

3.2 Queuing assumptions

1. FIFO
2. no bulking or reneging
3. arrivals are independent
4. service times are independent
5. arrival and service rates remain stable

3.3 Queuing performance for M/M/1

average number of packets in the queue

$$Lq = \frac{\lambda^2}{\mu(\mu - \lambda)}$$

average time packet spends on the queue

$$Wq = \frac{\lambda}{\mu(\mu - \lambda)}$$

4 Active Queue Management

4.1 Multiple Queues

- each output port has many queues: 1perFlow 1perClass
- How to choose next ?
- several approaches: Fair Queuing / Weighted Fair Queuing / Priority Queuing

4.2 Fair Queuing (FQ)

simple scheme : serving the output queue for each flow in a round-robin way.(skip empty flow)

1. Greedy flows are implicitly penalised.
2. **Problem** flows with large packets are favoured in terms of throughput in comparison to flows with small packets

Bit Round Fair Queuing (BRFQ) using a bit-by-bit round-robin discipline not whole packets.

1. no preferential treatment
2. good for classless best-effort traffic only

4.3 Weighted Fair Queuing (WFQ)

add weight to a round-robin scheme

- each connection gets a queue

- each connection reserves some bandwidth
- every packet is assigned a virtual finishing time

$$F_i^k = F_i^{k-1} + \frac{L_i^k}{\phi_i}$$

F is Virtual finishing time
L is Time to transmit the packet
Φ is the Bandwidth allocated

4.4 Priority Queuing (PQ)

Queues are assigned priorities from high to low.
Good for important traffic but can lead low priority queues to **starvation**. And, they maybe dropped finally.

Priority Queuing with Rate Limits solve the starvation problem.
A priority is served until a cap bandwidth rate is reached its "rate limit"

4.5 Proactive Packet Dscard

- as the queue occupancy grows, packets are dropped before the queue gets full
- TCP senders perceive packet loss as a congestion signal and back-off
- as such, TCP-based flows will back-off to helping alleviate congestion before transit router buffer get actually full
- the network do not oscillate between congestion and under-utilisation, with all TCP sources backing off almost simultaneously.

4.6 Random Early Detection (RED)

- RED used as a proactive packet discard mechanisms
- queue is split into 3 parts though two thresholds:0,TH_{min},TH_{max},1. TH is the abbreviation for threshold
- queue occupancy < part 1 added to the queue.
- queue occupancy in part 2 packet is dropped based on a calculated probability P_a which depends on various parameters and increases with queue utilisaion.
- queue occupancy > part3 the packet always dropped.

5 Quality of Service

1. Flow based Queuing : Integrated Services Architecture(RFC 1633) Uses RSVP
2. Class based Queuing : Differentiated Services Architecture RFC2475

5.1 IETF integrated Services Architecture

- providing QoS guarantees in IP networks for individual application sessions
- Resource reservation: routers maintain state info of allocated resources
- admit/deny new call setup requests

Call Admission arriving session must:

- Declare its QoS requirement:R-spec
- Characterize traffic it will send into network:T-spec

The protocol is RSVP : carry R-spec and T-spec to routers

RSVP

1. sender sends a PATH message along the way it checks if every router has resources
2. Receiver sends RESV message allocating resources in the router

attention:

1. every router needs to check every message
2. RSVP uses soft state: Messages need to be sent periodically otherwise reservation is removed

problems with IntServ/RSVP

- each connection need to store reservations in every routers on the PATH.
- very big cost in core routers.
- scalability has made intServ unsuccessful.

5.2 Diffserv Architecture

define two types of routers : edge router and core router.
edge router

- per-flow traffic management
- marks packets in classes
- as in-profile and out-profile

core router

- per-class traffic management
- buffering and scheduling
- based on marking at edge

Classification in IPv4

- packet is marked in the Type of Service (TOS) in IPv4 and Traffic Class in IPv6.
- 6 bits used for Differentiated Service Code Point (DSCP) and determine PHB that the packet will receive.
- 2 bits are currently unused.

PHB is **per-Hop Behaviors**

- Expedited Forwarding(EF) PHB
- Assured Forwarding(AF) PHB (more soft guarantees AF4 better AF3 better AF2 better AF1)
- Default(Best-Effort) with no QoS guarantees

Multidomain DiffServ To work across more than one domain ISPs have to agree on SLA(Service Level Agreements) for every type of traffic.
It is not clear how anybody can guarantee QoS to end-to-end applications.

Bandwidth Brokers would be a good solution to end-to-end

- each domain runs a Bandwidth Broker

- app contact BB in their domain
- requires standardization
- still an open research issue

5.3 The Over-Provisioning Alternative

- Make sure adequate resources are always available in the network given the expected traffic demand.
- it is possible in core network but harder in access network and in peering points between ISPs.

problems remains:

- no strict guarantees given the statistical nature of traffic.
- Moore's law : as capacity increases, demand will also increase to consume it.
- arguably not economical, especially for tier-2/tier-3 ISPs

In the other hand if we had admission control which accept flows in 99.999% of the cases. Do we need this?