MANCHESTER 1824
The University of Manchester

COMP28411 Computer Networks
Lecture 9

Nick Filer

Multimedia – 3

Some material from:

Kurose & Rose – Chapter 7 + Slides

Halsall – Multimedia Communications

18/11/2014 COMP28411 Multi-Media L2 NPF 1

MANCHESTER 1824
The University of Manchester

Summary

- Multicast Routing from Lecture 2.
- Quality of Service (QoS)
  - Scheduling
  - Policing
- If time:
  - **Digital Living Network Alliance (DLNA)** and
  - **Universal Plug and Play (UPnP)**

18/11/2014 COMP28411 Multi-Media L2 NPF 2

© University of Manchester 2013

MANCHESTER 1824
The University of Manchester

IGMP Multicast Operation

Internet **G**roup **M**anagement **P**rotocol

- Destination nodes (the network card) report multicast addresses they wish to receive/send traffic from/to.
- A multicast router on a subnet that has the lowest address handles reports and sends queries to maintain its group membership data. In v2, there is also a leave group message.
- So now the local router knows someone wants to use multicast.......
  - How does the multicast get to/from the local router?

TTL Conventions

Pre: 1996 – compare to IPV6 scopes.

0 = localhost

1 = same subnet

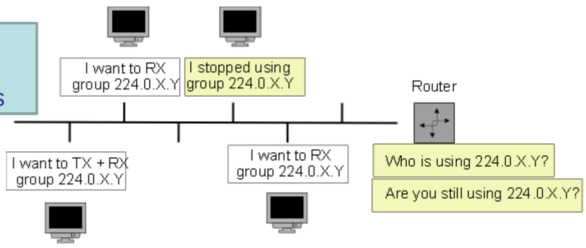
< 32 same site

< 64 same region

< 128 same continent

255 Unrestricted

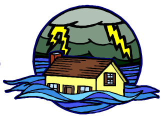
Example IGMP messages



18/11/2014

MANCHESTER 1824
The University of Manchester

Routing Between Sender and Receivers - 1



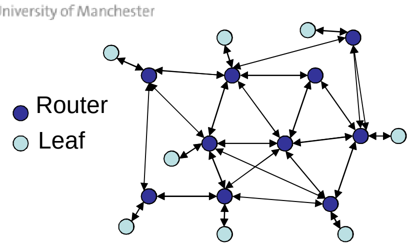
- Sender – Anywhere on the Internet
- Receivers – Can be anywhere
  - Both sender and receivers register with local routers using IGMP
  - How do they find one-another?
- Simplest and least efficient is FLOODING:
  - From source node(s) tell all neighbours, forward to all there neighbours until all connected nodes in tree/graph have received the search discarding repetitions).
    - Simple – no routing table needed – just record of recently seen addresses – but even this may be large!
    - Scaling issue – lots of duplication.

Example: Digital Living Network Alliance (DLNA) for sharing of digital media between devices <phone, computer, TV, Camera> uses multicast and Universal Plug and Play (UPnP) for discovery + control.

18/11/2014 COMP28411 Multi-Media L2 NPF 4

MANCHESTER 1824
The University of Manchester

Spanning Tree



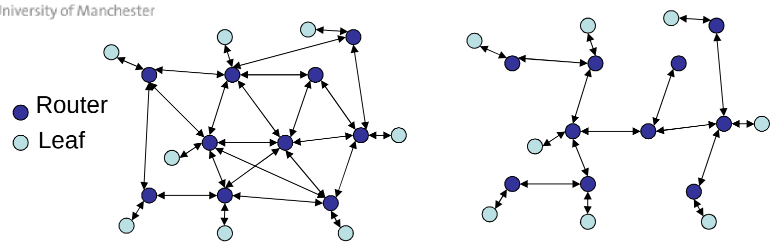
- Select a sub-set of connected nodes – spanning tree.
- Multicast router forwards packets to all nodes that are part of the spanning tree (not the one it arrived on!).
  - No loops
  - Still reaches all the tree eventually.
  - Lots of good algorithms to find (*minimum*) spanning trees.
  - But, concentrates traffic on a few core routes, not always the best path from source to all members.

18/11/2014 COMP28411 Multi-Media L2 NPF 5

MANCHESTER 1824
The University of Manchester

Spanning Tree

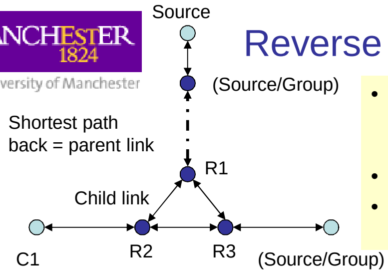
P



- Select a sub-set of connected nodes – spanning tree.
- Multicast router forwards packets to all nodes that are part of the spanning tree (not the one it arrived on!).
  - No loops
  - Still reaches all the tree eventually.
  - Lots of good algorithms to find (*minimum*) spanning trees.
  - But, concentrates traffic on a few core routes, not always the best path from source to all members.

18/11/2014 COMP28411 Multi-Media L2 NPF 6

Reverse Path Broadcasting - 1



- Router forwards packet if it arrives on a link the router thinks is shortest path back to (source/group).
- Otherwise discards packet.
- R2 considers R1 as on shortest link back, not R3.

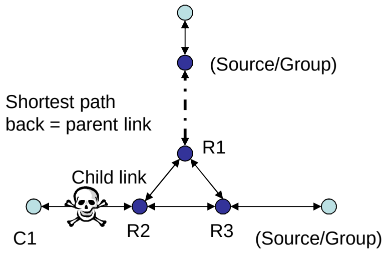
- Group specific spanning tree for each (potential/active?) source. Result is source rooted delivery trees for each source per group.
- Further pruning is if a neighbour router does not consider this router as being on its shortest path back to the source.
  - Easy as all routers have a full topological record.
  - Can either advertise (R1 ➔ R2, R1 ➔ R3), discard (R2 ➔ R3, R3 ➔ R2) or send backwards a “poison reverse” advert to upstream routers (C1☠➔ R2 ☠➔ R1… if no child in group).

Reverse Path Broadcasting - 2

- Reasonably efficient, quite simple.
- Routers only need relatively local knowledge.
- Packets always follow “shortest” (?) path.
- Packets from different sources in same group follow different trees/paths so lower likelihood of bottleneck.
- However, the forward adverts still happen whether or not the sub-tree has a group member.
  - R2 & C1 are searched before pruning later.

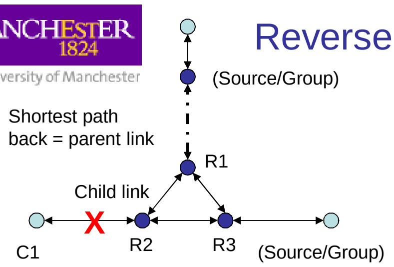
© University of Manchester 2013

Truncated Reverse Path Broadcasting



- Using IGMP, multicast routers work out the group memberships for leaf networks. So avoid forwarding if no current members of the group.
- The sub-network tree is pruned by the router.
- But only the final router does this removing some traffic on leaf sub-networks. (R2 does this)

Reverse Path Multicasting - 1



- So far, each leaf router (R2 & R3 above) receives the 1st multicast packet in a source/group.
- If there is a group member in any leaf sub-network the leaf router forwards the packet, otherwise it sends back a prune packet (R2 → R1).
- If R1 (n this example) gets prune messages from both R2 and R3 (all downstream interfaces, it can send the prune upstream.
  - Only LIVE tree branches are now used.
  - Prune information must be stored

© University of Manchester 2013

MANCHESTER 1824
The University of Manchester

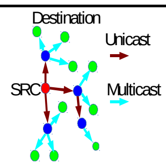
Reverse Path Multicasting - 2

- Because both the tree and the source + group memberships change the multicast tree must be **refreshed regularly**. This results in a full flood and prune.
- There are still scaling issues in the flooding and pruning.
- All routers need to keep information for each group and all its sources.
- In practice may need to cache/group before flooding of add & prune messages to reduce control traffic but at the expense of some extra latency.

18/11/2014 COMP28411 Multi-Media L2 NPF 11

MANCHESTER 1824
The University of Manchester

Core Based Routing



- A set of static “centres” are identified at different locations in the network. Multicast traffic is duplicated and may be unicast to these centres.
- Branches grow from core routers towards multicast users. Traffic is multicast from core routers to the leaves of the tree.
- This is more scalable.
  - Router only keep group, not source per group, information.
  - Full tree flooding is avoided as “centre” are statically defined and can be unicast to. Multicast is only used in local clusters.
- Issues:
  - Traffic concentration near core routers. Traffic from all sources uses common links towards core routers.
  - Shared links can create sub-optimal routes and therefore delays.

18/11/2014 COMP28411 Multi-Media L2 NPF 12

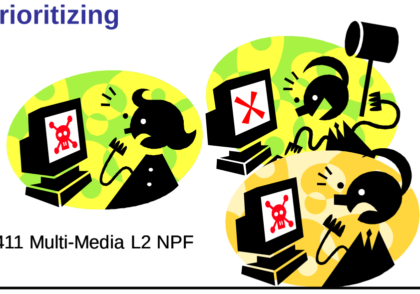
© University of Manchester 2013

Real-time Services Wanted?

Q

- What does the internet need to do so real-time multimedia works?
- **TCP + UDP + Real Time Protocol.**

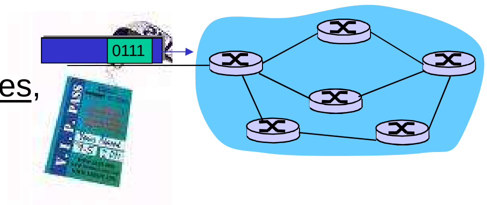
- What does the internet need to do so real-time multimedia always works perfectly?
- **Quality of Service (QoS)**
  - **Classes of Service & Prioritizing**
  - **Policing**
  - **Scheduling**



18/11/2014 COMP28411 Multi-Media L2 NPF 13

Providing Multiple Classes of Service - QoS

- Thus far: making the best of **best effort** service
  - **One-size fits all** service model
- Alternative: **multiple classes of service**
  - Partition traffic into classes
  - Network treats different classes of traffic differently (**analogy**: VIP service vs regular service)
- Granularity:
  - Differential service among multiple classes, not among individual connections

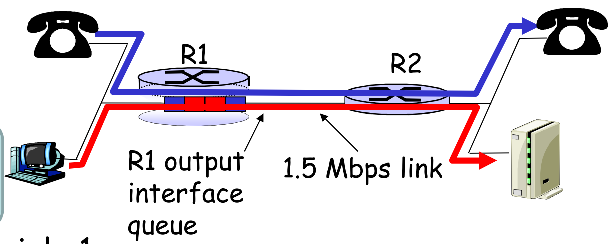


18/11/2014 COMP28411 Multi-Media L2 NPF 14

© University of Manchester 2013

Scenario: Mixed FTP and Audio

- Example: 1Mbps IP phone + FTP share 1.5 Mbps link.
  - Bursts of FTP can congest router, cause audio loss.
  - Want to give priority to audio over FTP.



Marks are labels. Look up: MPLS & RSVP for routing!

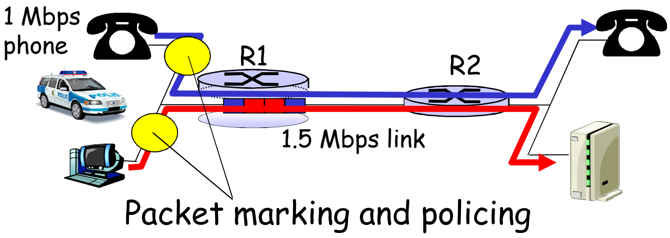
Principle 1

Packet **marking** needed for router to distinguish between different classes; and new router policy to treat packets accordingly

18/11/2014 COMP28411 Multi-Media L2 NPF 15

Principles for QOS Guarantees (more)

- What if applications misbehave (audio rate is higher than declared rate)?
  - **Policing**: force source adherence to bandwidth allocations
- Marking and policing at network edge:



Principle 2

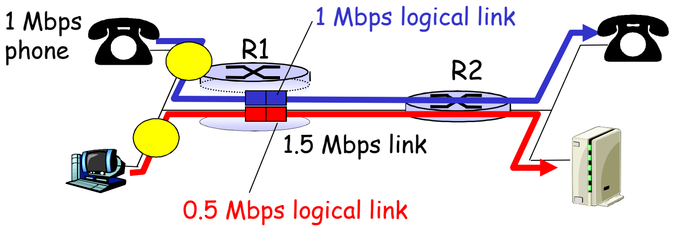
Provide protection (*isolation*) for one class from others

18/11/2014 COMP28411 Multi-Media L2 NPF 16

© University of Manchester 2013

Principles for QOS Guarantees (more)

- Allocating *fixed* (non-sharable) bandwidth to a flow can be *inefficient* in use of bandwidth if flows do not use their allocation! e.g. At night.

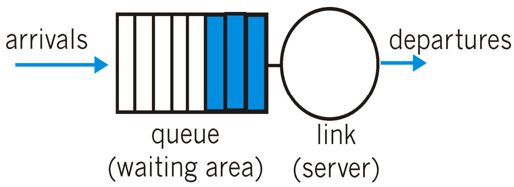


Principle 3

While providing isolation, it is desirable to <u>use resources as efficiently</u> as possible

Scheduling And Policing Mechanisms

- Scheduling: Choose next packet to send on link
- Policing: Action when resources (**total** OR **allocated**?) exceeded.
- FIFO (first in first out) scheduling: Send in order of arrival to queue
  - Discard policy: If packet arrives to full queue: who to discard?
    - Tail drop: Drop arriving packet ← **Default on Internet**
    - Priority: Drop/remove on priority basis
    - Random: Drop/remove randomly
    - Front drop: Good option for real-time media?



What if: Intermittent audio mixed with many large file transfer bursts?
Is it fair?
Jumbo packets up to 9K bytes not a problem but above 15K could delay Gigabit Ethernet for longer than 1500 bytes on 100Mbps Ethernet

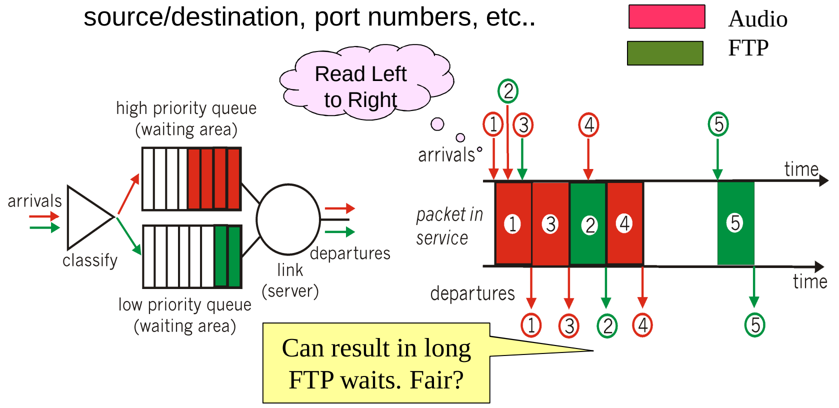
© University of Manchester 2013

MANCHESTER 1824
The University of Manchester

Scheduling Policies: more

Priority scheduling: Transmit highest priority queued packet

- Multiple *classes*, with different priorities
  - Class may depend on marking or other header info, e.g. IP source/destination, port numbers, etc..



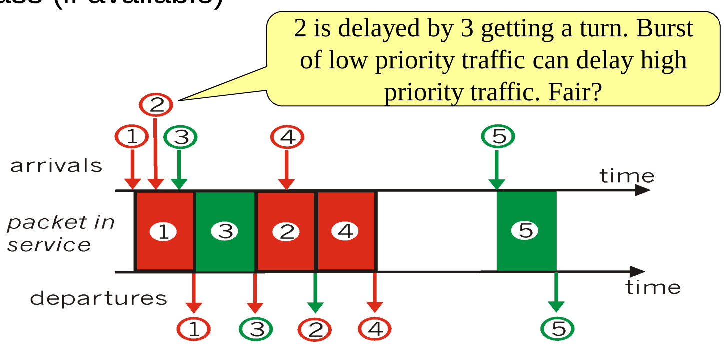
18/11/2014 COMP28411 Multi-Media L2 NPF 19

MANCHESTER 1824
The University of Manchester

Scheduling Policies: still more

Round Robin Scheduling:

- Multiple classes
- Cyclically scan class queues, serving one from each class (if available)



18/11/2014 COMP28411 Multi-Media L2 NPF 20

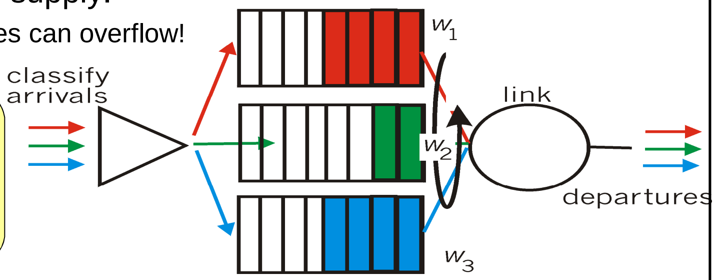
MANCHESTER 1824
The University of Manchester

Scheduling Policies: still more

Weighted Fair Queuing (WFQ):

- Generalized Round Robin.
- Each class gets weighted amount (fraction) of service in each cycle.
- Applied at queue exit which ensures demand does not exceed supply.
  - But queues can overflow!

Each gets fair share.
What happens to unused resource?
Bursts when demand is low/high?



18/11/2014 COMP28411 Multi-Media L2 NPF 21

MANCHESTER 1824
The University of Manchester

Policing Mechanisms

Goal: Limit traffic to not exceed declared parameters.

Two common-used criteria – used together:

1. *(Long term) Average Rate:* How many packets can be sent per unit time (in the long run)
   - Crucial question: What is the interval length? 100 packets per sec or 6000 packets per min have same average!
   - Short time – Better control of bursts. Long time – Less burst throttling.
2. *Peak Rate or (Max.) Burst Size :* maximum number of packets sent consecutively (with no intervening idle)
   - Limit peak rate to short periods. e.g., 6000 packets per min. (ppm) avg.; 1500 ppm
   - Must be able to maintain average rate.
   - Peak rate OK for short time or when others not also at peak.

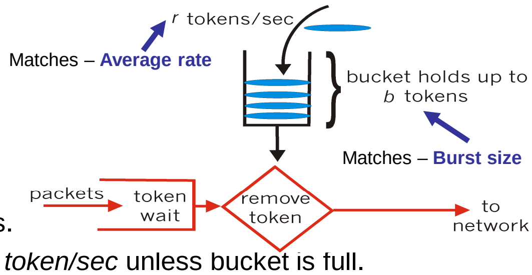
18/11/2014 COMP28411 Multi-Media L2 NPF 22

© University of Manchester 2013

Policing Mechanisms

Token (Leaky) Bucket: Limit input to specified Burst Size and Average Rate.

Acts as a meter. Packets only advance when there is a token available.

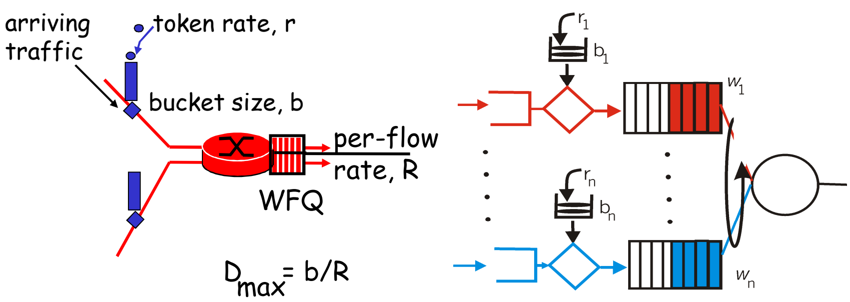


Bucket can hold b(urst) tokens.

- Tokens generated at *r(ate) token/sec* unless bucket is full.
  - Either put in low priority (e.g. best-effort) queue or dropped.
- *Over an interval of length t:*
  - *Number of packets admitted less than or equal to (r t + b).*
- If arrival rate traffic <= token rate (r) then
  - agreed bandwidth and delay/jitter constraints can be met.
  - Stored extra tokens used to clear bursts.

Policing Mechanisms (more)

- Token bucket and WFQ combine to provide guaranteed upper bound on delay, i.e., *QoS guarantee*!
  - Provided peak rate not exceeded for too long – buffer overflow. And
  - Total allocation does not exceed resources.



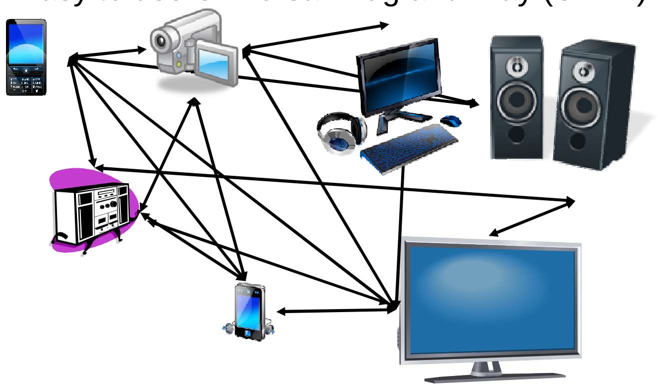
© University of Manchester 2013

Home Multimedia
If there is time….

- SIP or similar protocols work great for voice and often also for limited video.
- At home we need something very flexible to allow all our media devices to interact.
  - Throw media from storage to audio/display devices.
  - Handle mobility, devices coming and going.
  - Allow any device to find and use any other.
    - But subject to some security/authorization limits.
- **Digital Living Network Alliance (DLNA)** is one protocol family ....
- But is ONLY for local use. Does not explain, for example, how BBC iPlayer sends media to thousands of users?

Digital Living Network Alliance (DLNA)

- Easy to use Universal Plug and Play (UPnP) streaming



- Everything talks to everything – in theory!
  - In practice, lots talks to lots.

© University of Manchester 2013

MANCHESTER 1824
The University of Manchester

UPnP-1

- Based on TCP/IP, HTTP, XML, ... UDP port 1900
- Control points (CP) and controlled devices.
- Zero configuration! DNS/DHCP not required!
- Just sends data!
  - No executables, minimizes version & security issues.
- No machine/language restrictions.
- Address auto configuration using 169.154.0.0/16 or FE80::/10 addresses. Point to point. Not routable. Link local – no external connectivity.
  - Address is selected randomly (RFC 3927) using uniform distribution.
    - Seeded from MAC address of device. Why not time etc.?
    - Conflict resolution using ARP probes or similar.

18/11/2014 COMP28411 NPF MM1 27

MANCHESTER 1824
The University of Manchester

UPnP-2

- Name resolution – similar to DNS.
  - Each computer stores address (A/AAAA), message transfer (MX), service location record (SRV) data like DNS.
- Can then issue a request for IP address associated with hostname:
  - mDNS uses multicast address 224.0.0.251 or FF02::fb
  - DNS-SD (service discovery) uses standard DNS queries but must explicitly ask for non-local worldwide advertisement if wanted.
- Simple Service Discovery Protocol (SSDP) allows adverts to control points:
  - Can send adverts or listen for them passively – has a URL.
  - Uses the URL to find out lots more using XML.
  - Get a list of actions + variables the device can respond to.

18/11/2014 COMP28411 NPF MM1 28

© University of Manchester 2013

MANCHESTER 1824
The University of Manchester

UPnP-3

- Devices register to listen for events and associated values. Can respond using their own events.
- First event is usually to download a web page.
- Modern UPnP now supports remote access, NAT traversal and some form of authentication.

UPnP Startup steps

1. CP and device get addresses.
2. CP finds interesting device.
3. CP learns about device capabilities.
4. CP invokes actions on device.
5. CP listens for state changes on device.
6. CP controls device and/or views device status using HTML.

18/11/2014 COMP28411 NPF MM1 29

MANCHESTER 1824
The University of Manchester

DLNA

- Now we know how to connect devices. DLNA sits on top of UPnP to connect all sorts of media devices as clients or players to one another.
- DLNA provides lots of device classes with many transport methods (e.g. RTP) and codecs/transforms.
- The only big company not involved is using AirPlay instead. But there are Apps to work around this.
- On Android try: UPnP Monkey, MediaHouse UPnP – lots others.
- iPhone try: media:connect or Creation 5.

18/11/2014 COMP28411 NPF MM1 30

© University of Manchester 2013

Summary

- Delivering media is a continually developing solution.
- Demand, location, time of day, density of users all effect choice of method.
- We have:
  - **TCP** – End-to-end unicast, reliable but subject to delays, duplication, bottlenecks (hot-spots).
  - **UDP** - End to end unicast, unreliable, less delay problems due to accepting losses. Avoid duplication partially via multicast.
    - Multicast, lots of ideas and protocols. Demand sensitive but more efficient than unicast near tree leaves.
  - **P2P** using **unicast** or **multicast** - **great for load spreading**!

More Summary

- **Real time multi media**
  - Packet loss, delay and jitter.
  - Recovery from lost packets a few ideas given but lots more clever ideas
    - **fix** OR skip, play nothing
    - play previous, next or synthesise something
    - guess.
- **Quality of Service**
  - Shown how it can be done.
    - Where is it done?
    - Where/how is "**Peak Rate**" policed?
- **Next:** Jump down to **Data-Link** and **Physical Layers**

© University of Manchester 2013

Questions

- When is jitter a problem?
- Why doesn't having a higher data rate always improve the user experience of real-time media delivery?
- Why is it much easier to measure Round Trip Time (RTT) than one way packet latency?
- Which European/Asian/American/African capital cities can you VoIP to with little or no latency problems? Which do not work well?
- Why did iPlayer reputedly use P2P in the past? Why does it NOT do so now? (Am I wrong? It does use P2P?)
- Is tele-conferencing currently mainly unicast or multicast, P2P or centralized?

More Questions?

- QoS needs packets to be marked (class of service). Where are the markers put?
- What does policing do when it detects a stream using too many resources?
- Why is priority based scheduling sometimes unfair?
- A Weighted Fair Queue (WFQ) ensures the outbound link to a network is not over used. What happens if too much inbound traffic arrives?
- How does a token bucket aid in ensuring fair usage even when streams exceed there normal arrival rate?
- Explain why token bucket and WFQ together <u>can</u> guarantee an upper bound on the delay to packets passing through a router?

© University of Manchester 2013