

Introduction to Computer Networks

Differentiated Services (§5.4.6)



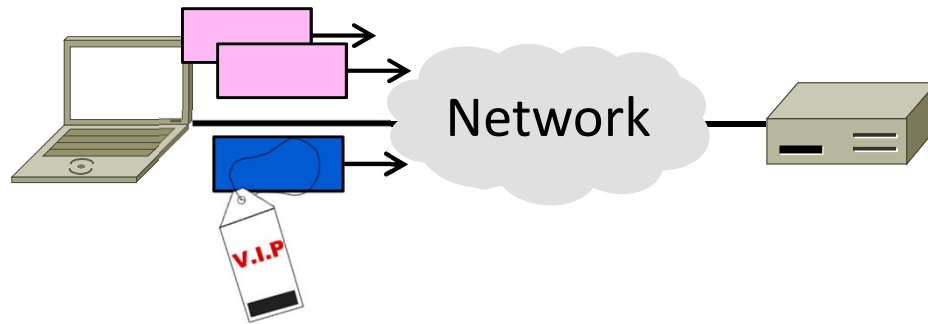
David Wetherall (djw@uw.edu)

Professor of Computer Science & Engineering

UNIVERSITY *of* WASHINGTON

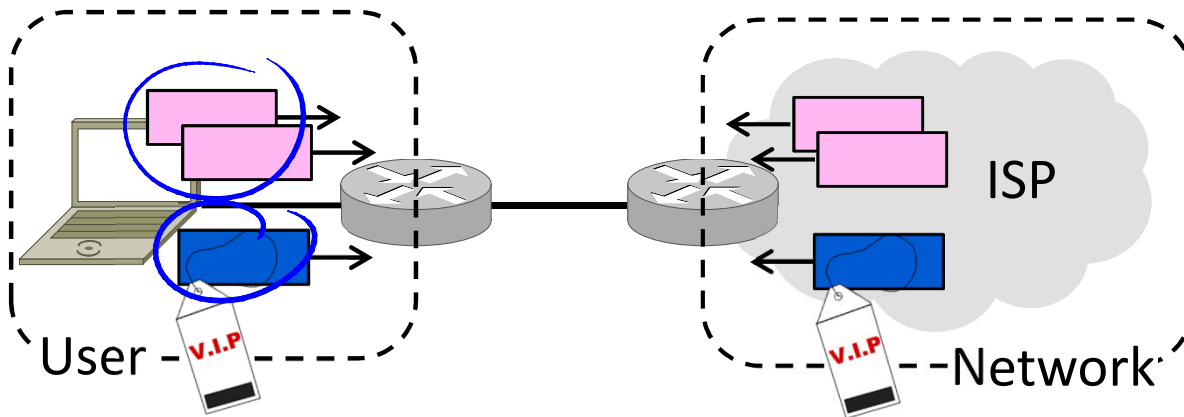
Topic

- Treating different traffic flows differently in the network
 - Coarse QOS (grades of service)
 - Gradually being deployed



Motivation

- User runs Skype and BitTorrent
 - Or remote desktop, gaming, web, etc.
- ➔ How can we give preference to flows?



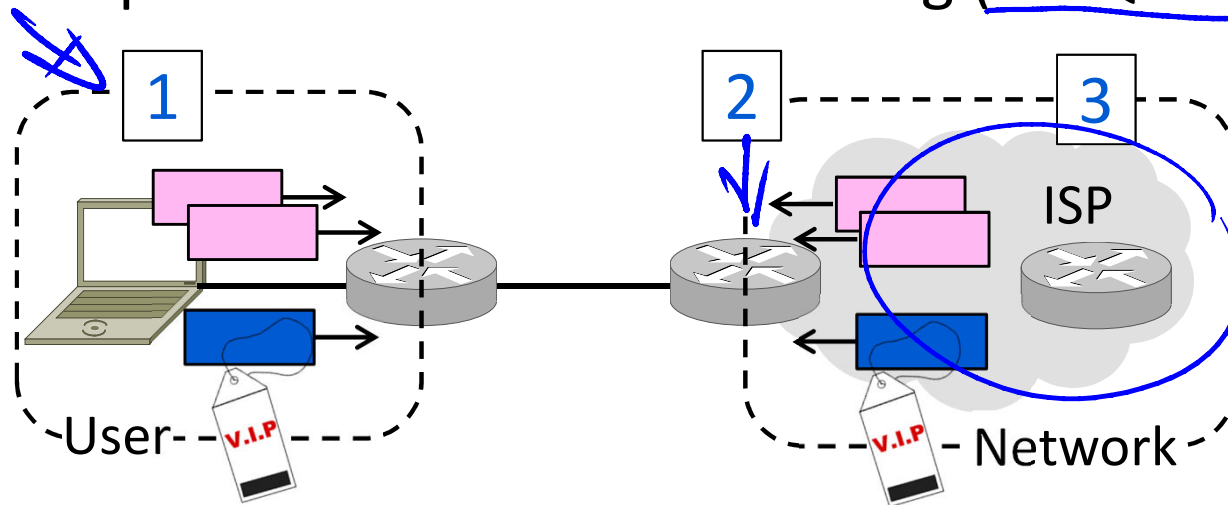
Differentiated Services

- Idea is to treat different kinds of traffic differently in the network
 - Have a few kinds of network service (GOLD, SILVER, BRONZE)
 - Different kinds get better or worse treatment in the network
 - Map apps to the right kind of service

Differentiated Services (2)

- Architecture:

1. User marks packet with desired service (e.g., Skype=GOLD)
2. Network polices traffic levels at boundary (token bucket)
3. Network provides different forwarding (WFQ at routers)



1. Marking Packets

- Use bits in IPv4/IPv6 header to mark the kind of service
 - 6-bit DSCP (Differentiated Services Code Point)

IPv4 Header

Version	IHL	Differentiated Services			Total length	
Identification				D F	M F	Fragment offset
Time to live		Protocol		Header checksum		
Source address						
Destination address						

Marking Packets (2)

- Many possible DSCP markings for different service/apps
- ➔ Supported services depend on configuration of network

Service Name / Meaning	DSCP Value	Traffic Need (App example)
Default forwarding / Best effort	<u>0</u>	<u>Elastic</u> (BitTorrent)
Assured forwarding / Enhanced effort	<u>10-38</u>	<u>Average rate</u> (streaming video)
Expedited forwarding / Real-time	46	<u>Low loss/delay</u> (VoIP, gaming)
Precedence / e.g., Network control	48	<u>High priority</u> (Routing protocol)

Marking Packets (3)

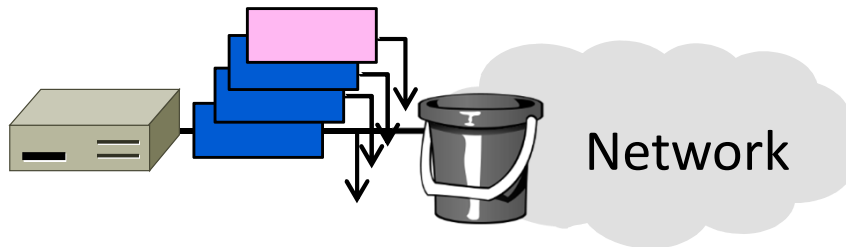
- Traffic is marked by user
 - Depends on local policies, e.g.,
gaming = expedited?
- May be done as part of host
 - Let OS or app classify their traffic
- May be done inside the network
 - Using heuristics, such as ports

2. Policing Packets

- Network (ISP) checks incoming traffic meets service contract
 - Not more expedited traffic than agreed (and paid for!)
 - Only allowed markings, e.g., no network control from users

Policing Packets (2)

- Policing is done with token bucket
 - ➔ Can demote “out of profile” traffic by re-marking (e.g., to default / best effort) or prioritizing for loss

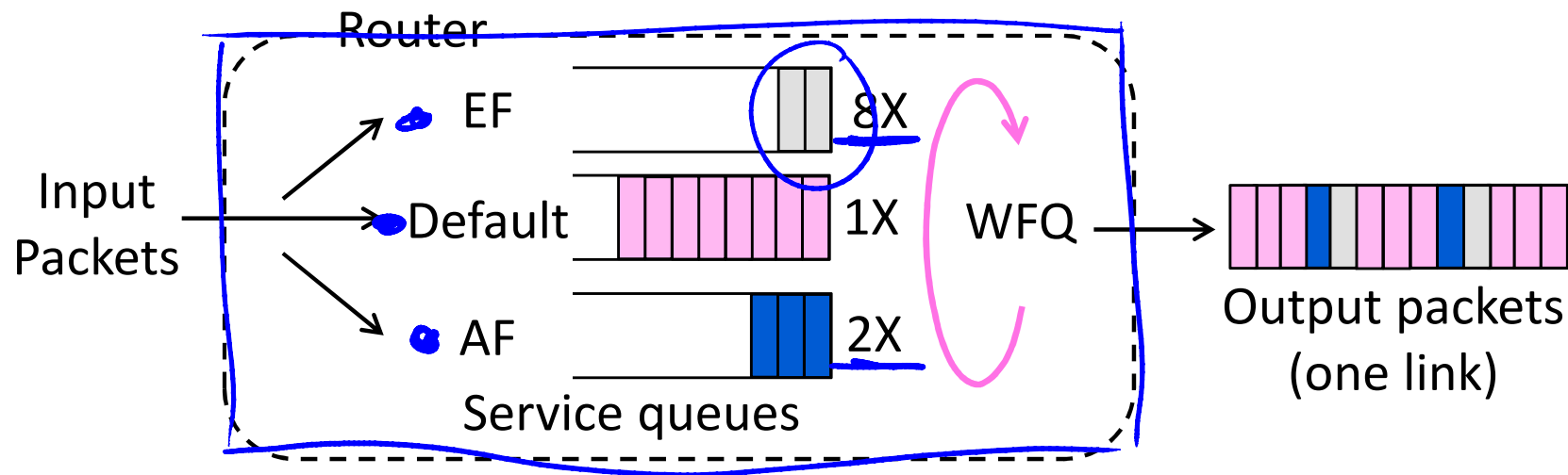


3. Forwarding Packets

- Network (ISP) routers use WFQ (and more) instead of FIFO
- The different kinds of service are the different flows/queues
- DSCP values are used to map packet to the right flow/queue

Forwarding Packets (2)

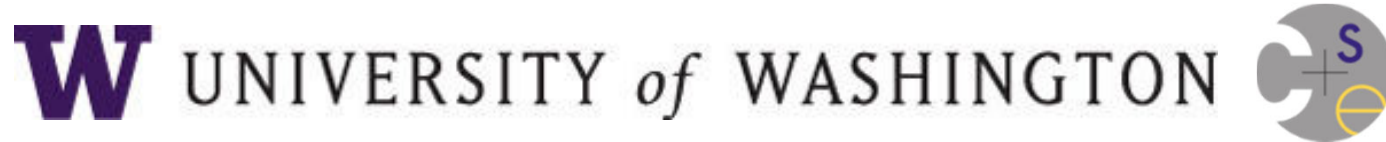
- Services are defined as “per hop behaviors”
 - No guarantee for end-to-end service through a network
 - Need small amounts of high priority traffic for good service



Deployment

- QOS provides value when it is deployed across the network
 - Not much use if only your ISP!
- QOS is tightly tied to pricing
 - “All my packets are high priority”
- Makes deployment slow/difficult ...

END



© 2013 D. Wetherall

Slide material from: TANENBAUM, ANDREW S.; WETHERALL, DAVID J., COMPUTER NETWORKS, 5th Edition, © 2011.
Electronically reproduced by permission of Pearson Education, Inc., Upper Saddle River, New Jersey