Network Infrastructures

A.A. 2019-2020
Prof. Francesca Cuomo

**Review on
Data Networking and the Internet**

2

Inter-Networks: Networks of Networks

- What is it ?
  - "Connect many disparate physical networks and make them function as a coordinated unit … " - Douglas Comer
    - Many => scale
    - Disparate => heterogeneity

- Result: Universal connectivity!
  - The inter-network looks like one large switch,
  - User interface is sub-network independent
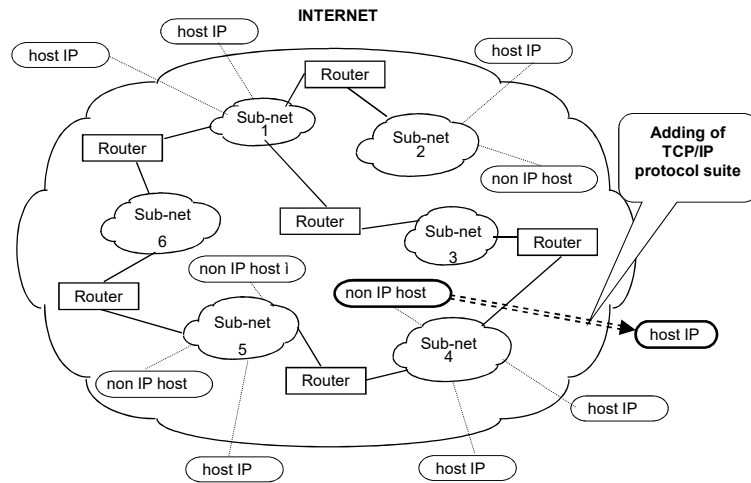
3

The Internet: A vision by domain

Country Code: from mask
- DE
- IT
- JP
- Other
- SE
- UK
- US

4

Inter-Networks: *Networks of Networks*
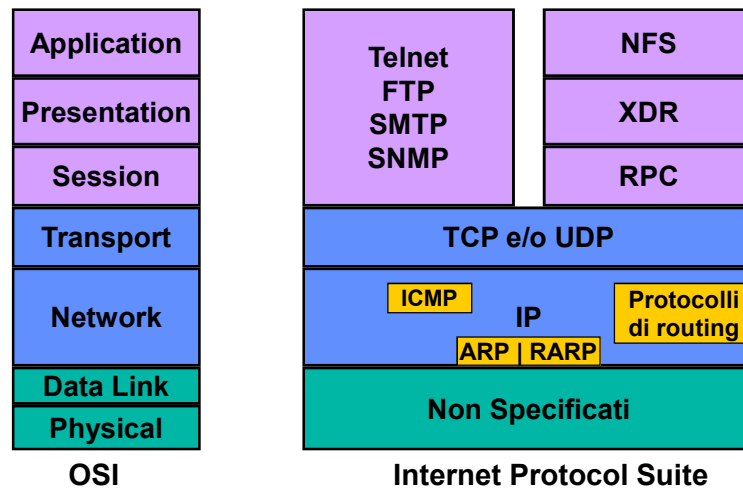
INTERNET

Adding of
TCP/IP
protocol suite
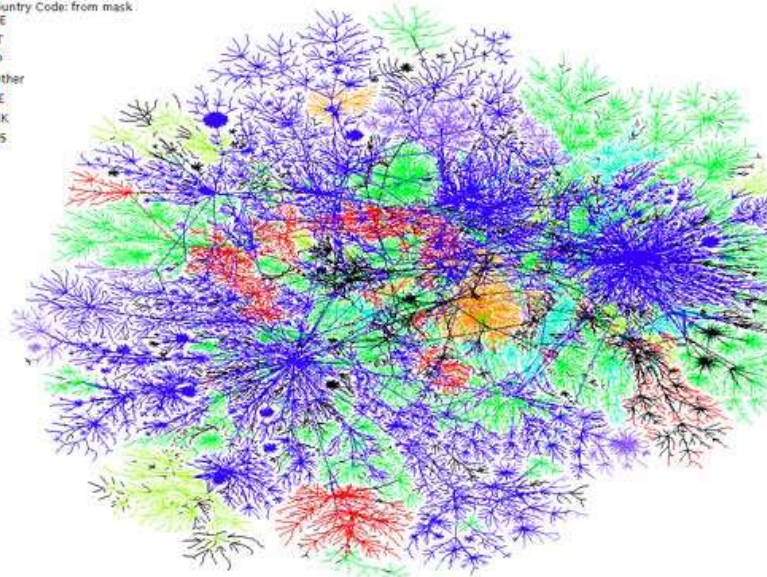
5

Inter-Networks: Networks of Networks

- Internetworking involves two fundamental problems: heterogeneity and scale

- Concepts:
  - Translation, overlays, address & name resolution, fragmentation: to handle heterogeneity
  - Hierarchical addressing, routing, naming, address allocation, congestion control: to handle scaling

6

Internet protocol suite

OSI	Internet Protocol Suite
Application	Telnet FTP SMTP SNMP / NFS XDR RPC
Presentation	
Session	
Transport	TCP e/o UDP
Network	ICMP IP Protocolli di routing / ARP | RARP
Data Link	Non Specificati
Physical	

7

IP: Internet Protocol

- Layer 3 protocol
- Defines
  - Packet format
  - Address format
  - Data (named datagram) forwarding procedures
- Best-effort service
  - connectionless
  - unrealiable
  - With no QoS guarantess
- Specified in RFC 791 (november 1981)

8

IP protocol

- Connectionless delivery
  - Stateless approach
    - » No state information on datagram kept in routers
    - » No connection concept at IP layer
  - Each datagram routed independently
    - » Two packets with the same source and destination can follow two different paths
    - » In practice, most packets follow a fixed route, unless
      - – Link faiulure
      - – Parallel links among routers
- No QoS guarantees
  - All packets treated fairly
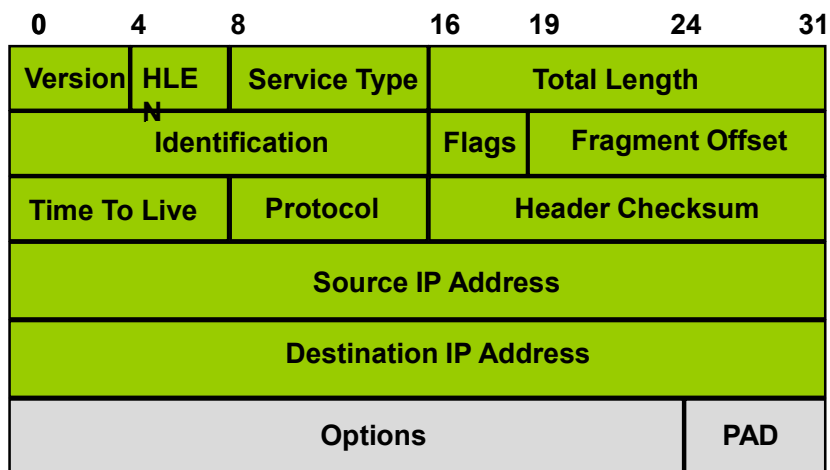 - Extensions to the traditional IP QoS model

9

IP protocol: unreliable delivery

- In case of:
  - Failure (ex. out of service router, link failure)
    - » Datagram dropped end error message sent to the source
  - Buffer shortage
    - » Datagram dropped (no error message sent, since the datagram cannot be stored)
  - Checksum error (error control only over the header!)
    - » Datagram dropped
    - » No error message sent, since address may be wrong

10

IP packet header

0	4	8	16	19	24	31

| Version | HLEN | Service Type | Total Length | | | |
Identification			Flags	Fragment Offset		
Time To Live		Protocol	Header Checksum			
Source IP Address						
Destination IP Address						
Options					PAD	

Standard size: 20 byte

11

Scalable Forwarding, Structured Addresses

- Address has structure which aids the forwarding process.
- Address assignment is done such that nodes which can be reached without resorting to L3 forwarding have the same prefix (network ID)

Network ID	Host ID

Demarcator
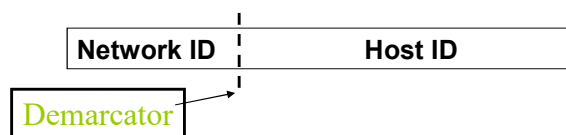
12

Scalable Forwarding, Structured Addresses

- A simple comparison of network ID of destination and current network (broadcast domain) identifies whether the destination is "directly" connected
  - I.e. Reachable through L2 forwarding only
- Within L3 forwarding, further structure can aid hierarchical organization of routing domains (because routing algorithms have other scalability issues)

13

Internet Routing Drivers

- Technology and economic aspects:
  - Internet built out of cheap, unreliable components as an overlay on top of leased telephone infrastructure for WAN transport.
    - » Cheaper components => fail more often => topology changes often => needs dynamic routing
  - Components (including end-systems) had computation capabilities.
    - » Distributed algorithms can be implemented
  - Cheap overlaid inter-networks => several entities could afford to leverage their existing (heterogeneous) LANs and leased lines to build inter-networks.
    - » Led to multiple administrative "clouds" which needed to inter-connect for global communication.

14

Internet Routing Model

- 2 key features:
  - Dynamic routing
  - Intra- and Inter-AS routing, AS = locus of admin control

- Internet organized as "autonomous systems" (AS).
  - AS is internally connected

- Interior Gateway Protocols (IGPs) within AS.
  - Eg: RIP, OSPF, HELLO

- Exterior Gateway Protocols (EGPs) for AS to AS routing.
  - Eg: EGP, BGP-4
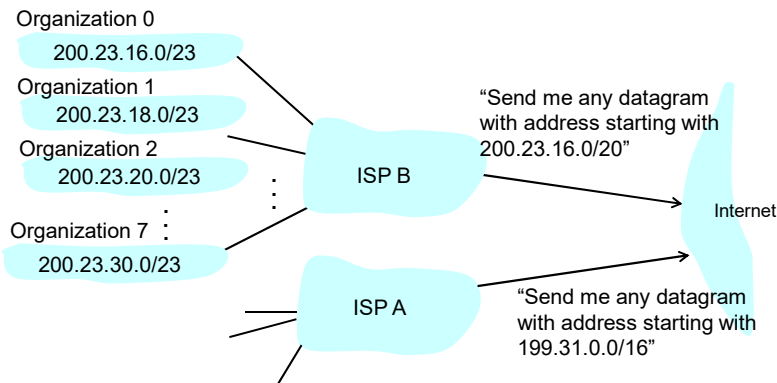
15

Hierarchical routing

- Ideal (conceptually simpler) case
  - All routers are identical
  - Flat network, no hierarchy
- Not useable in practice
  - Scalability: with 100 million of destination :
    » All destinations in a single routing rable?
    » Routing info exchange would require too much bandwidth
  - Administrative autonomy
    » Internet = network of networks
    » Each network administrator is willing to control rotuing functions within its domain

16

Hierarchical routing: route aggregation

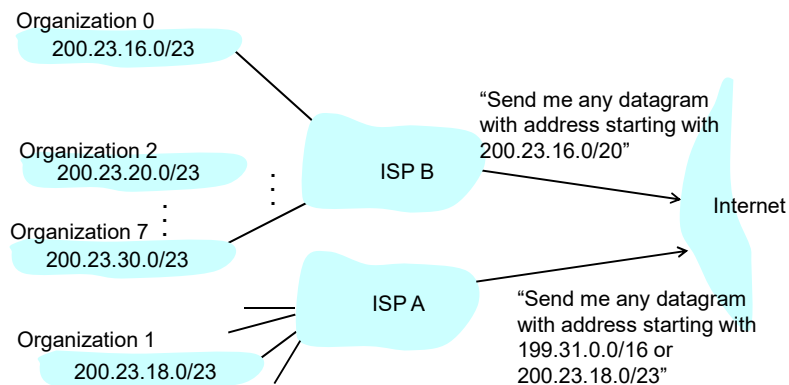- Hierarchical addressing permits more efficient announcements of routing infos

Organization 0
200.23.16.0/23

Organization 1
200.23.18.0/23

Organization 2
200.23.20.0/23

Organization 7
200.23.30.0/23

ISP B

ISP A

"Send me any datagram with address starting with 200.23.16.0/20"

Internet

"Send me any datagram with address starting with 199.31.0.0/16"

17

Hierarchical routing: route aggregation

- If ISP A has a more specific path to Organization 1

Organization 0
200.23.16.0/23

Organization 2
200.23.20.0/23

Organization 7
200.23.30.0/23

ISP B

ISP A

"Send me any datagram with address starting with 200.23.16.0/20"

Internet

Organization 1
200.23.18.0/23

"Send me any datagram with address starting with 199.31.0.0/16 or 200.23.18.0/23"

18

Hierarchical routing

- Router aggregated in Autonomous System (AS)
  - Networks with complex structure (many subnets and routers) but with the same administrative authority
  - Router within the same AS use the same routing protocol
  - Intra-AS routing protocols: (IGP: Interior Gateway Protocol)
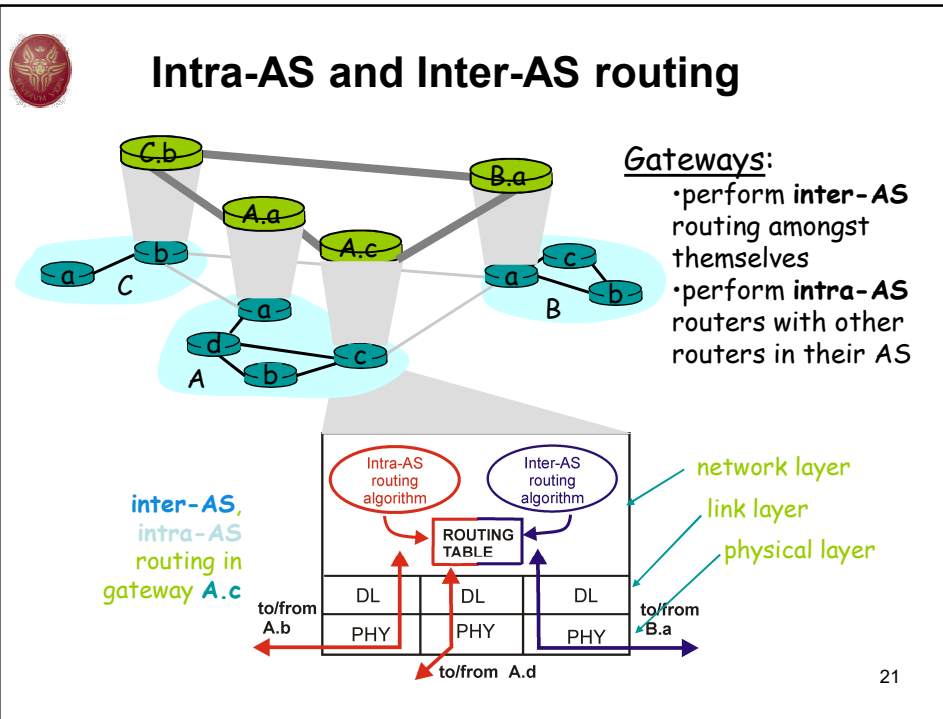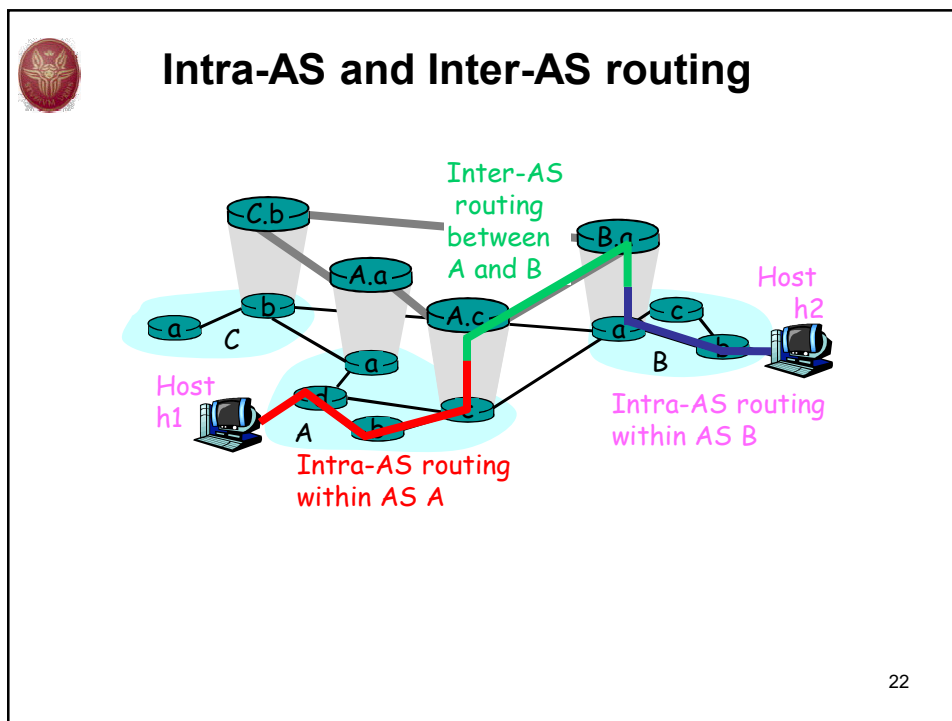   - » Routers belonging to different AS may use different IGP protocols

19

Hierarchical routing

- In each AS there exist "gateway" routers
  - Responsible to route to destinations external to the AS
  - Run intra-AS routing protocols with all other AS routers
  - Run also inter-AS routing protocols (EGP: Exterior Gateway Protocol)
- We can identify an internal routing (IGP) and an external routing (EGP)

20

Intra-AS and Inter-AS routing

Gateways:
- perform **inter-AS** routing amongst themselves
- perform **intra-AS** routers with other routers in their AS

inter-AS, intra-AS routing in gateway A.c

Intra-AS routing algorithm

Inter-AS routing algorithm

ROUTING TABLE

network layer
link layer
physical layer

to/from A.b

to/from B.a

| DL | DL | DL |
| PHY | PHY | PHY |

to/from A.d

21

Intra-AS and Inter-AS routing

Inter-AS routing between A and B

Host h2

Host h1

Intra-AS routing within AS A

Intra-AS routing within AS B

22

Requirements for Intra-AS Routing

- Should scale for the size of an AS.
  - Low end: 10s of routers (small enterprise)
  - High end: 1000s of routers (large ISP)
- Different requirements on routing convergence after topology changes
  - Low end: can tolerate some connectivity disruptions
  - High end: fast convergence essential to business (making money on transport)
- Operational/Admin/Management (OAM) Complexity
  - Low end: simple, self-configuring
  - High end: Self-configuring, but operator hooks for control
- Traffic engineering capabilities: high end only

23

Requirements for Inter-AS Routing

- Should scale for the size of the global Internet.
  - Focus on reachability, not optimality
  - Use address aggregation techniques to minimize core routing table sizes and associated control traffic
  - At the same time, it should allow flexibility in topological structure (eg: don't restrict to trees etc)
- Allow policy-based routing between autonomous systems
  - Policy refers to arbitrary preference among a menu of available options (based upon options' attributes)
  - In the case of routing, options include advertised AS-level routes to address prefixes
  - Extensible to meet the demands for newer policies.

24

The Congestion Problem

- *Problem: <u>demand outstrips available capacity</u>*
- If <u>information</u> about λ_i, λ and μ is <u>known</u> in a <u>central</u> location <u>where</u> control of λ_i or μ can be effected with <u>zero time</u> delays,
  - the congestion problem is solved!
- Unfortunately, we have incomplete info, require a distributed solution with time-varying time-delays

λ_i λ μ μ_i

λ_1

Demand

λ_n

Capacity
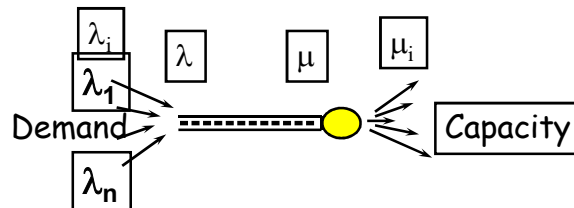
25

Congestion: A Close-up View

- <u>knee</u> – point after which
  - throughput increases very slowly
  - delay increases fast
- <u>cliff</u> – point after which
  - throughput starts to decrease very fast to zero (congestion collapse)
  - delay approaches infinity

- Note (in an M/M/1 queue)
  - delay = 1/(1 – utilization)

knee   cliff   packet loss

Throughput

congestion collapse

Load

Delay

Load
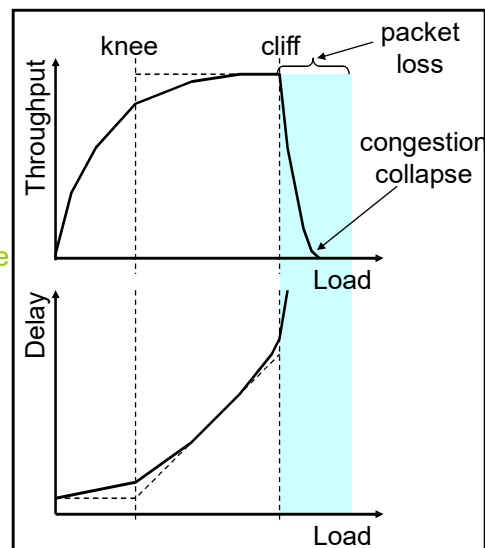
Congestion Control vs. Congestion Avoidance

- Congestion control goal
  - stay left of cliff
- Congestion avoidance goal
  - stay left of knee
- Right of cliff:
  - Congestion collapse
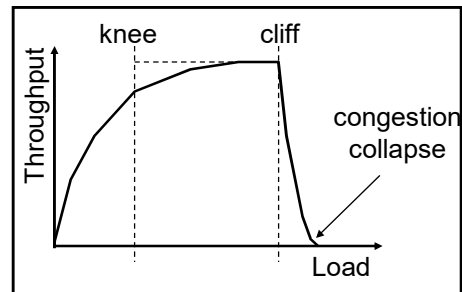
27

Goals of Congestion Control

- To guarantee stable operation of packet networks
  - Sub-goal: avoid congestion collapse

- To keep networks working in an efficient status
  - Eg: high throughput, low loss, low delay, and high utilization

- To provide fair allocations of network bandwidth among competing flows in steady state
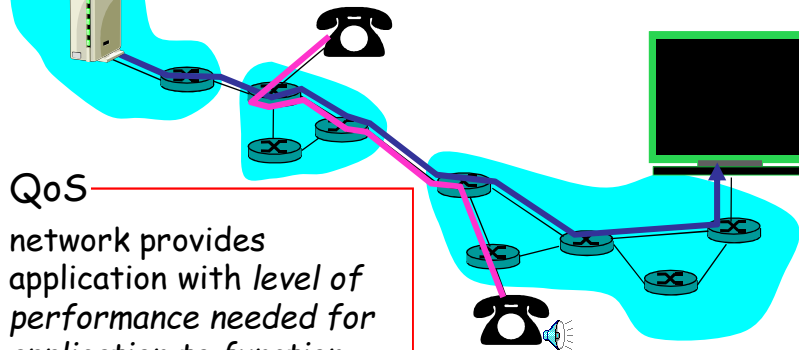 - For some value of "fair" ☺

28
28

Quality of Service: What is it?

Multimedia applications:
network audio and video

QoS

network provides application with *level of performance needed for application to function.*

29

QoS Challenges

- TCP/UDP/IP suite provides best-effort, no guarantees on expectation or variance of packet delay
- Streaming applications delay of 5 to 10 seconds is typical and has been acceptable, but performance deteriorate if links are congested (transoceanic)
- Real-Time Interactive requirements on delay and its jitter have been satisfied by over-provisioning (providing plenty of bandwidth), what will happen when the load increases?...

30

QoS Challenges

- Most router implementations use only First-Come-First-Serve (FCFS or FIFO) packet processing and transmission scheduling
- To mitigate impact of "best-effort" protocols, we can:
  - Use UDP to avoid TCP and its slow-start phase…
  - Buffer content at client and control playback to remedy jitter
  - Adapt compression level to available bandwidth

31

Fundamental QoS Problems

FIFO

Scheduling Discipline
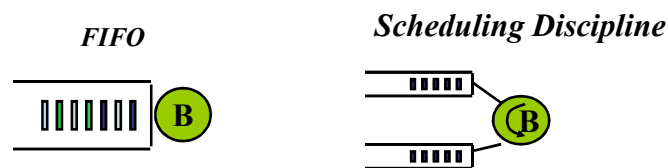
- In a FIFO service discipline, the performance assigned to one flow is *convoluted* with the arrivals of packets from all other flows!
  - Cant get QoS with a "free-for-all"
  - Need to use new scheduling disciplines which provide "*isolation*" of performance from arrival rates of background traffic
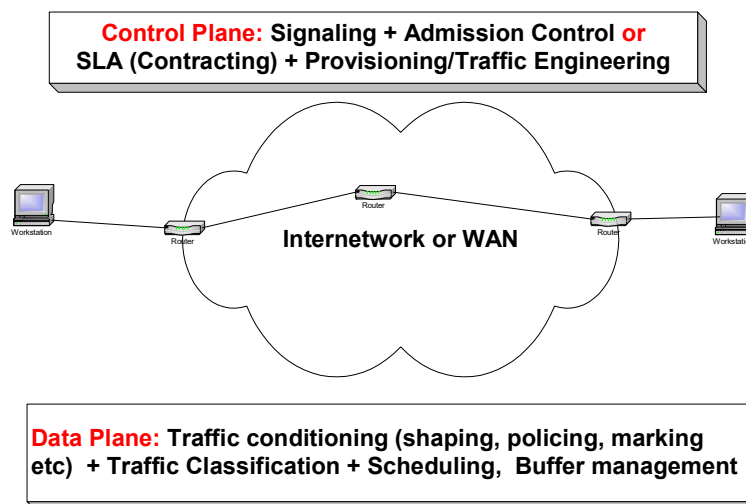
32

Solution Approaches in IP Networks

- Just add more bandwidth and enhance caching capabilities (over-provisioning)!
- Need major change of the protocols :
  - Incorporate resource reservation (bandwidth, processing, buffering), and new scheduling policies
  - Set up service level agreements with applications, monitor and enforce the agreements, charge accordingly
- Need moderate changes ("Differentiated Services"):
  - Use two traffic classes for all packets and differentiate service accordingly
  - Charge based on class of packets
  - Network capacity is provided to ensure first class packets incur no significant delay at routers

33

QoS Big Picture: Control/Data Planes

Control Plane: Signaling + Admission Control or SLA (Contracting) + Provisioning/Traffic Engineering

Workstation

Router

Router

Router

Internetwork or WAN

Workstation

Data Plane: Traffic conditioning (shaping, policing, marking etc) + Traffic Classification + Scheduling, Buffer management

34

Internet transport layer

- Two alternative protocols: TCP e UDP
- Different service models:
  - TCP is connection oriented, reliable, it provides flow and congestion control, it is stateful, it supports only unicast traffic
  - UDP is connectionless, unreliable, stateless, it supports multicast traffic
- Common characteristics:
  - Multiplexing and demultiplexing of application processes through the port mechanism
  - Error detection over header and dati (optional in UDP)

35

Mux/demux: ports

- Final destination of data is not the host but an application process running in the host
- Interface between application processes and the network architecture is named port
  - Integer number over 16 bit
  - There is an association between ports and processes
    » Public server process are statically associated to well-know ports, with an identifier smaller than 1024 (e.g.: 80 for WWW, 25 for email)
    » Client processes use ports dynamically assigned by the operating system, with an identifier larger than 1024
      - Each client process on a given host has a unique port number within that host

36

UDP: User Datagram Protocol

- Connectionless transport protocol
- No delivery guarantee
- Two main functions:
  - Application process multiplexing through port abstraction
  - checksum (optional) to verify data integrity
- Applications using UDP should solve (if interested)
  - Reliability issues
    » Data loss, data duplication
  - Sequence control
  - Flow and congestion control
- Standardized in RFC 768

37

UDP: packet format

0 4 8	16 19 24 31
UDP Source Port	UDP Destination Port
UDP Message Length	UDP Checksum
DATA	
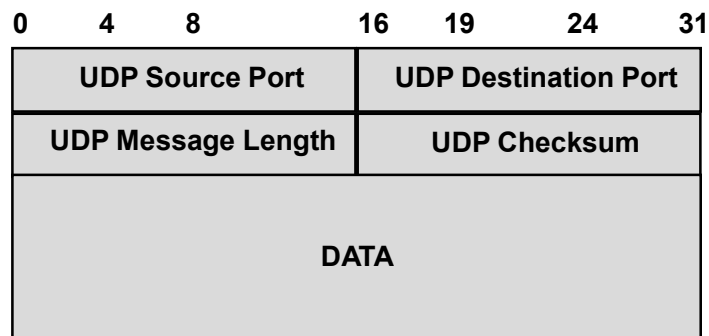
38

UDP: applicability

- UDP is useful when:
  - Operating in local area, a reliable network (NFS)
  - All application data are contained in a single packet, so that there is no need to open a connection for a single packet (DNS)
  - Full reliability is not fundamental (some intercative video/audio service)
  - A fast protocol is needed
    - » Connection opening overhead avoided
    - » Retransmission mechanisms to ensure reliability cannot be used due to strict timing constraints
  - Application manages retransission mechanisms (DNS)
  - Need to send data at constant rate or at a rate independent from the network (some interactive video-audio services)

39

TCP protocol

- TCP (Transmission Control Protocol) is
  - Connection oriented
  - Reliable (through retransmission)
    - » Correct and in-order delivery of stream of data
  - Flow control
  - Congestion control
- Used by applications requiring reliability
  - telnet (remote terminal)
  - ftp (file transfer protocol)
  - smtp (simple mail transfer protocol)
  - http (hypertext transfer protocol)

40

TCP

- Multiplexing/demultiplexing through ports
- Connection opened between two TCP entities (service similar to a virtual circuit)
  - bidirectional (full duplex)
  - With error and sequence control
- It is more complex than UDP, it requires more CPU and memory, state information (port numbers, window size, etc) must be kept in each host for each TCP connection

41

TCP

- TCP freely segments and reassembles data:
  - Manages byte stream generated by application protocols; unstructured data at TCP level
  - A FIFO buffer byte oriented is the interface between TCP and application processes
- Window protocol to ensure reliability
- Flow control and congestion control operates on the transmitter window size
  - Flow control executed by the TCP receiver exploiting the window field in the TCP header
  - Congestion control autonomously executed by the TCP transmitter
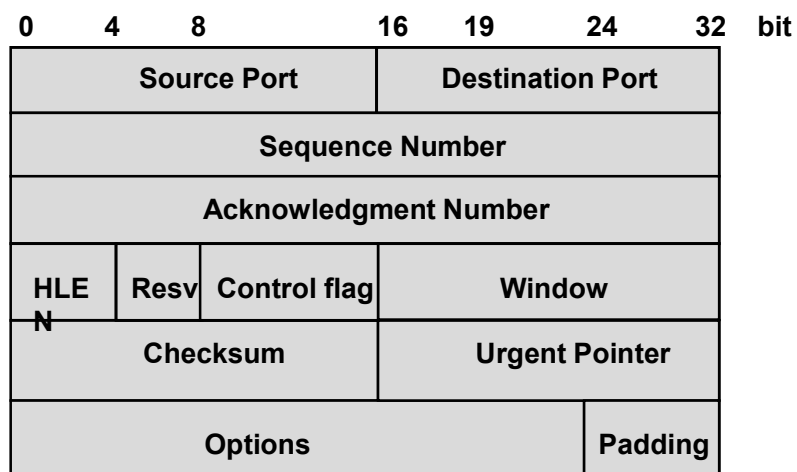
42

TCP: connection identification

- A TCP connection is identified uniquely by:
  - Source and destination IP addresses (layering principle violation)
  - Source and destination port numbers
  - Example: TCP connection identifed by porta 15320 on host with IP address 130.192.24.5 and port 80 on host with IP address 193.45.3.10
- Note that TCP and UDP use port numbers are independent

43

TCP: header

0	4	8	16	19	24	32	bit

Source Port	Destination Port

Sequence Number

Acknowledgment Number

HLEN	Resv	Control flag	Window

Checksum	Urgent Pointer

Options	Padding

44

RTP

- Real-Time Transport Protocol is an Internet protocol standard to manage real-time transmission of multimedia data
- RTP is commonly used in Internet telephony applications.
- RTP combines its data transport with a control protocol (RTCP), which makes it possible to monitor data delivery for large multicast
- RTP runs on top of UDP

45

RTP

- RTP includes:
  - a **sequence number**, which is used to detect lost packets;
  - **payload identification**, which describes the specific media encoding so that it can be changed if it has to adapt to a variation in bandwidth;
  - **frame indication**, which marks the beginning and end of each frame;
  - **source identification**, which identifies the originator of the frame;
  - **intramedia synchronization**, which uses timestamps to detect different delay jitter within a single stream and compensate for it

46

RTPC

- RTPC includes:
  - **quality of service** (QoS) feedback, which includes the numbers of lost packets, round-trip time, and jitter, so that the sources can adjust their data rates accordingly;
  - **session control**, which uses the RTCP BYE packet to allow participants to indicate that they are leaving a session;
  - **identification**, which includes a participant's name, e-mail address, and telephone number for the information of other participants;
  - **intermedia synchronization**, which enables the synchronization of separately transmitted audio and video streams. 47