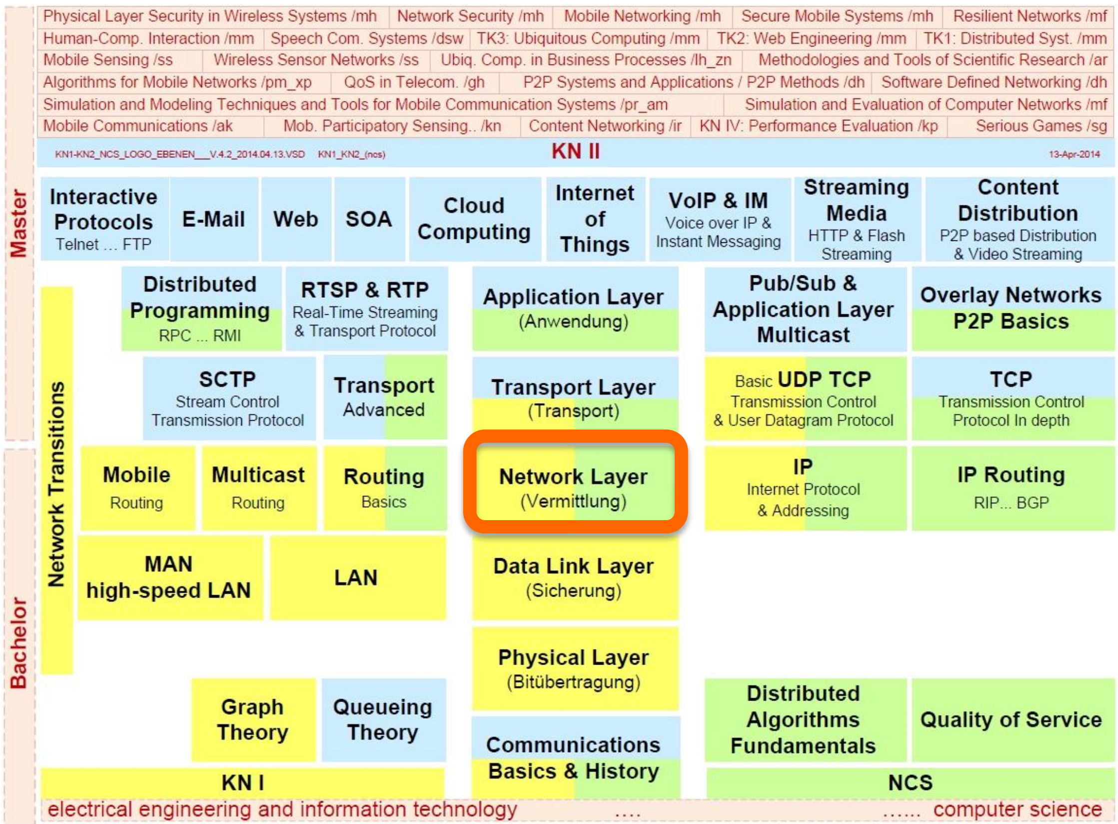
Communication Networks I

L3 Network Layer - Fundamentals

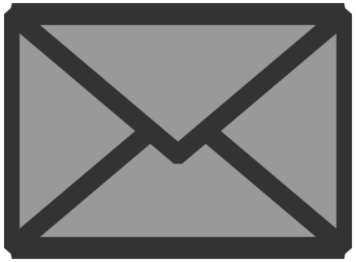


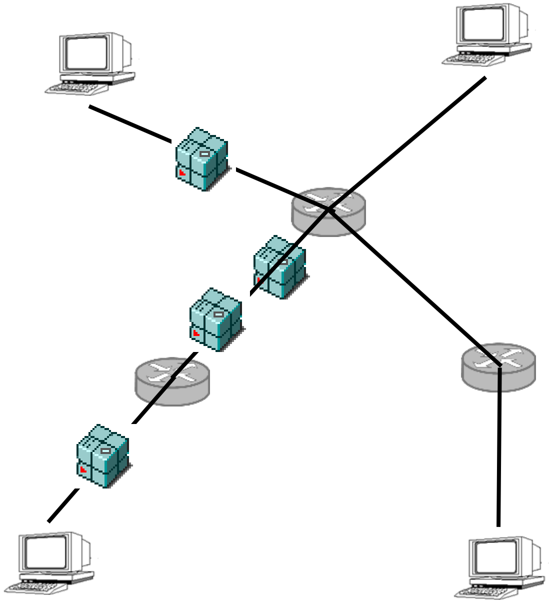
Prof. Dr.-Ing. **Ralf Steinmetz**

KOM - Multimedia Communications Lab

Overview

1 Introduction

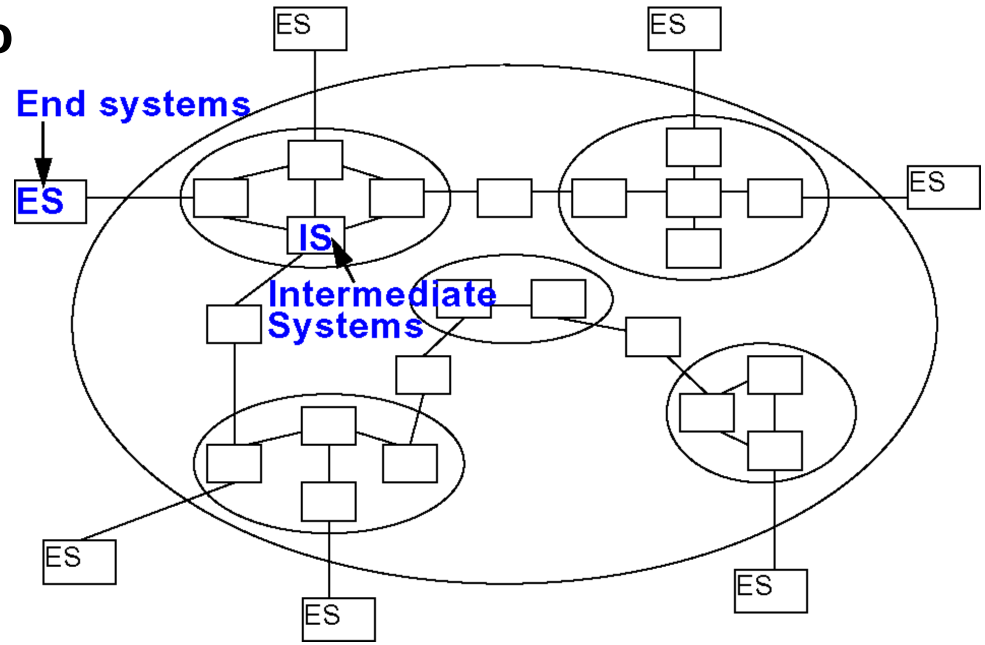




2 Functions (in) the Network Layer

Data transfer from end system to end system

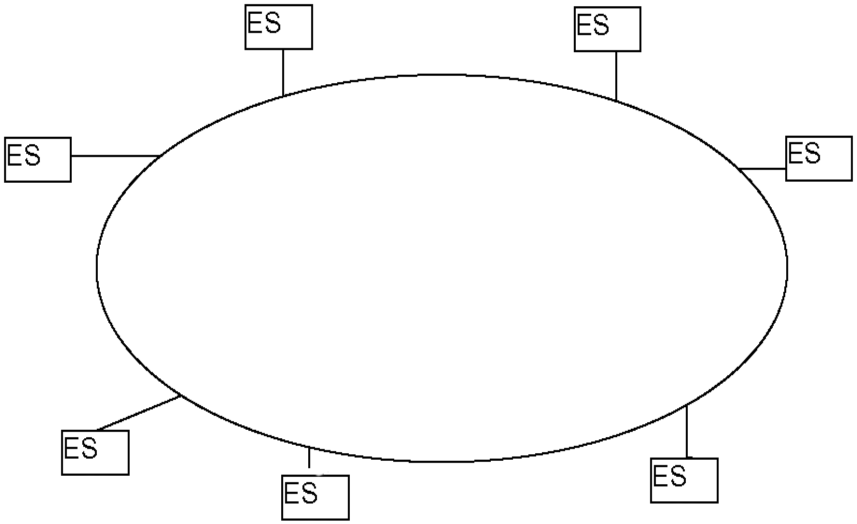
- Several hops, (heterogeneous) subnetworks
- Compensate for differences between end systems during transmission



Relevance of the interface: switching vs. transport service

- L1 up to L1,L2+L3: organization: carrier
- From L4 onward: user/customer/company

Functions (in) the Network Layer



The provided services are

- Standardized for end systems
- Independent from network technology
- Independent from number, type and topology of the subnetworks

SUBNETWORKS (IS 7498):

A multitude of one or several intermediary systems that

- provide switching functionalities
- through which open end systems can establish network connections

Functions (in) the Network Layer

Primary tasks

- Providing virtual circuits and datagram transmissions
- Routing
- Congestion control
- Internetworking – providing transitions between networks
- Addressing
- Quality of Service (QoS)
  - example: bandwidth, delay, error rate
  - negotiate costs vs. quality of service to be provided

Secondary tasks, based on type service and request

- Multiplexing of network connections
- Fragmentation and reassembling
- Error detection and correction
- Flow control as a means to correct congestion
- Maintaining the sequence

Functions (in) the Network Layer

Required knowledge

- Subnetwork topology
- Address / localization of the end system
- Packet / data stream communication requirements (Quality of Service)
- Network status (utilization,...)

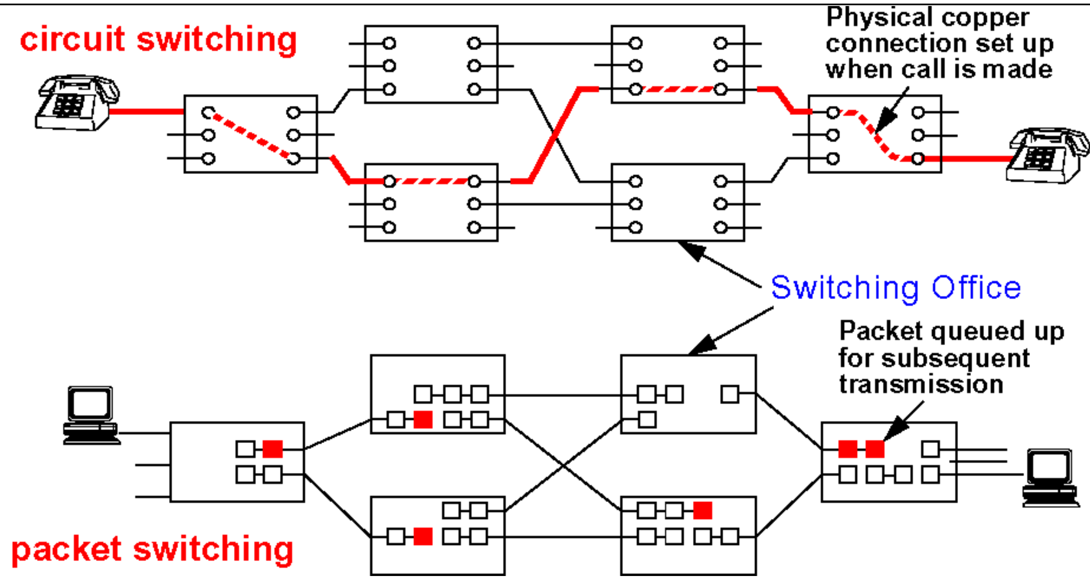
Examples

- X.25 (ISDN, ...)
- Internet protocol IP (TCP/IP,..)

Nomenclature:

Layer	Data Entity
Transport	…
Network	Packet
Data Link	Frame
Physical	Bit/Byte (bit stream)

3 Types of Switching



Circuit switching

- switching a physical connection

Message switching

- message is stored and passed on by one hop

Packet switching

- store-and-forward, but transmissions packets limited in size

Switching by virtual circuit

- packets (or cells) over a pre-defined path

3.1 Circuit Switching

Principle

- Connection (actually) exists physically for the duration of the conversation

Refers to

- Switching centers
- Connections between switching centers (frequency spectrum, dedicated ports)

Implementation examples

- Historically: on switching boards
- Mechanical positioning of the dialers
- Setting coupling points in circuits
- Early alternative at Broadband-ISDN: STM (Synchronous Transfer Mode)

Properties

- Connection has to occur before transmission
- Establishing a connection takes time
- Resource allocation too rigid (possibly waste of resources)
- Once connection is established it cannot be blocked anymore

3.2 Message Switching

Principle

- All data to be sent are treated as a "message"
- “Store and forward" network:
- In each node the message is handled as follows:
  1) accepted
  2) treatment of possible errors
  3) stored
  4) forwarded (as a whole to the next node)

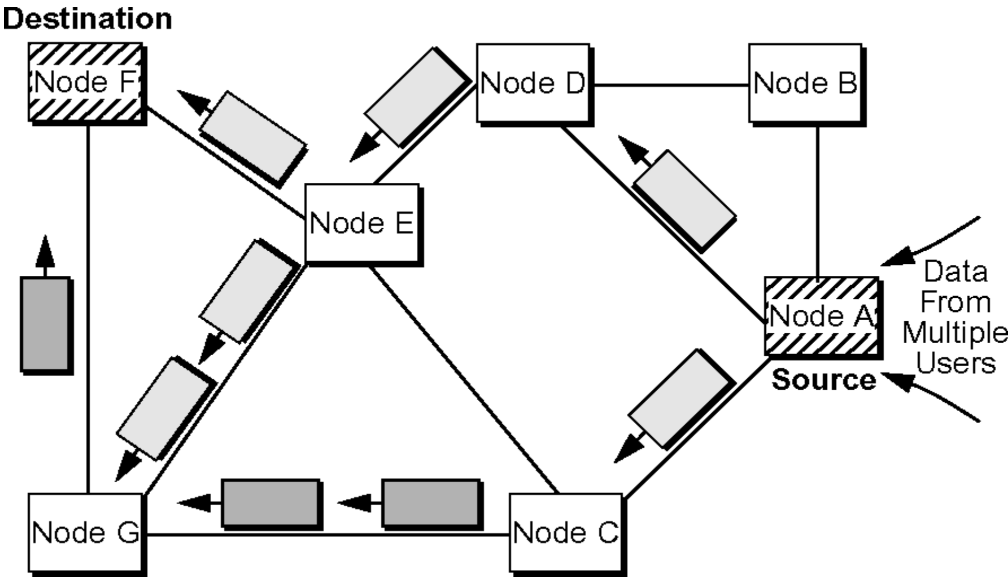
Example

- Early telegram service

Properties

- High memory requirements at the node (switching centers),
  - because message may be of any size
  - usually stored on secondary repository (hard disk)
- Node may be used to its full capacity over a longer period of time by one message,
  - i. e. better if packets are of limited size (packet switching)

3.3 Packet Switching - Datagram



Examples

- Old Datex-P Service
- Internet

Principle

- Packets of limited size
- Dynamic route search (no connect phase)
- No dedicated path from source to destination

Properties

- Possibly only reservation of average bandwidth (static reservation)
- Possibility of congestion
- High utilization of resources

3.4 Virtual Circuit Switching

Principle

- Setup path from source to destination for entire duration of call
- Using state information in nodes but no physical connection
- Connection setup: defines data path
- Messages: as in packet switching
  - all follow ONE path
  - but (may) have only the address of the network entry point, not the destination address, e.g., ATM: VPI/VCI

Examples

- ATM (Asynchronous Transfer Mode) PVC (permanent virtual circuit)
  - established "manually" (similar to dedicated lines)
- ATM SVC (switched virtual circuit)
  - signaling: connect and disconnect corresponding to the telephone network
- Internet Integrated Services
  - state established via signaling protocol (RSVP)
  - full addresses are used

Properties

- All messages of a connection are routed over the same pre-defined data path, i.e., sequence is maintained
- It is easier to ensure Quality of Service (see also ATM)

Implementation Virtual Circuit

Connection set-up phase

- Select a path
- Intermediate systems (IS) store path information
- Network reserves all resources required for the connection

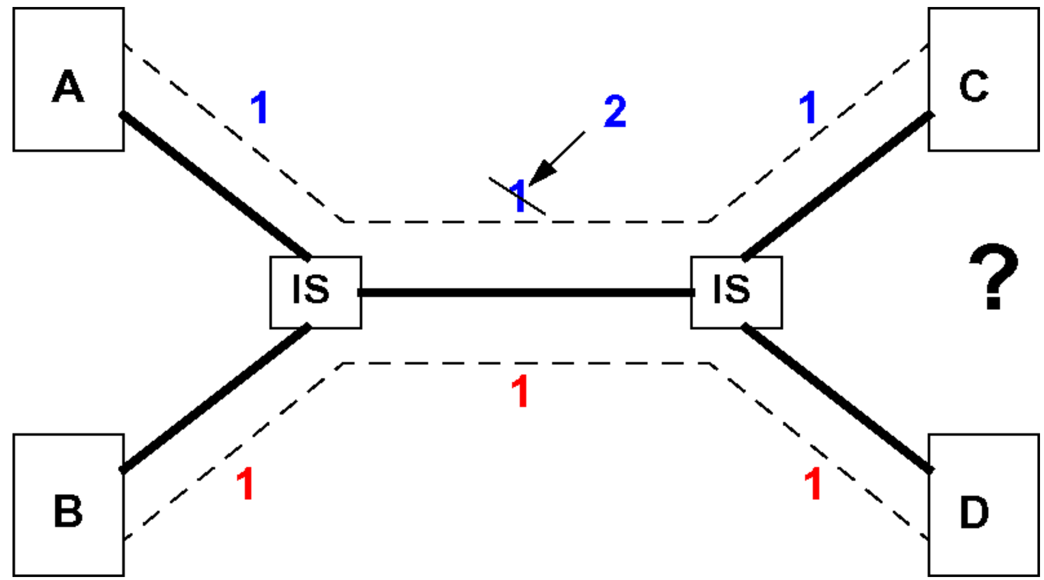
Data transfer phase: all packets follow the selected path

- Packet contains VC_number - identification of connection, but no address information
- IS uses the stored path information to determine the successor

Disconnect phase

- Network forgets the path
- Releases reserved resources

Implementation Virtual Circuit



End systems allocate

- VC-identifiers (VC-numbers) independently

Problem:

- The same VC-identifiers may be allocated to different paths

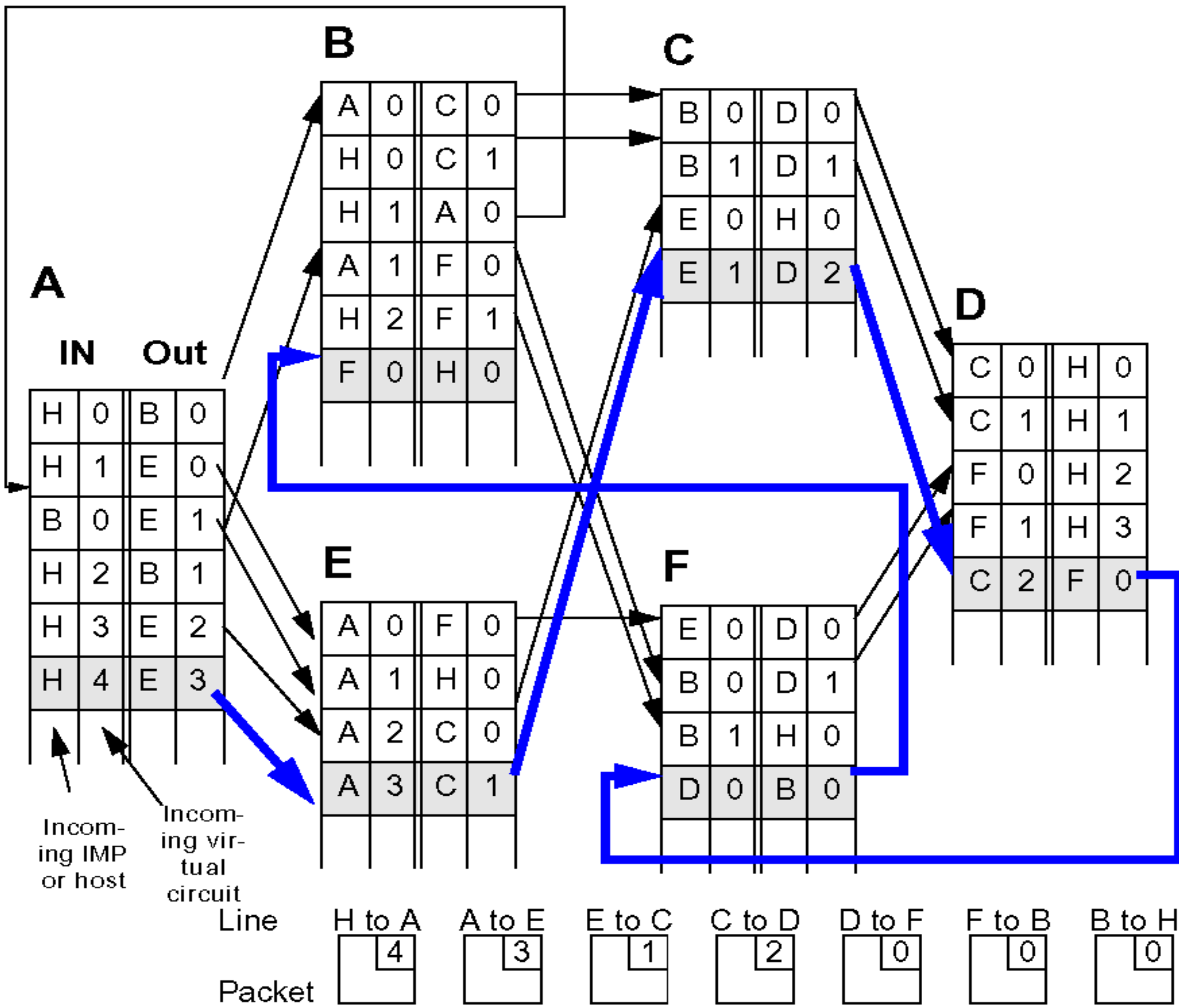
Solution: to allocate VC-numbers for virtual circuit segments

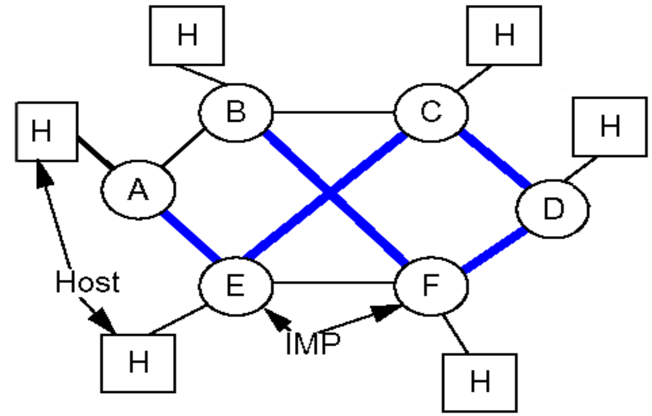
- IS differentiates between incoming and outgoing VC-number
  - 1. IS receives incoming VC-number in CONNECT.ind
  - 2. IS creates outgoing VC-number (unique between IS and successor(IS))
  - 3. IS sends outgoing VC-number in CONNECT.req

Implementation Virtual Circuit

TECHNISCHE
UNIVERSITÄT
DARMSTADT

Example:

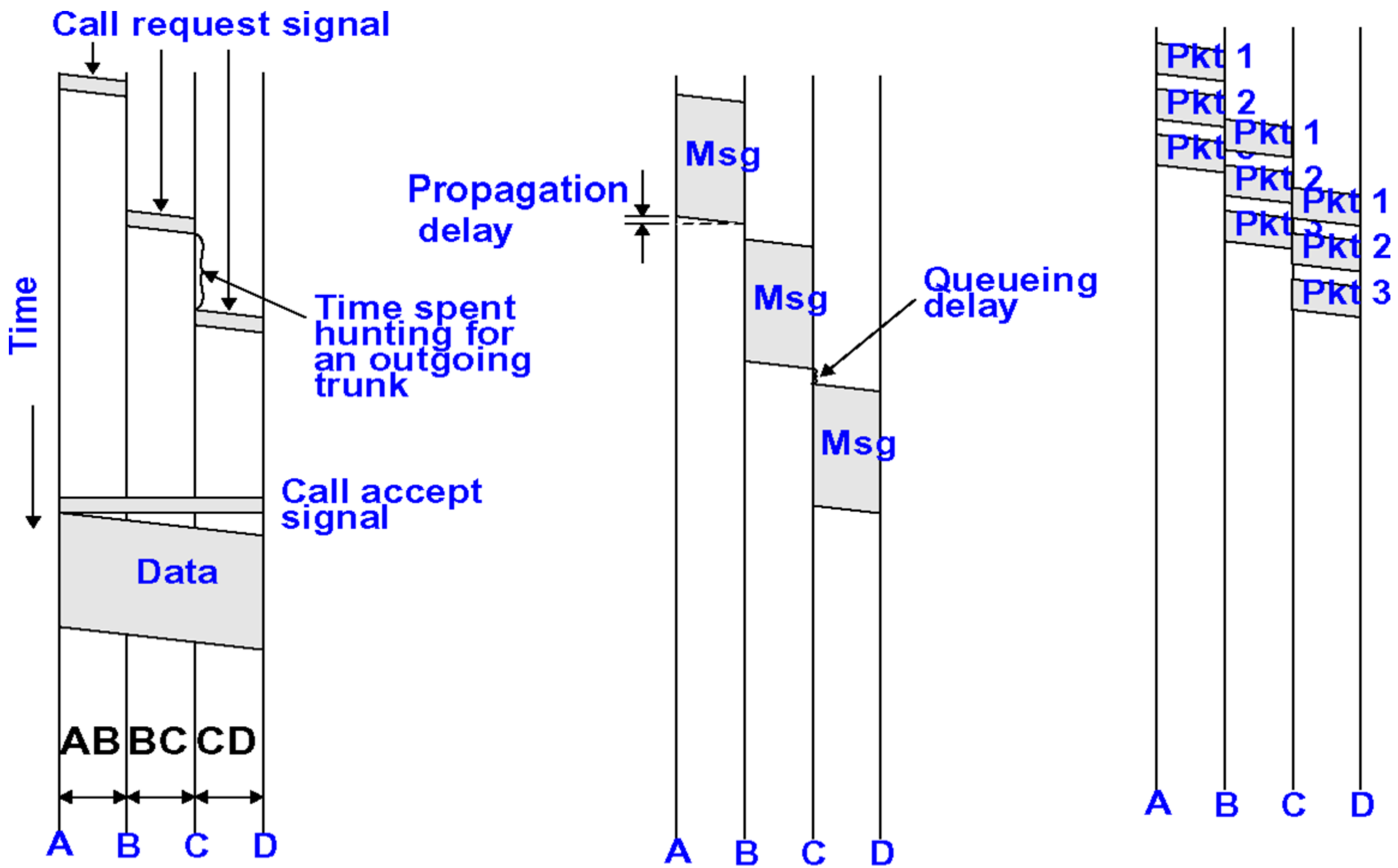




8 Simplex virtual circuits

Originating at A	Originating at B
0 - ABCD	0 - BCD
1 - AEFD	1 - BAE
2 - ABFD	2 - BF
3 - AEC	
4 - AECDFB	

3.5 Comparison



Circuit Switching　　Message Switching　　Packet Switching

Comparison: Circuit and Packet Switching

Circuit switching

- Connection establishment can take a long time
- Bandwidth is reserved
  - no danger of congestion
  - possibly poor bandwidth utilization (burst traffic)
- Continuous transmission time, because all data is transmitted over the same path
- Price calculation based on duration of connection

Packet switching

- Connect phase not absolutely necessary
- Dynamic allocation of bandwidth
  - danger of congestion
  - optimized bandwidth utilization
- Varying transmission time
  - because packets of a connection may use different paths
  - not suitable for isochronous data streams
- Price calculation based on transfer volume

Datagram vs. Virtual Circuit: A Comparison

Virtual circuit: destination address defined by connection

+ Packets contain short VC-number only
+ Low overhead during transfer phase
+ “Perfect" channel throughout the net
+ Resource reservation: "Quality of Service" guarantees possible

- Overhead for connection setup
- Memory for VC tables and state information needed in every IS
- Sensible to IS and link failures
- Resource reservation: potentially poor utilization

Datagram: IS routing table specifies possible path(s)

+ No connection setup delay
+ Less sensible to IS and link failures
+ Route selection for each datagram: quick reaction to failures

- Each packet contains the full destination and source address
- Route selection for each datagram: overhead
- QoS guarantees hardly possible

Types of Switching: Applicability

Circuit switching

- Telephone system
- Until now minor usage for computer networks, but various multimedia applications require isochronous data streams

Packet switching

- Used frequently for computer networks
- A bit more difficult for voice transmissions

Message switching

- Seldom used for computer systems
  - complex storage management (secondary storage)
  - "blockage" because of large messages

Virtual circuit switching

- Integrated services
- Voice transmission

Concepts

- Connection oriented vs. connectionless communication

Connection oriented

- Error free communication channel
- Usually error control: L3 (or network)
  - flow control, ...
- Usually duplex communication
- More favorable for real-time communications
- Telephone and telecommunication companies:
  - X.25, ATM, in mobile systems

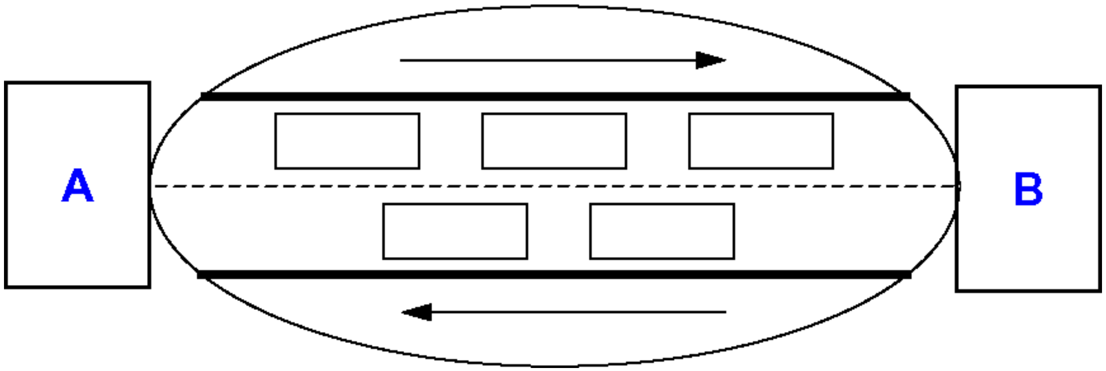
Connectionless

- Unreliable communication
- Hardly any error control: left to L4 or higher layers
  - maintaining sequence not ensured, ...
- Simplex communication
- More favorable for simple data communication:
  - SEND-PACKET, RECEIVE-PACKET
- Internet community: IP

4.1 Service: Connection Oriented Communication

Properties

- 3-phase interaction
  1) connect
  2) data transfer
  3) disconnect



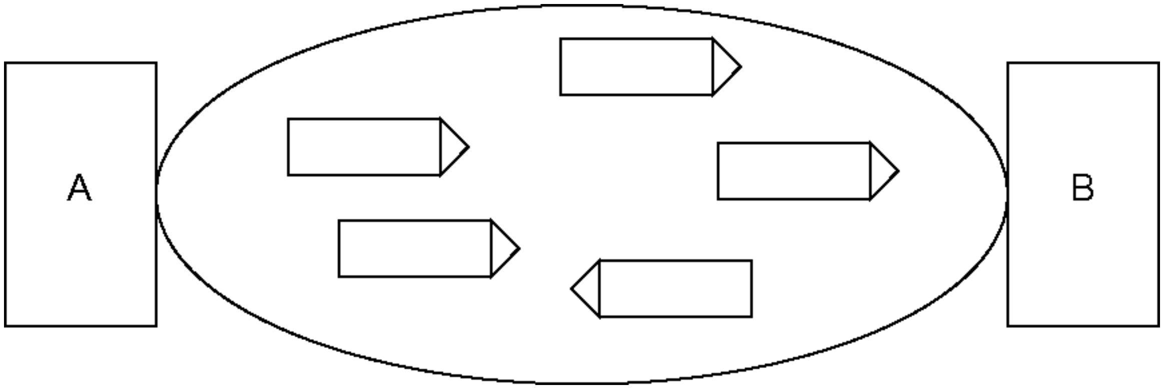
- Allows for QUALITY OF SERVICE NEGOTIATION
  - e.g., throughput, error probability, delay

- (Typically) RELIABLE COMMUNICATION in both directions
  - no loss, no duplicates, no modification
  - ensures maintenance of the correct sequence of transmitted data
- FLOW CONTROL
- Relatively complex protocols

Example

- Telephone service

4.2 Service: Connectionless Communication



Properties

- Network transmits packets as ISOLATED UNITS (datagram)
- UNRELIABLE COMMUNICATION:
  - loss, duplication, modification, sequence errors possible
- No flow control
- Comparatively SIMPLE PROTOCOLS

Example

- Mail delivery service

Services: Comparison of Concepts

Arguments pro a connection oriented service

- Simple, powerful paradigm
- Simplification of the upper layers (L4 - L7)
- Relieves end systems
- For some applications efficiency in time is more important than error-free transmission
  - e.g. real-time applications, digital voice transmission)
  - suitable for a wide range of applications

Arguments pro a connectionless service

- High flexibility and low complexity
- Costs for connects and disconnects are high for transaction oriented applications
- Easier to optimize the network load
- Compatibility and costs: IP common
- "END-TO-END ARGUMENTS" (Saltzer et al.):
  - secure communication requires error control within the application
  - but error control in one layer can replace the error control in the layer underneath it

Services of Layer 3 and their Implementations

		Service (upper layer/s)	
		Connectionless	**connection-oriented**
L3 Implementation	**Datagram**	**typically: UDP via IP**	**TCP via IP**
	Virtual circuit	**UDP/IP via ATM**	**typically: ATM AAL1 via ATM**

ISO IS 8348 Network Service Definition

2 Service classes

- Connection-oriented Network Service (CONS)
- Connectionless-mode Network Service (CLNS)

Implementations

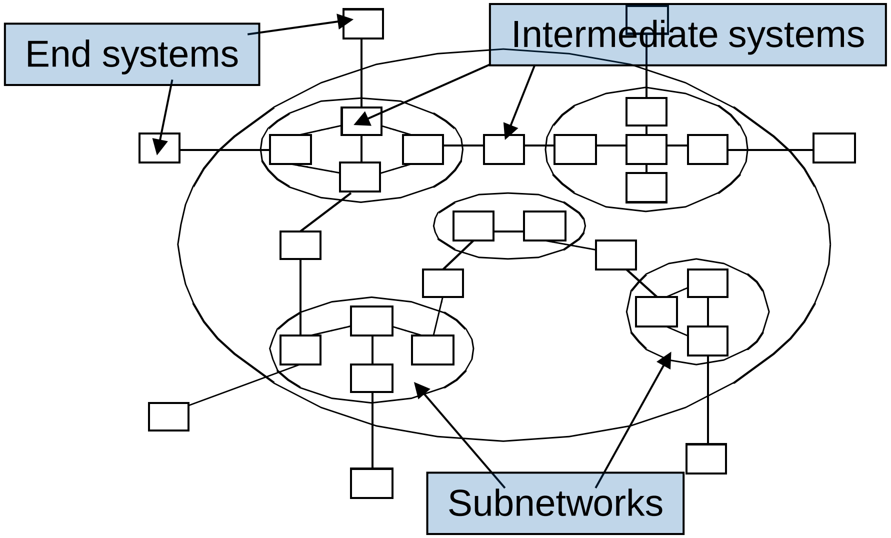
- Virtual circuit
- Datagram

Comment: service does not equal implementation!

5 Routing – Overview

Task of routing

- Comp. A wants to send message to B
- A and B are both part of a larger network
- To find a route (path)
  - Through the network from A to B
- Belongs to Network Layer
  - (layer 3 in OSI model)



Routing algorithm determines the path

- Network consists of
  - End systems and
  - Routers
- Router runs routing algorithm and forward packets to the right nodes
  - Defines on which outgoing line an incoming packet will be transmitted
- Given the network, routing algorithm finds a “good” path from A to B
  - “Good” typically means “lowest cost”

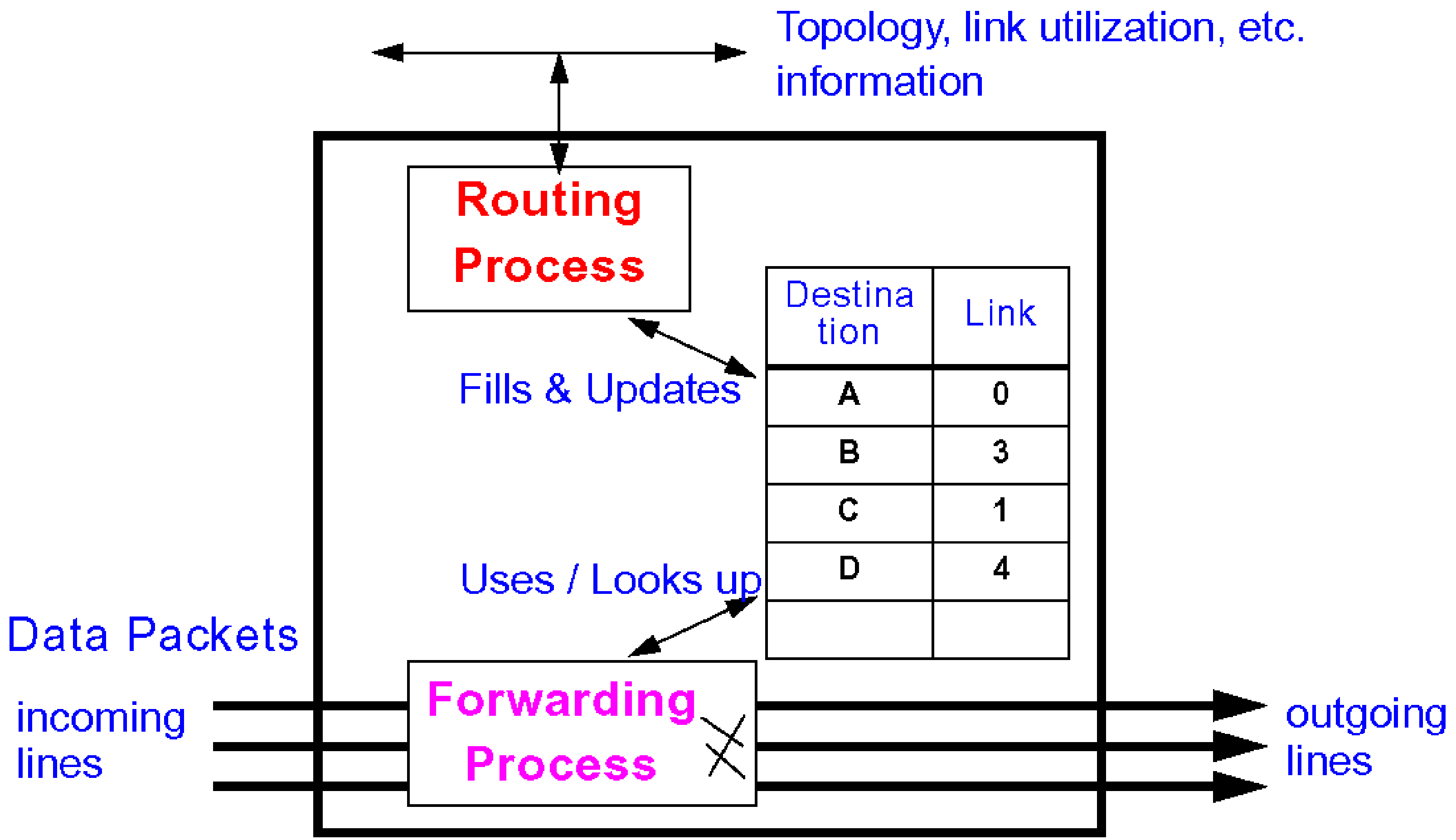
Different networks have different routing algorithms

- Internet uses several routing algorithms “simultaneously”

5.1 Routing: Foundations & Forwarding

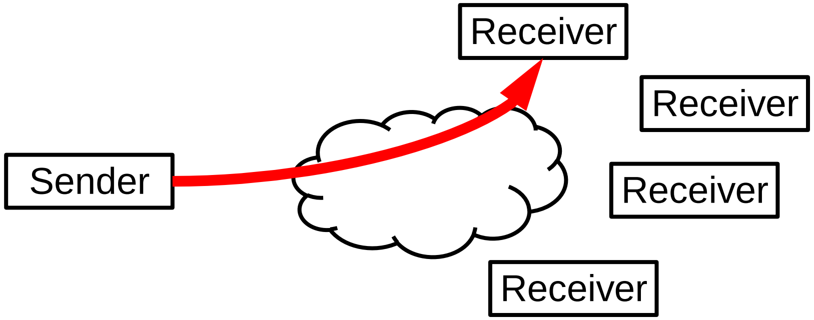
Distinction

- Routing: to take a decision which route to use
- Forwarding: to define what happens when a packet arrives

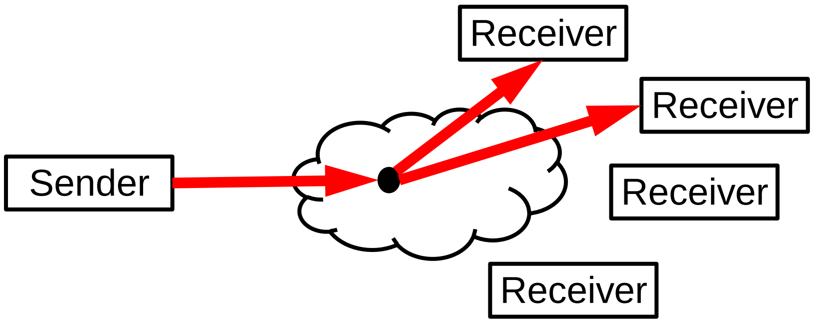


Terminology

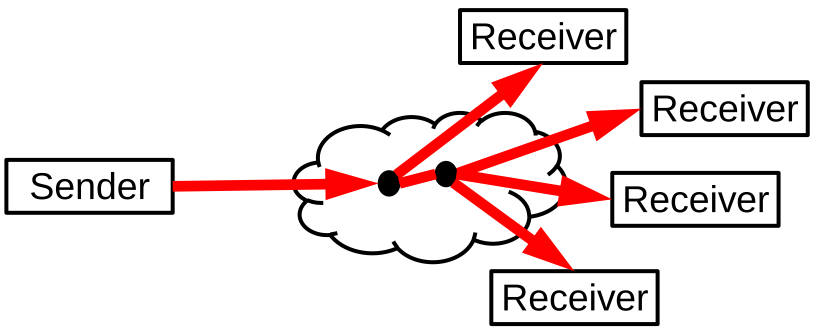
- Unicast: 1:1 communication



- Multicast: 1:n communication



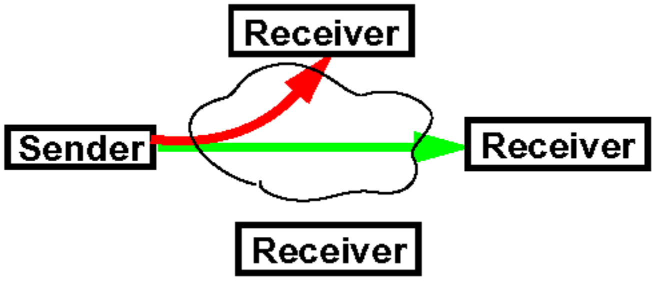
- Broadcast: 1:all communication



Multicast Routing

Multicast Definition

- Unicast: 1:1 communication
- Multicast: 1:n communication



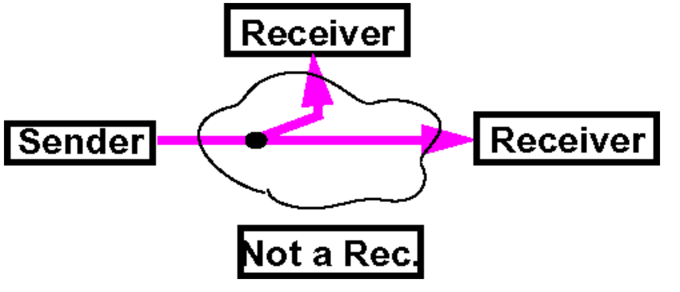
Tasks

- To send data to a group of end systems
- One-time sending instead of multiple sending
- To maintain the overall load at a low level

Results

- To lower load in the network
- To lower load at the sender

Precondition: group addressing

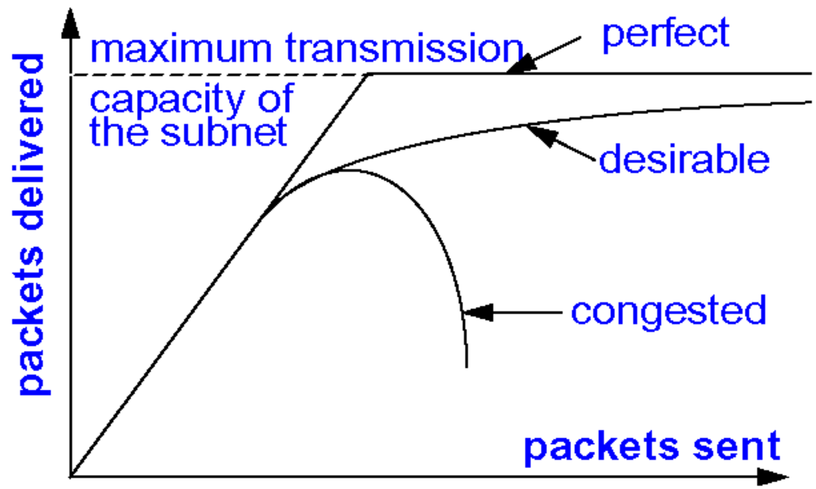


- Group membership may change, managed for example by
  - Internet Group Management Protocol (IGMP)
    - Group management (create, destroy, join, leave)
    - Somehow related protocols for session maintenance
    - Session Description Protocol (SDP)
    - Session Announcement Protocol (SAP)
    - Session Initiation Protocol (SIP)

6 Congestion Control - Basics

If too much traffic is offered

- Congestion occurs
- Performance degrades



Reasons for congestion, among others

- IS too slow for routing algorithms
- Incoming traffic overloads outgoing lines

Congestions tend to amplify themselves

Example:

IS drops packet due to congestion

→ Packet has to be retransmitted

→ Additional bandwidth used

→ Sender cannot release the buffer

→ Additional tying up of resources

Congestion control vs. Flow control	
managed by subnet (L3)	**concatenated point-to-point (L2)**
global issue	**more an end-to-end issue**
if possible, avoid from the beginning	**reduce effects**
may use flow control	

Congestion Control - Basics

General methods of resolution

- To increase capacity
- To decrease traffic

Strategy 1: to avoidance

- Traffic shaping, leaky bucket, token bucket, reservation (multicast), isarithmic congestion control
- Flow control (not discussed herein)

Strategy 2: to repair

- Drop packets, choke packets, hop-by-hop choke packets, fair queuing,...

i.e. Taxonomy according to Yang/Reedy 1995

1. Open loop

- To avoid (before congestion happens)
  - Initiate countermeasures at sender
  - Initiate countermeasures at receiver

2. Closed loop

- To repair
  - Explicit feedback: packets are sent from the point of congestion
  - Implicit feedback: source assumes that congestion occurred due to other effects

Congestion Control Mechanisms

Congestion Avoidance

- Principle: Appropriate communication system behavior and design
- Policies at various layers can affect congestion

Congestion Repair / Correction

- Principle: No resource reservation
- Necessary steps
  - 1. to detect a congestion
  - 2. to introduce appropriate procedures for reduction

TECHNISCHE UNIVERSITÄT DARMSTADT

Principle: appropriate communication system behavior and design

Policies at various layers can affect congestion

Data link layer

- Flow control
- Acknowledgements
- Error treatment / retransmission / FEC

Network layer

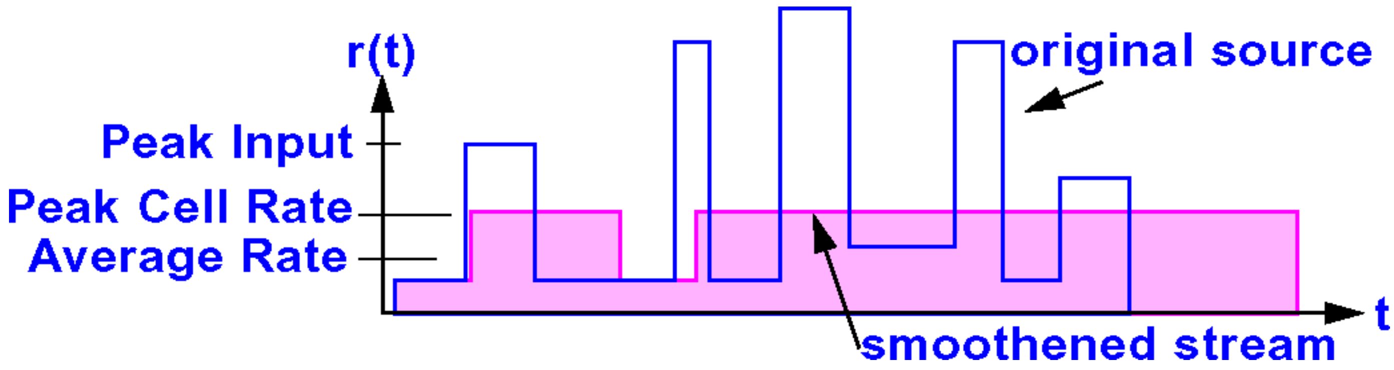
- Datagram (more complex) vs. virtual circuit (more procedures available)
- Packet queuing and scheduling in IS
- Packet dropping in IS (including packet lifetime)
- Selected route

Transport layer

- Basically the same as for the data link layer
- But some issues are harder (determining timeout interval)

Avoidance by Traffic Shaping

TECHNISCHE UNIVERSITÄT DARMSTADT



Motivation

- Congestion is often caused by bursts
- Bursts are relieved by smoothening the traffic (at the cost of a delay)

Application

- ”Traffic shaper” smoothens extremely fluctuating traffic
- Differentiated services, Integrated services
  - traffic classification and prioritization

→ Procedure

- To negotiate the traffic contract beforehand (e.g., flow specification)
- The traffic is shaped by the end device
  - average rate and
  - burstiness

Note

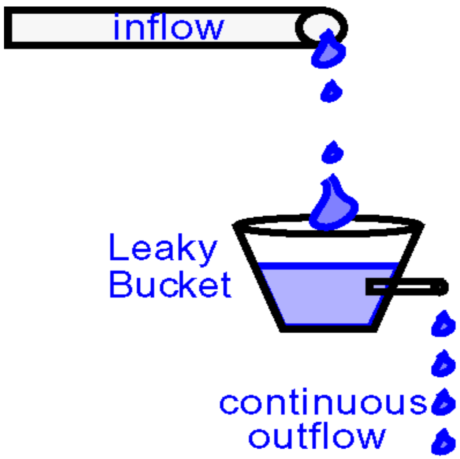
- Sliding window
  - refers only to packets
  - does not refer to rate
- Trade-off:
  - loss of cells/packets
  - vs. delay

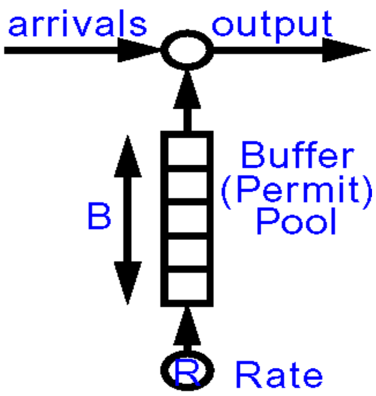
7.1 Traffic Shaping with Leaky Bucket

Principle

- Continuous outflow
- Congestion corresponds to data loss
- 1986: Turner

Bucket size determines maximum capacity until overflow (drop/loss) and possible delay





Another possibility is (*r, T*) shaping:

- Frames of *T* bits (system-wide), fraction *r* assigned per connection
- Within interval *T*, sender may not send more than *r* bits
- If “current packet” would exceed *r*, wait until next interval

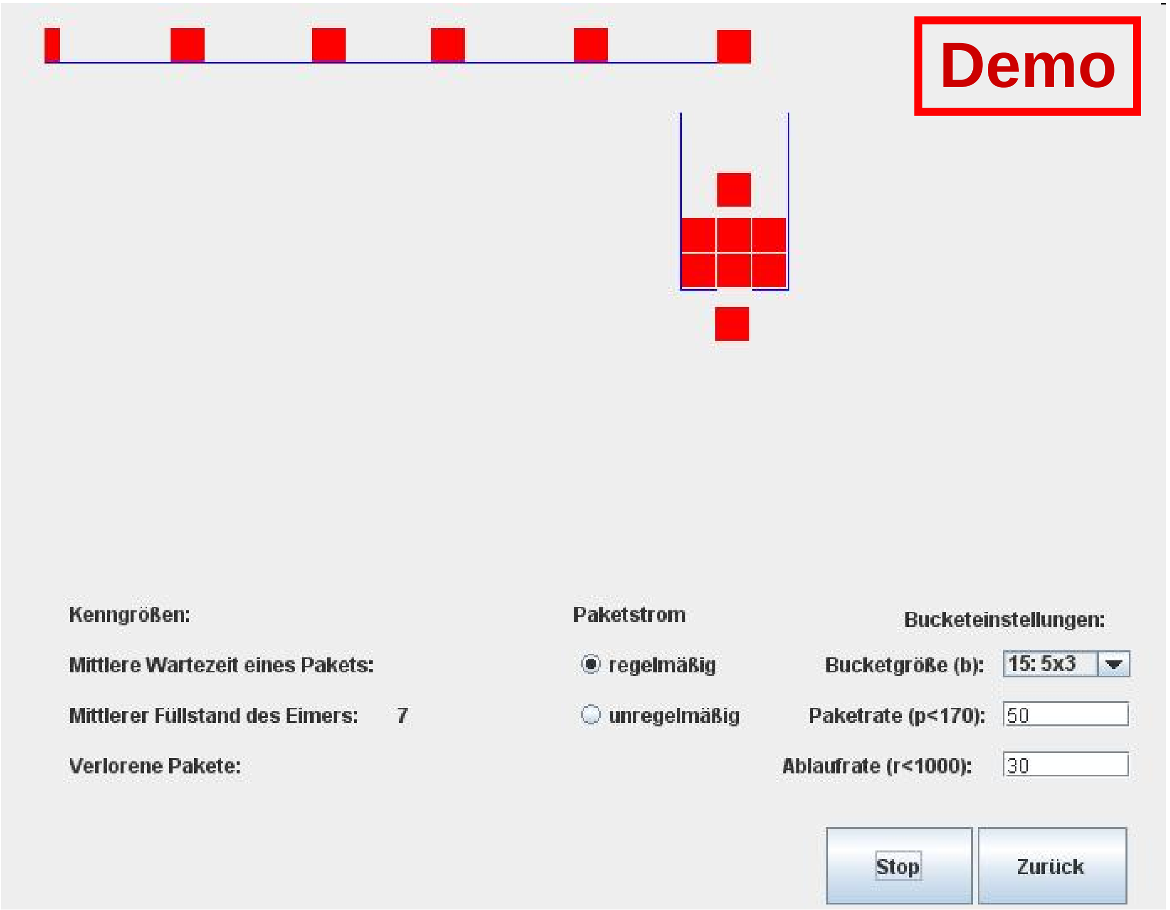
Implementation

- Easy if packet length stays constant
- Example

Leaky Bucket (and Token Bucket)

Simulates

- Leaky Bucket algorithm



See KN-1 Wiki and
Source: Prof. Dr. Carsten Vogt, FH Köln
http://www.nt.fh-koeln.de/fachgebiete/inf/vogt/mm/buckets/buckets.html

7.2 Traffic Shaping with Token Bucket

Principle

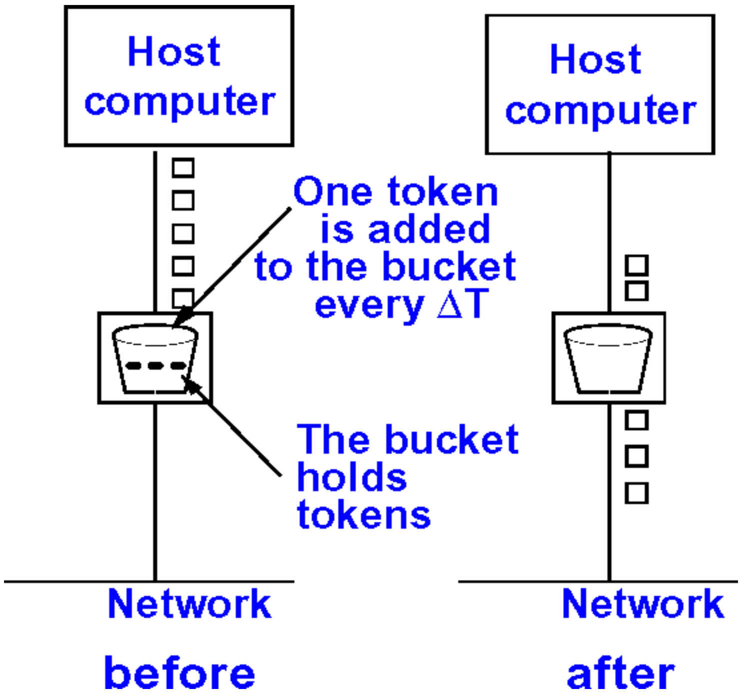
- Permit a certain amount of data to flow off for a certain amount of time
- Controlled by "tokens"
- Number of tokens limited

Implementation

- Add tokens periodically until maximum has been reached
- Remove token depending on the length of the packet (byte counter)

→ Comparison

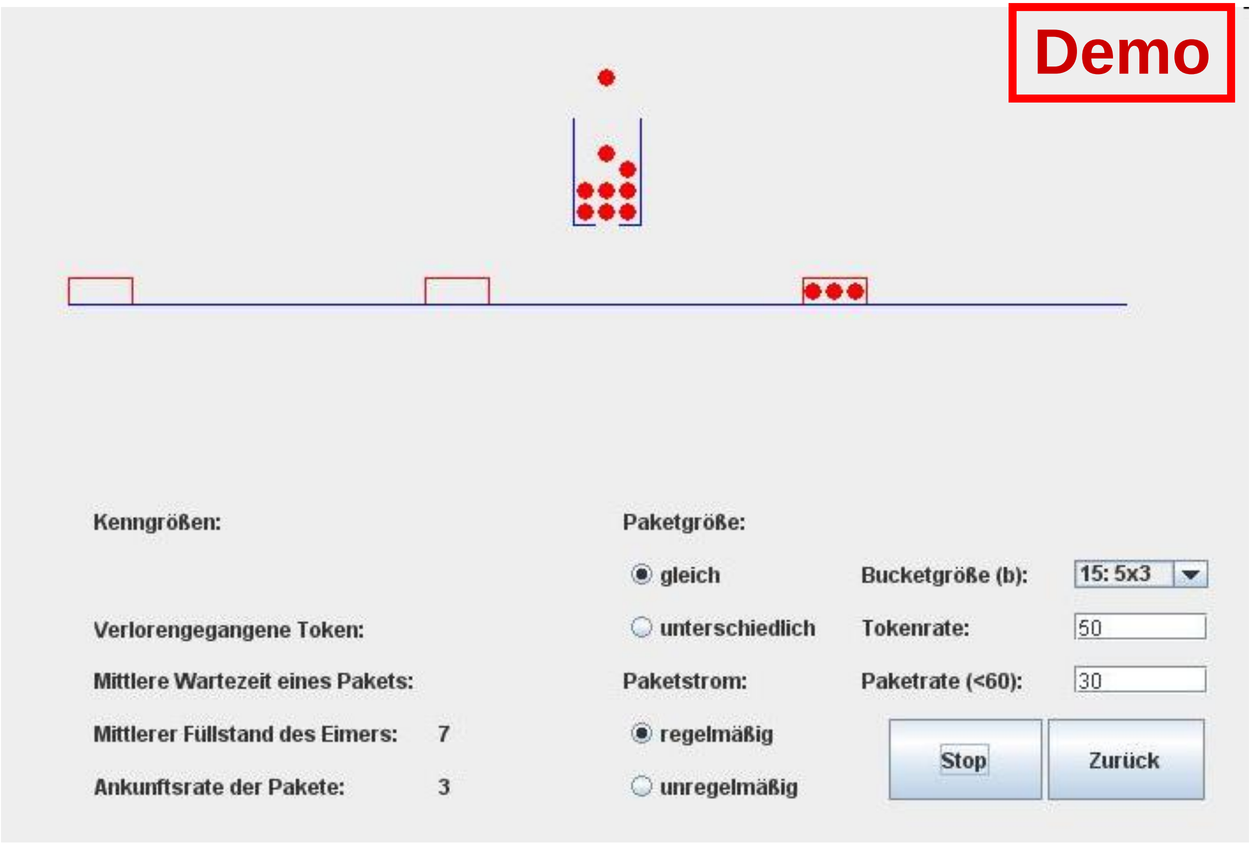
- Leaky Bucket
  - max. constant rate (at any point in time)
- Token Bucket
  - permits a limited burst



(Leaky Bucket and) Token Bucket

Simulates

- Token Bucket algorithm



See KN-1 Wiki and
Source: Prof. Dr. Carsten Vogt, FH Köln
http://www.nt.fh-koeln.de/fachgebiete/inf/vogt/mm/buckets/buckets.html

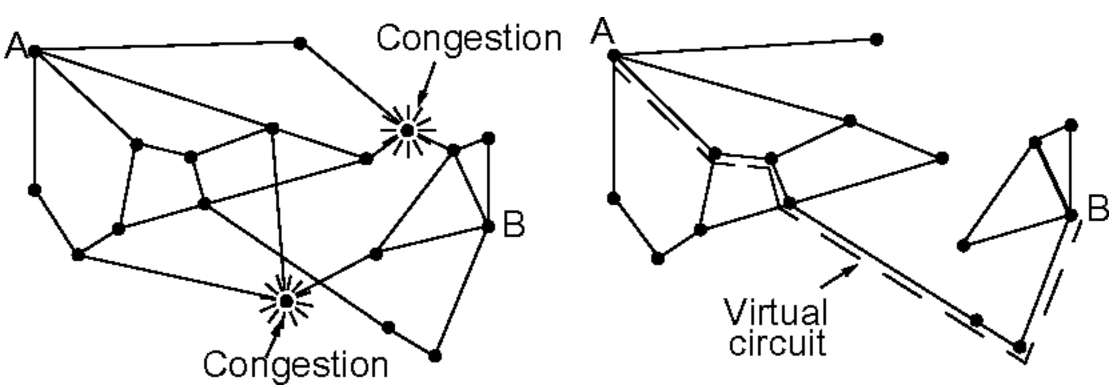
7.3 Avoidance by Reservation: Admission Control

Principle

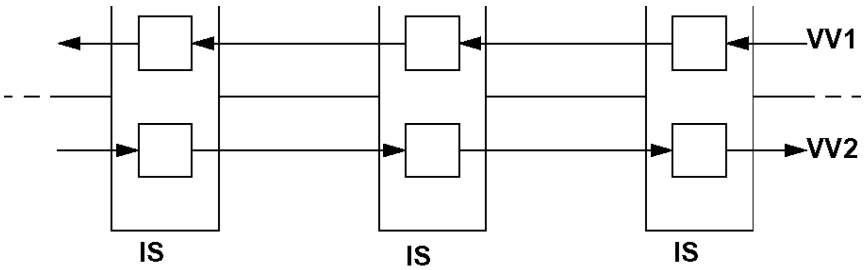
- Prerequisite: virtual circuits
- Reserving the necessary resources (incl. buffers) during connect
- If buffer or other resources not available
  - alternative path
  - desired connection refused

Example

- Network layer may adjust routing based on congestion
- When the actual connect occurs



Avoidance by Buffer Reservation



Principle: buffer reservation

Implementation variant: Stop-and-Wait protocol

- One buffer per IS and connection (simplex, VC=virtual circuit)

Implementation variant: Sliding Window protocol

- *m* buffer per IS and (simplex-) connection (*m* corresp. to the window size)

Properties

- Congestion not possible
- Buffers remain reserved, even if there is no data transmission for some periods

→ usually only with applications that require low delay & high bandwidth

  - e. g. digital voice transmission

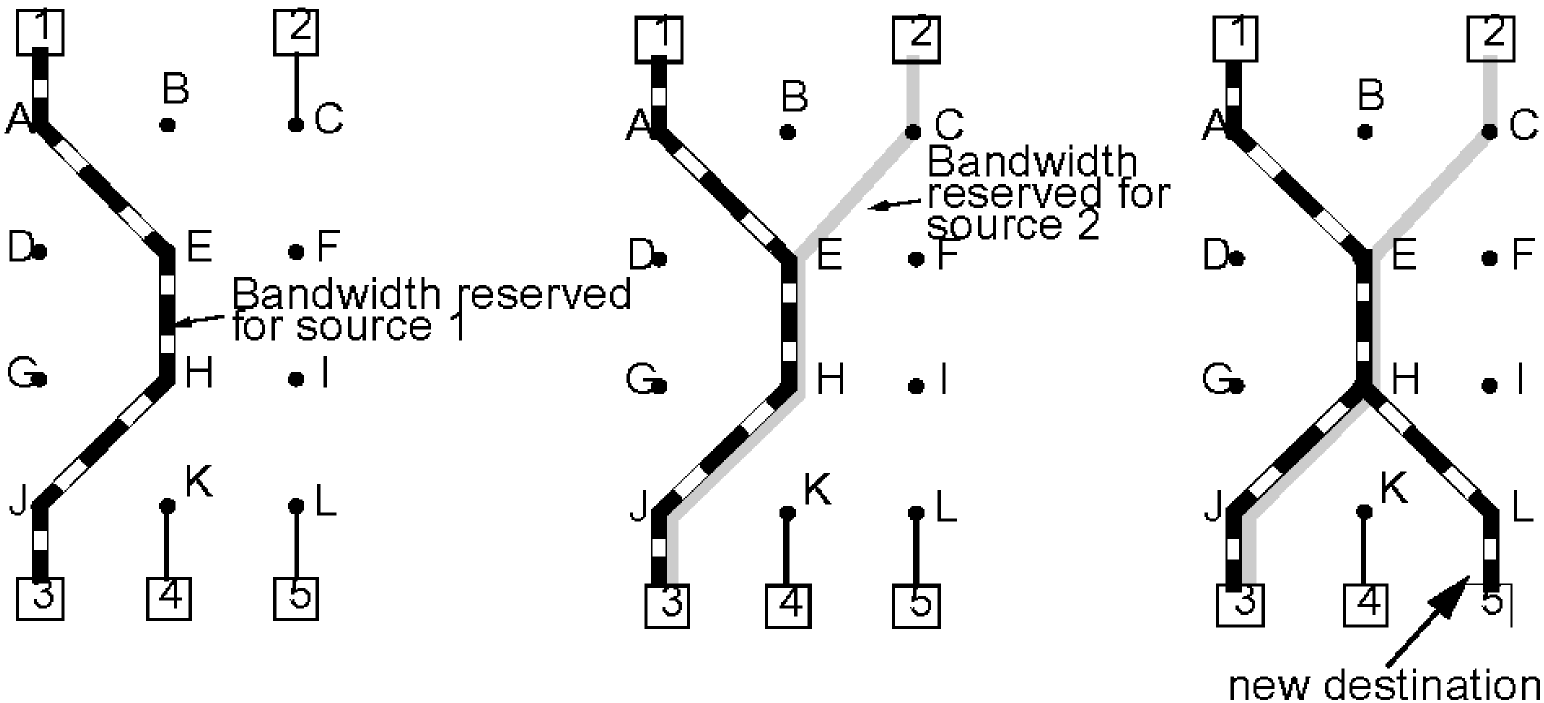
TECHNISCHE UNIVERSITÄT DARMSTADT

Reservation protocols

- Resource Reservation Protocol (RSVP)
- Stream Type Protocol Version 2 (ST-2)

Searching for the most ideal IS to connect to an multicast group

Example



7.4 Avoidance by Isarithmic Congestion Control

Principle

- Limiting the number of packets in the network by assigning "permits"
  - Amount of "permits" in the network
  - A "permit" is required for sending
    - when sending: "permit" is destroyed
    - when receiving: "permit" is generated

Problems

- Parts of the network may be overloaded
- Equal distribution of the "permits" is difficult
- Additional bandwidth for the transfer of "permits" necessary
- Bad for transmitting large data amounts (e.g. file transfer)
- Loss of "permits" hard to detect

TECHNISCHE UNIVERSITÄT DARMSTADT

Principle: no resource reservation

Necessary steps

1. to detect a congestion
2. to introduce appropriate procedures for reduction

Packet Dropping

Principle: incoming packet is dropped, if it cannot be buffered

Preconditions for

- Datagram:
  - no preparations necessary
- Connection-oriented service:
  - packet will be buffered until receipt has been acknowledged

… Buffer assignment methods

1. Permanent buffers per incoming line

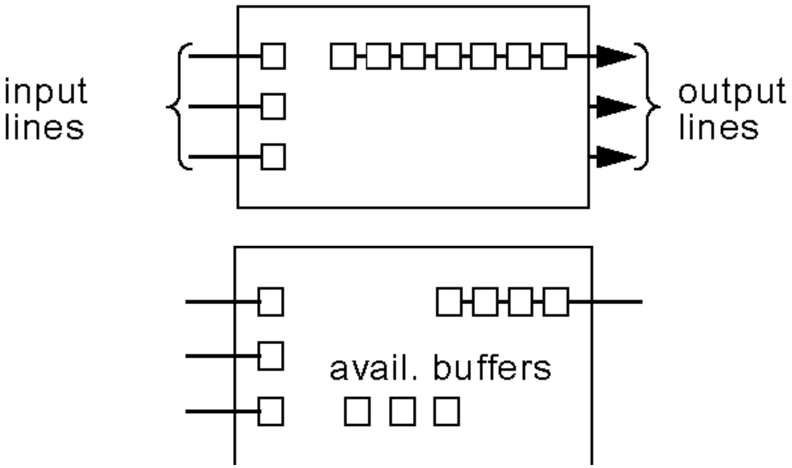
But, e.g.

- If an ACK would have to be discarded
- ACK may have been required to release buffer

→ **critical**

2. Maximum number of buffers per output line

- Example: packet dropped despite there are free lines
- Heuristic rule [Irland]



$$m = \frac{k}{\sqrt{s}}$$

m : max. number of buffers per output line

k : total number of buffers

s : number of output lines

3. Minimal number of buffers per output line

- Line cannot be starved

2. + 3. : Example ARPANET

- A combination of 2) and 3)

Packet Dropping - Buffer Assignment Methods

TECHNISCHE UNIVERSITÄT DARMSTADT

4. Content-related dropping: relevance

- Reference
  - data connection as a whole
  - single data packets
    - from one end system to another end system

- Examples
  - WWW document: images vs. text and structural information
  - File transfer:
    - old packets more important than new ones

    → algorithm to initiate correction process should start as late as possible

- Implementation of priorities in virtual circuits or datagrams

Packet Dropping

Properties

- Very simple

But

- retransmitted packets waste bandwidth:
- packet has to be sent *x* times before it is accepted, with

$$x = \frac{1}{1-p}$$

p : probability that packet will be dropped

Optimization necessary to reduce the wastage of bandwidth

- Dropping packets that have not gotten that far yet

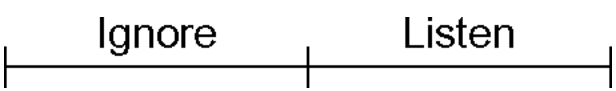
8.2 Choke Packets

Principle

- Reduce traffic during congestion by telling source to slow down

Proedure for Intermediate Station (IS):

- Each outgoing line (OL) has one variable : utilization
- Calculating utilization u ($0 \leq u \leq 1$) :
  - IS checks line usage f periodically ($f \in [0;1]$)
  - $u = a * u_{previous\_value} + (1 - a) * f$
  - $0 \leq a \leq 1$: constant determining to what extent "history" is taken into account
- $u > threshold$: OL changes to condition "warning"
- Send CHOKE PACKET to source (indicating destination)
- Tag packet (to avoid further choke packets from down stream IS) and forward it



Procedure for source

- Source receives the choke packet and reduces the data traffic to the destination in question by X_1%
- Source recognizes 2 phases: (gate time so that the algorithm can take effect)
  - Ignore: source ignores further Choke packets
  - Listen: source listens if more Choke packets are arriving

    Yes → further reduction by X_2%; go to Ignore phase

    No → increase the data traffic

Enhancements

- Varying choke packets depending on state of congestion
  - warning
  - acute warning
- Instead of utilization u use
  - queue length
  - ....

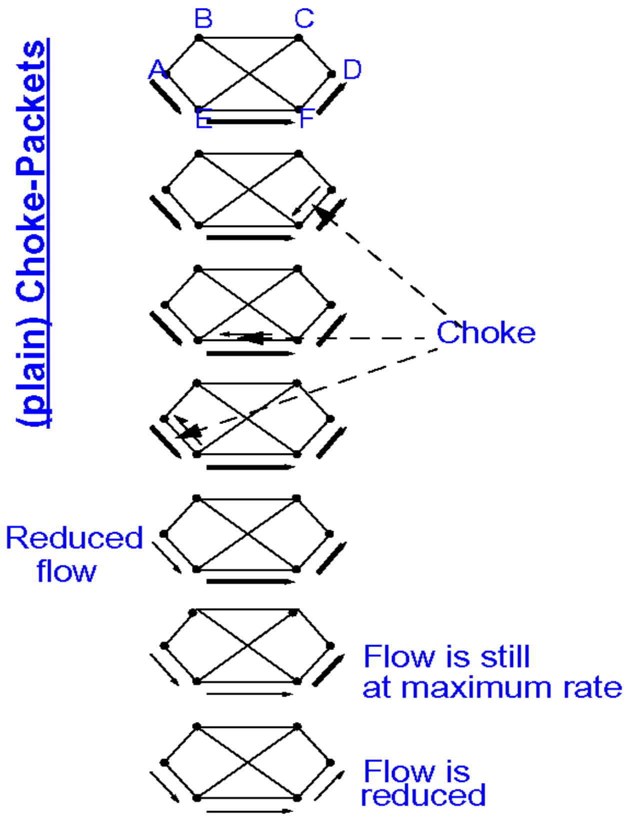
Properties

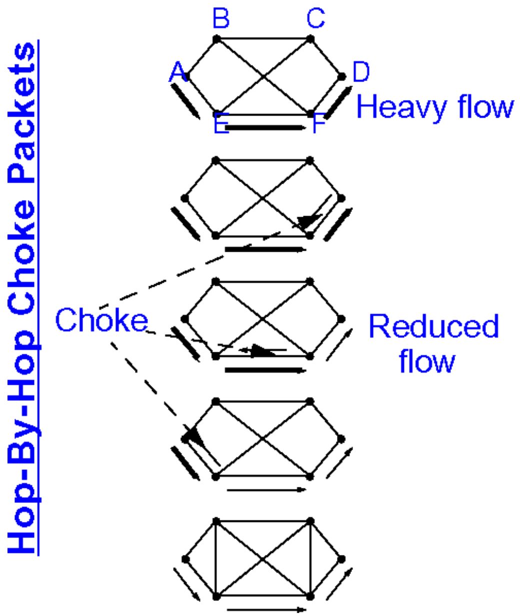
- Effective procedure
- But
  - possibly many choke packets in the network, even if ‘Choke bits’ may be included in the data at the senders to minimize reflux
  - end systems (ES) can (but do not have to) adjust the traffic
  - superimposed by mechanisms
    - L2 flow control, ...
    - L4 TCP, ..

Choke Packets: Hop-by-Hop Choke Packets

Principle: reaction to Choke packets already at IS (not only at ES)

Example





8.3 Fair Queuing

Background

- End system ES which adapts itself to the traffic should not be disadvantaged
  - Adapting by e.g., Choke-Packet algorithm

Principle

- At the IS on each outgoing line (of the IS) each ES receives its own queue
- Packet sending based on Round-Robin - always one packet of each queue (sender)

Enhancement "FAIR QUEUING WITH BYTE-BY-BYTE ROUND ROBIN"

- Adapt Round-Robin to packet length
- But weighting is not taken into account

Enhancement "WEIGHTED FAIR QUEUING"

- Favoring (statistically) certain traffic
- Criteria variants in relation to
  - VPs (virtual paths)
  - service specific (individual quality of service)
  - etc.

TECHNISCHE UNIVERSITÄT DARMSTADT

Idea

- Congestion should be attacked as early as possible
- Some transport protocols (e.g., TCP) react to lost packets by rate reduction

IS drops some packets before congestion is significant (i.e., early)

→ gives time to react

- Dropping starts when moving avg. of queue length exceeds threshold
  - small bursts pass through unharmed
  - only affects sustained overloads
  - packet drop probability is a function of mean queue length
    - prevents severe reaction to mild overload

RED; can MARK PACKETS INSTEAD OF DROPPING THEM

- Allows sources to detect network state without losses
- Improves performance of a network of cooperating TCP sources
- No bias against bursty sources
- Controls queue length regardless of endpoint cooperation

TECHNISCHE UNIVERSITÄT DARMSTADT

3 types of identifiers: Names, Addresses and Routes [Shoch 78]

"The NAME of a resource indicates WHAT we seek,
an ADDRESS indicates WHERE it is, and
a ROUTE says HOW TO GET THERE."

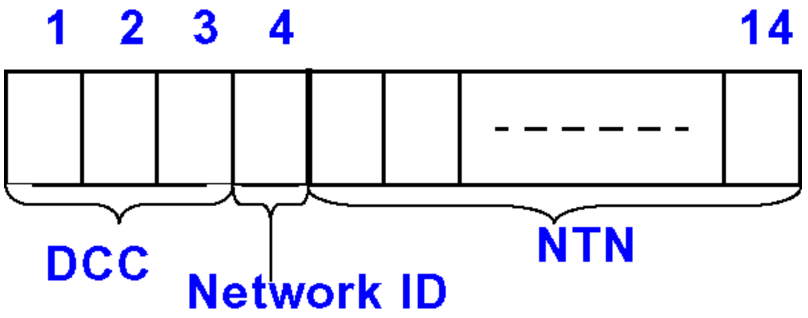
Objectives

- Global addressing concept for ES
- Simplified address allocation
- Addresses independent from
  - type and topology of the subnetworks
  - number and type of the subnetworks to which the ES have been connected
  - location of a source ES

9.1 X.121 Addressing

CCITT/ITU "numbering scheme"

- Addressing concept for public data networks
- A.o., used by X.25



X.121 address

- A maximum of 14 digits
- Consisting of
  - Data Network Identification Code (4 digits)
    - Data Country Code (digits 1 - 3)
    - Network Identification (digit 4)
  - Network Terminal Number (max. 10 digits)

Example:

DCC for USA: 310 - 329, i. e. max. 200 networks

DCC for Tonga: 539, i. e. max. 10 networks

9.2 OSI Addressing

Objective
- Global addressing concept for both existing and new subnetworks

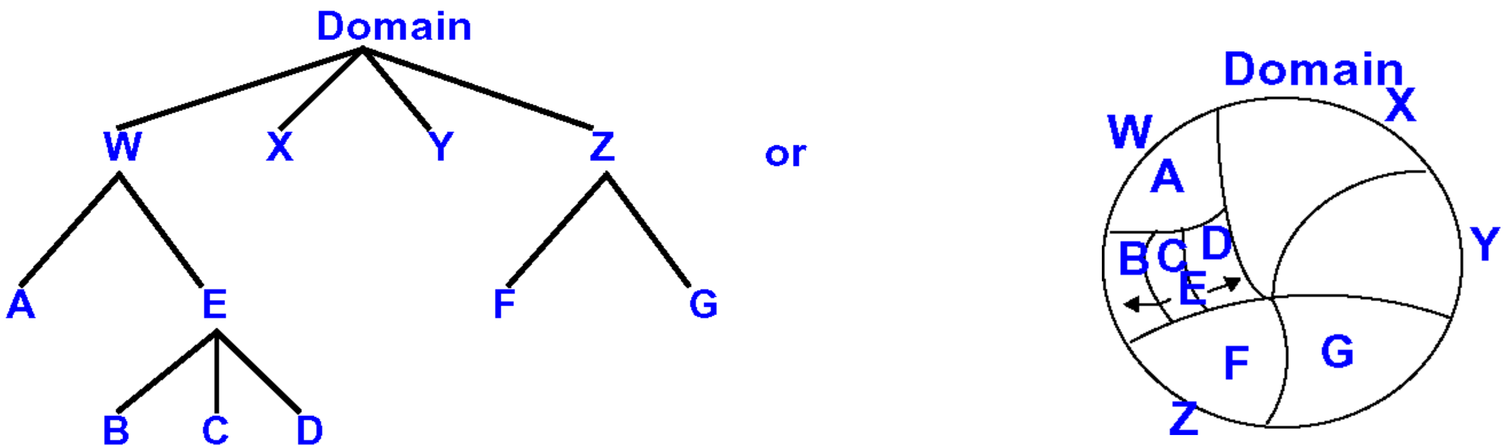
Situation: different concepts exist for
- Public networks:
  - X.121: data networks
  - F.69: telex
  - E.163: telephone network
  - E.164: ISDN, ...
- Private networks

→ i.e., a flexible and expandable concept is necessary

OSI method: unique Network Service Access Point (NSAP) identification

OSI method: hierarchic addresses
- OSI defines the ADDRESSING DOMAINS
- The domain contains the ADDRESSING AUTHORITY
- Addressing Authority
  - allocates addresses
  - creates new domains and delegates authority

OSI Addressing



Graphic representation of the domain hierarchy

A domain may be

- networks of one type
- networks of a geographical region
- networks of an organization
- ...

OSI Addressing: Structure

Address length: 20 bytes (binary) or 40 digits

IDP	DSP

Address structure

- Initial Domain Part (IDP) with
  - AUTHORITY AND FORMAT IDENTIFIER (AFI)
    - specifies how to interpret the IDI (syntax and semantics)
    - e.g. the format of the DSP (binary or digits)

IDI Format	DSP SYNTAX	
	Decimal	Binary
X.121	36	37
ISO DCC	38	39
F.69	40	41

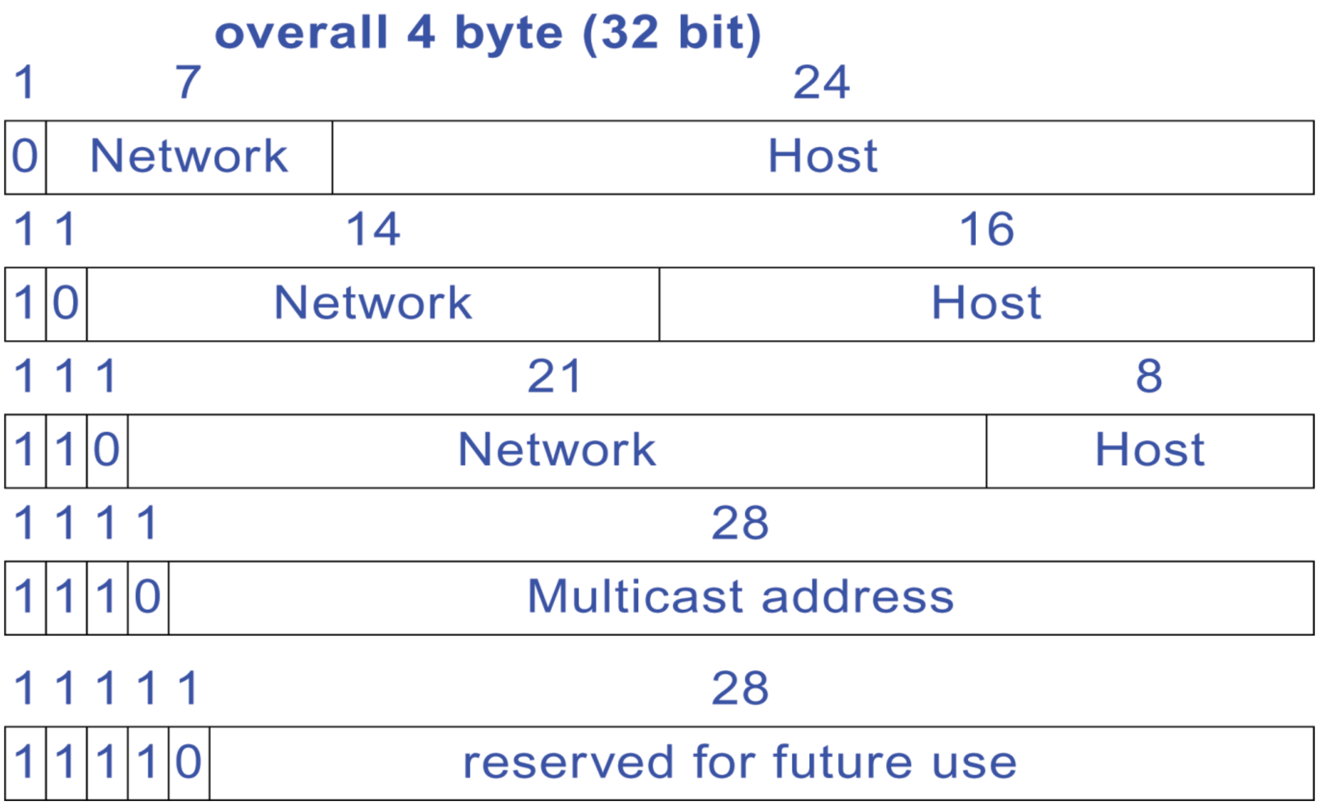
Character	National Character
50	51

- INITIAL DOMAIN IDENTIFIER(IDI)
  - Identifies the Addressing Authority (AA), responsible for ALLOCATING THE NSAP ADDRESSES
  - identifies the domain
- Domain Specific Part (DSP)
  - contains the address clearly identifying the ES within the domain

9.3 Internet Addresses (IP)

Global addressing concept for ES (and IS) in the Internet

- 32 bit address (amount is limited!)
- Each address is unique worldwide
- Structure: Net-ID (Subnet-ID), ES-ID



Internet Addresses (IP)

Notation

- Decimal value for each byte (0...255)
- Subdivided by dots
- Value range: 0.0.0.0 ... 255.255.255.255

Formats: 5 classes

A:	**1.0.0.0**	**up to**	**127.255.255.255**
B:	**128.0.0.0**	**up to**	**191.255.255.255**
C:	**192.0.0.0**	**up to**	**223.255.255.255**
D:	**224.0.0.0**	**up to**	**239.255.255.255 (Multicast)**
E:	**240.0.0.0**	**up to**	**247.255.255.255**

Broadcast addresses: (convention: 11...1 for Host-ID)

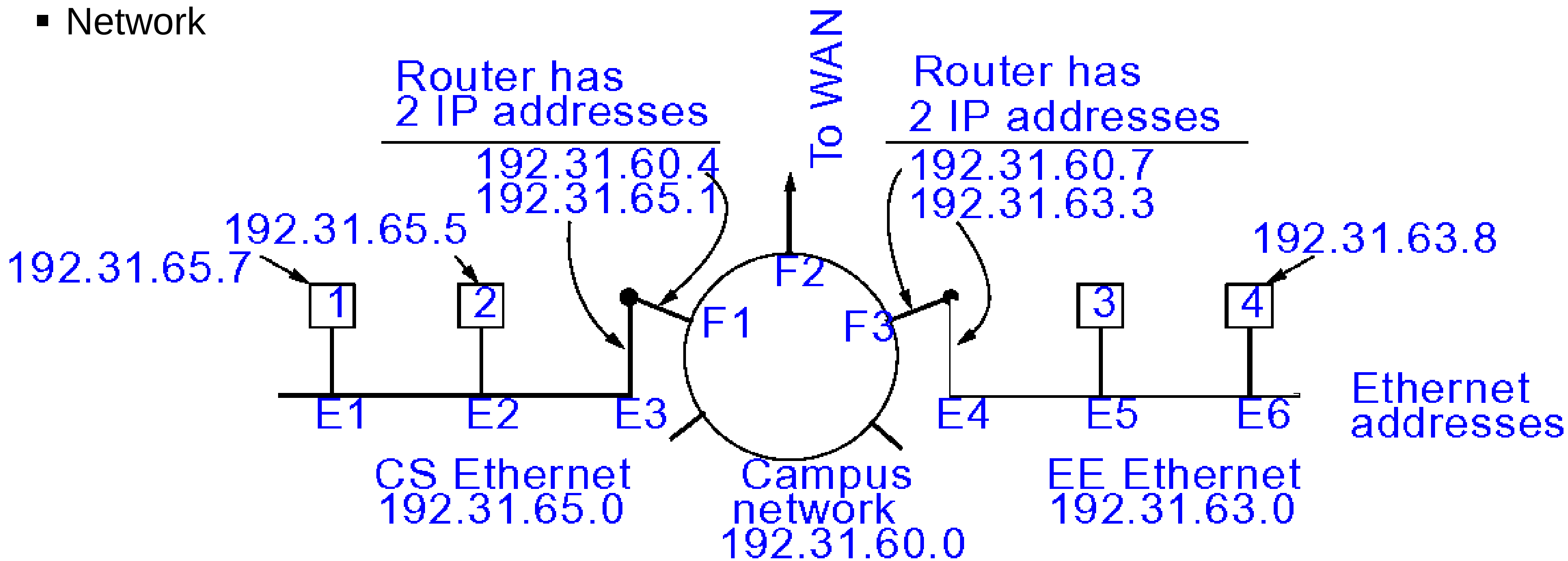
Internet Addresses (IP)

Address allocation

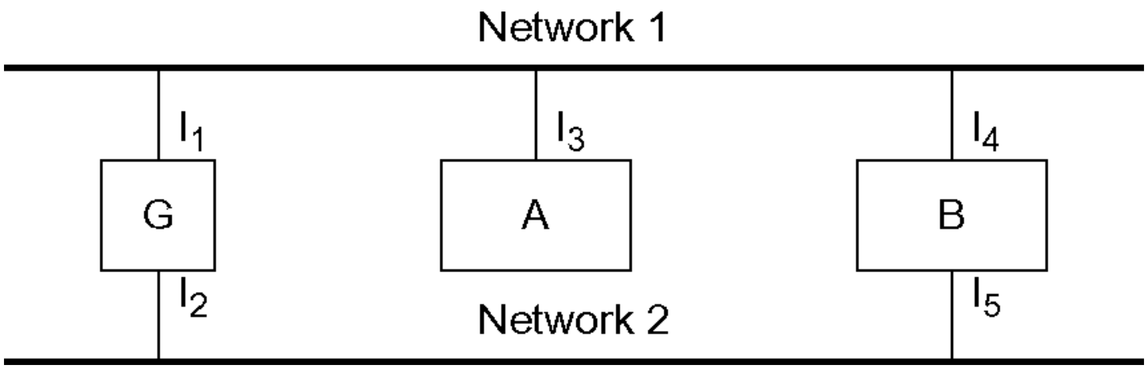
- Class allocation and network range:
  - by a central authority
  - Network Information Center NIC
- End system
  - local
  - possibly forming a subnetwork

Example

- Network



Internet Addresses (IP): A Critical Review



Addresses IDENTIFIY "NETWORK CONNECTIONS", not the ES

- “Multi-homed" ES have more than one address
- A change of the connection forces the modification of the address
- The address has an impact on the chosen route (constitutes a problem in the mobile area)

Example: A cannot reach B via address I5 if G fails

- Comment: is also valid for X.121

Amount of addresses

- Limited

TECHNISCHE UNIVERSITÄT DARMSTADT

IP Version 6 (IPv6)

- 16 byte length (instead of 4 byte length, i.e. approx. 3×10^{38})

Distribution

- Provider-based: approx. 16 mio. companies distribute addresses
- Geographic-based: distribution as it is today
- Link, site-used: address relevant only locally (security, Firewall concept)

E. g. new: Anycast

- Sending data to an individual of a group
- E. g., the one who is geographically the closest