RETELE DE CALCULATOARE

Internetwork Operation

Integrated Service Architecture

Differentiated Services

Networks Security Architecture

Internetwork Operation

Internet & private networks growth, new applications, real time multimedia … – new demands

First approach: Increase internet capacities: not enough

Need to support variety of traffic, variety of Quality of Service (QoS) requirements within the TCP/IP architecture

Specific problems:

- Multicasting
- Internetwork routing algorithms
- Integrated Service Architecture
- Differentiated Services

Multicasting

Addresses that refer to group of hosts on one or more networks

Used in:

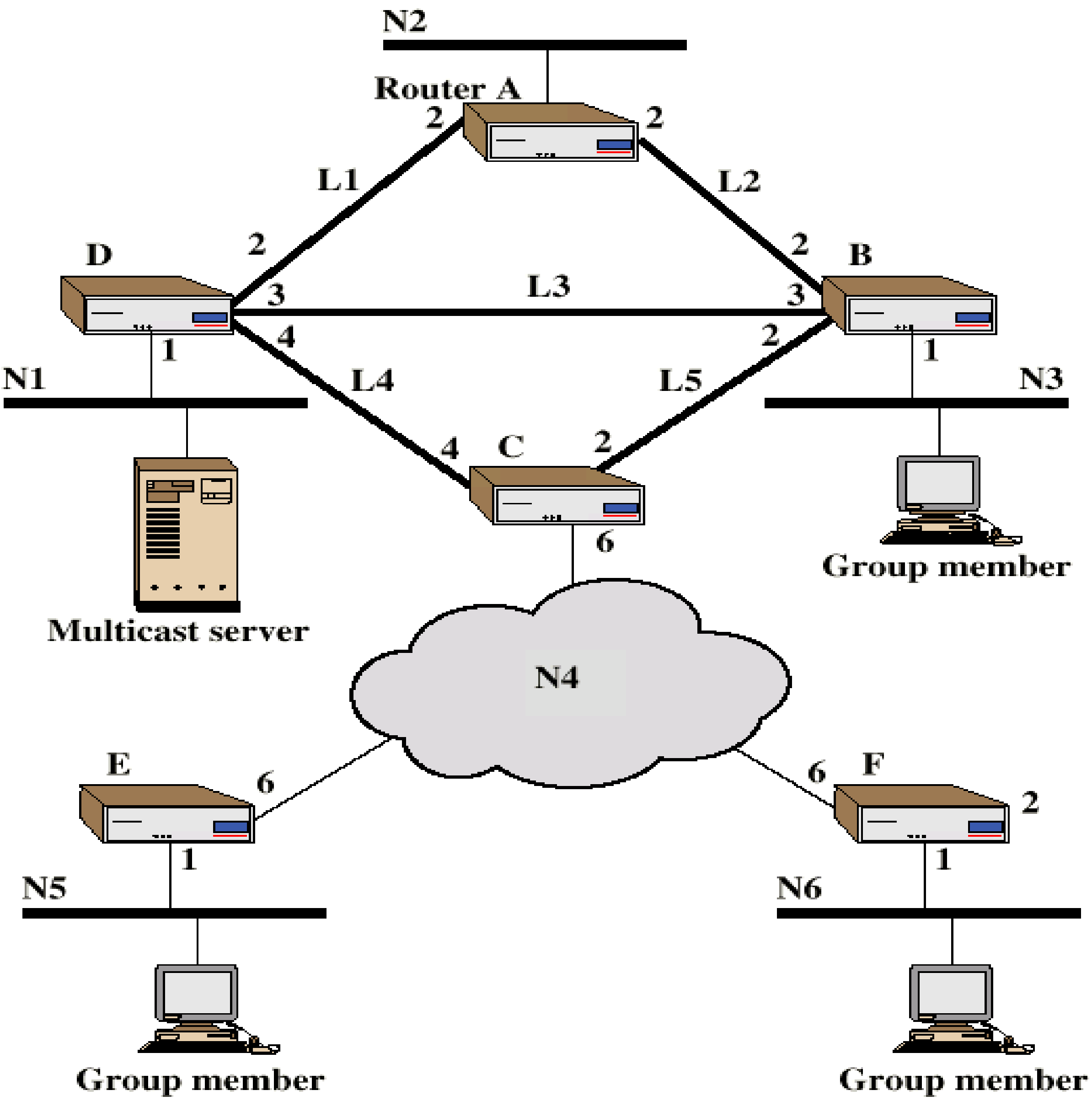
Multimedia stream "broadcasts"

Teleconferencing – a transmission from a station sent to all members

Database updating – for all copies of replicated files or databases

Distributed computing – resource sharing

Real time workgroups – real time exchange of information



Multicast Configuration

Multicast over a single Ethernet LAN segment is straightforward; provision for MAC multicast addresses, due to the broadcast nature of LAN

For Internet environment, more approaches:

Broadcast and Multiple Unicast

Broadcast a copy of packet to each network, even if does not contain group members

For figure behind, multicast server sends a packet to group hosts from networks N3, N5, N6: requires 13 copies of the packet

Multiple Unicast

Send packet only to networks that have hosts in group

Source knows location for each group member

11 packets

True Multicast

Use of following algorithm:

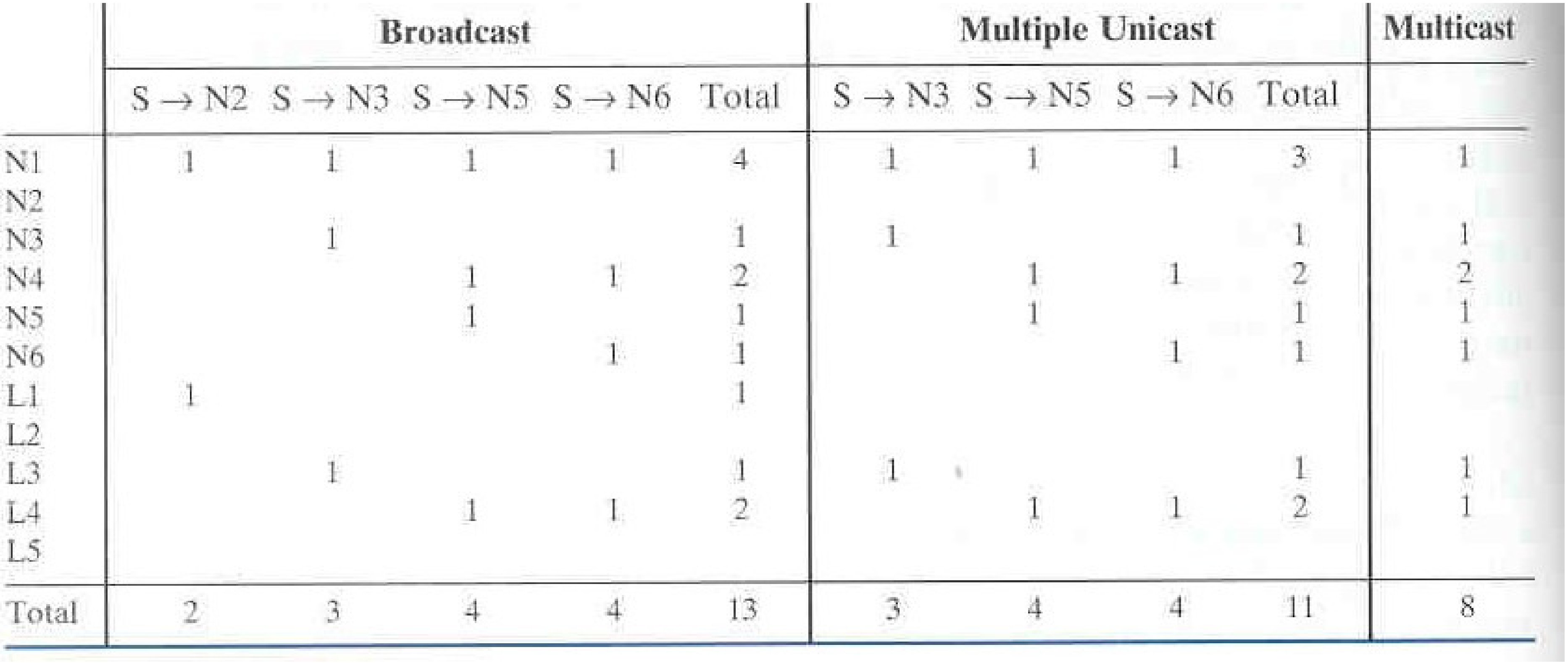
Determine least cost path to each network that has host in group

- Gives spanning tree configuration containing networks with group members

Transmit single packet along spanning tree

Routers replicate packets at branch points of the spanning tree

- 8 packets required for above example



	Broadcast					Multiple Unicast				Multicast
	S → N2	S → N3	S → N5	S → N6	Total	S → N3	S → N5	S → N6	Total	
N1	1	1	1	1	4	1	1	1	3	1
N2										
N3		1			1	1			1	1
N4			1	1	2		1	1	2	2
N5			1		1		1		1	1
N6				1	1			1	1	1
L1	1				1					
L2										
L3		1			1	1			1	1
L4			1	1	2		1	1	2	1
L5										
Total	2	3	4	4	13	3	4	4	11	8

Multicast problems:

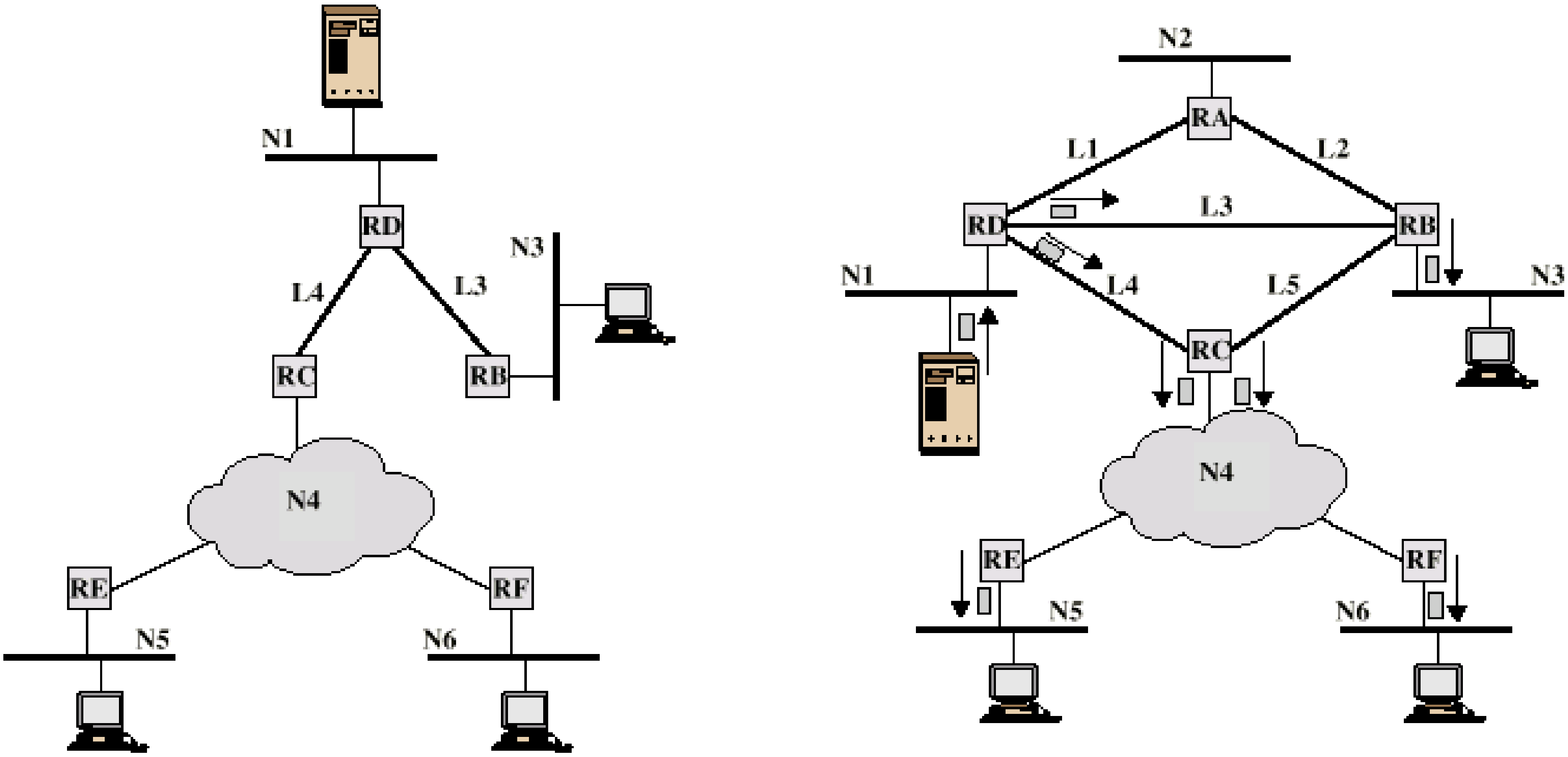
Router may have to forward more than one copy of packet (multiple output branches)

Convention needed to identify multicast addresses

IPv4 - Class D – starts with 1110 …

IPv6 - 8 bit prefix, all 1s, 4 bit flags field, 4 bit scope field, 112 bit group ID

Nodes (routers & source) must translate between IP multicast addresses and a list of networks containing group members; allows tree development



(a) Spanning tree from source to multicast group

(b) Packets generated for multicast transmission

Multicast transmission example

- Router must translate between IP multicast address and a network LAN multicast address (at the MAC level) in order to deliver packet to that LAN
- Mechanism required for hosts to dynamically join and leave multicast groups
- Routers must exchange info
  - Which networks include members of given group
  - Sufficient info to work out shortest path to each network (spanning tree)
  - Routing algorithm to work out shortest path
  - Routers must determine routing paths based on source and destination addresses, for avoiding packet duplication

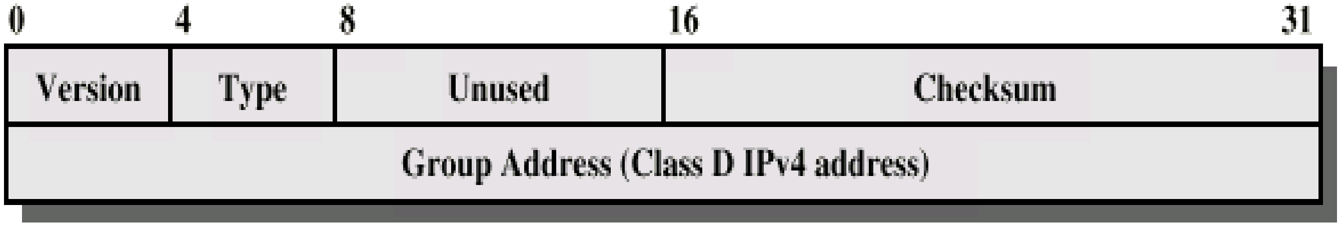
IGMP (Internet Group Management Protocol)

RFC 1112, initial developed for IPv4, but incorporated also in ICMPv6

Host and router exchange of **multicast group information**

Use broadcast LAN to transfer information among multiple hosts and routers

IGMP Fields



0	4	8	16	31
Version	Type	Unused	Checksum	
Group Address (Class D IPv4 address)				

Version - 1

Type

1 - query sent by a multicast router

O - report sent by a host

Checksum – 16 bit ones complement addition of all the 16-bit words in the message

Group address

Zero value in a request message

Valid group address in a report message

IGMP Operation

To join a group, hosts sends report message

- Group address of group to join
- Sent in a IP datagram with the same multicast destination address
- All hosts in group receive message and learn new member
- Routers listen to all multicast addresses to hear all reports

Routers periodically issue request messages (queries)

- Sent to *all-hosts* multicast address
- Host that want to stay in groups must read *all-hosts* messages and respond with report for each group it is in

Group Membership with IPv6

Function of IGMP included in ICMP v6; ICMPv6 contains a new type of message: group membership **termination** message, to allow host to leave the group

Routing Protocols

Routing protocols vs. routed protocols: remember the difference! IP is routed by RIP

Use of concepts:

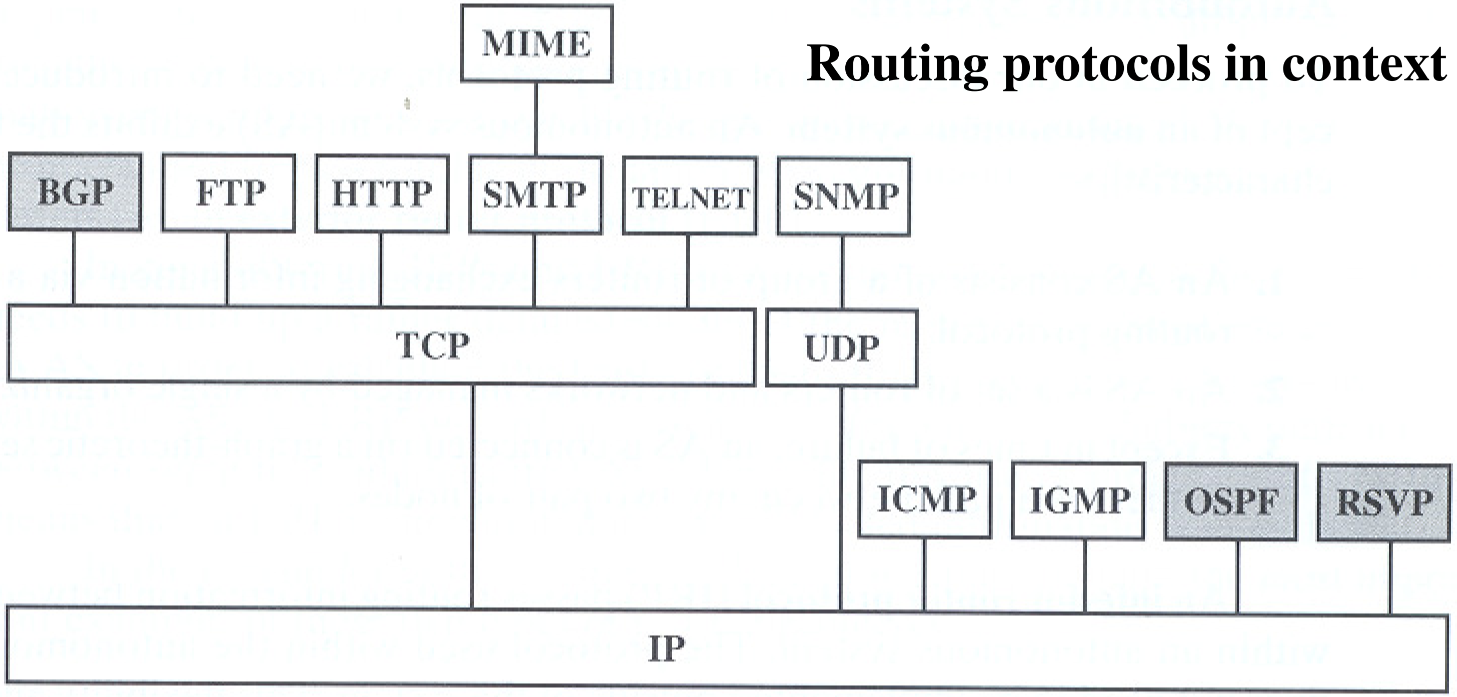
Routing Information

About topology and delays in the internet

Routing Algorithm

Used to make routing decisions based on different kind of routing information

Routing protocols in context



Autonomous Systems (AS)

Consists of:

Group of routers

Exchange information via a common routing protocol

Defined as a set of routers (gateways) and networks managed by a single organization

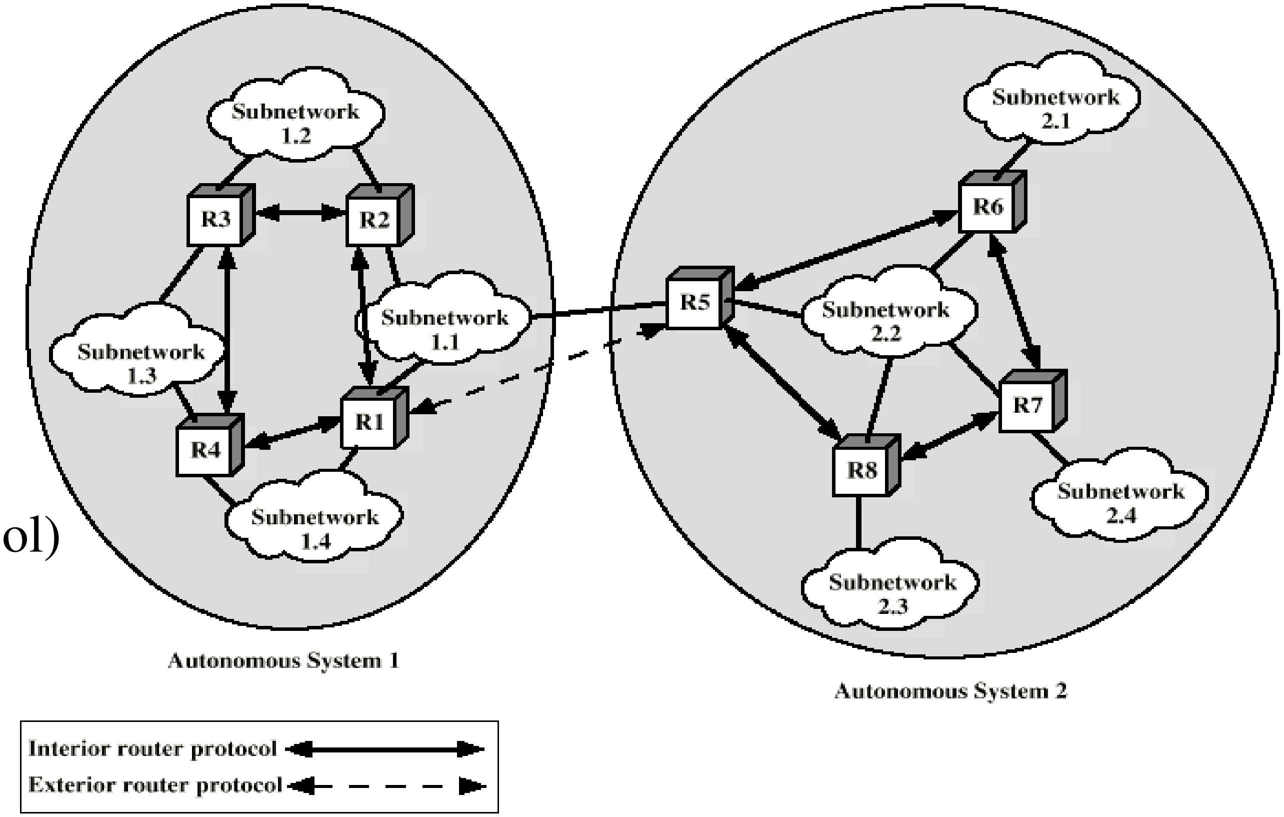
AS represents a connected network

There is at least one

route between any

pair of nodes

Two kind of protocols:
IRP (Interior Router Prot.)
ERP (Exterior Router Protocol)



Interior Router Protocol (IRP)

Passes routing information between routers within one AS

May be more than one AS in internet

Routing algorithms and tables may differ between different AS

IRP needs detailed model of interconnection within an AS

Examples: **RIP** (Routing Information Protocol), **IGRP** (Cisco proprietary RIP), **OSPF** (Open Shortest Path First)

Exterior Router Protocol (ERP)

Routers need some info about networks outside their AS

Used Exterior Router Protocol (ERP)

ERP supports summary information on reachability information between separated AS

Examples: **EGP** (External gateway protocol), **BGP** (Border Gateway Protocol)

Routing Information Protocol (RIP)

Based on the Bellman-Ford (or distance vector) algorithm

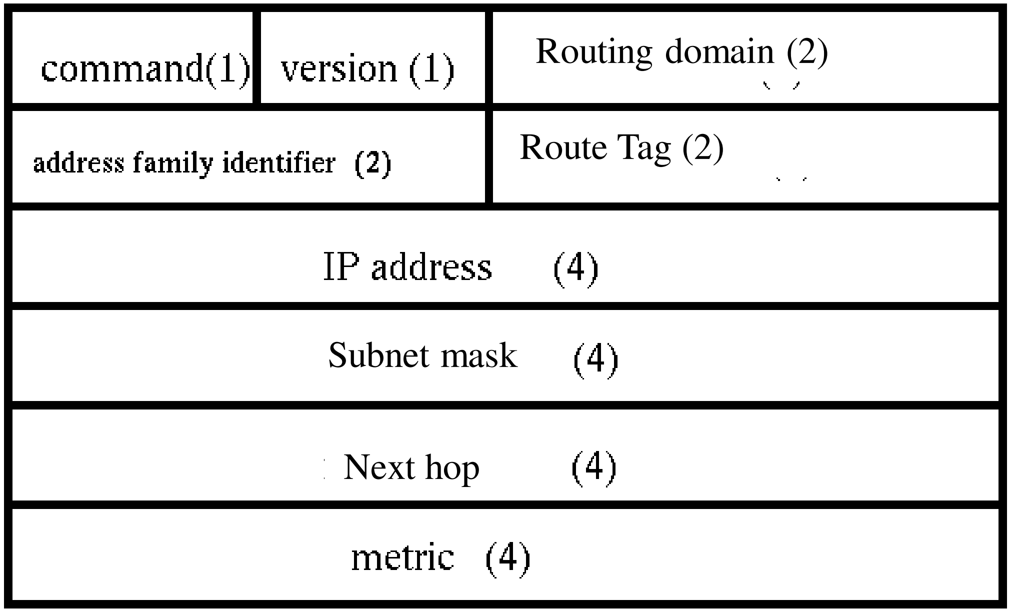
Early developed (‘80s); runs well on LANs & MANs, but too simple for WANs

Slow convergence (due to DV algorithm): changes in network state slowly advertised to the rest of the routers

Only one metric (hop count); not enough for optimum path in WAN (i.e. need to consider link delay, link utilization, etc.) ; IGRP examines link bandwidth & delay

Information change: every 30 seconds – updates

Format of the RIP header



command(1)
version (1)
Routing domain (2)
address family identifier (2)
Route Tag (2)
IP address (4)
Subnet mask (4)
Next hop (4)
metric (4)

Packet format (RIP packet fields):

The portion of the RIP datagram from *address family* field through *metric* may appear up to 25 times (up to 25 possible neighbors)

Command

request for the responding system to send all or part of its routing table
response contains all or part of the sender's routing table
may be sent in response to a request or poll, or it may be an update message

metric field (hop number): a value between 1 and 15 inclusive; 16 means ‘infinity’

address family identifier (allows routing multiple routed protocols); for IP is 2.

Route Tag (RT) field exists as a support for EGP's.

Carries an AS number

Router receiving a RIP entry with a non-zero RT value must re-advertise that value.

Routing domain field enables domains inter-work upon the same physical infrastructure

Implement various kinds of policies

Subnet Mask field contains the subnet mask which is applied to the *IP address* field, to yield the non-host portion of the address

Next Hop is the immediate next hop IP address to which packets to the destination specified by this route entry should be forwarded

Multi-casting is an optional feature in RIP 2 using IP address 224.0.0.9. This feature reduces unnecessary load on those hosts which are not listening to RIP 2. The IP multi-cast address is used for periodic broadcasts.

RIPv2 provides optional **authentication** mechanism. Simplest authentication type is use of a simple password; other would be MD5 mechanism.

Open Shortest Path First (OSPF)

IGP of Internet

Replaced **Routing Information Protocol** (RIP)

Uses **Link State** Routing Algorithm

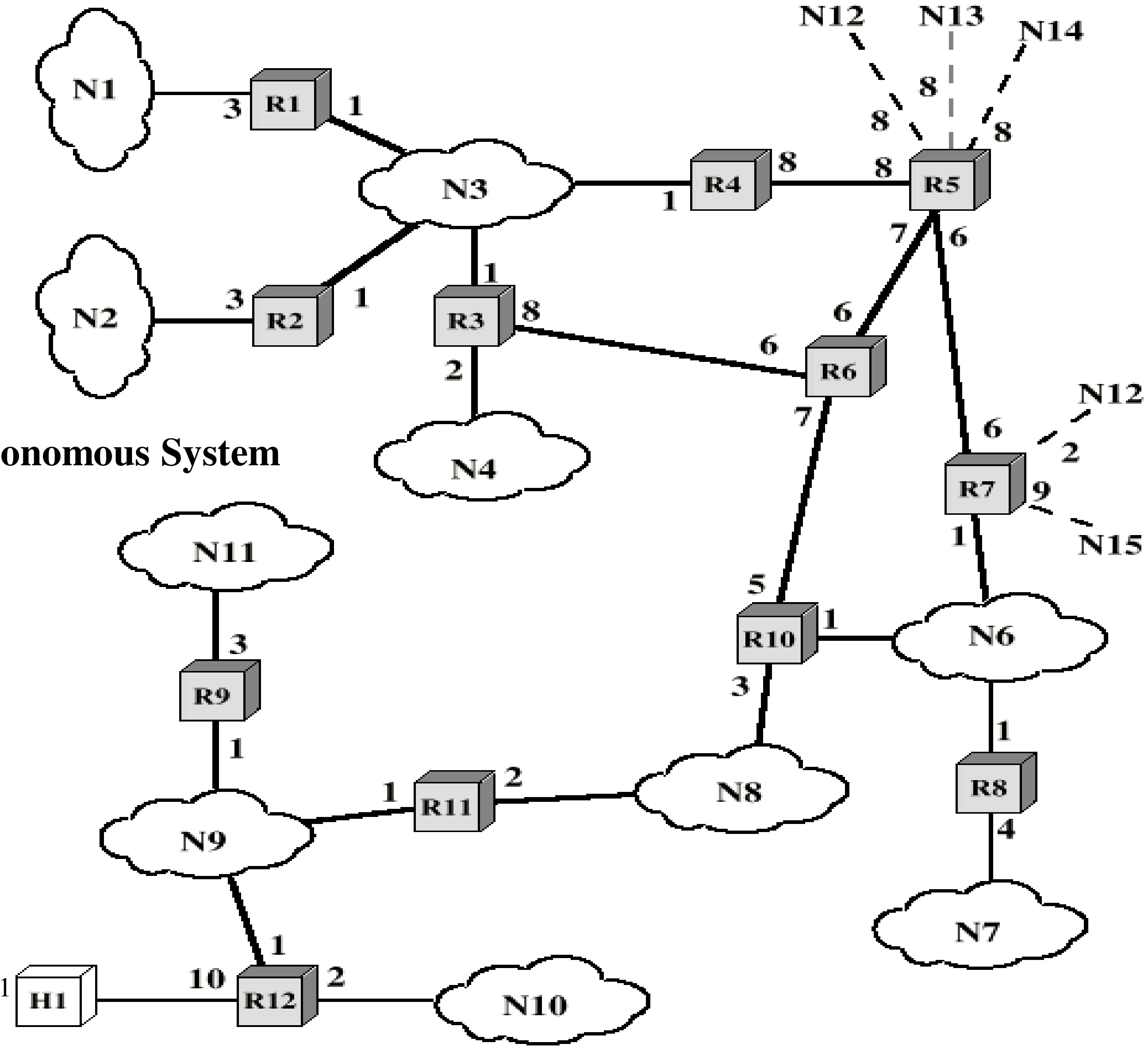
- Each router keeps list of state of local links to network
- Transmits update state info
- Little traffic as messages are small and not sent often
- RFC 2328

Route computed on least cost based on user cost metric

Topology stored as directed graph

- Vertices or nodes
    - Routers
    - Network(s)
        - Transit
        - Stub
- Edges
    - Graph edge
        - Connect two routers
        - Connect router to network

Sample Autonomous System



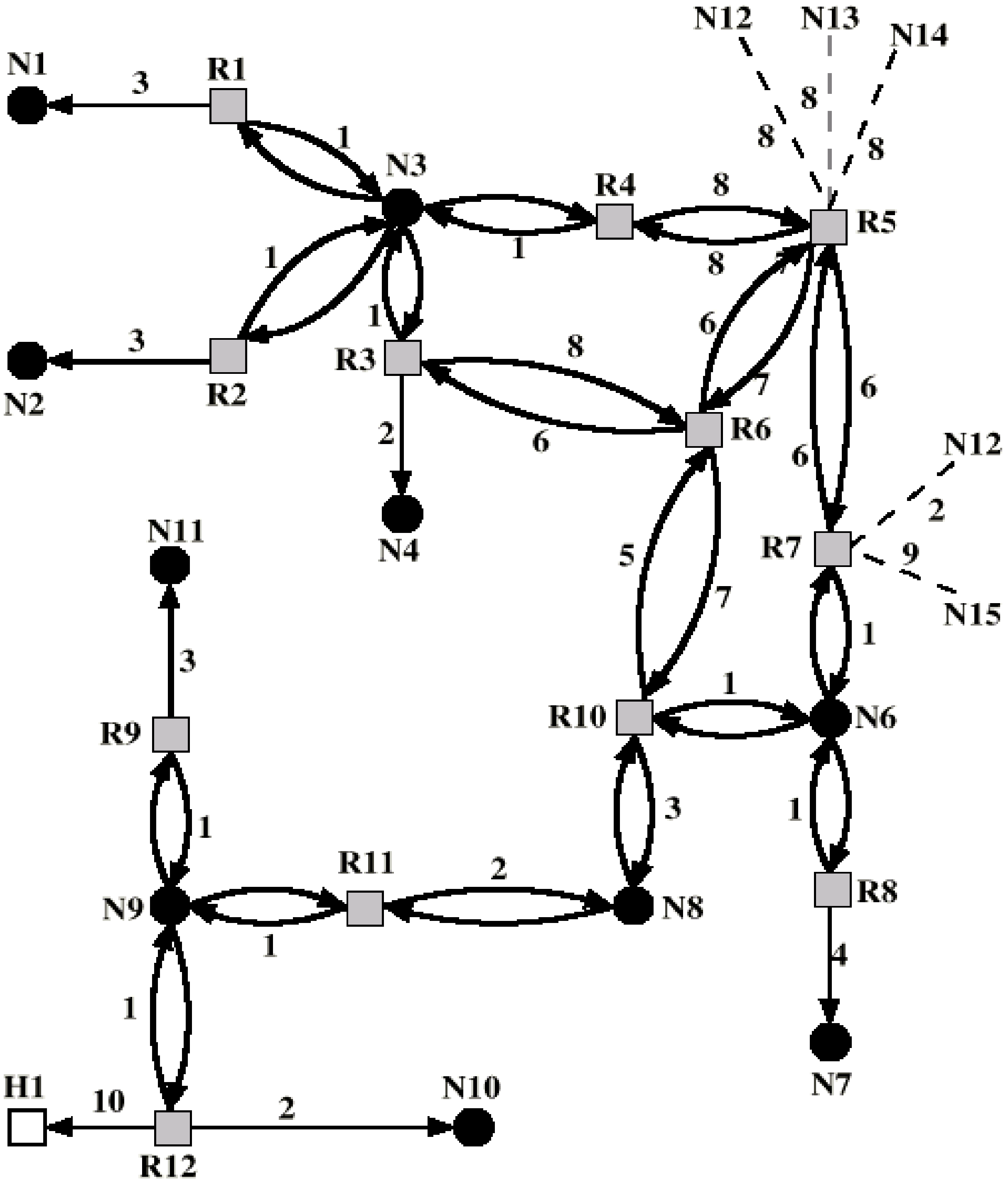
OSPF Operation

Dijkstra's algorithm used to find least cost path to all other networks

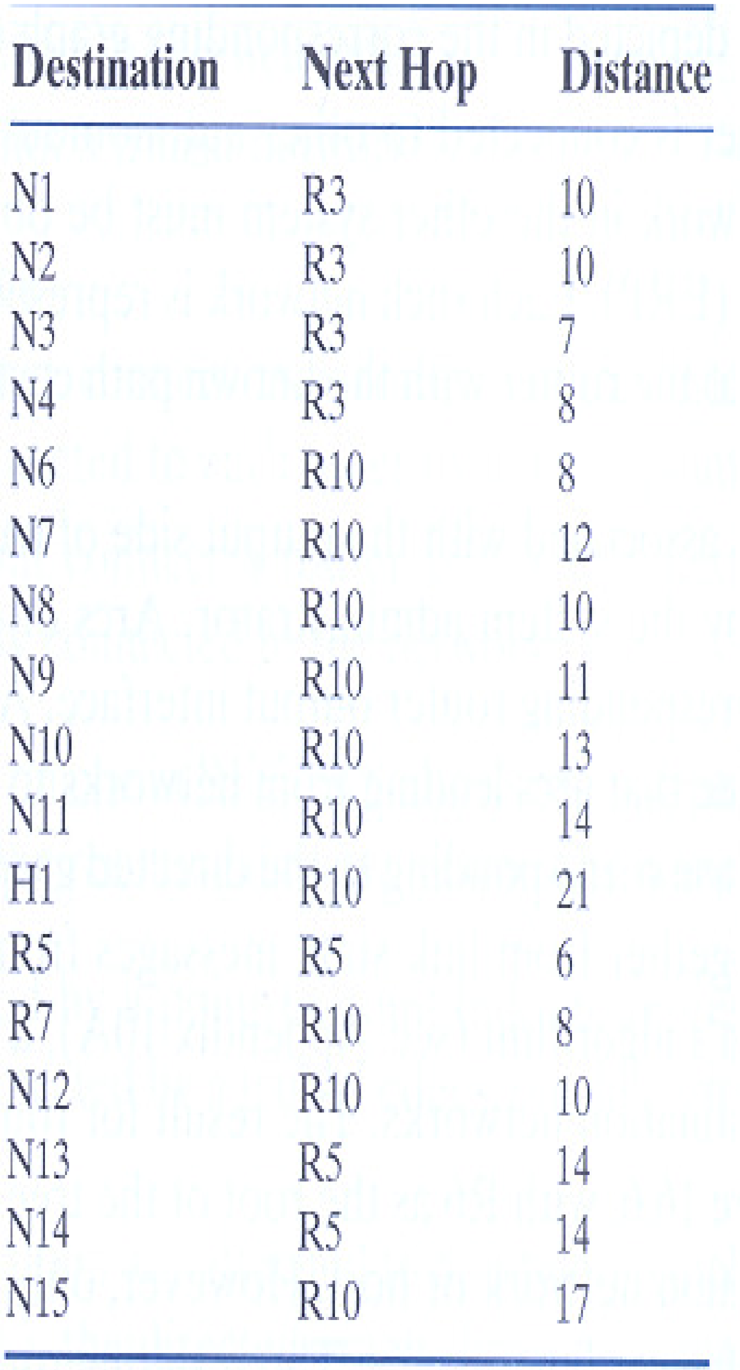
Next hop used in routing packets

Each router will find the whole extended network map (huge database =>

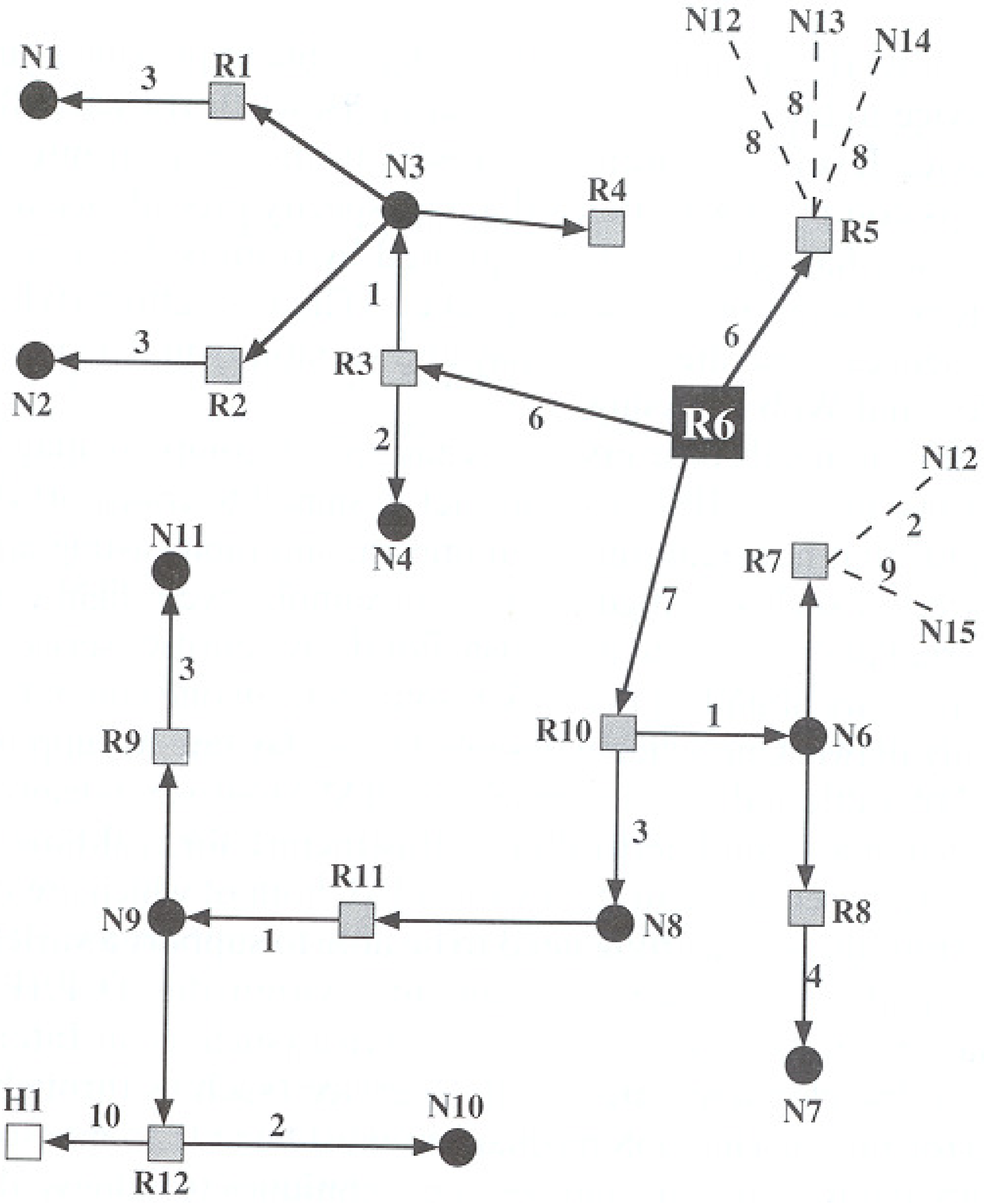
maintenance & update techniques)



Directed Graph for AS



Destination	Next Hop	Distance
N1	R3	10
N2	R3	10
N3	R3	7
N4	R3	8
N6	R10	8
N7	R10	12
N8	R10	10
N9	R10	11
N10	R10	13
N11	R10	14
H1	R10	21
R5	R5	6
R7	R10	8
N12	R10	10
N13	R5	14
N14	R5	14
N15	R10	17



SPF tree & routing table for router 6

Border Gateway Protocol (BGP)

For use with TCP/IP internets;

Preferred EGP of the Internet; follows first EGP implementation

Prevent routing loops in arbitrary topologies; allows policy-based route selection

BGP Routing Information Exchange

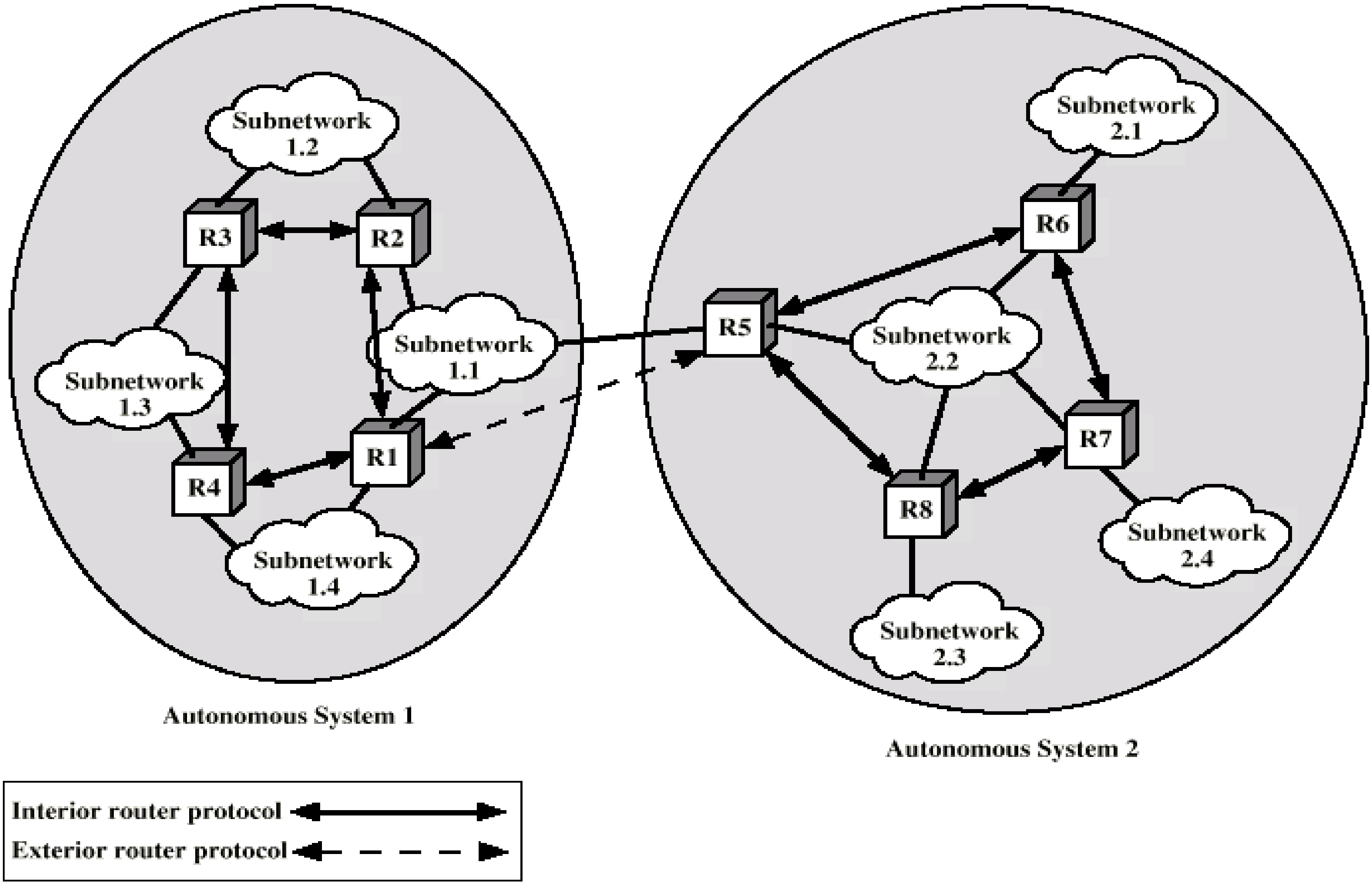
Within AS, router builds topology picture using some IGP

Router issues *Update* message to other routers outside AS using BGP

These routers exchange info with other routers in other AS (over TCP connections)

Routers must then decide the best routes

Sample example with 2 ASs



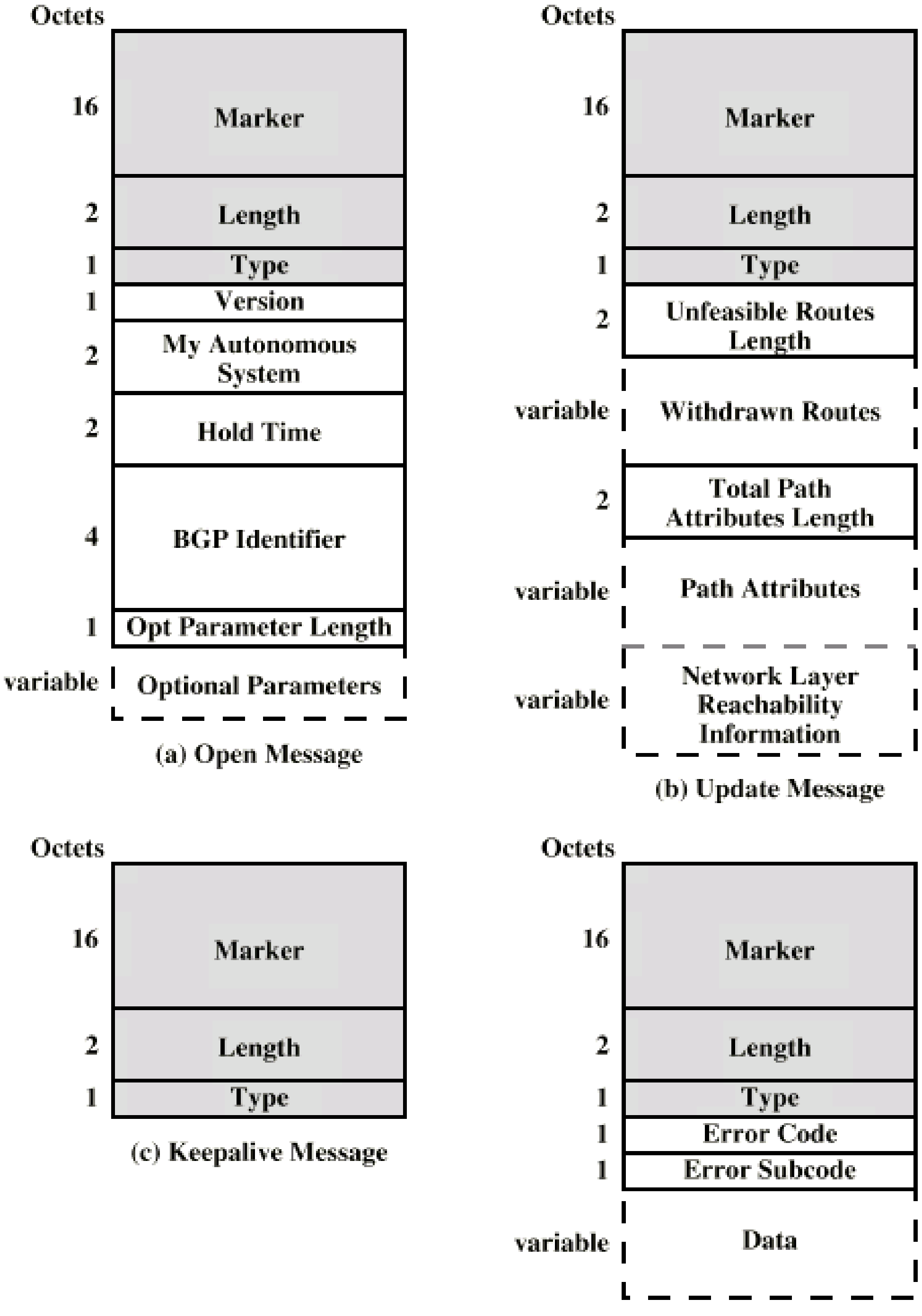
BGP-4 Messages sent over TCP connections:

Open – open relationship between routers

Update –information about a router or multiple routes

Keep alive – ACK for *Open* or periodic confirmation for relationship

Notification – error condition detected



Octets
16 Marker
2 Length
1 Type
1 Version
2 My Autonomous System
2 Hold Time
4 BGP Identifier
1 Opt Parameter Length
variable Optional Parameters

(a) Open Message

Octets
16 Marker
2 Length
1 Type
2 Unfeasible Routes Length
variable Withdrawn Routes
2 Total Path Attributes Length
variable Path Attributes
variable Network Layer Reachability Information

(b) Update Message

Octets
16 Marker
2 Length
1 Type

(c) Keepalive Message

Octets
16 Marker
2 Length
1 Type
1 Error Code
1 Error Subcode
variable Data

(d) Notification Message

Two routers are **neighbors** if they are attached to same network; if in different AS and intend to exchange info, need for procedures:

Functional Procedures

Neighbor acquisition – request for change of info, and ACK or NACK response; use of *Open* & *Keepalive* messages

Neighbor reachability – relationship maintenance; use of periodic *Keepalive* messages

Network reachability – routers maintain a database with networks can reach; periodic updates of changes with *Update* messages

A few more detailed: to establish a neighbor relationship, a router must:

Open a TCP connection to the router of interest

Send *Open* message, with both addresses

Includes proposed *Hold time* value (interval between successive maintenance messages – *Keepalive* & *Update*)

Receiver selects minimum of its Hold time and that sent by source of *Open* message

BGP Message Types

Keep Alive

To tell other routers that this router is still there

Update

Info about single routes through internet; info available for being added to each router database

List of routes previously advertised by this router and now being withdrawn

Includes *path attributes* info

Origin (information generated by a IGP or EGP)

AS_Path (list of AS traversed)

Next_hop (IP address of used border router)

Multi_Exit_Disc (Info about routers internal to AS)

Local_pref (Inform other routers within AS about preference for a route)

Atomic_Aggregate, Aggregator (Route Aggregation: Uses address tree structure to reduce amount of info needed)

Uses of AS Path and Next Hop

- *AS_Path*
  - Enables routing policy
    - Avoid a particular AS
    - Security
    - Performance
    - Quality
    - Number of AS crossed
- *Next_Hop*
  - IP address of the used border router
  - Only a few routers within an AS implement BGP
    - Responsible for informing outside routers of routes to other networks in AS

Network Layer Reachability Information (NLRI) field – list of all networks within AS

Notification message: error reporting

Message header error

  Authentication and syntax

Open message error

  Syntax and option not recognized

  Unacceptable hold time

Update message error

  Syntax and validity errors

Hold time expired

  Connection is closed

Finite state machine error

Cease

  Used to close a connection when there is no error

Historically, IP-based internets provided **best-effort** delivery services for applications, e.g. all datagrams equally treated, no service levels, no reservations, no guaranties

Changes in traffic demands require variety of quality of service (QoS)

Today: Internet phone, multimedia, multicast transmissions => traffic variety

ATM first supported TCP (UDP) traffic alongside real-time traffic; building new ATM infrastructure quite expensive (why ATM to desktop, if there is IP?)

Need for improving IP, allowing new type of services!

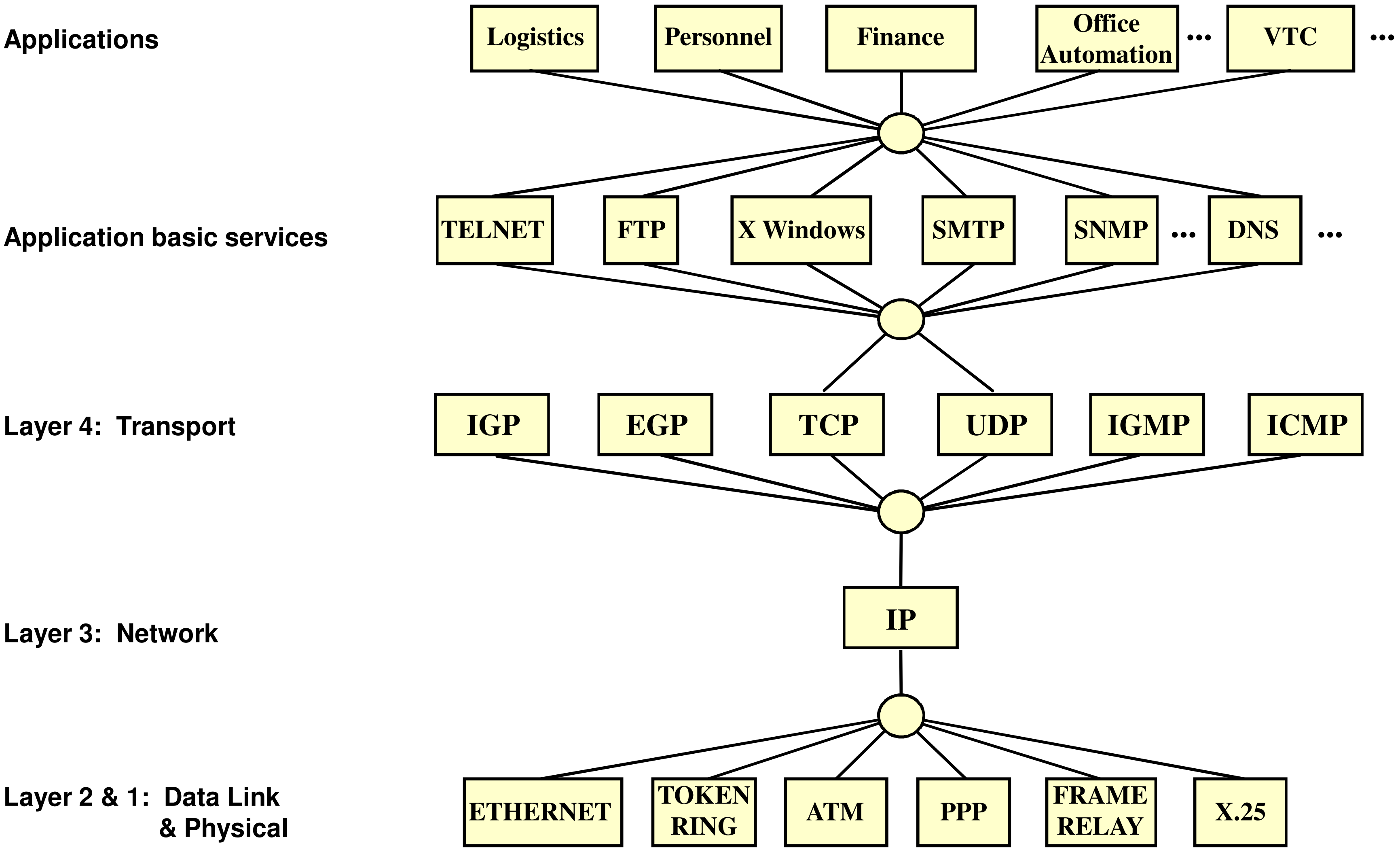
QoS mechanism implies translation of a request for service (with defined parameters for quality) into a set of traffic characteristics (throughput, delay, jitter, error rate …), being able to measure and maintain them. Changes in IP network infrastructure:

New functionality required in routers, new routing strategies

New means of requesting QoS to the internets, obtaining necessary network resources

ISA defined by RFC 1633, for allowing QoS transport over Ip-based internets

Today assertion: **Everything over IP & IP over Everything**



Applications: Logistics, Personnel, Finance, Office Automation ... VTC ...

Application basic services: TELNET, FTP, X Windows, SMTP, SNMP ... DNS ...

Layer 4: Transport: IGP, EGP, TCP, UDP, IGMP, ICMP

Layer 3: Network: IP

Layer 2 & 1: Data Link & Physical: ETHERNET, TOKEN RING, ATM, PPP, FRAME RELAY, X.25

Internet Traffic

Elastic

Can cope (adjust) with wide changes in internet delay and/or throughput; still ok for application run; examples of ‘elastic’ TCP applications, running well on TCP/IP, but differing in requirements:

FTP sensitive to throughput, delay proportional with the file size

E-Mail insensitive to delay

Network Management sensitive to delay in times of heavy congestion

Web access quite sensitive to delay

Inelastic

Does not easily adapt to variations

e.g. real time traffic

Do not react properly (do not reduce demand) facing congestion

Requirements for Inelastic Traffic

Throughput (a minimum throughput requested)

Delay (delay sensitive applications, stock trading, on line transactions)

Jitter (Delay variation): videoconferences request a reasonable jitter upper bound

Packet loss: real time applications vary in the amount of packet loss they can sustain

Implications on IP based networks:

Requirement for preferential treatment of certain types of traffic

Requirement for elastic traffic to be supported as well, not being crowded off the internet, due to the supplied high load from inelastic applications

Quality of Service in Computer Networks

Necessity

- Different traffic types: elastic, inelastic
- User requirements
- Original Internet: best effort type, not guarranteed services

[IETF] QoS defined as ability to segment traffic or to differentiate between types of traffic, any network treating specifically any traffic flow

[RFC 2386] QoS represents a set of requirements for services any network must fulfill when transporting the data flow

QoS parameters:

- loss rate
- delay
 delay variance (jitter)
- bandwidth
- network availability

Frameworks for QoS implementation

- Integrated Services Architecture (ISA, IntServ))

Resource allocation for fulfilling the applications requirements (real time applications especially)

Resources are allocated for every flow, in explicit manner: RSVP (Resource Reservation Setup Protocol) - protocol setting the resouces allocation

Drawback: lack of scalability

- Differentiated Services Architecture (DiffServ)

Simpler architecture, providing more service levels

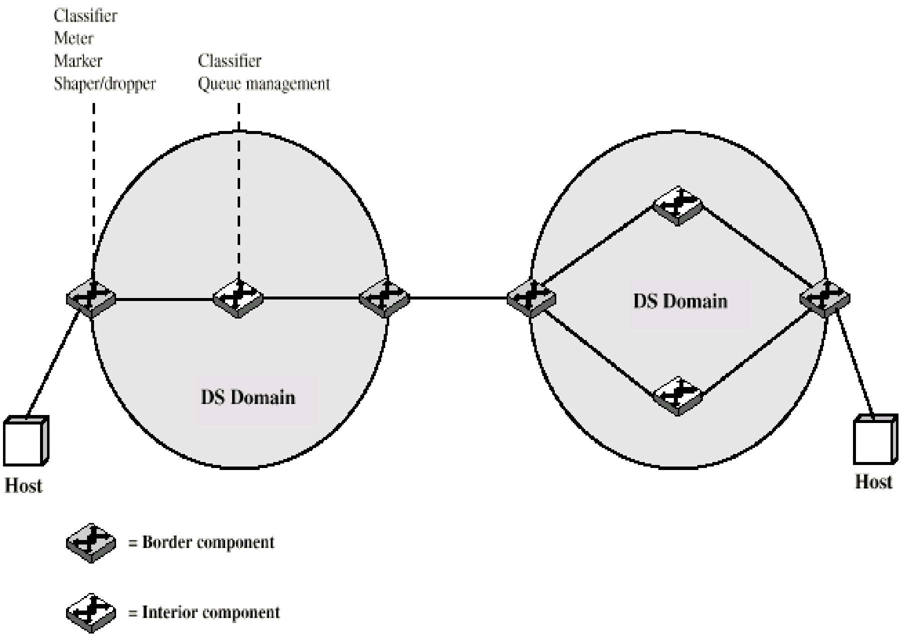
Traffic divided in classes (forwarding classes)

Resource allocation based on classes

Classes represent predefined forwarding hop behavior)

DS domains, with **border routers** and **interior routers**

Drawback: not enough admission control, to guarantee end to end QoS

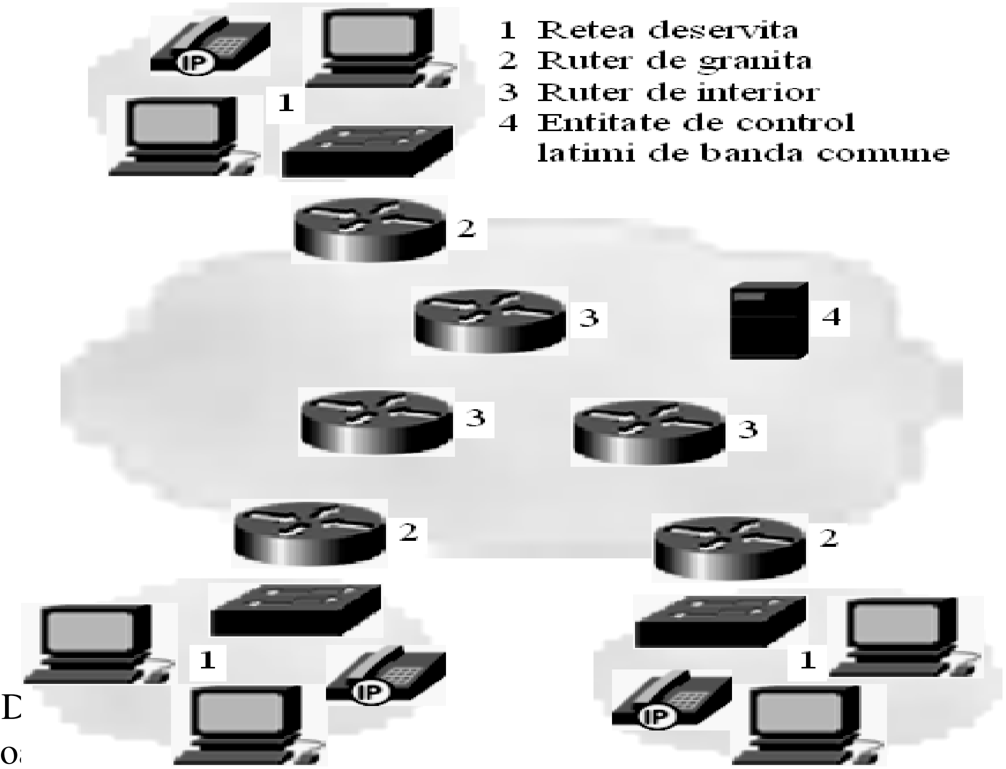


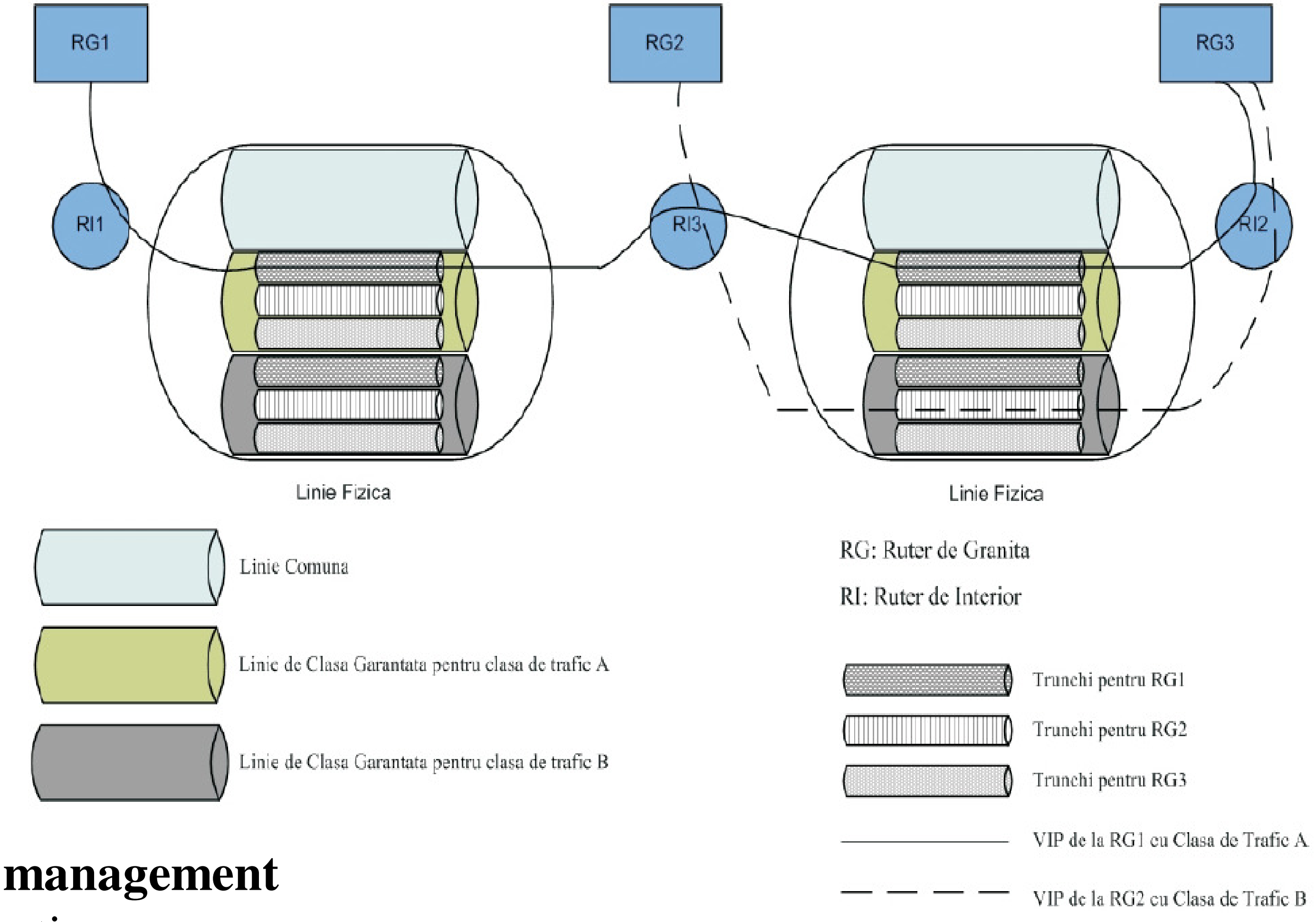
- End-to-End QoS Framework with Self-Adaptive Bandwidth Reconfiguration (SAR)

Edge router **–** per flow admission control, end to end bandwidth reservation, dynamic bandwidth reconfiguration, mapping of flows to traffic classes

Interior (core) router – traffic class differentiation, traffic class interpretation

Bandwidth control entity – monitoring, updating of common bandwidths, control of extra bandwidth requirements




RG1
RG2
RG3
RI1
RI3
RI2
Linie Fizica
Linie Fizica
Linie Comuna
Linie de Clasa Garantata pentru clasa de trafic A
Linie de Clasa Garantata pentru clasa de trafic B
RG: Ruter de Granita
RI: Ruter de Interior
Trunchi pentru RG1
Trunchi pentru RG2
Trunchi pentru RG3
VIP de la RG1 cu Clasa de Trafic A
VIP de la RG2 cu Clasa de Trafic B

SAR – Bandwidth management

Hierarchical organization

Guaranteed Line (LG) – minimum bandwidth for any class and trunck

LG devided in more Lines of Guaranteed Class (LCG)

Each LCG is reserved to a traffic class
LCG is further divided in trunks
Each trunk is dedicated to an edge router

Common Line (LC)

Offer a common bandwidth may be used by any trunk (a kind of special reserve)

Any edge router watches its available bandwidth available to assigned trunks and achieves the admission control

Trunks assigned bandwidth has a guaranteed minimal value, and using the Common Line, it may be adjusted depending on network traffic

Any trunk may get additional bandwidth, without condition from the available bandwidth for the class it belongs

Approaches: Centralized control, router assisted, edge to edge

Integrated Services Architecture

ISA Approach

Congestion controlled by

- Routing algorithms, minimizing routing delays
- Packet discard politics

ISA associates each IP packet with a flow (stream of IP packets, resulting from a single activity and requiring same QoS)

- Unidirectional
- Can be multicast

ISA functions for congestion management & QoS transport:

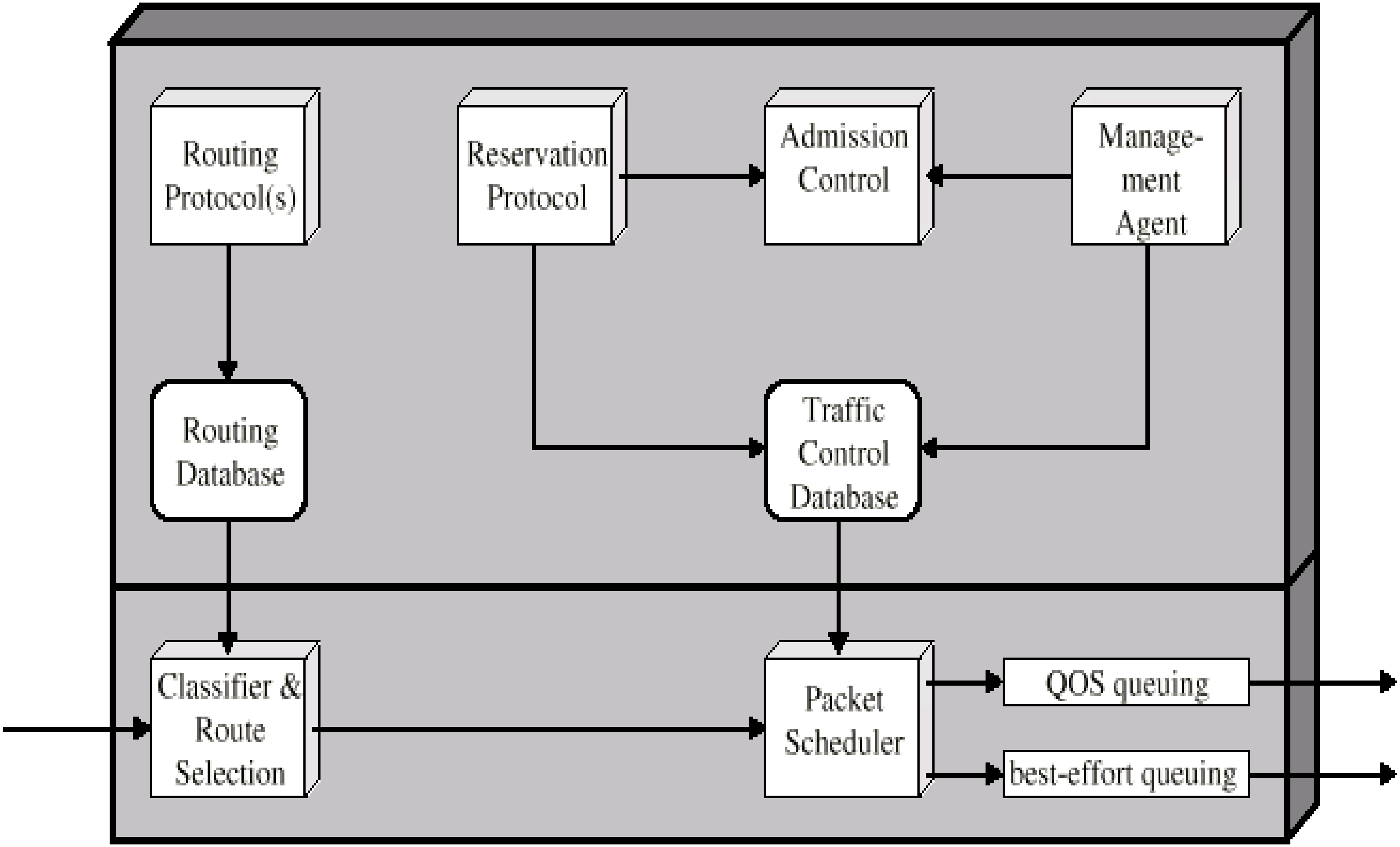
Admission Control

Routing Algorithm

Queuing discipline

Discard policy

ISA implemented in a router



Admission control: for QoS transport (other than best-effort), a reservation is needed for every new flow (use of RSVP); if reservation impossible, discard flow

Routing algorithm: decision made based on a variety of QoS parameters (delay, throughput, delay variance …); example OSPF

Queuing discipline: queuing policies for router interfaces, dealing with each flow requirements

Discard policy: discarding packets in router queues in such a way to meet QoS requirements and managing congestion

ISA Services

Guaranteed Service

- Provides assured data rate
- Upper bound on queuing delay through the network
- No queuing loss (no buffer overflow in routers)

Applicable to real time applications

Controlled load

Approximates behavior to that of applications receiving best effort service on unloaded network conditions

No specific upper bound on queuing delay

Very high delivery success (almost no queuing loss)

Useful for adaptive real time applications, no problems with congestion control

Best Effort

For backward compatibility

ISA uses: Token Bucket Traffic Specification

Token replenishment rate *R*

Continually sustainable data rate, for long terms

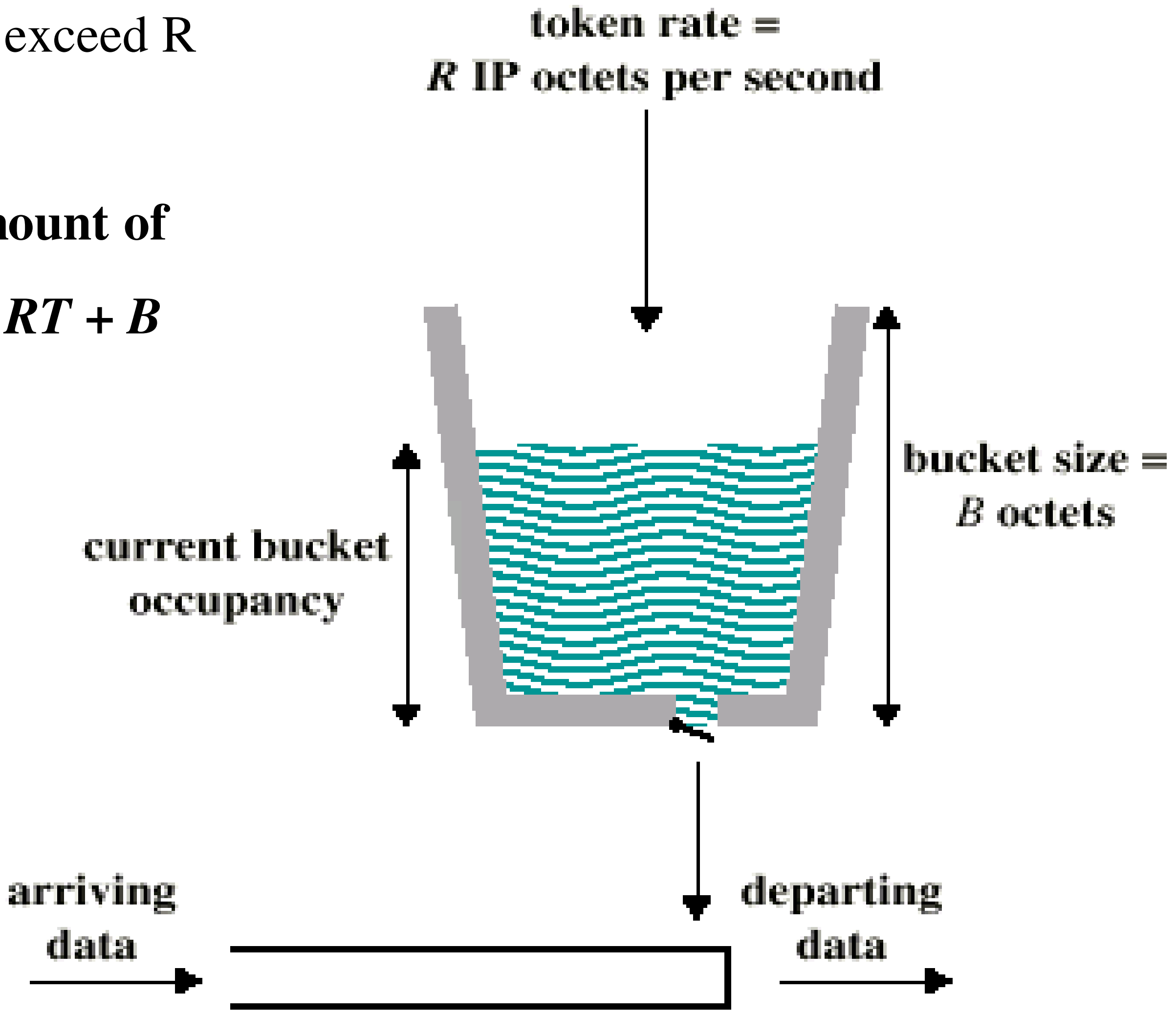
Bucket size *B*

Amount that data rate can exceed R

for short period

During time period *T* amount of

data sent can not exceed *RT* + *B*



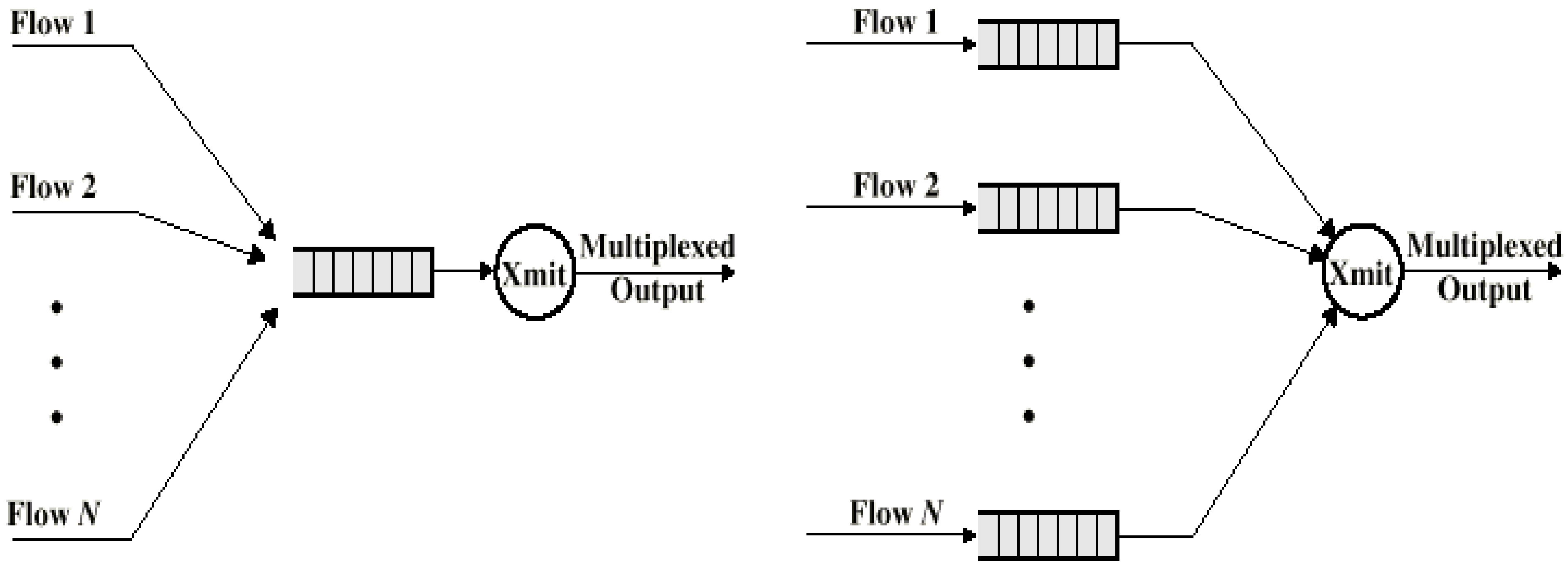
Queuing Discipline

Traditionally FIFO (First In First Out)

- No special treatment for high priority flow packets in the queue
- Large packet can hold up smaller packets (increased delay per packet)
- Greedy connection can crowd out less greedy connections

Fair queuing (overcomes FIFO drawbacks)

- Queue maintained at each output port
- Packet placed in queue for its flow
- Round robin servicing
- Skip empty queues
- Can have weighted fair queuing (WFQ)



(a) FIFO Queuing

(b) Fair Queuing

Resource Reservation Protocol (RSVP)

RFC 2205

Simplest case:

Unicast applications can reserve resources in routers to meet QoS

If router can not meet request, application informed

Multicast is more demanding

Traffic may be reduced

Some members of group may not require delivery from particular source over given time

e.g. selection of one from a number of possible “tuning channels”

Some group members may only be able to handle a portion of the transmission

e.g. from a video transmission with a basic component and an enhanced component

Internet resource reservation needs being dynamic, coping with network route changes

(not the ATM case – based on permanent connections)

Concept of Soft State

Set of state information in router that expires unless regularly refreshed from the entity that requested the state (e.g. a route change for a given transmission implies some soft states expire, so need for new resource reservation)

Applications must periodically renew reservation requests during transmission

RSVP Goals

Ability for heterogeneous receivers to make specific reservations

Deal gracefully with changes in multicast group membership

Specify resource requirements such that aggregate resources for a multicast group reflect requirements actually needed

Enable receivers to select one source from among multiple sources

Deal gracefully with changes in routes, automatically restoring the resource reservation along the new path

Control protocol overhead, aggregate RSVP messages for minimizing RSVP traffic

Independency of routing protocol; **RSVP is not a routing protocol!!!**

RSVP Characteristics

Makes reservations for both Unicast and Multicast transmissions

Makes reservations for unidirectional data flow – use a simplex algorithm

Receiver initiates and maintains reservation for a data flow (due to multicast specificity)

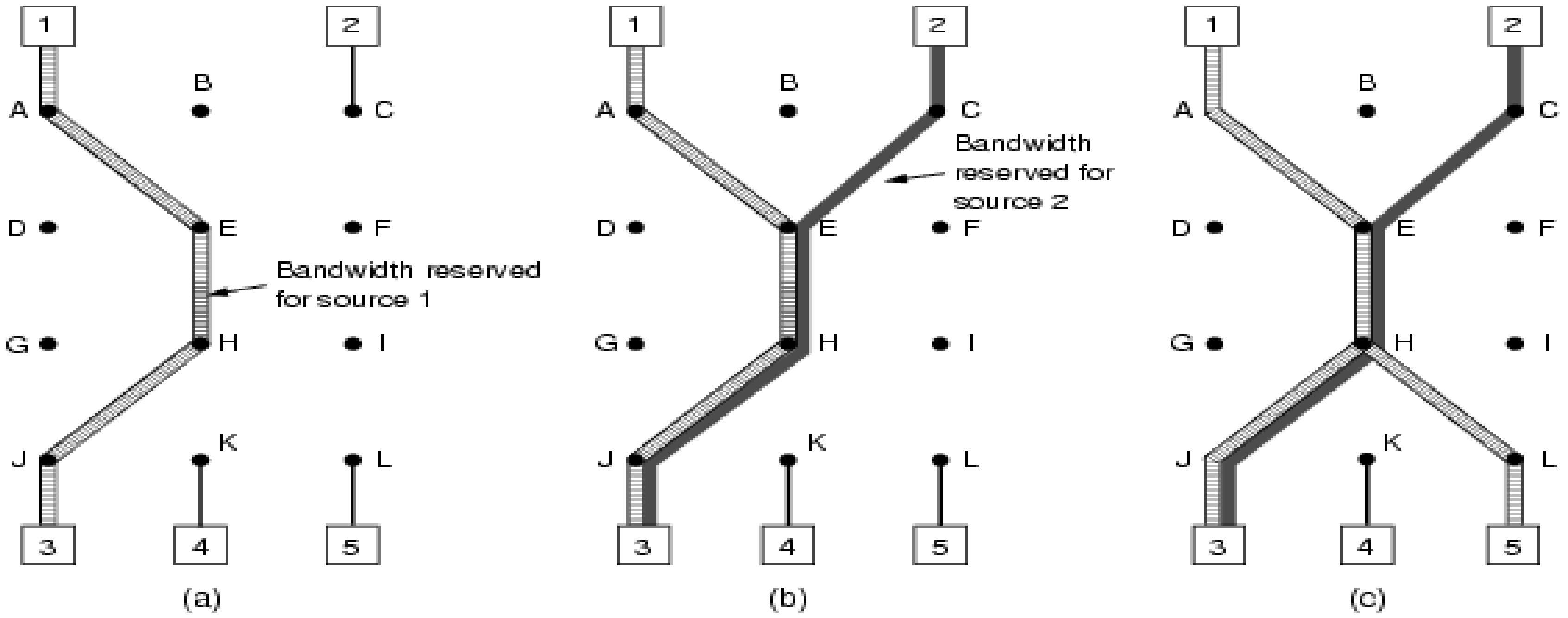
routers can aggregate multicast resource reservations, taking advantage of shared path segments along the distribution tree (see next figure)

Maintains soft state in the internet

Provide different reservation styles, aggregating these => a more efficient resource use

Transparent operation through non-RSVP routers (through ‘best effort’ routers)

Support for IPv4 and IPv6


1
2
B
A
C
D
E
F
Bandwidth reserved for source 1
G
H
I
J
K
L
3
4
5
(a)
Bandwidth reserved for source 2
(b)
(c)

(a) Host 3 requests a channel to host 1. (b) Host 3 then requests a second channel, to host 2. (c) Host 5 requests a channel to host 1.

Data Flow Concepts for RSVP

Session

Data flow identified by its destination; once reservation made at a router by the data flow destination, router consider this a session

Flow descriptor

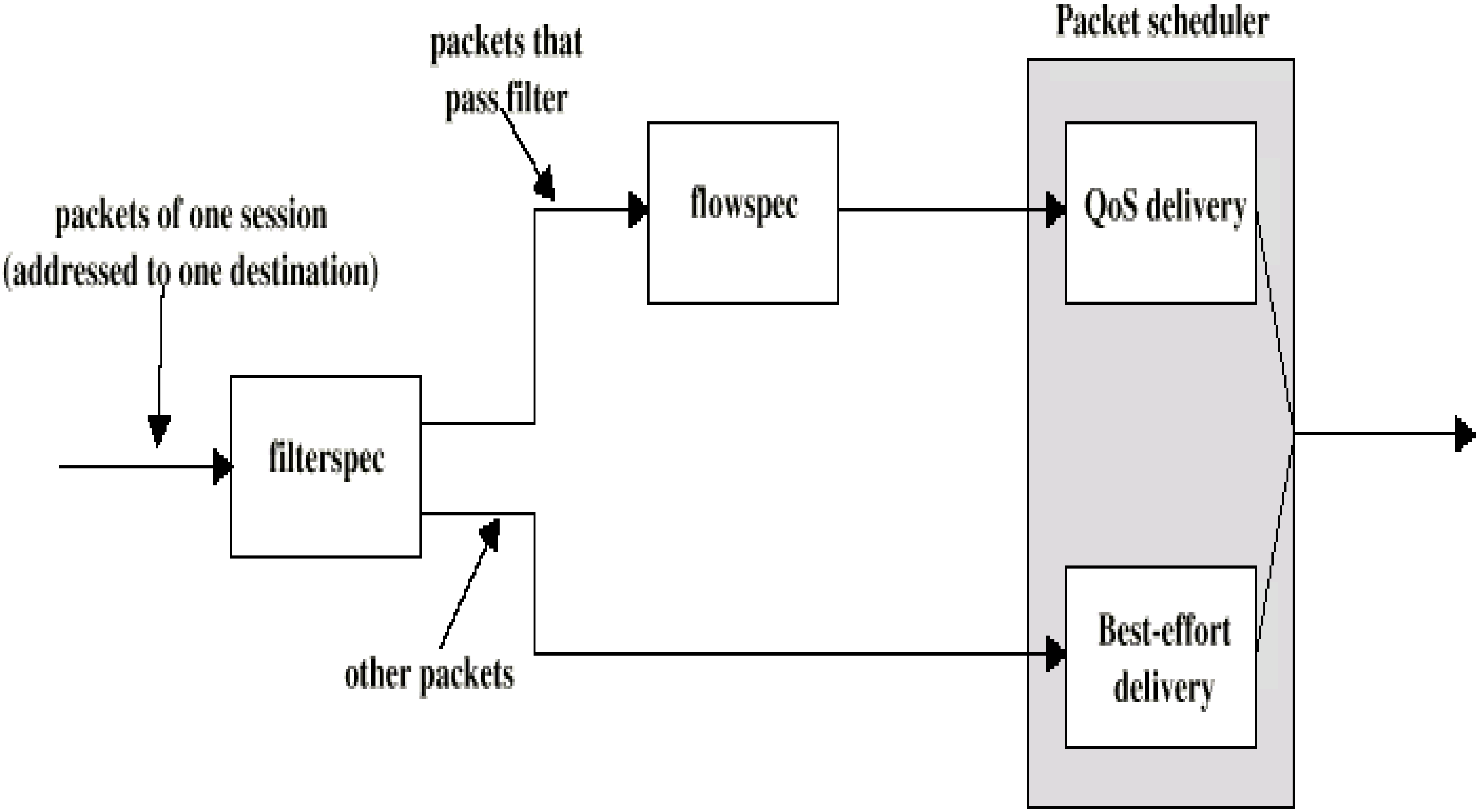
Denotes the reservation request issued by destination

Made up (consist) of flowspec and filterspec

Flowspec gives required QoS

Filterspec defines set of packets for which reservation is required

See next slide


Packet scheduler
packets that
pass filter
packets of one session
(addressed to one destination)
flowspec
QoS delivery
filterspec
other packets
Best-effort
delivery

RSVP Message Types (protocol mechanisms)

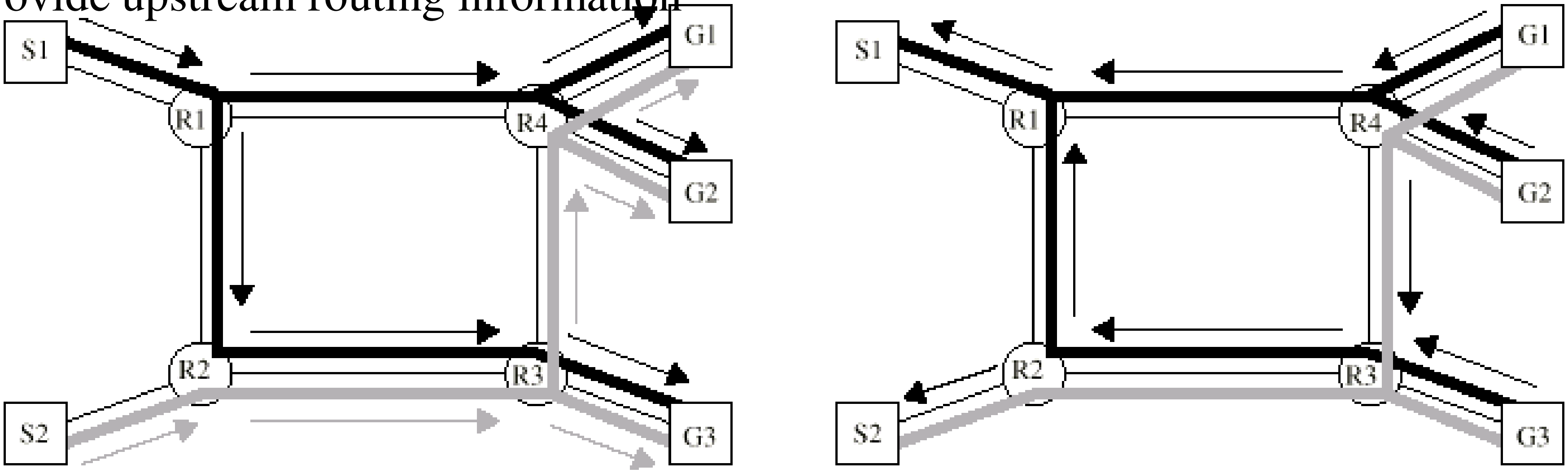
Two basic message types:

Resv

- Originate at multicast receivers
- Propagate upstream through the distribution tree
- Create soft states within routers
- Reach sending host enabling it to set up traffic control for first hop

Path

- Provide upstream routing information



(a) Data distrubution to a multicast group

(b) Merged Resv Messages

Operation From Host Perspective

Receiver joins multicast group (IGMP *join* message)

Potential sender issues Path message

Receiver gets message identifying the sender

Receiver has reverse path info and may start sending Resv messages

Resv messages propagate through internet and is delivered to sender

Sender starts transmitting data packets

Receiver starts receiving data packets

Differentiated Services (DS)

ISA + RSVP allow QoS traffic over IP, but add a lot of control signaling + extra state management into routers (complex task to implement)

DS provide simple, easy to implement, low overhead tool **to support range of network services, differentiated on basis of performance** (different QoS for different traffic flows)

DS architecture characteristics:

IP Packets labeled for differing QoS treatment (**DS octet**) using existing IPv4 *Type of Service* or IPv6 *Traffic class* (one octet length fields)

Service level agreement (SLA) is established between provider and customer, prior to use of DS (separately from application level)

Provides a built-in aggregation mechanism

Good scaling to larger networks and loads

Multiple voice connections are handled not individually, but in aggregate

DS implemented within routers by queuing and forwarding packets based on DS octet, so no extra state info on packet flows stored

DS Services

Defined within DS domain

- Contiguous portion of internet over which consistent set of DS policies are administered
- Typically under control of one organization
- Defined by service level agreements (SLA)

SLA Parameters are:

Detailed service performance

- Expected throughput
- Drop probability
- Latency

Constraints on ingress and egress points at which the service is provided

Traffic profiles, e.g. token bucket parameters for that service

Disposition of traffic submitted in excess of profile

Example of Services

Level A - low latency delivery

Level B - low loss delivery

Level C - 90% of traffic will experience < 50ms latency

Level D - 95% in profile traffic delivered

Packets are labeled using DS octet

DS Octet contains DS Codepoint:

Leftmost 6 bits of DS octet used for DS codepoints (gives packets class for DS):

Actually 3 pools of code points

xxxxx0 assignment as standards (all 0's means default class – e.g. best effort)

xxxx11 experimental or local use

xxxx01 experimental or local but may be allocated for standards in future

DS Codepoint contains *Class* & *Drop Precedence* sub-fields

DS Octet – compatibility with IP’s *Type of Service* field (*Drop Precedence* sub-field)

Drop Precedence defines priority associated with IP packet (local resource allocation in router)

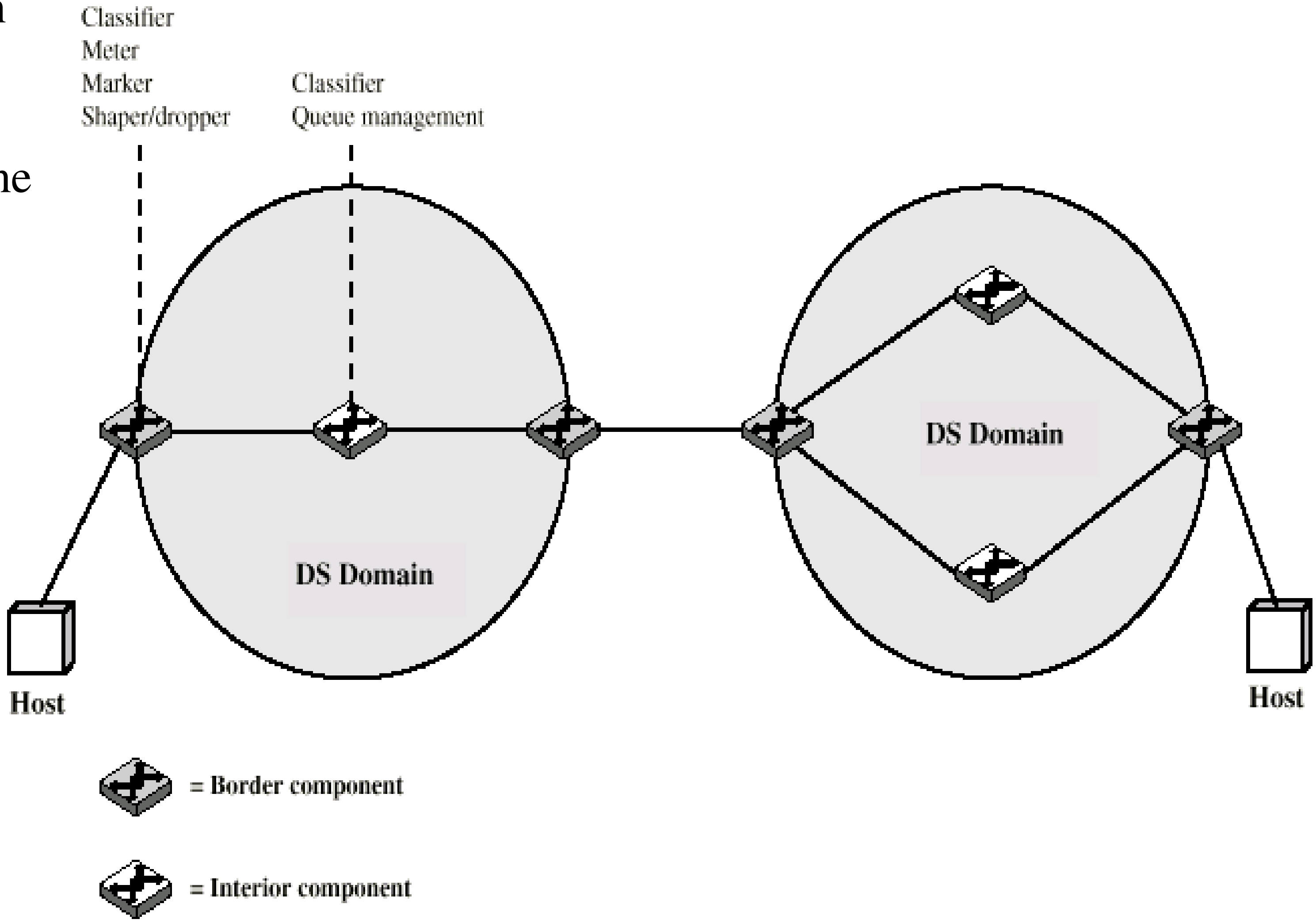
Router in a DS domain will treat packet using one possible approach, based on:

Routing selection

Network service

Queuing discipline

DS Domains



DS Configuration and Operation

Within DS domain, interpretation of DS codepoints is uniform

Routers in DS domain are boundary (border) nodes or interior nodes

Traffic conditioning functions:

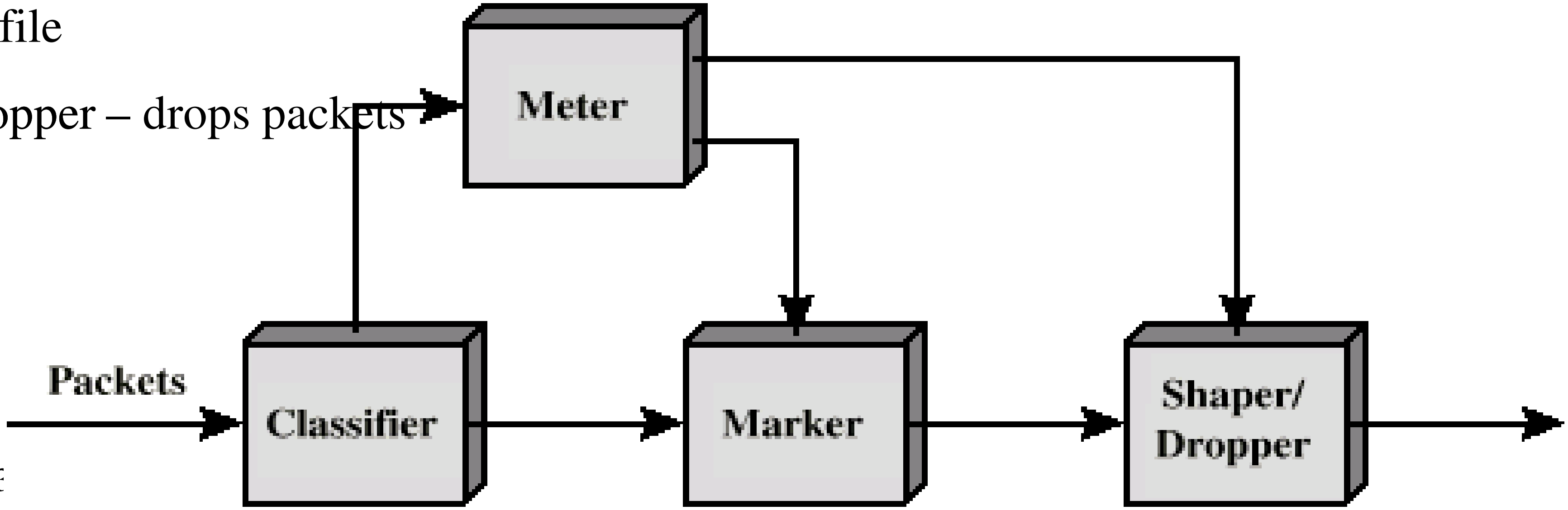
Classifier of IP packets in DS classes based on DS codepoints

Meter – measures traffic for conformance with the profile

Marker – re-marking packets to accommodate the new profile (packets exceeding a throughput for a guaranteed rate may be re-marked for best-effort)

Shaper – traffic shaping for not exceeding traffic rate specified in that class profile

Dropper – drops packets



DS Traffic Conditioner

DS Specifications refer to the forwarding treatment provided at router as per-hop-behavior PHB

PHB available at all DS domain routers

PHB types:

Expedited Forwarding PHB

Allows Premium Service; based on two parts:

- traffic aggregate (flow of packets with particular service for a specific user) has a well-defined minimum departure rate

-policing & shaping the aggregate arrival flow for being less than min. departure rate for every router

Assured Forwarding PHB

Service superior to best-effort, without using resource reservation or discriminations among flows from different users

- four Assured Forwarding classes (traffic profiles) are defined

-user may select a AF class for fulfilling application requirements

-within each class, packets are marked with a drop precedence value (is preferable to discard packets with a higher drop precedence value)