Routing Protocols

Router

A router is a device that determines the next network point to which a packet should be forwarded toward its destination

Allow different networks to communicate with each other

A router creates and maintain a table of the available routes and their conditions and uses this information to determine the best route for a given packet.

A packet will travel through a number of network points with routers before arriving at its destination.

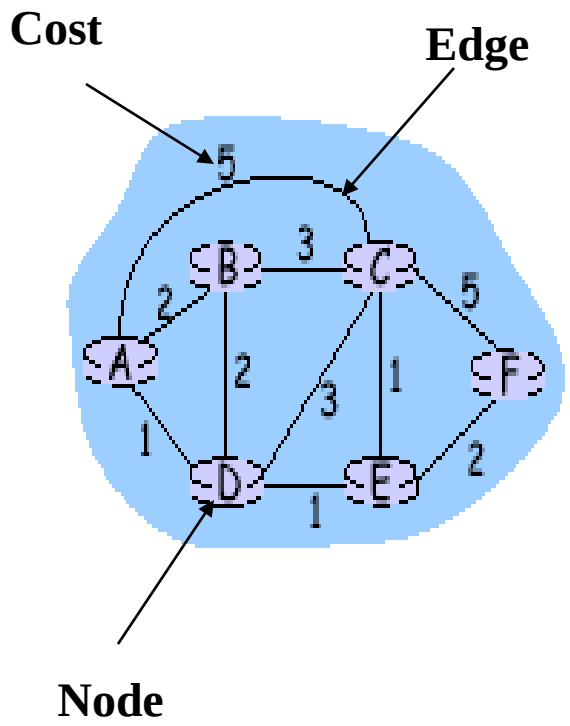
There can be multiple routes defined. The route with a lower weight/metric will be tried first.

Routing (IP routing)

- Routing Protocol: determines the **best path** (route) that the packets should follow to arrive to the desired destination
- Routing Protocols: A **software** in the network layer that implements **routing algorithms** and responsible for:
  - Filling and updating routing tables (by finding the shortest paths from each source to each destination) This part is called **Routing**
  - Deciding which output interface an incoming packet should be transmitted on (by referring to the routing table). This part is called **Forwarding**

Graph representation of a network

- Graph **nodes** are **routers**
- Graph **edges** are **physical links**
  - Each link has a value which represents the "cost" of sending a packet across the link
  - The **cost** is assigned based on a **metric**
  - Cost metric can be:
    - Number of networks (**hops or routers**)
    - Geographic distance
    - Link delay
    - Capacity (speed)
    - Reliability
    - Combination of the above
- How to select a "good" path???
  - Good path is the one with **minimum cost** = $\sum$ Total cost from src to dest



Routing Protocols

Static Routing

- Routes change **slowly** over time
- Shortest paths are pre-computed offline by a special computer running the routing algorithm
- Resulted information is entered manually by the administrator into the routing tables
- **Can not** update automatically if there is a change in the network or failure
- Used in **small** networks

Dynamic Routing

- Each router or host learns the state of the network by communicating with its neighbors.
- Based on the collected information, each node can fill its routing table
- More complexity is added to the router

- Networks typically use a combination of both static and dynamic routing.

Static Routing

- Static routing has several primary uses:
- Providing ease of routing table maintenance in smaller networks that are not expected to grow significantly.
- Routing to and from a stub network. A network with only one default route out and no knowledge of any remote networks.
- Accessing a single default router. This is used to represent a path to any network that does not have a match in the routing table.

Static Routing Advantages and Disadvantages

Advantages	Disadvantages
Easy to implement in a small network.	Suitable only for simple topologies or for special purposes such as a default static route. Configuration complexity increases dramatically as network grows.
Very secure. No advertisements are sent as compared to dynamic routing protocols.	
Route to destination is always the same.	Manual intervention required to re-route traffic.
No routing algorithm or update mechanism required; therefore, extra resources (CPU or RAM) are not required.	

Dynamic Routing

The Evolution of Dynamic Routing Protocols

- Dynamic routing protocols used in networks since the late 1980s
- Newer versions support the communication based on IPv6

- Why *Dynamic Routing Protocols*?
  - Each router acts independently, based on information in its router forwarding table
  - Dynamic routing protocols allow routers to share information in their router forwarding tables

Purpose of Dynamic Routing Protocols

Routing Protocols are used to facilitate the exchange of routing information between routers.

The purpose of dynamic routing protocols includes:

- Discovery of remote networks
- Maintaining up-to-date routing information
- Choosing the best path to destination networks
- Ability to find a new best path if the current path is no longer available

Main components of dynamic routing protocols include:

- **Data structures -** Routing protocols typically use tables or databases for its operations. This information is kept in RAM.
- **Routing protocol messages -** Routing protocols use various types of messages to discover neighboring routers, exchange routing information, and other tasks to learn and maintain accurate information about the network.
- **Algorithm -** Routing protocols use algorithms for facilitating routing information for best path determination.

Dynamic Routing Advantages and Disadvantages

Advantages	Disadvantages
Suitable in all topologies where multiple routers are required.	Can be more complex to implement.
Generally independent of the network size.	Less secure. Additional configuration settings are required to secure.
Automatically adapts topology to reroute traffic if possible.	Route depends on the current topology.
	Requires additional CPU, RAM, and link bandwidth.

Dynamic Routing Protocol Operation

In general, the operations of a dynamic routing protocol can be described as follows:

1.The router sends and receives routing messages on its interfaces.

2.The router shares routing messages and routing information with other routers that are using the same routing protocol.

3.Routers exchange routing information to learn about remote networks.

4.When a router detects a topology change the routing protocol can advertise this change to other routers.

How to reduce number of entries in the routing table?

- Network-Specific routing (Destination Network IP Address is listed in the table)
- Host Specific Routing (Destination Host IP Address is listed in the table)
- Default Routing

Route method versus next-hop method

a. Routing tables based on route

Destination	Route
Host B	R1, R2, host B

Routing table for host A

Destination	Route
Host B	R2, host B

Routing table for R1

Destination	Route
Host B	Host B

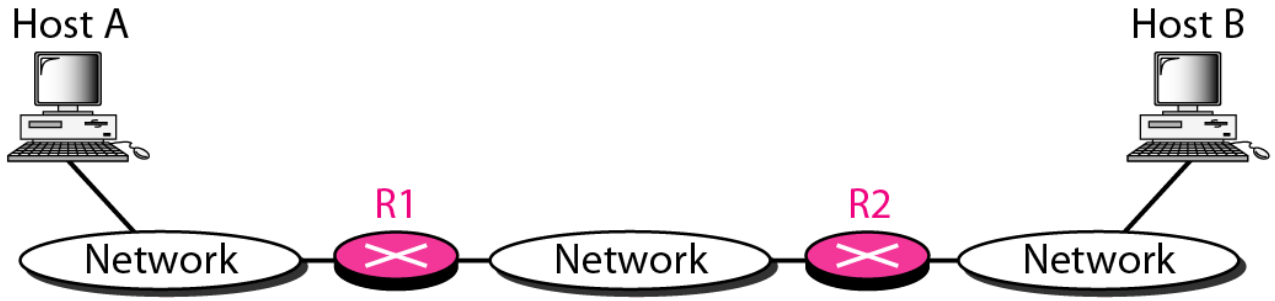
Routing table for R2

b. Routing tables based on next hop

Destination	Next hop
Host B	R1

Destination	Next hop
Host B	R2

Destination	Next hop
Host B	---



In next-hop routing, Routing table holds the information (IP address) that leads to the next hop (router) instead of holding information about the complete path

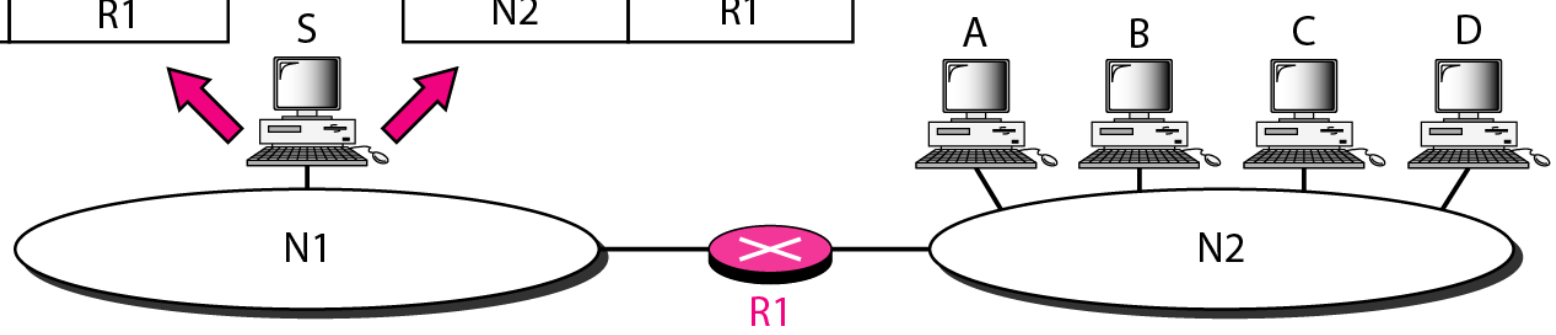
Host-specific versus network-specific method

Routing table for host S based on host-specific method

Destination	Next hop
A	R1
B	R1
C	R1
D	R1

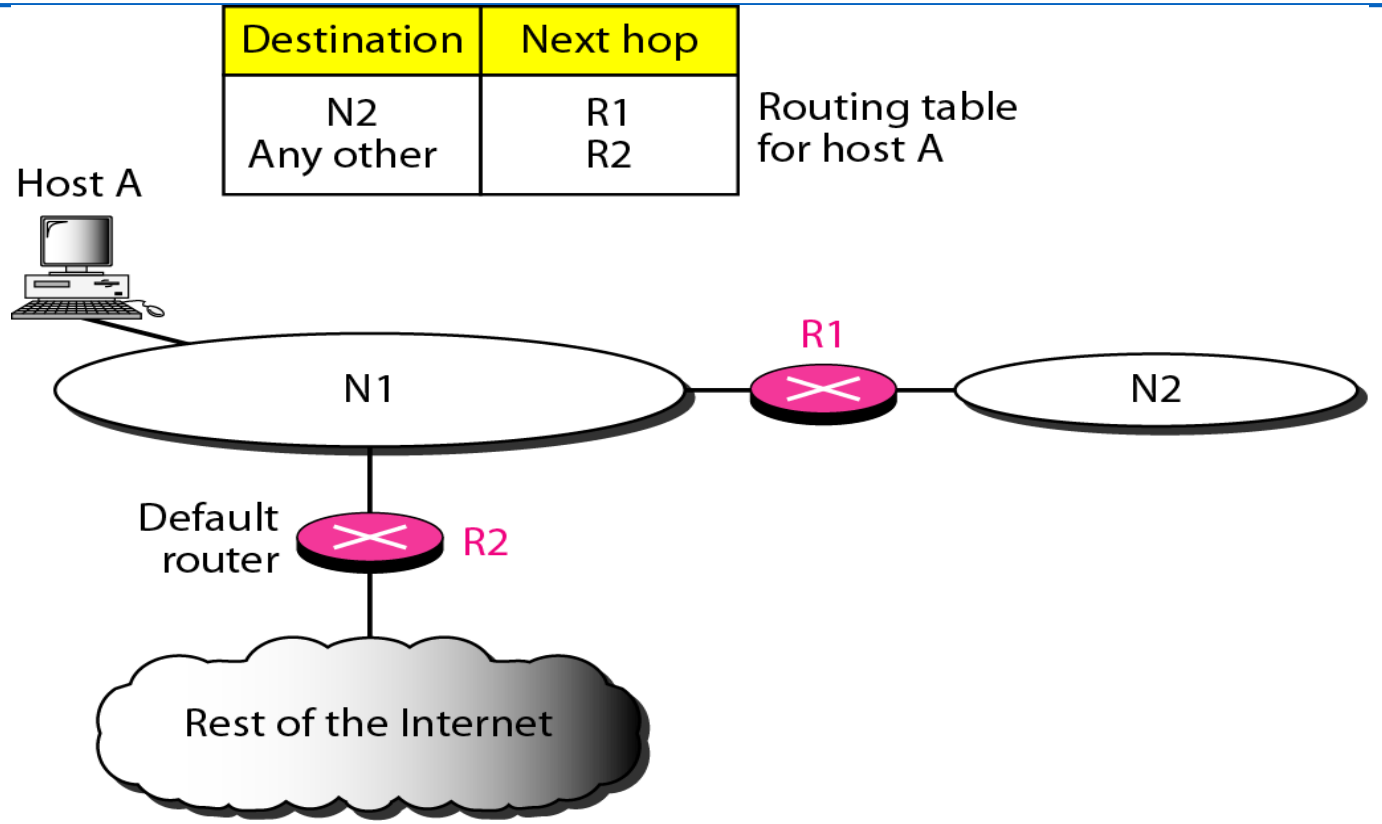
Routing table for host S based on network-specific method

Destination	Next hop
N2	R1

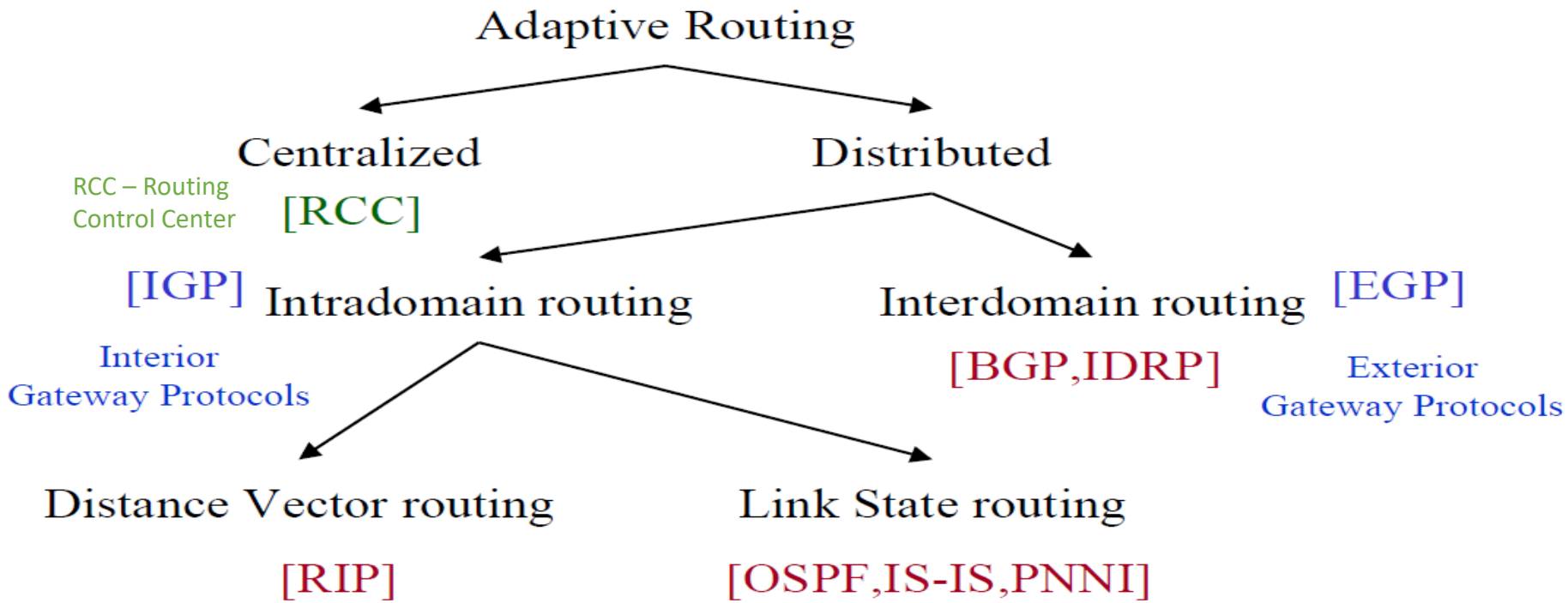


Instead of having entry for each host connected to the same network, the table contains only a single entry for the address of the network itself

Default method



Default router is used if the destination network address is not found in the routing table


Adaptive Routing
Centralized
Distributed
RCC – Routing Control Center
[RCC]
[IGP]
Intradomain routing
Interdomain routing
[EGP]
Interior Gateway Protocols
[BGP,IDRP]
Exterior Gateway Protocols
Distance Vector routing
Link State routing
[RIP]
[OSPF,IS-IS,PNNI]

Routing Protocols Classification

	Interior Gateway Protocols				Exterior Gateway Protocols
	Distance Vector		Link-State		Path Vector
IPv4	RIPv2	EIGRP	OSPFv2	IS-IS	BGP-4
IPv6	RIPng	EIGRP for IPv6	OSPFv3	IS-IS for IPv6	BGP-MP

IGP (Interior Gateway Protocol): Route data within an Autonomous System
RIP (Routing Information Protocol)
RIP-2 (RIP Version 2)
IGRP (Interior Gateway Routing Protocol)
EIGRP (Enhanced Interior Gateway Routing Protocol)
OSPF (Open Shortest Path First)
IS-IS (Intermediate System-Intermediate System)

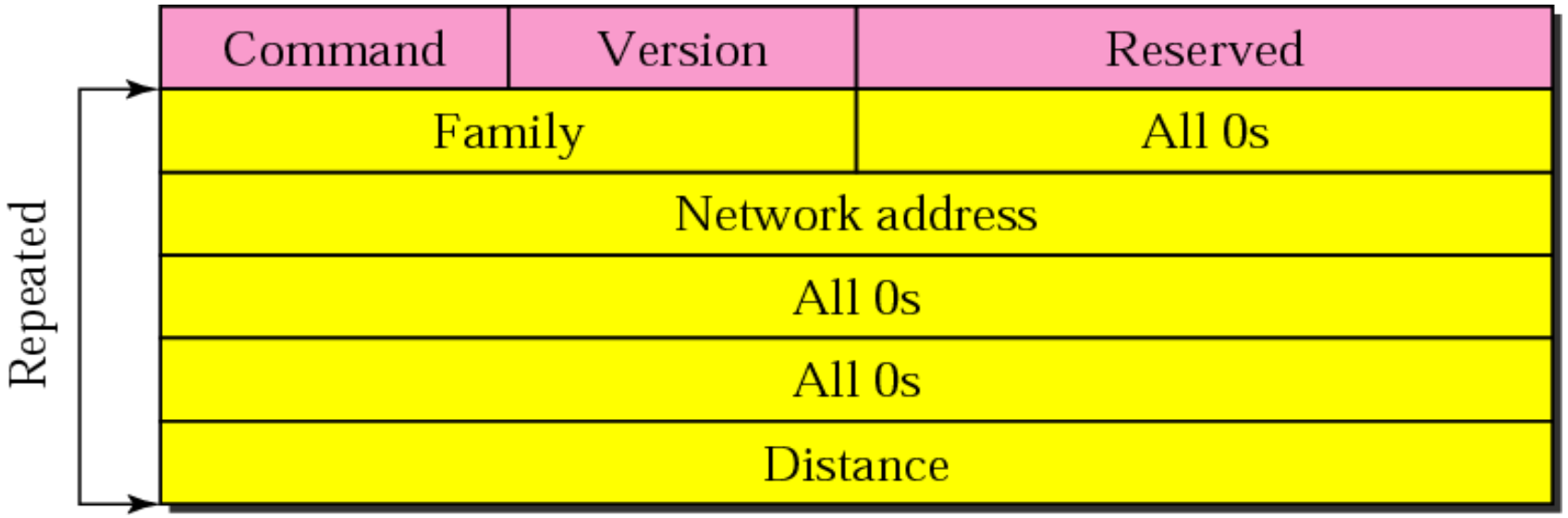
EGP (Exterior Gateway Protocol): Route data between Autonomous Systems

BGP (Border Gateway Protocol)

Routing Information Protocol (RIP)

- *Routing Information protocol (RIP)* is the simplest dynamic routing protocol
  - Each router broadcasts its entire routing table frequently
  - Broadcasting makes RIP unsuitable for large networks
- RIP is a *Distance Vector Protocol*
  - Learning Routing Information
  - *Slow Convergence*
- RIP is the simplest dynamic routing protocol
  - Broadcasts go to *hosts* as well as to routers
  - RIP interrupts hosts frequently, slowing them down; Unsuitable for large networks
- RIP is Limited
  - RIP routing table has a field to indicate the number of router *hops* to a distant host
  - The RIP maximum is 15 *hops*
  - Farther networks are ignored
  - Unsuitable for very large networks

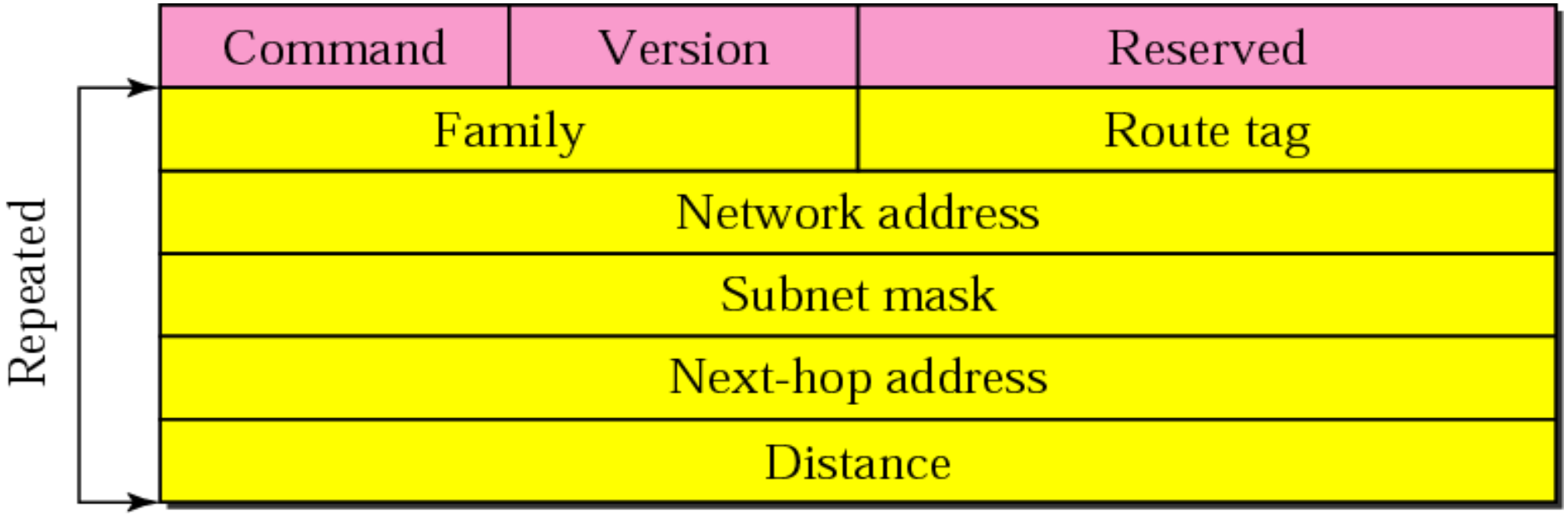
RIP message format



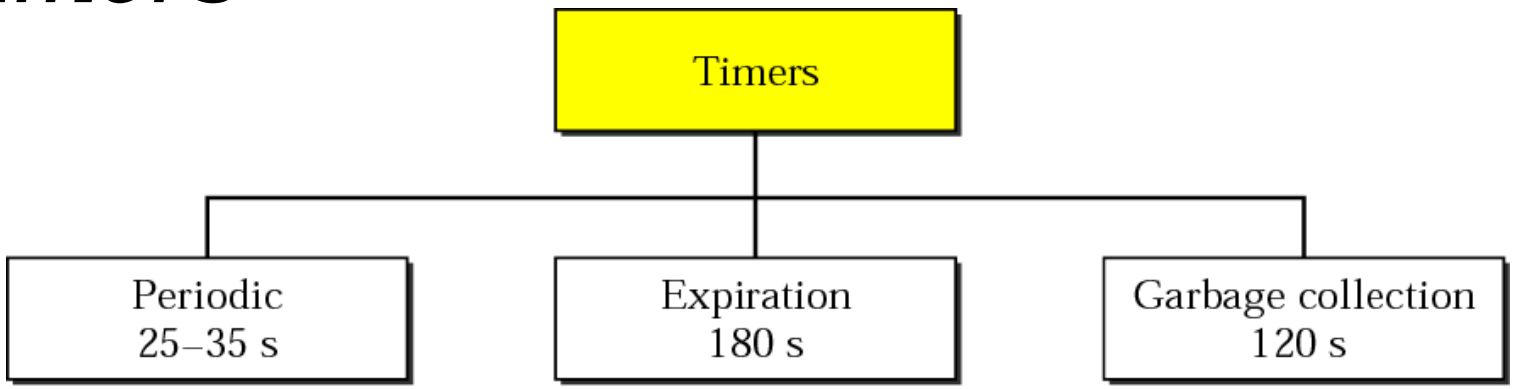
Command: request (1) or response (2)
Version: 1 or 2
Family: TCP/IP has value 2
Network address: address of the destination network
Distance: hop count from the advertising router to the destination network

RIP version 2 format

Version 2 supports subnet masks



RIP timers



Periodic timer: controls the advertising of regular updates

Expiration timer: governs the validity of a router. When a router receives info, sets timer to 180s. No update within 180s? Route set to 16, which means unreachable.

Garbage collection timer: Set to 120s after route set to 16. When timer expires, then toss route info.

Open Shortest Path First (RFC 1247) OSPF

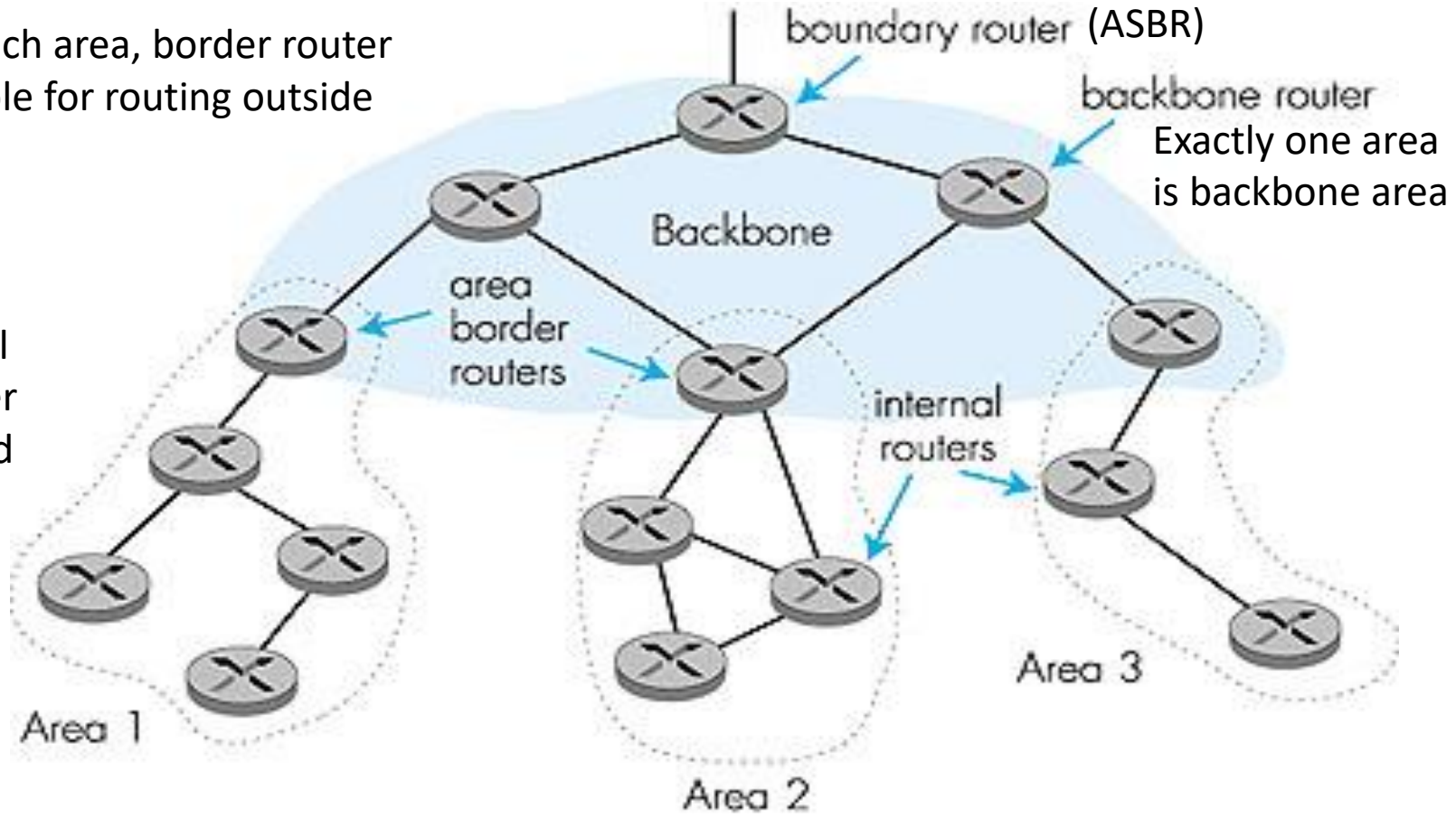
- Link-state
- Uses IP, has a value in the IP Header (8 bit protocol field)
- Interior routing protocol, its domain is also an Autonomous System (An A**utonomous System** (**AS**) is a collection of connected Internet Protocol (IP) routing prefixes under the control of one or more network operators on behalf of a single administrative entity or domain that presents a common, clearly defined routing policy to the internet).
- Divides an AS into areas and uses areas to route packets hierarchically within AS

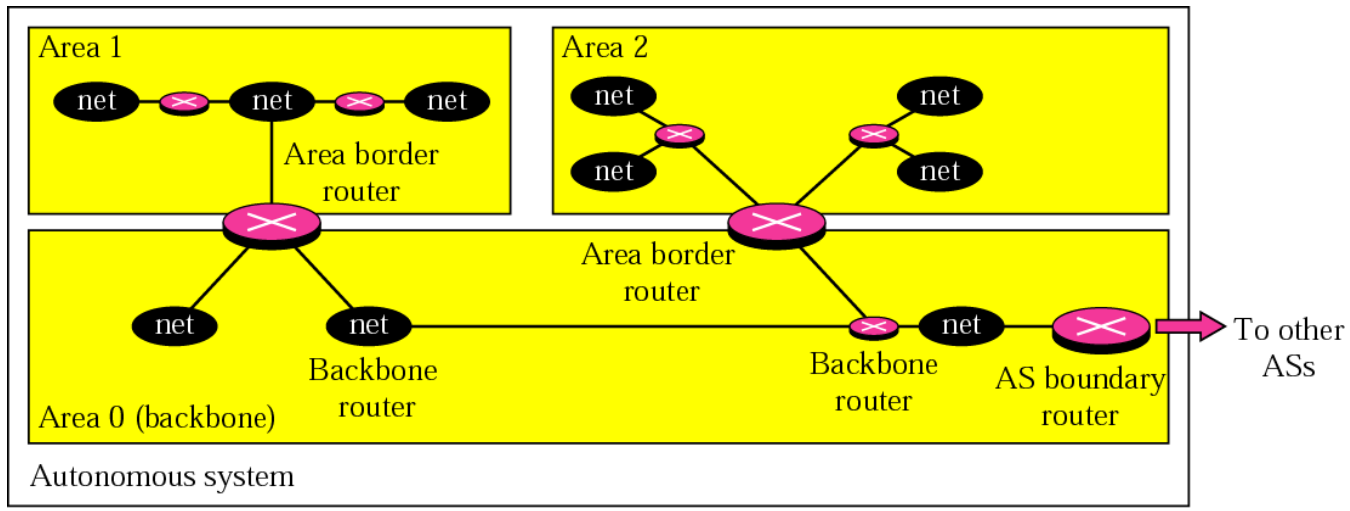
- Special routers (autonomous system boundary routers) or backbone routers responsible to dissipate information about other AS into the current system.
- Metric based on type of service
  - Minimum delay (rtt), maximum throughput, reliability, etc..
- Complex
  - LSP databases to be protected
- Uses *designated routers* to reduce number of endpoints

OSPF AS organized into a 2-level hierarchy

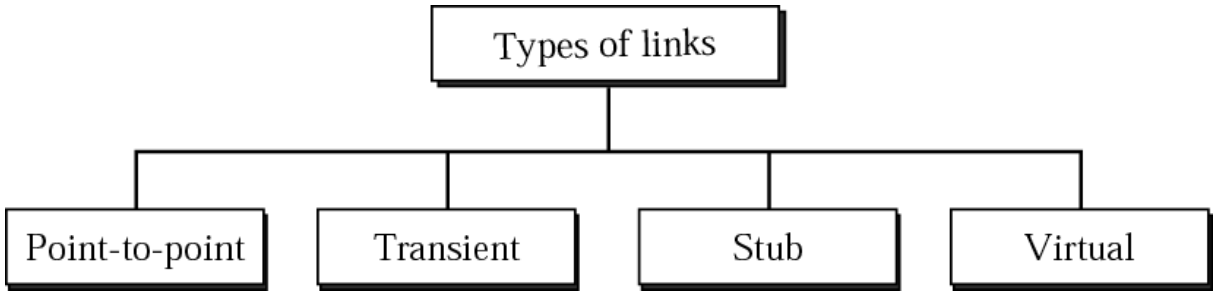
Within each area, border router responsible for routing outside the area

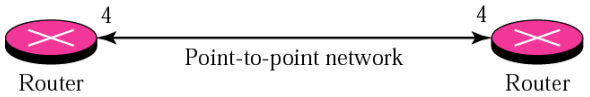
Backbone area contains all area border routers and possibly others

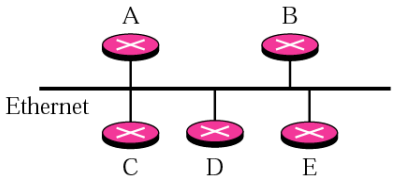



Area 1
net
net
net
Area border
router
Area 2
net
net
net
net
Area border
router
net
net
net
Backbone
router
Backbone
router
AS boundary
router
To other
ASs
Area 0 (backbone)
Autonomous system

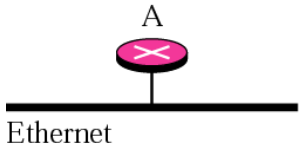
OSPF (type of links)





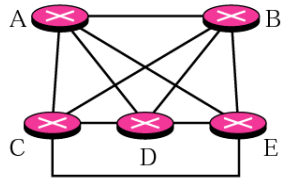


a. Transient network

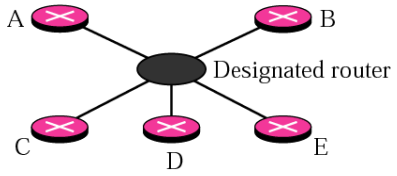


a. Stub network

b. Representation



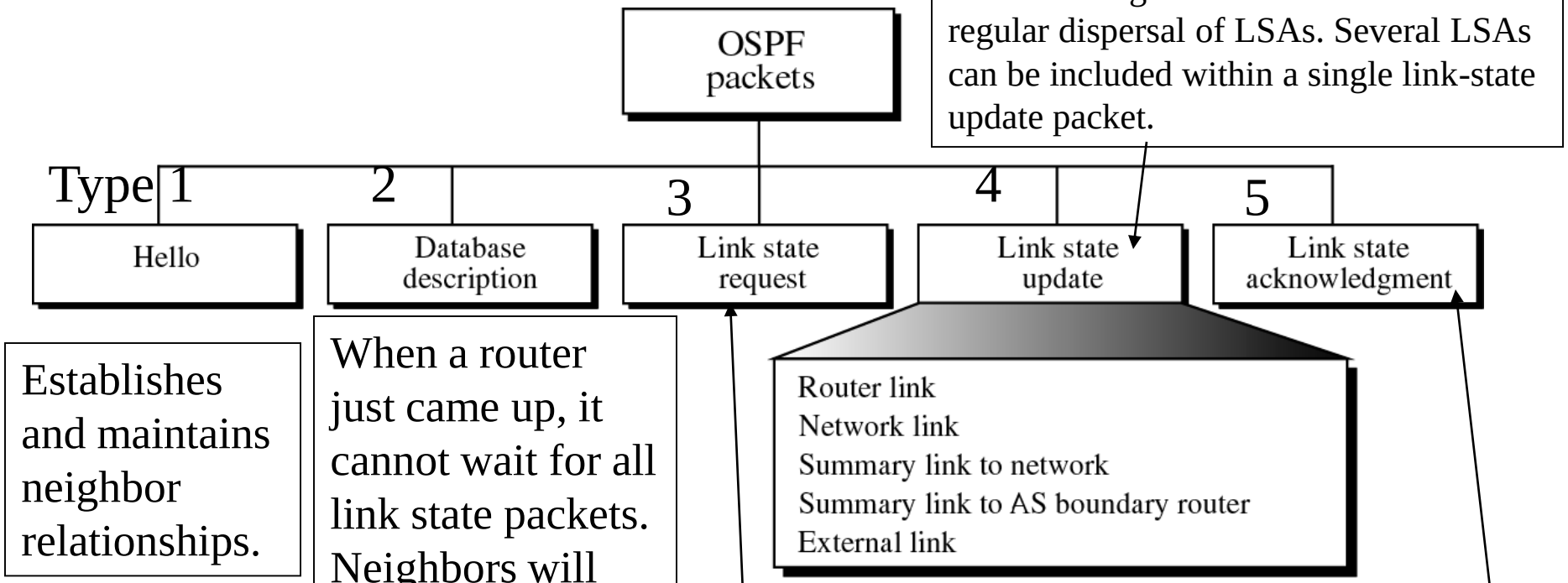
b. Unrealistic representation



c. Realistic representation

Five types of OSPF packets

- Hello
- Database description
- Link-State Request/Update/Acknowledgement



Responds to a link-state request packet. These messages also are used for the regular dispersal of LSAs. Several LSAs can be included within a single link-state update packet.

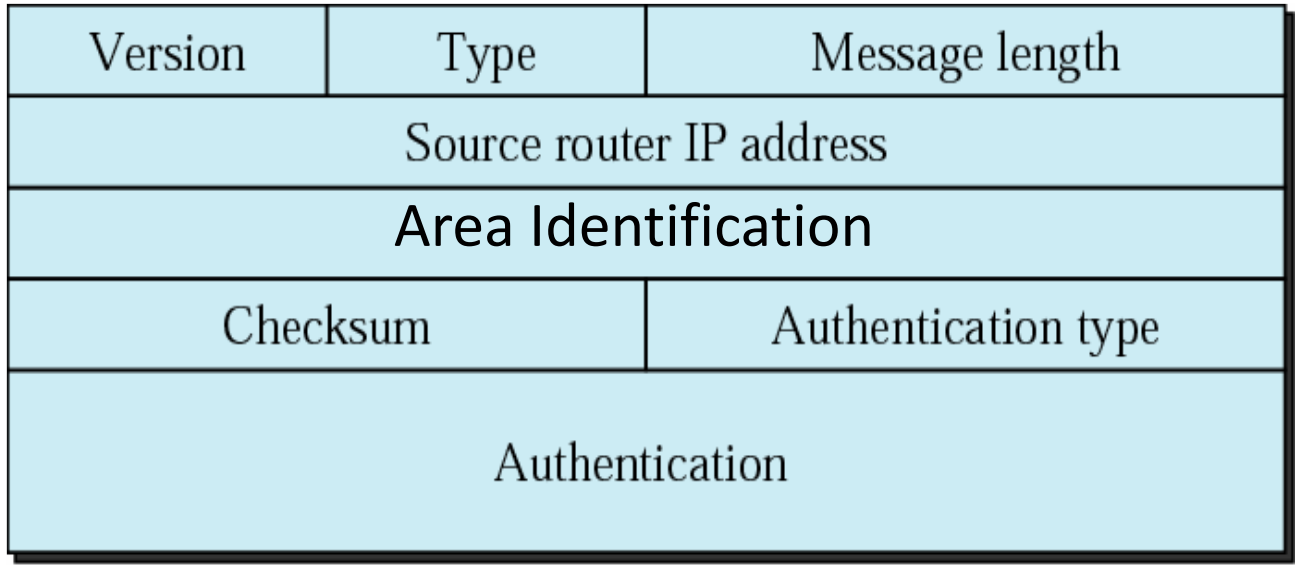
Establishes and maintains neighbor relationships.

When a router just came up, it cannot wait for all link state packets. Neighbors will send it a database description (not the full database but like an outline). From this, the router can then ask for information it does not have.

Requests pieces of the topological database from neighbor routers. These messages are exchanged after a router discovers (by examining database-description packets) that parts of its topological database are out of date.

•Ack-nowledges link-state update packets.

OSPF common header



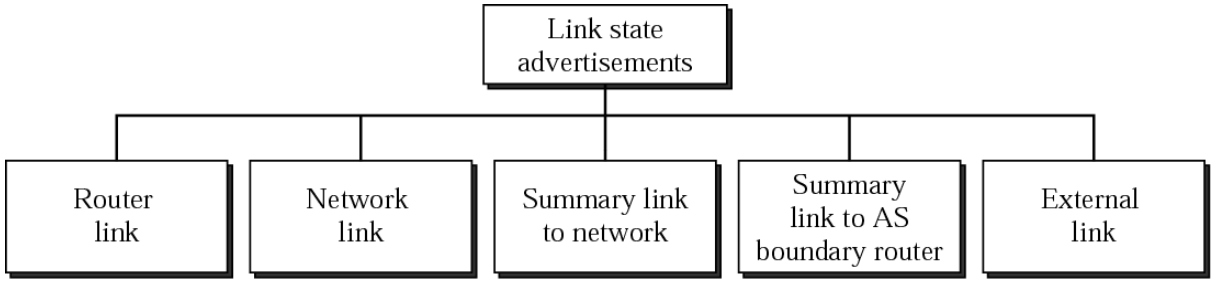
- All OSPF packets share the same header
- Version: 8-bit
  - The version of the OSPF protocol.
- Type: 8-bit
  - The type of the packet
- Message length: 16-bit
  - The length of the total message including the header
- Source route IP address: 32-bit
  - The IP address of the router that sends the packet

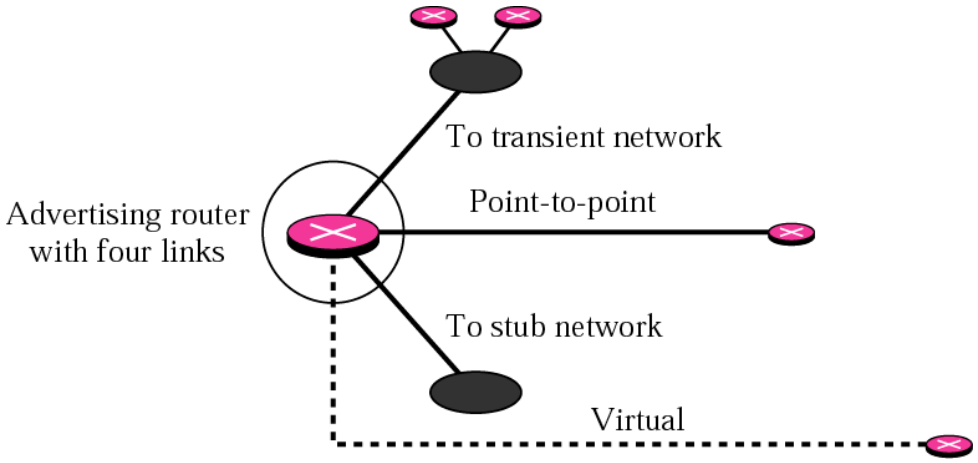
- Area identification: 32-bit
  - The area within which the routing take place
- Checksum: 16-bit
  - Error detection on the entire packet excluding the authentication type and authentication data field
- Authentication type: 16-bit
  - Define the authentication method used in this area 0: none, 1: password
- Authentication: 64-bit
  - The actual value of the authentication data
  - Filled with 0 if type = 0; eight-character password if type = 1

Link state updates

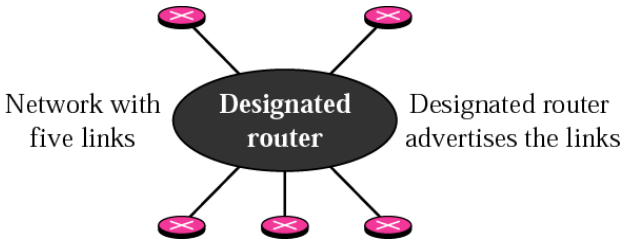
- Each Link State Update packet carries a set of new link state advertisements (LSAs) one hop further away from their point of origination.
- A single Link State Update packet may contain the LSAs of several routers.
- Each LSA is tagged with the ID of the originating router and a checksum of its link state contents.

OSPF (link state advertisement)



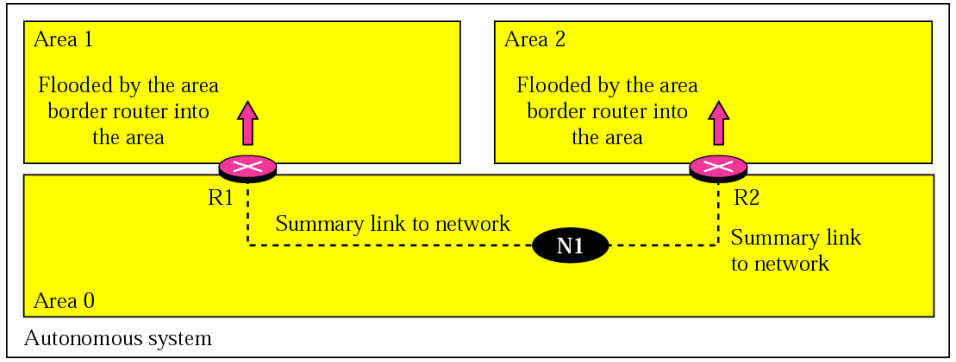


Router Link



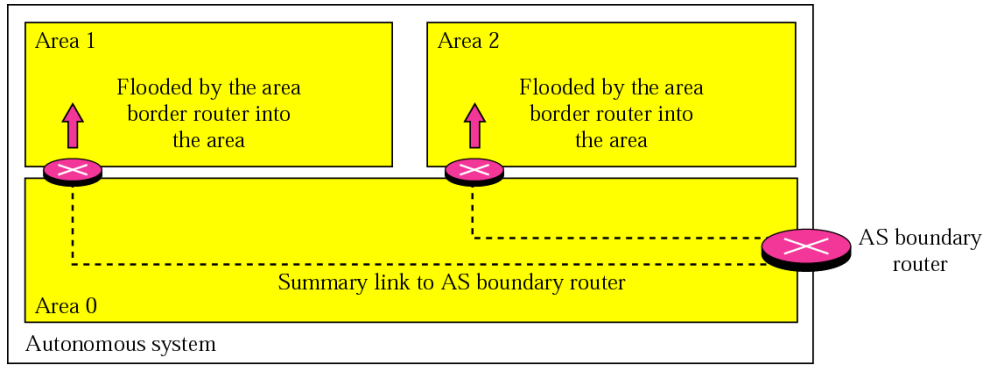
Network Link

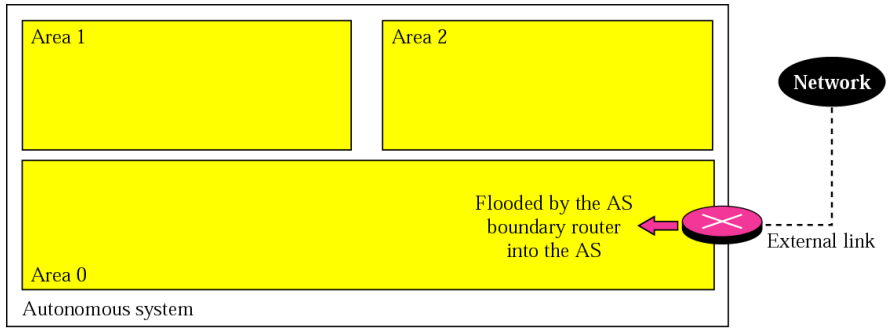
OSPF (LSA cont.)



Summary link to Network

Summary link to AS boundary router





External Link

OSPF operations

- Hello protocol
- Database synchronization
- Propagation of link-state information
- Building of routing table

Hello Protocol

- Hello packets are transmitted to all interfaces periodically
- Discover neighbors, establish and maintain neighbor adjacency relationships
- Elect Designated Router (DR) if there are multiple routers in a broadcast network

Database synchronization

- Two neighboring routers exchange database description packets to synchronize their link-state databases.
- Database description includes only a list of LSA headers. New or more up-to-date LSAs will be requested later
- Packets sent by master are acknowledged by slave

Propagation of link-state information

- Link-state request sent
  - When a router wants to update parts of its link-state database
- Link-state update sent
  - When a link state is requested, or
  - When a link-state changes, or
  - Periodically
- Link-state acknowledgement sent in response to a link-state update
  - Link-state updates retransmitted periodically until acknowledged

Flooding LSAs

- A node receiving a link-state update selectively first installs each LSA in the update into its LSA database
- Then it decides on which of its other links to flood the LSA
  - it may decide not to flood an LSA out a particular interface if there is a high probability that the attached neighbors have already received the LSA.

Building of routing table

- Router S has knowledge of the entire area topology (complete link-state database)
- Some algorithm such as Dijkstra's is used to generate shortest path tree, rooted at router S
- Only the next hop will be used in the routing table

Border Gateway Protocol (RFC 1771)

Why the *distance vector routing* and *link state routing* are not good candidates for inter autonomous system routing?

Distance vector routing

- Not preferred for inter-AS routing (exterior routing protocol)
  - Assumes all routers have a common distance metrics to judge route preferences.
    - If routers have different meanings of a metric, it may not be possible to create stable, loop free routes.
  - A given AS may have different priorities from another AS.
  - Gives no information about the ASs that will be visited.
- There are occasions in which the route with the smallest hop count is not the preferred route
- For example, we may not want a packet to pass through an AS that is not secure even it is the shortest path
- Unstable

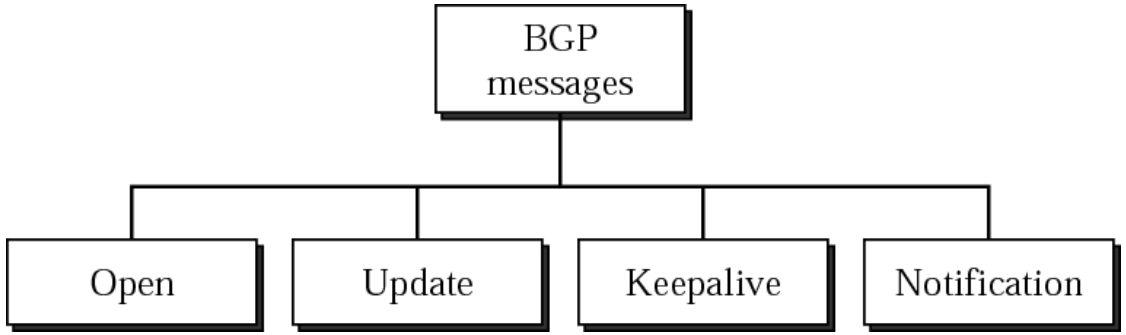
Link state routing

- An internet is usually too big for this routing method
- Link-state routing protocol
  - Different metrics.
  - Flooding is not realistic.
  - If used, each router must have a huge link state database
- It would take a long time for each router to calculate its routing table by Dijkstra algorithm

BGP

- An inter-autonomous system routing protocol
- Based on the *path vector routing* method
- Path vector routing
  - No metrics,
  - Information about which networks can be reached by a given router and ASs to be crossed.
  - distance vector annotated with entire path
  - also with policy attributes
  - guaranteed loop-free
- Differs from DVA
  - Path vector approach does not include a distance or cost estimate
  - Lists all of the ASs visited to reach destination network.
- Can use non-tree backbone topologies
- Uses TCP to disseminate DVs
  - reliable
  - but subject to TCP flow control
- Policies are complex to set up

BGP Messages



- Messages are sent over TCP connections on port 179.
- Functional procedures
  - Neighbor acquisition (open message, acceptance through Keepalive message)
  - Neighbor reachability (periodic Keepalive messages)
  - Network reachability (broadcast an update message)
    - Each routers maintains a database of networks that can be reached
    - + preferred route to this network.
- RFC does not address
    - How a router knows the address of another router.
    - Up to network admin.