פרק 9 חלק ב'
פרוטוקולי ניתוב ופתרונות גיבוי

- Bridge and Switch
- Routing Protocols
- Redundancy and Load Balance

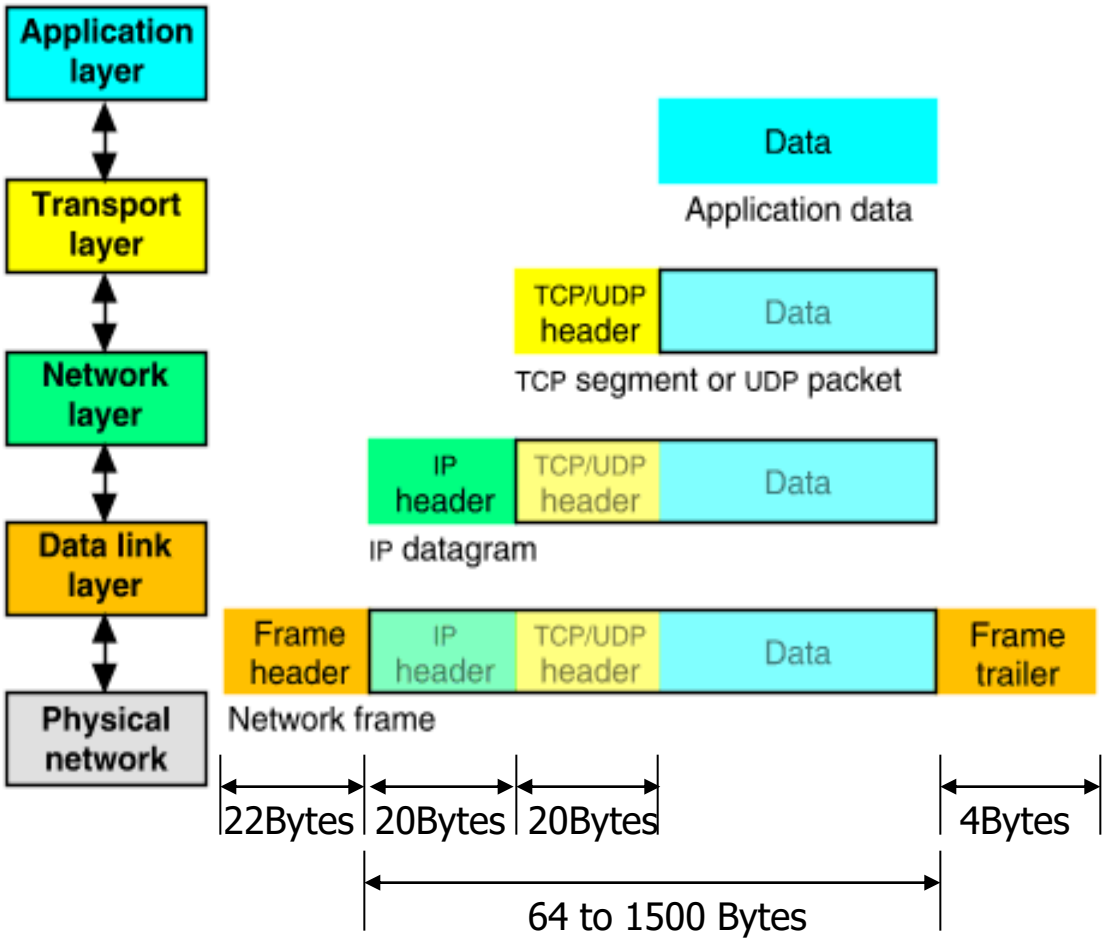
חזרה על מודל ISO/OSI

- Seven network “layers”
  - Layer 1 : Physical – cables
  - Layer 2 : Data Link – Ethernet
  - Layer 3 : Network – IP
  - Layer 4 : Transport – TCP/UDP
  - Layer 5 : Session
  - Layer 6 : Presentation
  - Layer 7 : Application

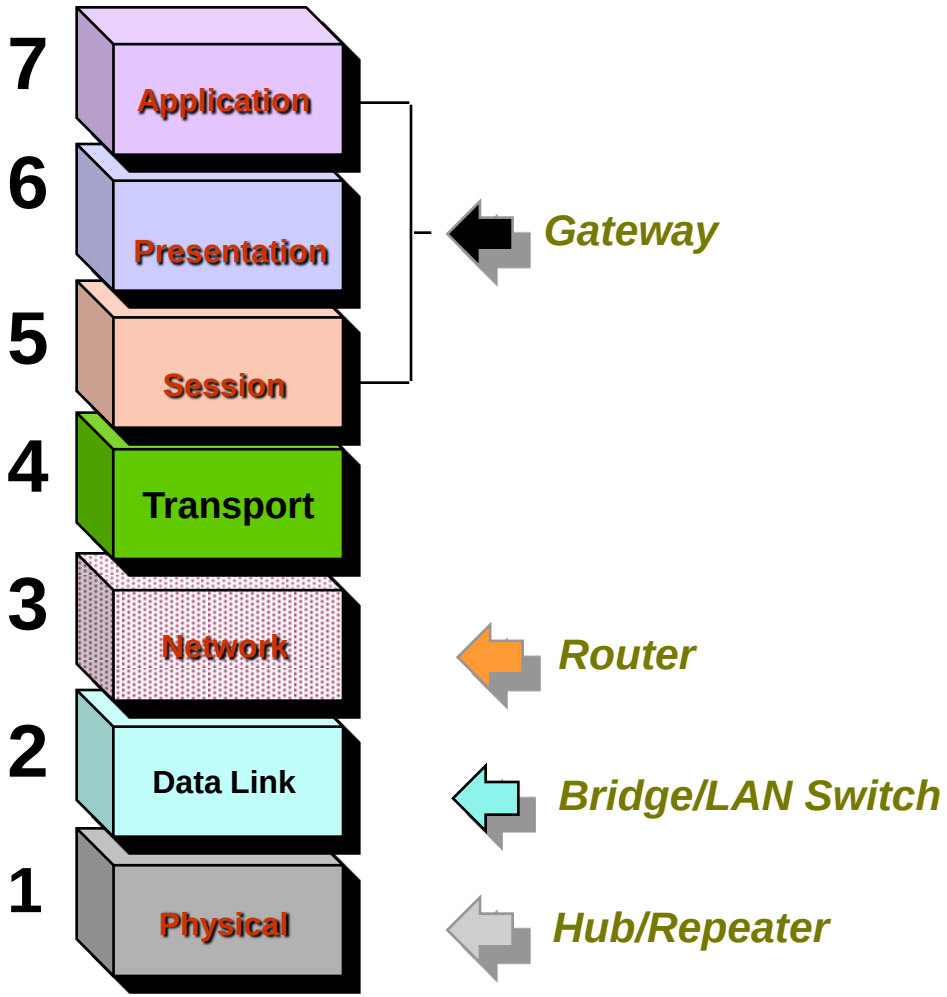
OSI: Open Systems Interconnect

Packet Encapsulation

- The data is sent down the protocol stack
- Each layer adds to the data by prepending headers

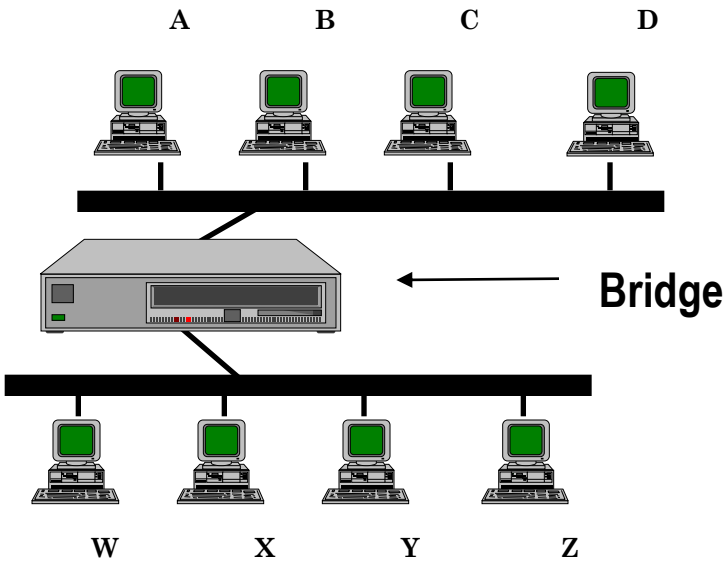


Internetworking Components



The Bridge/Switch

- The Learning Algorithm
  - Table of the MAC Addresses on each port
  - At initialization the table is empty
  - The Bridge listens and accepts all frames, and acts according to the following algorithm
    - If the Destination MAC address
      - is in the table of an outgoing port, forward the frame to that port
      - If it is not in the table, forward to all outgoing ports
    - Add the source address to the table with a timer (300sec)
- A LAN Switch is a multi-port Bridge

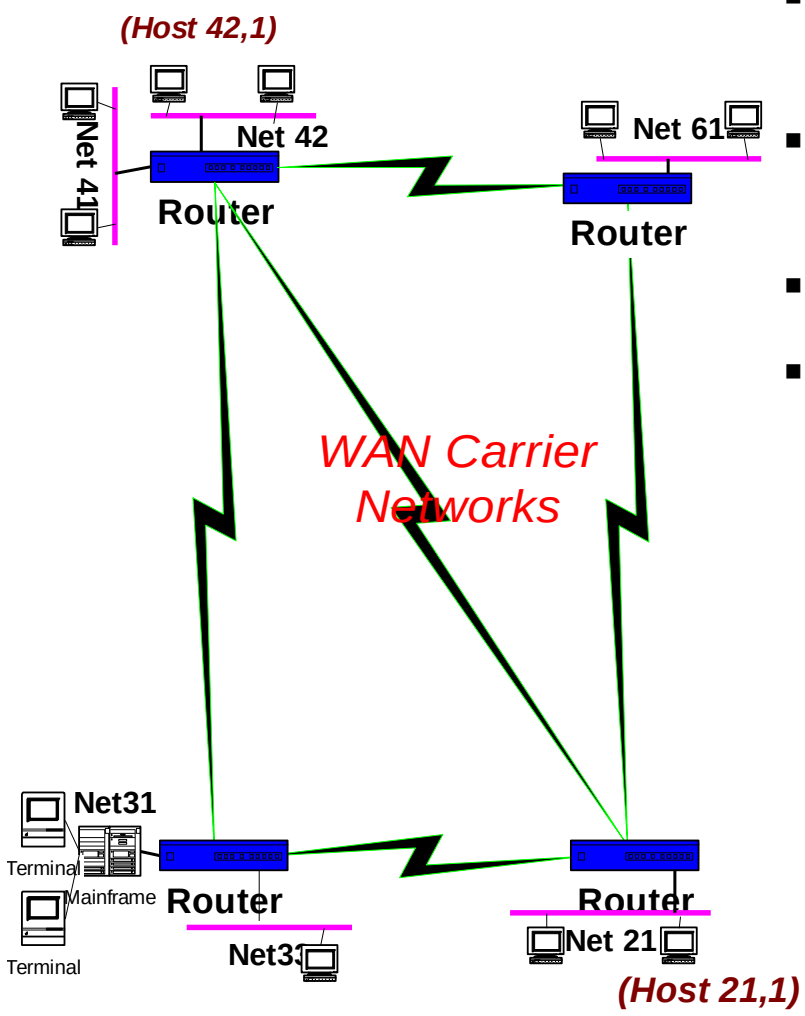


The Algorithm cannot handle loops

A 24 Port LAN Switch Example

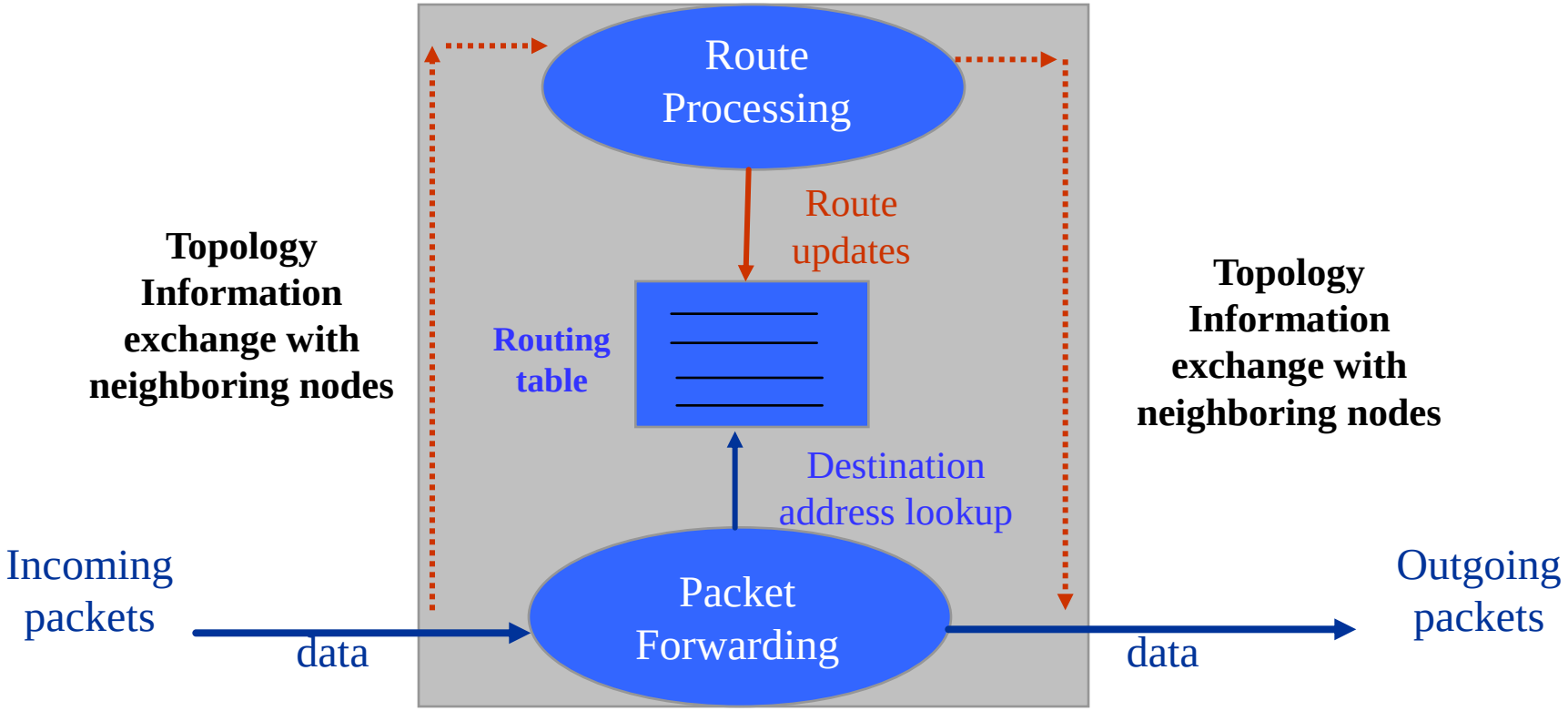
- Ports
  - 22 auto sensing 10/100/1000 ports
  - 2 Dual Personality Ports each port can be used as either
    - RJ-45 10/100/1000 port
    - or open mini-GBIC slot (for use with Fibre Optics mini-GBIC transceivers)
- Performance
  - Latency
    - for 100 Mb < 4.7 μs (64-byte packets)
    - for 1000 Mb < 3.0 μs (64-byte packets)
  - Throughput up to 35.7 million pps (64-byte packets)
  - Switching capacity: 48 Gbps
  - MAC address table size: 8000 entries

Routing Technology



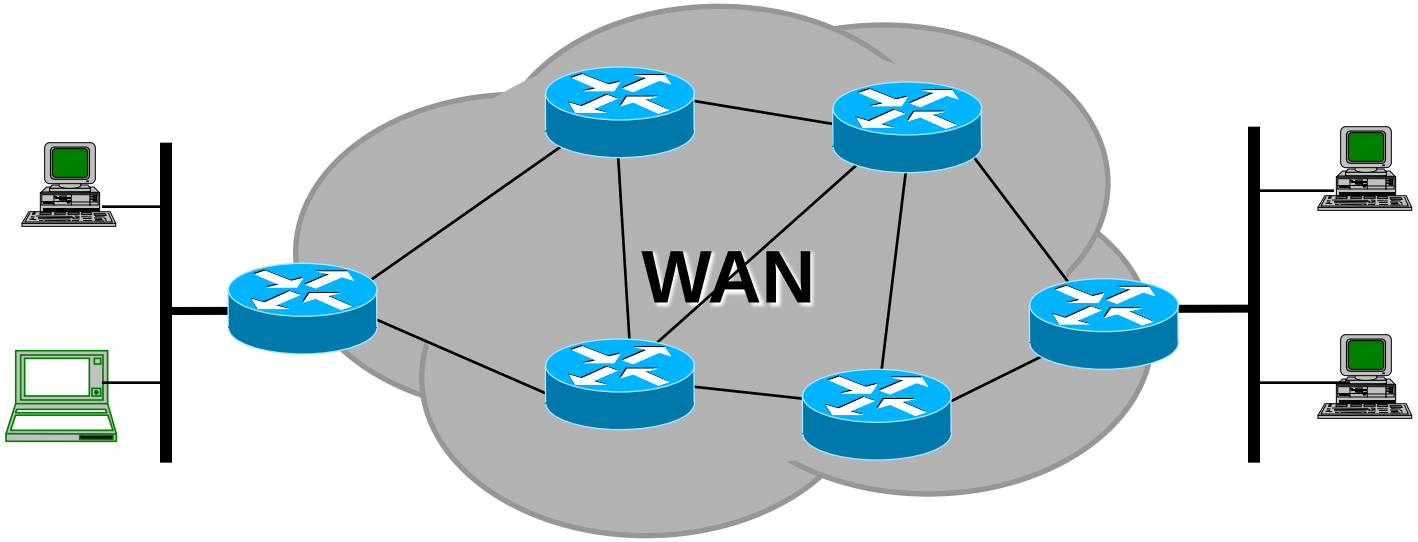
- In the real world an internet connects different networks, particularly LANs and WANs
- Routers understand the specific protocols of the networks they connect
- The term Gateway is also used
- Routing Technology
  - Defines a common addressing scheme
    - (Network, Host)
  - Find the *best* path to deliver packets between workstations
  - Best could be
    - Shortest
    - Fastest
    - Least congested
    - Most secure

The Router



- Frame Received, checked at Layer2 stripped and Packet passed to Layer3
- Destination Address checked against Routing Table for best match
- Packet passed to appropriate outgoing interface and Framed for output

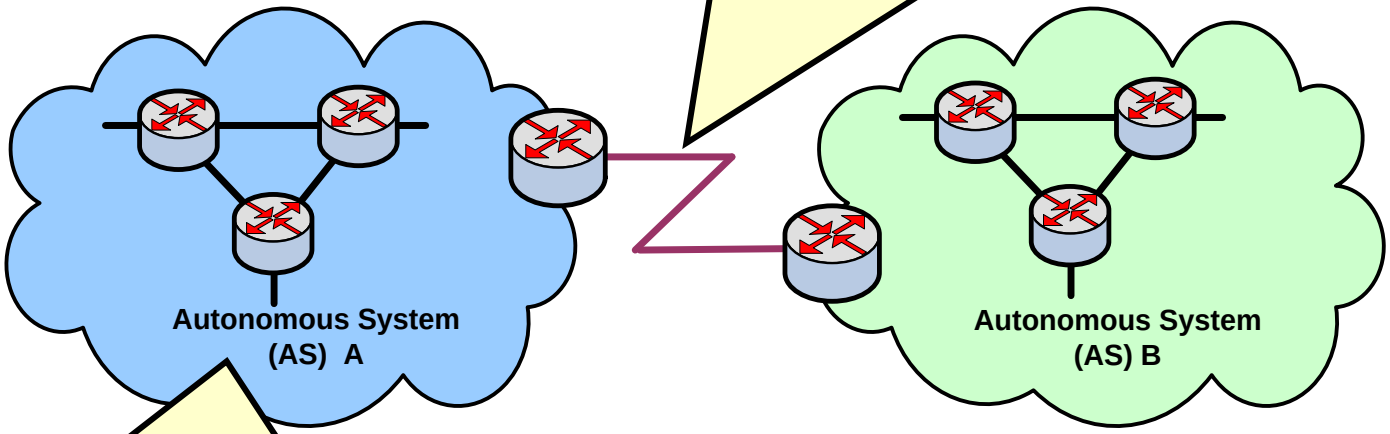
Routing Protocols



- Static
  - Statically set up by Network Administration
- Dynamic
  - Learned and constructed by routing protocols
- Routing Protocol (Algorithm)
  - The Algorithm used to send topology information and updates across the network

Dynamic Routing Protocols

BGP (Border Gateway Protocol) :
Inter-domain protocol
Exchanges routing information between the routers in a network of AS

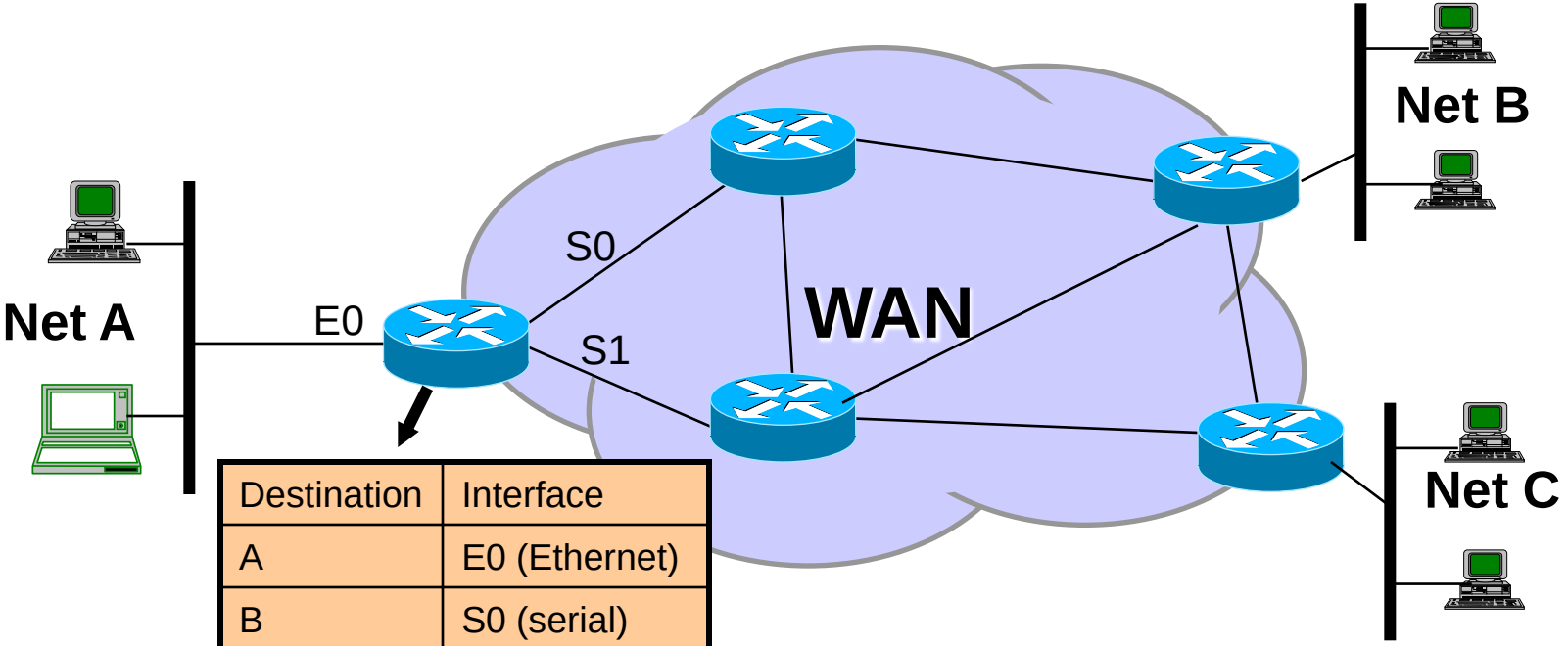


IGP (Interior Gateway Protocol) :
Exchanges routing information between routers within an AS

Commonly used IGPs:
- **RIP - Routing Information Protocol (legacy)**
- **OSPF - Open Shortest Path First Protocol**

An Autonomous **system (AS)** is a collection of IP networks and routers under the control of one entity that presents a common routing policy.

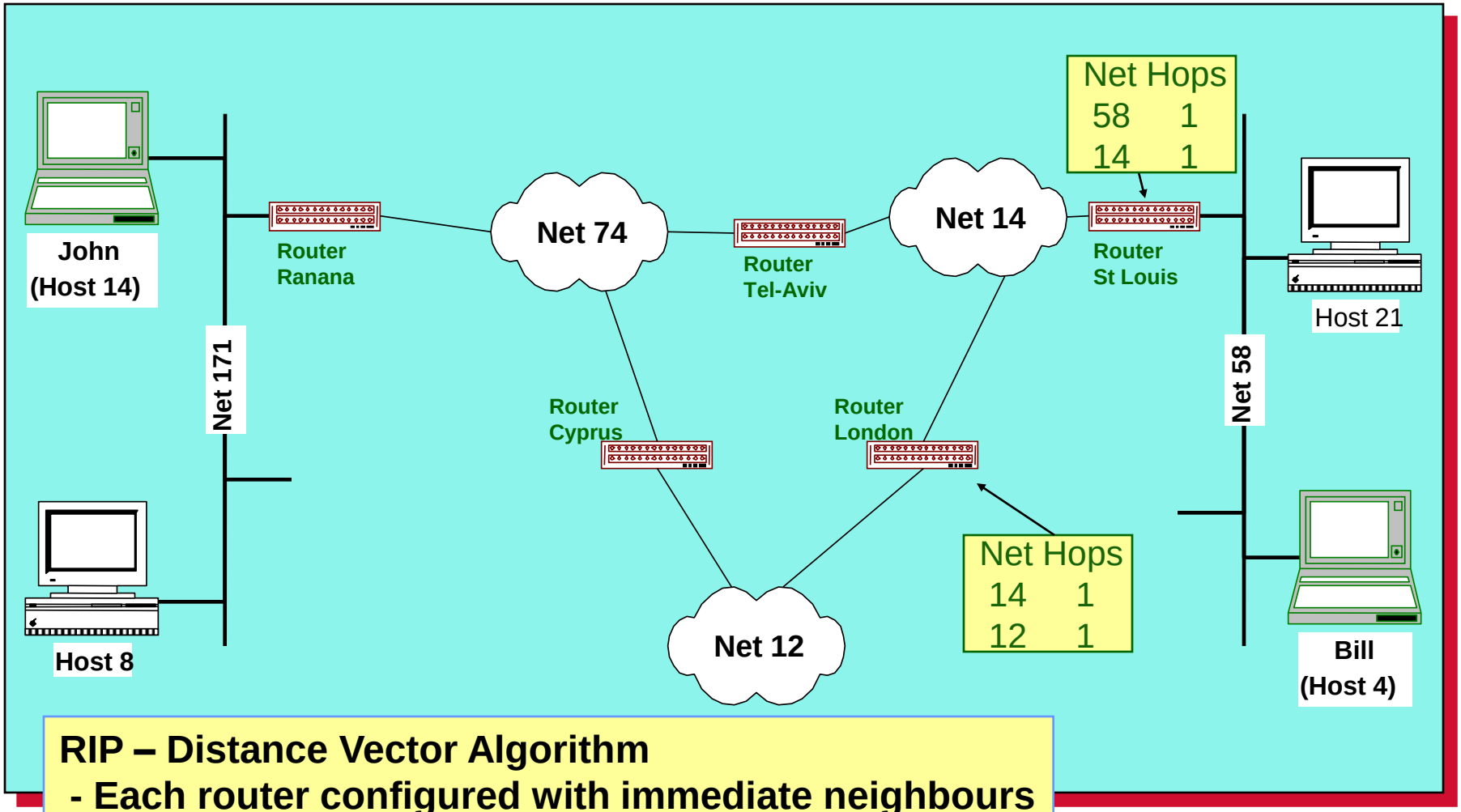
Routing Table



Destination	Interface
A	E0 (Ethernet)
B	S0 (serial)
C	S1 (serial)

- The crucial element of the router
  - defines the topology of the network
  - must be consistent with other router's tables
- Routing Table – a mix of static and dynamic routing
  - static routes for access or stub networks
  - dynamic routes for core and distribution networks
  - Default route

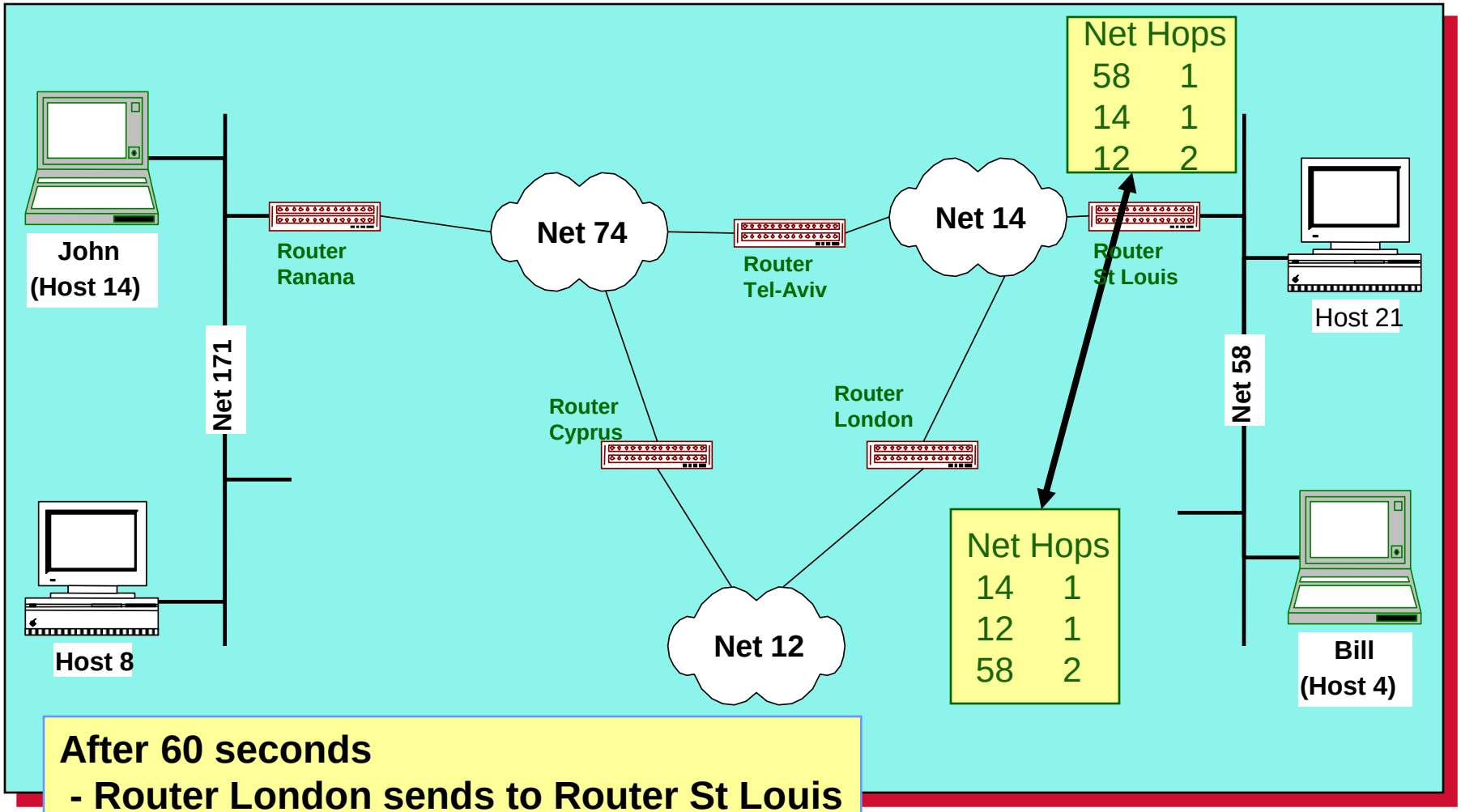
RIP - Routing Information Protocol -1



RIP – Distance Vector Algorithm

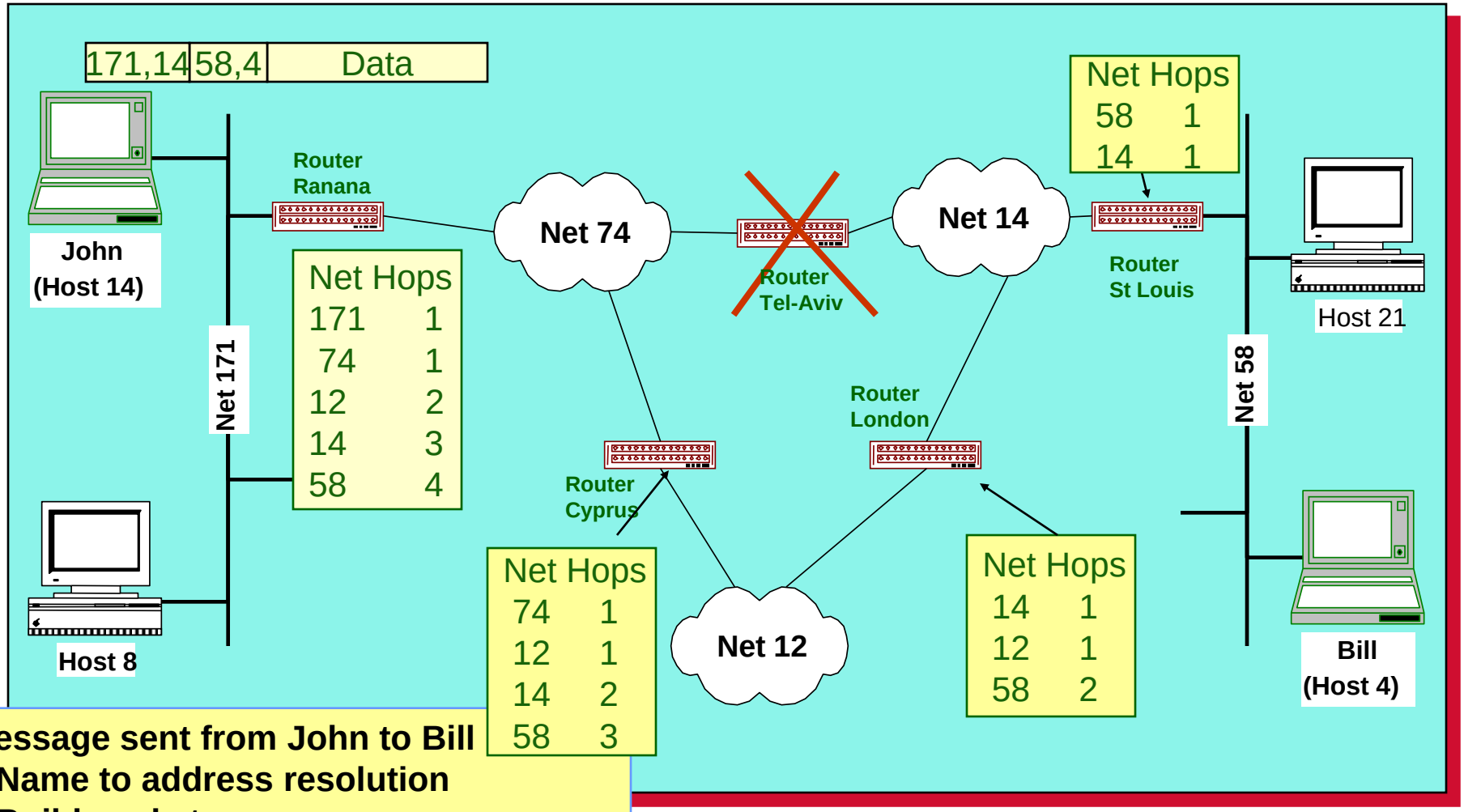
- **Each router configured with immediate neighbours**
- **At timed intervals information sent to neighbours**

RIP - Routing Information Protocol - 2



After 60 seconds
- Router London sends to Router St Louis
- Router St Louis sends to Router London

RIP - Routing Information Protocol - 3

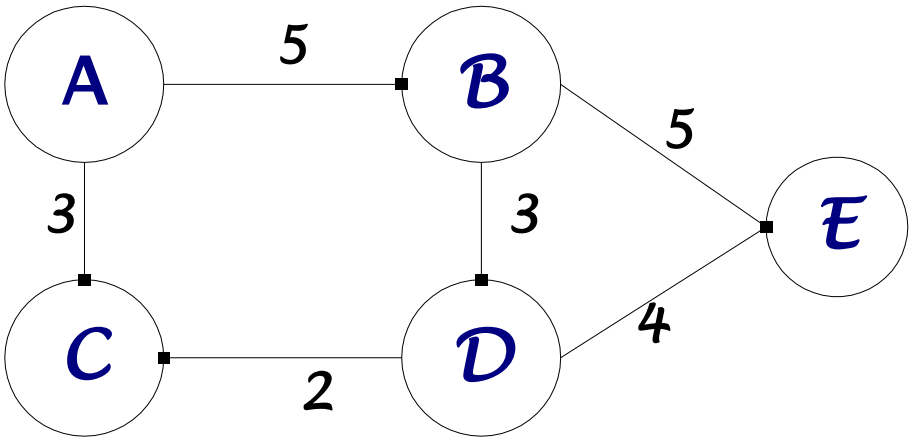


Message sent from John to Bill
- **Name to address resolution**
- **Build packet**
- **If on different network send to Router**

OSPF Background

- Developed by IETF – RFC1247
  - Designed for Internet TCP/IP environment
- OSPF v2 described in RFC2328/STD54
- OSPF v3 described in RFC2740 - IPv6
- Link state/Shortest Path First Technology
- Dynamic Routing
- Fast Convergence
- Route authentication

Link State (OSPF) Routing

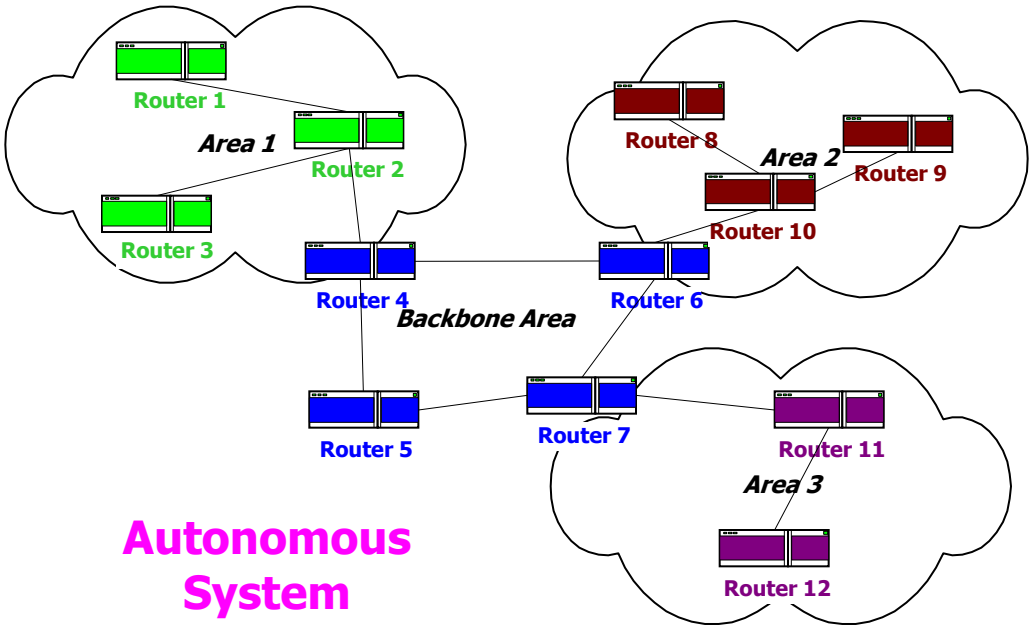


	Cost/Metric	Delay	Security
A – B	5	50ms	8
A – C	3	40ms	5
B - D	3	80ms	6
C – D	2	70ms	9
B – E	5	50ms	9
D - E	4	70ms	4

- An OSPF Network is treated as graph connecting nodes with links
- Each link can have several “metrics”
- Router floods network with Link State Packet when link changes status
- Router creates Routing table using SPF algorithm

OSPF – Open Shortest Path First

- OSPF - Link State Protocol
- Can Operate within a Hierarchy
  - Autonomous System (AS)
  - Areas within AS
- Link State Advertisements (LSAs) sent by each Router to all other Routers within Area
- Routers accumulate the LSAs and use the SPF algorithm to calculate the Shortest Path to each network
- Can Support
  - One or more metrics
  - TOS - Type of Service (with more than one metric)
- EGP - Exterior Gateway Protocol to connect Autonomous Systems (Inter-Domain Routing).



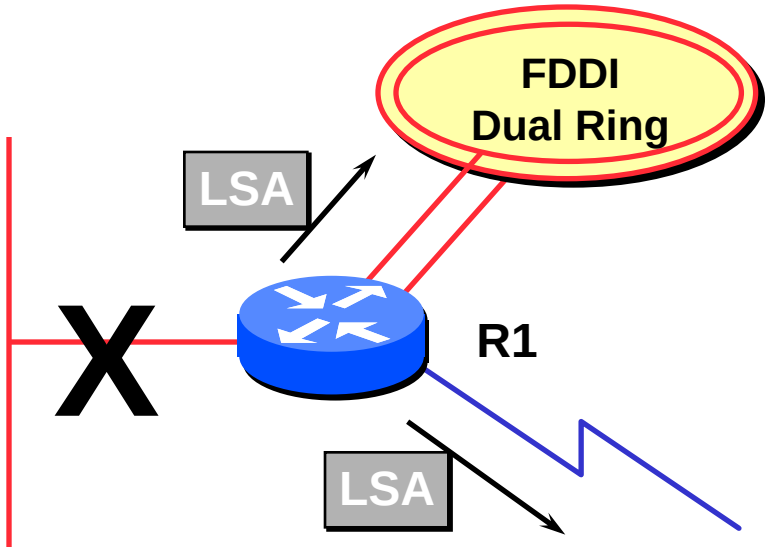
Link State Algorithm

- Each router contains a database containing a map of the whole topology
  - Links
  - Their state (including cost)
- All routers have the same information
- All routers calculate the best path to every destination
- Any link state changes are flooded across the network
  - "Global spread of local knowledge"

Link State Routing

- Automatic neighbor discovery
  - Neighbors are physically connected routers
- Each router constructs a Link State Packet (LSP)
  - Distributes the LSP to neighbours…
  - …using an LSA (Link State Announcement)
- Each router computes its best path to every destination
- On network failure
  - New LSPs are flooded
  - All routers re-compute routing table

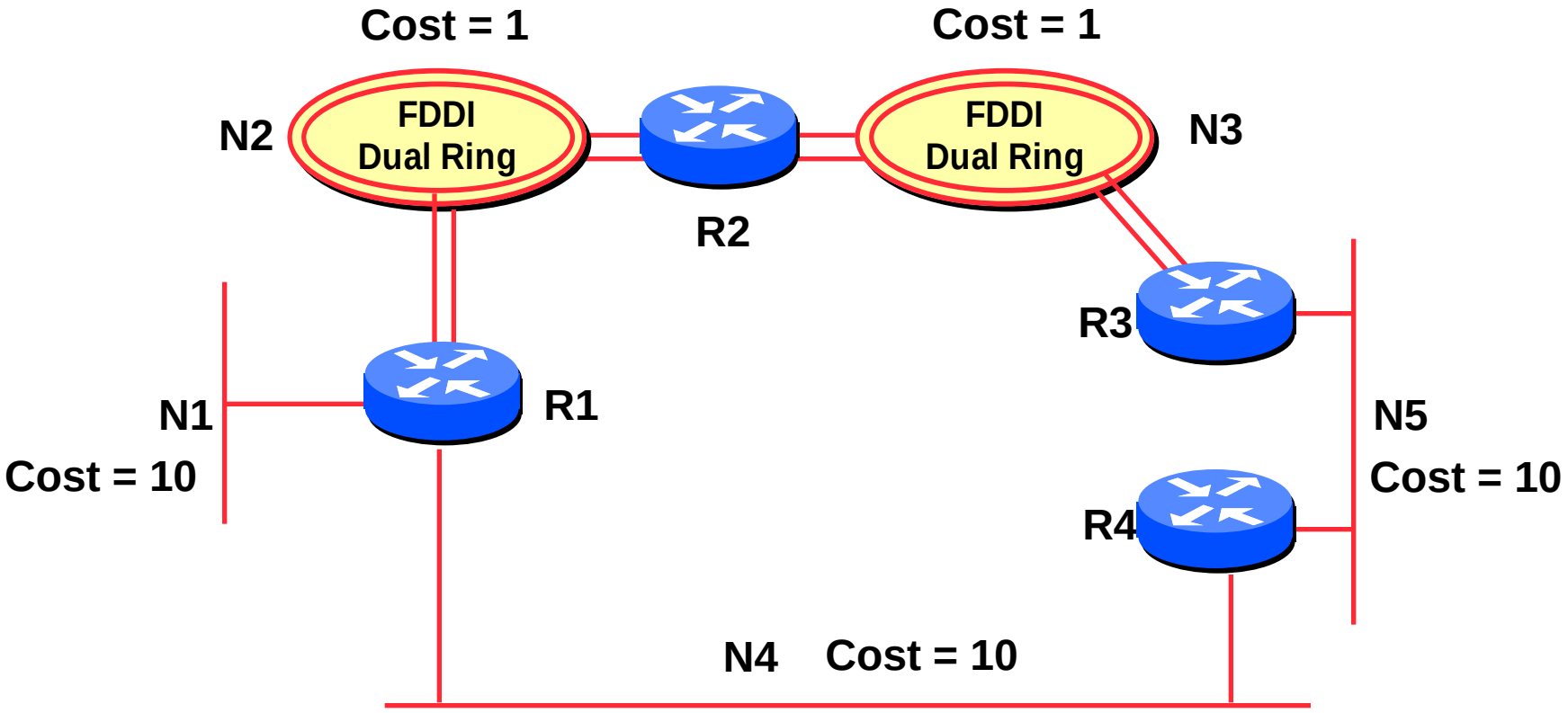
Low Bandwidth Requirements



- Only changes are propagated
- Multicast used on multi-access broadcast networks
  - 224.0.0.5 used for all OSPF speakers
  - 224.0.0.6 used for DR and BDR routers

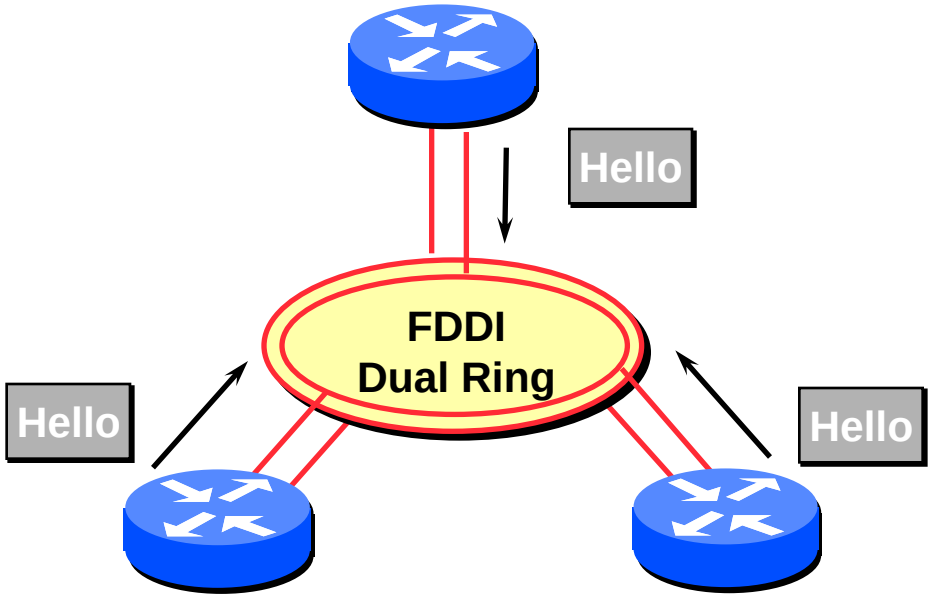
“Shortest Path First”

- The optimal path is determined by the sum of the interface costs



OSPF: How it works

- Hello Protocol
  - Responsible for establishing and maintaining neighbour relationships
  - Elects Designated Router on broadcast networks



OSPF: How it works

- Hello Protocol
  - Hello Packets sent periodically on all OSPF enabled interfaces
  - Adjacencies formed between some neighbors
- Hello Packet
  - Contains information like Router Priority, Hello Interval, a list of known neighbours, Router Dead Interval, and the network mask

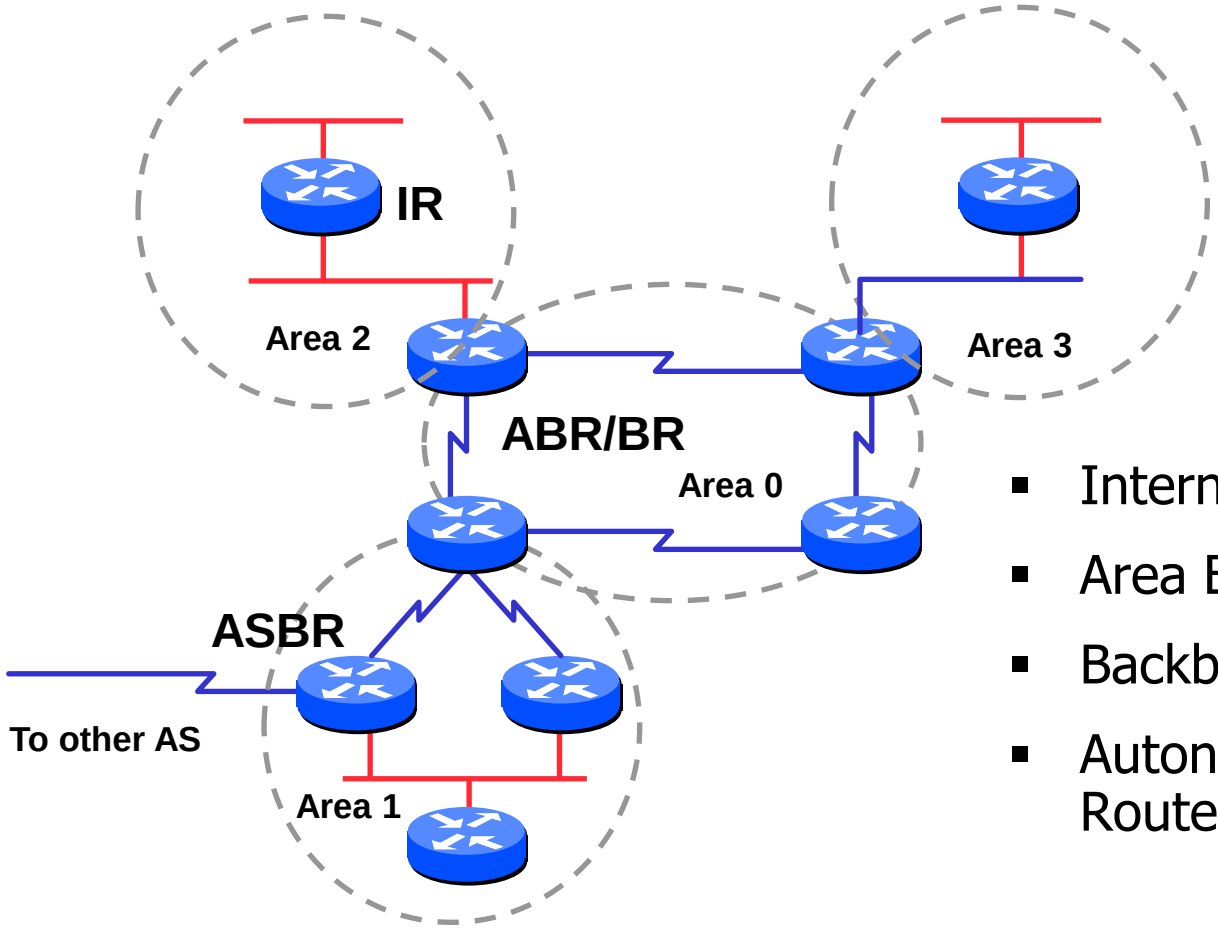
OSPF: How it works

- Trade Information using LSAs
  - LSAs are added to the OSPF database
  - LSAs are passed on to OSPF neighbors
- Each router builds an identical link state database
- SPF algorithm run on the database
- Forwarding table built from the SPF tree

OSPF: How it works

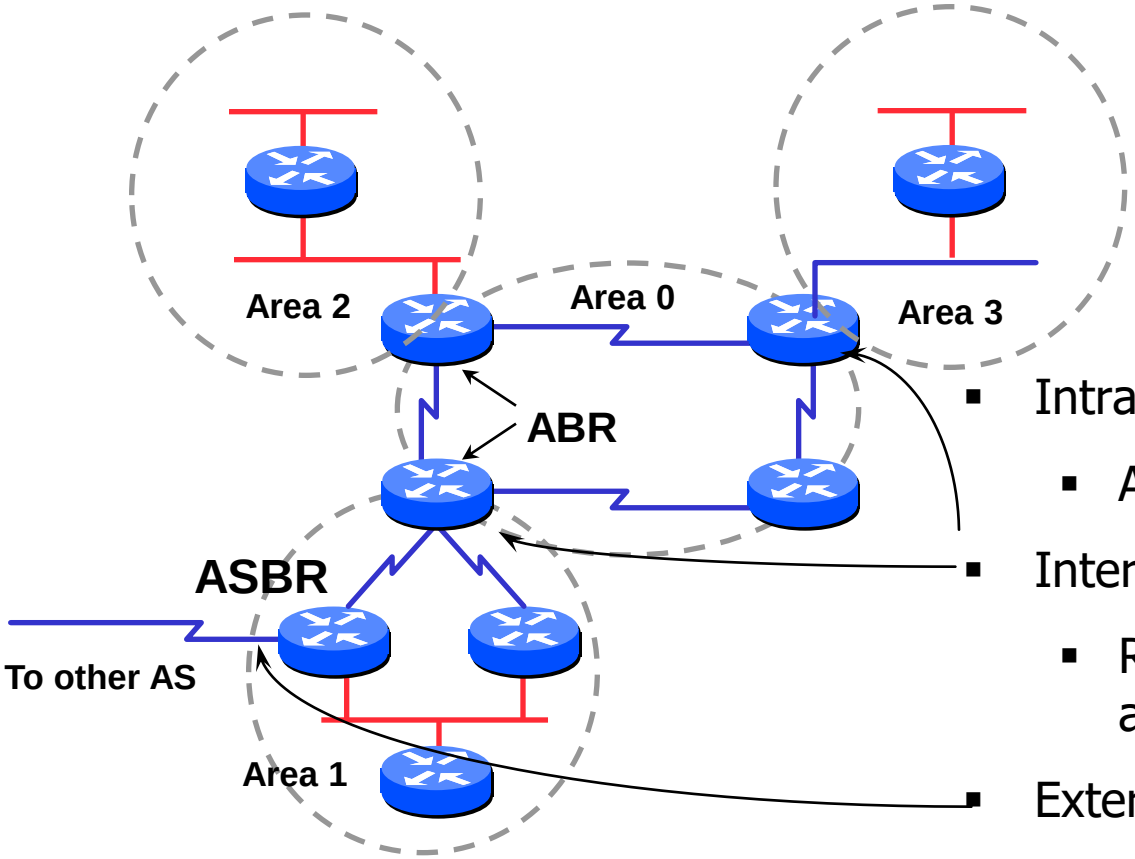
- When change occurs:
  - Announce the change to all OSPF neighbors
  - All routers run the SPF algorithm on the revised database
  - Install any change in the forwarding table

Classification of Routers



- Internal Router (IR)
- Area Border Router (ABR)
- Backbone Router (BR)
- Autonomous System Border Router (ASBR)

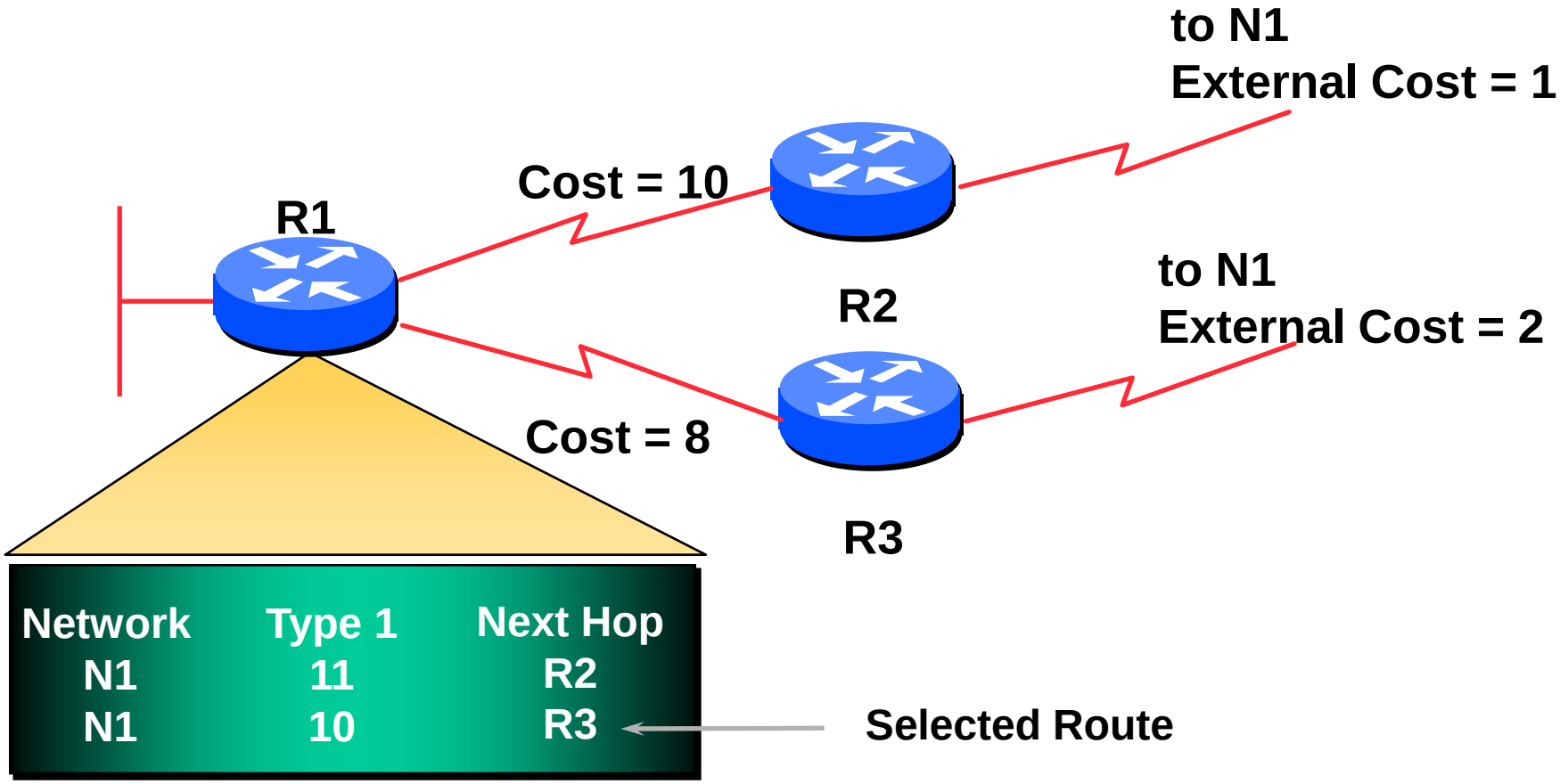
OSPF Route Types



- Intra-Area route
  - All routes inside an area
- Inter-Area route
  - Routes advertised from one area to another area by an ABR
- External route
  - Routes imported into OSPF from another routing protocol by an ASBR

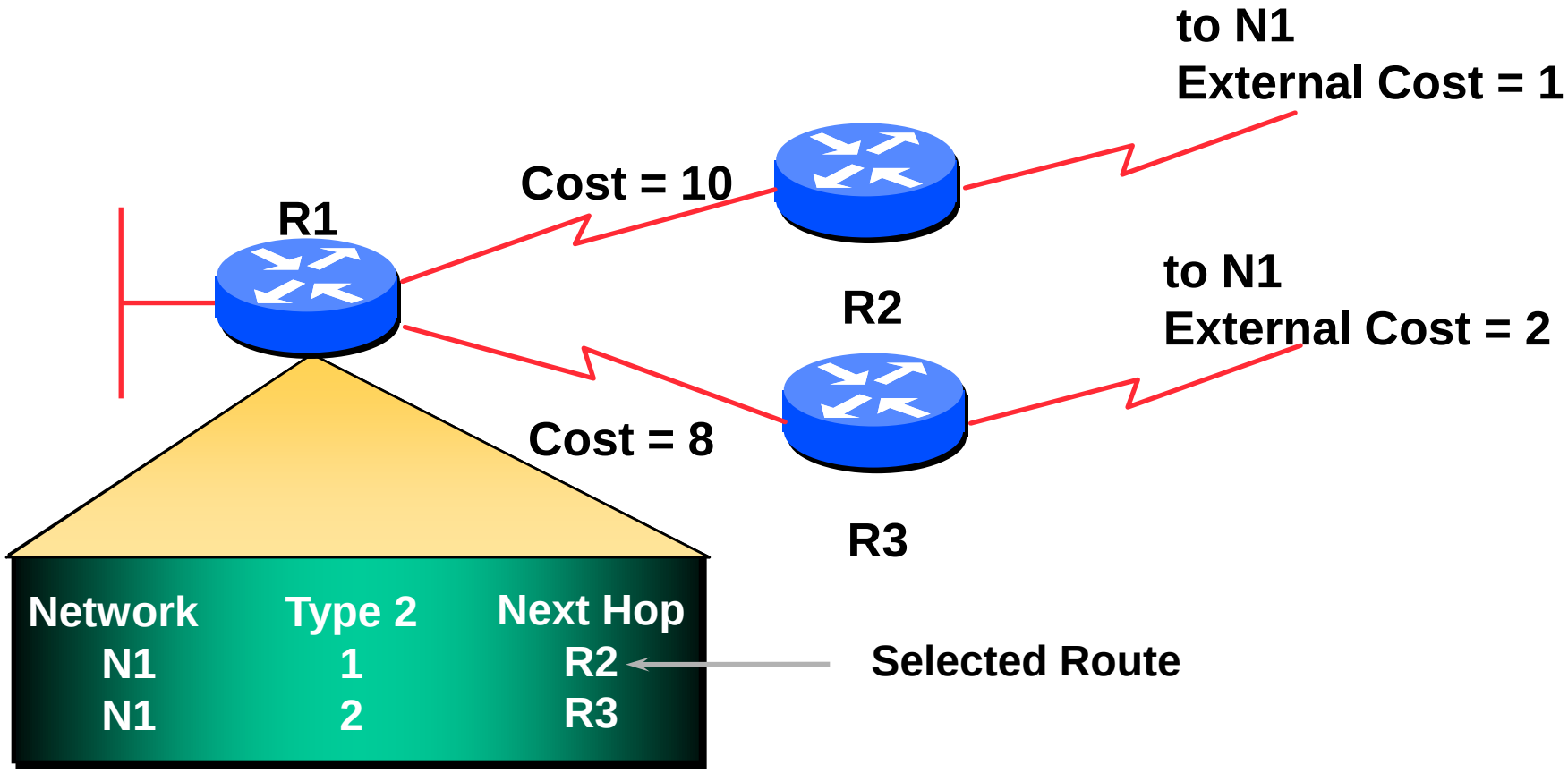
External Routes

- Type 1 external metric: metrics are added to the summarised internal link cost



External Routes

- Type 2 external metric: metrics are compared without adding to the internal link cost



Route Authentication

- Now recommended to use route authentication for OSPF
  - …and all other routing protocols
- Susceptible to denial of service attacks
  - OSPF runs on TCP/IP
  - Automatic neighbour discovery

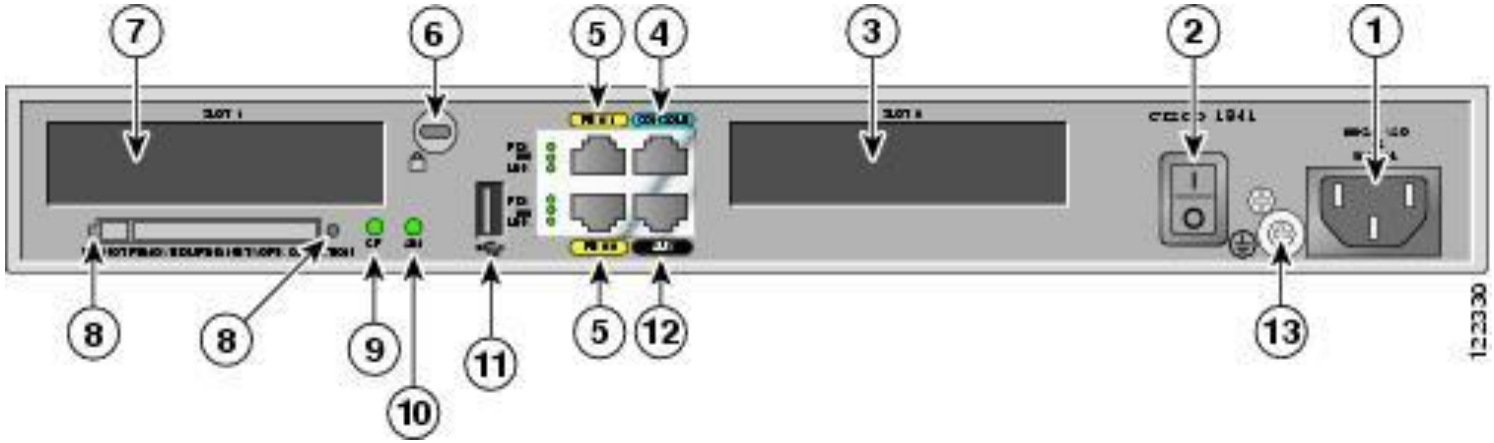
The World of Routers

- Routers
  - Core
    - Main Campus
    - Carrier Class
  - Enterprise
    - Main & Branch Office
  - Carrier Edge/Access
  - Home Router
    - Broadband Access
- Interfaces
  - LAN – Ethernet
  - WAN – LL, FR, ATM, Ethernet..

- Vendor Specific
  - Hardware/Software
  - Operating System, User Interface
  - Routing Algorithms
    - Standard, Proprietary
  - Filtering and Security
    - Access Lists
    - Firewall
  - Quality of Service Features

Cisco 1800 Series Router

Rear Panel



1	Power	8	Compact Flash Slot
2	On/Off Switch	9	Compact Flash LED
3	Serial Slot 0 (WAN)	10	AIM LED
4	Console Port	11	USB Slot
5	Fast Ethernet Slots & LEDS	12	Auxiliary Port (Remote Console)
6	Kensington security slot	13	Chassis Ground
7	Serial Slot 1 (WAN)		

Core Router

Juniper MX960

- Juniper Core/Backbone Router
- Layer 2 and Layer 3 Features
- IP VPN Routing
  - Virtual routing and IP Address space for each customer
- Ports
  - Up to 480 1GE ports or 48 10GE ports

Routing and Switching

	LAN Switching	Routing
Networks	LANs	Any to Any
Forwarding Address	MAC	Layer 3 (IP)
Decision Table	MAC Station Address Table	Network Address Routing Table

Challenges

Redundancy and Load Balance

- Avoiding Single Point of Failure
- Traffic Sharing - Lower Traffic stress per node
- Lower the probability for network outage and services down-time
- Network outages may cost a business substantial amount of money
- Many services (such as 911) require High availability (99.999%) and disaster recovery

Redundancy and Load Balance

- Availability is one of the three fundamentals of the CIA security model
- Business Continuity Planning and Disaster Recovery Planning are already common practices in critical infrastructures
- The Maximum Tolerable Downtime of a business unit is often over-estimated
  - This is why network architects should avoid single points of failure in a network infrastructure
  - Should provide reliable fail-over systems or high availability systems

Several Solutions

- Several Protocols for Redundancy and high availability:
  - VRRP – Virtual Router Redundancy Protocol (RFC 3768)
  - HSRP – Hot Standby Routing Protocol (RFC 2281/Cisco proprietary standard)
  - CARP – Common Address Redundancy Protocol (OpenBSD)
  - IRDP - ICMP Router Discovery Protocol (RFC 1256)
    - Extension of ICMP (Internet Control Message Protocol) that allows hosts to actively find a new router when their default gateway fails

- Several Protocols for Load Balancing
  - MHSRP – Multigroup HSRP (Cisco Proprietary)
  - GLBP – GW Load Balancing Protocol (Cisco Proprietary)

VRRP – Virtual Router Redundancy Protocol (RFC 3768)

- Specifies an election protocol
  - Dynamically assigns responsibility for a virtual router to one of the VRRP routers on a LAN
- The Master - The VRRP router controlling the IP address(es) associated with a virtual router
  - Forwards packets sent to these IP addresses
- If the Master fails -The election process provides dynamic fail over in the forwarding responsibility
- This allows any of the virtual router IP addresses on the LAN to be used as the default first hop router by end-hosts

VRRP main profile

- Active/Standby failover mode at Layer 3
  - One nominated Master (Active router). Others in a Backup mode
- Status distribution – every one second (default value)
- ID 112 – Protocol type at the IP Header
- VRRP Multicast address- 224.0.0.18
- VRRP V3 supports IPV6

VRRP main profile

- Advantage
  - This is a Standard (not proprietary method)
  - High availability without requiring configuration of dynamic routing or router discovery protocols on every end-host
  - Some VRRP configurations are able to do a basic load sharing in the network
- Disadvantage
  - VRRP load sharing configuration cannot balance the traffic automatically when some part of network topology changes
  - VRRP should be manually reconfigured if needed
  - Hello/Hold timers in seconds (in some Cisco routers can use ms units. VRRP V3 supports ms units)

HSRP – Hot-Standby Routing Protocol (RFC 2281)

- HSRP works allowing two routers to share the same virtual IP and MAC addresses
- End devices simply send their packets to further destination through these virtual addresses, as a standard default gateway
- One of the routers, called the active router, will receive and forward the packets
- The other router, called standby router, is just tracking the state of the active router
  - it is not participating on traffic forwarding
  - one router is always active, and the other acts as a standby, switching to active role in case the first should fail
- HSRP routers sharing a virtual IP address communicate each other by sending multicast packets periodically
  - If the active router stops sending these packets for any reason, one of the standby routers will immediately take the responsibility of the IP and MAC addresses, keeping alive the traffic forwarding.

HSRP main profile

- Multicast address 224.0.0.2
- Keep alive over UDP port 1985
- Hello-time. 8 bits. Interval between hello messages. Default = 3 seconds
- Hold-time. 8 bits. Validity of hello messages. Default = 10 seconds
- Priority. 8 bits. Value used for electing active and standby routers
- Higher priority wins. In case of two routers with equal priority: the router with the higher IP address wins
- Authentication Data. 8 bytes. A password in clear text.
- Virtual IP Address. 32 bits. The virtual IP address used by this group

HSRP main profile

- Advantages of HSRP
  - Easy to configure
  - The protocol does not affect the routing tables or hosts configuration.
  - The traffic increase caused by HSRP is minimal

- Disadvantages of HSRP
  - Three second recovery time is hardly acceptable for real time traffic, such as voice over IP traffic
  - Security issues
  - HSRP is a Cisco proprietary protocol

CARP – Common Address Redundancy Protocol (OpenBSD)

- CARP has been developed after VRRP
  - VRRP has a possible overlapping with a Cisco patent
- CARP can be considered a secure and free alternative to the VRRP and HSRP
  - The CARP advertisement is protected by a SHA1 HMAC (Hash-based Message Authentication Code)
- CARP provides a backup if the default gateway fails
  - In such case, the backup device has the permission to respond instead
  - It allows some degree of configurable load sharing between systems
  - Supports both IPv4 and IPv6

CARP Mechanism

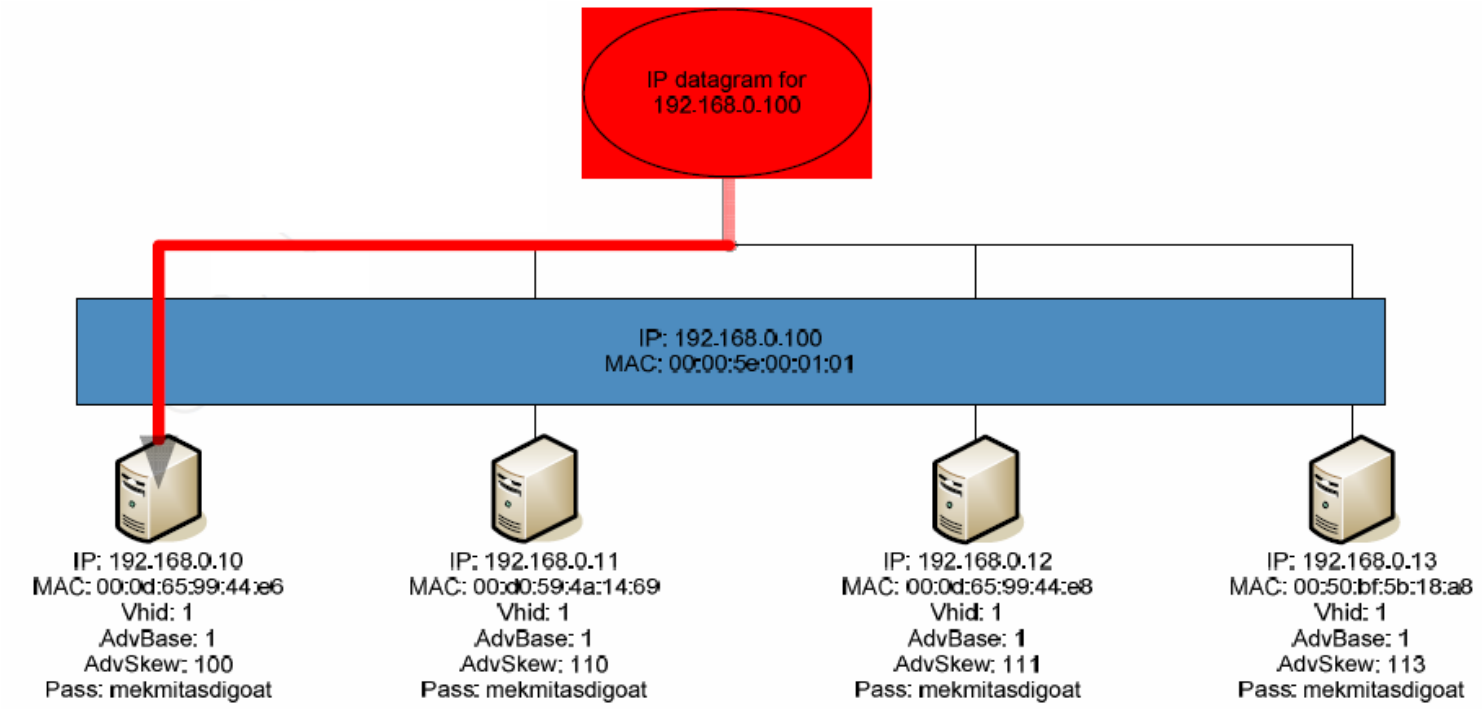
- CARP uses the technique of a virtual IP address floating around several CARP nodes
  - There is one master node and one or more slave nodes
  - The master node will always respond to request to the virtual IP address
  - The slave nodes will discard those requests
    - If the Master node is unavailable one of the salve nodes will take over
- For every setup: virtual host id, a virtual IP address and a virtual hardware address
  - For example: Virtual host id (vhid): 1 , Virtual IP: 192.168.0.100

CARP Mechanism

- Every CARP node in the cluster will have the same virtual hardware address, virtual host id and virtual IP address
- Every node needs to have 3 extra parameters to make this work
  - *Advertisement base* and *advertisement skew*
    - influence the interval by which the advertisements are sent
  - *Password* used to authenticate advertisements

CARP Mechanism

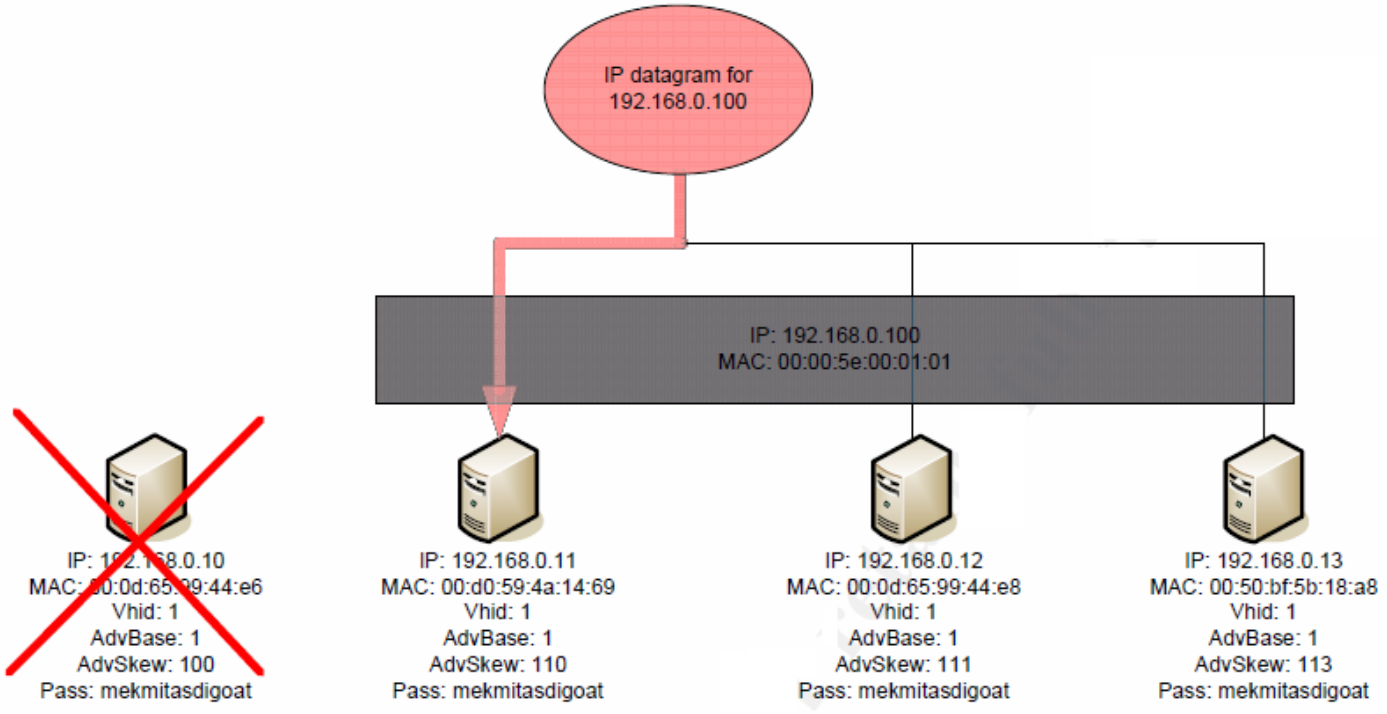
- The master node in the CARP infrastructure sends out CARP advertisements with the highest frequency.
  - This can be influenced by changing the adv base and adv skew parameters.
  - The function of the master is to reply to ARP requests for the virtual IP address with the virtual hardware address.



CARP infrastructure in a normal state

CARP Mechanism

- Every node on the infrastructure listens to the advertisements of the master node
  - checks if their advertisement interval is smaller than the one of the master
  - If for some reason the master node fails to send out advertisements, all slave nodes will notice this and will sent out an advertisement based on their own parameters
  - All the nodes will listen to the other advertisements, and the one with the highest frequency will take over the function of the master node



CARP infrastructure when master fails

CARP Mechanism

- If the original master node joins the CARP cluster again
  - It will be a slave node
- The same election procedure will start and if configured correctly, it will become the master of the CARP infrastructure again

CARP Packet Format

- A CARP packet is encapsulated in an IP datagram
  - Source address - the primary IP address of the interface through which the packet was sent
  - Destination address - the VRRP multicast address 224.0.0.18
- Similar to VRRP, the Time-To-Live value MUST always be 255
  - A CARP packet which does not use this TTL value is dropped immediately
- The protocol number used is 112 (same as VRRP)

CARP Packet Format

0 1 2 3 4 5 6 7	8 9 0 1 2 3 4 5 6 7	8 9 0 1 2 3 4 5 6 7	8 9 0 1
Version	type	vhid	advskew	authlen
pad1	advbase	chsum
counter [0]
counter [1]
md [0]	md [1]	md [2]	md [3]
. . .
md [17]	md [18]	md [19]	md [20]

CARP Packet Fields

- Version (4 bits) - The version of the CARP protocol. This is statically defined as 2
- Type (4 bits) - defines the type of CARP packet. This value can be 0x01 (advertisement) or 0x02 (leave group)
- vhid (8 bits) - Virtual host id.
- advskew (8 bits) - Advertisement skew.
- authlen (8 bits) - Size of Counter field + md field in 32 bit chunks. Statically defined as 7
- Pad1 (8 bits) - Unused, must be 0
- advbase (8 bits) - Advertisement interval
- cksum (16 bits) - Checksum
- counter (64 bits) - Two counters used for replay detection
- Md (160 bits) - SHA-1 HMAC generated with the *pass* parameter as secret key, and counter, version, type, vhid, and virtual IP address as the message digest

CARP Advantages

- CARP is designed to be free patent
- Offers good load balance features
- high security because encrypted advertisements
  - Confidentiality, Integrity and Non-repudiation
  - CARP uses a HMAC SHA-1 scheme to check the integrity and authenticity of an advertisement
  - It also protects the data in the CARP packet by using symmetric encryption and thereby preserves the confidentiality of the information about the cluster such as the virtual IP address

CARP vs. HSRP/VRRP

- The big difference between HSRP/VRRP and CARP
  - Not in the technique of virtual floating addresses
  - Supporting IPv6
  - Security control by using strong SHA-1 HMAC, and hiding the virtual IP address in the CARP advertisement

Summary

- Internetworking Devices
  - Layer 1 – Repeater
  - Layer 2 – Bridge/Switch
  - Layer 3 – Routing
  - Layer 4-7 – Gateway
- Routers keep in touch using Routing Algorithms such as RIP and OSPF
- Gateways allow connection between completely different network protocol environments
- Several protocols for high availability and load-sharing are available in the market