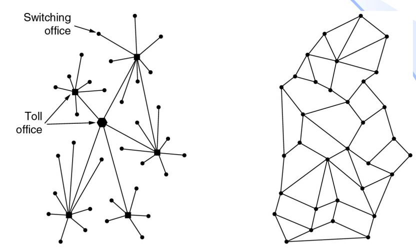
Routing Information Protocol (RIP)

Dr. Miguel Angel León Chávez

The ARPANET

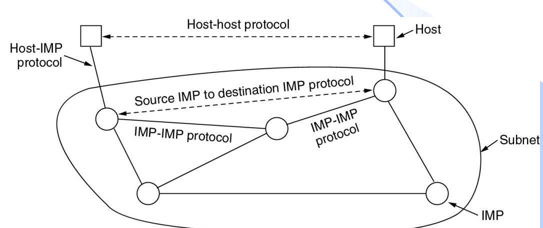
- (a) Structure of the telephone system.
- (b) Baran's proposed distributed switching system.



(a) (b)

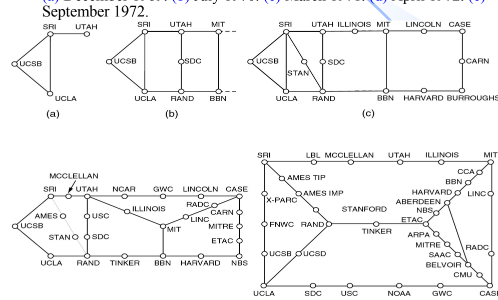
The ARPANET (2)

- The original ARPANET design.



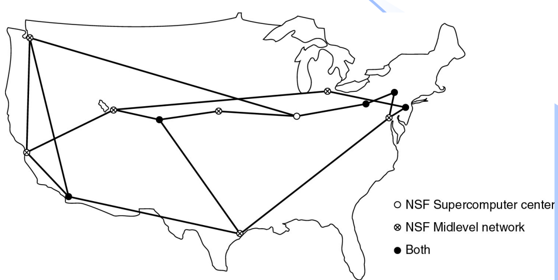
The ARPANET (3)

- Growth of the ARPANET
  - (a) December 1969. (b) July 1970. (c) March 1971. (d) April 1972. (e) September 1972.

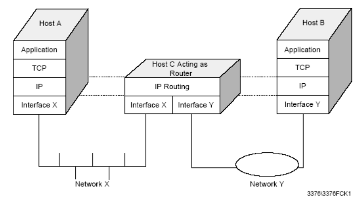


NSFNET

- The NSFNET backbone in 1988.



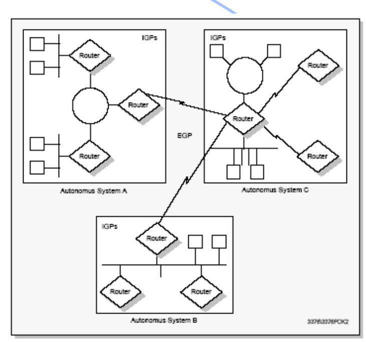
IP Routing



Routing process

- **routed**
  - Pronounced "route D." This is a basic routing daemon for interior routing supplied with the majority of TCP/IP implementations. It uses the RIP protocol
- **gated**
  - Pronounced "gate D." This is a more sophisticated daemon on UNIX-based systems for interior and exterior routing. It can employ a number of additional protocols such as OSPF and BGP

Autonomous Systems



Routing Algorithms

- **Dynamic** routing algorithms allow routers to exchange route or link information, from which the best paths to reach destinations in an internetwork are calculated.
- **Static** routing requires that routes be configured manually for each router, which constitutes one major reason why system administrators shy away from this technique if they have a choice.

Distance Vector Routing

- Each router in an internetwork maintains the distance from itself to every known destination in a distance vector table.
- Distance vector tables consist of a series of destinations (vectors) and costs (distances) to reach them and define the lowest costs to destinations at the time of transmission.
- The distances in the tables are computed from information provided by neighbor routers. Each router transmits its own distance vector table across the shared network.

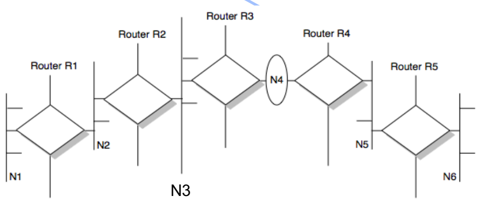
Distance Vector Routing

1. Each router is configured with an identifier and a cost for each of its network links. The cost is normally fixed at 1, reflecting a single hop, but can reflect some other measurement taken for the link such as the traffic, speed, etc.
2. Each router initializes with a distance vector table containing zero for itself, one for directly attached networks, and infinity for every other destination.
3. Each router periodically (typically every 30 seconds) transmits its distance vector table to each of its neighbors. It can also transmit the table when a link first comes up or when the table changes.

Distance Vector Routing

4. Each router saves the most recent table it receives from each neighbor and uses the information to calculate its own distance vector table.
5. The total cost to each destination is calculated by adding the cost reported to it in a neighbor's distance vector table to the cost of the link to that neighbor.
6. The distance vector table (the routing table) for the router is then created by taking the lowest cost calculated for each destination.

Distance Vector Routing



Router R2 Distance Vector Table

Net	Next Hop	Metric
N1	R1	2
N2	=	1
N3	=	1
N4	R3	2
N5	R3	3
N6	R3	4

Router R3 Distance Vector Table

Net	Next Hop	Metric
N1	R2	3
N2	R2	2
N3	=	1
N4	=	1
N5	R4	2
N6	R4	3

Router R4 Distance Vector Table

Net	Next Hop	Metric
N1	R3	4
N2	R3	3
N3	R3	2
N4	=	1
N5	=	1
N6	R5	2

3376\3376FCK3

Distance Vector Routing

- The distance vector algorithm produces a stable routing table after a period directly related to the number of routers across the network.
- This period is referred to as the **convergence time** and represents the time it takes for distance vector information to traverse the network.
- In a large internetwork, this time may become too long to be useful.
- However it is very simple to implement

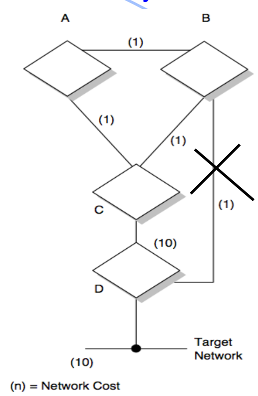
Distance Vector Routing

- Disadvantages:
  - The instability caused by old routes persisting in an internetwork
  - The long convergence time on large internetworks
  - The limit to the size of an internetwork imposed by maximum hop counts
  - The fact that distance vector tables are always transmitted even if their contents have not changed

The Count to Infinity Problem

- Counting to infinity occurs when a network becomes unreachable, but erroneous routes to that network persist because of the time for the distance vector tables to converge.

The Count to Infinity Problem example



The Count to Infinity Problem example

- Each of the routers A, B, C and D has routes to all networks. If we show only the routes to the target network, we will see they are as follows:
  - For D : Directly connected network. Metric 1.
  - For B : Route via D. Metric 2.
  - For C : Route via B. Metric 3.
  - For A : Route via B. Metric 3.
- If the link from B to D fails, then all routes will be adjusted in time to use the link from C to D.
- However, the convergence time for this can be considerable.

The Count to Infinity Problem example

Time ⇒ ⇒

D:	Direct	1	Direct	1	Direct	1	Direct	1	....	Direct	1	Direct	1
B:	Unreachable		C	4	C	5	C	6		C	11	C	12
C:	B	3	A	4	A	5	A	6		A	11	D	11
A:	B	3	C	4	C	5	C	6	....	C	11	C	12

3376\3376FCK5

The Count to Infinity Problem example

1. Initially A and C have a route to D via B.
2. Link from D to B fails.
3. A and C then send updates based on the route to D via B even after the link has failed.
4. B then believes it has a route to D via either A or C. But, in reality it does not have such a route, as the routes are vestiges of the previous route via B, which has failed.
5. A and C then see that the route via B has failed, but believe a route exists via one another.

The Count to Infinity Problem

- Slowly the distance vector tables converge, but not until the metrics have counted up, in theory, to infinity.
- To avoid this happening, practical implementations of distance vector have a low value for infinity; for example, RIP uses a maximum metric of 16.
- The manner in which the metrics increment to infinity gives rise to the term counting to infinity.

Routing Information Protocol (RIP)

- RFCs 1058, 1388, 1723
- RIP is based on the Xerox PUP and XNS routing protocols
- RIP is a distance vector routing protocol suitable for small networks
- RIP-1 and RIP-2
- RIP is very widely used because the code was incorporated on the Berkeley Software Distribution (BSD) UNIX operating system

RIP

- RIP sends and receives datagrams using UDP port 520.
- RIP datagrams have a maximum size of 512 octets and tables larger than this must be sent in multiple datagrams.
- RIP datagrams are normally broadcast onto LANs using the LAN MAC all-stations broadcast address and the IP network or subnetwork broadcast address. They are specifically addressed on point-to-point and multi-access non-broadcast networks, using the destination router IP address.

RIP

- RIP specifies two packet types: request and response.
  - A request packet is sent by routers to ask neighbors to send part of their distance vector table (if the packet contains destinations), or all their table (if no destinations have been specified).
  - A response packet is sent by routers to advertise their distance vector table in the following circumstances:
    - Every 30 seconds
    - In response to a request packet
    - When distance vector tables change (if triggered updates are supported)

RIP packet format for IP

Number of Octets	Field	
1	Command	Request = 1 Response = 2
1	Version	Version = 1
2	Reserved	
2	2	Address Family Identifier for IP
2	Reserved	May be Repeated
4	IP Address	
8	Reserved	
4	Metric	

3376\3376FCK8

RIP-2

- RFCs 1723, 2453
- It has the advantages of easy implementation and lower overheads.

RIP-2 packet

Number of Octets	Field	
1	Command	Request = 1 Response = 2
1	Version	
2	Reserved	
2	X'FFFF'	
2	Authentic Type	0 = No Authentication 2 = Password Data
16	Authentication Data	Password if Type 2 Selected
2	2	May be Repeated
2	Reserved	
4	IP Address	
4	Subnet Mask	
4	Next Hop	
4	Metric	

3376\3376FCKZ

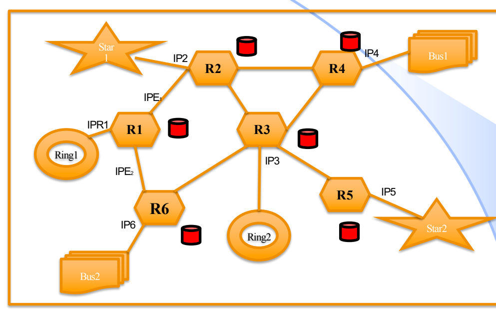
RIP-2 packet

- **Version** is 2.
  - This tells RIP-1 routers to ignore the fields designated as must be zero.
- **Address Family**
  - May be X'FFFF' in the first entry only, indicating that this entry is an authentication entry.
- **Authentication Type**
  - Defines how the remaining 16 bytes are to be used. The only defined types are 0 indicating no authentication and 2 indicating that the field contains password data.
- **Authentication Data**
  - The password is 16 bytes, plain text ASCII, left adjusted and padded with ASCII NULLs (X'00').

RIP-2 packet

- **Route Tag**
  - Is a field intended for communicating information about the origin of the route information. It is intended for interoperation between RIP and other routing protocols. RIP-2 implementations must preserve this tag, but RIP-2 does not further specify how it is to be used.
- **Subnet Mask**
  - The subnet mask associated with the subnet referred to by this entry.
- **Next Hop**
  - A recommendation about the next hop that the router should use to send datagrams to the subnet or host given in this entry.

Práctica - RIP



IP1 ≠ IP2 ≠ … IP6

Clase B

References

- Murhammer, M. W., O. Atakan, S. Bretz, L. R. Pugh, K. Suzuki, D. H. Wood. *TCP/IP Tutorial and Technical Overview*, IBM, 1998.
- Tanenbaum, A.S. *Computer Networks*, Ed. PEARSON, 5th Edition, 2012.