Group work

- Group list and topics to be submitted by Fri 27th Jan
- Topics available from today on the webpage http://www.dsg.cs.tcd.ie/~reynoldv/4BA2
- 3 people per group
- To be submitted on the 17th Feb
- Email your chosen <topic, group members> to me at vinny.reynolds@cs.tcd.ie before tomorrow evening.
- + 2 other topics..

Groups

Webpage
Keith Mahony
Antonio Karpova
Andy Phillips

Analysis of IP version suitability for various application domains
Conal O’ Brien
Brian Brazil
David Collins

-
Karen Molony
David Roche
Kevin Williams

Topics

- Phone based location services
- Decentralised load balancing in P2P networks
- Evolution of P2P technologies
- Search in decentralised P2P systems
- Peer to Peer streaming technologies
- Power efficiency in sensor networking
- Interplanetary networking
- Role of ATM in todays internet
- Game networking middleware
- Music recommendation systems
- DRM technologies
- Civil liberties in DRM
- Web censorship
- Modern spam analysis
- RFID's
- Evolution of AI in Gamebots

Internet Control Message Protocol

- ICMP is a separate protocol that uses IP to transport messages
  - But part of the internet protocol suite
- Integral part of IP; all IP modules *must* support ICMP
  - ICMPv4, ICMPv6
- ICMP does not guarantee delivery
- Necessary to inspect the contents at the IP layer
  - Delivery to application
- Two general types of ICMP messages:

- Information messages, e.g. if a host is alive

- Error indication messages, e.g. if a router had to drop a datagram

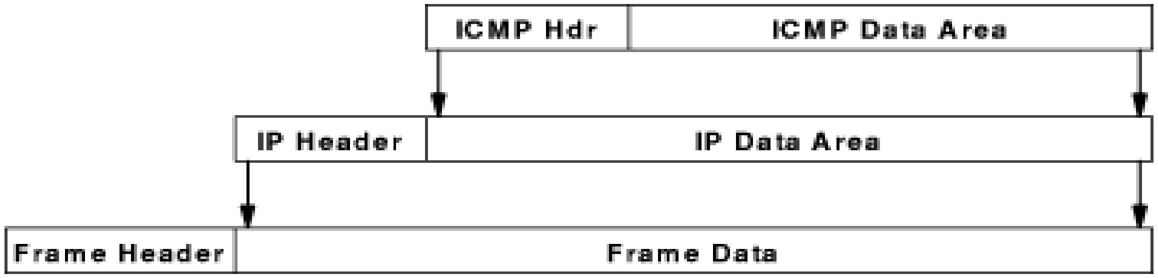
- Purpose: Feedback about problems, *not* to make IP reliable

ICMP Messages

- Source quench: Routers that run out of buffer space to sender to reduce rate
- Time exceeded: TTL reduced to zero, expiration of reassembly timer
- Destination unreachable: Routers that cannot deliver a datagram, host or network
- Redirect: Routers to suggest route changes
- Parameter problem: Datagram parameter incorrect
- Echo request/reply: Reply carries request
- Others….

ICMP Message Transport

- Datagrams carrying ICMP messages do not have special priority
- If a datagram carrying an ICMP *error* message causes an error, no error message is sent



ICMP Applications

- Ping:

 - Sends out ICMP echo packets and counts how long it takes to receive an ICMP echo reply

 - Then displays the minimum, maximum, and average time it takes to ``ping'' the destination

- Traceroute:

 - Sends out a packet with TTL set to 1

 - The first hop that receives the packet decrements TTL to 0 and sends an ICMP TTL exceeded message to the sender

 - Traceroute displays the IP address of the hop that sent the TTL exceeded message and the amount of time it took for the message to be received

 - Traceroute then sends out a packet with TTL set to 2 and the process continues

 - Eventually the destination is reached or the maximum TTL is reached (usually 30)

ICMP Attacks (1/2)

- Inverse mapping:

- Step 1: Attacker sends an ICMP reply message to a range of IP addresses presumably behind a filtering device

- Step 2: Upon receiving the series of ICMP reply messages, since the filtering device does not keep state of the list of ICMP requests, it will allow these packets to reach their destination

- Step 3: If there is an internal router, the router will respond with a ICMP host unreachable for every host that it cannot reach, thus giving the attacker knowledge of all hosts which are present behind the filtering device

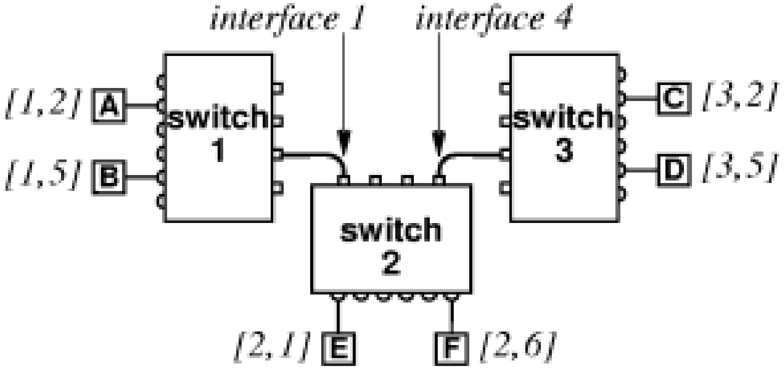
ICMP Attacks (2/2)

- Smurf attack:

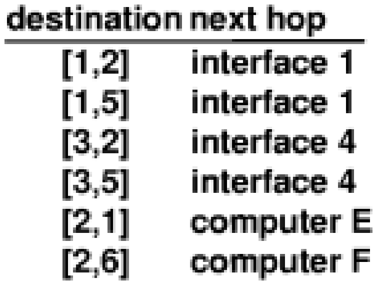
  - Step 1: Attacker finds some network(s) that will respond to the network's broadcast address
  - Step 2: Attacker spoofs the IP address of the victim host and sends a great number of ICMP echo request packets to the broadcast address of the above network(s)
  - Step 3: Now all the hosts on that network will respond to that ICMP echo request with a corresponding ICMP reply request back to the spoofed IP address (the victim)
  - Step 4: This will send a whole bunch of ICMP echo replies to the victim and its network thus causing congestion and even total denial of service

Next-hop Forwarding

- Performed by packet switch
- Uses table of routes
- Table gives *next hop* for each destination
- Source independence



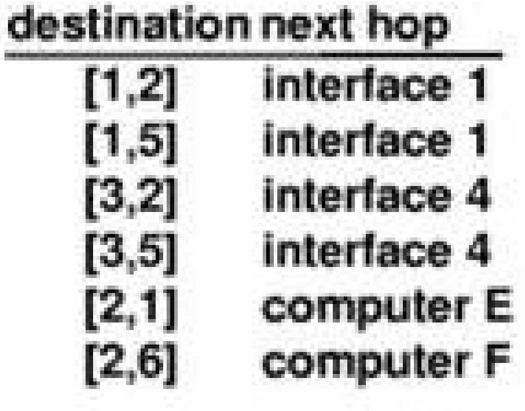
(a)



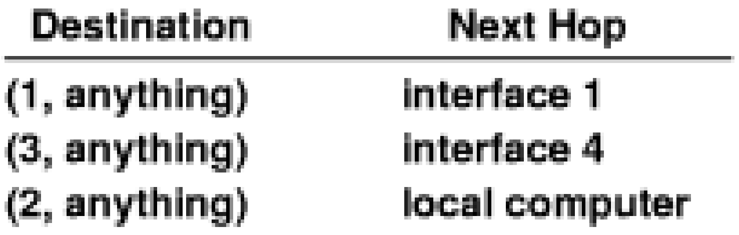
destination	next hop
[1,2]	interface 1
[1,5]	interface 1
[3,2]	interface 4
[3,5]	interface 4
[2,1]	computer E
[2,6]	computer F

(b)

Forwarding Table Abbreviations



destination	next hop
[1,2]	interface 1
[1,5]	interface 1
[3,2]	interface 4
[3,5]	interface 4
[2,1]	computer E
[2,6]	computer F



Destination	Next Hop
(1, anything)	interface 1
(3, anything)	interface 4
(2, anything)	local computer

- Many entries point to same next hop
- Can be condensed; one entry per destination switch instead of one entry per destination computer

- Improves lookup efficiency

- Smaller table (reduction very important in WAN switches)

- Default route (same next-hop value)

Source of Routing Table Information

- Manual

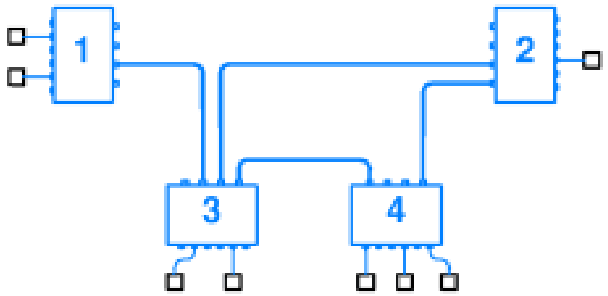
  - Table created off-line by hand
  - Useful in small networks
  - Useful if routes never change

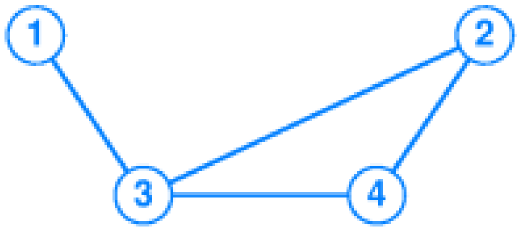
- Automatic routing

  - Software creates/updates table at run-time
  - Needed in large, dynamic networks
  - Changes routes when failures occur

    * Or in mobility scenarios (e.g. in ad hoc networks)

Relationship to Graph Theory





destin- ation	next hop
1	-
2	(1,3)
3	(1,3)
4	(1,3)

node 1

destin- ation	next hop
1	(2,3)
2	-
3	(2,3)
4	(2,4)

node 2

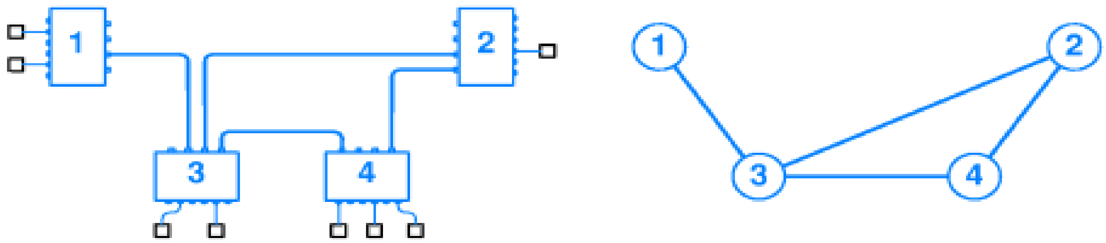
destin- ation	next hop
1	(3,1)
2	(3,2)
3	-
4	(3,4)

node 3

destin- ation	next hop
1	(4,3)
2	(4,2)
3	(4,3)
4	-

node 4

Compressed Routing Table



destination	next hop
1	-
2	(1,3)
3	(1,3)
4	(1,3)

node 1

destination	next hop
1	(2,3)
2	-
3	(2,3)
4	(2,4)

node 2

destination	next hop
1	(3,1)
2	(3,2)
3	-
4	(3,4)

node 3

destination	next hop
1	(4,3)
2	(4,2)
3	(4,3)
4	-

node 4

destination	next hop
1	-
*	(1,3)

node 1

destination	next hop
2	-
4	(2,4)
*	(2,3)

node 2

destination	next hop
1	(3,1)
2	(3,2)
3	-
4	(3,4)

node 3

destination	next hop
2	(4,2)
4	-
*	(4,3)

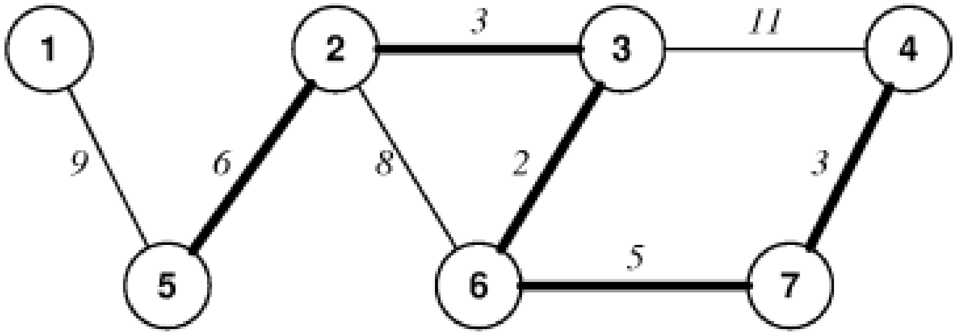
node 4

Shortest Path Computation

- Algorithms from graph theory
- No central authority (distributed computation)
- A switch:

  - Must learn route to each destination
  - Only communicates with directly connected neighbors

Illustration of Minimum Weight Path



- Label on edge represents ``distance’’
- Possible distance measure:

 - Geographic distance

 - Economic cost

 - Inverse of capacity

- Darkened path is the minimum weight path from 4 to 5

Algorithms for Computing Shortest Paths

- Distance Vector (DV)

 - Switches exchange information in their routing tables

- Link-state

 - Switches exchange link status information

- Both used in practice

Distance Vector

- Periodic, neighboring switches engage in two-way exchange of information
- During exchange, sender switch sends:

 - List of pairs

 - Each pair gives (destination, distance)

- Each Receiver:

 - Compares each item in list to local routes

 - Changes if better path exists

- Cost of the route is based on number of hops (number of routers to pass)
- Recalculation occurs when links fail

Distance Vector Algorithm

- Let

- *N* = neighbor that sent the routing message containing the pair (V,D) where:

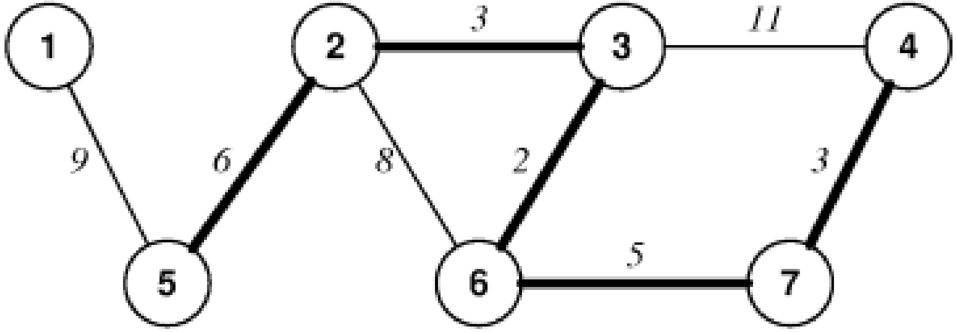
  * *V* = destination in a pair

  * *D* = distance in a pair

  * *C* = *D* + the cost to reach the sender (N)

- If no local route to *V* exists or local route has cost greater than *C*, install a route with next hop *N* and cost *C*
- Else ignore pair

Distance Vector Example



- Consider transmission of one DV message
- Node 2 sends to 3, 5, and 6
- Node 6 installs cost 8 route to 2
- Later 3 sends update to 6
- 6 changes route to make 3 the next hop for destination 2