Computer Networks (CS425)

Instructor: Dr. Dheeraj Sanghi

Prev| Next| Index

ARP,RARP,ICMP Protocols

Address Resolution Protocol

If a machine talks to another machine in the same network, it requires its physical or MAC address. But ,since the application has given the destination's IP address it requires some mechanism to bind the IP address with its MAC address.This is done through Address Resolution protocol (ARP).IP address of the destination node is broadcast and the destination node informs the source of its MAC address.

1. Assume broadcast nature of LAN
2. Broadcast IP address of the destination
3. Destination replies it with its MAC address.
4. Source maintains a cache of IP and MAC address bindings

But this means that every time machine A wants to send packets to machine B, A has to send an ARP packet to resolve the MAC address of B and hence this will increase the traffic load too much, so to reduce the communication cost computers that use ARP maintains a cache of recently acquired IP_to_MAC address bindings, i.e. they dont have to use ARP repeatedly. ARP Refinements Several refinements of ARP are possible: When machine A wants to send packets to macine B, it is possible that machine B is going to send packets to machine A in the near future.So to avoid ARP for machine B, A should put its IP_to_MAC address binding in the special packet while requesting for the MAC address of B. Since A broadcasts its initial request for the MAC address of B, every machine on the network should extract and store in its cache the IP_to_MAC address binding of A When a new machine appears on the network (e.g. when an operating system reboots) it can broadcast its IP_to_MAC address binding so that all other machines can store it in their caches. This will eliminate a lot of ARP packets by all other machines, when they want to communicate with this new machine.

Example displaying the use of Address Resolution Protocol:

Consider a scenario where a computer tries to contact some remote machine using ping program, assuming that there has been no exchange of IP datagrams previously between the two machines and therefore arp packet must be sent to identify the MAC address of the remote machine.
The arp request message (who is A.A.A.A tell B.B.B.B where the two are IP

addresses) is broadcast on the local area network with an Ethernet protocol type 0x806. The packet is discarded by all the machines except the target machine which responds with an arp response message (A.A.A.A is hh:hh:hh:hh:hh:hh where hh:hh:hh:hh:hh:hh is the Ethernet source address). This packet is unicast to the machine with IP address B.B.B.B. Since the arp request message included the hardware address (Ethernet source address) of the requesting computer, target machine doesn't require another arp message to figure it out.

Reverse Address Resolution Protocol

RARP is a protocol by which a physical machine in a local area network can request to learn its IP address from a gateway server's Address Resolution Protocol table or cache. This is needed since the machine may not have permanently attacded disk where it can store its IP address permanently. A network administrator creates a table in a local area network's gateway router that maps the physical machine (or Medium Access Control - MAC) addresses to corresponding Internet Protocol addresses. When a new machine is set up, its RARP client program requests from the RARP server on the router to be sent its IP address. Assuming that an entry has been set up in the router table, the RARP server will return the IP address to the machine which can store it for future use.

Detailed Mechanism

Both the machine that issues the request and the server that responds use physical network addresses during their brief communication. Usually, the requester does not know the physical address. So, the request is broadcasted to all the machines on the network. Now, the requester must identify istelf uniquely to the server. For this either CPU serial number or the machine's physical network address can be used. But using the physical address as a unique id has two advantages.

- These addresses are always available and do not have to be bound into bootstrap code.
- Because the identifying information depends on the network and not on the CPU vendor, all machines on a given network will supply unique identifiers.

Request:
Like an ARP message, a RARP message is sent from one machine to the another encapsulated in the data portion of a network frame. An ethernet frame carrying a RARP request has the usual preamle, Ethernet source and destination addresses, and packet type fields in front of the frame. The frame conatins the value 8035 (base 16) to identify the contents of the frame as a RARP message. The data portion of the frame contains the 28-octet RARP message. The sender braodcasts a RARP request that specifies itself as both the sender and target machine, and supplies its physical network address in the target hardware address field. All machines on the network receive the request, but only those authorised to supply the RARP services process the

request and send a reply, such machines are known informally as RARP servers. For RARP to succeed, the network must contain at least one RARP server.
Reply:
Servers answers request by filling in the target protocol address field, changing the message type from request to reply, and sending the reply back directly to the machine making the request.

Timing RARP Transactions
Since RARP uses the physical network directly, no other protocol software will time the response or retransmit the request. RARP software must handle these tasks. Some workstations that rely on RARP to boot, choose to retry indefinitely until the receive a response. Other implementations announce failure after only a few tries to avoid flooding the network with unnecessary broadcast.

Mulitple RARP Servers
Advantage: More reliability. Diadvantage: Overloading may result when all servers respond. So, to get away with disadvantage we have primary and secondary servers. Each machine that makes RARP request is assigned a primary server. Normally, the primary server responds but if it fails, then requester may time out and rebroadcast the request.Whenever a secondary server receives a second copy of the request within a short time of the first, it responds. But, still there might be a problem that all secondary servers respond, thus overloading the network. So, the solution adopted is to avoid having all secondary servers transmit responses simultaneously. Each secondary server that receives the request computes a random delay and then sends a response.

Drawbacks of RARP

- Since it operates at low level, it requires direct addresss to the network which makes it difficult for an application programmer to build a server.
- It doesn't fully utilizes the capability of a network like ethernet which is enforced to send a minimum packet size since the reply from the server contains only one small piece of information, the 32-bit internet address.

RARP is formally described in RFC903.

ICMP Internet Control Message Protocol

This protocol discusses a mechanism that gateways and hosts use to communicate control or error information.The Internet protocol provides unreliable,connectionless datagram service,and that a datagram travels from gateway to gateway until it reaches one that can deliver it directly to its final destination. If a gateway cannot route or deliver a datagram,or if the gateway detects an unusual condition, like network congestion, that affects its ability to forward the datagram, it needs to instruct the original source to take action to avoid or correct the problem. The Internet Control Message Protocol allows gateways to send error or control messages to other gateways or hosts;ICMP provides communication between the Internet Protocol software on one machine and the Internet Protocol software on another. This is a special purpose message mechanism added by the designers to the TCP/IP protocols. This is to allow gateways in an internet to report errors or provide information about unexpecter circumstances. The IP protocol itself contains nothing to help the sender test connectivity or learn about failures.

Error Reporting vs Error Correction

ICMP only reports error conditions to the original source; the source must relate errors to individual application programs and take action to correct problems. It provides a way for gateway to report the error It does not fully specify the action to be taken for each possible error. ICMP is restricted to communicate with the original source but not intermediate sources.

ICMP Message Delivery

ICMP messages travel across the internet in the data portion of an IP datagram,which itself travels across the internet in the data portion of an IP datagram,which itself travels across each physical network in the data portion of a frame.Datagrams carryin ICMP messages are routed exactly like datagrams carrying information for users;there is no additional reliability or priority.An exception is made to the error handling procedures if an IP datagram carrying an ICMP messages are not generated for errors that result from datagrams carrying ICMP error messages.

ICMP Message Format

It has three fields;an 8-bit integer message TYPE field that identifies the message,an 8-bit CODE field that provides further information about the message type,and a 16-bit CHECKSUM field(ICMP uses the same additive checksum algorithm as IP,but the ICMP checksum only covers the ICMP message).In addition , ICMP messages that report errors always include the header and first 64 data bits of the datagram causing the problem. The ICMP TYPE field defines the meaning of the message as well as its format.

The Types include :

TYPE FIELD	**ICMP MESSAGE TYPE**
0	ECHO REPLY
3	DESTINATION UNREACHABLE
4	SOURCE QUENCH
5	REDIRECT(CHANGE A ROUTE)
8	ECHO REQUEST
11	TIME EXCEEDED FOR A DATAGRAM
12	PARAMETER PROBLEM ON A DATAGRAM
13	TIMESTAMP REQUEST
14	TIMESTAMP REPLY
15	INFORMATION REQUEST(OBSOLETE)
16	INFORMATION REPLY(OBSOLETE)
17	ADDRESS MASK REQUEST
18	ADDRESS MASK REPLY TESTING

DESTINATION

Reachabilty and Status :
TCP/IP protocols provide facilities to help network managers or users identify network problems.One of the most frequently used debugging tools invokes the ICMP echo request and echo reply messages.A host or gateway sends an ICMP echo request message to a specified destination.Any machine that receives an echo request formulates an echo reply and returns to the original sender.The request contains an optional data area; the reply contains a copy of the data sent in the request.The echo request and associated reply can be used to test whether a destination is reachable and responding.Because both the request and reply travel in IP datagrams,successful receipt of a reply verifies that major pieces of the transport system work.
1.1 : IP software on the source must route the datagram
2.2 : Intermediate gateways between the source and destination must be operating and must route datagram correctly.
3.3 : The destination machine must be running , and both ICMP and IP software must be working.
4.4 : Routes in gateways along the return path must be correct.

Echo Request and Reply
The field listed OPTIONAL DATA is a variable length field that contains data to be returned to the sender.An echo reply always returns exactly the same data as was received in the request.Fields IDENTIFIER and SEQUENCE NUMBER are used by the sender to match replies to request.The value of the TYPE field specifies whether the message is a request(8) or a reply(0).

Reports of Unreachable Destinations
The Code field in a destination unreachable message contains an integer that further describes th problem.Possible values are :

CODE VALUE	**MEANING**
0	NETWORK UNREACHABLE
1	HOST UNREACHABLE
2	PROTOCOL UNREACHABLE
3	PORT UNREACHABLE
4	FRAGMENTATION NEEDED AND DF SET
5	SOURCE ROOT FAILED
6	DESTINATION NETWORK UNKNOWN
7	DESTINATION HOST UNKNOWN
8	SOURCE HOST ISOLATED
9	COMMUNICATION WITH DESTINATION NETWORK ADMINISTRATIVELY PROHIBITED
10	COMMUNICATION WTTH DESTINATION HOST ADMINISTRATIVELY PROHIBITED
11	NETWORK UNREACHABLE FOR TYPE OF SERVICE
12	HOST UNREACHABLE FOR TYPE OF SERVICE

Whenever an error prevents a gateway from routing or delivering a datagram, the gateway sends a destination unreachable message back to the source and then drops the datagram.Network unreachable errors usually imply roting failures ; host unreachable errors imply delivery failures.Because the message contains a short prefix of the datagram that caused the problem, the source will know exactly which address is unreachable. Destinations may be unreachable because hardware is temporarily out of service, because the sender specified a nonexistent destination address, or because the gateway does not have a route to the destination network. Although gateways send destination unreachable messages if they cannot route or deliver datagrams, not all such errors can be detected.If the datagram contains the source route option with an incorrect route, it may trigger a source route failure message.If a gateway needs to fragment adatagram but the "don't fragment" bit is set, the gateway sends a fragmentation needed message back to the source.

Congestion and Datagram Flow Control :
Gateways cannot reserve memory or communication resources in advance of receiving datagrams because IP is connectionless. The result is, gateways can overrun with traffic, a condition known as congestion.Congestion arises due to two reasons :

1. A high speed computer may be able to generate traffic faster than a network can transfer it .
2. If many computers sumultaneously need to send datagrams through a single gateway , the gateway can experience congestion, even though no single source causes the problem.

When datagrams arrive too quickly for a host or a gateway to process, it enqueues them in memory temporarily.If the traffic continues, the host or gateway eventually exhausts menory ans must discard additional datagrams that arrive. A machine uses ICMP source quench messages to releive congestion. A source quench message is a request for the source to reduce its current rate of datagram transmission.
There is no ICMP messages to reverse the effect of a source quench.
Source Quench :
Source quench messages have a field that contains a datagram prefix in addition to the usual ICMP TYPE,CODE,CHECKSUM fields.Congested gateways send one source quench message each time they discard a datagram; the datagram prefix identifies the datagram that was dropped.

Route Change Requests From Gateways :
Internet routing tables are initialized by hosts from a configuration file at system startup, and system administrators seldom make routing changes during normal operations.Gateways exchange routing information periodically to accomadate network changes and keep their routes up-to-date.The general rule is , Gateways are assumed to know correct routes; host begin wint minimal routing information and learn new routes from gateways.
The GATEWAY INTERNET ADDRESS field contains the address of a gateway that the host is to use to reach the destination mentioned in the datagram header. The INTERNET HEADER field contains IP header plus the next 64 bits of the datagram that triggered the message.The CODE field of an ICMP

redirect message further specifies how to interpret the destination address, based on values assigned as follows :

Code Value	Meaning
0	REDIRECT DATAGRAMS FOR THE NET
1	REDIRECT DATAGRAMS FOR THE HOST
2	REDIRECT DATAGRAMS FOR THE TYPE OF SERVICE AND NET
3	REDIRECT DATAGRAMS FOR THE TYPE OF SERVICE AND HOST

Gateways only send ICMP redirect requests to hosts and not to other gateways.

Detecting Circular or Excessively Long Routes :
Internet gateways compute a next hop using local tables, errors in routing tables can produce a routing cycle for some destination. A routing cycle can consist of two gateways that each route a datagram for a particular destination to other, or it can consist of several gateways.To prevent datagrams from circling forever in a TCP/IP internet, each IP datagram contains a time-to-live counter , sometimes called a hop count. A gateway decrements the time-to-live counter whenever it processes the datagram and discards the datagram when the count reaches zero. Whenever a gateway discards a datagram because its hop count has reached zero or because a timeout occured while waiting for fragments of a datagram ,it sends an ICMP time exceeded message back to the datagram's source, A gateway sends this message whenever a datagram is discarded because the time-to-live field in the datagram header has reached zero or because its reassembly timer expired while waiting for fragments.
The code field explains the nature of the timeout :

Code Value	Meaning
0	TIME-TO-LIVE COUNT EXCEEDED
1	FRAGMENT REASSEMBLY TIME EXCEEDED

Fragment reassembly refers to the task of collecting all the fragments from a datagram.

Reprting Other Problems :
When a gateway or host finds problems with a datagram not covered by previous ICMP error messages it sends a parameter problem message to the original source.To make the message unambigous, the sender uses the POINTER field in the message header to identify the octet in the datagram that caused the problem. Code 1 is used to report that a required option is missing; the POINTER field is not used for code 1.

Clock Synchronization nd Transmit the estimation :
ICMP messages are used to obtain the time from another machine.A requesting machine sends an ICMP timestamp request message to another machine, asking that the second machine return its current value of the time of day. The receiving machine returns a timestamp reply back to the machine making the request. TCP/IP protocol suite includes several protocols that can be used to synchronize clocks. This is one of the simplest techniques used by

TCP/IP. The TYPE field idintifies the message as a request (13) or a reply (14); the IDENTIFIER and SEQUENCE NUMBER fields are used by the source to associate replies with requests.The ORIGINATE TIMESTAMP filed is filled in by the original sendet just before the packet is transmitted, the RECEIVE TIMESTAMP field is filled immediately upon receipt of a request, and the TRANSMIT TIMESTAMP field is filled immediately before the reply is transmitted. Hosts use the three timestamp fields to compute estimates of the delay time between them and to synchronize their clock.A host can compute the total time required for a request to travel to a destination, be transformed into a reply, and return. In practice, accurate estimation of round-trip delay can be difficult and substantially restirct the utility of ICMP timestanp messages.To obtain an accurate estimate to round trip delay one must take many measurements and average them.

Obtaining a Subnet Mask:

Subnet addressing is used by the hosts to extract some bits in the hostid portion of their IP address to identify a physical network.To participate in subnet addressing, hosts need to know which bits of the 32-bit internet address correspond to the physical network and which correspond to host identifiers. The information needed to interpret the address is represented in a 32-bit quatity called the subnet mask. To learn the subnet mask used for the local network, a machine can send an address mask request message to a gateway and receive an address mask reply. The TYPE field in an address mask message specifies whether the message is a request (17) or a reply (18). A reply contains the nework's subnet address mask in the ADDRESS MASK field.The IDENTIFIER and SEQUENCE NUMBER fields allow a machine to associate replies with requests.

back to top
Prev| Next | Index