Address Resolution Protocol (ARP)

In computer networking using the internet protocol suite, the Address Resolution Protocol is a method for finding a host's Ethernet (MAC) address from its IP address. The sender broadcasts an ARP packet containing the Internet address of another host and waits for it (or some other host) to send back its Ethernet address. Each host maintains a cache of address translations to reduce delay and loading. ARP allows the Internet address to be independent of the Ethernet address but it works only if all hosts support it.

ARP is defined in RFC 826.

The alternative for hosts that do not do ARP is to use a pre-configured mapping of IP addresses to MAC addresses.

Variants of the ARP protocol

ARP was not originally designed as an IP-only protocol, even though it is in practice used almost exclusively to resolve IP addresses to MAC addresses.

ARP can be used to resolve MAC addresses for many different Layer 3 protocols. ARP has also been adapted to resolve other kinds of Layer 2 addresses; for example, ATMARP is used to resolve ATM NSAP addresses in the Classical IP over ATM protocol.

Border Gateway Protocol (BGP)

The Border Gateway Protocol (BGP) is the core routing protocol of the Internet. It works by maintaining a table of IP networks or 'prefixes' which designate network reachability between autonomous systems (AS). It is described as a path vector protocol. BGP does not use technical metrics, but makes routing decisions based on network policies or rules. The current version of BGP, BGP version 4, is specified in request for comment RFC 1771.

BGP supports classless interdomain routing and uses route aggregation to decrease the size of routing tables. Since 1994, version four of the protocol has been in use on the Internet; all previous versions are considered obsolete.

BGP was created to replace the EGP routing protocol to allow fully decentralized routing in order to allow the removal of the NSFNET Internet backbone network. This allowed the Internet to become a truly decentralized system.

Very large private IP networks can also make use of BGP; an example would be the joining of a number of large OSPF networks where OSPF by itself would not scale to size. Another reason to use BGP would be multihoming a network for better redundancy.

Most Internet users do not use BGP directly. However, since most Internet service providers must use BGP to establish routing between one another, it is one of the most important protocols of the Internet. Compare and contrast this with Signalling System 7, which is the inter-provider core call setup protocol on the PSTN.

BGP operation

BGP neighbours, or peers, are established by manual configuration between routers to create a TCP session on port 179, BGP speaker will periodically, every 60 seconds by default, send 19-byte keepalive messages to maintain the connection. Among routing protocols, BGP is unique in using TCP as its transport protocol.

When BGP is running inside an AS, it is referred to as Internal BGP (IBGP Interior Border Gateway Protocol). When BGP runs between autonomous systems, it is called External BGP (EBGP Exterior Border Gateway Protocol). If the role of a BGP router is to route IBGP traffic, it is called a transit router. Routers that sit on the boundary of an AS and that use EBGP to exchange information with the ISP are called border or edge routers.

All routers within a single AS and participating in BGP routing must be configured in a full mesh: each router must be configured as peer to every other router. This causes obvious scaling problems, since the number of required connections grows quadratically with the number of routers involved. To get around this, two solutions are built into BGP: route reflectors (RFC 2796) and confederations (RFC 3065).

Route reflectors reduce the number of connections required in an AS. A single router (or two for redundancy) can be made a route reflector: other routers in the AS need only be configured as peer to them.

Confederations are used in very large networks where a large AS can be configured to encompass smaller more manageable internal ASs. Confederations can be used in conjunction with route reflectors.

BGP problems and mitigation

Routing table growth

One of the largest problems faced by BGP, and indeed the Internet infrastructure as a whole, comes from the growth of the Internet routing table. If the global routing table grows to the point where some older, less capable, routers cannot cope with the memory requirements or the CPU load of maintaining the table, these routers will cease to be effective gateways between the parts of the Internet they connect. In addition, and perhaps even more importantly, larger routing tables take longer to stabilize (see above) after a major connectivity change, leaving network service unreliable, or even unavailable, in the interim.

Until 2001, the global routing table was growing exponentially, threatening an eventual widespread breakdown of connectivity. In an attempt to prevent this from happening, there is now a cooperative effort by ISPs to keep the global routing table as small as possible, by using CIDR and route aggregation. This has slowed the growth of the routing table to a linear process, greatly extending the time available before older routers need to be replaced.

BOOTP

In computing, BOOTP, short for Bootstrap Protocol, is a UDP network protocol used by a network client to obtain its IP address automatically. It is usually done in booting process of computers or operating systems running on them. The BOOTP servers assign the IP-address from a pool of addresses to each client. It was originally defined in RFC 951.

This protocol enables 'diskless workstation' computers to obtain an IP address prior to loading any advanced operating system. Historically, it has been used for UNIX-like diskless workstations (which also obtained the location of their boot image using this protocol) and also by Corporations to 'roll out' a pre-configured Windows installation to newly purchased PCs (typically in a Windows NT network environment).

Originally requiring the use of a boot floppy disk to establish the initial network connection, the protocol became embedded in the BIOS of some Network cards themselves (such as 3c905c) and in many modern Motherboards thus allowing direct Network Booting.

Recently those with an interest in diskless stand-alone media center PCs have shown new interest in this method of booting a Windows Operating System (see eg. Personal Computer World, Feb 2005, pg 156 'Putting the Boot in').

DHCP (Dynamic Host Configuration Protocol) is a more advanced protocol based on BOOTP, but is far more complex to implement. Most DHCP servers also offer BOOTP support. The introduction of duration based leases is the fundamental addition found in DHCP, hence the use of Dynamic in the name of the protocol.

Classless Inter-Domain Routing

Classless Inter-Domain Routing (CIDR), introduced starting in 1993, is the latest refinement to the way IP addresses are interpreted. It replaced the previous generation of IP address syntax, classful networks. It allowed increased flexibility when dividing ranges of IP addresses into separate networks. It thereby promoted:
More efficient use of increasingly scarce IPv4 addresses.
Greater use of hierarchy in address assignments (prefix aggregation), lowering the overhead of the Internet-wide routing.

Background

IP addresses are separated into two parts: the network address (which identifies a whole network or subnet), and the host address (which identifies a particular machine's connection or interface to that network). This division is used to control how traffic was routed in and among IP networks.

Historically, the IP address space was divided into three main 'classes of network', where each class had a fixed network size. The class, and hence the length of the subnet mask and the number of hosts on the network, could always be determined from the most significant bits of the IP address. Without any other way of specifying the length of a subnet mask, routing protocols necessarily used the class of the IP address specified in route advertisements to determine the size of the routing prefixes to be set up in the routing tables.

CIDR and masks

A subnet mask is a bitmask which shows where the network address ends and the host address begins. CIDR uses variable length subnet masks (VLSM) to allocate IP addresses to subnets according to individual need, rather than some general network-wide rule. Thus the network/host division can occur at any bit boundary in the address. The process can be recursive, with a portion of the address space being further divided into even smaller portions, through the use of masks which cover more bits.

Because the normal class distinctions are ignored, the new system was called classless routing. This led to the original system being called, by back-formation, classful routing.

CIDR/VLSM network addresses are now used throughout the public Internet, although they are also used elsewhere, particularly in large private networks. An average desktop LAN user generally does not see them in practice, as their LAN network is usually numbered using special private RFC 1918 addresses.

Prefix aggregation

Another benefit of CIDR is the possibility of routing prefix aggregation. For example, sixteen contiguous /24 networks could now be aggregated together, and advertised to the outside world as a single /20 route (if the first 20 bits of their network addresses match). Two contiguous /20s could then be aggregated to a /19, and so forth. This allowed a significant reduction in the number of routes that had to be advertised over the Internet, preventing 'routing table explosion' from overwhelming routers, and stopping the Internet from expanding further.

CIDR notation

The standard notation for a CIDR address range begins with the network address (padded on the right with the appropriate number of zero-valued bits - up to 4 octets for IPv4, and up to 8 16-bit hexadecimal fields for IPv6). This is followed by a "/" character and a prefix length, in bits, defining the length of the subnet mask, which determines the size of the network.

For example (a more complete IPv4 subnetting reference table is available):
192.168.0.0/24 represents the 256 IPv4 addresses 192.168.0.0 through 192.168.0.255 inclusive, with 192.168.0.255 being the broadcast address for the network.
192.168.0.0/22 represents the 1024 IPv4 addresses 192.168.0.0 through 192.168.3.255 inclusive, with 192.168.3.255 being the broadcast address for the network.
2002:C0A8::/48 represents the IPv6 addresses 2002:C0A8:0:0:0:0:0:0 through 2002:C0A8:0:FFFF:FFFF:FFFF:FFFF:FFFF, inclusive.

For IPv4, an alternative representation uses the network address followed by the network's subnet mask, written in dotted decimal form:
192.168.0.0/24 could be written 192.168.0.0 255.255.255.0
192.168.0.0/22 could be written 192.168.0.0 255.255.252.0

Classful network

Classful networking is the name given to the first round of changes to the structure of the IP address in IPv4.

Originally, the 32-bit IPv4 address consisted simply of an 8-bit network number field (which specified the particular network a host was attached to), and a rest field, which gave the address of the host within that network. (This format was picked before the advent of local area networks (LANs), when there were only a few, large, networks such as the ARPANET.)

This resulted in a very low count (256) of network numbers being available, and very early on, as LANs started to appear, it became obvious that that would not be enough.

Classes

As a kludge, the definition of the meaning of IP addresses was changed, to allow three different sizes of network number field (and associated rest fields), as specified in the table below (in bits):

Class	Leading bits	Network number	Rest
Class A	0	7	24
Class B	10	14	16
Class C	110	21	8
Class D (multicast)	1110		
Class E (reserved)	1111		

The larger network number fields allowed a larger number of networks, thereby temporarily allowing the continued growth of the Internet.

The IP address netmask, which is so commonly associated with an IP address today, was not required, as the mask length was purely a function of the IP address. Any network device could inspect the first few bits of a 32 bit IP address to see which class it belonged to.

The method of determining whether one address belongs to the same physical network as another IP address worked as it had originally (but see subnet). For each address, the portion of the address which contained the network number was determined, and the contents of the rest part of the address was ignored. If the network numbers matched, the two addresses were on the same network.

The replacement of classes

This first round of changes was not enough to work in the long run, however; an IP address shortage still developed. The principal problem was that most sites were too big for a "class C" network number, and received a "class B" number instead. With the rapid growth of the Internet, the available pool of class B addresses (basically 214, or about 16,000 total) was rapidly being depleted. Classful networking was replaced by Classless Inter-Domain Routing (CIDR), starting in about 1993, to solve this problem (and others).

Early allocations of IP addresses by IANA were in some cases not made very efficiently, which contributed to the problem. (However, the commonly-held notion that some organizations unfairly or unnecessarily received class A networks is a canard; most such allocations date to the period before the introduction of address classes, when the only thing available was what later became known as "class A" network numbers.)

Dynamic Host Configuration Protocol – DHCP

Dynamic Host Configuration Protocol (DHCP) is a client-server networking protocol. A DHCP server provides configuration parameters specific to the DHCP client host requesting, generally, information required by the host to participate on the Internet network. DHCP also provides a mechanism for allocation of IP addresses to hosts.

DHCP appeared as a standard protocol in October 1993. RFC 2131 provides the latest (March 1997) DHCP definition.

IP Address Allocation

The DHCP protocol provides three methods of IP address allocation:
manual allocation, where the allocation is based on a table with MAC address - IP address pairs manually filled by the server admin. Only requesting clients with a MAC address listed in this table get the IP address according to the table.
automatic allocation, where a free IP address of a range given by the admin is permanently assigned to a requesting client.
dynamic allocation, the only method which provides dynamic reuse of IP addresses. A network administrator assigns a range of IP addresses to DHCP, and each client computer on the LAN has its TCP/IP software configured to request an IP address from the DHCP server when that client computer's network interface card starts up. The request-and-grant process uses a lease concept with a controllable time period. This eases the network installation procedure on the client computer side considerably.

Some DHCP server implementations can update the DNS name associated with the client hosts to reflect the new IP address by way of the DNS update protocol which was established with RFC 2136.

Implementations

Microsoft introduced DHCP on their NT server with Windows NT version 3.5 in late 1994. Despite being called a new feature from Microsoft, it was not invented by them.

The Internet Software Consortium published DHCP software distributions for Unix variants with version 1.0.0 of the ISC DHCP Server released on December 6, 1997 and a more RFC compliant version 2.0 on June 22, 1999. The software is available at http://www.isc.org/sw/dhcp/

Other major implementations included Cisco with a DHCP server made available in Cisco IOS 12.0 in February 1999 and Sun who added DHCP support in the July 2001 release of Solaris 8.

Cisco Systems offers DHCP servers in routers and switches with their IOS software. Moreover they offer Cisco Network Registrar (CNR) which is a highly scalable and flexible DNS, DHCP and TFTP server.

Protocol Anatomy

DHCP uses the same two IANA assigned ports for BOOTP: 67/udp for the server side, and 68/udp for the client side.

DHCP Discover

The client broadcasts on the local physical subnet to find available servers. The local router can be configured to forward DHCP packets to a DHCP server on a different subnet. This client implementation creates a UDP packet with the broadcast destination of 255.255.255.255 and also requests its last known IP address of 192.168.1.100 although this is not necessary and may be ignored by the server.

DHCP Offer

The server determines the configuration based on the client's hardware address that is specified in the CHADDR field. Here the server, 192.168.1.1, specifies the IP address in the YIADDR field.

DHCP Request

The client selects a configuration out of the DHCP Offer packets it received. Again, this client requests the 192.168.1.100 address that the server specified.

DHCP Acknowledge

The server acknowledges the request and broadcasts that on the local subnet. The client is expected to configure its network interface with the supplied options.

DHCP Release

The client sends a request to the DHCP server to release the DHCP and the client unconfigures its IP address.

Distance-vector routing protocol

A distance-vector routing protocol is a routing protocol used in routing of packet-switched networks in computer communications, as in for example the Routing Information Protocol for Internet traffic. They use the Bellman-Ford algorithm to calculate paths.

Examples of distance-vector routing protocols include RIPv1 or 2 and IGRP.

Workings

The distance-vector routing protocol assumes a network connected through several routers, each of which is connected to two or more computer networks. Each network may be connected to one or more routers.

The description below describes a very simple distance-vector routing protocol:
In the first stages, the router makes a list of which networks it can reach, and how many hops it will cost. In the outset this will be the two or more networks to which this router is connected. The number of hops for these networks will be 1. This table is called a routing table.
Periodically (typically every 30 seconds) the routing table is shared with other routers on each of the connected networks via some specified inter-router protocol. These routers will add 1 to every hop-count in the table, as it associates a hop cost of 1 for reaching the router that sent the table. This information is just shared inbetween physically connected routers ("neighbors"), so routers on other networks are not reached by the new routing tables yet.
A new routing table is constructed based on the directly configured network interfaces, as before, with the addition of the new information received from other routers. The hop-count is used as a cost measure for each path. The table also contains a column stating which router offered this hop count, so that the router knows who is next in line for reaching a certain network.
Bad routing paths are then purged from the new routing table. If two identical paths to the same network exists, only the one with the smallest hop-count is kept. When the new table has been cleaned up, it may be used to replace the existing routing table used for packet forwarding.
The new routing table is then communicated to all neighbors of this router. This way the routing information will spread and eventually all routers know the routing path to each network, which router it shall use to reach this network, and to which router it shall route next.

Advantages and disadvantages

Distance-vector routing protocols are simple and efficient in small networks, and require little, if any management. However, they do not scale well, and have poor convergence properties, which has led to the development of more complex but more scalable link-state routing protocols for use in large networks.

Interior Gateway Protocol - IGP

Internal Gateway Protocol (IGP) refers to a routing protocol that is used within an autonomous system. The most commonly used IGPs are RIP, OSPF and IS-IS.

When using a routing protocol such as BGP in a network, the routes received have a next hop that is not necessarily directly connected. The IGP is used to "resolve" these next hops.

IP address

An IP address (Internet Protocol address) is a unique number, similar in concept to a telephone number, used by network devices (routers, computers, time-servers, FAX machines, some telephones) attached to a network to refer to each other when sending information through a LAN (Local Area Network) or a WAN (Wide Area Network) or the Internet for example. This allows devices passing the information onwards on behalf of the sender to know where to send it next, and for the device receiving the information to know that it is the intended destination.

An example IP address is 207.142.131.236. Converting a number address to a more human-readable form called a domain address (www.wikipedia.org) is done via the Domain Name System. The process of conversion is known as resolution of the domain name.

More detail

The Internet Protocol (IP) knows each logical host interface by a number, the so-called IP address. On any given network, this number must be unique among all the host interfaces that communicate through this network. Users of the Internet are sometimes given a host name in addition to their numerical IP address by their Internet service provider.

The IP addresses of users browsing the world wide web are used to enable communications with the server of the web site. Also, it is usually in the header of email messages one sends. In fact, for all programs that utilize the TCP/IP protocol, the sender IP address and destination IP address are required in order to establish communications and send data.

Depending on one's Internet connection the IP address can be the same every time one connects (called a static IP address), or different every time one connects, (called a dynamic IP address). In order to use a dynamic IP address, there must exist a server which can provide the address. IP addresses are usually given out through a service called DHCP or the Dynamic Host Configuration Protocol.

Internet addresses are needed not only for unique enumeration of hosted interfaces, but also for routing purposes, therefore a high fraction of them are always unused or reserved.

The unique nature of IP addresses makes it possible in many situations to track which computer - and by extension, which person - has sent a message or engaged in some other activity on the internet. This information has been used by law enforcement authorities to identify criminal suspects. The dynamically-assigned nature of many IP addresses can make this more difficult.

IP version 4

Addressing

In version 4 of the Internet protocol (IPv4), the current standard protocol for the Internet, IP addresses consist of 32 bits, which makes for 4,294,967,296 (over 4 billion) unique host interface addresses in theory. In practice, because addresses are allocated in blocks, many unused addresses are unavailable (much like unused phone numbers in a sparsely-populated area code), so that there is some pressure to extend the address range via IP version 6 (see below).

IPv4 addresses are commonly expressed as a dotted quad, four octets (8 bits) separated by periods. The host known as www.wikipedia.org currently has the number 3482223596, written as 207.142.131.236 in base-256: 3482223596 equals 207×2563 + 142×2562 + 131×2561 + 236×2560. (Resolving the name "www.wikipedia.org" to its associated number is handled by Domain Name System servers.)

IPv4 addresses were originally divided into two parts: the network and the host. A later change increased that to three parts: the network, the subnetwork, and the host, in that order. However, with the advent of classless inter-domain routing (CIDR), this distinction is no longer meaningful, and the address can have an arbitrary number of levels of hierarchy. (Technically, this was already true any time after the advent of subnets, since a site could elect to have more than one level of subnetting inside a network number.)

Assignment

The actual assignment of an address is not arbitrary. An organization, typically an Internet service provider, requests an assignment of a netblock from a registry such as the American Registry for Internet Numbers (ARIN). The network number comprises a range of addresses which the organization is free to allocate as they wish. An organization that has exhausted a significant part of its allocated address space can request another netblock.

Exhaustion

Some private IP address space has been allocated via RFC 1918. This means the addresses are available for any use by anyone and therefore the same RFC 1918 IP addresses can be reused. However they are not routable on the Internet. They are used extensively due to the shortage of registerable addresses. Network address translation (NAT) is required to connect those networks to the Internet.

While a number of measures have been taken to conserve the limited existing IPv4 address space (such as the use of NAT and Private Addressing), the number of 32-bit IP addresses is not sufficient to accommodate the long-term growth of the Internet. For this reason, the plan is that the Internet 128-bit IPv6 addressing scheme will be adopted over the next 5 to 15 years.

IP version 6

In IPv6, the new (but not yet widely deployed) standard protocol for the Internet, addresses are 128 bits wide, which, even with generous assignment of netblocks, should suffice for the foreseeable future. In theory, there would be exactly 2128, or about 3.403 × 1038 unique host interface addresses. If the earth were made entirely out of 1 cubic millimetre grains of sand, then you could give a unique address to each grain in 300 million planets the size of the earth. This large address space will be sparsely populated, which makes it possible to again encode more routing information into the addresses themselves.

A version 6 address is written as eight 4-digit (16-bit) hexadecimal numbers separated by colons. One string of zeros per address may be left out, so that 1080::800:0:417A is the same as 1080:0:0:0:0:800:0:417A.

Global unicast IPv6 addresses are constructed as two parts: a 64-bit routing part followed by a 64-bit host identifier.

Netblocks are specified as in the modern alternative for IPv4: network number, followed by a slash, and the number of relevant bits of the network number (in decimal). Example: 12AB::CD30:0:0:0:0/60 includes all addresses starting with 12AB00000000CD3.

IPv6 has many improvements over IPv4 other than just bigger address space, including autorenumbering and mandatory use of Ipsec.

Internet Protocol

The Internet Protocol (IP) is a data-oriented protocol used by source and destination hosts for communicating data across a packet-switched internetwork.

Data in an IP internetwork are sent in blocks referred to as packets or datagrams (the terms are basically synonymous in IP). In particular, in IP no setup of "path" is needed before a host tries to send packets to a host it has previously not communicated with.

The Internet Protocol provides an unreliable datagram service (also called best effort); i.e. it makes almost no guarantees about the packet. The packet may arrive damaged, it may be out of order (compared to other packets sent between the same hosts), it may be duplicated, or it may be dropped entirely. If an application needs reliability, it is provided by other means, typically by upper level protocols transported on top of IP.

Packet switches, or internetwork routers, forward IP datagrams across interconnected layer 2 networks. The lack of any delivery guarantees means that the design of packet switches is made much simpler. (Note that if the network does drop, reorder or otherwise damage a lot of packets, the performance seen by the user will be poor, so most network elements do try hard to not do these things - hence the best effort term. However, an occasional error will produce no noticeable effect.)

IP is the common element found in today's public Internet. The current and most popular network layer protocol in use today is IPv4; this version of the protocol is assigned version 4. IPv6 is the proposed successor to IPv4; the Internet is slowly running out of addresses, and IPv6 has 128-bit source and destination addresses, providing more addresses than IPv4's 32 bits. Versions 0 through 3 were either reserved or unused. Version 5 was used for an experimental stream protocol. Other version numbers have been assigned, usually for experimental protocols, but have not been widely used.

IP addressing and routing

Perhaps the most complex aspects of IP are addressing and routing. Addressing refers to how end hosts are assigned IP addresses and how subnetworks of IP host addresses are divided and grouped together. IP routing is performed by all hosts, but most importantly by internetwork routers, which typically use either interior gateway protocols (IGPs) or external gateway protocols (EGPs) to help make IP datagram forwarding decisions across IP connected networks.

Open Shortest Path First

Open Shortest Path First (OSPF) is a link-state, hierarchical Interior Gateway Protocol (IGP) routing protocol. The well-known Dijkstra's algorithm is used to calculate the shortest path tree. It uses cost as its routing metric. A link state database is constructed of the network topology which is identical on all routers in the area.

OSPF is perhaps the most widely used IGP in large networks. It can operate securely, using MD5 to authenticate peers before forming adjacencies, and before accepting link-state advertisements. A natural successor to RIP, it was VLSM capable or classless from its inception. A newer version of OSPF (OSPFv3) now supports IPv6 as well. Multicast extensions to OSPF (MOSPF) have been defined, however these are not widely used. OSPF can "tag" routes, and propagate these tags along with the routes.

An OSPF network can be broken up into smaller networks. A special area called the backbone area forms the core of the network, and other areas are connected to it. Inter-area routing goes via the backbone. All areas must connect to the backbone; if no direct connection is possible, a virtual link may be established.

Routers in the same broadcast domain or at each end of a point to point link form adjacencies when they have discovered each other. The routers elect a designated router (DR) and backup designated router (BDR) which act as hub to reduce traffic between routers. OSPF uses both unicast and multicast to send 'hello packets' and link state updates. Multicast addresses 224.0.0.5 and 224.0.0.6 are used. In contrast to RIP or BGP, OSPF does not use TCP or UDP but uses IP directly, using IP protocol 89.

Area types

An OSPF network is divided into areas. These are logical groupings of routers whose information may be summarized towards the rest of the network. Several "special" area types are defined:

Backbone area

The backbone area (also known as area zero) forms the core of an OSPF network. All other areas are connected to it, and intra-area routing happens via a router connected to the backbone area.

Stub area

A stub area is an area which doesn't receive external routes. External routes are defined as routes which were distributed in OSPF via another routing protocol. Therefore, stub areas typically need to rely on a default route to send traffic to routes outside the stub..

Not-so-stubby area

Also referred to as NSSA, a not-so-stubby area is a type of stub area that can import AS external routes and send them to the backbone, but cannot receive AS external routes from the backbone or other areas.

OSPF router types

OSPF defines various router types. These are logical definitions, and a router that uses OSPF may be classified as more than one of the following types. For example, a router that is connected to more than one area, and which receives routes from a BGP process connected to another AS, is both an ABR and an ASBR.

Area Border Router

An Area Border Router (ABR) is a router that connects one or more OSPF areas to the main backbone network. It is considered a member of all areas it is connected to. An ABR keeps multiple copies of the link-state database in memory, one for each area.

Autonomous System Border Router

An ASBR is a router connected to more than one autonomous system (AS), and which exchanges routing information with routers in other ASs. ASBRs typically also run a non-IGP routing protocol, such as BGP. An ASBR is used to distribute routes received from other ASs throughout its own AS.

Internal router

A router is called an internal router (IR) if it only has OSPF adjacencies with routers in the same area.

Backbone router

A backbone router (BR) is a router with an interface in to the backbone area. An ABR would be a BR, although the reverse need not be true.

Reverse Address Resolution Protocol (RARP)

Reverse address resolution protocol (RARP) is a protocol used to resolve an IP address from a given hardware address (such as an Ethernet address). The primary limitations were that each MAC had to be manually configured on a central server, and it was limited to only the IP address, leaving subnetting, gateways, and other information to be configured by hand. It was later obsoleted by BOOTP, which had a much greater feature set.

Another disadvantage with RARP compared to BOOTP is the fact that it is a non-IP protocol. This means that it can't be handled with the TCP/IP stack already present on the client computer. Thus the client must have special functionality in order to handle the raw RARP packet.

RARP is the complement of ARP. RARP is described in RFC 903

Routing Information Protocol - RIP

The Routing Information Protocol (RIP) is one of the most commonly used Interior Gateway Protocol (IGP) routing protocols on internal networks (and to a lesser extent, networks connected to the Internet), which helps routers dynamically adapt to changes of network connections by communicating information about which networks each router can reach and how far away those networks are.

Although RIP is still actively used, it is generally considered to have been obsoleted by routing protocols such as OSPF and IS-IS, although EIGRP, a somewhat more capable protocol in the same basic family as RIP (destination-vector routing protocols), also sees some use.

History

The routing algorithm used in RIP, the Bellman-Ford algorithm, was first deployed in a computer network in 1969, as the initial routing algorithm of the ARPANET.

The earliest version of the specific protocol that became RIP was the Gateway Information Protocol, part of Xerox Parc's PARC Universal Packet internetworking protocol suite. A later version, named the Routing Information Protocol, was part of Xerox Network Services.

A version of RIP which supported IP addresses was later included in the Berkeley Software Distribution (BSD) of the UNIX operating system, as the routed server, and various other vendors would impliment their own versions of the routing server. Eventualy RFC 1058 was issued to unify the various implimentations under a single standard.

Technical details

RIP is a distance-vector routing protocol, which employs the hop count as a routing metric. The maximum number of hops allowed with RIP is 15. Each RIP router transmits full updates every 30 seconds by default, generating large amounts of network traffic in lower bandwidth networks. It runs above the network layer of the Internet protocol suite, using UDP port 520 to carry its data. A mechanism called split horizon with limited poison reverse is used to avoid routing loops. Routers of some brands also use a holddown mechanism known as heuristics, whose usefulness is arguable and is not a part of the standard protocol.

In many current networking environments RIP would not be the first choice for routing as its convergence times and scalability are poor compared to OSPF or IS-IS, and the hop limit severely limits the size of network it can be used in. On the other hand, it is easier to configure.

Routing

Routing is the means of discovering paths in networks; typically communication networks, to provide paths through the network fabric along which information can be sent. In computer networks, the data is split up into packets, each handled individually. Circuit-based networks, such as the voice telephone network, also perform routing, to find paths for telephone calls.

Routing is usually directed by routing tables, which maintain a record of the best routes to various network destinaion locations.

Small networks may involve hand configuration. Large networks involve complex topologies and may change constantly, making the constructing of routing tables very problematic. Nevertheless, most of the PSTN uses pre-computed routing tables, with fallback routes if the most direct route is blocked: see routing in the PSTN. Automatic routing protocols attempt to solve this problem with dynamically updated routing tables. These are updated intermittently by the routing software, based on information carried by the routing protocol, and allow the network to be nearly autonomous in avoiding network failures and blockages.

Routing directs forwarding, the passing of logically addressed packets from their local subnetwork toward their ultimate destination. In large networks, packets may pass through many intermediary destinations before reaching their destination. Routing and forwarding both occur at layer 3 of the OSI seven-layer model.

The hardware used in routing includes hubs, switches and routers.

Dynamic routing basics

If a designated path is no longer available, the existing nodes must determine an alternate route to use to get their data to its destination. This is usually accomplished through the use of a routing protocol using one of two broad classes of routing algorithms; distance vector algorithms and link state algorithms, which together account for nearly every routing algorithm in use on the Internet.

Distance vector algorithms

Distance vector algorithms use the Bellman-Ford algorithm. When this used, the link between each node in the network is assigned a number, the cost. Nodes will send information from point A to point B via the path that results in the lowest total cost (i.e. the sum of the costs of the links between the nodes used).

The algorithm is very simple. When a node first starts, it only knows of its immediate neighbours, and the direct cost to them. (This information, the list of destinations, the total cost to each, and the next hop to send data to to get there, is the routing table, or distance table.) Each node, on a regular basis, sends to each neighbour its own current idea of the total cost to get to all the destinations it knows of. The neighbouring node(s) examine this information, and compare it to what they already 'know'; anything which represents an improvement on what they already have, they insert in their own routing table. Over time, all the nodes in the network will discover the best next hop for all destinations, and the best total cost.

When one of the nodes involved goes down, those nodes which used it as their next hop for certain destinations discard those entries, and create a new routing table. This is then passed to all adjacent nodes, which then repeat the process. Eventually all the nodes are updated, and will then discover new paths to all the destinations which are still reachable.

Link state algorithms

When link state algorithms are used, the fundamental data each node uses is a map of the network, in the form of a graph. To produce this, each node floods the entire network with information about what other nodes it is connected to, and each node then independently assembles this information into a map. Using this map, each router then independently determines the best route from it to every other node.

The algorithm used to do this, Dijkstra's algorithm, does this by building another data structure, a tree, with the node itself as the root, and containing every other node in the network. It starts with a tree containing only itself. Then, one at a time, from the set of nodes which have not yet been added to the tree, it adds the node which has the lowest cost to reach an adjacent node which is already in the tree. This continues until every node has been added to the tree.

This tree is then used to construct the routing table, giving the best next hop, etc, to get from the node itself to any other node in the network.

Routed versus routing protocol

There is often confusion between routed protocol and routing protocol:

Routed protocol: Any network protocol that provides enough information in its network layer address to allow a packet to be forwarded from one host to another host based on the addressing scheme. Routed protocols define the format and use of the fields within a packet. Packets generally are conveyed from end system to end system. IP is an example of a routed protocol.
Routing protocols: facilitate the exchange of routing information between networks, allowing routers to build routing tables dynamically. Traditional IP routing stays simple because it uses next-hop routing where the router only needs to consider where it sends the packet, and does not need to consider the subsequent path of the packet on the remaining hops.

Although this dynamic routing can become very complex, it makes the Internet very flexible, and has allowed it to grow in size by more than eight orders of magnitude over the years since adopting IP.

A routing metric consists of any value used by routing algorithms to determine whether one route is superior to another. Metrics can cover such information as bandwidth, delay, hop count, path cost, load, MTU, reliability, and communication cost. The routing table stores only the best possible routes, while link-state or topological databases may store all other information.

Administrative distance is the feature used by routers to select the best path when there are two or more different routes to the same destination from two different routing protocols. Administrative distance defines the reliability of a routing protocol. Each routing protocol is prioritized in order of most to least reliable using an administrative distance value.

Depending on the relationship of the router relative to other autonomous systems, various classes of routing protocols exist:
Ad hoc network routing protocols appear in networks with no or little infrastructure. For a list of a couple of the proposed protocols, see the Ad hoc protocol list
Interior Gateway Protocols (IGPs) exchange routing information within a single autonomous system. Common examples include:
IGRP (Interior Gateway Routing Protocol)
EIGRP (Enhanced Interior Gateway Routing Protocol)
OSPF (Open Shortest Path First)
RIP (Routing Information Protocol)
IS-IS (Intermediate System to Intermediate System)

Note: The impression in various Cisco marketing documents to the contrary, EIGRP is definitely not a link-state protocol, or any sort of "hybrid" thereof.
Exterior Gateway Protocols (EGPs) route between separate autonomous systems. EGPs include:
EGP (the original Exterior Gateway Protocol used to connect to the former Internet backbone network -- now obsolete)
BGP (Border Gateway Protocol: current version, BGPv4, was adopted around 1995)

Real-time Transport Protocol (RTP)

The Real-time Transport Protocol (or RTP) defines a standardized packet format for delivering audio and video over the Internet. It was developed by the Audio-Video Transport Working Group of the IETF and first published in 1996 as RFC 1889.

It was originally designed as a multicast protocol, but has since been applied in many unicast applications. It is frequently used in streaming media systems (in conjunction with RTSP) as well as videoconferencing and push to talk systems (in conjunction with H.323 or SIP), making it the technical foundation of the Voice over IP industry. It goes along with the RTP Control Protocol (RTCP) and it's built on top of User Datagram Protocol (in OSI model).

According to RFC 1889, the services provided by RTP include:

- Payload-type identification
- Sequence numbering
- Time stamping
- Delivery monitoring

RTP ensures consistent delivery order of voice packets in an IP internetwork.

Transmission Control Protocol (TCP)

The Transmission Control Protocol (TCP) is one of the core protocols of the Internet protocol suite. Using TCP, applications on networked hosts can create connections to one another, over which they can exchange data. The protocol guarantees reliable and in-order delivery of sender to receiver data. TCP also distinguishes data for multiple, concurrent applications (e.g. web server and email server) running on the same host.

TCP supports many of the Internet's most popular application protocols and resulting applications, including the world wide web, email and Secure Shell.

Technical overview

Transmission Control Protocol (TCP) is a connection-oriented, reliable-delivery byte-stream transport layer communication protocol, currently documented in IETF RFC 793.

In the Internet protocol suite, TCP is the intermediate layer between the Internet Protocol below it, and an application above it. Applications often need reliable pipe-like connections to each other, whereas the Internet Protocol does not provide such streams, but rather only unreliable packets. TCP does the task of the transport layer in the simplified OSI model of computer networks.

Source Port	*Destination Port*	*Sequence Number*	*Acknowledgement Number*
Data Offset	*Reserved Flags*	*Window Checksum*	*Urgent Pointer*
Options (optional)	*Data*		

Applications send streams of 8-bit bytes to TCP for delivery through the network, and TCP divides the byte stream into appropriately sized segments (usually delineated by the maximum transmission unit (MTU) size of the data link layer of the network the computer is attached to). TCP then passes the resulting packets to the Internet Protocol, for delivery through an internet to the TCP module of the entity at the other end. TCP checks to make sure that no packets are lost by giving each byte a sequence number, which is also used to make sure that the data are delivered to the entity at the other end in the correct order. The TCP module at the far end sends back an acknowledgement for packets which have been successfully received; a timer at the sending TCP will cause a timeout if an acknowledgement is not received within a reasonable round-trip time (or RTT), and the (presumably lost) data will then be re-transmitted. The TCP checks that no bytes are damaged by using a checksum; one is computed at the sender for each block of data before it is sent, and checked at the receiver.

Protocol operation in detail

TCP connections contain three phases: connection establishment, data transfer and connection termination. A 3-way handshake is used to establish a connection. A four-way handshake is used to disconnect. During connection establishment, parameters such as sequence numbers are initialized to help ensure ordered delivery and robustness.

Connection establishment (3-way handshake)

While it is possible for a pair of end hosts to initiate connection between themselves simultaneously, typically one end opens a socket and listens passively for a connection from the other. This is commonly referred to as a passive open, and it designates the server-side of a connection. The client-side of a connection initiates an active open by sending an initial SYN segment to the server as part of the 3-way handshake. The server-side should respond to a valid SYN request with a SYN/ACK. Finally, the client-side should respond to the server with an ACK, completing the 3-way handshake and connection establishment phase.

Port states

A connection progresses through a series of states: LISTEN, SYN-SENT, SYN-RECEIVED, ESTABLISHED, FIN-WAIT-1, FIN-WAIT-2, CLOSE-WAIT, CLOSING, LAST-ACK, TIME-WAIT, and CLOSED.

LISTEN: represents waiting for a connection request from any remote TCP and port.

TIME-WAIT: represents waiting for enough time to pass to be sure the remote TCP received the acknowledgment of its connection termination request. According to RFC 793 a connection can stay in TIME_WAIT for a maximum of four minutes.

Data transfer

During the data transfer phase, a number of key mechanisms determine TCP's reliability and robustness. These include using sequence numbers for ordering received TCP segments and detecting duplicate data, checksums for segment error detection, and acknowledgements and timers for detecting and adjusting to loss or delay.

During the TCP connection establishment phase, initial sequence numbers (ISNs) are exchanged between the two TCP speakers. These sequence numbers are used to identify data in the byte stream, and are numbers that identify (and count) application data bytes. There are always a pair of sequence numbers included in every TCP segment, which are referred to as the sequence number and the acknowledgement number. A TCP sender refers to its own sequence number simply as the sequence number, while the TCP sender refers to receiver's sequence number as the acknowledgement number. To maintain reliability, a receiver acknowledges TCP segment data by indicating it has received up to some location of contiguous bytes in the stream. An enhancement to TCP, called selective acknowledgement (SACK), allows a TCP receiver to acknowledge out of order blocks.

Through the use of sequence and acknowledgement numbers, TCP can properly deliver received segments in the correct byte stream order to a receiving application. Sequence numbers are 32-bit, unsigned numbers, which wrap to zero on the next byte in the stream after 232-1. One key to maintaining robustness and security for TCP connections is in the selection of the ISN.

A 16-bit checksum, consisting of the one's complement of the one's complement sum of the contents of the TCP segment header and data, is computed by a sender, and included in a segment transmission. (The one's complement sum is used because the end-around carry of that method means that it can be computed in any multiple of that length - 16-bit, 32-bit, 64-bit, etc - and the result, once folded, will be the same.) The TCP receiver recomputes the checksum on the received TCP header and data. The complement was used (above) so that the receiver does not have to zero the checksum field, after saving the checksum value elsewhere; instead, the receiver simply computes the one's complement sum with the checksum in situ, and the result should be -0. If so, the segment is assumed to have arrived intact and without error.

Note that the TCP checksum also covers a 96 bit pseudo header containing the Source Address, the Destination Address, the Protocol, and TCP length. This provides protection against misrouted segments.

The TCP checksum is a quite weak check by modern standards. Data Link Layers with a high probability of bit error rates may require additional link error correction/detection capabilities. If TCP were to be redesigned today, it would most probably have a 32-bit cyclic redundancy check specified as an error check instead of the current checksum. The weak checksum is partially compensated for by the common use of a CRC or better integrity check at layer 2, below both TCP and IP, such as is used in PPP or the Ethernet frame. However, this does not mean that the 16-bit TCP checksum is redundant: remarkably, surveys of Internet traffic have shown that software and hardware errors that introduce errors in packets between CRC-protected hops are common, and that the end-to-end 16-bit TCP checksum catches most of these simple errors. This is the end-to-end principle at work.

Acknowledgements for data sent, or lack of acknowledgements, are used by senders to implicitly interpret network conditions between the TCP sender and receiver. Coupled with timers, TCP senders and receivers can alter the behavior of the flow of data. This is more generally referred to as flow control, congestion control and/or network congestion avoidance. TCP uses a number of mechanisms to achieve high performance and avoid congesting the network (i.e. send data faster than either the network, or the host on the other end, can utilize it). These mechanisms include the use of a sliding window, the slow-start algorithm, the congestion avoidance algorithm, the fast retransmit and fast recovery algorithms, and more. Enhancing TCP to reliably handle loss, minimize errors, manage congestion and go fast in very high-speed environments are ongoing areas of research and standards development.

TCP window size

The TCP receive window size is the amount of received data (in bytes) that can be buffered during a connection. The sending host can send only that amount of data before it must wait for an acknowledgment and window update from the receiving host. The Windows TCP/IP stack is designed to self-tune itself in most environments, and uses larger default window sizes than earlier versions.

Window scaling

For more efficient use of high bandwidth networks, a larger TCP window size may be used. The TCP window size field controls the flow of data and is limited to 2 bytes, or a window size of 65,535 bytes.

Since the size field cannot be expanded, a scaling factor is used. TCP window scale, as defined in RFC 1323, is an option used to increase the maximum window size from 65,535 bytes to 1 Gigabyte. Scaling up to larger window sizes is a part of what is necessary for TCP Tuning.

The window scale option is used only during the TCP 3-way handshake. The window scale value represents the number of bits to left-shift the 16-bit window size field. The window scale value can be set from 0 (no shift) to 14.

Connection termination

The connection termination phase uses a four-way handshake, with each side of the connection terminating independently. When an endpoint wishes to stop its half of the connection, it transmits a FIN packet, which the other end acknowledges with an ACK. Therefore, a typical teardown requires a pair of FIN and ACK segments from each TCP endpoint.

A connection can be "half-open", in which case one side has terminated its end, but the other has not. The side which has terminated can no longer send any data into the connection, but the other side can.

TCP ports

TCP uses the notion of port numbers to identify sending and receiving applications. Each side of a TCP connection has an associated 16-bit unsigned port number assigned to the sending or receiving application. Ports are categorized into three basic categories: well known, registered and dynamic/private. The well known ports are assigned by the Internet Assigned Numbers Authority (IANA) and are typically used by system-level or root processes. Well known applications running as servers and passively listening for connections typically use these ports. Some examples include: FTP (21), TELNET (23), SMTP (25) and HTTP (80). Registered ports are typically used by end user applications as ephemeral source ports when contacting servers, but they can also identify named services that have been registered by a third party. Dynamic/private ports can also be used by end user applications, but are less commonly so. Dynamic/private ports do not contain any meaning outside of any particular TCP connection. There are 65535 possible ports officially recognized.

TCP Over Wireless

TCP was optimized for wired networks. Any packet loss is considered as a congestion and hence window size is reduced dramatically as a precaution. However wireless links are known to experience sporadic and usually temporary losses due to fading, shadowing, handoff etc. which cannot be considered as congestion. Erroneous back-off the window size due to wireless packet loss is followed by a congestion avoidance phase with a conservative increase which causes the radio link to be underutilized. Note that radio resources are extremely valuable in wireless communications. Extensive research has been done over this subject to combat these harmful effects. Suggested solutions can be categorized as end-to-end solutions (which require modifications at the client and/or server), link layer solutions (such as RLP in CDMA2000), or proxy based solutions (which require some changes in the network without modifying end nodes).

Alternatives to TCP

TCP is not appropriate for many applications, The big problem (at least with normal implmentations) is that the application cannot get at the packets coming after a lost packet until the lost packet is retransmitted. This causes problems for real-time applications such as streaming multimedia (such as Internet radio), real-time multiplayer games and voice over IP (VoIP) where it is sometimes more useful to get most of the data in a timely fasion than it is to get all of the data in order.

Also for embedded systems the complexity of TCP can be a problem. The best known example of this is netbooting which generally uses TFTP. Finally some tricks such as transmitting data between two hosts that are both behind NAT (using STUN or similar systems) is far simpler if you don't have a complex protocol like TCP in your way.

Generally where TCP is unsuitable the User Datagram Protocol (UDP) is used, This provides the application multiplexing and checksums that TCP does but does not handle building streams or retransmission giving the application developer the ability to code those in a way suitable for the situation and/or to replace them with other methods like forward error correction or interpolation.

SCTP is another IP protocol which provides reliable stream oriented services not so dissimilar from TCP. It is newer and considerably more complex than TCP so has not yet seen widespread deployment, however it is especially designed to be used in situations where reliability and near-realtime considerations are important.

User Datagram Protocol – (UDP)

The User Datagram Protocol (UDP) is one of the core protocols of the Internet protocol suite. Using UDP, programs on networked computers can send short messages known as datagrams to one another. UDP does not provide the reliability and ordering guarantees that TCP does; datagrams may arrive out of order or go missing without notice. However, as a result, UDP is faster and more efficient for many lightweight or time-sensitive purposes. Also its stateless nature is useful for servers that answer small queries for huge numbers of clients.

Common network applications that use UDP include the Domain Name System (DNS), streaming media applications, Voice over IP, and online games.

Technical overview

User Datagram Protocol (UDP) is a minimal message-oriented transport layer protocol that is currently documented in IETF RFC 768.

In the TCP/IP model, UDP provides a very simple interface between a network layer below and an application layer above. UDP provides no guarantees for message delivery and a UDP sender retains no state on UDP messages once sent onto the network. (For this reason UDP is sometimes expanded to "Unreliable Datagram Protocol".) UDP adds only application multiplexing and data checksumming on top of an IP datagram.

Source Port	*Destination Port*	*Length*	*Checksum Data*

The UDP header consists of only 4 header fields of which two are optional. The source and destination port fields are 16-bit fields that identify the sending and receiving process. Since UDP is stateless and a UDP sender may not solicit replies, the source port is optional. If not used, the source port should be set to zero. The port fields are followed by a mandatory zomg length field indicating the length in bytes of the UDP datagram including the data. The minimum value is 8 bytes. The remaining header field is a 16-bit checksum field covering the header and data. The checksum is also optional, but is almost always used in practice.

Lacking reliability, UDP applications must generally be willing to accept some loss, errors or duplication. Some applications such as TFTP may add rudimentary reliability mechanisms into the application layer as needed. Most often, UDP applications do not require reliability mechanisms and may even be hindered by them. Streaming media, real-time multiplayer games and voice over IP (VoIP) are examples of applications that often use UDP. If an application requires a high degree of reliability, a protocol such as the Transmission Control Protocol or erasure codes may be used instead.

Lacking any congestion avoidance and control mechanisms, network-based mechanisms are required to minimize potential congestion collapse effects of uncontrolled, high rate UDP traffic loads. In other words, since UDP senders cannot detect congestion, network-based elements such as routers using packet queueing and dropping techniques will often be the only tool available to slow down excessive UDP traffic. The Datagram Congestion Control Protocol (DCCP) is being designed as a partial solution to this potential problem by adding end host congestion control behavior to high-rate UDP streams such as streaming media.

While the total amount of UDP traffic found on a typical network is often on the order of only a few percent, numerous key applications use UDP, including the Domain Name System (DNS), the simple network management protocol (SNMP), the Dynamic Host Configuration Protocol (DHCP) and the Routing Information Protocol (RIP), just to name a few.

MAC address

In computer networking a media access control address (MAC address) is a unique identifier attached to most forms of networking equipment. Most layer 2 network protocols use one of three numbering spaces managed by the IEEE: MAC-48, EUI-48, and EUI-64, which are designed to be globally unique. Not all communications protocols use MAC addresses, and not all protocols which do require such globally unique identifiers. The IEEE claims trademarks on the names "EUI-48" and "EUI-64". (The "EUI" stands for Extended Unique Identifier.)

ARP/RARP is commonly used to map the layer 2 MAC address to an address in a layer 3 protocol such as Internet Protocol (IP). On broadcast networks such as Ethernet the MAC address allows each host to be uniquely identified and allows frames to be marked for specific hosts. It thus forms the basis of most the layer 2 networking upon which higher OSI Layer protocols build to produce complex, functioning networks.

Address details

The original IEEE 802 MAC address, now officially called "MAC-48", comes from the Ethernet specification. Since the original designers of Ethernet had the foresight to use a 48-bit address space, there are potentially 248 or 281,474,976,710,656 possible MAC addresses.

All three numbering systems use the same format, and differ only in the length of the identifier. The first three octets (in transmission order) identify the organization which issued the identifier, and are known as the Organisational Unique Identifier (OUI). The following three (MAC-48 and EUI-48) or five (EUI-64) octets are assigned by that organization in nearly any manner they please, subject to the constraint of uniqueness. The IEEE expects the MAC-48 space to be exhausted no sooner than the year 2100; EUI-64s are not expected to run out.

MAC addresses permanently attached to a product by the manufacturer are known as "burned-in addresses" (BIA) or sometimes as "Universally Administered Addresses" (UAA). The BIA can be overridden with a "Locally Administered Address" (LAA). The following technologies use the MAC-48 identifier format: Ethernet, Token ring, 802.11 wireless networks, Bluetooth, FDDI, ATM (switched virtual connections only, as part of an NSAP address), SCSI and Fibre Channel (as part of a World Wide Name)

The distinction between EUI-48 and MAC-48 identifiers is purely semantic: MAC-48 is used for network hardware; EUI-48 is used to identify other sorts of devices and software. (Thus, by definition, an EUI-48 is not in fact a "MAC address", although it is syntactically indistinguishable from one and assigned from the same numbering space.)

EUI-64 identifiers are used in:
FireWire
IPv6 (as the low-order 64 bits of a unicast network address)

The IEEE has built in several special address types to allow more than one Network Interface Card to be addressed at one time:
The broadcast address, all one bits, is received by all stations on a local area network.
Multicast addresses, used with both Ethernet and FDDI, are received by stations on a LAN which have been configured to do so. Multicast addresses have the least significant bit of their first octet set to one.
Functional addresses identify one of more Token Ring NICs that provide a particular service, defined in IEEE 802.5.

In addition, the EUI-64 numbering system encompasses both MAC-48 and EUI-48 identifiers by a simple translation mechanism. To convert a MAC-48 into an EUI-64, copy the OUI, append the two octets 'FF-FF', and then copy the organization-specified part. To convert an EUI-48 into an EUI-64, the same process is used, but the sequence inserted is 'FF-FE'. In both cases, the process can be trivially reversed when necessary. Organizations issuing EUI-64s are cautioned against issuing identifiers which would be confused with these forms. The IEEE's policy is to discourage new uses of 48-bit identifiers in favor of the EUI-64 system.

Confusingly IPv6 -- one of the most prominent standards that uses EUI-64 -- applies these rules inconsistenly. Due to an error in the appendix to the specification of IPv6 addressing, it is currently standard practice in IPv6 to extend MAC-48 addresses (such as IEEE 802 MAC address) to EUI-64 using 'FF-FE' rather than 'FF-FF'; it remains to be seen how this inconsistency will be resolved in the future.

Printed format

The standard format for printing MAC-48 addresses in human-readable media is three groups of four hexadecimal digits, separated by dots (.), in transmission order; e.g., 0123.4567.89ab. However, very few products do this. The most common format is six groups of two hexadecimal digits, separated by colons (:) or hyphens (-), still in transmission order, as in 01:23:45:67:89:ab or 01-23-45-67-89-ab; this form is also commonly used for EUI-64.

Changing MAC addresses

Although physical MAC addresses are permanent by design, several mechanisms allow modification, or "spoofing", of the MAC address that is reported by the operating system. This can be useful for privacy reasons, for instance when connecting to a Wi-Fi hotspot, or to ensure interoperability. Some internet service providers bind their service to a specific MAC address; if the user then changes their network card or intends to install a router, the service won't work anymore. Changing the MAC address of the new interface will solve the problem. Similarly, some software licenses are bound to a specific MAC address. Changing the MAC address in this way is not permanent: after a reboot, it will revert to the MAC address physically stored in the card.
As a MAC address can be changed, it can be unwise to rely on this as a single method of authentication. IEEE 802.1x is an emerging standard better suited to authenticating devices at a low level.