CS4254

Computer Network Architecture and Programming

Dr. Ayman A. Abdel-Hamid
Computer Science Department
Virginia Tech

Internet Protocol Suite

Outline

•Internet Protocol Suite

TCP/IP: The Big Picture 1/10

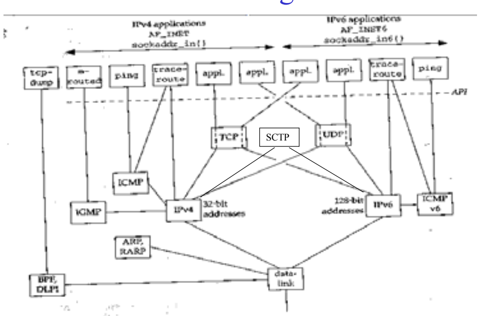


Figure 2.1 Overview of TCP/IP protocols.

TCP/IP: The Big Picture 2/10

Network Layer

IP: Internet Protocol (IPv4 and IPv6)

•Unreliable service
•Performs routing (Supported by routing protocols, e.g., BGP)
•Provide Internet-wide addressing (logical addressing)
•Fragment datagrams, as needed for underlying network

ICMP: Internet Control Message Protocol

•Handles error and control information between routers and hosts

•ICMP messages generated and processed by networking software and not user processes

TCP/IP: The Big Picture 3/10

Network Layer

IGMP: Internet Group Management Protocol

•Used with multicasting

ARP: Address Resolution Protocol

•Maps an IP (network) address into a hardware (network interface) address (such as an Ethernet address)

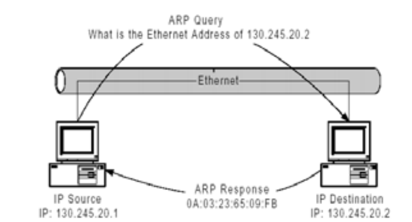
RARP: Reverse Address Resolution Protocol

•Maps a hardware address into an IP address

ICMPv6

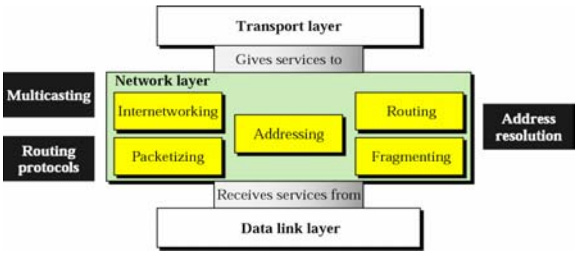
•Combines ICMPv4, IGMP, and ARP

TCP/IP: The Big Picture 4/10

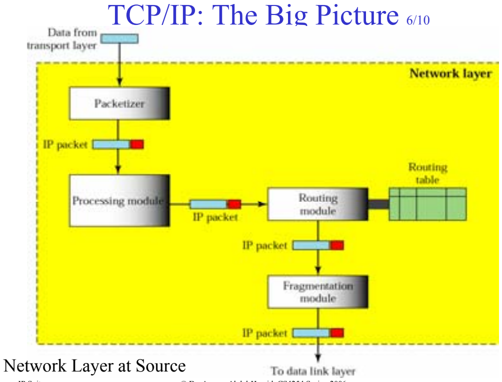


ARP (ARP responses are cached)

TCP/IP: The Big Picture 5/10

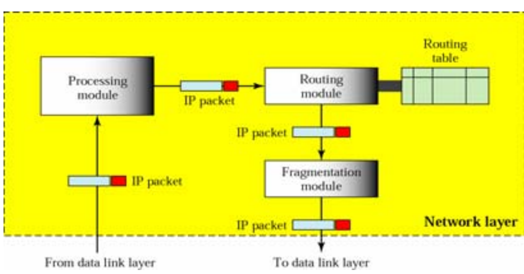


TCP/IP: The Big Picture 6/10



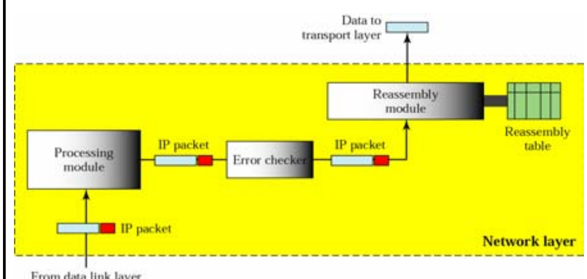
Network Layer at Source

TCP/IP: The Big Picture 7/10



Network Layer at Router

TCP/IP: The Big Picture 8/10



Network Layer at Destination

TCP/IP: The Big Picture 9/10

Transport Layer

TCP: Transmission Control Protocol

- Byte stream transfer
- Reliable, connection-oriented service
- Point-to-point (one-to-one) service only

UDP: User Datagram Protocol

- Unreliable (“best effort”) datagram service
- Point-to-point, multicast (one-to-many), and
- broadcast (one-to-all)

TCP/IP: The Big Picture 10/10

Transport Layer

SCTP: Stream Control Transmission Protocol [RFC 2960]

- Connection oriented
- Provides reliable full-duplex association
- Provides a message service
  - In TCP, a stream is a sequence of bytes
  - In SCTP, a stream is a sequence of messages
- Can use IPv4 and IPv6 on same association
  - Several streams within same association

Internetworking

•Motivation → Heterogeneity and scale

•IP is the glue that connects heterogeneous networks giving the illusion of a homogenous one

•Features

- ➢Best Effort Service Model
- ➢Global Addressing Scheme

•The Internet Protocol (IP) delivers datagrams across networks through routers (unreliable datagram service)

- ➢Datagrams (packets) may or may not be delivered
- ➢Datagrams may arrive at destination out of order
- ➢Datagrams may be arbitrarily delayed

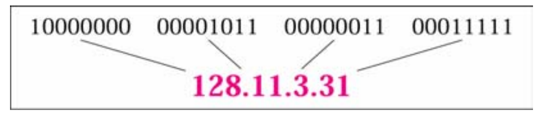
IP Addressing 1/11

•Global (public) IP addresses are *unique* (universal)

•Private IP addresses are not globally unique

- ➢No router will forward a packet that has a private IP address as a destination address

•Dotted decimal notation



IP Addressing 2/11

Classful addressing

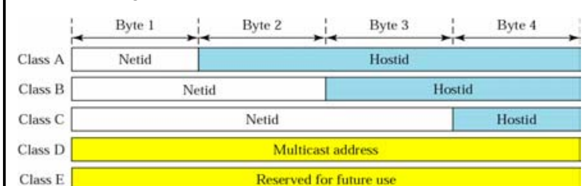
•Five classes: A, B, C, D, and E

IP Addressing 3/11

Classful addressing

•*Hierarchical*: Network ID (*Netid*) and Host ID (*Hostid*)

•Each class is divided into a fixed number of blocks with each block having a fixed size



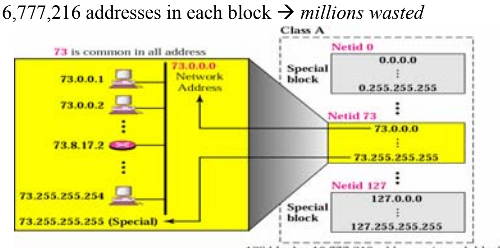
IP Addressing 4/11

Classful addressing

•Class A divided into 128 blocks (each block a different *Netid*)

•First block 0.0.0.0 to 0.255.255.255

•16,777,216 addresses in each block → *millions wasted*



IP Addressing 5/11

Classful addressing

•Class B

- ➢divided into 16,384 blocks
- ➢16 blocks for private addresses → only 16,368 blocks for assignment)
- ➢Each block contains 65,536 addresses → *midsize organizations*

•Class C

- ➢Divided into 2,097,152 blocks
- ➢256 for private addresses → 2,096,896 blocks for assignment
- ➢Each block contains 256 addresses → *small organizations*

IP Addressing 6/11

Classful addressing

•*Network address*: an address that defines the network itself, e.g., 123.0.0.0 (class A), 141.14.0.0 (class B), and 221.45.71.0 (class C)

• Packets are routed to an organization based on the network address

•To find the network address → apply a *netmask* (default mask)

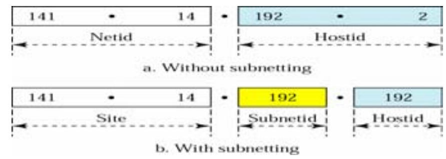
- AND netmask with address
- A netmask will retain the *Netid* of the block and sets the *Hostid* to 0s
- e.g., 190.240.7.91 → class B, default mask is 255.255.0.0 → network address is 190.240.0.0
- Could express address as 190.240.7.91/16 (*slash notation* → netmask has 1s in first 16 bits and 0s elsewhere)

IP Addressing 7/11

Classful addressing

•*Subnetting*

- Network address used to route packets to the network
- Outside world recognizes network, not individual hosts on the network (later reach host using the *Hostid*)
- Motivation for subnetting: *Assemble hosts into groups*
- Three levels of hierarchy: site, subnet, and host



IP Addressing 8/11

Classful addressing

•*Subnetting*

- A packet reaches a site based on the network address (using the netmask)
- Routers inside the organization route based on subnetwork address)
- To find subnet address → apply a subnet mask
  - ✓AND subnet mask with address
  - ✓e.g., 190.240.33.91 with /24 subnet mask (network address is 190.240.0.0 and subnet address is 190.240.33.0)
  - ✓Can you figure out 190.240.33.91/19?

IP Addressing 9/11

Broadcast Addresses

•Special addresses used for broadcasting

- Directed broadcast
  - ✓network (or subnet) plus *Hostid* that is all 1's
  - ✓All hosts on a specified network (or subnet)
- Limited broadcast
  - ✓all 1's (network and *Hostid*)
  - ✓Picked up by all other nodes on the LAN
  - ✓Not forwarded

•Example: broadcasting for 128.173.92.96

- Directed broadcast (using subnet): 128.173.255.255
- Limited broadcast: 255.255.255.255

IP Addressing 10/11

Classless addressing

•Classful addressing problematic

- Fixed block size and address waste
- ISPs are granted several class B or C blocks and then subdivide range between customers

•In 1996, *classless addressing* introduced

- *Variable-length blocks that belong to no class*
- Organization given first address and mask
- Can use subnets
- Classless Inter-Domain Routing (CIDR)

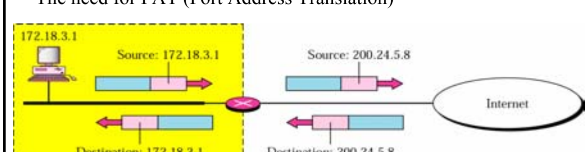
IP Addressing 11/11

Network Address Translation (NAT)

•Use a number of private (internal) addresses (home users and small businesses) when assigned ONE (or a small set) externally

- NAT router replaces source address in outgoing packets with global NAT address
- NAT router replaces destination address in incoming packets with appropriate private address

•The need for PAT (Port Address Translation)



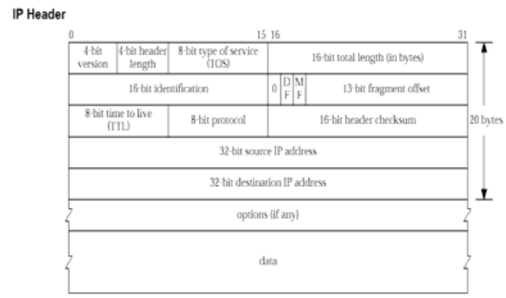
IP Datagrams

•IP datagrams include
- ➢Header, minimum size of 20 bytes
- ➢Data

•Datagram size
- ➢Less than or equal to *maximum transmission unit* (MTU) of the underlying network (Ethernet MTU is 1,500 bytes)
- ➢*MTU is the maximum amount of data that a link-layer packet can carry*

•Fragmentation
- ➢Packets may need to be fragmented at intermediate nodes if packet is too big for an intermediate network
  - ✓*Path MTU less than link MTU at sender*
  - ✓*Remember in IPv4, hosts and routers fragment datagrams*
  - ✓*In IPv6, only hosts perform fragmentation*
- ➢Receiver reassembles fragments to form entire IP packet

IP Datagram Format



IP Header Fields 1/2

•Identification: unique datagram identifier

•Total Length: length of this datagram + header, in bytes
- ➢Minimum datagram size in IPv4 is 576 bytes (in IPv6 → 1,500 bytes)
- ➢Use 576 (Minimum MTU) if path MTU unknown, or path MTU if on a connected network (datagram may be fragmented)

•Internet Header Length:
- ➢length of header in 32-bit words (+options)
- ➢Max is 15 allowing for sizes (header +options) of 60 bytes

•Fragment Offset: offset of fragment in this datagram in 8-byte units

•Flags (DF and MF): indicate if last fragment, and If datagram should not be fragmented (What happens if need to fragment and DF is set?)

•Time To Live: maximum number of routers through which the datagram may pass
- ➢Decremented at each router
- ➢Used to prevent looping in the network
- ➢Also used to limit scope of multicast datagrams

IP Header Fields 2/2

•Protocol: identifies higher level protocol that provided data

•Version: IP version identifier (currently 4)

•Type of Service: (historical)
- ➢Maximize throughput, minimize delay, maximize reliability, minimize cost (no guarantees, though)
- ➢Now replaced with 6-bit Differential Services Code Point and 2-bit Explicit Congestion Notification

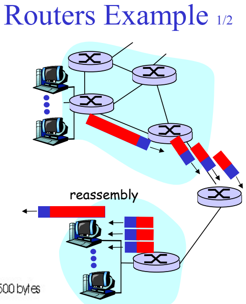
•Header Checksum: checksum over header (protects addresses, lengths, etc.) → 16-bit 1's complement of 1's complement sum of 16-bit W

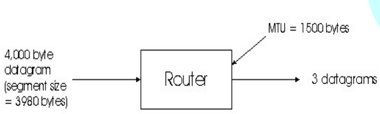
•Source IP Address and Destination IP Address

•Options (rarely used, may not be supported by routers)
- ➢Security and handling restrictions
- ➢Record route
- ➢Loose source routing (datagram passes through listed nodes and others)
- ➢Strict source routing (datagram must pass through only each listed node)

IPv4 Fragmentation by Routers Example 1/2

•In adhering to end-to-end principle
- ➢*If a router fragments a datagram, reassembly is only performed at destination*
- ➢*Reassembly at routers would complicate network performance*





Datagram size = 4,000 bytes
Identification = *x*

IPv4 Fragmentation by Routers Example 2/2

1st fragment
- ➢1480 bytes in the data field of the IP datagram (total length = 1500)
- ➢identification = *x*
- ➢offset = 0 (meaning the data should be inserted beginning at byte 0)
- ➢flag = 1 (meaning there is more)

2nd fragment
- ➢1480 bytes in the data field of the IP datagram (total length = 1500)
- ➢identification = *x*
- ➢offset = 1,480 (meaning the data should be inserted beginning at byte 1,480
- ➢flag = 1 (meaning there is more)

3rd fragment
- ➢1020 bytes (=3980-1480-1480) in the data field of the IP datagram (Total length = 1040)
- ➢identification = *x*
- ➢offset = 2,960 (meaning the data should be inserted beginning at byte 2,960)
- ➢flag = 0 (meaning this is the last fragment)