Week 7 Lecture 1

# Network Layer Outline

Data plane and control plane. In week 7 we look at data plane and week 8 we look at control plane

## Function of the network player

* Transport segment from sending to receiving host
* On sending side encapsulates segments into datagrams
* On receiving side, delivers segments to transport layer
* Network layer protocols in every host, router.
* Router examines header fields in all datagrams passing through it

*Takeaway: all the routers are running the bottom three layers*

**Forwarding:** move packets from router’s input to appropriate router output

**Routing:** determine route taken by packets from source to destination

It is every important to differentiate these two concepts. Routing is the process of planning the entire trip, forwarding is the process of getting through single intersection.

## Routers forwarding

Routers keep forwarding table locally, the router checks the value in the arriving packet’s header and decide the next link to forward to. The forwarding table is determined by the routing algorithm.

# Data Plane vs Control Plane

## Data plane

Determines how datagram arriving on router input port is forwarded to router output port (It is very important to differentiate router port with port in application layer).

**Service Model**

The network layer does not guarantee whatsoever is provided by IP layer in TCP/IP protocol stack. It is “best effort service”.

## Host, Router, Network Layer Functions

**Routing protocols (forwarding table):**

* Path selection
* RIP, OSPF, BGP

**IP protocol:**

* Addressing conventions
* Datagram format
* Packet handling conventions

**ICMP protocol:**

* Error reporting
* Router signalling

## IP packet Structure

**Fields for Reading Packet CorrectlyTable

Description automatically generated with medium confidence**

1. Version number (4 bits), Typically, “4” (for IPv4)
2. Header length (4 bits), Typically, “5” (for a 20-byte IPv4 header), can be more when IP options are used
3. Total length (16 bits), Maximum size is 65,535 bytes (216 -1)
4. Demultiplexing, tell end host how to handle packet, extract the payload and push to the upper layer(TCP or UDP for example)
5. Fields are reaching destination and back

A picture containing table

Description automatically generated**Checksum, TTL, and Fragmentation fields**

* Loop: TTL, time to live field, recommended default value is 64, it is used to discard packet that is looping forever in the network
* Header corrupted: Checksum, it has its own checkout, but is only computed over the packet header, not on the actual payload because TCP UDP already run checksums on the payload.
* Packet too big: fragmentation. Cause: different link layer protocol has different MTU, a router receives the datagram which could be too big for the next link. Certain field allow receiver to reassemble these fragments at the destination

**IP fragmentation, reassembly (example)**

Diagram

Description automatically generated

*In the example above, the receiver knows they are fragments of a large datagram by looking at the ID, the receiver knows the order by looking at the offset values. The receiver knows if all fragments have been received by looking at the MF Flag (if the value is 1)*

The IPv4 fragmentation procedure is as follows

1. Router breaks up datagram in sizes that the output link can support
2. Router copies IP header to pieces
3. Router adjusts length of pieces
4. Router sets offset of pieces to indicate position
5. Router sets MF flag=1 on all pieces except the last to indate “more fragments”
6. Router re-computes the checksum
7. The receiving host uses the Id field with the MF flag field and offset to reassemble the datagram

## No fragmentation

Diagram

Description automatically generated

**Host**

* + Sends a big packet to test whether all routers in path to the destination can support or not, for example, the source would send a segment of MTU 1400 bytes, then it comes back with ICMP message and says the outgoing link can only support MTU 1200 bytes, the source will try 1200 bytes.
  + Set DF (Do not fragment) flag, if this flag is in the segment, then the link cannot fragment the segment

**Routers**

* + Drops the packet if it is too large (as DF is set)
  + Provides feedback to Host with ICMP message telling the maximum supported size

**What is a network**? Device interfaces with same network part of IP address, can physically reach each other without intervening router

Diagram

Description automatically generatedDiagram

Description automatically generated

# IP Addressing

IP address is 32-bit identifier for host, router interface. For example, the computer is connected in the ethernet as well as Wi-Fi, then the computer has two IP addresses.

**IP address meanings:**

* The first three parts: network part
* The fourth block: host part

**Key points:**

1. If a datagram is sent to xxx.xxx.xxx.255, it is referred as the broadcast address, the datagram will be sent to every interface in the network.
2. Xxx.xxx.xxx.0, where the host bit are all ones, they are called the network address

## Classes, classful address

* If the first bit is a 0
  + The address belongs to class A
* Else if the second bit is a 0
  + The address belongs to class B
* Else if the third bit is a 0
  + The address belongs to class C
* Else if the fourth bit is a 0
  + The address belongs to class D
* Else
  + The address belongs to class E

### Issues with this classful address

Can’t handle rapidly growing number of organizations with small and medium-sized subnets. A class C (24 bits) subnet could accommodate only up to 2^8 − 2 = 254 hosts (two of the 2 = 256 addresses are reserved for special use)—too small for many organizations. However, a class B (/16) subnet, which supports up to 65,634 hosts, was too large. Under classful addressing, an organization with, say, 2,000 hosts was typically allocated a class B (/16) subnet address. This led to a rapid depletion of the class B address space and poor utilization of the assigned address space.

## Subnetting (very important, will be in the exam)

Chart

Description automatically generatedGraphical user interface, text, application

Description automatically generatedSubnetting is the process of dividing the class A, B or C networks into more manageable chunks that are suited to a network’s size and structure. Subnetting allows 3 levels of hierarchy, netid, subnetid and hostid. The original netid remains the same and designates the site. Subnetting remains transparent outside of the site. The process of subnetting simply extends the point where the 1’s of the mask stop and 0’s start. Some host ID bits are sacrificed to gain network ID bits.

Notation: address format: a.b.c.d/x, where x is # bits in network portion of address. For instance, 128.119.254.0/25, /25 means the bits for network address. For example, how many IP addresses belong to the subnet 128.119.254.0/25? What are the IP addresses at the two endpoints of this range? The answer is 2^7 = 128 addresses (126 are usable).

## CIDR: classless interdomain routing

Very important Question

An ISP is granted a block of addresses starting with 190.100.0.0/16. The ISP needs to distribute these addresses to three groups of customers as follows:

* The first group has 64 customers: each needs 256 addresses.
* The second group has 128 customers: each needs 128 addresses.
* The third group has 128 customers: each needs 64 addresses.

For 1st group, each customer needs 256 addresses. This means the suffix length is 8 (28 = 256). The prefix length is then 32 - 8 = 24.

A picture containing shape

Description automatically generated

Total = 64 x 256 = 16,384

For 2nd group, each customer needs 128 addresses. This means the suffix length is 7 (27 = 128). The prefix length is then 32 - 7 = 25.

A picture containing shape

Description automatically generated

Total = 128 x 128 = 16,384

For 3rd group, each customer needs 64 addresses. This means the suffix length is 6 (26 = 64). The prefix length is then 32 - 6 = 26

Text

Description automatically generated with medium confidence

Total = 128 x 64 = 8,192

Diagram, schematic

Description automatically generated

Number of granted addresses: 65,536

Number of allocated addresses: 40,960

Number of available addresses: 24,576

# DHCP: Dynamic Host Configuration Protocol

DHCP allows hosts to dynamically obtain its IP address from a network server when it joins a network. The host can renew its lease on an address in use.

The process of obtaining an IP address with DHCP is

1. The host broadcasts a “DHCP discover” message
2. The DHCP server responds with a “DHCP offer” message
3. The host requests an IP address with a “DHCP request” message
4. The DHCP server sends an address with a “DHCP ack” message

## Control Plane

Determines how datagram is routed among routers along end-to-end path from source to destination

**Traditional routing algorithms (what we study in this course)**

* Individual routing algorithm components in each router interact in the control plane (we look at this in details in week 8).

**Software-defined networking (not in the exam)**

* A distinct controller interacts with local control agents (CAs)