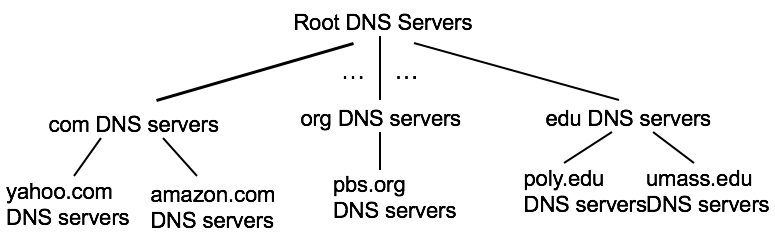
# CS 456

* Terminology:
  + ISP: internet service provider
  + Transmission rate = bandwidth
  + Packet switch = forward packet
  + WAN = wide area network (network that extends over a large geographical distance)
  + LAN is connection between WAN and hosts who outside the WAN
  + Unicast is a piece of information is sent from one point to another point.
  + Broadcast is a piece of information is sent from one point to all other points.
  + Multicast is a piece of information is sent from one or more points to a set of other points.
  + Anycast is a piece of information is sent from one point to anyone in the group
* Chapter 1:
  + Application layer: (supporting network applications): FTP, SMTP, HTTP, block chain
  + socket
  + Transport layer (process-process data transfer): TCP, UDP,
  + Network layer (routing of datagrams from source to destination): IP, routing protocols, ICMP protocols, DHCP
  + Link layer (data transfer between neighboring network elements): data transfer, Ethernet, LAN,MPLS
  + Physical layer (bits “on the wire”): bits on the wire
* Chapter 2: Application layer
  + Two possible architecture structure:
    - Client-Server: Server always on host, scaling, intermittently connected, dynamic IP
    - Peer-to-Peer: arbitrary end system, self-scalability, peers are intermittently connecting and change IP address
  + Web and HTTP (hypertext transfer): use HTML (objects) and every object is addressable by URL, stateless (don’t remember the information)
    - HTTP uses TCP to connect (persistence new [multiple objects sent for one connection, 1RRT per object] and non-persistence old [only one object sent for one connection, 2RRT per object, often open parallel TCP connections to fetch])
    - User-server cookie: in header of HTTP header, keeping state on users’ host, managed by users’ browser, ID created by server
    - web caches (proxy server): reduce the chance fetch from origin server => reduce the response time, reduce traffic
  + DNS (Domain name system):
    - IP address⬄ name (application layer)
    - Distributed system: reduce traffic, okay with single point of failure, easy to maintain
    - Services: 1. translation, 2. Host aliasing(two or more domain name for single site), 3. Mail server aliasing 4. Load distribution
    - hierarchical system, top to down
    - DNS name resolutions: 1. Iterated query (ask everyone and get feedbacks) 2. Recursive query (local DNS asks through the path, heavy load.)
    - Attack: DDOS (using traffic with root server, use filter), redirect: intercept query and poisoning
  + Able to afford 1 Billion users:
    - Mega server (no)
    - **Content distributed network**: store multiple copy at CDN (local servers)
* Chapter 3: Transport layer:
  + Service: provide *logical communication* between app processes. Sender break app into segments, server reassemble
  + TCP: reliable, has flow control (controlled by receiver, ensure that sender only send things receiver able to handle, untracked packets will fill up buffer, receiver stop senders if it is full, solution: gobackN and selective repeat) and congestion control (everyone in the network has fair amount to access resources, reduce sending speed for window => lost and delay), three handshakes to connect
  + UDP: replace update data, no connection requires
  + multiplexing at sender: handle data from multiple sockets, add transport header
  + demultiplexing at receiver: use header info to deliver received segments to correct socket
* Chapter 4: Network Layer

Role： move packet from one host to another

Packet switch: a general packet-switching device that transfers a packet from input link interface to output interface, according to the value in a field in the header of the packet, some call **link-layer switches**(base on link-layer frame/device), other call **routers**

Two functions:

1. Forwarding (router local action)
2. Routing (network wide)
3. Connection setup (routers along the path handshake for connection) some architectures such as ATM, frame layer…

Router: has a forwarding table by comparing the header of the packet,

created by routing algorithm

Routing algorithm: (configure its forward table)

1. Centralized: executing on a central router and be downloaded for each router
2. Decentralized: distributed system, run in every router

Network service model:

1. Guaranteed delivery
2. Guaranteed delivery with bounded delay
3. In order packet delivery
4. Guaranteed minimal bandwidth
5. Guaranteed maximum jitter: the amount of time between the transmission of two successive packets at the sender is equal to the amount of time between their receipt
6. Security services: use a secret key only known by source and destination

Internet is using best-effort service(NOTHING IS PROVIDED)

Computer network which only provide connection service at the network layer are called **virtual circuit network**, only provide connectionless service is called **Datagram network** (transport layer has TCP and UDP)

**VC** consists:

1. a path (every packets take the same path)
2. VC number, number for link in the path, one path has different VC number, replace new number of each traversing packet
   1. Reduce the length of the VC field in the packet header
   2. VC setup is considerably simplified by permitting a different number
   3. If not, the routers have to exchange a substantial number of message to agree on a common VC number to connect
3. Entries in the forwarding table, Maintain connection state information (new connection: entry add in, connection release: delete from the table)

VC setup: determine the path, add entry in the forwarding table, may reserve resources (bandwidth)

Data transfer

VC teardown: inform the end system on the other side to termination and update on the forwarding table

**Datagram network**: Stamps the packet with the address of the destination and pop the packet into the network. Use prefix matches links in forwarding table, if multi match, longest prefix matching rule, every packet will take a different path base on their source and destination

Forwarding table updates every 1 to 5 mins, since stateless

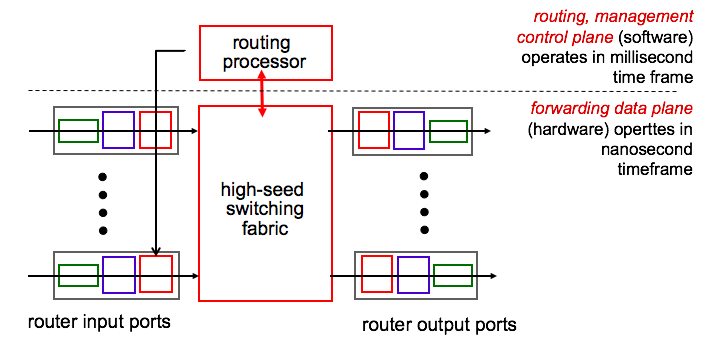
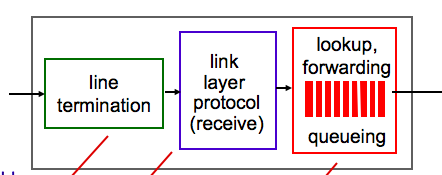
Packet in network = datagram

What is inside a router?

**Input port:**

* performance link layer function and interoperate with link layer
* lookup, forwarding queueing: is going to find out which output port to pick and block in queue (longest prefix match & performed in hardware with algorithm)
* other process: 1. Physical and link layer process 2. Checksum, packet version, etc 3. Update counters used in for network management

**Output port:** flip input port, stores packets and transmit to the outgoing link by preform link layer and physical layer function

**Routing processor:** execute the routing protocols, maintain routing tables and forwarding table

**Switching fabric:** packet switch/forward

1. switching via memory: simplest, earliest, give cpu (routing processor) via interrupt, lookup, no more than 2 packet can forward at the same time => modern router use shared memory to multiprocess
2. switching via a bus: put all packets on a shared bus, output port match label when bus comes through
3. switching via an interconnection network: no bandwidth limit, allowed multiprocessor (parallar) if source and destination are different

why queue? Happen when 1. switch is too fast, outgoing port only can handle one packet a time. 2. Switch is too slow, input port has to wait. If queues grow large the memory in router will exhausted=> packet loss => drop arriving packet(drop-tail) / remove one or more already queued packets

number of packet dropping and marking policies: active queue management, create random early detection algorithm (a weighted average is maintained for the length of the output queue,

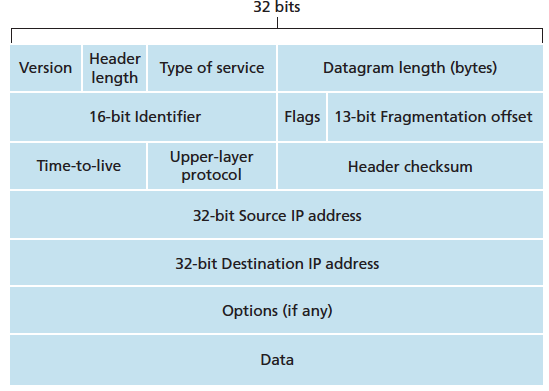
if ave length < minuimum threshold, then admit to the queue,

if ave length < maximum threshold / queue is full, then marked and dropped,

if in between, base on the probability)

need a packet scheduler for quality of service guarantees

**Internet Protocol (IP):**

IPv4: (IPv6 is different)

4bits 4 bits ex: low delay, reliability total length,16 bits

if datagram split, same for one 0 is last packet order, must correct, ow, crash

if 0, drop

Detect bit error

Lookup in DNS

IP address has to be globally unique, hosts and links in router has IP Address, managed by ICANN, assigned by Dynamic host configuration protocol (DHCP) in network administrator (update its list of available IP address, four steps: 1. serve discovery: new host send a UDP message (source IP, discover message) to port 67 2. Server offer: many DHCP servers will offer, include the IP address 3. Request 4.ACK)

**Classless Inter-Domain Routing (CIDR)**: address format: a.b.c.d/x

Subnet: three host interface and one router interface

Subnet mask: /x, x indicates the leftmost x bits of the 32 bit define the subnet address

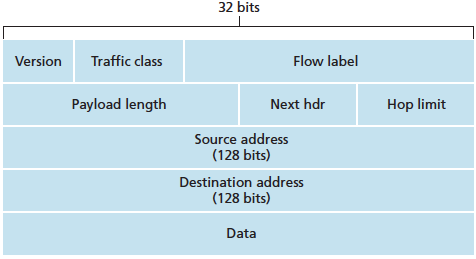
**Network address translation (NAT):** handle addressing when packets are sent to or received from the global internet. Violate P2P but popular.

When a new client appear, NAT generate a new port number to it and replace IP address with a WAN-side IP address. Add entry in NAT translation table.

Pro: 1. security local address is not known by outside world 2. Change local devices’ address and no need to notify outside world 3. Change ISP address without change devices’ address

Internet control message protocol(ICMP): used by hosts and routers to communicate network-layer information, put in payload, not used in practice. ex: reporting error

IPV6: 32 bit IP address is used up, header format helps speed processing/forwarding



Similar to TOS in IPV4 8 20 bit label a set of packets

belonging to the same flow

timer

Changes in IPV6: 1. no more fragmentation/ Reassembly => drop the packet with ICMP(ICMPv6 is created for it) 2. No more checksum, since other protocols have this 3. No more options

Transitioning from IPV4 to IPV6:

1. declare a flag day: a given time and date when all Internet machines would be turned off and upgraded from IPV4 to IPV6.
2. Dual-stack approach: IPv6 nodes also have a complete IPv4 implementation. If either the sender or the receiver is only 4 capable, a 4 datagram must be used. Conversion will lose info.
3. Tunneling: 6 put entire datagram into 4’s datagram (source and destination are two 4 in the path), because during the path, the router no need to know what is in the data.

IP Security: IPsec provide cryptographic agreement (allow two communicating hosts to agree on cryptographic algorithm and key), encryption of IP datagram payloads, data integrity (allow receiver host verify the datagram), origin authentication (make sure the source is correct)

Routing algorithms:

There are two types of algorithms: global = centralized (all routers have complete topology, link cost info)=> link state algorithm (Dijkstra’s algorithm), decentralized (router knows physically connected neighbors, iterative process of computation, exchange of info with neighbors) => distance vector algorithm (Bellman-Ford equation)

Details: there are others but all come from LS and DV

**Dijkstra’s algorithm:** loop through all the nodes and update the table, only replace the content with lower cost

**Bellman-Ford algorithm:** cost of least path from xau to y = min(cost to neighbor + cost from neighbor to y) through all x’s neighbor. If link cost change, notify neighbors and change there dv table. Time bases on the new cost

**Comparison:**

LS: O(n**2**) algorithm requires O(nE) msgs DV: may be fast, maybe infinite

can advertise incorrect *link* cost can advertise incorrect *path* cost

each node computes only its *own* table use other’s => error spread

Hierarchical routing:

A homogenous set of routers all executing the same routing algorithm is too simple in practice based on two reasons,

1. Scale: when the number of router increases, any updates on the link will cost both algorithms are unable to handle (LS no bandwidth to send packet, DV never converge)
2. Administrative autonomy: organizes should able to administer its network and able to connect with outside world

Can be solved in **autonomous system (ASs):** a set of routers are under same administrative control (autonomous system routing protocol including RIP and OSPF), gateway router can forward packet outside the AS, only one to any one part of outside world, need to know which gateway router to send (obtain reachability information from neighboring ASs and internal AS) => inter-AS routing protocol (BGP4) if there are multiple gateway routers can be choose, then pick the least cost gateway routers (**hot potato routing**))

**Routing information protocol (RIP):** idealized DV protocol. Cost is from source to a destination subnet = **hop.** Updates and exchange happen in every 30s in RIP response message use UDP

**Open shortest path first (OSPF):** LS, deployed upper-tier ISP, small subnet run Dijkstra’s algorithm itself and run as a node in the AS. Advance:

Security (exchange between OSPF routers can be authenticated, preventing malicious intruders), Multiple same cost paths, Integrated support for unicast and multicast routing, allow hierarchy within a single routing domain (algorithm=>area border router => backbone area => boundary router => AS)

**Border Gateway protocol (BGP4):**

* **eBGP: obtain subnet reachability information from neighbouring ASes**
* **iBGP: propagate reachability information to all AS-internal routers.**
* **Use semi-permanent Tcp connection for peers**
* **Prefix + attribute = route**
* **Attribute:**

AS-PATH: advertisement for the prefix has passed, prevent looping

Next-Hop: router interface that begins the AS-PATH, properly configure their forwarding table

* Import policy: whether to accept or filter the route, base on preferences, shortest AS-PATH, closest NEXT-HOP (least cost path)

Broadcast routing algorithm:

1. N-way-unicast: make N copy, inefficient, depend on routing infrastructure

2. Flooding: the source node sends a copy of the packet to all of its neighbours, recursively. If cycle, endless broadcast, useless packets all around. Broadcast storm

3. Controlled flooding: solve broadcast storm by judiciously choosing when to flood a packet by using: 1. Sequence number controlled flooding (every node has a list of all packet and source address who received) need overlay network 2.reverse path forwarding (RPF) only accept packet from the node which on its own shortest unicast path to source

4. Spanning tree broadcast: avoid the transmission of redundant broadcast packet, find minimum spanning tree. Using centre-based spanning tree.

Multicast routing algorithm:

1. a group shared tree: a tree includes all edge routers with attached hosts belonging to the multicast group. First all routers send message to the centre, until find the router already belong to the group
2. a source based tree: a single shared routing tree to route packets from all senders.

Software define network (SDN): a rethink , three layers, like os

1. forwarding is same before, switch flow table computed, installed by controller, using protocol (ex: openFlow, SNMP) to communicate with controller
2. southbound API
3. SDN controller: maintain network state information
4. Northbound API
5. Network control application: “brains” of control: implement control functions

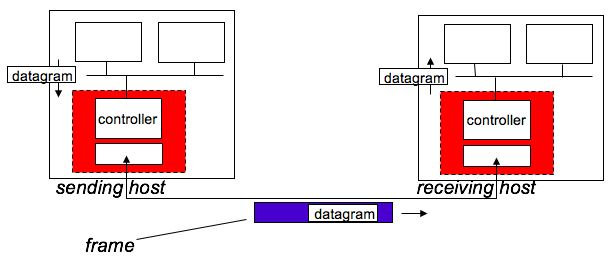
Chapter 6: Link layer

Service: 1. move a datagram from one ode to an adjacent node. 2. Framing: build the frame in datagram 2. link access: A Medium access control protocol, the sender can send a frame whenever the link is idle=> multiple access 3. Reliable delivery (no error): useful in high error rate link such as wireless link 4. Error detection and correction

**Where is the link layer implemented?** In a network adapter (= network interface card, hardware) &software in CPU

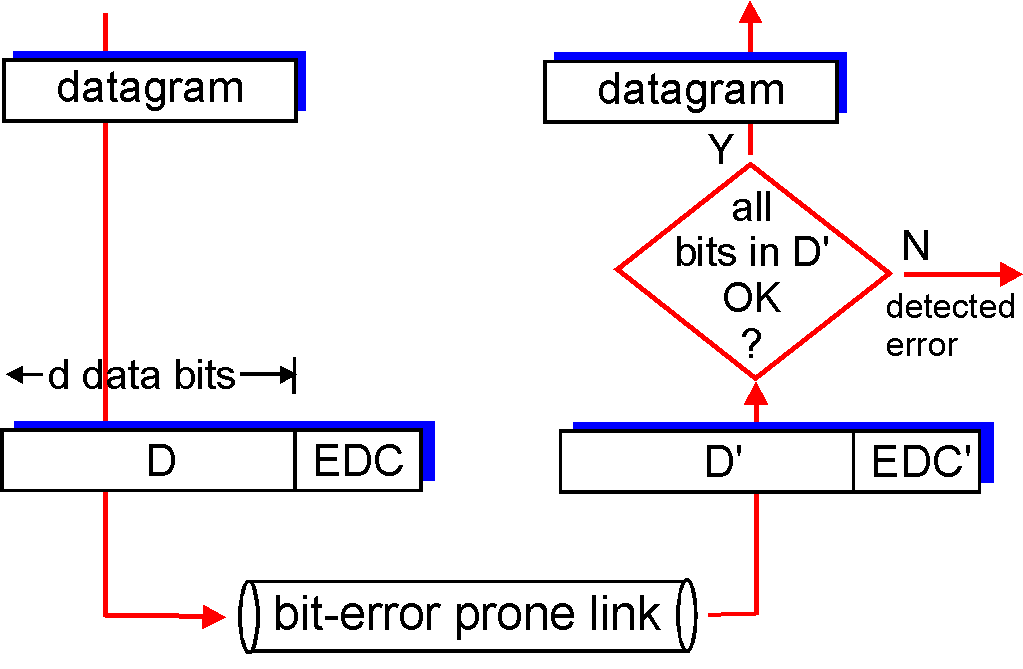
Sender: encapsulate the datagram in a link-layer frame, transmit the fame into communication link, error correction.

Receiver: receive the frame, extract the network layer datagram, error detection



Error detection and correction technique：

* EDC= Error Detection and Correction bits (redundancy)
* D = Data protected by error checking, may include header fields ,d bits

there are errors are undetected

ways to detect: parity checks, checksum, cyclic redundancy check

receiver can both detect and correct error = forward error correction

**Parity check:** even parity scheme: number of 1s in d+1 is even. Odd parity scheme: number of 1s is odd. => many errors will undetected => make a two dimension:s parity check, parity bits will also follow the scheme.

**Checksum:** sum all the bits in D and check with EDC, used in transport layer (TCP and UDP) because it operates in software, need to be simple and fast, small packet

**Cyclic Redundancy check (CRC):**  = polynomial codes, used in link layer,

Process: sender and receiver must first agree on an r+1 bit pattern = generator (G)

G ‘s leftmost bit is 1

D+R is divisible by G, no remainder = correct

Therefore, D\*2^r = nG XOR R (XOR = [(A+B)\*(N\_A + N\_B)] &D\*2^r is D’s binary form )

=> R = remainder(D\*2^r / G) base on the remainder == CRC to detect, not

Two types of network links:

1. point to point link

2. Broadcast (single shared broadcast channel: collision when receiver receive packets at the same time =>

multiple(medium) access protocol (determine when node can transmit: 1. channel partitioning (divide channel into smaller “pieces”, ex time slot (TDM), frequency (FDM)) 2. random access (allow Collison, recover from collisions, no priority, slotted ALOH, CSMA) 3. Take turns(ex: polling, token passing))

random access:

**Slotted ALOHA:** when a node has fresh frame to send, it waits until the beginning of the next slot, transmit entire frame. If there is a collision, the node detects the collision before the end of the slot, retransmit its frame in each subsequent slot with probability p.

Pros: transmit in the full rate, decentralized, simple, works well when there is only one active node

Cons: wasted slot, a lot of collisions, when there are many nodes, detect collision is more than real transmit

**Carrier sense multiple access (CSMA):** listen before transmit, collisions can still occur (because of channel propagation delay), collision detection (listen while it is transmitting, it stops and wait if someone is talking)

Ethernet CSMA/CD algorithm: like above, but if detect another transmission, abort and back off

Take turns:

Polling protocol: one node is master node, round robin tell nodes their turn to transmit. NO more collisions => efficiency, but there is polling delay

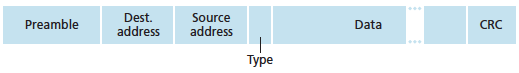
Token passing protocol: no master node, passing token to other nodes, only the node who has token can transmit until maximum frames or done. Cons: a failure can crash the entire channel, token overhead

Hosts and routers ‘s adapters have link layer address (=MAC address, LAN address, physical address), never change and unique, 48 bits, hexadecimal. If destination is right, accept. Otherwise discard. If need go through other adapter, sending adapter insert a special MAC broadcast Address in to destination field.

**Address resolution Protocol**: translate IP addresses to link-layer address. Resolve Ip Address only for hosts and router interface on the same subnet (LAN). How? Each host and router has an ARP table with TTL (the entry will delete after it).

Sender read from the table, if not found. Create ARP packet with IP address broadcast everyone, everyone checks and responds, then update the table. If send to another LAN, IP address is destination, but Mac address is router’s. then router will change the destination and source to forward again

**Ethernet**: bus and hub before become switch. Connectionless, like UDP, error just discard, lost is lost, sender resend or not base on UDP or TCP. Ethernet’s MAC protocol: unslotted *CSMA/CD with binary back off.*

structure:

MAC address 6 bytes

min 46,

max 1500 bytes

start lock, block lock, wakeup call

Switches:

Switch functions: both work with switch table (difference with forwarding table is, st uses MAC address, not IP. No need configure => self-learning)

Filtering: determine whether a frame should be forward or drop.

Forwarding: determine where the frame should be direct.

When no entry about the dest, broadcast the frame. If I am the dest, filter function => drop. If need forwarding, forward function

Properties of Link-layer Switching:

1. Elimination of collisions: buffer packet, Ethernet protocol used on *each* incoming link = >
2. Heterogeneous多样的 Links
3. Security & management: no need administrator fix, just disconnect

Drawbacks of configured hierarchically:

Lack of traffic isolation: security issue, efficiency, if the entry is not in the table, broadcast can be messy

Inefficient use of switch: when there are a lot of small groups

Managing users: if people moves, the physical cabling must be changed.

**Virtual local Area network (VLANS):** multiple virtual local area networks to be defined over a single physical local area network infrastructure. connection between VLAN and new VLAN is called VLAN trunking, using Ethernet frame + tag (which VLAN)

**port-based VLAN:** switch ports grouped (by switch management software), user only can reach its own port group, dynamically assigned (port change owner), different groups use router to send frame.

Multiprotocol label switching (MPLS): goal is high-speed IP forwarding using fixed length label (instead of IP address). Forward packet base on the label and forwarding table, no need find a path first. Each MPLS router signaling to create forwarding table

Top of Rack switch: interconnect the hosts in the rack with each other and with other switches.

Load balance advantages: balance the work load across hosts, provide a NAT-like function => preventing clients from contacting hosts directly => security

rich interconnection among switches, racks:

* increased throughput between racks (multiple routing paths possible)
* increased reliability via redundancy

Wireless and mobile network:

Base station: Cell tower and access point

Infrastructure mode: base station connects mobiles into wired network

Handoff: mobile host moves from one base station to another

Ad hoc mode: no base station, node can only transmit to other node within link coverage (single hop + no infrastructure)

IEEE 802.11: a set of MAC and physical layer specifications for implementing wireless local area network

Classify wireless network according to two criteria: => four situations

1. whether a packet in the wireless network crosses exactly one wireless hop or multiple wireless hops.
2. Whether there is infrastructure such as a base station in the network

Wireless characteristics:

1. Decreasing signal strength.越远信号越差

2. interference from other source: noise

3. multipath propagation: signal reflects off object and arriving ad destination slightly different.

4.more likely have bit error

5. Signal to noise ratio: relative measure of the strength of the received signal. Measured in dB (decibel). Larger SNR, lower the BER (bit error rate), easier for the receiver to extract the transmitted signal from noise. To do so: 1. Increase its transmission power (little gain, more energy expends by the sender)

6. A modulation with higher bit transmission rate => higher BER

7. Dynamic selection of the physical layer modulation technique can be used adapt the modulation technique to channel conditions.

8. Hidden terminal problem, may not able hear other people is transmitting, so CSMA/CD is not good enough

CDMA: belongs to channel partitioning protocol, really IMPORTANT in wireless network.

1. Each user has an unique code
2. All user share same frequency, but different chipping rate (code). Allow multiple users.
3. Encoded signal = original data bit \* chipping sequence, multiple senders the encoded message will be sum of each bit
4. Decode to get data

WIFI: IEEE 802.11 wireless LANs

Has a/b/g, three versions, g is the most popular.

All use

1. the same medium access protocol (CSMA/CA)

2. same frame structure for their link layer

3. can reduce their transmission rate

4. allow both infrastructure and ad hoc mode

Architecture: Basic service set (BSS)

BSS: contains one or more wireless stations and central base station (known as access point), identify by MAC address. Two BSS connect by routers or switch.

When network installs an AP, assign one or two-word Service Set Identifier (SSID) and a **channel** number to the AP (several AP can share one channel number, 11 channels). If two channel are non-overlapping if and only if they are separated by four or more channels

Wifi Jungle: is any physical location where a wireless station receives a sufficiently strong signal from two or more APs. Have to pick one AP to associate, how?

**Associating** = wireless station creates a virtual wire between itself and the AP.

802.11 requires that an AP periodically send beacon frames (SSID and MAC), wireless host scans the 11 channels, seek any unknown AP and select (no algorithm).

Two ways to scan: passive scanning (APs send beacon frames) and active scanning (broadcasting a probe frame from host).

After select, send an association request frame to AP, AP responds with an association response frame. The AP will give the IP address in its subnet.

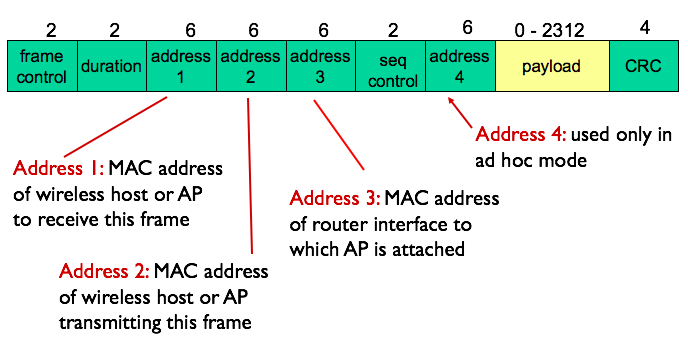
Authentication server using passwords to restrict users

host may transmit data frame at the same time. So we use CSMA/CA and ARQ

Why not collision detection? 1. Able to detect => sending (station’ s own signal) and receiving (determine whether other people are transmitting) at the same time. strength of receiving is very small, too much cost to upgrade 2.even rich enough, fading and hidden terminal problem still is a problem.

CSMA/CA: source wait time = distributed inter frame space , send data. Destination receive? wait, waiting time = short Inter frame spacing, send ack. source never receive ack, channel is busy? Assume error, random backoff time, retransmit. error again? Give up. Still may happen collision. SO, add Request to Send (RTS) control frame and Clear to Send (CTS) control frame to reserve access to the channel. Want to send data? Send RTS to AP, indicates needed transmitting time and ACK frame. AP received? Broadcasting a CTS frame, this gives the permission and tell others in AP’s range => no more hidden. May collision, but since RTS are small, so easy to recover. Destination ack one person, also using broadcast. But CTS and RTS causing delay, so only use for big data.

802.11 frame:

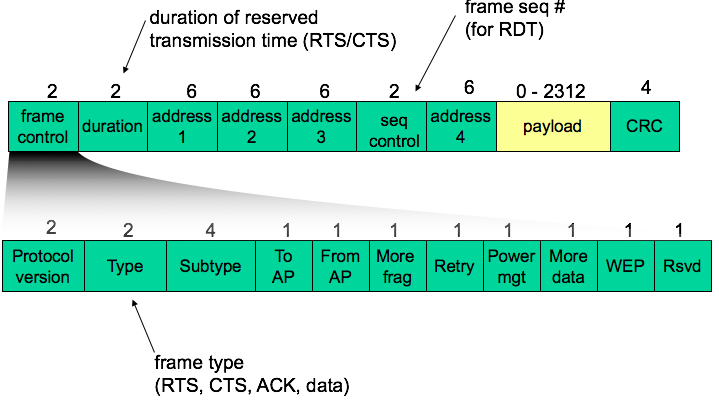
address 2: source MAC

address 1: transmitting AP’s MAC

address 3: important,

help AP to construct the

Ethernet frame



Mobility:

If host remains in the same IP subnet, IP address doesn’t change and keep TCP connections, switch will self-learning and update.

Else, IP change, TCP connection lost

Advanced features in 802.11

1. Rate adaptation: SNR and BER changes automatically base on the distance (unacked frame)
2. Power management: a node can go to sleep, AP will not transmit frame to this node. When node is wake if AP to mobile frames to be sent.

Personal area network:

Bluetooth (802.15.1): replacement for cables (headphone, mouse), Ad hoc network, range = piconet, up to 8 devices, one master, others are slaves (need permission to send)

Cellular Internet Access:

Motivation: mobile on a bus and train.

Cell = Geographic coverage areas, each cell has its own base transceiver station (BTS)

1G: voice only communication

GSM = 2G: voice and data, combined FDM/TDM, has a base station controller (BSC, connect BTS and MSC) which allocate BTS radio channel to paging, mobile switching center (MSC) provides user authorization and accounting (determine whether a mobile device is allowed to connect the cellular network), contain 5 BSC, and gateway MSC

3G: increasing emphasis on data capabilities and higher speed radio access links, new cellular data network operates in parallel with existing cellular voice network,

4G (LTE): Evolved packet core (EPC): no separation between voice and data. IP packet tunnelled from base station to gateway.

Security:

1. confidentiality: only sender, intended receiver should “understand” message contents

2. authentication: sender, receiver want to confirm identity of each other

3. message integrity: sender, receiver want to ensure message not altered (in transit, or afterwards) without detection

4. access and availability: services must be accessible and available to users

WEP: in order to be security

Each packet separately encrypted. Symmetric stream cipher (encrypted each bit, ex: RC4), WEP use RC4

encryption

1. Sender calculates Integrity check value (ICV), each side has 104 bit shared key.
2. Sender creates initialization vector(IV,24 bits), append to share key => generator to get keystream
3. Mac payload = IV + key ID + (data + ICV) = > encrypted by RC4 = bytes of keystream => XORed with data + ICV

Decryption:

1. extracts IV

2. IV + shared secret key = pseudo random generator => keystream

3. XOR keystream decrypt data + ICV

end authentication with NONCE => WEP authentication between AP and host

s want to connect, r send nonce (R), s reply r = encrypted R with shared secret key

Security hole of WEP: 24 bit IV per frame -> IV will be reused

Attacker let alice to encrpt known plaintext d\_i, ci = di xor ki^iv => only don’t know ki^iv and it knows the encrypting key sequence. When IV reuse, attacker knows

Improvement:

1. stronger forms

2. key distribution

3. uses authentication server (AS) separate from AP (client and AS generate Master key (MK), client and AS derive Pairwise Master Key (PMK), AS sends to AP, client and AP uses PMK to derive Temporal key (TK) to encryption)

what is mobility?

High mobility: mobile user passing through multiple AP and maintaining ongoing connections

Approaches: mobile has a permanent address and home agent at home, care of address is the address for current using foreign address, recorded at home network.

Correspondent the one want to send data.

Visited network: network mobile currently in, router in it is foreign agent

1. routing handle it: routers advertise permanent address of mobile node via usual routing table exchange not working

2. end system handle it:

registration: mobile contact foreign agent on entering network, foreign agent contact home network, care of address established

1. *indirect routing:* communication from correspondent to mobile goes through home agent, then forwarded to remote, inefficient

*2. direct routing:* correspondent gets foreign address of mobile, sends directly to mobile, if move to new visited network, anchor (old) foreign agent forward packets to the new agent

home network has a home location register (HLR) = database for all the info about devices

visited network has a visitor location register (VLR) database with entry of each user currently in network

firewall: stateless packet filter (don’t care about the traffic, only base on the packet header), statefull packet filter (care about traffic, track TCP and UDP connection) application gateway (a gateway between host and network), IDS: intrusion detection system (deep inspection on content, in case of virus)