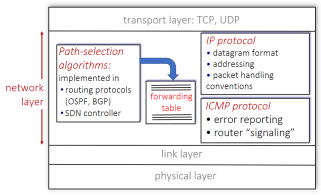
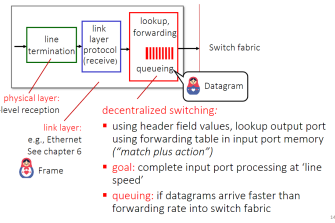
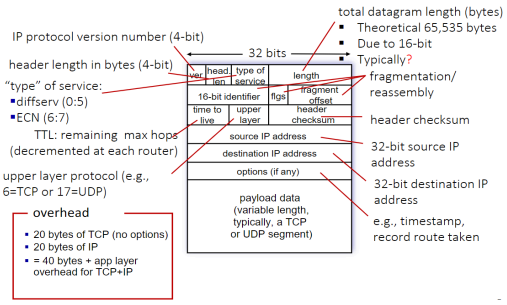
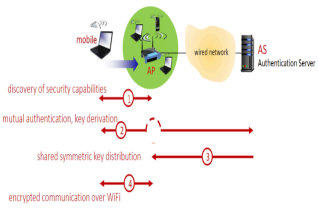
Transport segment from sending to receiving hosts | **On sending side**: Encapsulates segments into datagrams | **On receiving side**: application transport network link physical Delivers segments to transport layer Network layer protocols in every host, router Router: Examines IP header fields in all datagrams passing through it | **Forwarding data plane**: move packets from a router's input link to appropriate output link, local-action, takes place in a few nanoseconds, and implemented inhardware | Local per-router function,Determines how to forward datagram from router input port to output port | **Routing, management control plane**: determine route taken by packets from source to destination, in milliseconds, implemented in software, and Routing algorithms | Network - wide logic, Determines how to route, datagram among routers, along end-end path | **Routing Algorithms**: Handle both forwarding and routing functions,communicates with other router's algorithm to compute the values for its forwarding table, exchanging routing messages containing routing information according to a routing protocol | **SDN**: Physically separate remote controller, Controller is implemented in software, Controller computes, installs forwarding tables in routers, Router performs forwarding only. | **IPv4 Address**: Unique numerical label assigned to a host when it connects to the Internet, 32-bit number uniquely identifies network interface between a host and router Represented with the dotted-quad notation (4 groups of numbers called octets) Each octet can have up to 3 decimal numbers e.g.: 200.23.16.5 | **Interface**: connection between host/router and physical link, router's have multiple interfaces, host has one or two physical interface | **Switch**: Transfer packet from input buffer to appropriate output buffer| each switch has a switch table, each entry: ▪ (MAC address of host, interface to reach host, time stamp) ▪ looks like a routing table switch learns which hosts can be reached through which interfaces when frame received, switch "learns" location of sender: incoming LAN segment records sender/location pair in switch table | **Buffering** required when datagrams arrive from fabric faster than link transmission rate. **Drop policy**: Scheduling discipline chooses among queued datagrams fortransmission Datagrams can be lost due to congestion, lack of buffers | **Subnet** ▪ device interfaces that can physically reach each other without passing through an intervening router | **Differentiated Services Code Point (DSCP)**: Total 8 levels.specifies level of service and priority for network traffic o Class Selector 0 (CSO): a **Best Effort** or Default transmission, no special treatment or priority | interfaces connected by a wired Ethernet interfaces connected by Ethernet switches or by wireless WiFi interfaces connected by WiFi base station | **IP addresses** have structure: Subnet part: devices in same subnet have common high order bits, Prefix or Network ID, Host part: remaining low order bits, Host ID. Recipe for defining subnets: detach each interface from its host or router, creating "islands" of isolated networks, each isolated network is called a subnet | **CIDR** : Classless Inter–Domain Routing | Idea: Flexible division between prefix and suffix | Offer better tradeoff between size of routing table and efficient use of IP address space | **Authority**; Nonprofit organization, allocates IP addresses, manages DNS root servers, assigns domain names, and, resolves domain name disputes, assigns IP addresses to RIRs, RIRs form Address Supporting Organization of ICANN (ASO-ICANN), Handle the allocation and management of address within their regions | Which assign subnet portion to Large institutions (ISPs) Which assign addresses to Hosts | Hierarchical addressing allows efficient advertisement of routing information | The ability of advertising multiple networks using a single prefix referred to as **address/route aggregation**, or route summarization. Renumbering organizations is costly. | **DHCP**: Dynamic Host Configuration Protocol: Dynamically get address from a server •"plug-and-play". DHCP message encapsulated in UDP, encapsulated in IP | Goal: allow host to dynamically obtain IP address from network server when it joins network o can renew its lease on address in use ▪ allows reuse of addresses (only hold address while connected/"on") ▪ support for mobile users who want to join network (more shortly) | **DHCP overview**: ▪ host broadcasts "DHCP discover" msg [optional] DHCP server responds with "DHCP offer" msg [optional] host requests IP address: "DHCP request" msg DHCP server sends address: "DHCP ack" msg | **Implementation NAT router must**: outgoing datagrams: replace (source IP address, port #) of every outgoing datagram to (NAT IP address, new port #) 0 . ... remote clients/servers will respond using (NAT IP address, new port #) as destination address. | **"autonomous systems" (AS)**: Region of a network under a single administrative entity | **incoming** datagrams: replace (NAT IP address, new port #) in dest fields of every incoming datagram with corresponding (source IP address, port #) stored in NAT table | NAT(16 bit) is controversial: o routers should only process up to layer 3 ▪ violates end-to-end argument ▪ NAT possibility must be considered by app designers, e.g., P2P applications | **ICMP**: "Signaling" ▪ Hosts & routers communicate network- level information o error reporting: unreachable host, network, port, protocol ▪ HTTP session: "Destination network unreachable" ▪ The router created and sent the ICMP message o Status check: echo request/reply (used by ping) ▪ ICMP is in Network layer in between IP and TCP/UDP: o ICMP messages are in IP payload o Upper layer protocol number of 1 Next header: identify upper layer protocol for data | **Routing protocol goal**: determine "good" paths o equivalently, routes o from sending hosts to receiving host, o through network of routers ▪ Path: sequence of routers packets traverse from given initial source host to destination host o Distance: shortest o Loss: least congested o Latency: fastest o Establish paths between nodes | **Link-state Routing algo**: Implementation of Dijkstra's algorithm o net topology, link costs known to all nodes ▪ accomplished via "link state broadcast" ▪ all nodes have same info ▪ computes least cost paths from one node ('source') to all other nodes gives forwarding table for that node ▪ iterative: after k iterations, know least cost path to k destinations o link costs depend on traffic volume o link costs are not symmetrico Symmetric if the load both directions on the link is the same.o route oscillation can occur | **Distance vector**: a router's least-known costs to other routers ▪ Each node periodically sends its own estimated distance vector to neighbors only when its DV changes ▪ when x receives a new DV from a neighbor, it updates its own DV using the Bellman - Ford equation | **Each router maintains a table** o Best known distance from itself and its neighbors to all routers ▪ Each local iteration caused by: o Local link cost change o Message from neighbor ▪ Notify neighbors only when its DV changes o neighbors then notify their neighbors if necessary | **Internet routing protocols** o constructing and updating forwarding tables at routers ▪ scaling ▪ computing, communicating, and storing routing information require enormous amounts of memory o can't store all destination addresses in forwarding tables! o forwarding table exchange would swamp links! ▪ administrative autonomy o internet is network of networks each network admin may want to control routing in its own network | Has two levels ▪ Each AS runs an intra-domain routing protocol that establishes routes within its domain o AS: region of network under a single administrative entity o Link State o Distance Vector ASs participate in an inter-domain routing protocol that establishes routes between domains. | **Forwarding** table is configured by both **intra**- and **inter**-AS routing algorithm o Intra-AS sets entries for internal destinations o Inter-AS & Intra-AS sets entries for external destinations | **Advertising multiple networks** using a single prefix referred to as address/route aggregation, or route summarization 16 Hierarchical addressing: Route Aggregation | **Hot potato routing**: send packet towards closest of two routers. | all routers need run both intra- and inter- domain routing protocols | **IGP**: "Interior Gateway Protocol" = Intra-domain routing protocol o provide internal reachability | **RIP**: Routing Information Protocol o Distance vector algorithm o Distance metric: # of hops (max = 15 hops) RIP Advertisements: o Distance vectors: exchanged among neighbors every 30 sec via Response Message o Each advertisement: list of up to 25 destination nets within AS o Link Failure and Recovery ▪ If no advertisement heard after 180 sec à neighbor/link declared dead o routes via neighbor invalidated o new advertisements sent to neighbors o neighbors in turn send out new advertisements (if tables changed) o link failure info quickly propagates to entire net RIP Table processing ▪ RIP routing tables managed by application-level process called route-d ▪ advertisements sent in UDP packets, periodically repeated | **OSPF**: Open Shortest Path First o Uses Link State algorithm ▪ LS dissemination ▪ Topology map at each node ▪ Route computation using Dijkstra's algorithm o OSPF advertisement carries one entry per neighbor router o Advertisements disseminated to entire AS (via flooding) ▪ Carried in OSPF messages directly over IP (rather than TCP or UDP) determine a shortest-path tree to all subnets ▪ the network administrator configures link costs ▪ Router broadcast routing information to all routers in AS ▪ broadcasts LS periodically, at least once every 30 minutes o OSPF protocol sends HELLO message to neighbor to check link status o Security: all OSPF messages authenticated o Multiple same-cost paths allowed o For each link, multiple cost metrics for different TOS o Integrated uni- and multi-cast support: ▪ Multicast OSPF uses same topology database as OSPF o Hierarchical OSPF in large domains | **BGP**: Border Gateway Routing Protocol protocol that glues the thousands of ISPs together o a BGP connection spans two ASs is called an **eBGP** connection, and ▪ a BGP session between routers in the same AS is called an **iBGP** connection o iBGP connections do not always correspond to physical links to propagate the reachability information, both iBGP and eBGP sessions are used | **Data-Link layer** responsibility transferring frames from one node to adjacent node over a link. Frame transfers over different links using associate link protocols | **Link layer services**(simliar to transport layer, ex checkum, determine misdelivery of packets): Flow Control: o pacing between adjacent sending and receiving nodes ▪ Error Detection: o errors caused by signal attenuation, noise, interference o receiver detects presence of errors: ▪ signals sender for retransmission or drops frame ▪ Error Correction: o receiver identifies and corrects bit error(s) without resorting to retransmission | **Half-duplex** nodes at both ends of link can transmit, but not at same time ▪ Framing o link-layer protocols encapsulate datagram into frame, adding header, and trailer ▪ structure of the frame is specified by the link-layer protocol o Continuous bit stream at physical layer ▪ Link access o channel access if the medium is share | **NIC:** interface between communication line and link. Network interface card, network adapter, LAN adapter, physical network interface, or driver ▪ implements many link layer services including framing, link access, error detection, and so on ▪ much of a link-layer controller's functionality is implemented in hardware Point-to-point protocol (PPP) for dial-up access ▪ enables dial-up connections to the Internet ▪ link between host and switch ▪ Switched Ethernet to broadcast (shared wire or medium) ▪ traditional Ethernet ▪ Medium Access Protocol is needed ▪ need to detect collision ▪ A medium access control (MAC) protocol specifies frame transmission onto the link Channel Partitioning Protocols o Time Division Multiple Access (TDMA) (need to allocate the time slot to a connecting host) TDM uses multiple wires for the host } Channel Partitioning Protocols o Frequency Division Multiple Access (FDMA) | **CDMA** allows multiple users to simultaneously use the same frequency band by assigning unique codes to each user to differentiate their data.all users share same frequency, but each user has own "chipping" sequence (i.e., code) to encode data o Chipping sequence or unique code rate is much higher than data o allows multiple users to "coexist" and transmit simultaneously with minimal interference▪ encoding: o inner product: (original data) X (chipping sequence) ▪ decoding: o summed inner-product: (encoded data) X (chipping sequence)channel sums together transmissions by sender 1 and 2using same code as sender 1, receiver recovers sender 1's original data from summed channel data | **Multiple Access Protocols** 16 ▪ Random Access Protocols o a transmitting node always transmits at the full rate of the channel o If collision occurs, ▪ each node repeatedly retransmits its frame till it gets through ▪ each node retransmits with an independent random delay | **Switches**: o operate at the link layer o switch link-layer frames not network-layer datagrams o don't recognize network-layer addresses, and o don't use routing algorithms like OSPF o use link-layer addresses to forward link-layer frames | **32-bit IP address**: o network-layer address o Configured, or learned dynamically o used to get datagram to destination IP subnet ▪ MAC address: o used to get datagram from one interface to another physically connected interface (same network) o 48-bit MAC address (e.g. 1A-2F-BB-76-09-AD in HEX) Unique, hard- coded in the adapter ROM when it is built ▪ Broadcast address (FF-FF-FF-FF-FF-FF) ▪ Send the frame to all adapters | ARP Table: IP to MAC address mappings for some LAN nodes ▪ Address map is cached in RAM | **Zero padding** extend a signal (or spectrum) with zeros. ▪ A frame check sequence (FCS) is an error-detecting code | **ARP** (Address Resolution Protocol) is a link-layer protocol used to map an IP address to a machine's physical hardware address on a local network segment. | Both connect segments of LANs ▪ Hubs are layer-1 devices that act on bits rather than frames o A hub-based star topology is also a broadcast LAN o Hosts connected to hub are in the same contention domain ▪ Switches are layer-2 devices that forward the messages to the selected port o Hosts connected by switches are in the same broadcast domain ▪ Point-to-point link between a computer and a switch | **Preamble** in Ethernet serves to synchronize the receiver's clock with the incoming data stream and allows for the accurate detection of the beginning of a frame, facilitating collision detection and error prevention in data transmission | **Connectionless service** =: No handshaking between sending and receiving adapter. o analogous to ▪ IP's layer-3 datagram service and ▪ UDP's layer-4 connectionless service ▪ **Unreliable service**: receiving adapter doesn't send ACKs or NACKs to sending adapter o stream of datagrams passed to network layer can have gaps o gaps will be filled if app is using TCP o otherwise, app will see the gaps | **Taking-turns protocols** o Polling protocol ▪ master-slave concept, master node polls slave node in a round-robin fashion o Token-passing protocol ▪ a special-purpose frame, token, is exchanged among the nodes in some fixed order ▪ after receiving, a node holds it, only, if it needs to transmit ▪ otherwise, it immediately forwards it to the next node | **Shared medium with bus or star topology** with hubs o Multiple active users at a time, ▪ collision results in no packet being received (interference) o No active user at all, channel goes idle (bandwidth wasted) ▪ Thus, only one user send at a time is desired o Half-duplex: nodes take turns in transmissions ▪ Baseband communication: o FDMA doesn't offer baseband communication (!) ▪ High sender utilization is required o TDMA doesn't give high sender utilization (Stop and Wait) o Node's turn delay proportional to number of hosts ▪ CDMA is suitable for wireless cellular communication ▪ Simple distributed algorithm is required o no fancy token-passing schemes that avoid collisions | **Collisions can occur**: o propagation delay means ▪ two nodes may not hear each other's carrier ▪ Just started transmission ▪ Collision: o entire packet transmission time wasted ▪ role of distance and propagation delay in determining collision prob | **Colliding transmissions aborted**, reduces channel wastage o Jamming signal: inform all other stations that they shouldn't transmit ▪ Implementation: o Easy to implement in wired LANs: ▪ measure signal strengths, ▪ compare transmitted and received signals o Difficult in wireless LANs | **Point-to-point** in star topology with switches ▪ Full duplex: can send and receive at the same time ▪ Switches are link layer device o stores and forwards Ethernet frames o examines frame header and selectively forwards frame based on MAC destination address ▪ Transparent o hosts are unaware of presence of switches o a host/router addresses a frame to another host/router; not to a switch o Same as a router, switch output interfaces have buffers ▪ plug-and-play, self-learning o Switches do not need to be configured ad hoc mode ▪ no base stations ▪ nodes can only transmit to other nodes within link coverage ▪ nodes organize themselves into a network: route among themselves interference from other sources on wireless network frequencies: motors, appliances •signal-to-noise ratio o larger SNR – easier to extract signal from noise (a "good thing") ▪ SNR versus BER tradeoff o given physical layer: increase power - > increase SNR->decrease BER o SNR may change with mobility: dynamically adapt physical layer (modulation technique, rate) | **Host**: must associate with an AP o scans channels, listening for beacon frames containing service set identifier (SSID) and AP's MAC address o selects AP to associate with; initiates association protocol o may perform authentication o will typically then run DHCP to get IP address in AP's subnet Passive scanning: (1) Beacon frames sent from APs (2) Association Request frame sent: H1 to selected AP (3) Association Response frame sent from selected AP to H1 Active scanning: (1) Probe Request frame broadcast from H1 (2) Probe Response frames sent from APs (3) Association Request frame sent: H1 to selected AP (4) Association Response frame sent from selected AP to H1 | **Multiple access** has two different channel accessing mechanisms o the distributed coordination function (DCF) and ▪ Random access protocol ▪ CSMA with collision avoidance (CSMA/CA) o point coordination function (PCF) ▪ Taking – Turns Protocol ▪ Polling protocol: master-slave concept, master node polls slave node in a round-robin fashion (time slices, time quanta): o the enhanced distributed coordination function (EDCF) Like Ethernet, uses CSMA: o random access o carrier sense: listen before transmitting ▪ don't collide with ongoing transmission ▪ Unlike Ethernet: o no collision detection – transmit all frames to completion o with acknowledgment – because without collision detection, you don't know if your transmission collided or noto difficult to receive (sense collisions) when transmitting due to weak received signals (Path Loss) o can't sense all collisions in any case: hidden terminal •avoid collisions -- **CSMA/CA(Collision Avoidance)** | **Short IFS** o Shortest IFS (used for ACK, CTS, poll response) o Used for immediate response actions ▪ Distributed coordination function IFS (DIFS) o Second Longest IFS (data, RTS) o Used as minimum delay of asynchronous frames contending for access ▪ Extended Interframe space (EIFS) o Longest IFS o Used when received frame containing errors ▪ Point coordination function IFS (PIFS) o Mid length IFS o Used by centralized controller in PCF scheme when using polls | **Idea**: sender "reserves" channel use for data frames plus ACK o sender sends request-to-send (RTS) packet to AP using CSMA ▪ RTSs may still collide with each other (but they're small!) o AP broadcasts clear-to-send (CTS) in response to RTS ▪ CTS heard by all nodes o sender transmits data frame o other stations defer transmissions | **Network Allocation Vector (NAV)**: o a virtual carrier-sensing mechanism **CW(i) =** (CW(i-1)+1)*2 –1' | o **send HTTP** request, client first opens TCP socket to web server ▪ TCP SYN segment (step 1 in 3-way handshake) inter- domain routed to web server ▪ web server responds with TCP SYNACK (step 2 in 3- way handshake) ▪ TCP connection established! ▪ HTTP request sent into TCP socket ▪ IP datagram containing HTTP request routed to www.google.com ▪ web server responds with HTTP reply (containing web page) ▪ IP datagram containing HTTP reply routed back to client | Network security: confidentiality, authentication, message integrity, accessa availability | **Packet sniffing** is the process of intercepting and monitoring data packets as they travel over a network ▪ wiretapping and planting spy software on any of nodes involved ▪ promiscuous NIC reads all packets passing by | **IP spoofing** : active attack threatening integrity o creation of "raw" IP packets with a false source IP address ▪ to impersonate a host o allows to carry out malicious actions ▪ stealing information, infecting device with malware, or crashing server **Packet filtering**: o most common way to find IP spoofing o detect inconsistencies between packet IP address and desired IP addresses in access control list (ACL) ▪ maintained in routers and firewalls | **Ingress filtering**: o

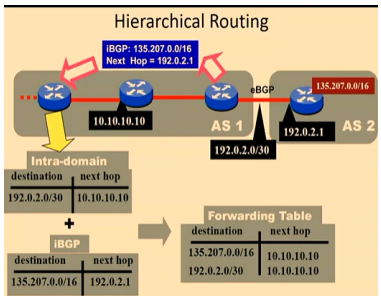
assesses incoming packets whether a permitted source IP address o packets which look suspicious will be dropped ▪ Egress filtering: o assesses outgoing packets whether source IP address on the organization's network o designed to prevent IP spoofing from insiders | **DDOS**: o generates many requests to a server that crashes o may intercept and delete a server's response to a client that shows the server is not responding o may also intercept requests from the clients, causing the clients to send requests many times and overload the system | **identify**: o Suspicious amounts of traffic from a single IP address or IP range o A flood of traffic from users who share a single behavioral profile, such as device type, geolocation, or web browser version o An unexplained surge in requests to a single page or endpoint o Odd traffic patterns such as spikes at odd hours of the day | **Synchronize Attack**: o Buggy implementations allow unfinished connections to eat up all memory, leading to crash o Better implementations limit the number of unfinished connections o Once limit reached, new SYNs are dropped ▪ Countermeasures o filter out flooded packets (e.g., SYN) before reaching host ▪ throw out good with bad o traceback to source of floods (most likely an innocent, with a computer which is compromised) | An application gateway is an application-specific server through which all application data- must pass require all telnet users to telnet through gateway. 2. for authorized users, gateway sets up telnet connection to destination host. Gateway relays data between 2 connections 3. router filter blocks all telnet connections not originating from gateway | **Hash function properties**: o many-to-1 o produces fixed-size msg digest (fingerprint) o given message digest x, computationally infeasible to find m such that x = H(m) | A digital signature is a secure, cryptographic way to confirm the authenticity of a digital message and the identity of the sender. | **Certification authority (CA)**: binds public key to particular entity When Alice wants Bob's public key: o gets Bob's certificate Nonce: number (R) used only once –in-a-lifetime | **Internet Protocol Security (IPsec)** Provides datagram – level: o Integrity o Authentication o replay attack prevention o Confidentiality. Two modes of operation: **transport mode**: o only datagram payload is encrypted, authenticated **tunneling mode**: o entire datagram is encrypted, authenticated o encrypted datagram encapsulated in new datagram with new IP header, tunneled to destination payload | before sending data, the source and destination entities create a network-layer logical connection , This logical connection is called a "**security association (SA)**" SA is a simplex (unidirectional) connection from source to destination If both entities want to send secure datagrams to each other, then two SAs need to be established Both entitles maintain state information about SA o recall: TCP endpoints also maintain state info IP is connectionless; IPsec is connection oriented! | **policy**: o Security policy database (SPD) indicates "what" to do with arriving datagram, depending on ▪ source/ destination IP address ▪ protocol number o Security association database (SAD) indicates "how" to do it | 1. Choose 2 large prime #s p = 5, q = 7 2. Compute n = pq = 5*7 = 35, z = (p-1 = 4)*(q-1 = 6) = 24 3. Choose e = 5 (with e = 5 < n = 35) that has no common factors with z = 24 o e = 5, z = 24 are "relatively prime" 4. Choose d = 29 such that ed – 1 = (5*29 – 1 = 144) is exactly divisible by z = 24 (i.e. 144/24 = 6) o in other words: ed (= 145) mod z (=24) = 1 (% = modulus or remainder) 5. Public key is (n,e)≡(35,5) and Private key is (n,d) ≡ (35,29)1. (n,e)≡(35,5) and (n,d) ≡ (35,29) as computed. Interpreting each letter as # between 1- 26 o with a being 1, and z being 26. To encrypt bit pattern, m, compute, c = me mod n o i.e., remainder when m is / by nTo decrypt received bit pattern, c, compute m = cd mod n o i.e., remainder when cd is / by n 3. Magic happen $m = me \bmod n \; d \bmod n = med \bmod n$











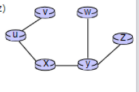
- Example: Given address: 167.199.170.82/27
- Subnet mask: /27
- First address: 167.199.170.64/27
- Last address: 167.199.170.95/27
- Subnet mask in binary (dotted-octet):
  - 11111111 . 11111111 . 11111111 . 11100000
- Subnet mask in decimal (dotted-decimal): 255.255.255.224

A host Address	10100111 . 11000111 . 10101010 . 01010010	Prefix / Suffix
Network Address	10100111 . 11000111 . 10101010 . 01000000	Prefix / Suffix
	10100111 . 11000111 . 10101010 . 01011111	Prefix / Suffix
Subnet Mask	11111111 . 11111111 . 11111111 . 11100000	Prefix / Suffix

AND!

Dijkstra's algorithm: Complexity

itep	N'	v D(v),p(v)	w D(w),p(w)	x D(x),p(x)	y D(y),p(y)	z D(z),p(z)
0	u	2,u	5,u	1,u	∞	∞
1	ux	2,u	4,x		2,x	∞
2	uxy	2,u	3,y			4,y
3	uxyv		3,y			4,y
4	uxyvw					4,y
5	uxyvwz					



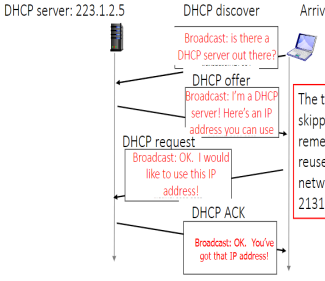
- algorithm complexity: *n* nodes
  - each of *n* iteration: need to check all nodes, *w*, not in *N'*
  - $n(n+1)/2$ comparisons: $O(n^2)$ complexity
  - more efficient implementations possible: $O(n \log n)$
- message complexity:
  - each router must *broadcast* its link state information to other *n* routers
  - efficient broadcast algorithms: $O(n)$ link crossings to disseminate a broadcast message from one source
  - each router's message crosses $O(n)$ links: overall message complexity: $O(n^2)$

each node:

wait for (change in local link cost or msg from neighbor)

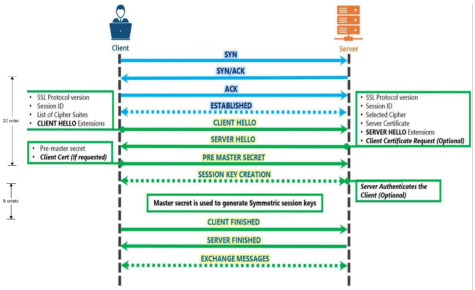
recompute DV estimates using DV received from neighbor

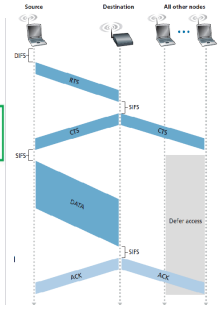
if DV to any destination has changed, *notify* neighbors

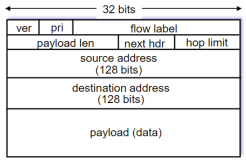


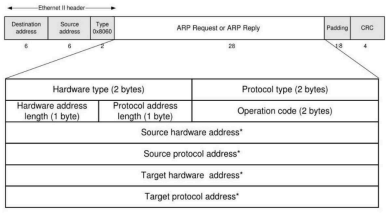
The two steps above can be skipped "if a client remembers and wishes to reuse a previously allocated network address" [RFC 2131]

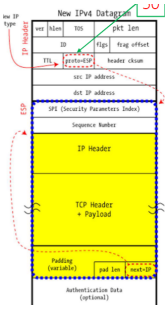
- ICMP: [RFC 792]
- ICMP:
  - Type: type of the message
  - Code: further qualifies the specific message
  - Checksum: checksum for ICMP header plus data
  - Message: contains specific data based upon the type and code fields
  - Data: if present, contains original IP header (20 – 60 bytes) plus 8 bytes of original IP data
    - To identify the error causing datagram











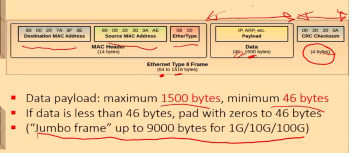
- Filtering: determines whether a frame should be forwarded or dropped
- Forwarding: determines the interfaces to which a frame should be directed and moved
- Switch filtering and forwarding are done with a switch table

when a frame arrives at switch:

1. record incoming link, MAC address of sending host
2. index switch table using destination MAC address
3. if entry found for destination
   then {
   if destination on segment from which frame arrived then drop frame;
   else forward frame on interface indicated by entry;
   }
   else flood; forward on all but interface on which the frame has arrived

Ethernet Frame Structure

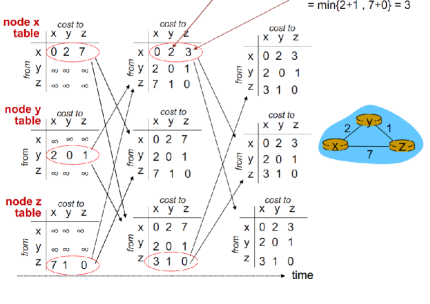
Application Layer	▪ Broadcasted frames are dropped if address mismatch
Transport Layer	▪ Type: indicates the types of the Ethernet frame o (Ethernet II, 802.2 LLC,...)
Network Layer	▪ CRC: checked at receiver, if error is detected, the frame is simply dropped
(Data) Link Layer	
Physical Layer	▪ Data payload: maximum 1500 bytes, minimum 46 bytes ▪ If data is less than 46 bytes, pad with zeros to 46 bytes ▪ ("Jumbo frame" up to 9000 bytes for 1G/10G/100G)



Distance – Vector Algorithm

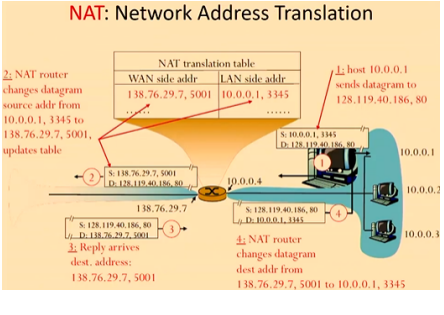
$D_x(y) = \min\{c(x,y) + D_y(y), c(x,z) + D_z(y)\}$
$= \min\{2+0 , 7+1\} = 2$

$D_x(z) = \min\{c(x,y) + D_y(z), c(x,z) + D_z(z)\}$
$= \min\{2+1 , 7+0\} = 3$



	hubs	routers	switches
traffic isolation	no	yes	yes
plug & play	yes	no*	yes
optimal routing	no	yes	no
cut through	yes	no	yes*

NAT: Network Address Translation



Intra-AS Routing: IGP

RIP Advertisements:

- Distance vectors: exchanged among neighbors every 30 sec via Response Message (also called advertisement)
- Each advertisement: list of up to 25 destination nets within AS