EECS 388: Introduction to Computer Security

Network Attacks and Defenses, Part I: Networking Concepts

Feb 18, 2015

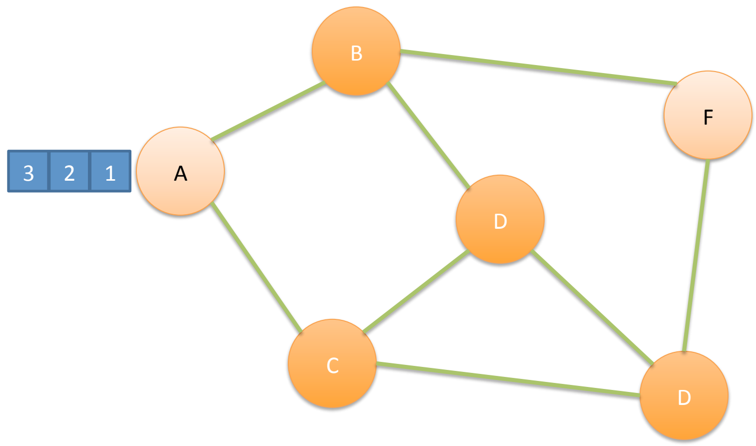
1

Circuit and Packet Switching

- Circuit switching
  - Legacy phone network
  - Single route through sequence of hardware devices established when two nodes start communication
  - Data sent along route
  - Route maintained until communication ends
- Packet switching
  - Internet
  - Data split into packets
  - Packets transported independently through network
  - Each packet handled on a best efforts basis
  - Packets may follow different routes

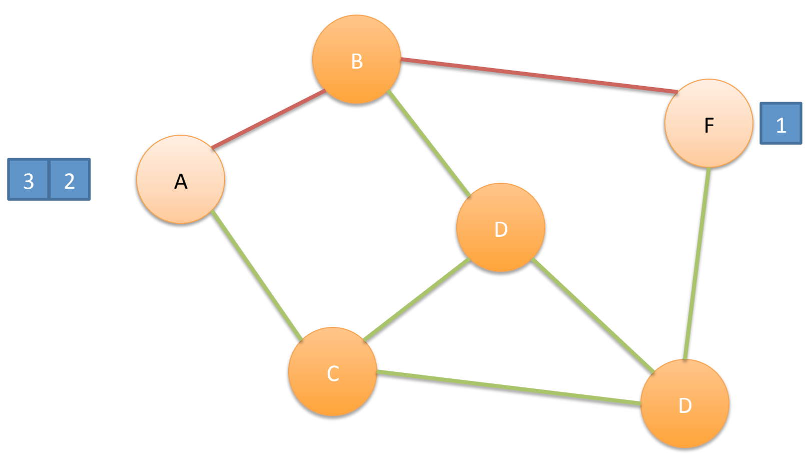
2

Packet Switching



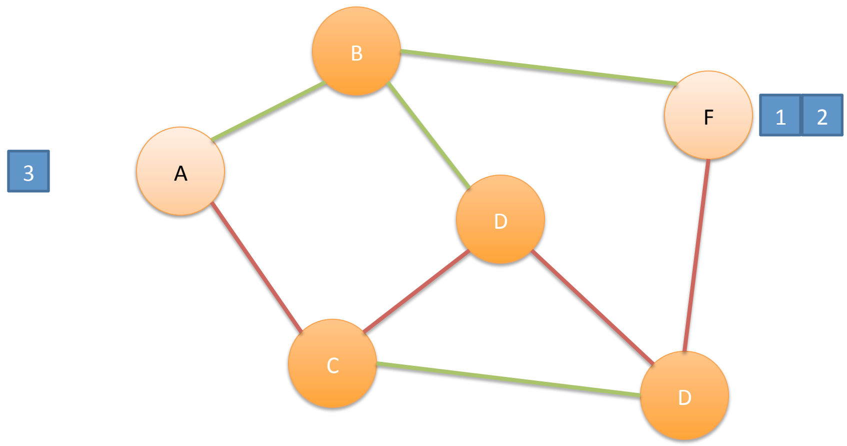
3

Packet Switching



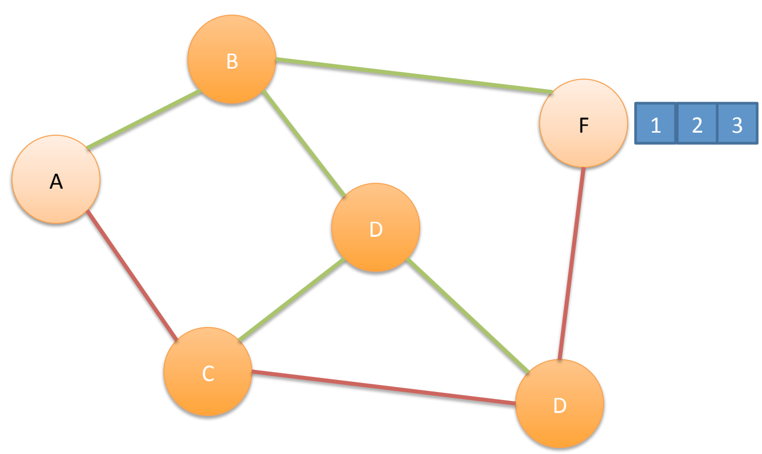
4

Packet Switching



5

Packet Switching



6

Network Layers

- Network models typically use a stack of layers
  - Higher layers use the services of lower layers via encapsulation
  - A layer can be implemented in hardware or software
  - The bottom-most layer must be in hardware
- A network device may implement several layers
- A communication channel between two nodes is established for each layer
  - Actual channel at the bottom layer
  - Virtual channel at higher layers

7

Reference Models

	OSI Model	Internet Model	Internet Protocol Suite
7	Application		
6	Presentation		
5	Session	Application	FTP, HTTP
4	Transport	Transport	TCP, UDP
3	Network	Internet	IP (ICMP) ARP, RARP
2	Link	Net. Interface	Not Specified
1	Physical	Physical	

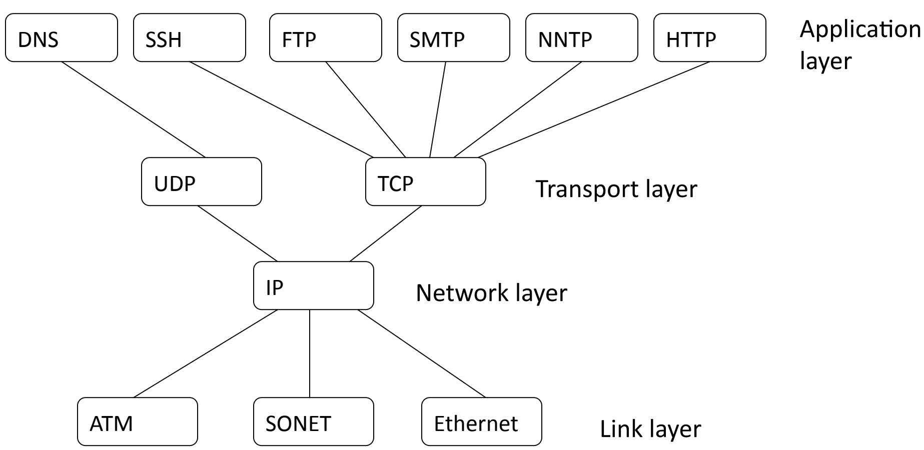
8

Protocols

- A protocol defines the rules for communication between computers
- Protocols are broadly classified as connectionless and connection oriented
- Connectionless protocol
  - Sends data out as soon as there is enough data to be transmitted
  - E.g., user datagram protocol (UDP)
- Connection-oriented protocol
  - Provides a reliable connection stream between two nodes
  - Consists of set up, transmission, and tear down phases
  - Creates virtual circuit-switched network
  - E.g., transmission control protocol (TCP)

9

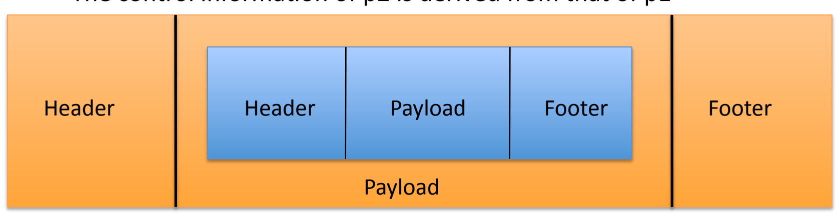
Layering of protocols



10

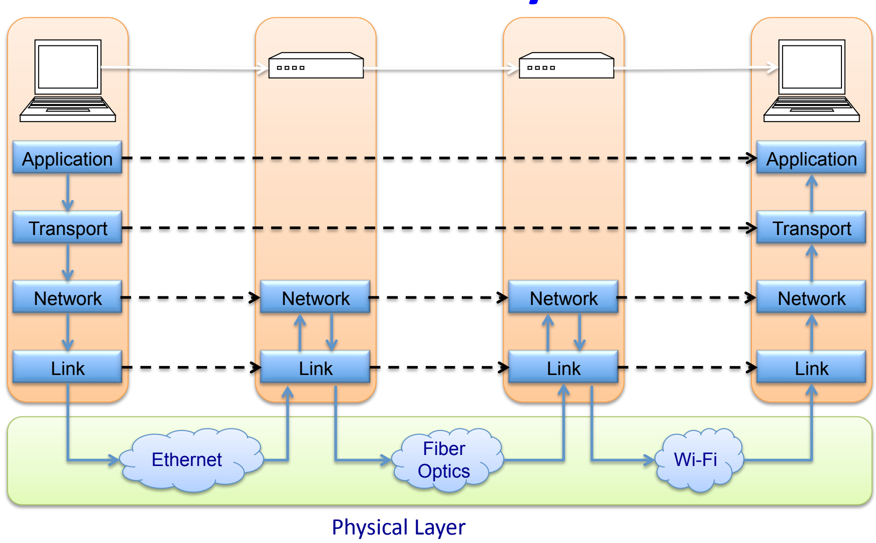
Encapsulation

- A packet typically consists of
  - Control information for addressing the packet: header and footer
  - Data: payload
- A network protocol N1 can use the services of another network protocol N2
  - A packet p1 of N1 is encapsulated into a packet p2 of N2
  - The payload of p2 is p1
  - The control information of p2 is derived from that of p1



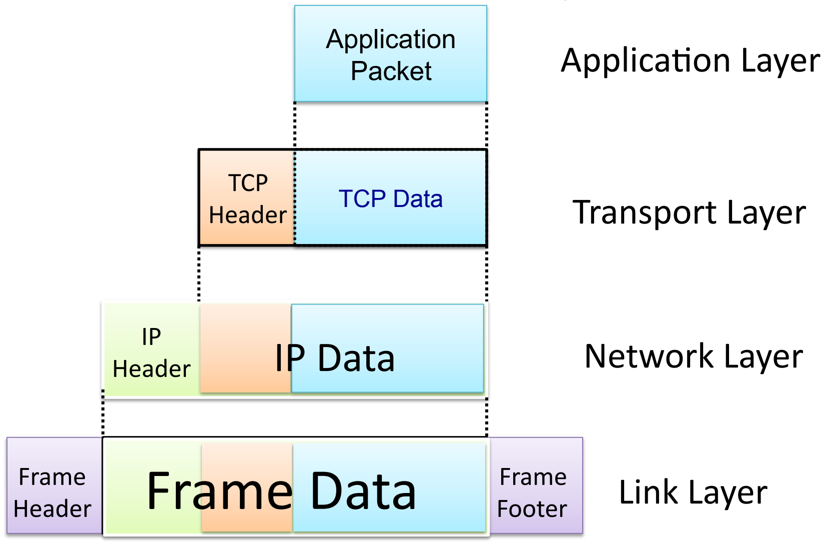
11

Internet Layers



12

Internet Packet Encapsulation



13

Network Interfaces

- Network interface: device connecting a computer to a network
  - Ethernet card
  - WiFi adapter
- A computer may have multiple network interfaces
- Packets transmitted between network interfaces
- Most local area networks, (including Ethernet and WiFi) broadcast frames
- In regular mode, each network interface gets the frames intended for it
- Traffic sniffing can be accomplished by configuring the network interface to read all frames (promiscuous mode)

14

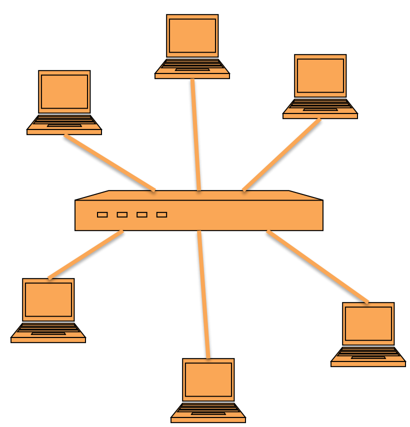
MAC Addresses

- Most network interfaces come with a predefined MAC address
- A MAC address is a 48-bit number usually represented in hex
  - E.g., 00-1A-92-D4-BF-86
- The first three octets of any MAC address are IEEE-assigned Organizationally Unique Identifiers
  - E.g., Cisco 00-1A-A1, D-Link 00-1B-11, ASUSTek 00-1A-92
- The next three can be assigned by organizations as they please, with uniqueness being the only constraint
- Organizations can utilize MAC addresses to identify computers on their network
- MAC address can be reconfigured by network interface driver software

15

Switch

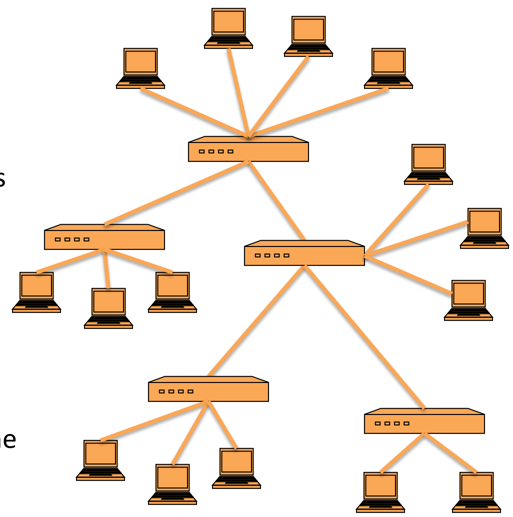
- A switch is a common network device
  - Operates at the link layer
  - Has multiple ports, each connected to a computer
- Operation of a switch
  - Learn the MAC address of each computer connected to it
  - Forward frames only to the destination computer



16

Combining Switches

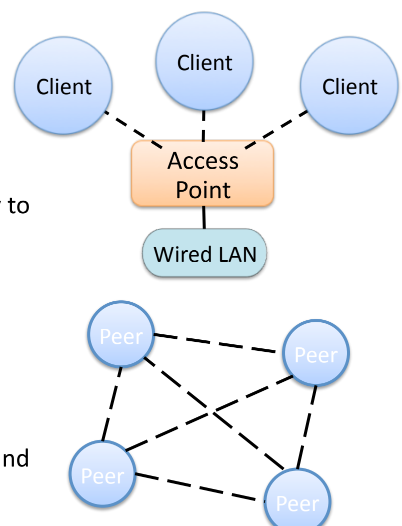
- Switches can be arranged into a tree
- Each port learns the MAC addresses of the machines in the segment (subtree) connected to it
- Fragments to unknown MAC addresses are broadcast
- Frames to MAC addresses in the same segment as the sender are ignored



17

Types of Wireless Networks

- Infrastructure
  - Client machines establish a radio connection to a special network device, called access point
  - Access points connected to a wired network, which provides a gateway to the internet
  - Most common type of wireless network
- Peer-to-peer
  - Multiple peer machines connect to each other
  - Typically used in ad-hoc networks and internet connection sharing

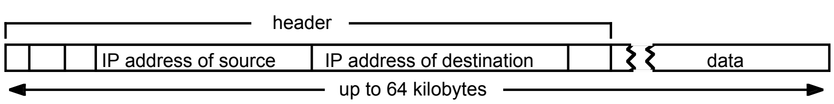


18

Internet Protocol

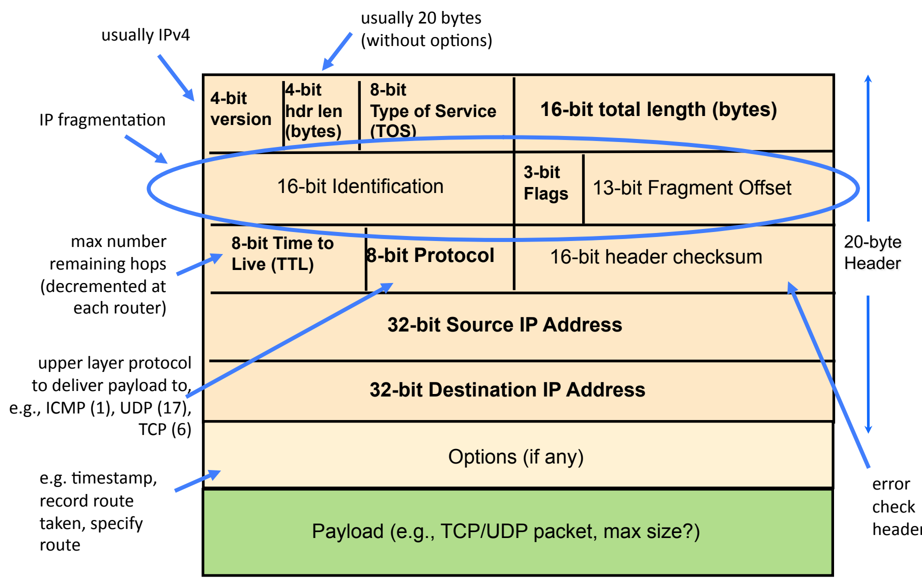
- Connectionless
  - Each packet is transported independently from other packets
- Unreliable
  - Delivery on a best effort basis
  - No acknowledgments
  - Packets may be lost, reordered, corrupted, or duplicated
- IP packets
  - Encapsulate TCP and UDP packets
  - Encapsulated into link-layer frames

IP packet layout



- IP header includes
  - Source address
  - Destination address
  - Packet length (up to 64KB)
  - Time to live (up to 255)
  - IP protocol version
  - Fragmentation information
  - Transport layer protocol information (e.g., TCP)

IPv4 Packet Header Format



21

IP Addressing

- IP address used to route datagrams through network.
- IPv4 32 bit address, IPv6 128 bit address.
- Divided into two parts: network and host.
- Network part: Used to route packets. (ZIP code)
- Host part: Used to identify an individual host. (House number)
- Usually represented in dotted decimal notation: 141.211.144.212
- Each number represents 8 bits: 0-255.

22

Decimal representation of Internet addresses

	octet 1	octet 2	octet 3		Range of addresses
	Network ID	Host ID			
Class A:	1 to 127	0 to 255	0 to 255	0 to 255	1.0.0.0 to 127.255.255.255
	Network ID		Host ID		
Class B:	128 to 191	0 to 255	0 to 255	0 to 255	128.0.0.0 to 191.255.255.255
	Network ID			Host ID	
Class C:	192 to 223	0 to 255	0 to 255	1 to 254	192.0.0.0 to 223.255.255.255
	Multicast address				
Class D (multicast):	224 to 239	0 to 255	0 to 255	1 to 254	224.0.0.0 to 239.255.255.255
Class E (reserved):	240 to 255	0 to 255	0 to 255	1 to 254	240.0.0.0 to 255.255.255.255

Classless Interdomain Routing (CIDR)

- Allow division between network and host portion on any bit boundary.
  - More efficient use of address space.
  - Allows division/aggregation of sub-assignments.
- Networks now identified by network address and the length of the network portion: 141.213.8.0/24
- Hosts identified by address and network mask: 141.213.8.1, 255.255.255.0.
- WHY? Rapid depletion of class B address space and poor utilization of the assigned address space

IP subnets

CIDR prefix length	Subnet Mask	Number of hosts
/8	255.0.0.0	2^{24}
/9	255.128.0.0	2^{23}
/10	255.192.0.0	2^{22}
/24	255.255.255.0	$2^8 = 256$
/25	255.255.255.128	$2^7 = 128$
/26	255.255.255.192	$2^6 = 64$
/27	255.255.255.224	$2^5 = 32$
/28	255.255.255.240	$2^4 = 16$
/29	255.255.255.248	$2^3 = 8$
/30	255.255.255.252	$2^2 = 4$

Special IP addresses

Prefix	Suffix	Type of Address	Purpose
all-0s	all-0s	this computer	used during bootstrap
network	all-0s	network	identifies a network
network	all-1s	directed broadcast	broadcast on a specified net
all-1s	all-1s	limited broadcast	broadcast on a local net
127	any	loopback	testing

IP Address Space and ICANN

- Hosts on the internet must have unique IP addresses
- Internet Corporation for Assigned Names and Numbers
  - International nonprofit organization
  - Incorporated in the US
  - Allocates IP address space
  - Manages top-level domains
- Historical bias in favor of US corporations and nonprofit organizations

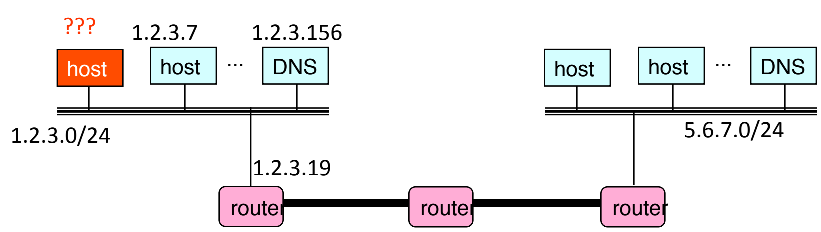
- Examples

  003/8 May 94 General Electric
  009/8 Aug 92 IBM
  012/8 Jun 95 AT&T Bell Labs
  013/8 Sep 91 Xerox Corporation
  015/8 Jul 94 Hewlett-Packard
  017/8 Jul 92 Apple Computer
  018/8 Jan 94 MIT
  019/8 May 95 Ford Motor
  040/8 Jun 94 Eli Lily
  043/8 Jan 91 Japan Inet
  044/8 Jul 92 Amateur Radio Digital
  047/8 Jan 91 Bell-Northern Res.
  048/8 May 95 Prudential Securities
  054/8 Mar 92 Merck
  055/8 Apr 95 Boeing
  056/8 Jun 94 U.S. Postal Service

27

How To Bootstrap an End Host?

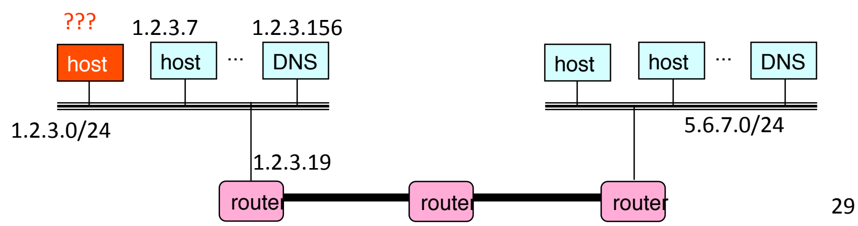
- What local DNS server to use?
- What IP address the host should use?
- How to send packets to remote destinations?



28

Avoiding Manual Configuration

- Dynamic Host Configuration Protocol (DHCP)
  - End host learns how to send packets
  - Learn IP address, DNS servers, and gateway
- Address Resolution Protocol (ARP)
  - Others learn how to send packets to the end host
  - Learn mapping between IP & interface addresses

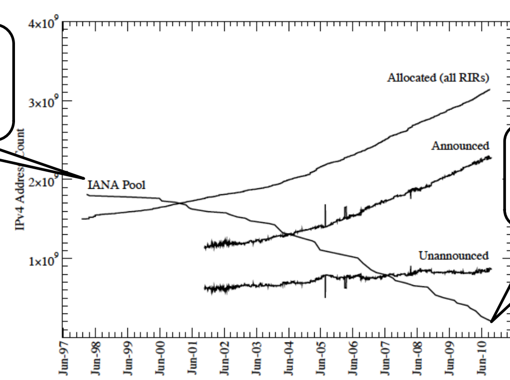


29

Problem: IP Address Exhaustion

- IPv4 Addresses are 32 bits wide: **~3.7Bn usable addresses**
- **All devices** on the Internet **require an address**
- Given Internet growth rate, addresses have been diminishing fast…

1988: Started with 3.7Bn usable free; By 1997: just 1.8Bn left



IANA exhausted free address pool in February 2011

30

Solution Strategies

- Under address scarcity, how do we continue to support Internet growth?
- Three ways of mitigating exhaustion of a scarce resource:
  - **Sharing**:
    - Share addresses in time via Dynamic Host Configuration Protocol (DHCP)
    - Share addresses in port space via, e.g. Carrier-grade NAT (CGN)
  - **More efficient utilization**:
    - **Stricter policy** for new address allocations
    - **Reallocation** of unused or otherwise reclaimed addresses
    - **Address markets** for the efficient distribution of addresses
  - **Transition** to another resource:
    - Replace IPv4 with **IPv6**, which provides the ultimate long-term solution with a practically inexhaustible address space

31

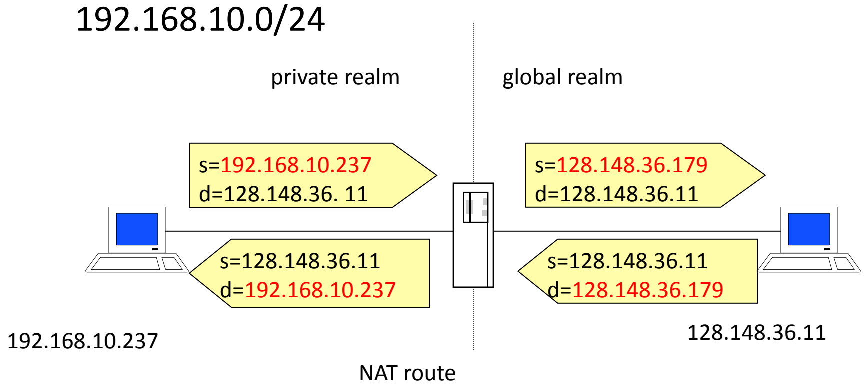
Network Address Translation

- Introduced in the early 90s to alleviate IPv4 address space congestion
- Relies on translating addresses in an internal network, to an external address that is used for communication to and from the outside world
- NAT is usually implemented by placing a router in between the internal private network and the public network.
- Saves IP address space since not every terminal needs a globally unique IP address, only an organizationally unique one
- While NAT should really be transparent to all high level services, this is sadly not true because a lot of high level communication uses things on IP

32

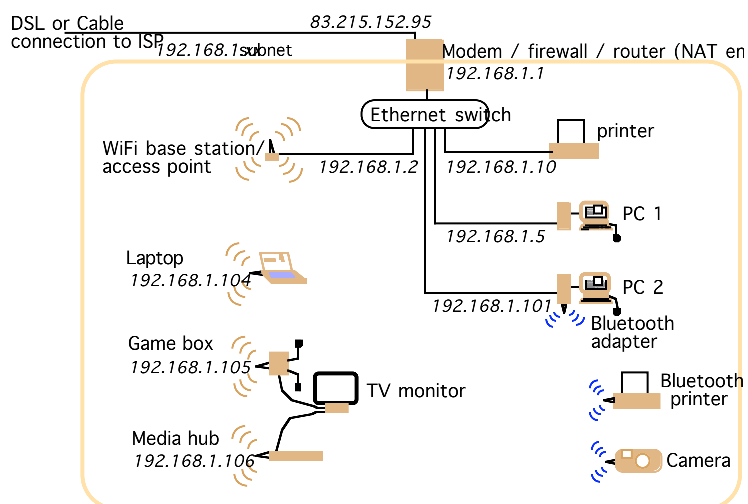
Translation

- Router has a pool of private addresses 192.168.10.0/24



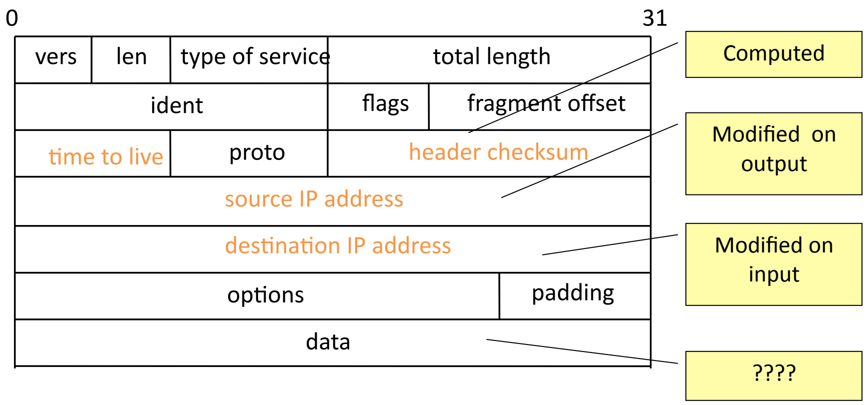
33

A typical NAT-based home network (CDK Figure 3.18)



34

IP Packet Modifications



35

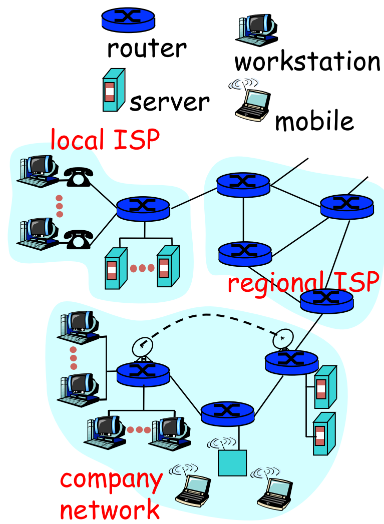
What is the Internet?

36

What's the Internet: "nuts and bolts" view

- millions of connected computing devices: *hosts, end-systems*
  - PCs workstations, servers
  - PDAs phones, toasters

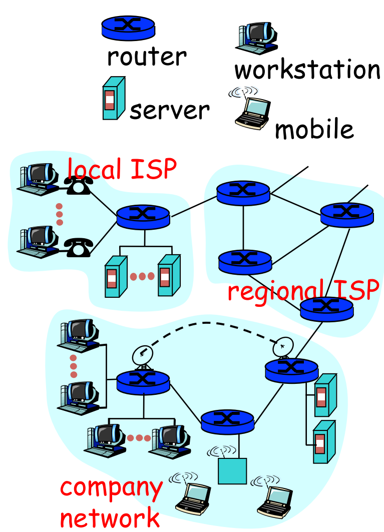
  running *network apps*
- *communication links*
  - fiber, copper, radio, satellite
  - transmission rate = ***bandwidth***
- *routers:* forward packets (chunks of data)



37

What's the Internet: "nuts and bolts" view

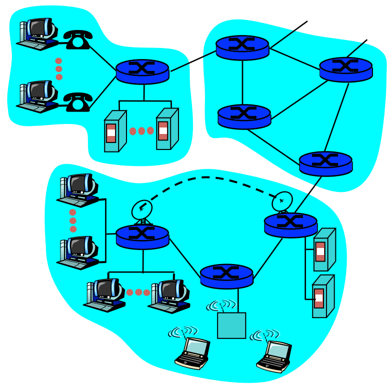
- *protocols* control sending, receiving of msgs
  - e.g., TCP, IP, HTTP, FTP, PPP
- *Internet: "network of networks"*
  - loosely hierarchical
  - public Internet versus private intranet
- Internet standards
  - RFC: Request for comments
  - IETF: Internet Engineering Task Force



38

What's the Internet: a service view

- communication *infrastructure* enables distributed applications:
  - Web, email, games, e-commerce, database., voting, file (MP3) sharing
- communication services provided to apps:
  - connectionless
  - connection-oriented



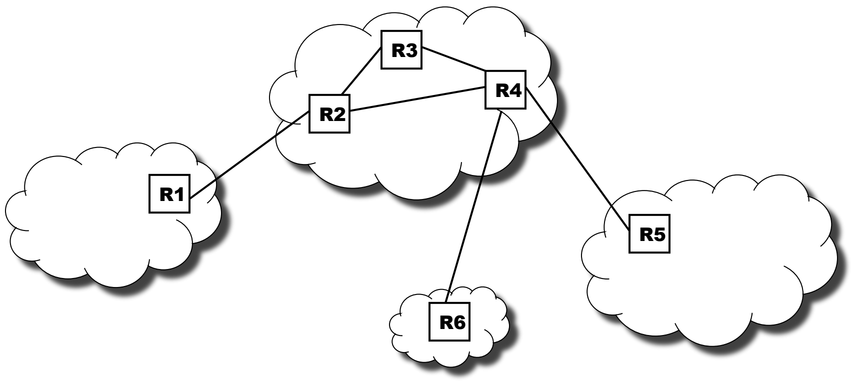
39

Internet design

- Put the intelligence in the end hosts and keep the network simple.
  - Packet switched instead of circuit switched.
  - Best effort delivery.
  - Force transport layer to deal with delay and loss.
- Reliable in the face of failures.
  - No session state on routers.
  - Allows routers to be added and removed without causing large disturbances.

40

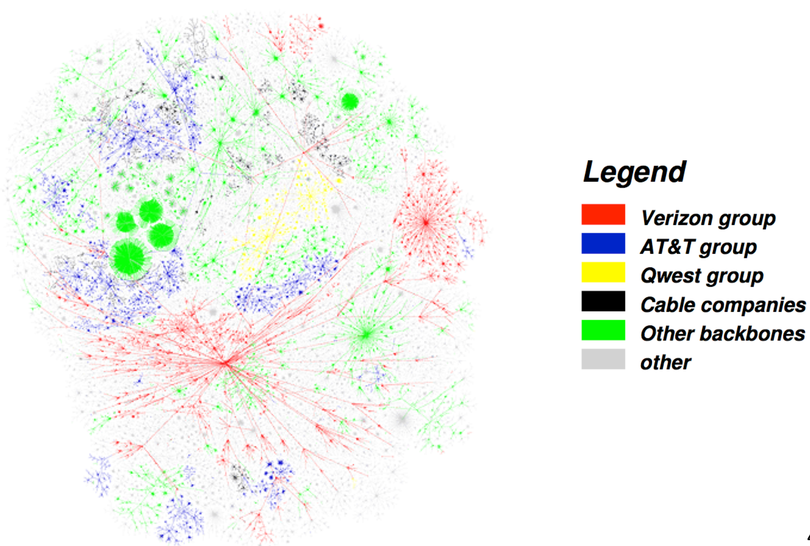
Autonomous Systems (AS)



- The Internet is a collection of autonomous systems.
- AS: A set of routers and networks under the same administrative control.
- Inter-domain vs. intra-domain routing.

41

The Internet Backbone

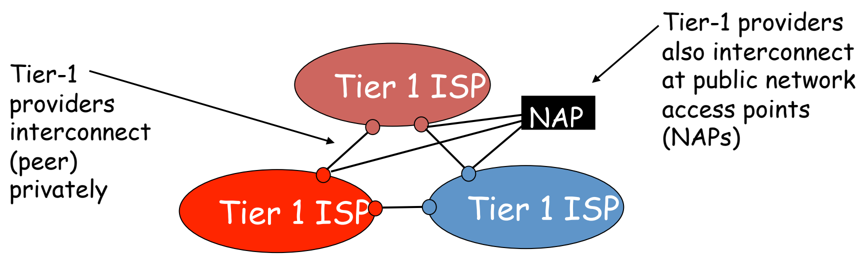


42

http://advice.cio.com/node/209

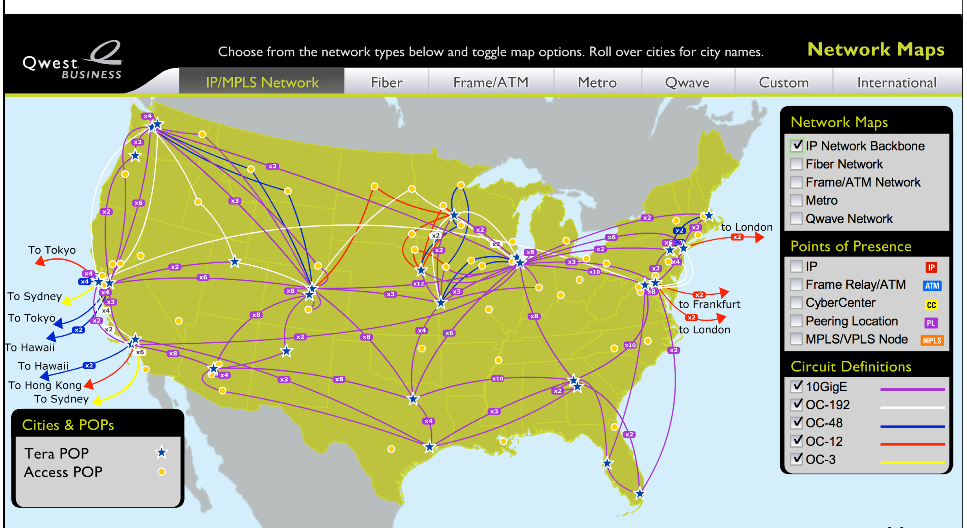
Internet structure: network of networks

- roughly hierarchical
- at center: "tier-1" ISPs (e.g., UUNet, BBN/Genuity, Sprint, AT&T), national/international coverage
  - treat each other as equals



43

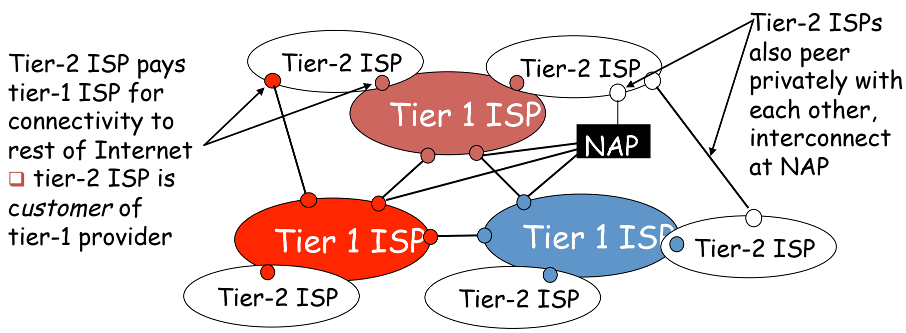
Qwest's backbone



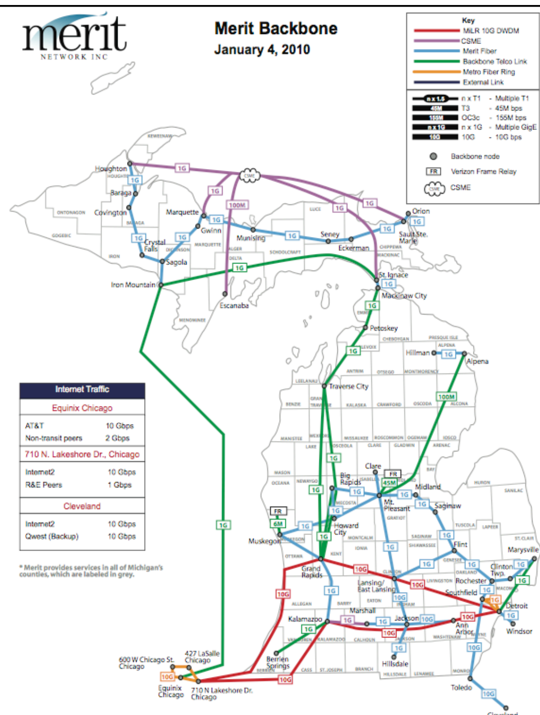
44

Internet structure: network of networks

- "Tier-2" ISPs: smaller (often regional) ISPs
  - Connect to one or more tier-1 ISPs, possibly other tier-2 ISPs



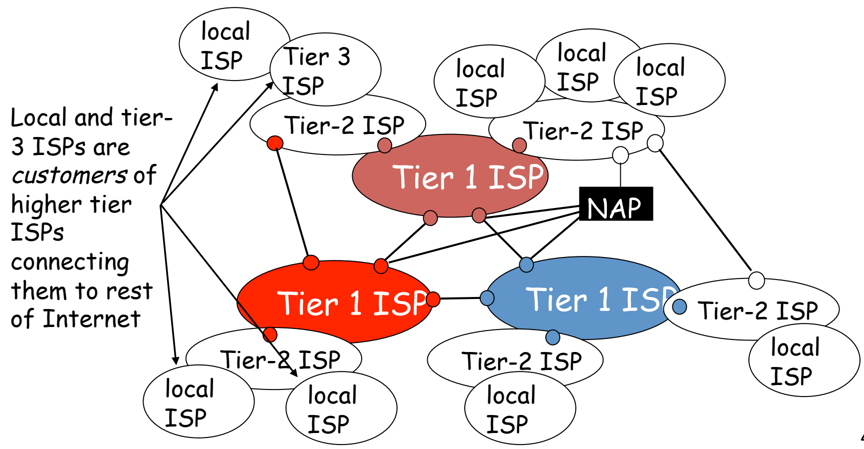
45



46

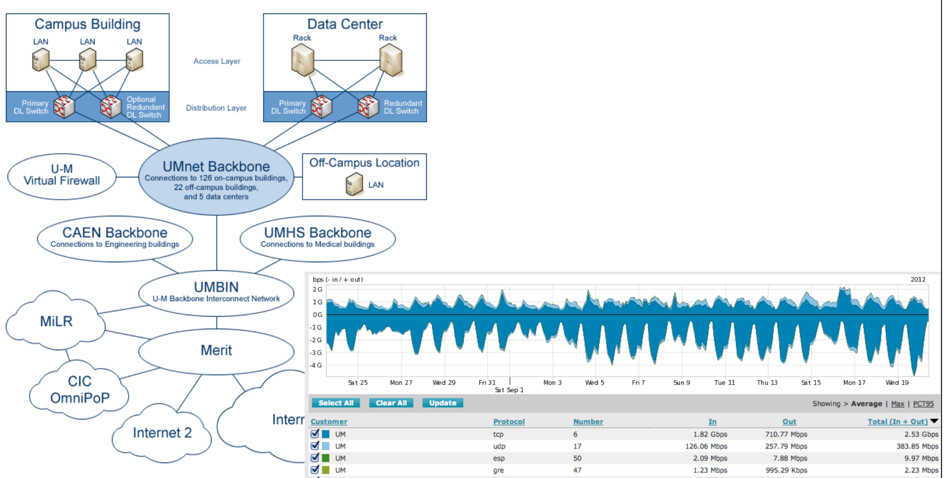
Internet structure: network of networks

- "Tier-3" ISPs and local ISPs
  - last hop ("access") network (closest to end systems)



47

UMnet Backbone



48

Connection-oriented service

<u>*Goal:*</u> data transfer between end systems

- *handshaking:* setup (prepare for) data transfer ahead of time
  - Hello, hello back human protocol
  - *set up "state"* in two communicating hosts
- TCP - Transmission Control Protocol
  - Internet's connection-oriented service

<u>TCP service</u> [RFC 793]

- Byte-steam abstraction: reliably delivering a stream of bytes from S to R
- *reliable, in-order* byte-stream data transfer
  - loss: acknowledgements and retransmissions
- *flow control:*
  - sender won't overwhelm receiver
- *congestion control:*
  - senders "slow down sending rate" when network congested

49

Network edge: connectionless service

<u>*Goal:*</u> data transfer between end systems

- Goal is same as before!
- No handshaking
- No connection state maintained on end hosts

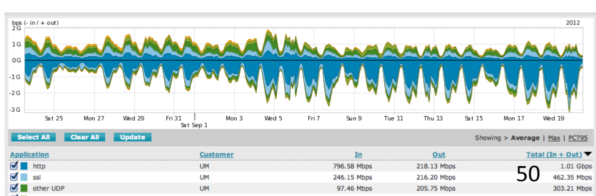
- UDP - User Datagram Protocol [RFC 768]: Internet's connectionless service
  - unreliable data transfer
  - no flow control
  - no congestion control

<u>Apps using TCP:</u>

- HTTP (Web), FTP (file transfer), Telnet (remote login), SMTP (email)

<u>Apps using UDP:</u>

- streaming media, teleconferencing, DNS, Internet telephony



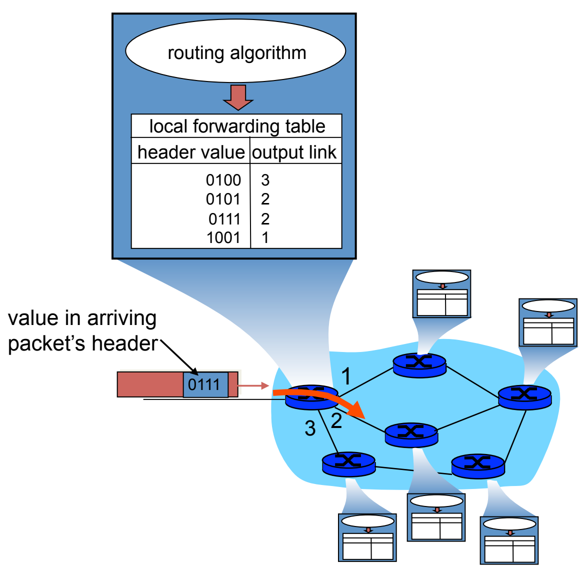
50

IP Routing

- A router bridges two or more networks
  - Operates at the network layer
  - Maintains tables to forward packets to the appropriate network
  - Forwarding decisions based solely on the destination address
- Routing table
  - Maps ranges of addresses to LANs or other gateway routers

51

Interplay between routing and forwarding



52

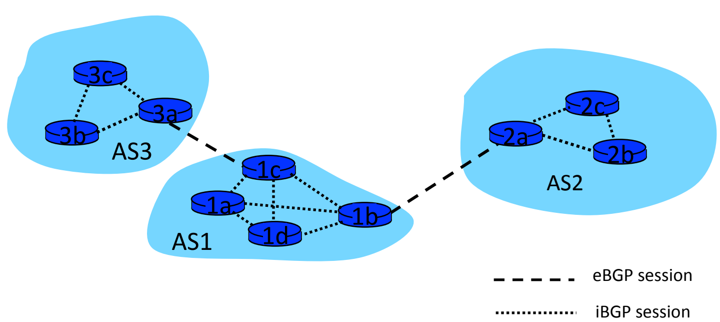
Internet inter-AS routing: BGP

- BGP (Border Gateway Protocol): *the* de facto standard
- BGP provides each AS a means to:
  1. Obtain subnet reachability information from neighboring ASs.
  2. Propagate the reachability information to all routers internal to the AS.
  3. Determine "good" routes to subnets based on reachability information and policy.
- Allows a subnet to advertise its existence to rest of the Internet: *"I am here"*

53

BGP basics

- Pairs of routers (BGP peers) exchange routing info over semi-permanent TCP connections: BGP sessions
- Note that BGP sessions do not correspond to physical links.
- When AS2 advertises a prefix to AS1, AS2 is *promising* it will forward any datagrams destined to that prefix towards the prefix.
  - AS2 can aggregate prefixes in its advertisement



54

DNS: Domain Name System

People: many identifiers:
- SSN, name, passport #

Internet hosts, routers:
- IP address (32 bit) - used for addressing datagrams
- "name", e.g., www.eecs.umich.edu - used by humans

Q: map between IP addresses and name ?

Domain Name System:
- *distributed database* implemented in hierarchy of many *name servers*
- *application-layer protocol* host, routers, name servers to communicate to *resolve* names (address/name translation)
  - note: core Internet function, implemented as application-layer protocol
  - complexity at network's "edge"

55

DNS name servers

Why not centralize DNS?
- single point of failure
- traffic volume
- distant centralized database
- Maintenance

doesn't *scale!*

Record Type	Million Queries	Percentage
A	1,220	70.4%
AAAA	206	11.9%
MX	152	8.8%
DS	69	4.0%
NS	25	1.4%
ANY	19	1.1%
TXT	18	1.0%
SOA	6	0.4%
A6	5	0.3%
SPF	4	0.3%
Other	8	0.5%
Total	1,732	

Table 8: Top 10 Resource Records Requested

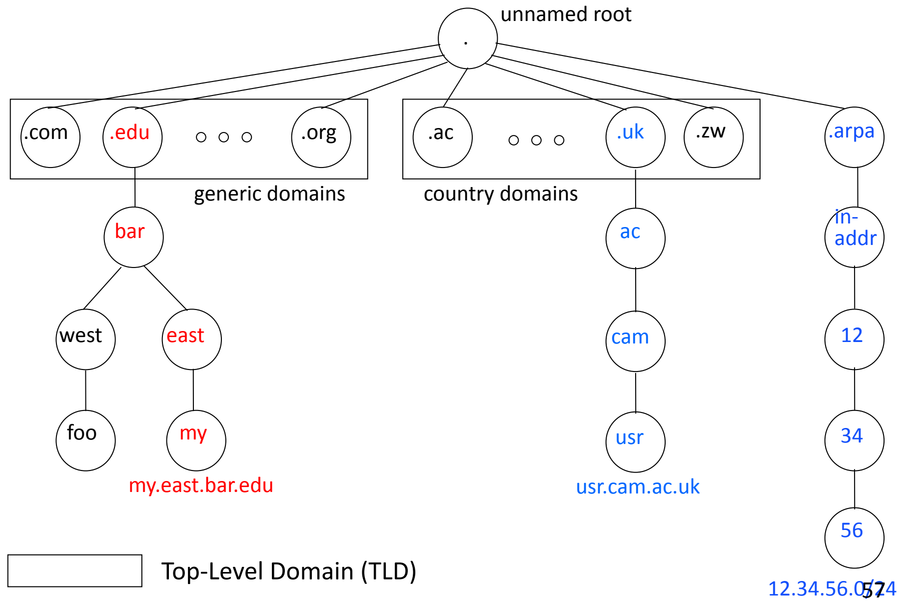
- no server has all name-to-IP address mappings

local name servers:
- each ISP, company has *local (default) name server*
- host DNS query first goes to local name server

authoritative name server:
- for a host: stores that host's IP address, name
- can perform name/address translation for that host's name

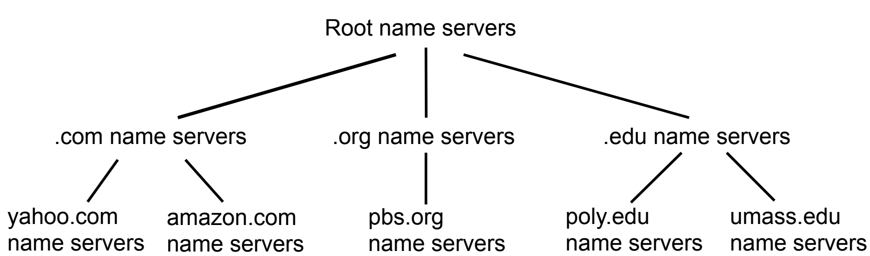
56

DNS Hierarchical Name Space



57

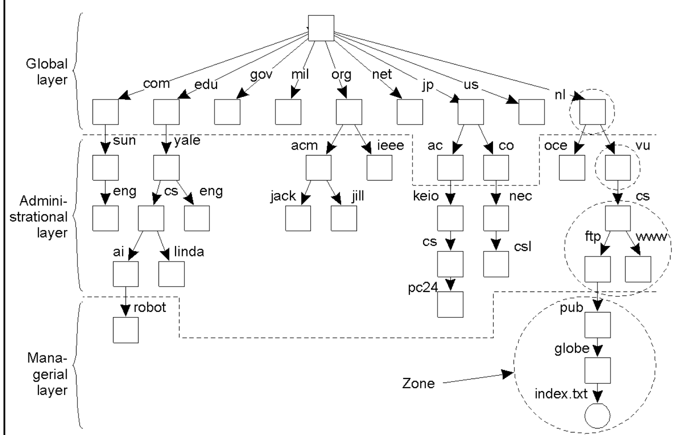
Distributed Hierarchical Database (1st Approx)



- Client wants IP for `www.amazon.com`:
- Client queries a root server to find `.com` name server
- Client queries `.com` name server to get `amazon.com` name server
- Client queries `amazon.com` name server to get IP address for [`www.amazon.com`](www.amazon.com)

58

Name Space Distribution

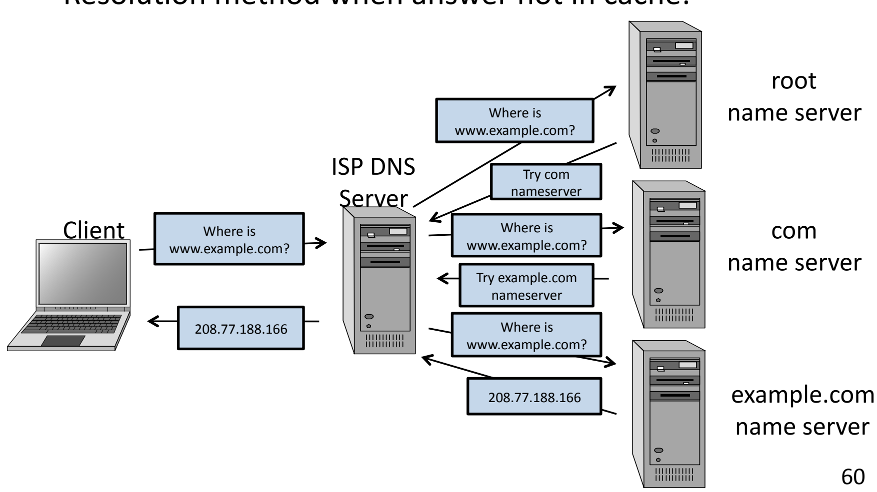


- 1 24537172 arin.net
- 2 17003127 verisign.com
- 3 14529802 apnic.net
- 4 14526895 gslb.com
- 5 10917319 manitu.net
- 6 9167881 sorbs.net
- 7 8701029 msft.net
- 8 8595104 google.com
- 9 7520954 amazon.com
- 10 7450839 register.com
- 11 7034622 gtld-servers.net
- 12 6937887 facebook.com
- 13 6779616 coremetrics.com
- 14 6574735 msecnd.net
- 15 6570337 root-servers.net
- 16 5725087 amazonaws.com
- 17 5663948 akamai.net
- 18 5309527 weather.com
- 19 4943117 name-services.com
- 20 4902683 yahoo.com

59

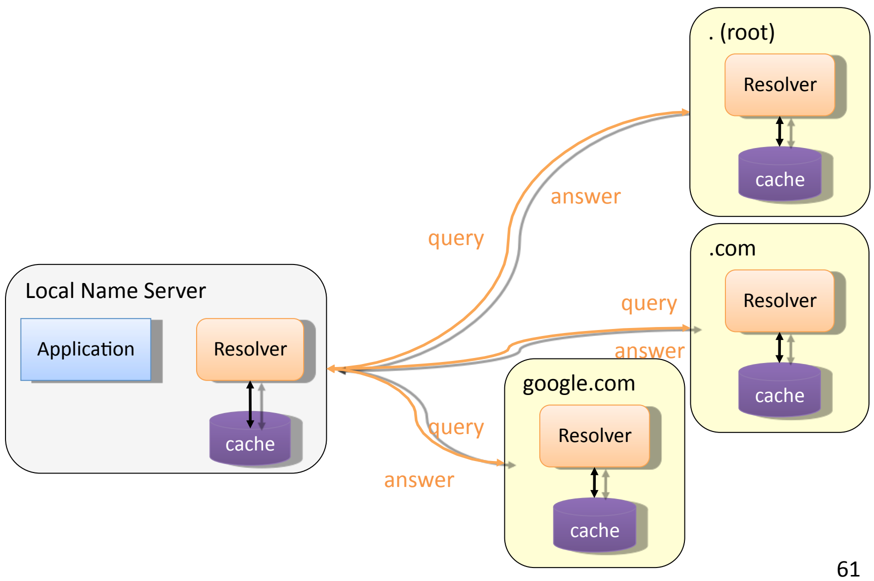
Name Resolution

- Zone: collection of connected nodes with the same authoritative DNS server
  Resolution method when answer not in cache:



60

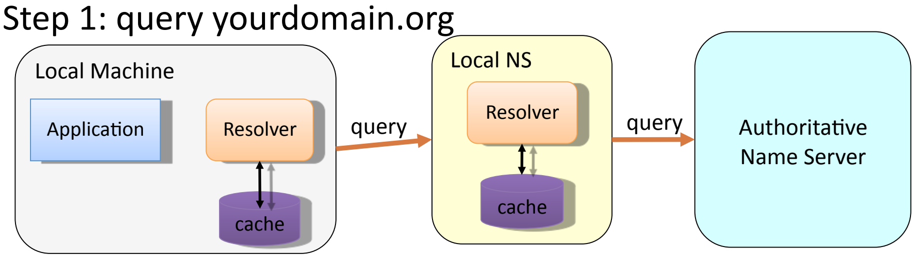
Iterative Name Resolution



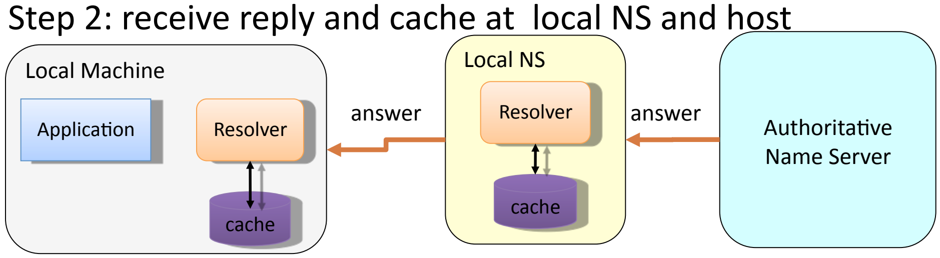
61

DNS Caching

Step 1: query yourdomain.org



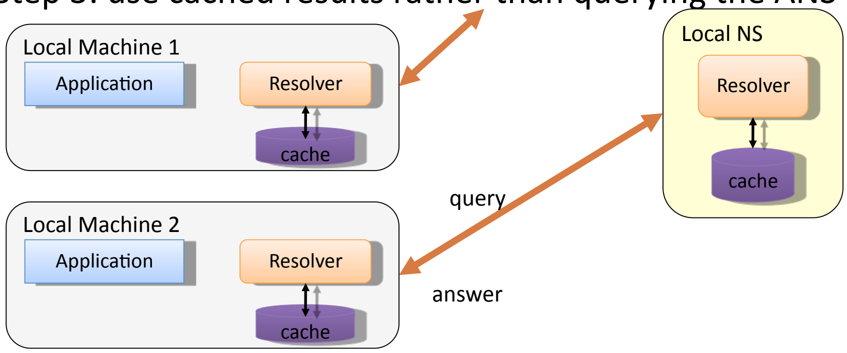
Step 2: receive reply and cache at local NS and host



62

DNS Caching (con'd)

Step 3: use cached results rather than querying the ANS



Step 4: Evict cache entries upon ttl expiration

63