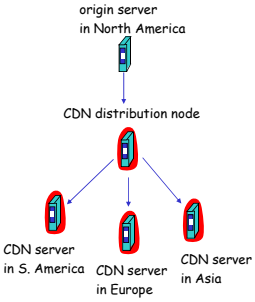
Chapter 7 outline

- 7.1 Multimedia Networking Applications
- 7.2 Streaming stored audio and video
- 7.3 Real-time Multimedia: Internet Phone study
- 7.4 Protocols for Real-Time Interactive Applications
  - RTP,RTCP,SIP
- 7.5 Distributing Multimedia: content distribution networks
- 7.6 Beyond Best Effort
- 7.7 Scheduling and Policing Mechanisms
- 7.8 Integrated Services and Differentiated Services
- 7.9 RSVP

Content distribution networks (CDNs)

Content replication

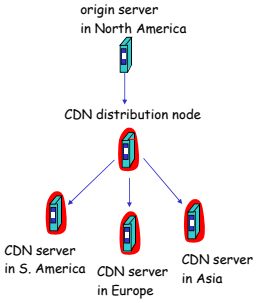
- Challenging to stream large files (e.g., video) from single origin server in real time
- Solution: replicate content at hundreds of servers throughout Internet
  - content downloaded to CDN servers ahead of time
  - placing content "close" to user avoids impairments (loss, delay) of sending content over long paths
  - CDN server typically in edge/access network



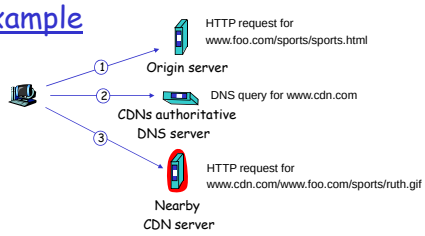
Content distribution networks (CDNs)

Content replication

- CDN (e.g., Akamai) customer is the content provider (e.g., CNN)
- CDN replicates customers' content in CDN servers. When provider updates content, CDN updates servers



CDN example



origin server (www.foo.com)

- distributes HTML
- replaces:
  http://www.foo.com/sports.ruth.gif
  with
  http://www.cdn.com/www.foo.com/sports/ruth.gif

CDN company (cdn.com)

- distributes gif files
- uses its authoritative DNS server to route redirect requests

More about CDNs

routing requests

- CDN creates a "map", indicating distances from leaf ISPs and CDN nodes
- when query arrives at authoritative DNS server:
  - server determines ISP from which query originates
  - uses "map" to determine best CDN server
- CDN nodes create application-layer overlay network

Chapter 7 outline

- 7.1 Multimedia Networking Applications
- 7.2 Streaming stored audio and video
- 7.3 Real-time Multimedia: Internet Phone study
- 7.4 Protocols for Real-Time Interactive Applications
  - RTP,RTCP,SIP
- 7.5 Distributing Multimedia: content distribution networks
- 7.6 Beyond Best Effort
- 7.7 Scheduling and Policing Mechanisms
- 7.8 Integrated Services and Differentiated Services
- 7.9 RSVP

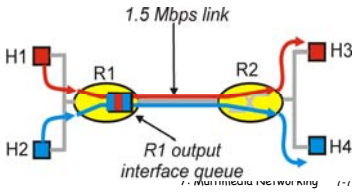
Improving QOS in IP Networks

Thus far: "making the best of best effort"

Future: next generation Internet with QoS guarantees

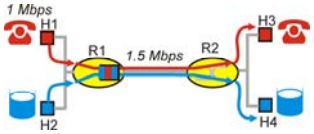
- RSVP: signaling for resource reservations
- Differentiated Services: differential guarantees
- Integrated Services: firm guarantees

- simple model for sharing and congestion studies:



Principles for QOS Guarantees

- Example: 1MbpsI P phone, FTP share 1.5 Mbps link.
  - bursts of FTP can congest router, cause audio loss
  - want to give priority to audio over FTP

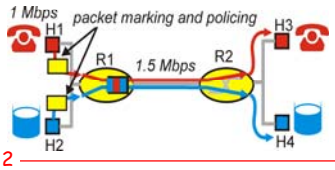


Principle 1

packet marking needed for router to distinguish between different classes; and new router policy to treat packets accordingly

Principles for QOS Guarantees (more)

- what if applications misbehave (audio sends higher than declared rate)
  - policing: force source adherence to bandwidth allocations
- marking and policing at network edge:
  - similar to ATM UNI (User Network Interface)

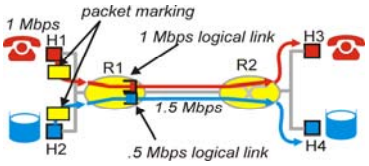


Principle 2

provide protection (*isolation*) for one class from others

Principles for QOS Guarantees (more)

- Allocating *fixed* (non-sharable) bandwidth to flow: *inefficient* use of bandwidth if flows doesn't use its allocation

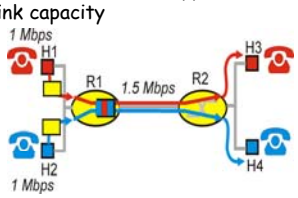


Principle 3

While providing isolation, it is desirable to use resources as efficiently as possible

Principles for QOS Guarantees (more)

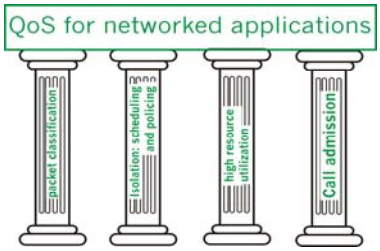
- *Basic fact of life:* can not support traffic demands beyond link capacity



Principle 4

Call Admission: flow declares its needs, network may block call (e.g., busy signal) if it cannot meet needs

Summary of QoS Principles



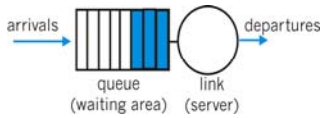
Let's next look at mechanisms for achieving this ….

Chapter 7 outline

- 7.1 Multimedia Networking Applications
- 7.2 Streaming stored audio and video
- 7.3 Real-time Multimedia: Internet Phone study
- 7.4 Protocols for Real-Time Interactive Applications
  - RTP,RTCP,SIP
- 7.5 Distributing Multimedia: content distribution networks
- 7.6 Beyond Best Effort
- 7.7 Scheduling and Policing Mechanisms
- 7.8 Integrated Services and Differentiated Services
- 7.9 RSVP

Scheduling And Policing Mechanisms

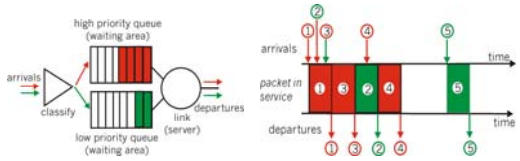
- scheduling: choose next packet to send on link
- FIFO (first in first out) scheduling: send in order of arrival to queue
  - real-world example?
  - discard policy: if packet arrives to full queue: who to discard?
    - Tail drop: drop arriving packet
    - priority: drop/remove on priority basis
    - random: drop/remove randomly



Scheduling Policies: more

Priority scheduling: transmit highest priority queued packet

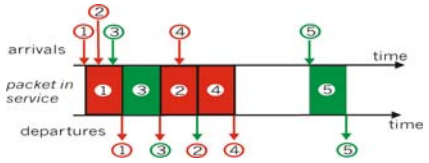
- multiple *classes*, with different priorities
  - class may depend on marking or other header info, e.g. IP source/dest, port numbers, etc..
  - Real world example?



Scheduling Policies: still more

round robin scheduling:

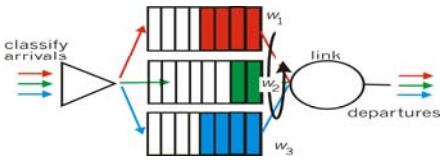
- multiple classes
- cyclically scan class queues, serving one from each class (if available)
- real world example?



Scheduling Policies: still more

Weighted Fair Queuing:

- generalized Round Robin
- each class gets weighted amount of service in each cycle
- real-world example?



Policing Mechanisms

Goal: limit traffic to not exceed declared parameters

Three common-used criteria:

- *(Long term) Average Rate:* how many pkts can be sent per unit time (in the long run)
  - crucial question: what is the interval length: 100 packets per sec or 6000 packets per min have same average!
- *Peak Rate:* e.g., 6000 pkts per min. (ppm) avg.; 1500 ppm peak rate
- *(Max.) Burst Size:* max. number of pkts sent consecutively (with no intervening idle)

Multimedia Networking: Summary

- multimedia applications and requirements
- making the best of today's best effort service
- scheduling and policing mechanisms

Chapter 8: Network Security

Chapter goals:

- understand principles of network security:
  - cryptography and its *many* uses beyond "confidentiality"
  - authentication
  - message integrity
  - key distribution
- security in practice:
  - firewalls
  - security in application, transport, network, link layers

What is network security?

Confidentiality: only sender, intended receiver should "understand" message contents
- sender encrypts message
- receiver decrypts message

Authentication: sender, receiver want to confirm identity of each other

Message Integrity: sender, receiver want to ensure message not altered (in transit, or afterwards) without detection

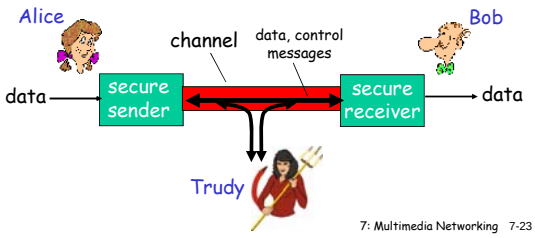
Access and Availability: services must be accessible and available to users

Location & Privacy Practice

- How many ways have you been located today?
  - When I charged my gas to a credit card.
  - When I walked by the security camera in an secured area.
  - When I carry my cell phone, turned on.
  - When I put my card in the ATM machine.
  - When I drove through a monitored intersection.
  - When I used Google Search.
  - When I signed in to Amazon.com.
  - When I scanned my ID card to enter a room.
  - When I used my laptop computer on campus.
  - When I passed by a Bluetooth-enabled printer.

Friends and enemies: Alice, Bob, Trudy

- well-known in network security world
- Bob, Alice (lovers!) want to communicate "securely"
- Trudy (intruder) may intercept, delete, add messages

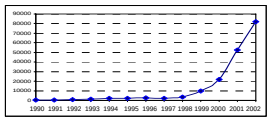


Who might Bob, Alice be?

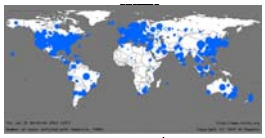
- … well, *real-life* Bobs and Alices!
- Web browser/server for electronic transactions (e.g., on-line purchases)
- on-line banking client/server
- DNS servers
- routers exchanging routing table updates
- other examples?

Information Assurance

- Sophistication of cyber attacks and their severity is increasing
- ARL, the Army, DOD and Other U.S. Government Agencies are major targets for sophisticated state sponsored cyber terrorists
  - Cyber strategies can be a major force multiplier and equalizer
  - Across DoD, computer assets have been compromised, information has been stolen, putting technological advantage and battlefield superiority at risk
- Security mechanisms always have inevitable vulnerabilities
  - Firewalls are not sufficient to ensure security in computer networks
  - Insider attacks



INCIDENTS REPORTED TO COMPUTER EMERGENCY RESPONSE TEAM/COORDINATION



SPREAD OF SQL SLAMMER WORM 10 MINUTES AFTER ITS DEPLOYMENT

There are bad guys (and girls) out there!

Q: What can a "bad guy" do?

A: a lot!

- *eavesdrop:* intercept messages
- actively *insert* messages into connection
- *impersonation:* can fake (spoof) source address in packet (or any field in packet)
- *hijacking:* "take over" ongoing connection by removing sender or receiver, inserting himself in place
- *denial of service*: prevent service from being used by others (e.g., by overloading resources)

more on this later ……

Proactive measures

- establish a site security policy
- install latest versions of software and apply recommended patches
- strip down default services
- restrict access to hosts
- stay current with new security issues
- apply OS and server patches immediately
- do regular backups
- monitor system activity and integrity
- implement a firewall

connect the system to your network

Protecting your network

- host-based protection
- designing your network
- traffic filtering
- firewalls

Tools

- lsof – lists open files and network sockets
- ps – find processes and where they were run from (parent processes)
- netstat – lists current network sessions and open ports

Strip down default services

port	type	name
7	TCP/UDP	echo
9	TCP/UDP	discard
13	TCP/UDP	daytime
19	TCP/UDP	chargen
21	TCP	ftp ●
23	TCP	telnet ●
37	TCP/UDP	time
53	TCP/UDP	domain
69	UDP	tftp
110	TCP	pop3 ●
113	TCP/UDP	auth
161	UDP	snmp

port	type	name
513	UDP	who
514	UDP	syslog
517	UDP	talk
2049	TCP/UDP	NFS
512	TCP	exec ●
513	TCP	login ●
514	TCP	shell ●

services marked with ● use cleartext passwords

Use encryption

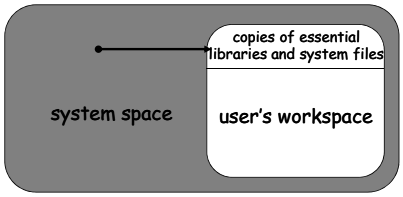
- do you really need telnet and ftp access?
- SSH (Secure Shell) gives the same functionality, with session encryption
- use APOP authentication for POP3
- use CRAM-MD5 authentication for IMAP4
- combine with one-time passwords (S/Key)
  - you can require one-time password logins from specific hosts only

Encryption is not everything

- not a solution against keyboard sniffers
- SSL doesen't eliminate server vulnerabilities
- be very careful with custom-designed encryption algorhytms (often XOR "encryption" with random keys)
- one-time passwords protect only against system access, not sniffing

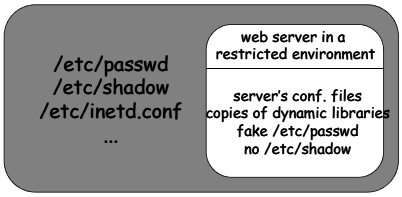
Restrict users and services

- to minimize possible damage, restrict users and services to a closed environment (chroot)



chroot environment

- exploits of the web server can't affect system files



Snapshot of the system

- save important tools on floppy/CD-ROM
  - ls, ps, netstat, w, finger, su, login, sh (or bash), df, top, ifconfig, find, grep
- save configuration files
  - inetd.conf, hosts.allow, hosts.deny, syslog.conf, ...
- calculate MD5 checksums (TripWire)
- access/modification/creation timestamps

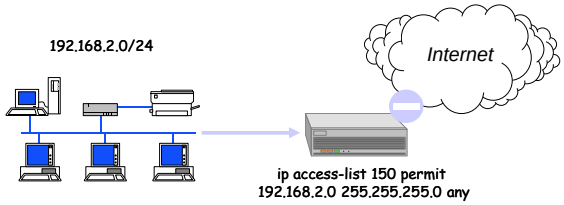
```
ls -alRu > /floppy/timestamp_access.txt
ls -alRc > /floppy/timestamp_modification.txt
ls -alR > /floppy/timestamp_creation.txt
```

Design your network

- will you offer public services (web server, dial-up users, anonymous ftp server)
- split networks on public and private subnets
- determine which services you need
- filter traffic between subnets and the internet

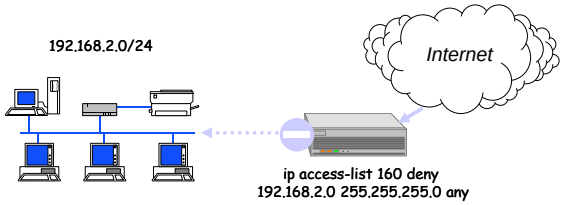
Basic router filtering
Prevent spoofing

- drop packets that have source address different from the assigned range



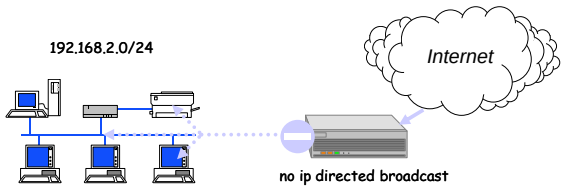
Basic router filtering
Guard against IP address trust exploits

- drop packets with your network's source address coming from internet



Basic router filtering
Don't help flooders

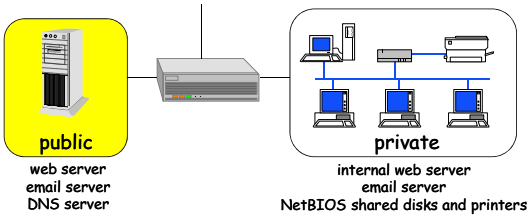
- prevent your network being used as a DoS amplifier



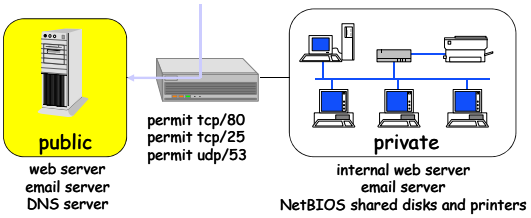
Division of the network

- public segment
  - DNS server
  - public web server
  - mail server (MX record points to it)
- private segment
  - internal web server
  - SMB/NetBIOS shares
  - mail server (retrieves mail from the mail server on the public segment)

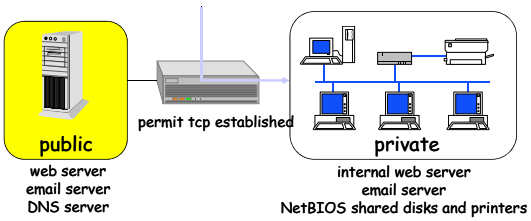
Filtering traffic (1)



Filtering traffic (2)



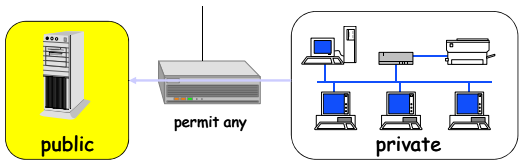
Filtering traffic (3)



web server
email server
DNS server

internal web server
email server
NetBIOS shared disks and printers

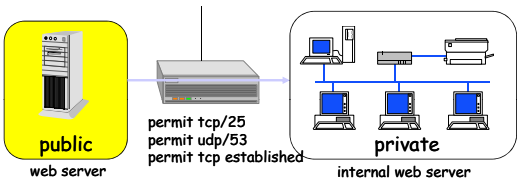
Filtering traffic (4)



web server
email server
DNS server

internal web server
email server
NetBIOS shared disks and printers

Filtering traffic



web server
email server
DNS server

internal web server
email server
NetBIOS shared disks and printers