CSIS 4222

Ch 4: Other Internet Applications
File Access and Email
Ch 23: Network Address Translation (NAT)
Ch 24: IPv6

Network File System

- File transfer not needed for all data transfers
- File access service allows remote clients to copy or change small parts of file
- File access mechanism used with TCP/IP is Network File System (NFS)
  – Allows client to copy or change pieces of file
  – Allows shared file access
  – Integrates into computer's file system

Email

- Originally was just file transfer (UUCP)
- Has two parts:
  – User agents (mail readers)
  – Message transfer agents

Electronic Mail

- Originally was just file transfer (UUCP)
- Internet email specifications:

Type	Description
Transfer	A protocol used to move a copy of an email message from one computer to another
Access	A protocol that allows a user to access their mailbox and to view or send email messages
Representation	A protocol that specifies the format of an email message when stored on disk

Figure 4.12 The three types of protocols used with email.

Email Representation Standards (RFC2822)

- RFC (Request For Comments) 2822 Mail Message Format
  (Student hackers win over industry giants - X.400)
  – A mail message is represented as a text file and consists of
    - a header section
    - a blank line
    - and a body
  – Header lines each have the form:
    Keyword: information
    - From:, To:, Subject:, Cc:

Email Representation Standards (MIME)

- Originally all email was ASCII (7-bit, 1000 chars/line max.)
- Multi-purpose Internet Mail Extensions (MIME) extends email to allow transfer of non-text data in a message
  – MIME specifies how a binary file can be encoded into printable characters
  – The Base64 encoding standard is most popular

Message Transfer Agents

- SMTP (Simple Mail Transfer Protocol)
  - Source machine establishes TCP connection to port 25 of destination
  - Email deamon listens to this port, accepts incoming connection, and copies message to appropriate mailbox
- Email gateways are needed for systems using different protocols

---

ISPs, Mail Servers, and Mail Access

Figure 4.14 An email configuration where an ISP runs an email server and provides a user access to a mailbox.

ISPs, Mail Servers, and Mail Access

- Web browser access to email:
  - ISP provides a special web page that displays messages from a user's mailbox
  - Email access from any computer without special mail interface application
- Mail application can download an entire mailbox onto a local computer
  - User can process email when disconnected from the Internet
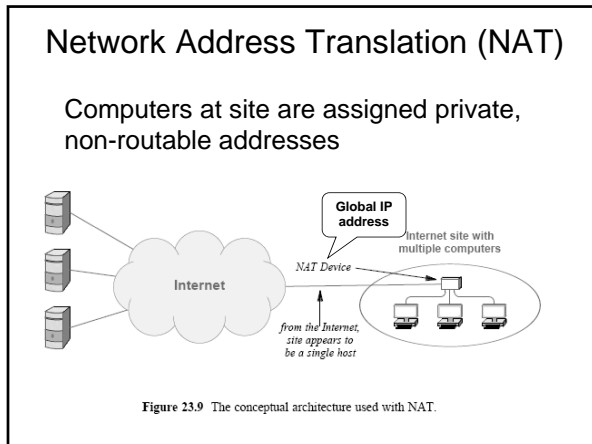

Message Transfer Agents

- POP3 (Post Office Protocol)
  - Fetches email from a mailbox on a remote server
  - Stores email on user's local machine
  - May or may not delete message from mailbox on server
- IMAP4 (Interactive Mail Access Protocol)
  - Interacts directly with server
  - Does not copy & store email on local machine
- Other proprietary protocols, like Microsoft Exchange

Network Address Translation (NAT)

- Motivated by exhaustion of IP address space
- An extension of original addressing scheme
- Allows multiple computers to share a single address
  - Site appears as if it consists of a single host computer with a valid IP address
- Requires a device to perform packet translation

NAT Details

- Site obtains a single, globally valid IP address
  - Assigns a *private* address to each computer
- NAT runs as an in-line service
  - It must be placed on the connection between the Internet and a site
- Most implementations embed NAT in another device
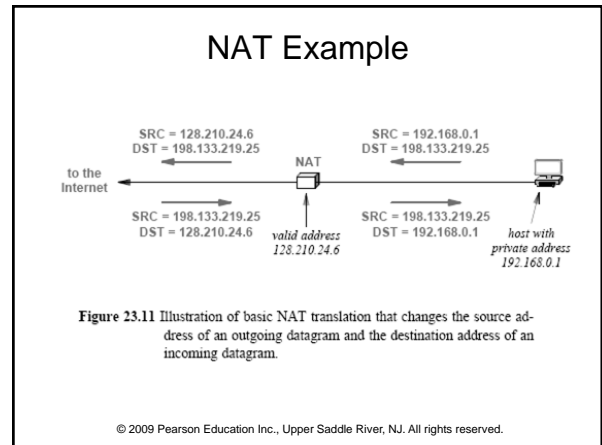 - Like a router or Wi-Fi wireless access point

Network Address Translation (NAT)

Computers at site are assigned private, non-routable addresses

Figure 23.9 The conceptual architecture used with NAT.

NAT Operation

- When viewed from the Internet
  - All datagrams sent from the site appear to originate from one host
  - All datagrams sent to the site appear to be sent to one host
- When viewed from a host in the site
  - The Internet appears to accept and route private addresses

NAT and Private Addresses

Cannot assign a single IP address to multiple computers

- The NAT device itself is assigned a globally-valid IP address
  - The NAT device appears as a host on the Internet
- Each computer at the site is assigned a unique private address (non-routable)

Block	Description
10.0.0.0/8	Class A private address block
169.254.0.0/16	Class B private address block
172.16.0.0/12	16 contiguous Class B blocks
192.168.0.0/16	256 contiguous Class C blocks

NAT Example

Figure 23.11 Illustration of basic NAT translation that changes the source address of an outgoing datagram and the destination address of an incoming datagram.

NAT Example

Most implementations of NAT use a translation table to store the information needed to rewrite addresses

Direction	Field	Old Value	New Value
out	IP Source	192.168.0.1	128.210.24.6
	IP Destination	198.133.219.25	-- no change --
in	IP Source	198.133.219.25	-- no change --
	IP Destination	128.210.24.6	192.168.0.1

Network Address and Port Translation (NAPT)

- By far the most common form of NAT
- Can change TCP or UDP protocol port numbers as well as IP addresses
- Allows
  - Multiple computers at site to communicate with a single destination
  - Multiple users on given computer to communicate with the same destination

Transport-Layer NAT (NAPT)

NAPT operates on transport-layer headers
– NAPT entries are 4-tuples of source & destination IP addresses and protocol port numbers
– NAPT chooses alternative source port numbers to avoid conflicts

Dir.	Fields	Old Value	New Value
out	IP SRC:TCP SRC	192.168.0.1:30000	128.10.24.6:40001
out	IP SRC:TCP SRC	192.168.0.2:30000	128.10.24.6:40002
in	IP DEST:TCP DEST	128.10.19.20:40001	192.168.0.1:30000
in	IP DEST:TCP DEST	128.10.19.20:40002	192.168.0.2:30000

NAT and Servers

• NAT system builds a translation table automatically by watching outgoing traffic
• This does not work well for communication initiated from the Internet to the site

Example: If multiple computers at a site each run a web server the NAT device cannot know which computer should receive an incoming web connection

• Twice NAT is a variant that allows a site to run multiple servers
– Interacts with the site's DNS server

NAT for Home Use

• NAT is very useful for residence or small business with a broadband connection
– Allows a set of computers to share the connection without purchasing additional IP addresses
• NAT software can make a PC act as a NAT device
• Also, can use cheap dedicated NAT hardware
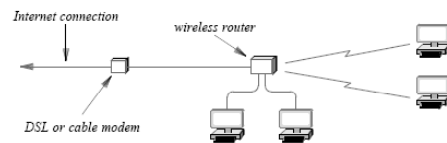– Wireless routers

NAT for Home Use

Figure 23.14 Illustration of the connections for a wireless router.

IPv6 - The Motivation for Change

• Originally, 32-bit IP address were selected
– Allowed the Internet to include over a million networks
• The Internet is growing exponentially
– Size doubles in less than a year
• Scarcity of available addresses was considered crucial when work began on a new version of IP in 1993
– No emergency occurred
– IP has not been changed
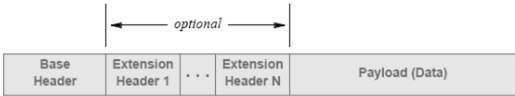• Think of the importance of IP and the cost to change!

IPv6 Features

• Keeps many successful features of IPv4
• But IPv6 changes all the details
– Address Size: 128 bits
• Large enough address space to accommodate continued growth of Internet for many decades
– Header Format: completely different
– Support for Real-Time Traffic: audio and video applications
– Extensible Protocol: Can add new features

IPv6 Datagram Format

An IPv6 datagram contains
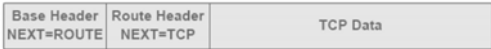- a base header
- zero or more extension headers
- payload

Base Header	Extension Header 1	· · · Extension Header N	Payload (Data)

optional

Why Multiple Headers?

- Economy
  - Saves space
  - A given datagram is expected to use only a small subset
  - Can define a large set of features without requiring each datagram header to have at least one field for each
- Extensibility
  - How to add a new feature to a protocol?
  - IPv4 requires a complete change to accommodate new feature
  - In IPv6 existing protocol headers can remain unchanged
    - A new NEXT HEADER type is defined as well as a new header format

Base Header NEXT=ROUTE	Route Header NEXT=TCP	TCP Data

IPv6 Addressing

- IPv6 address occupies 128 bits
  - Written in colon hexadecimal notation (colon hex)
    69DC : 8864 : FFFF : FFFF : 0 : 1280 : 8C0A : FFFF
- Like CIDR addresses, the division between prefix and suffix can occur on an arbitrary boundary
  - Addresses have a multi-level hierarchy
    - highest level corresponds to an ISP
    - next level corresponds to an organization
    - the next to a site, etc.

IPv6 Addressing

Transitioning to IPv6
- The designers mapped existing IPv4 addresses into the IPv6 address space
- Any IPv6 address that begins with 96-zero bits contains an IPv4 address in the low-order 32-bits

IPv6 – When?

- Proponents claimed that IPv6 was needed because IPv4 could not handle audio or video, was not secure, and would run out of addresses
- Meanwhile, IPv4 has adapted
  - runs multimedia applications
  - offers as much security as IPv6
  - NAT and CIDR have extended the IPv4 addressing capabilities
- IPv4 continues as the fundamental protocol of the Internet

IPv6 – Ever?

- At this point, there is no technical reason to adopt IPv6
- IPv6 packet processing incurs more overhead
  - Moving to IPv6 may limit the speeds with which packets can be sent
- The motivation for IPv6 becomes an economic tradeoff
- Who knows when customers will decide that the high cost justifies a change