TUNNELS, VPNS, AND NATS

Internet Protocols

CSC / ECE 573

Fall, 2005

N. C. State University

Announcements

Today's Lecture

I. VPNs

II. Application Gateways

III. NAT / NAPT

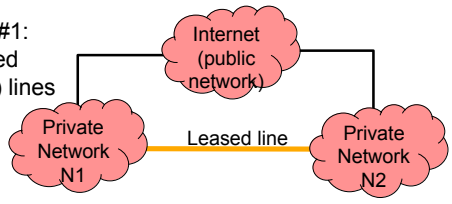
VIRTUAL PRIVATE NETWORKS

Private and Public Networks

- Internet addresses are public; globally unique and meaningful
  - e.g., for routing purposes
  - servers want to be found, and clients want to be reachable
- Some people want private addresses! Why? ...
  - provides flexibility in re-assigning addresses
  - conceals internal network configuration / topology
  - protects hosts

Interconnecting Private Networks

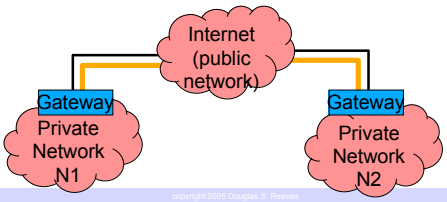
- Choice #1: dedicated (leased) lines



- Features
  - excellent reliability, availability, predictability
  - excellent protection, isolation from the public Internet
- Expensive! Is there a lower-cost way?

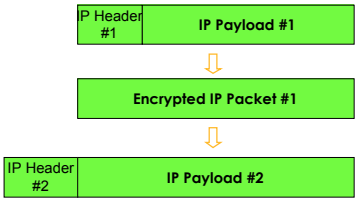
Choice #2: VPNs

- *VPN* = Virtual Private Networks
- Establish a connection through the Internet that "acts like" a leased line!
- VPNs = **tunneling + encryption**



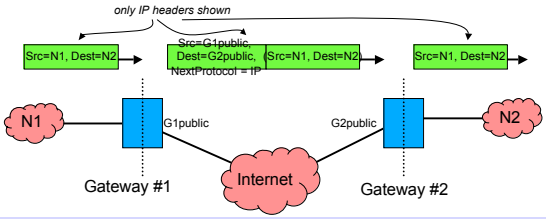
Tunneling (Encapsulation) + Encryption

- IP-inside-of-IP!
- A "virtual" dedicated connection



VPN Example

- Tunnel endpoints (*gateways*) needed for encapsulation / decapsulation
  - sit at the boundary between public/private networks
- Definitely lower cost than leased lines



Some Tunneling Choices

- Application layer?
- IP layer?
- Lower layers (MPLS, optical, ...)?
- Where should the gateway be located
  - host
  - router?

Some Uses of Tunneling

- VPNs
- Multicast over Unicast (MBONE)
- IPv6 over IPv4 (6BONE)
- X-BONE (generalized IP-in-IP)
- Application-layer (overlay) networks
  - e.g., peer-to-peer

Challenges in Tunneling

- Overhead introduced (extra header)
- Routing Inefficiency (why?)
- Gateway expense, administration
  - if gateways aren't used, then hosts have to be upgraded
- Can the Internet provide other leased-line properties…
  - guaranteed bandwidth for tunnels?
  - guaranteed reliability / availability for tunnels?

APPLICATION LAYER GATEWAYS

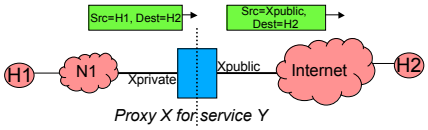
Connecting Private to Public Networks

- Even people in private networks (wishing to remain anonymous) want access to public services
  - e.g., web, mail, ftp, …
- How can you establish communication without revealing your private address?
  - (i.e., how correspond with someone without giving away your home address?)

Connecting Private to Public (cont'd)

- Analogy: use a post-office box
  - a "public delivery service" gets mail to your PO box
  - a "private delivery service" gets mail from your PO box to you
  - key point: you must be able to trust the provider of the PO box (why?)

Application Gateways (Proxies)



Proxy X for service Y

1. For service Y at H2, user at private address H1 sends request to Proxy X
2. X forwards H1's request to H2, after substituting X's public address for H1's address
3. H2 responds to X
4. X "remembers" this is a response to a request from H1, forwards the response back to H1

Application Gateway Examples

- Web proxy
- Mail relays and servers
- "Anonymizers"
- Transcoders
- ...

Other Benefits of Application Gateways

- May do some transformation of requests and/or responses, e.g.,
  - remove pop-up ads
  - remove spam
  - compress images
- A gateway can also be a translator
  - between versions of a protocol or application
- Another potential benefit... load balancing
  - gateway redirects requests among a set of servers

Drawbacks of Application Gateways

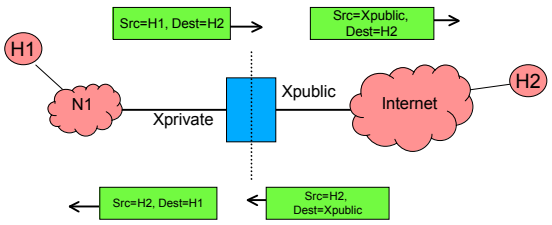
- Expense
- Extra latency
- Application specific; a gateway for every application?

NETWORK ADDRESS TRANSLATION

Network Address Translation (NAT) (RFC3022)

- NAT translates private addresses to public addresses, and vice versa
  - a cheaper, more general solution than application gateways
  - however, less functionality
- Instead of translating at the application layer, translates at the IP layer

Example



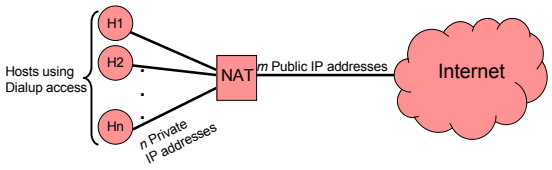
Address translator for IP addresses only

Permanent NAT

- *Permanent* means
  one private IP address ⇔ one public IP address
- Address bindings may be created…
  - statically: configured manually by administrator or DHCP
  - dynamically: when a packet is sent from the private to the public network
  - on demand: when a host in the public network requests a DNS translation for a server hostname to a server public address
- When is it safe to terminate an address binding?

Reducing the Number of Public Addresses

- If there are *n* hosts in the private network, but only *m*<*n* need public addresses at the same time, the NAT only needs to provide *m* public addresses



Network Address Port Translation (*NAPT*)

- What if *m* = 1?
- Solution: do *port-mapping*
  - host on private network generates packet with private SrcIP=*a*, SrcPort=*p*
  - NAPT maps this to the public SrcIP=*A*, SrcPort=*P*
- Example:

Private IP Addr	Private IP Port	Public IP Addr	Public IP Port
192.168.0.3	2004	152.14.62.55	13135
192.168.0.3	4471	152.14.62.55	13147
192.168.0.6	1942	152.14.62.55	13151
192.168.0.6	2004	152.14.62.55	13158

NAPT (cont'd)

- Reminder: how many TCP and UDP ports are there?
  - is this enough?
  - what if there are thousands of connections to a single server?
  - what if there are multiple servers using the same source port?

Challenges of NAT

- Some application payloads contain IP addresses and/or port numbers
  - ex.: FTP, SIP, ICMP, …
- The NAT/NAPT box has to understand the payload format and do translations there, too ☹
  - greatly complicates NAT/NAPT
  - how many should you support, and how upgrade?
- What if the payload is encrypted / authenticated?
- IP "purists" dislike NAT

Summary

- Tunneling is a powerful concept with many uses
  - incurs overhead, but provides great flexibility
- Tunneling + encryption = VPN
- NAT / NAPT are very handy for getting more "mileage" out of current IPv4 address space
  - but they make life more difficult for protocol designers

Next Lecture

- IPv6