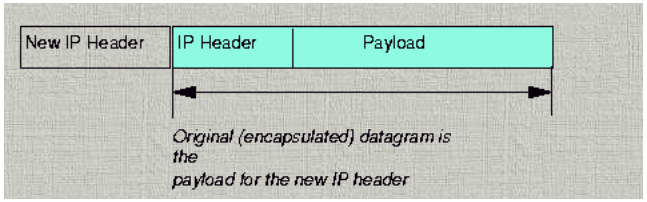
Tunneling and Translating

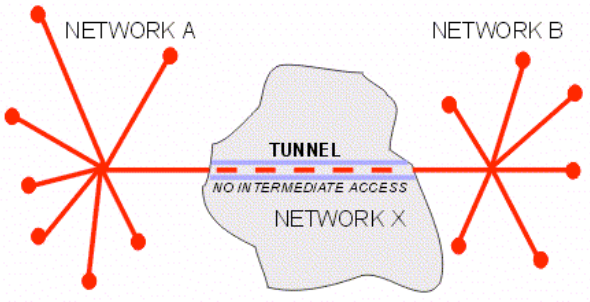
CSE461

Tunneling

- Encapsulate one protocol in another
  - Make IP look like IPV6, or secure IP, or..



- May rely on PROXY architecture
  - –A *network agent* that translates from the tunneled protocol to the tunneling protocol.



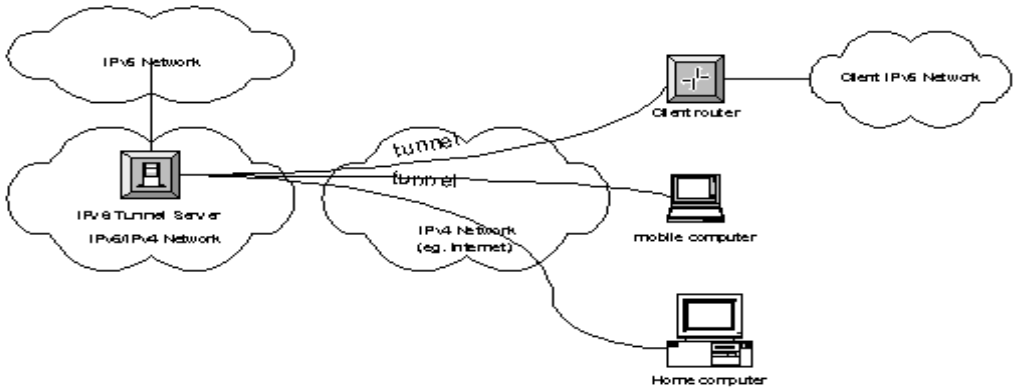
•Permits broad, but gradual, deployment of new services

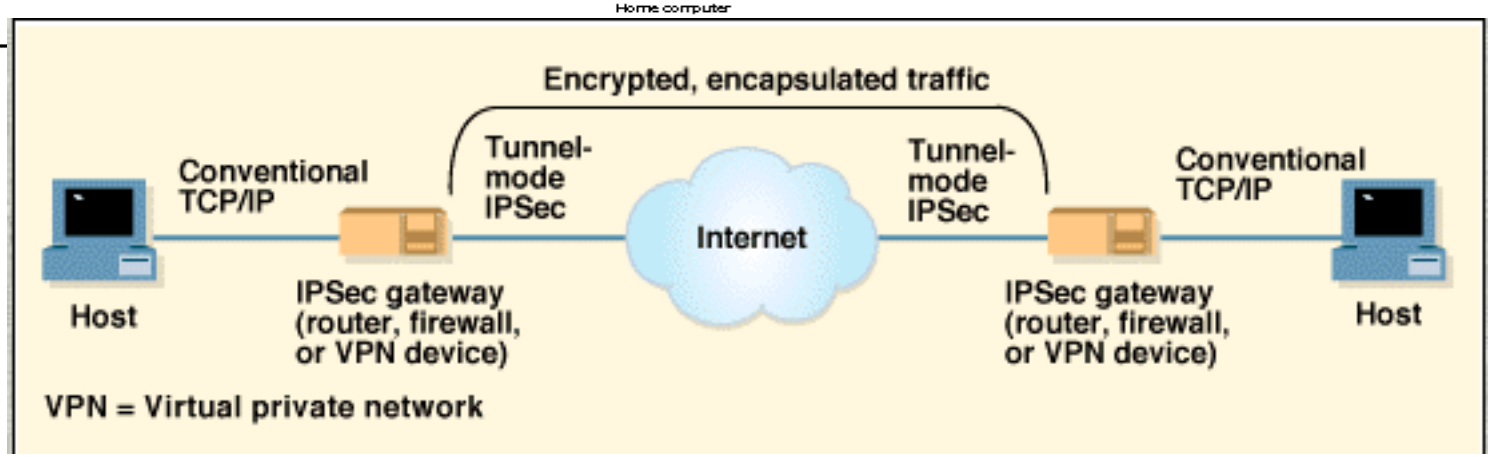
  - –Build tomorrow's services on today's.
  - •Anticipates that a given service may one day be "built into" the network.

Example: IPV6 Tunnel

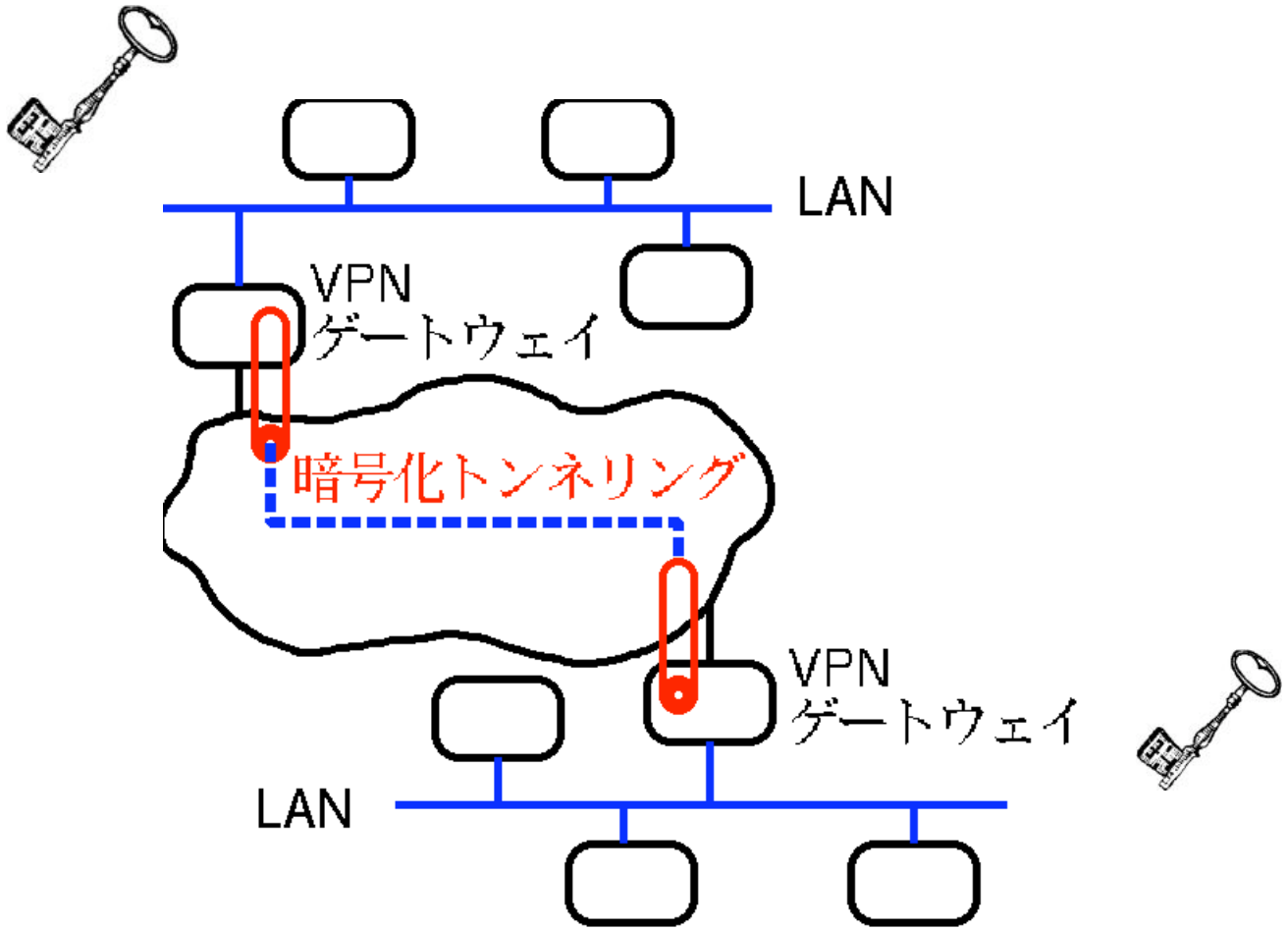
IPv6 tunnel server model

- IPv6 tunnel server: gives IPv6 connectivity to clients over an IPv4 network





Example: VPN Tunnel



Mobile IP

- Problem: How to enable a node to move from one IP subnet to another.

Mobile IP

RFC 2002: http://www.cis.ohio-state.edu/htbin/rfc/rfc2002.html
RFC 2290: http://www.cis.ohio-state.edu/htbin/rfc/rfc2290.html
RFC 2344: http://www.isi.edu/in-notes/rfc2344.txt

The Mobile IP protocol enables nodes to move from one IP subnet to another. Each mobile node is always identified by its home address, regardless of its current point of attachment to the Internet. While situated away from its home, a mobile node is also associated with a care-of address, which provides information about its current point of attachment to the Internet. The protocol allows registration of the care-of address with a home agent. The home agent sends datagrams destined for the mobile node through a tunnel to the care-of address. After arriving at the end of the tunnel, each datagram is then delivered to the mobile node. It can be used for mobility across both homogeneous and heterogeneous media. Mobile IP defines a set of new control messages, sent with UDP, Registration Request and Registration Reply.
The IP packet consists of the IP source and destination addresses, followed by the UDP source and destination ports, followed by the Mobile IP fields. Mobile IP packets can be either registration request or registration reply.
The format of the Mobile IP registration request message is shown in the following illustration:

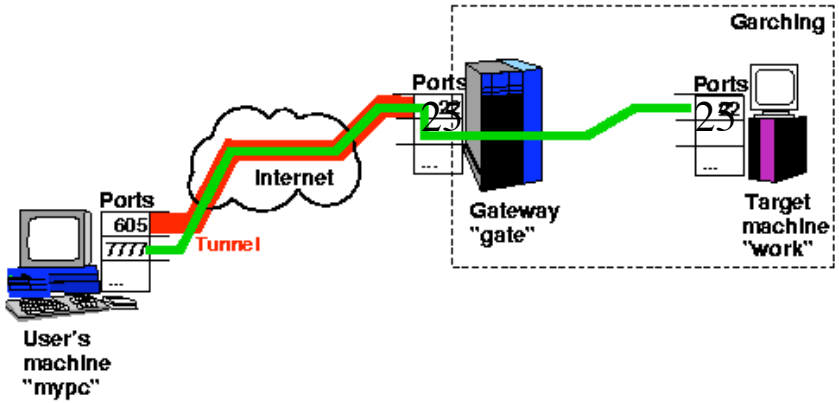
8	9	10	11	12	13	14	15	16	Octet
Type	S	B	D	M	G	V	T	Rsv	2
Lifetime									4
Home address									8
Home agent									12
Care of address									16
Identification									20
Extensions ...									...

Mobile IP registration request message structure

SSH Tunnel (Port Forwarding)

- Transport packets destined for one endpoint to another
  - Eg, “please revector all packets sent to my ip address, port 1029, to 128.95.1.4:3000”

```
[laptop:Edu/461/Slides] bershad% ssh -N -L 7777:june.cs.washington.edu:25 hugh.cs.washington.edu
```



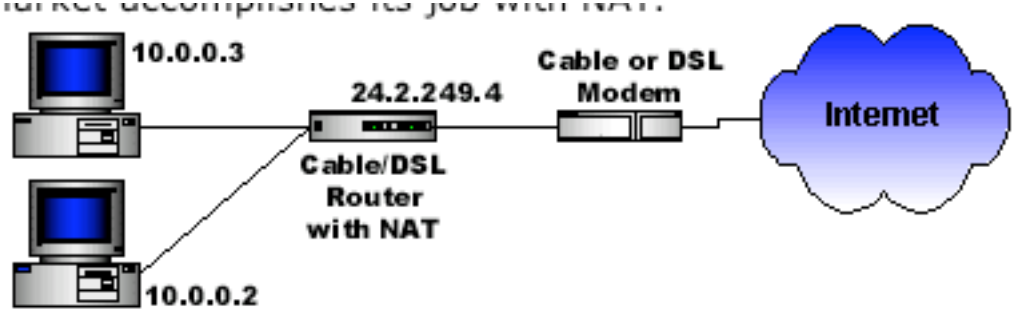

```
[laptop:~] bershad% telnet localhost 7777
Trying ::1...
Connected to localhost.
Escape character is '^]'.
220 june.cs.washington.edu ESMTP Sendmail 8.13.0/8.13.0/1.4; Mon, 29 Nov 2004 15:02:06 -0800 (PS
T)
helo
501 5.0.0 helo requires domain address
```

Translation

- Mechanically “mutate” the packets on ingress/egress
- Requires some sort of real or apparent proxy

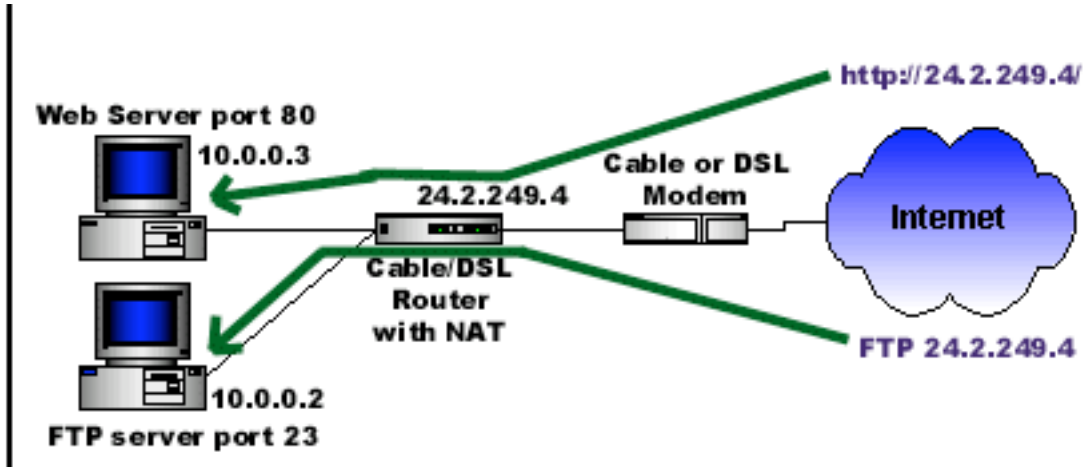
Network Address Translation RFC 1631

- Problem: How to give everybody their own network
  - Subnets (Class A, B, C, D…)
  - IPV6
  - NATted Networks
- Idea: Burn 1 IP address and not a whole subnet
  - Assign network ingress/egress a routable network address
  - Assign hosts a “non routable” network address
  - Translate IP packets as they come and go



Challenges with NAT

- A non-routable address is not very routable



VOIP, Web servers, etc require special “hacks”

10., 192., 172., 169!!

Protocol “Leakage”

- Translators only work well if they translate everything that needs to be translated.
- What if the data portion of the conversation “reveals” something about the part that is being translated
  - Active vs. Passive mode FTP
- Forces us to make smarter and smarter (“statefuller”) NATters

Bootstrapping

- Problem: How to assign a protocol "identifier" to a dumb host?
  - IP address, host name, etc.
- Assume
  - Some unique ID (enet address)
  - Broadcast

DHCP

1. What is DHCP?

   DHCP stands for "Dynamic Host Configuration Protocol".

2. What is DHCP's purpose?

   DHCP's purpose is to enable individual computers on an IP network to extract their configurations from a server (the 'DHCP server') or servers, in particular, servers that have no exact information about the individual computers until they request the information. The overall purpose of this is to reduce the work necessary to administer a large IP network. The most significant piece of information distributed in this manner is the IP address.

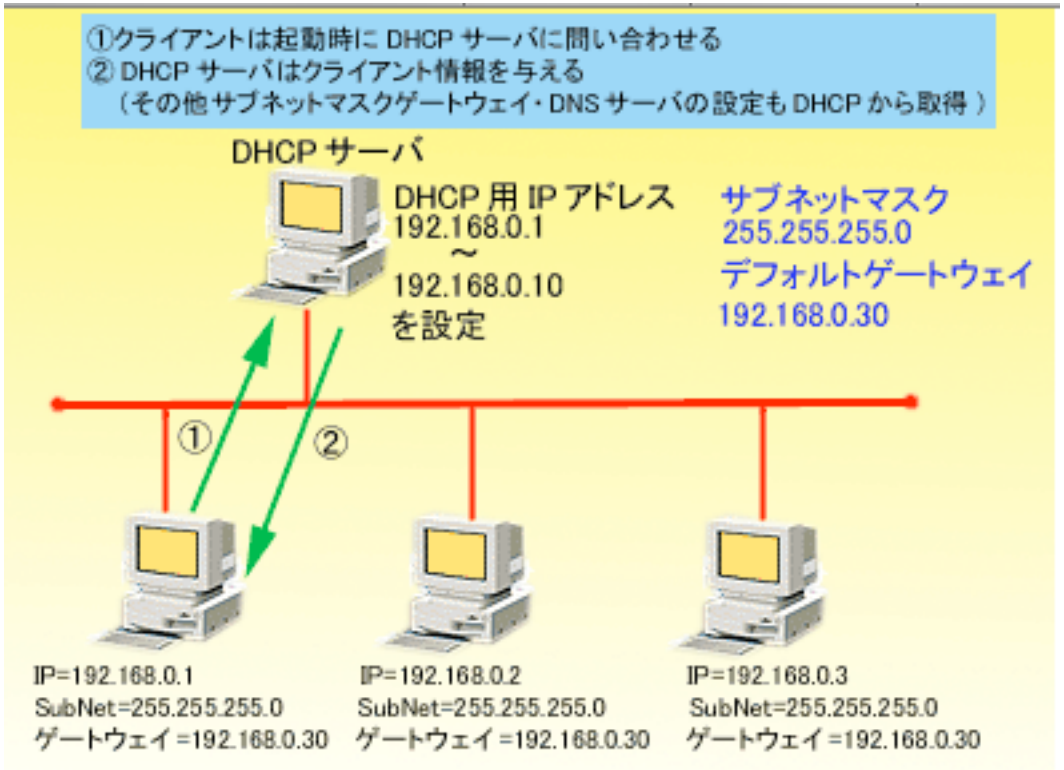
4. Who Created It? How Was It Created?

   DHCP was created by the Dynamic Host Configuration Working Group of the Internet Engineering Task Force (IETF; a volunteer organization which defines protocols for use on the Internet). As such, it's definition is recorded in an Internet RFC and the Internet Activities Board (IAB) is asserting its status as to Internet Standardization. As of this writing (June 1998), DHCP is an Internet Draft Standard Protocol and is Elective. BOOTP is an Internet Draft Standard Protocol and is Recommended. For more information on Internet standardization, see RFC2300 (May 1998)

5. How is it different than BOOTP or RARP?

   DHCP is based on BOOTP and maintains some backward compatibility. The main difference is that BOOTP was designed for manual pre-configuration of the host information in a server database, while DHCP allows for dynamic allocation of network addresses and configurations to newly attached hosts. Additionally, DHCP allows for recovery and reallocation of network addresses through a leasing mechanism.

DHCP In Action



DHCP+NAT

- One gives you an address that's potentially always changing
- Another conceals your internal addressing structure from the outside world
- Where is this great?
- Where is this lousy?

Summary

- Protocols we already know lend themselves well to new protocols
- New protocols may directly leverage existing ones
- Or they may support them
- Interactions which often “feel” like bugs are often indicators of a more general property.