

**PART XIX**

**PRIVATE NETWORK INTERCONNECTION  
(NAT AND VPN)**

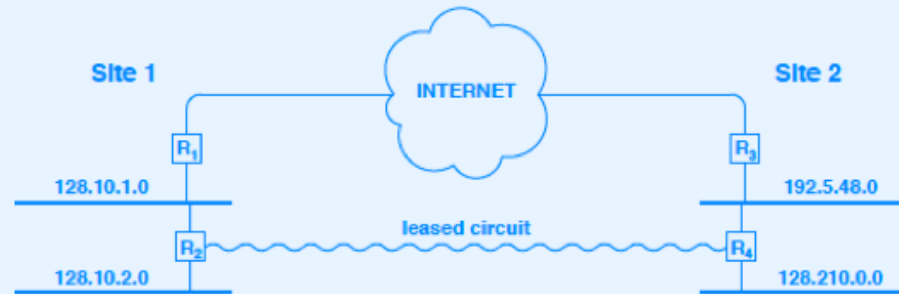
## Definitions

- An internet is *private* to one group (sometimes called *isolated*) if none of the facilities or traffic is accessible to other groups
  - Typical implementation involves using leased lines to interconnect routers at various sites of the group
- The global Internet is *public* because facilities are shared among all subscribers

## **Hybrid Architecture**

- Permits some traffic to go over private connections
- Allows contact with global Internet

## Example Of Hybrid Architecture



## **The Cost Of Private And Public Networks**

- Private network extremely expensive
- Public Internet access inexpensive
- Goal: combine safety of private network with low cost of global Internet

## Question

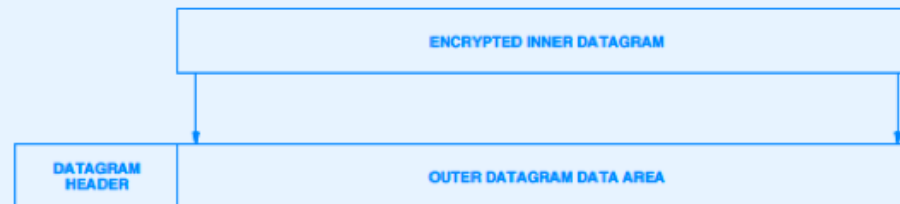
*How can an organization that uses the global Internet to connect its sites keep its data private?*

- *Answer: Virtual Private Network (VPN)*

## Virtual Private Network

- Connect all sites to global Internet
- Protect data as it passes from one site to another
  - Encryption
  - IP-in-IP tunneling

## Illustration Of Encapsulation Used With VPN

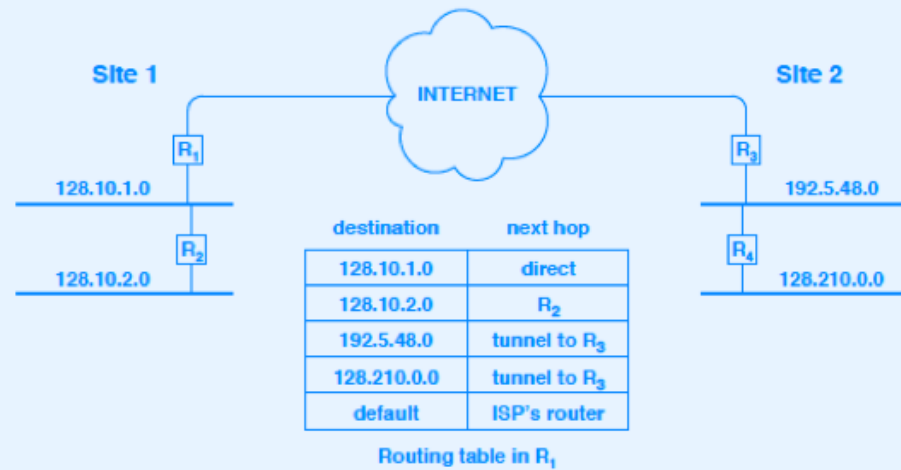




## **The Point**

*A Virtual Private Network sends data across the Internet, but encrypts intersite transmissions to guarantee privacy.*

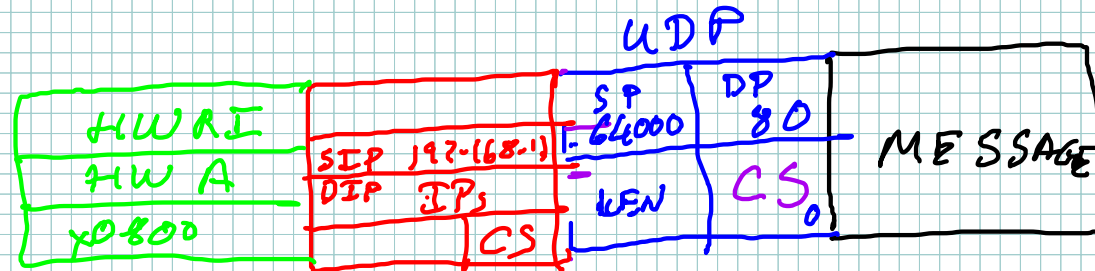
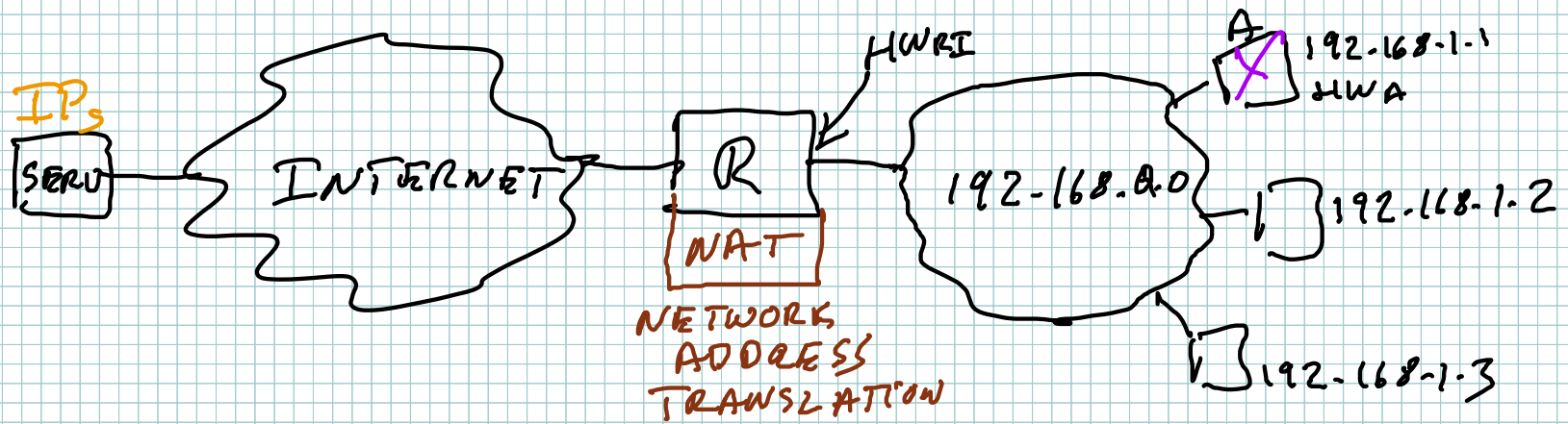
## Example Of VPN Addressing And Routing



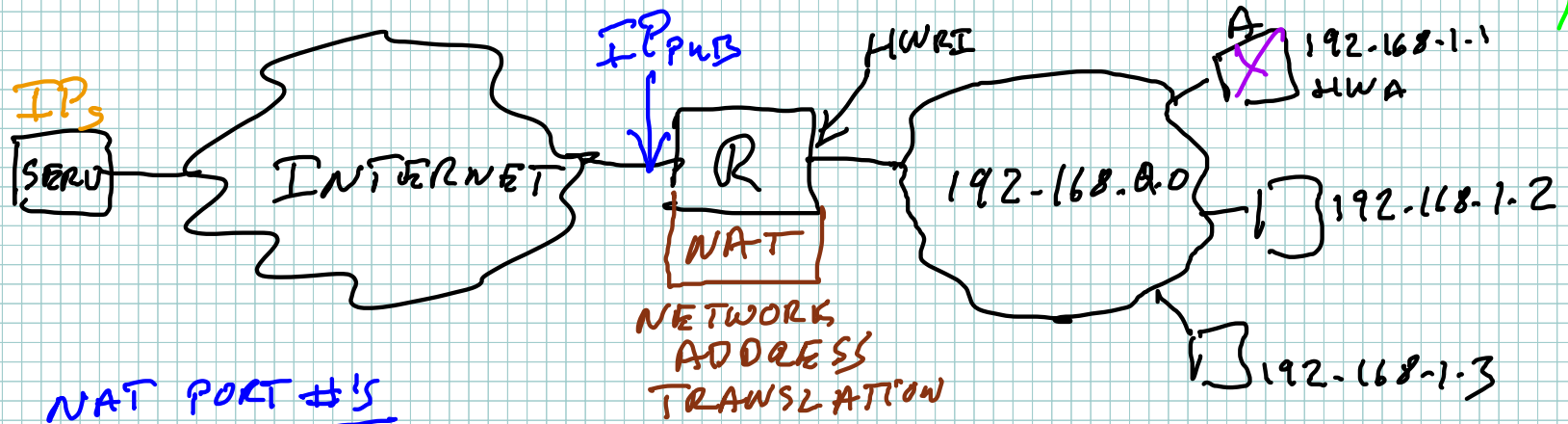
## Example VPN With Private Addresses



- Advantage: only one globally valid IP address needed per site



ORIGINAL MESSAGE  
FROM A TO R

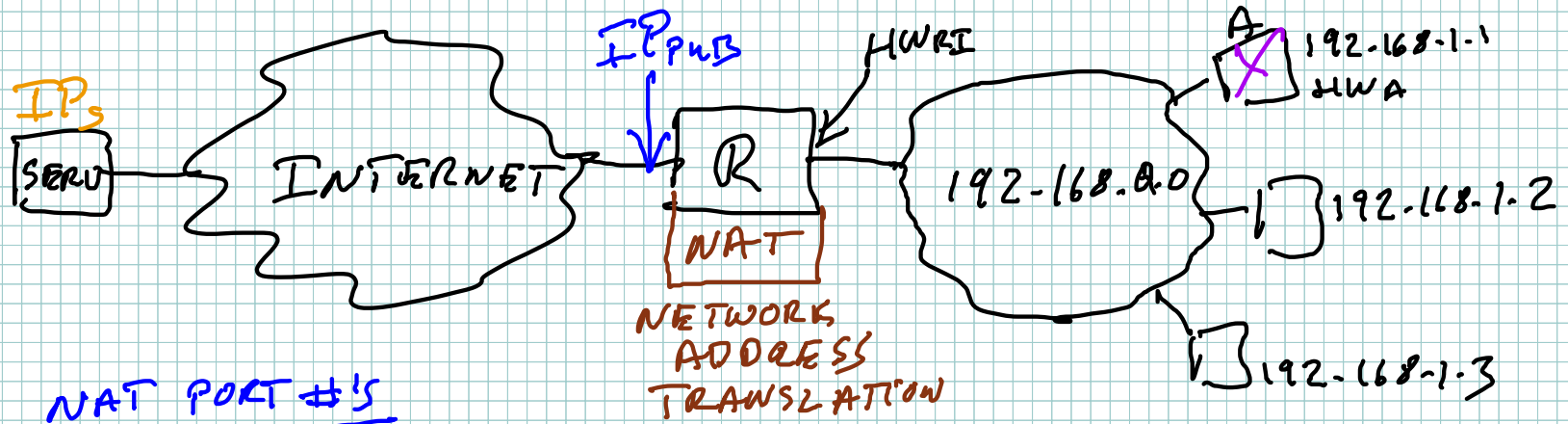


NAT PORT #S

P<sub>1</sub>, P<sub>2</sub>, P<sub>3</sub>, P<sub>4</sub> ..., P<sub>N</sub>

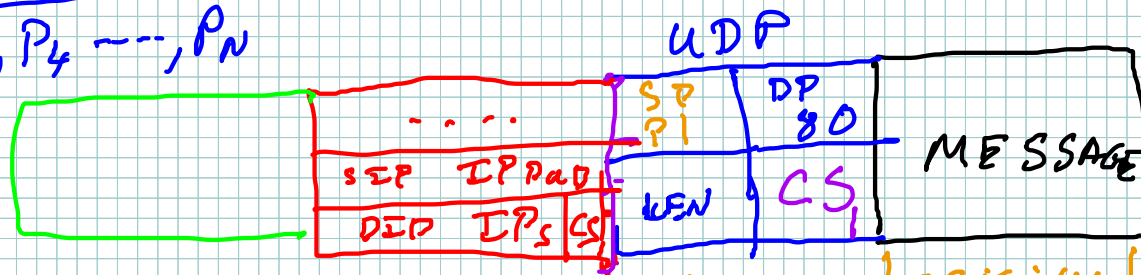
NAT IN R  
CAPTURES  
INFO FROM  
MESSAGE

ORIGINAL SRC PORT	NAT PORT	ORIGINAL IP	PROTOCOL
62000	P <sub>1</sub>	192.168.1.1	UDP



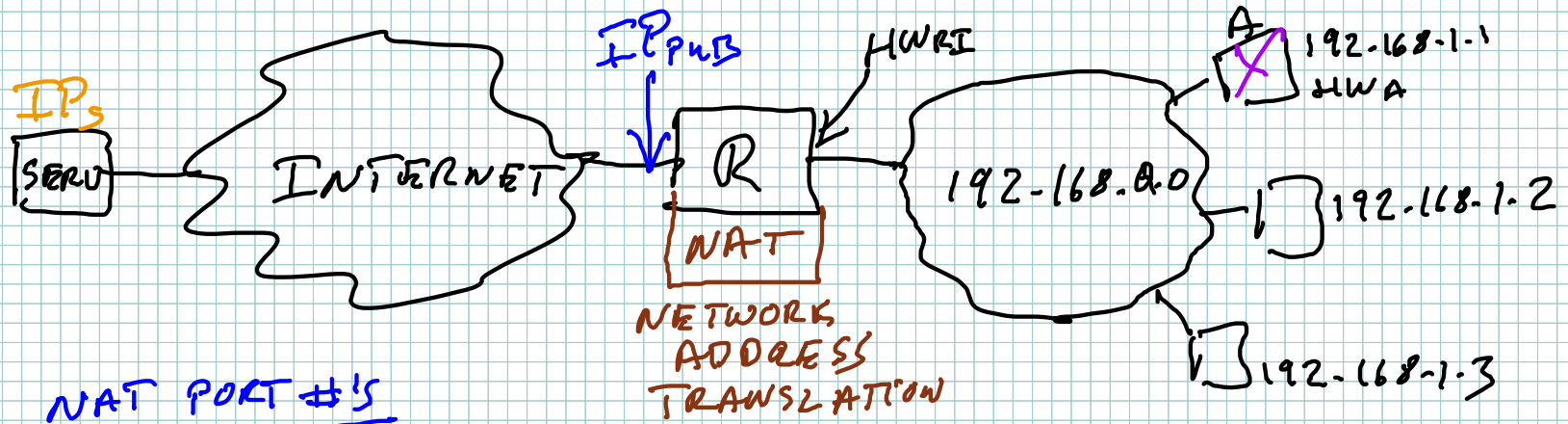
NAT PORT #'S

$P_1, P_2, P_3, P_4, \dots, P_N$

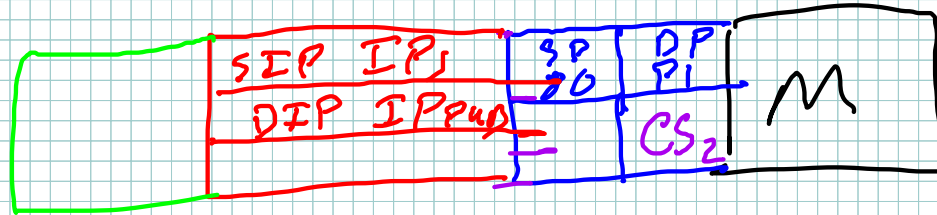


NAT  
CHANGES  
ON WAY OUT

ORIGINAL SRC PORT	NAT PORT	ORIGINAL IP	PROTOCOL
62000	P1	192.168.1.1	UDP

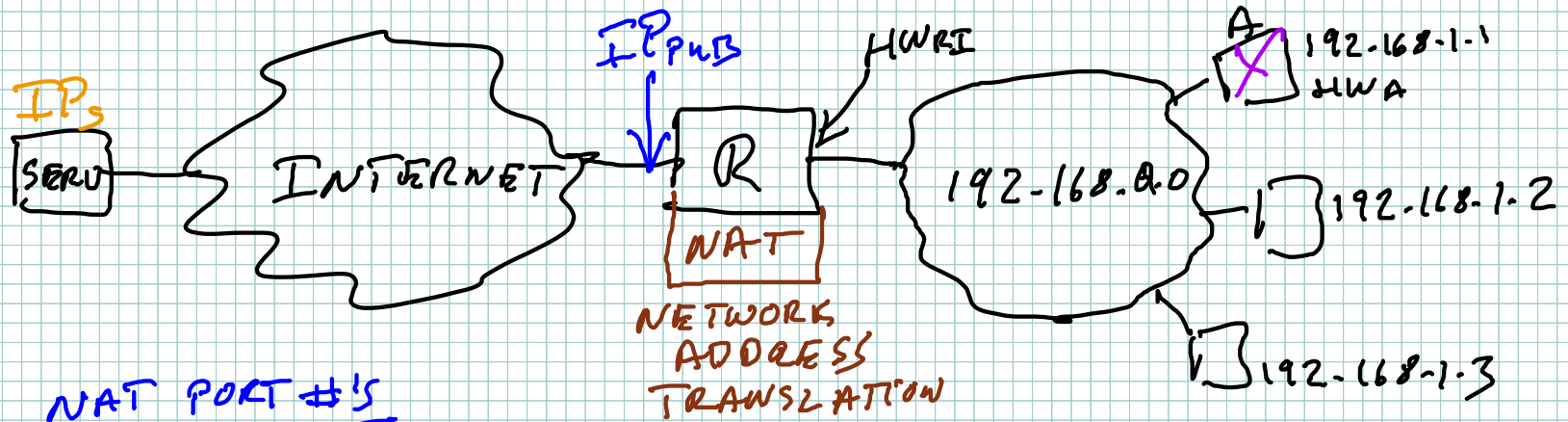


NAT PORT #S  
P<sub>1</sub>, P<sub>2</sub>, P<sub>3</sub>, P<sub>4</sub> ..., P<sub>N</sub>



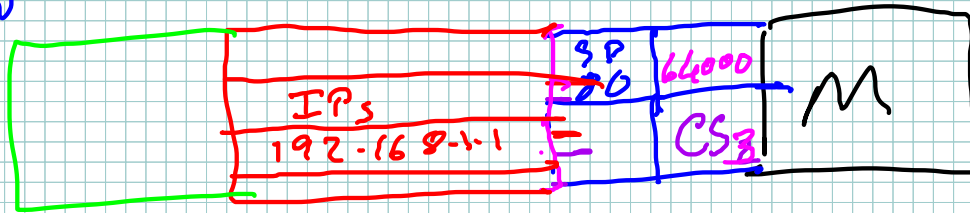
RESPONSE  
FROM SERV

ORIGINAL SRC PORT	NAT PORT	ORIGINAL IP	PROTOCOL
62000	P <sub>1</sub>	192-168-1-1	UDP



NAT PORT #S

$P_1, P_2, P_3, P_4, \dots, P_N$



ORIGINAL SRC PORT	NAT PORT	ORIGINAL IP	PROTOCOL
66000	$P_1$	192.168.1.1	UDP

BACK AT  
ROUTER

CHANGES FOR  
DELIVERY TO A



## General Access With Private Addresses

- Question: how can a site provide multiple computers at the site access to Internet services without assigning each computer a globally-valid IP address?
- Two answers
  - Application gateway (one needed for each service)
  - *Network Address Translation (NAT)*

## **Network Address Translation (NAT)**

- Extension to IP addressing
- IP-level access to the Internet through a single IP address
- Transparent to both ends
- Implementation
  - Typically software
  - Usually installed in IP router
  - Special-purpose hardware for highest speed

## Network Address Translation (NAT) (continued)

- Pioneered in Unix program *slirp*
- Also known as
  - *Masquerade* (Linux)
  - *Internet Connection Sharing* (Microsoft)
- Inexpensive implementations available for home use

## NAT Details

- Organization
  - Obtains one globally valid address per Internet connection
  - Assigns nonroutable addresses internally (net 10)
  - Runs NAT software in router connecting to Internet
- NAT
  - Replaces source address in outgoing datagram
  - Replaces destination address in incoming datagram
  - Also handles higher layer protocols (e.g., pseudo header for TCP or UDP)

## NAT Translation Table

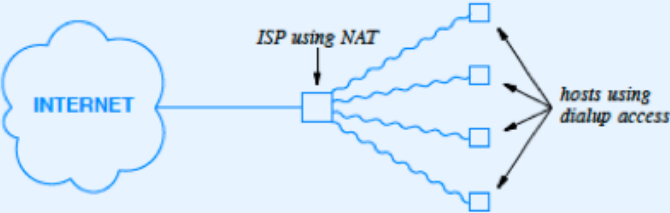
- NAT uses translation table
- Entry in table specifies local (private) endpoint and global destination.
- Typical paradigm
  - Entry in table created as side-effect of datagram leaving site
  - Entry in table used to reverse address mapping for incoming datagram

## Example NAT Translation Table

Private Address	Private Port	External Address	External Port	NAT Port	Protocol Used
10.0.0.5	21023	128.10.19.20	80	14003	tcp
10.0.0.1	386	128.10.19.20	80	14010	tcp
10.0.2.6	26600	207.200.75.200	21	14012	tcp
10.0.0.3	1274	128.210.1.5	80	14007	tcp

- Variant of NAT that uses protocol port numbers is known as *Network Address and Port Translation (NAPT)*

# Use Of NAT By An ISP



## Higher Layer Protocols And NAT

- NAT must
  - Change IP headers
  - Possibly change TCP or UDP source ports
  - Recompute TCP or UDP checksums
  - Translate ICMP messages
  - Translate port numbers in an FTP session



## **Applications And NAT**

*NAT affects ICMP, TCP, UDP, and other higher-layer protocols; except for a few standard applications like FTP, an application protocol that passes IP addresses or protocol port numbers as data will not operate correctly across NAT.*

## Summary

- Virtual Private Networks (VPNs) combine the advantages of low cost Internet connections with the safety of private networks
- VPNs use encryption and tunneling
- Network Address Translation allows a site to multiplex communication with multiple computers through a single, globally valid IP address.
- NAT uses a table to translate addresses in outgoing and incoming datagrams