EECS 489
Computer Networks

IPv6, NAT, Tunneling, and VPN

Agenda

- NAT
- Tunneling
- VPN

The IP Address Space

- Address space crunch: Classfull
  - 128 “Class A” blocks of 2^{24} addresses – Too big
  - 16K “Class B” blocks of 16K addresses
  - 2M “Class C” blocks of 256 addresses – Too small
  - Wasteful allocation
  - Classless addresses is a solution
    - Now can have networks at arbitrary power of 2 boundary

The IP Address Space - context

- How many IP addresses are there?
  - 2^{32} = 4Billon
- Compare that with
  - How many people in the world?
    - 8.1 Billion people
  - How many smart phones?
    - ~ 6.8 Billion
  - How many connected computers?
    - ~22 billion (2018)
  - Internet of Things projected to connect 22 billion devices by 2025
  - You get my point – right!

IPv6

- Motivated (prematurely) by address exhaustion
  - Addresses four times as big (128-bit)
  - How big is that?
  - 340 trillion, trillion, trillion addresses
- Focused on simplifying IP
  - Got rid of all fields that were not absolutely necessary
- Result is an elegant, if unambitious, protocol

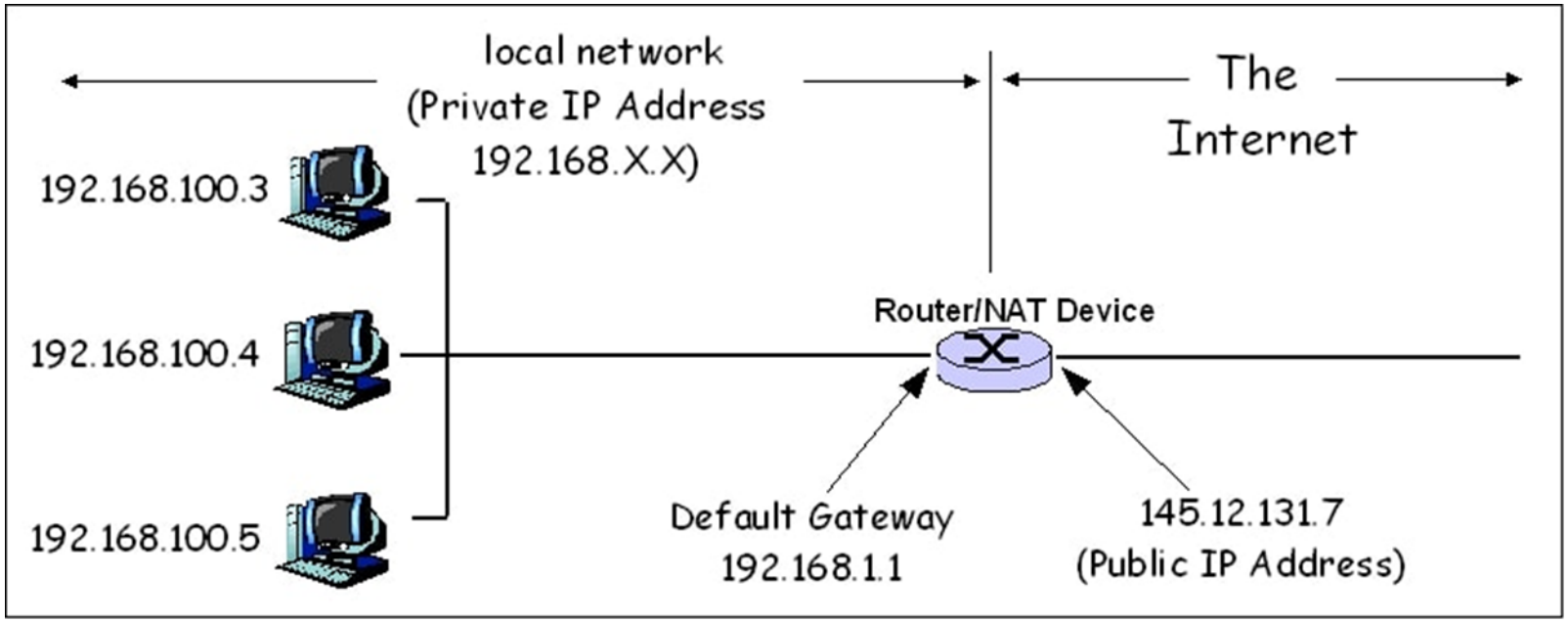
IPv4 to IPv6

- Interoperability with IPv4 is necessary for gradual deployment
- Combination of mechanisms:
  - Dual stack operation: IPv6 nodes support both address types
  - Tunnel IP v6 packets through IP v4 clouds
  - IPv4-IPv6 translation at edge of network
    - NAT must not only translate addresses but also translate between IPv4 and IPv6 protocols
  - IPv6 addresses based on IPv4 – no benefit!
- Now… More on NATs and tunnels

Network Address Translators (NATs)

- NATs originally invented as a quick and dirty hack to create more addresses
- Took on a life of their own
  - May have substantially delayed IPv6 deployment by reducing the address pressure
  - You probably encounter them every day

NAT

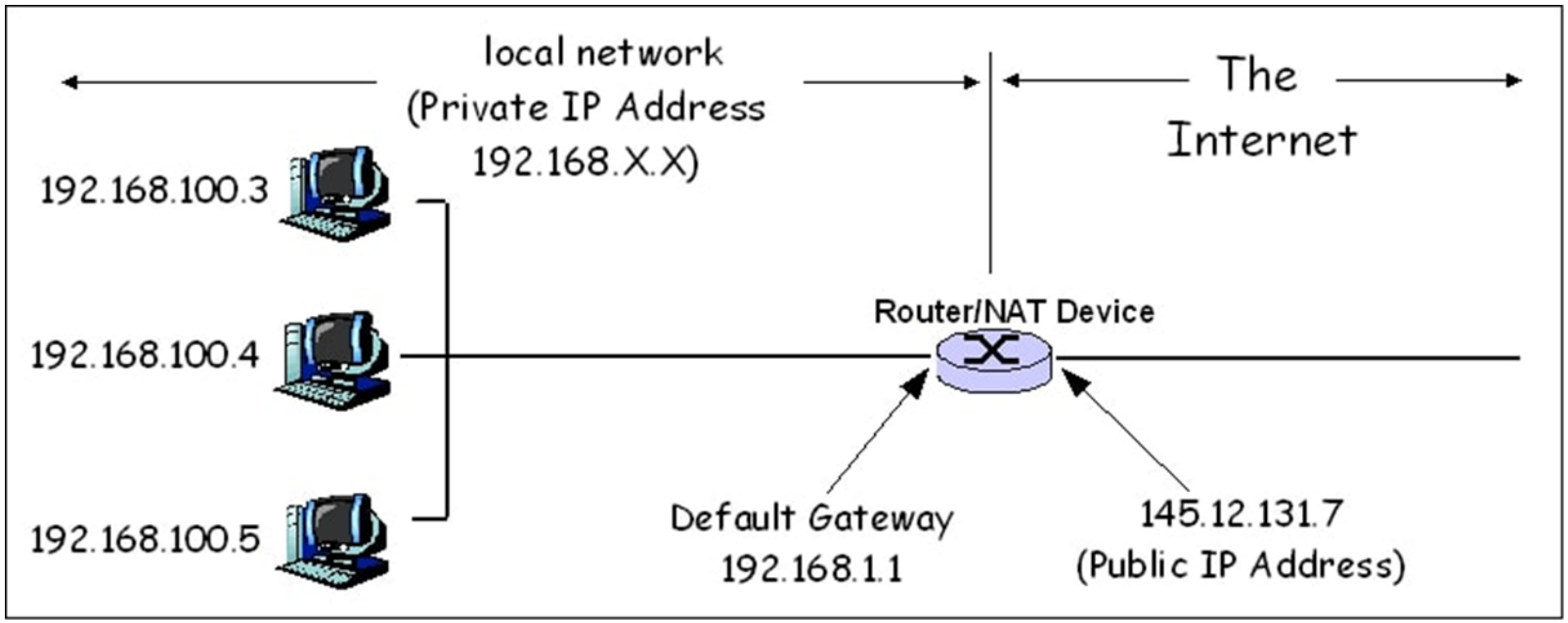


*

- Not enough IP addresses for every host in organization
- Security
  - Don't want every machine in organization known to outside world
  - Want to control or monitor traffic in / out of organization

*https://www.comparitech.com/blog/vpn-privacy/nat-firewall/

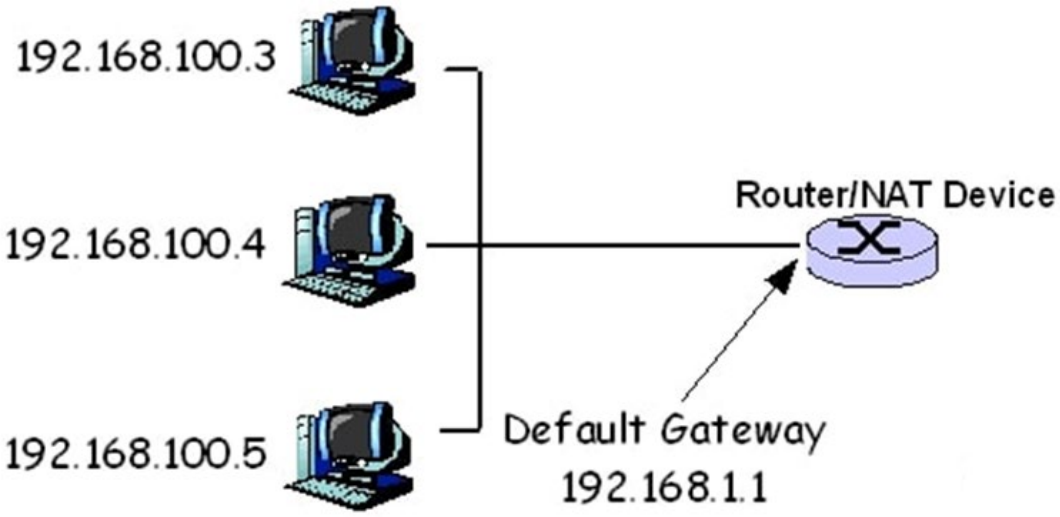
Reducing IP Addresses



- Most machines within organization are used by individuals
  - For most applications, they act as clients
- Small number of machines act as servers for entire organization
  - E.g., mail server, web, …
  - All traffic to outside passes through firewall

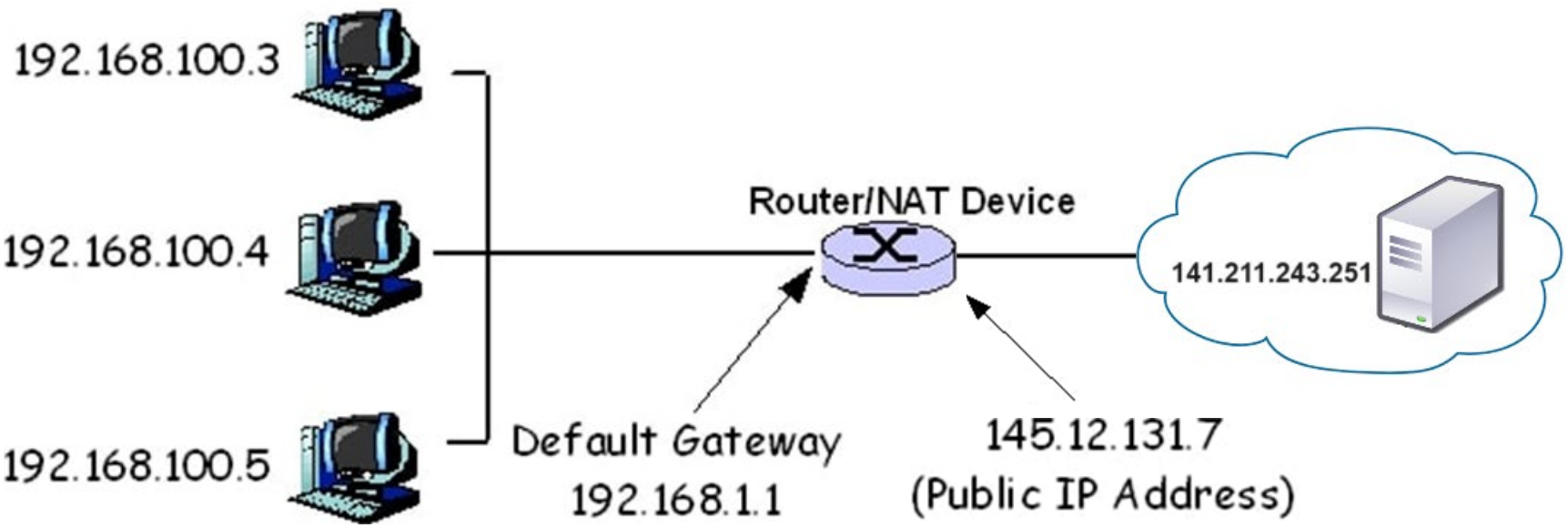
(Most) machines within organization do not need public IP addresses!

Network Address Translation



- Within Organization
  - Assign every host an unregistered IP address
    - IP addresses 10/8 & 192.168/16 unassigned
  - Route within organization by IP protocol, can do subnetting, …
- Firewall/NAT
  - Does not let any packets from internal nodes escape
  - Outside world does not need to know about internal addresses

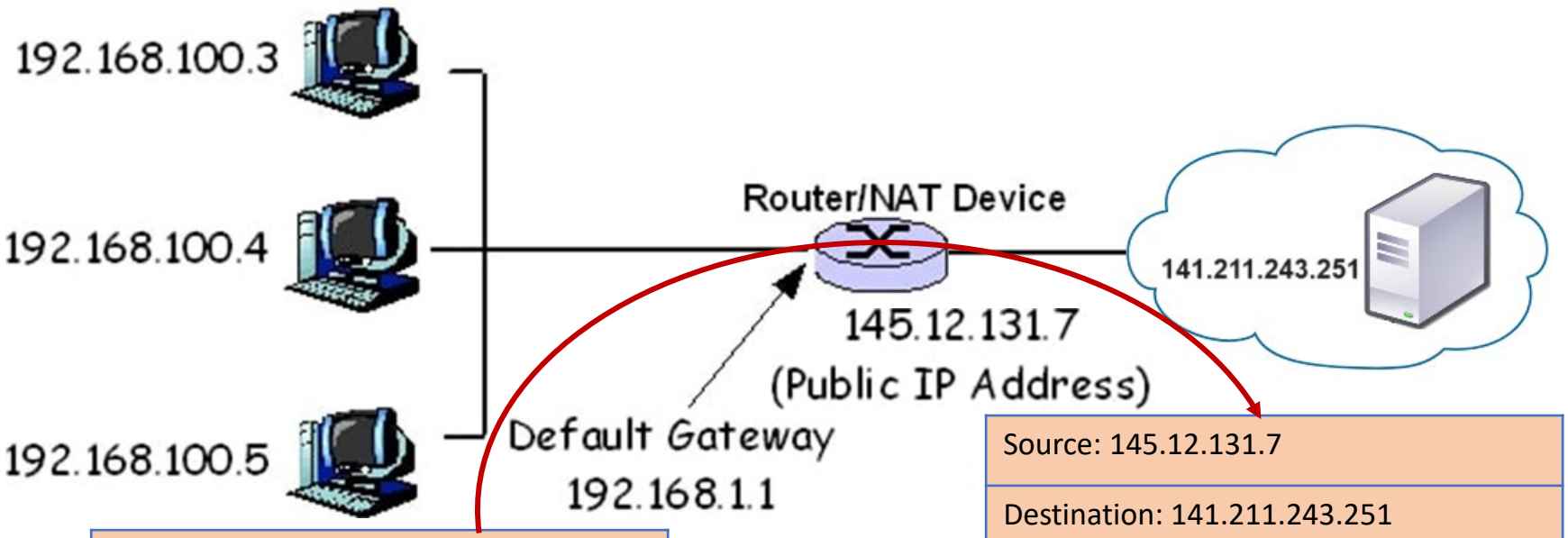
NAT: Opening Client Connection



- Client 192.168.100.5 wants to connect to server 141.211.243.251:80
  - OS assigns ephemeral port (1000)
- Connection request intercepted by firewall
  - Maps client to port of firewall (5000)
  - Creates NAT table entry

Internal Address	Internal Port	NAT Port
192.168.100.5	1000	5000

NAT: Client Request



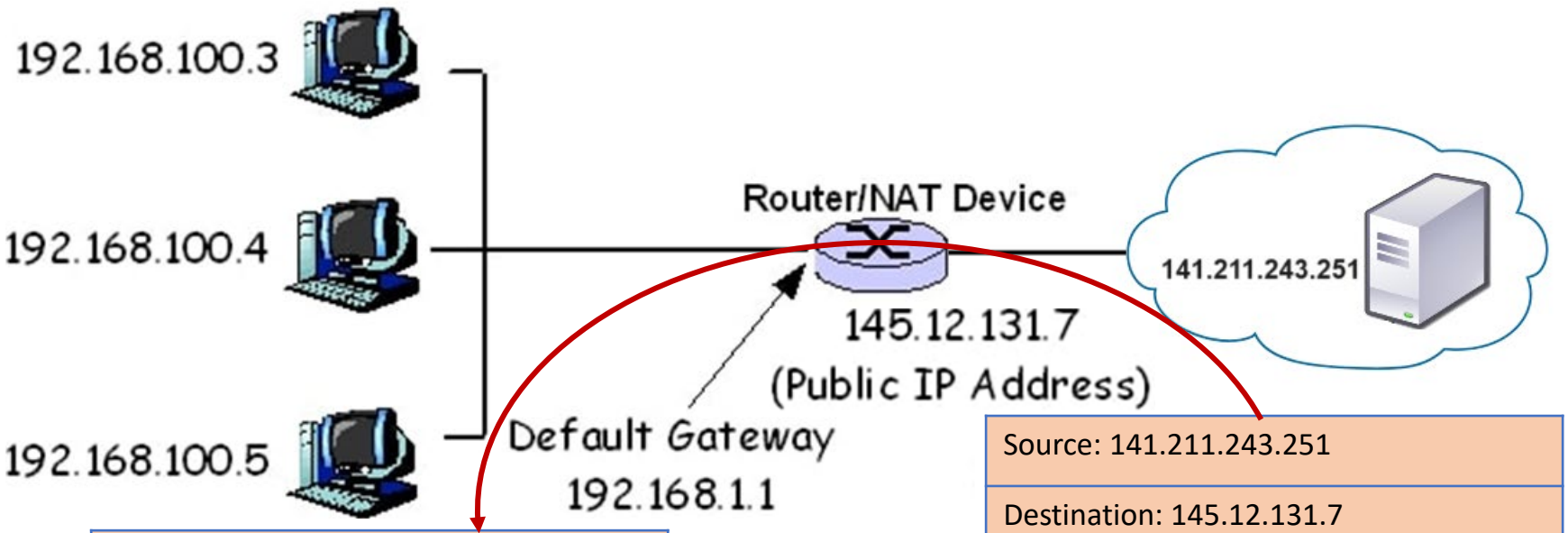
Source: 192.168.100.5
Destination: 141.211.243.251
Source Port: 1000
Destination Port: 80

Source: 145.12.131.7
Destination: 141.211.243.251
Source Port: 5000
Destination Port: 80

Internal Address	Internal Port	NAT Port
192.168.100.5	1000	5000

- Firewall acts as proxy for client
  - Intercepts message from client and marks itself as sender

NAT: Server Response



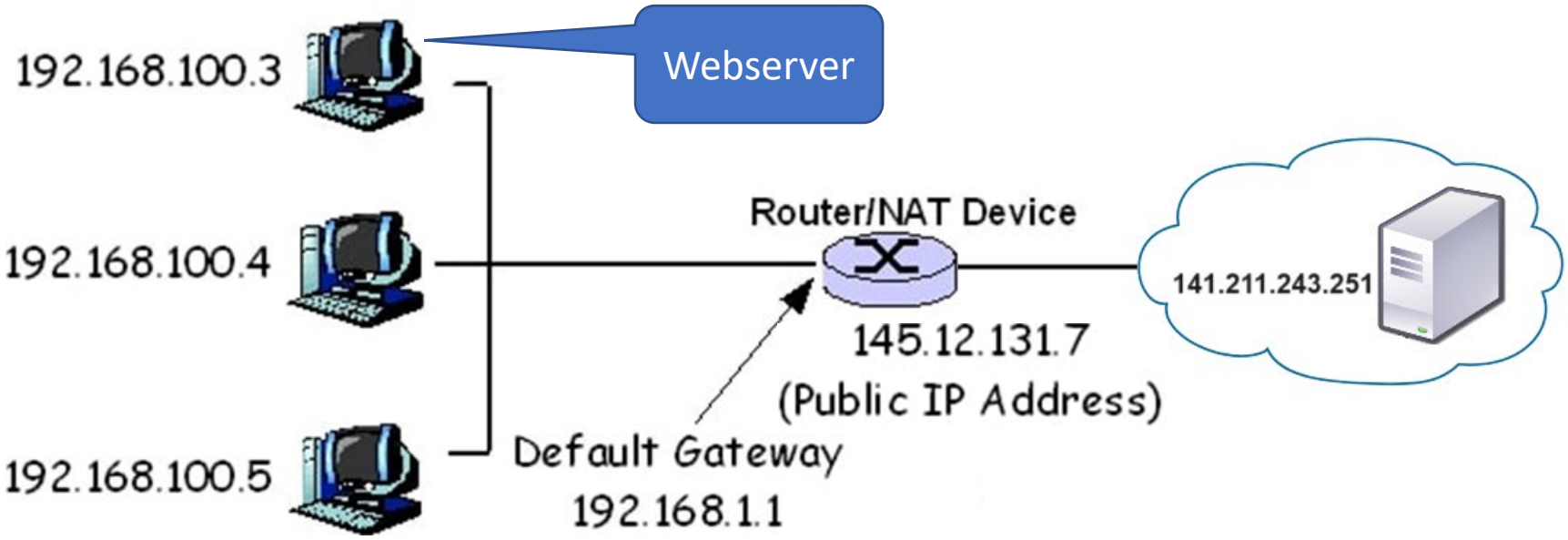
Source: 141.211.243.251
Destination: 192.168.100.5
Source Port: 80
Destination Port: 1000

Source: 141.211.243.251
Destination: 145.12.131.7
Source Port: 80
Destination Port: 5000

Internal Address	Internal Port	NAT Port
192.168.100.5	1000	5000

- Firewall acts as proxy for client
  - Acts as destination for server messages
  - Relabels destination to local addresses

NAT: Enabling Servers



Internal Address	Internal Port	NAT Port
192.168.100.3	80	80

- Port Mapping
  - Manually configure NAT table to include entry for well-known port
  - External users give address 145.12.131.7:80
  - Requests forwarded to server

NAT – Pros and Cons

- Advantages:
  - Hides IP addresses used in internal network
    - Easy to change ISP: only NAT box needs to have IP address
    - Fewer registered IP addresses required
  - Basic protection against remote attack
    - Does not expose internal structure to outside world
    - Can control what packets come in and out of system
    - Can reliably determine whether packet from inside or outside Disadvantages
- Disadvantages
  - Contrary to the “open addressing” scheme envisioned for IP Addressing
  - Hard to support peer-to-peer applications.
    Peer-peer apps, multi-player games have problems –
    who is the server?

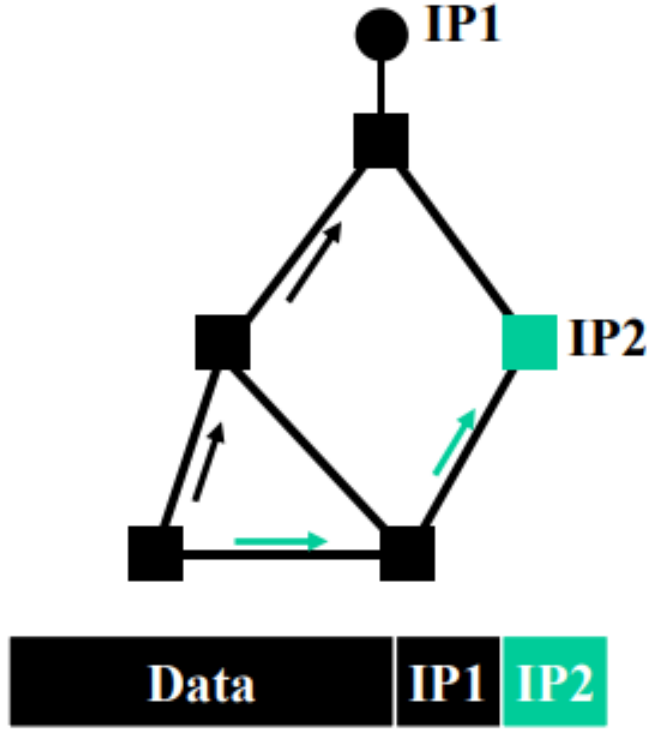
Tunneling

Motivation

- There are many cases where not all routers have the same features or consistent state
- An experimental IP feature is only selectively deployed - how do we use this feature e-e?
- A few are using a protocol other than IPv4 how can they communicate?
  - E.g., incremental deployment of IPv6
- I am traveling with a UMich laptop -
  how can I can I keep my UMich IP address?
  E.g., must have UMich address to use services

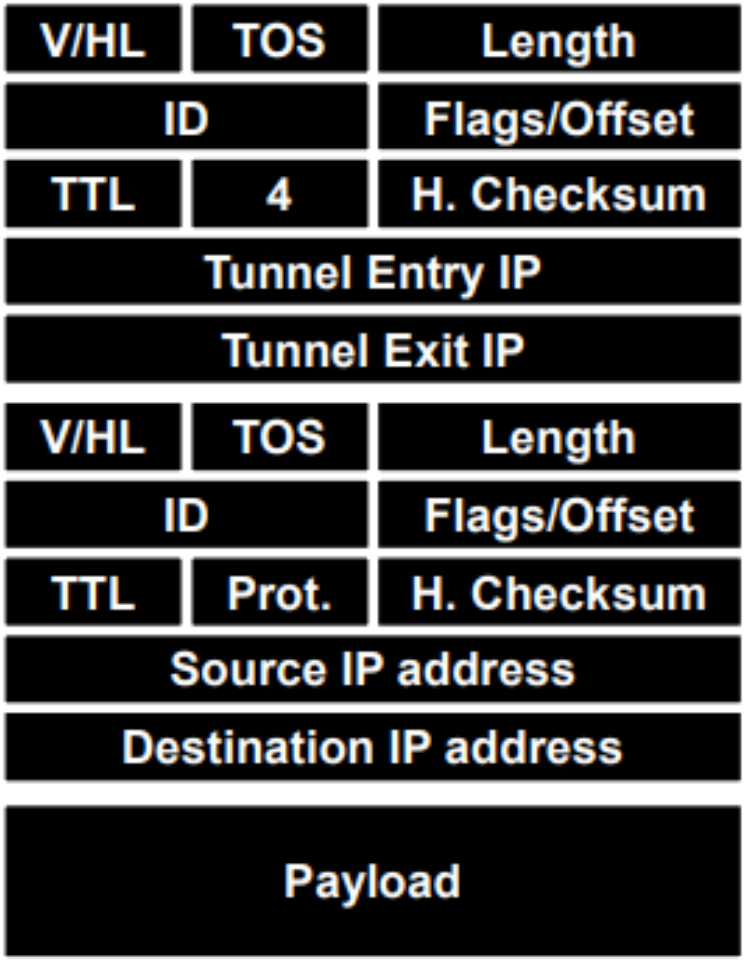
Tunneling

- Force a packet to go to a specific point in the network.
  - Path taken is different from the regular routing
- Achieved by adding an extra IP header to the packet with a new destination address.
  - Similar to putting a letter in another envelope
  - preferable to using IP source routing option
- Used increasingly to deal with special routing requirements or new features.
  - Mobile IP,
  - Multicast, IPv6, research, ..

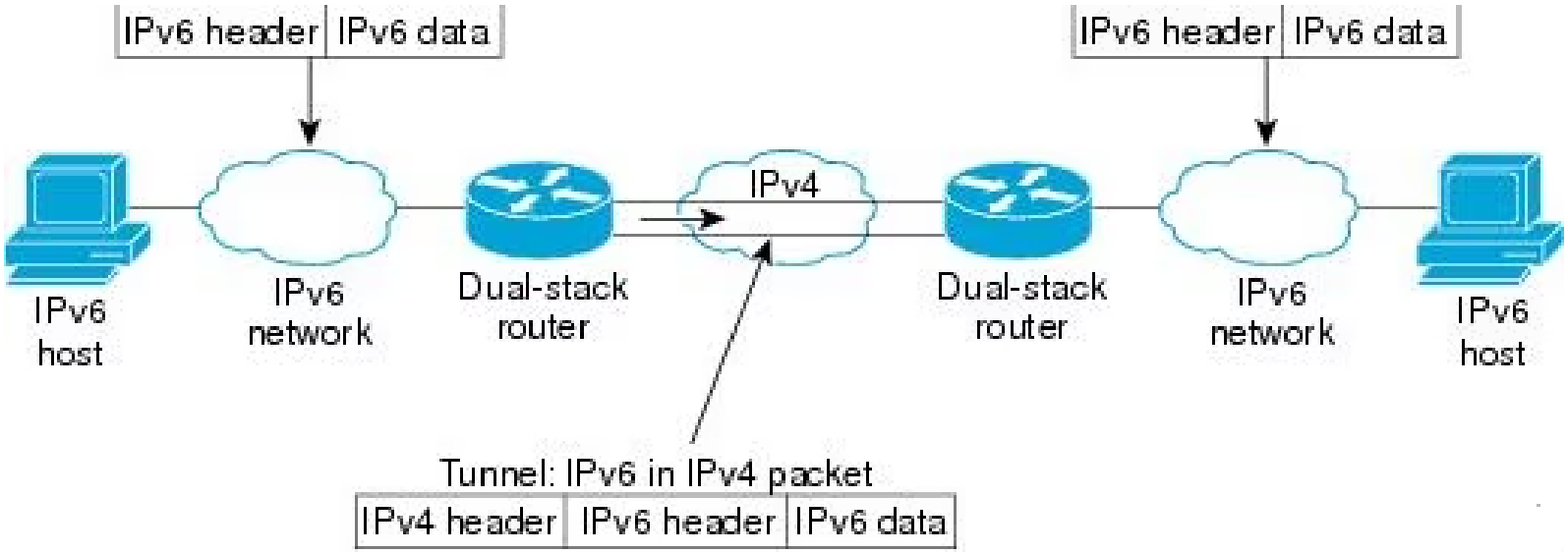


IP-in-IP Tunneling

- Described in RFC 1993.
- IP source and destination address identify tunnel endpoints.
- Protocol id = 4.
  - IP
- Several fields are copies of the inner-IP header.
  - TOS, some flags, ..
- Inner header is not modified, except for decrementing TTL.



Tunneling Example



https://www.cisco.com/c/en/us/td/docs/ios/12_4/interface/configuration/guide/inb_tun.html

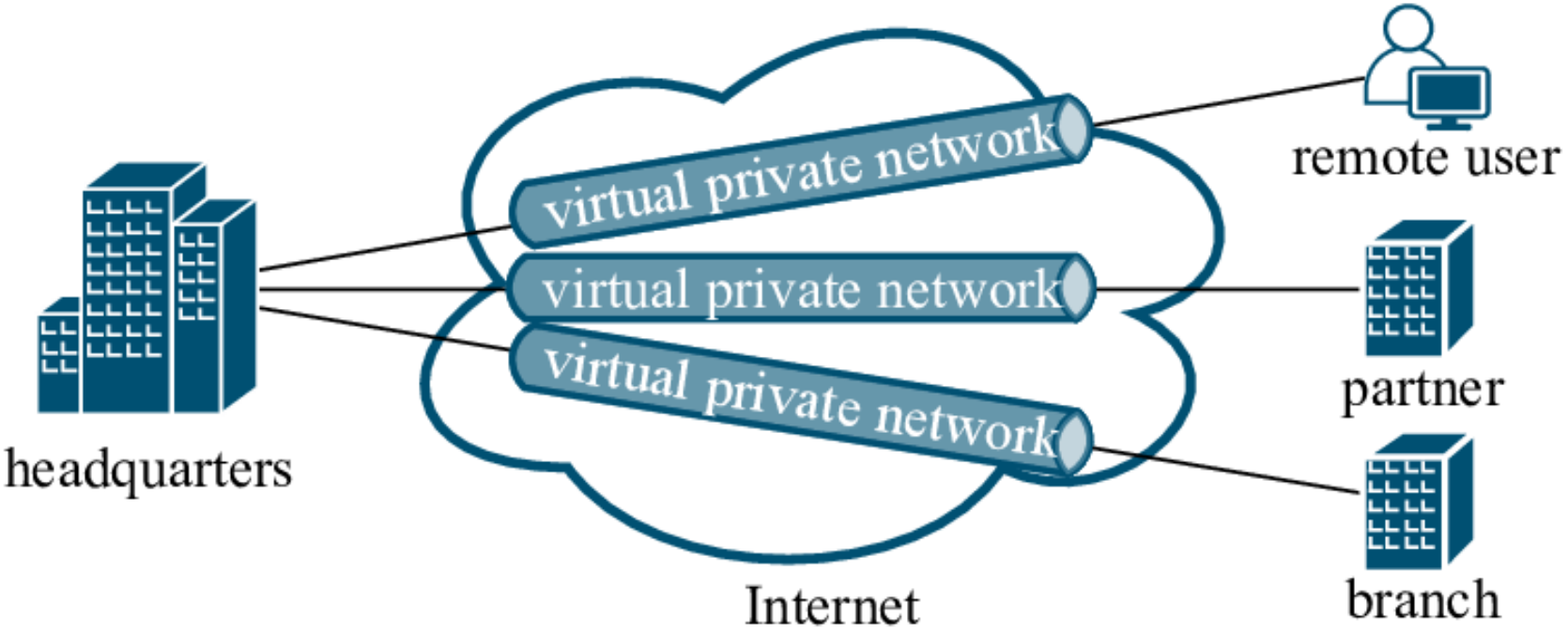
Tunneling Applications

- Virtual private networks.
  - Connect subnets of a corporation using IP tunnels
  - Often combined with IP Sec
- Support for new or unusual protocols.
  - Routers that support the protocols use tunnels to “bypass” routers that do not support it
  - E.g. multicast, IPv6
- Force packets to follow non-standard routes.
  - Routing is based on outer-header
  - E.g. mobile IP

Virtual Private Networks through Tunneling

- Concept
  - Appears as if two hosts connected directly
- Usage in VPN
  - Create tunnel between client & firewall
  - Remote client appears to have direct connection to internal network

VPN Example



Zorello, Ligia & Troia, Sebastian & Giannotti, Serena & Alvizu, Rodolfo & Bregni, Stefano & Maier, Guido. (2020).
On the Network Slicing for Enterprise Services with Hybrid SDN.
10.1109/LATINCOM50620.2020.9282318.