

Network Address Translation (NAT)

Jeffrey Shafer

Review: Private IPv4 Addressing

- Not routable on public internet
 - No chance of conflict with a valid public IP
- Why do I want private addresses?
 - Not every printer / fax machine / IPod / etc. needs to be publicly accessible from the Internet
 - Useful for local collections of computers not connected to internet

Name	IP address range	Number of IPs
24-bit block	10.0.0.0 – 10.255.255.255	16,777,216
20-bit block	172.16.0.0 – 172.31.255.255	1,048,576
16-bit block	192.168.0.0 – 192.168.255.255	65,536

Preview: TCP and UDP

- Two common protocols nested inside IP packets

TCP

- Reliability guaranteed
- Connection-based
 - Stream of data between two endpoints
 - Must explicitly open and close

UDP

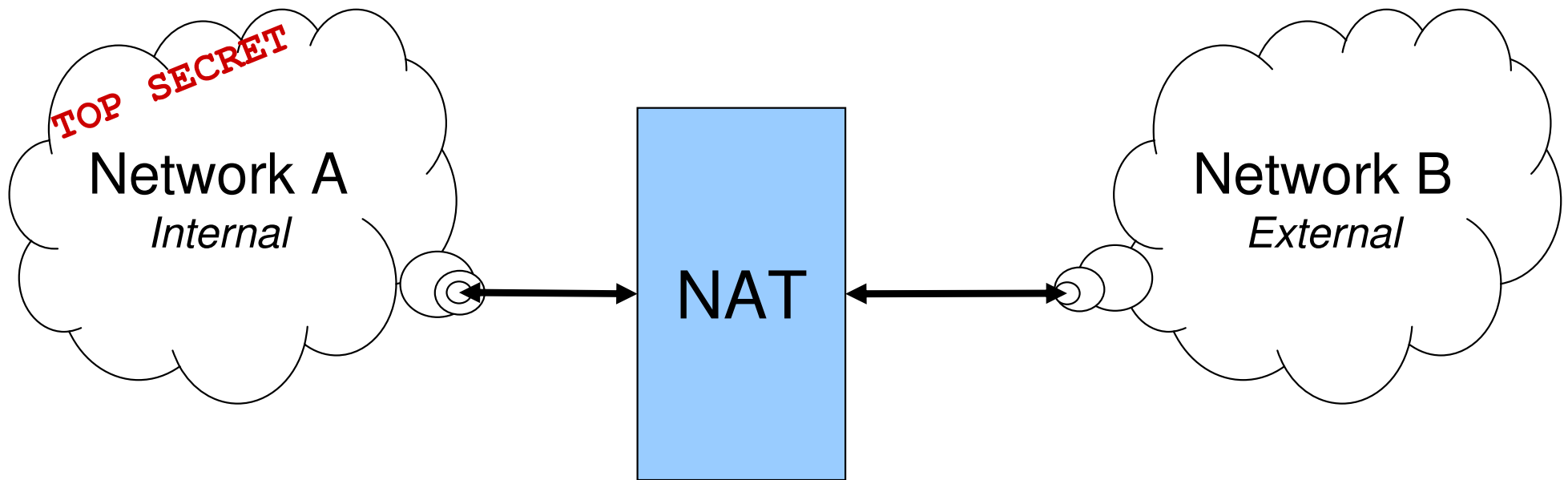
- Delivery not guaranteed
- No connections
 - Each packet is independent (like IP)

- Each protocol uses port numbers to distinguish between independent data streams

Network Address Translation

- Translate / route packets between one IP address space and another
 - Commonly translates from private IP range to public IP range (but the concept can be generalized to two public address ranges)
 - Accomplished by modifying packet header
 - Source address
 - Destination address
 - IP port number
 - IP / TCP / UDP checksums
- Not every NAT technique modifies every field!

Network Address Translation



■ Network A

- Multiple computers trying to access network B
- Don't want to reveal network A's structure to network B

■ Network B

- Traffic from network A appears with addresses in Network B's space
- May be mapped as single or multiple addresses

Is a NAT Device a Router?

- Internal and External networks are completely separate
 - MAC addresses are not propagated across NAT unit – just like a router!
- IP packets must be routed to NAT to reach external network
 - The NAT unit is often the final router on the internal network
- Most actual NAT devices contains a built-in 2-port router with a minimal set of routing capabilities
 - Table lookups
 - Modify packet headers
 - Recalculate checksums

Why Use Address Translation?

- Allows multiple hosts on private network to access public network through a single address
 - Overcomes policy problems (e.g. buying extra IPs from your ISP costs \$\$)
 - Overcomes IPv4 address shortages in developing world
- Disguises internal network structure
 - All requests appear to originate from NAT unit
 - Increases “security”
- Allows you to use entire 10.x.x.x private address space and remap to smaller public address range
 - Very convenient for clean network topology and simplified router forwarding tables

Types of Translation

- Terms are used interchangeably
- Network Address Translation (NAT)
 - Translates only the address fields, not ports
 - Every machine on network A gets a unique address on network B
- Port Address Translation (PAT)
 - Translates address and port numbers
 - Allows multiple machines on network A to share single IP address on network B
 - All requests appear to come from PAT unit

Network Address Translation Types

- One-to-One Mapping

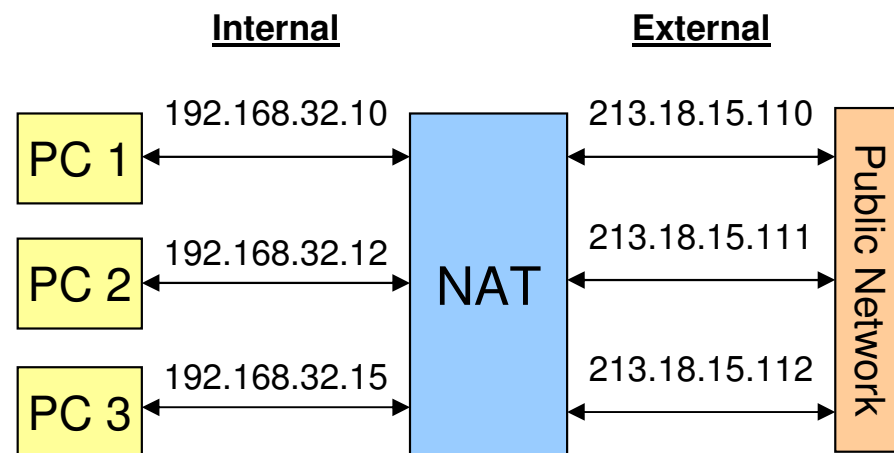
- Every internal IP gets a different external IP

- Static

- Internal IP is always mapped to same External IP

- Dynamic / Pooled

- Internal IP is mapped to random external IP

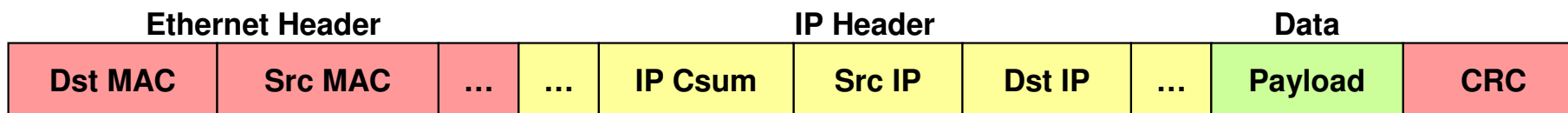
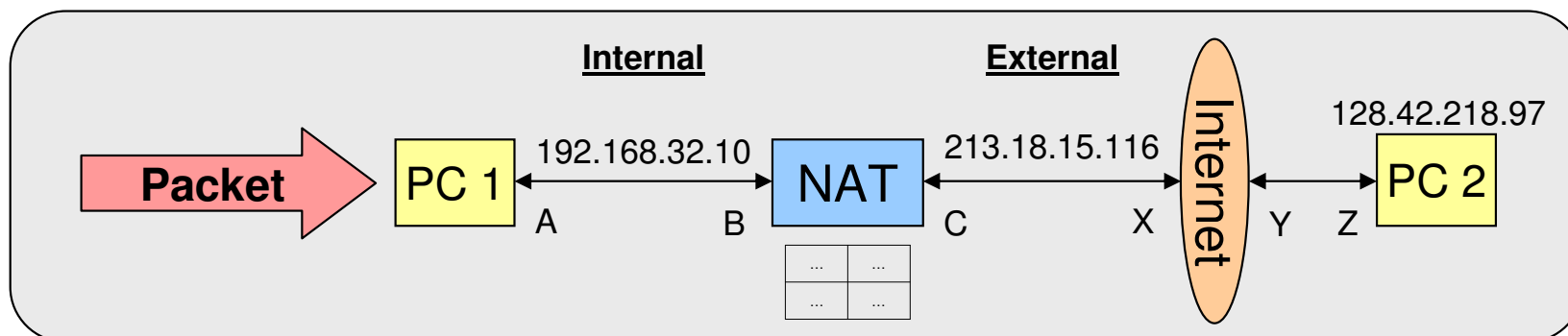


NAT Mapping Table: Static or Dynamic

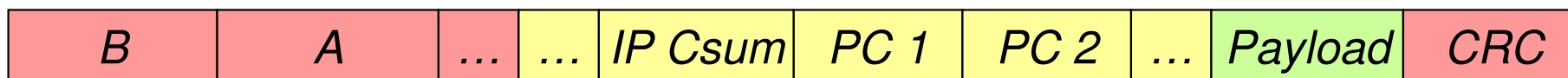
Internal IP	External IP
192.168.32.10	213.18.15.116
192.168.32.12	213.18.15.112
192.168.32.15	213.18.15.125
...	...

Not shown in Table: MAC Addresses!

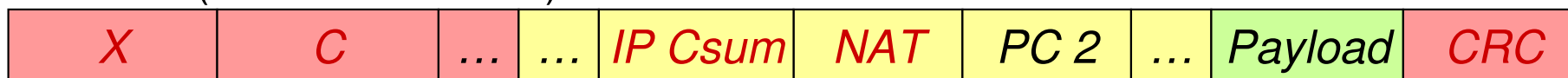
NAT Mechanics – Outbound Packet



Before NAT (internal network)

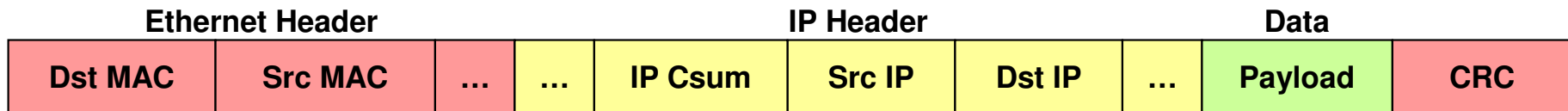
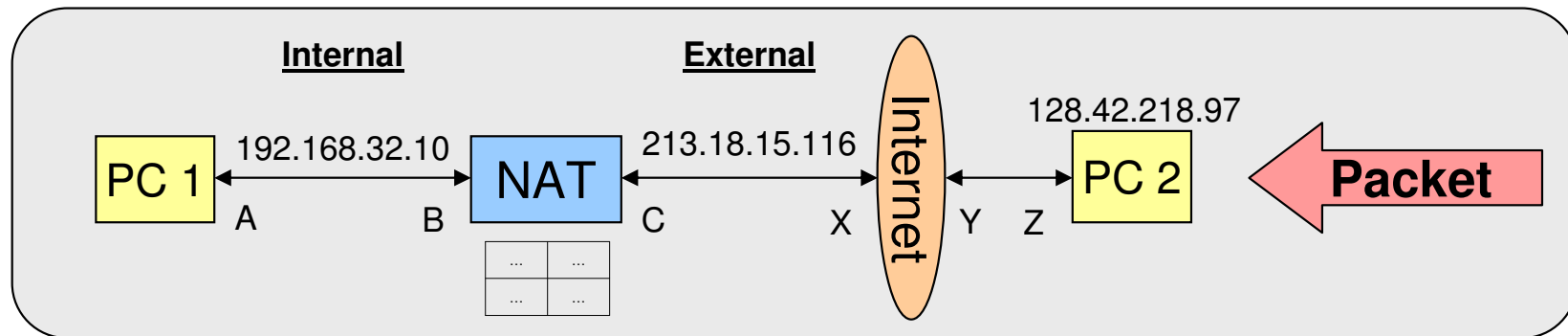


After NAT (external network)

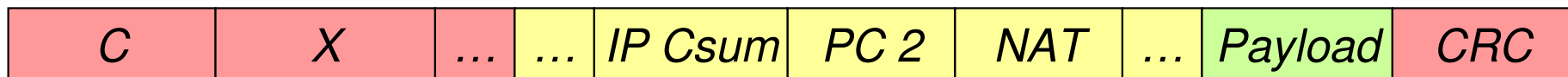


- Save internal IP and MAC to mapping table
- Recalculate checksums (Ethernet CRC, IP header, TCP/UDP/... headers)
- Replace source IP and MAC with NAT unit

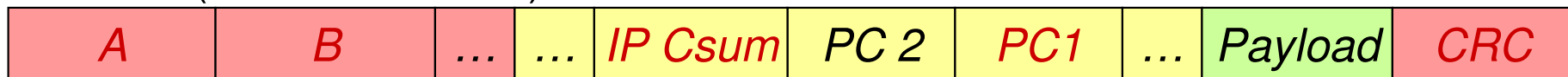
NAT Mechanics – Inbound Packet



Before NAT (external network)

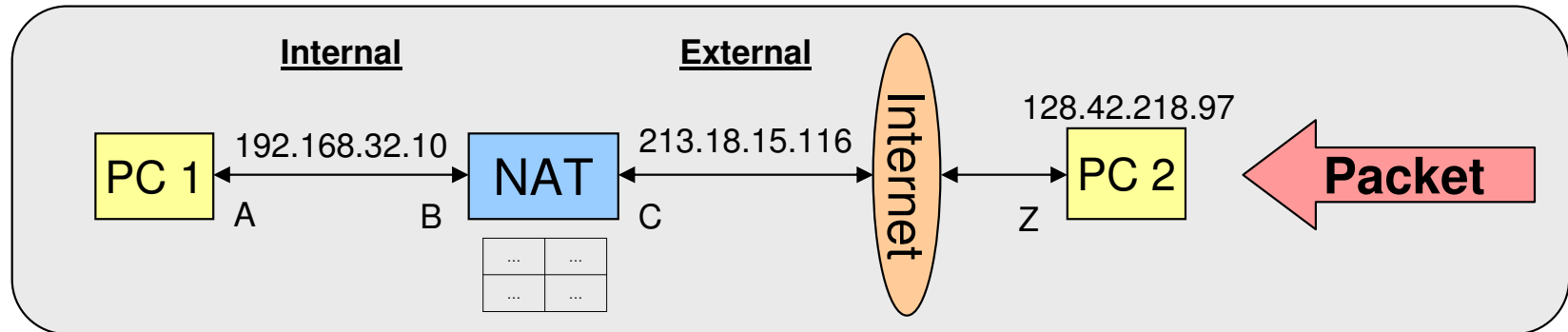


After NAT (internal network)



- Lookup Dst IP in mapping table. Only forward if match found
- Replace Dst IP and MAC with private address
- Update checksums (CRC, IP, TCP/UDP/...)

NAT Mechanics – Inbound Packet

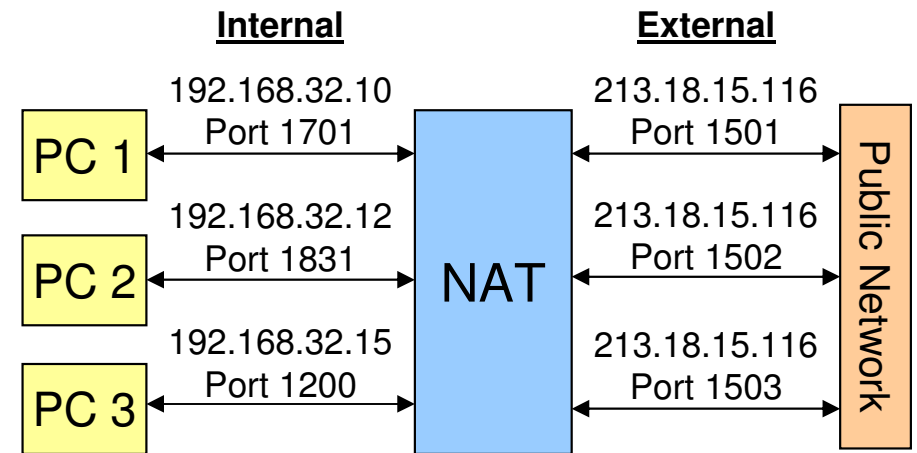


- What happens if a router sends a packet to the NAT unit, but no valid mapping exists for the destination IP?
 - Packet is dropped

Port Address Translation

■ IP Overloading

- Many internal IPs are mapped to one (or a few) external IPs
- TCP/UDP port number is also changed and used to identify unique connections between internal and external hosts
- Usually dynamic



NAT Mapping Table

Internal IP	Internal Port	External IP	External Port
192.168.32.10	1701	213.18.15.116	1501
192.168.32.12	1831	213.18.15.116	1502
192.168.32.15	1200	213.18.15.116	1503
...

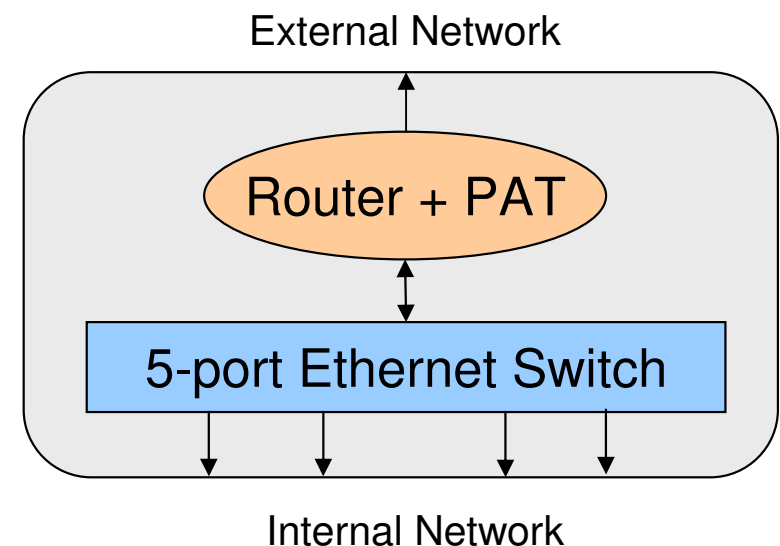
Not shown in Table: MAC Addresses!

Clearing Mappings

- When should a mapping be removed from a NAT?
 - Static NAT - Never?
 - Dynamic NAT - Only if the host is idle for a long time?
- When should a mapping be removed from a PAT?
 - TCP – Close of connection or reasonable timeout
 - Connection is framed by SYN and FIN packets
 - UDP – Unable to determine close of “connection”, so must use reasonable timeout instead

Home Broadband “Router”

- What is this device?
- Port Address Translation (PAT), plus a...
 - 4-port switch
 - Router
 - DHCP server
 - Wireless access point?
 - Stateful firewall?
 - Blinking LEDs?



NAT/PAT – Protocol Problems

- PAT Fails: Protocols that require incoming connections
 - Example: FTP Active Mode
 - Client sends request
 - Server attempts to open new connection back to client to send data
 - No entry in PAT table so connection is rejected
 - Example: SIP / RTP (VOIP telecommunication)

- NAT / PAT Fails: Protocols that carry IP address / port values in their payload
 - Example: IPsec (and other tunneling / VPN protocols)
 - NAT changes src/dst addresses in header but is unable to fix encrypted payload. Packet fails security check and is discarded because receiver detects (correctly) that the packet was altered in transit

- NAT / PAT Fails: Protocols that use checksums which include IP addresses
 - NAT only knows how to recalculate checksums for IP/TCP/UDP packets, not any new protocol that might be developed

Application-Level Gateway (ALG)

- Technique to avoid breaking common protocols
- NAT device runs multiple ALGs
 - Each ALG looks for a different protocol
 - Rewrites packet payload to fix problems
- Common ALG modules
 - FTP, BitTorrent, SIP, RTSP, File transfer in IM applications, etc...
- Not future proof
 - Each ALG is a fix for a specific protocol
 - Need to upgrade NAT software as new applications are developed

Severs and PAT

- Is there an simple way to enable servers to function behind a PAT?
- Administrator can insert static mappings into mapping tables
 - e.g. All incoming TCP requests on port 80 should always be forwarded to IP A.B.C.D, port 80 (enables a web server)
- Must be configured in advance
- Doesn't scale well
 - What if I have two web servers behind my PAT?
 - What if I don't know the incoming port #?

Severs and NAT

- Do I need to do anything to get my servers behind NAT to work?
 - No – IP address mapping is already one-to-one
 - A static mapping would be helpful for the clients...

NAT and Security

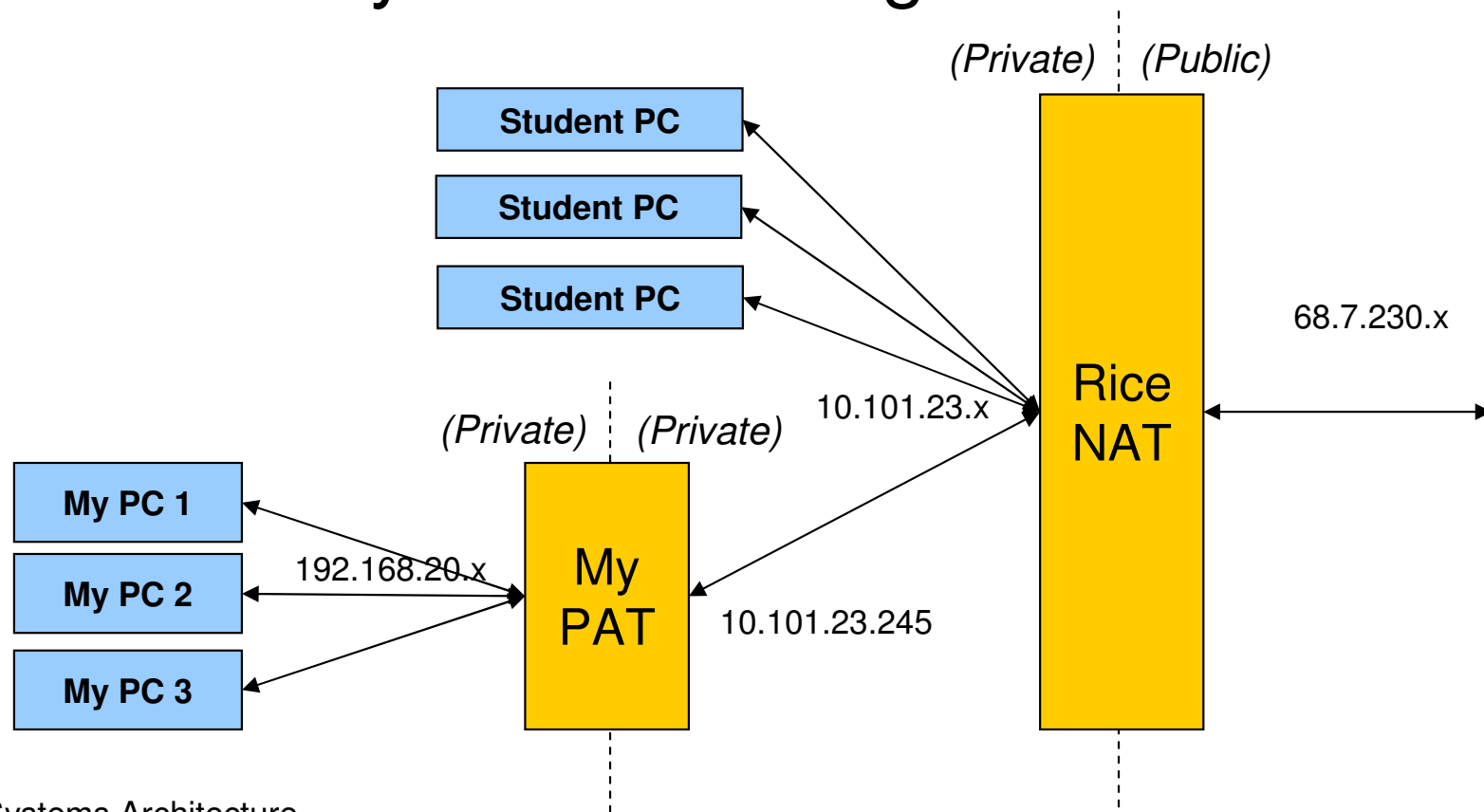
- NAT is often advertised as being essential for security
- Claim is mostly deceptive
 - Security through obscurity?
 - *“If evil hacker on public network can’t see me, I must be secure!”*
 - Computers on private network using PAT are hidden
 - Protects against worms scanning for exploits as long as there are no static mappings allowing outside access
 - If your parents have a simple PAT in front of their unpatched Windows box, they’re protected against some worms

NAT and Security

- Provides no protection against whole classes of malware
 - A security flaw in your PDF viewer can still be exploited by a bad download
 - The user can still do dangerous / stupid things (“Click on Angelina_Jolie.exe for free pictures!”)
- Limited protection on larger networks
 - Servers must be publicly accessible to perform their function (via fixed port or IP mapping)
 - If your IIS webserver or Linux server with remote SSH is unpatched, it is still vulnerable to worms
 - Once compromised, this machine provides entry vector to reach internal network, which may be completely unprotected!
- Don't let your guard down - Security in depth

Nesting IP Ranges via NAT

- Allowed to have multiple levels of NAT
 - Each level performs translation independently without any understanding of entire network



Future of NAT

- Is NAT still needed with IPv6? IPv6 has:
 - Much larger address range – No need for NAT to save IP addresses
 - No private IP address ranges
- Network architects want to remove NAT “hack” from new IPv6 networks
 - ALG support can be a nightmare!
- NAT can still be used with IPv6
 - Nothing about NAT requires that one of the address ranges be private

Affinity Group Connectivity Through Internal and External Firewalls v.06

