NATs are Evil

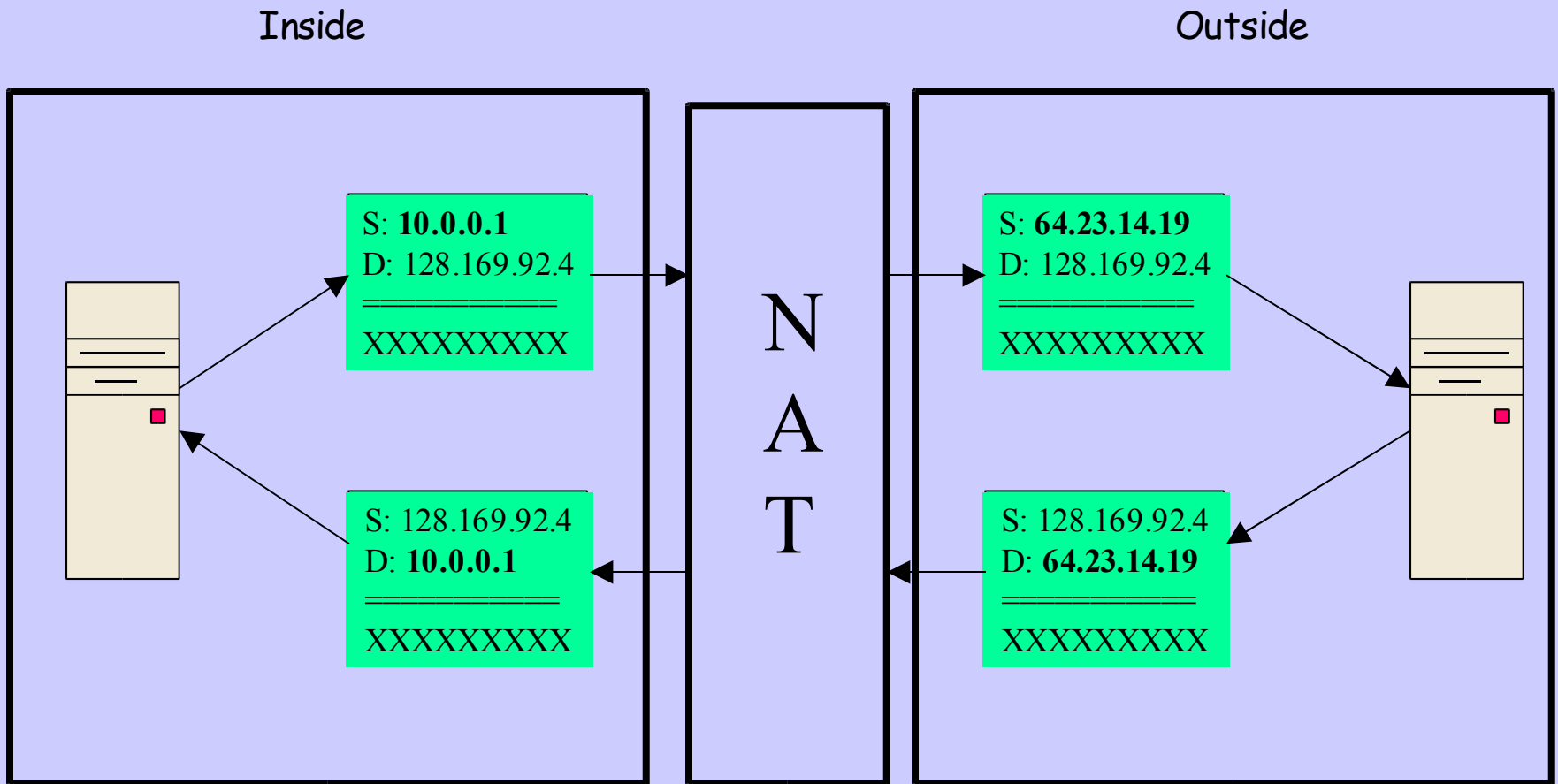# Well, Maybe just Bad for You

APNIC / Kuala Lampur
2004.02.26

Randy Bush <randy@iij.com>
Keith Moore <moore@cs.utk.edu>

What is a NAT?

- A NAT translates source or destination addresses in an IP packet

- May translate in one or multiple directions

- May connect private IP network to public Internet, or between private IP networks

- Domain and range of translation function may intersect

Example of a NAT

Inside

Outside

S: **10.0.0.1**
D: 128.169.92.4
═══════════
XXXXXXXXX

S: **64.23.14.19**
D: 128.169.92.4
═══════════
XXXXXXXXX

N
A
T

S: 128.169.92.4
D: **10.0.0.1**
═══════════
XXXXXXXXX

S: 128.169.92.4
D: **64.23.14.19**
═══════════
XXXXXXXXX

Copyright 2004, Randy Bush

Dynamic Assignment

- Each NAT maintains a table which maps addresses/ports from one address 'realm' to another

- Mappings are created when the NAT guesses they are needed

- Mappings are freed when the NAT guesses they are no longer needed

- Hosts behind a dynamic NAT get their addresses via DHCP

Application Layer Gateways

- Application-specific code embedded in a NAT

- May translate addresses within payload (not just header)

- May create/delete/reference translation entries

- Separate code required for each application

- NATs often provide ALGs for: FTP, DNS, SIP, RealAudio, H.323, SNMP

- New ALGs are continually needed

Where the Smarts Are

- Traditional Voice has stupid edge devices, phone instruments, and a very smart core

- The Internet has smart edges, computers with operating systems, applications, ..., and a simple stupid core, which just does packet forwarding

- Adding an entirely new Internet service is just a matter of distributing an application to a few consenting desktops (until NATs)

- Compare that to adding a service to Voice

If NATs Had Existed
No New End-to-End Services

- How long did it take telcos to deploy rotary dialing? Over a decade at massive expense!
- How long did it take the telcos to convert to TouchTone dialing? They're still doing it!
- E-mail was a service **added** to the ARPANET
- HTTP, I.e., "the web" would have taken a decade to deploy
- With NATs, tomorrow's killer application will be difficult to deploy
- Today's new applications are hard to deploy because they require ALGs

Problems Caused by NATs

- Break global addressability
- Break IP fragmentation
- Host-to-address bindings are not stable
- Increase difficulty in deploying new applications
- Degrade network reliability and scalability
- Make network management, fault detection and diagnosis more difficult
  (see www.cs.utk.edu/~moore/what-nats-break.html)

Security?

- There is a belief that NATs provide security

- Does changing my name badge stop a mugger?

- Have NATs slowed email viruses and worms? No.

- Have NATs slowed DDoS attacks? No.

- They just happen to be associated with Firewalls.

So, Why so Many NATs?

- <u>False</u> perception that RIRs will not give an LIR needed/justified space

- Difficulty of a large ISP (cable, DSL, …) to do customer-by-customer need-based allocation

- Techno-colonialist Carrier ISPs not allocating or routing reasonable allocations to developing economies

Un-NATting

- So you have a NATted network
- What can you do?
- Design actual address space need if the NATs were not there
- Contact your RIR/NIR with these data and a plan, as justification for a un-NATted portable IP allocation
- Give your customers real addresses!