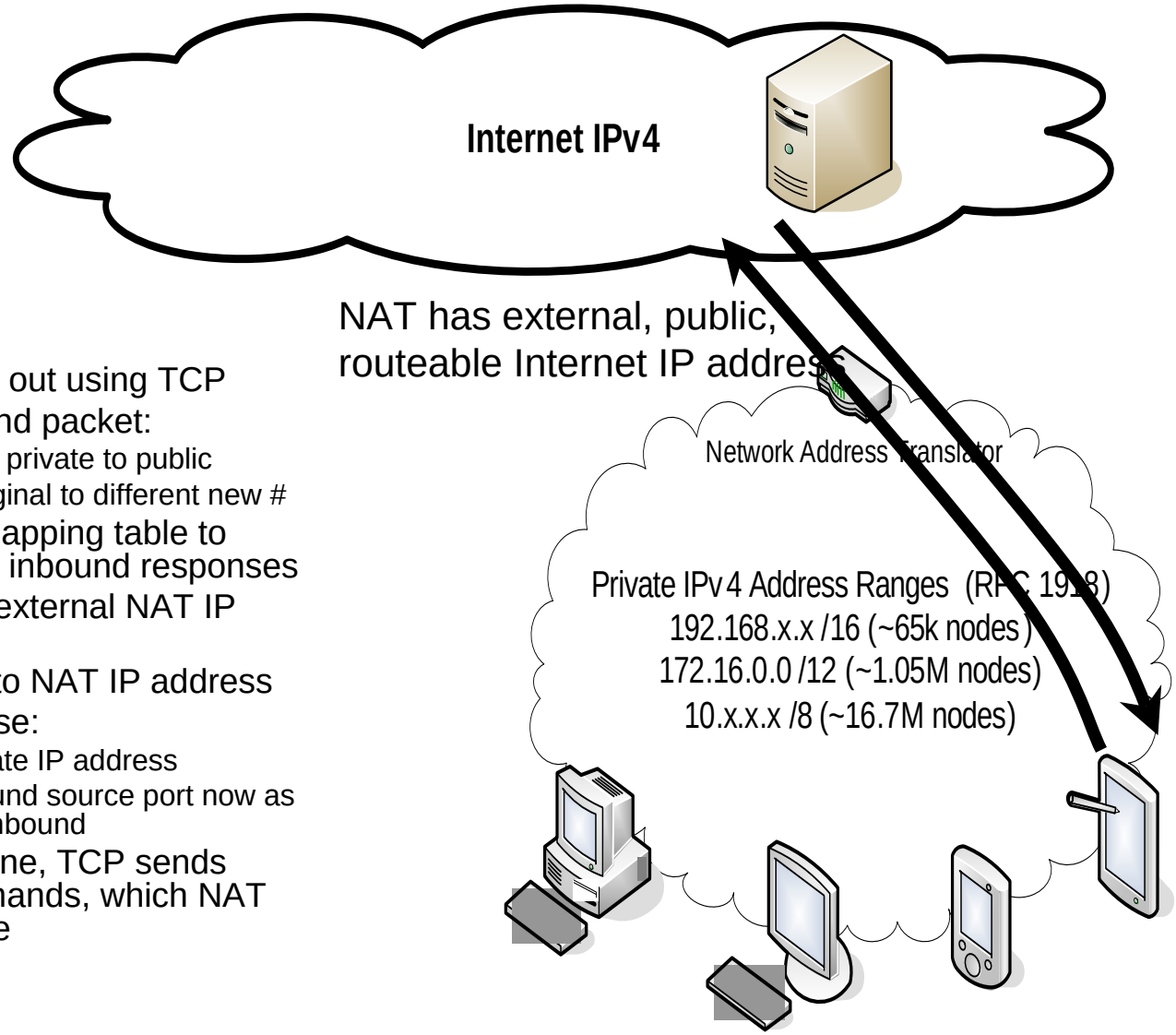
Why IPv6 is necessary for new communication scenarios

Tony Hain – Cisco
William Dixon – V6 Security

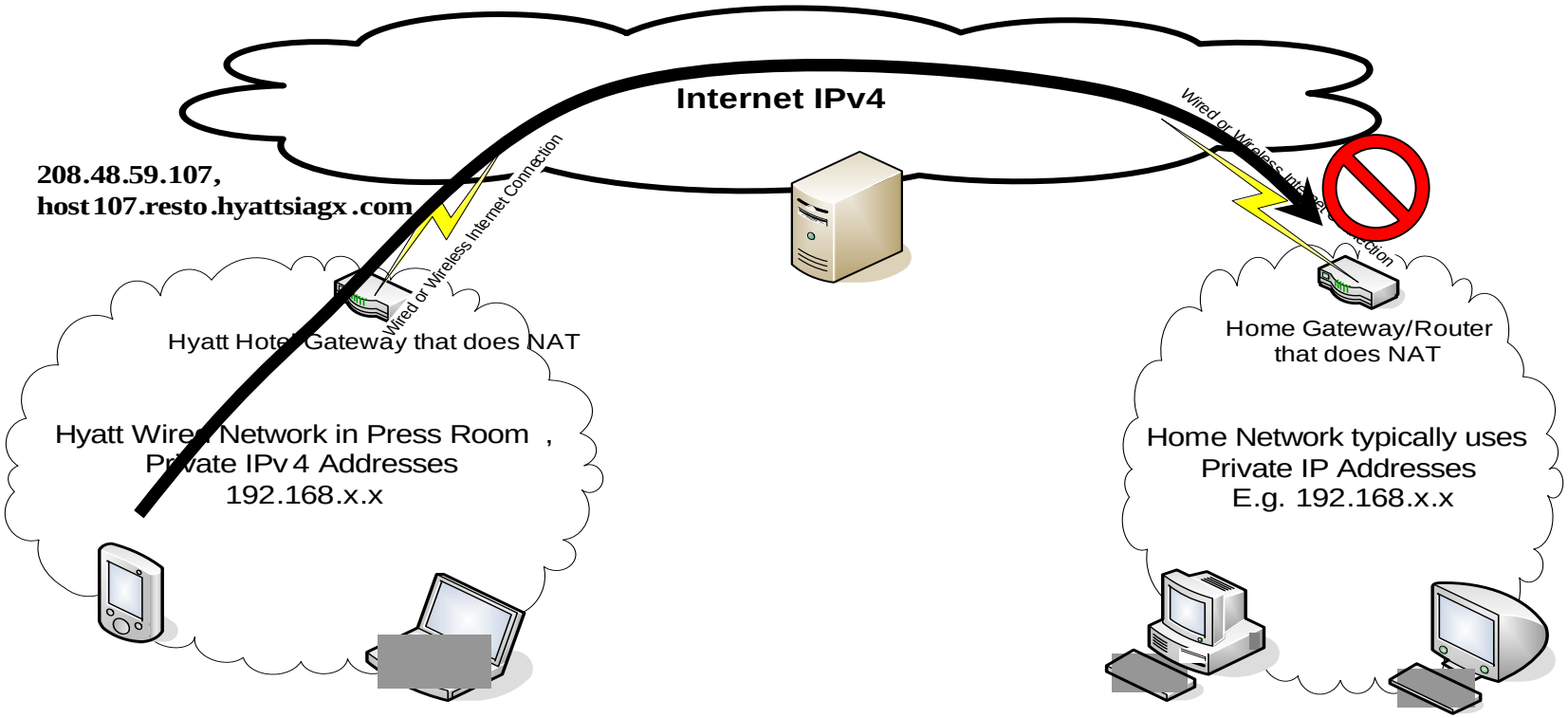
For IPv6 Coalition Summit
Reston, VA May 26, 2005

How IPv4 NAT Works



- Internal node connects out using TCP
- NAT translates outbound packet:
  - source address from private to public
  - Source port from original to different new #
- NAT creates state in mapping table to process corresponding inbound responses
- Internet server sees 1 external NAT IP address only
- Server TCP responds to NAT IP address
- NAT translates response:
  - to internal node private IP address
  - Using original outbound source port now as destination port for inbound
- When connection is done, TCP sends “finish” or “reset” commands, which NAT sees, so it deletes state

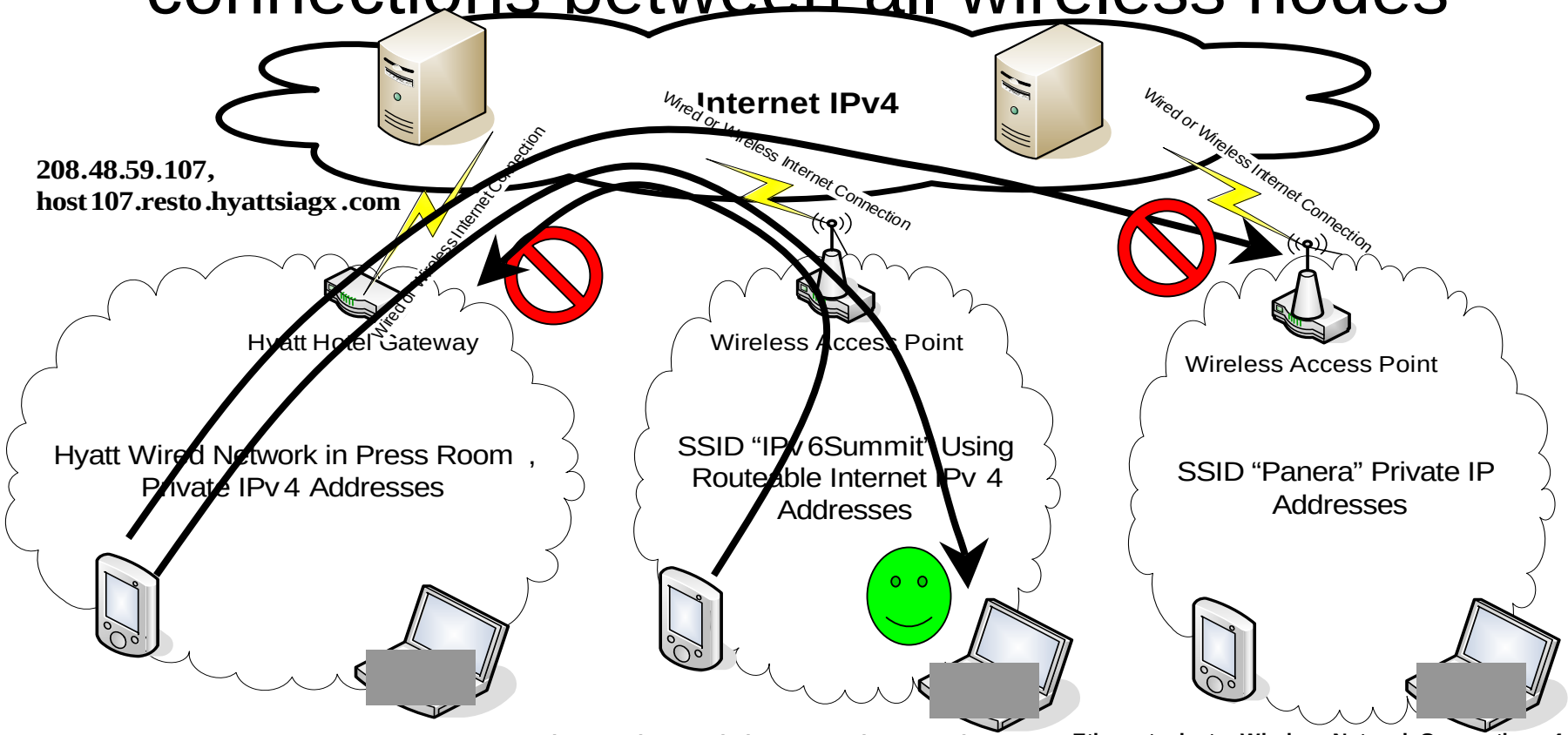
Inbound Connections Through NAT Not possible without admin configuration



Ethernet adapter Local Area Connection :
Connection-specific DNS Suffix . :
Description . . . . . : 3Com 3C920 Integrated Fast Ethernet Controller (3C905C-TX Compatible)

IP Address. . . . . : 192.168.1.2
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
DHCP Server . . . . . : 192.168.1.1
DNS Servers . . . . . : 192.168.1.1

The IPv6 conference network doesn't allow connections between all wireless nodes



Ethernet adapter Local Area Connection :

Connection-specific DNS Suffix . :
Description . . . . . : 3Com 3C920 Integrated Fast Ethernet Controller (3C905C-TX Compatible)

IP Address. . . . . : 192.168.1.2
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
DHCP Server . . . . . : 192.168.1.1
DNS Servers . . . . . : 192.168.1.1

Ethernet adapter Wireless Network Connection 4:

Connection-specific DNS Suffix . : jfk.gblx.com
Description . . . . . : Belkin 802.11g Network Adapter

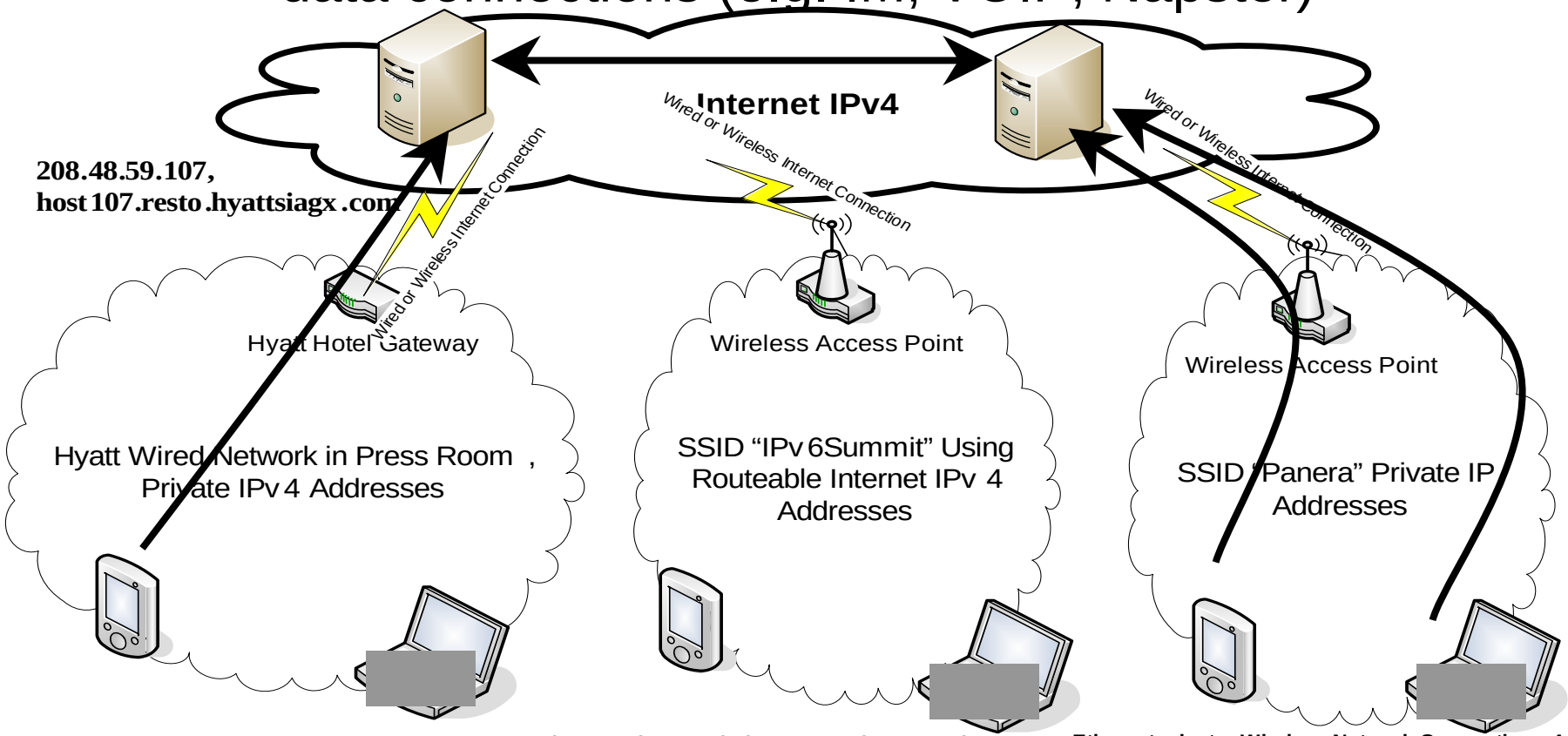
IP Address. . . . . : 208.48.182.55
Subnet Mask . . . . . : 255.255.254.0
Default Gateway . . . . . : 208.48.182.1
DHCP Server . . . . . : 10.20.20.2
DNS Servers . . . . . : 64.212.106.84
64.212.106.85

Ethernet adapter Wireless Network Connection 4:

Connection-specific DNS Suffix . : savvis.net
Description . . . . . : Belkin 802.11g Network Adapter

IP Address. . . . . : 10.0.50.77
Subnet Mask . . . . . : 255.255.255.0
IP Address. . . . . : fe80::211:50ff:fe35:8482%7
Default Gateway . . . . . : 10.0.50.4
DHCP Server . . . . . : 10.0.50.4
DNS Servers . . . . . : 209.144.50.113
209.144.50.125

Peer to Peer applications required to build rendezvous and proxy architecture for IPv4 peer discovery and relaying data connections (e.g. IM, VOIP, Napster)



Ethernet adapter Local Area Connection :

Connection-specific DNS Suffix . :
Description . . . . . : 3Com 3C920 Integrated Fast Ethernet Controller (3C905C-TX Compatible)

IP Address. . . . . : 192.168.1.2
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
DHCP Server . . . . . : 192.168.1.1
DNS Servers . . . . . : 192.168.1.1

Ethernet adapter Wireless Network Connection 4:

Connection-specific DNS Suffix . : jfk.gblx.com
Description . . . . . : Belkin 802.11g Network Adapter

IP Address. . . . . : 208.48.182.55
Subnet Mask . . . . . : 255.255.254.0
Default Gateway . . . . . : 208.48.182.1
DHCP Server . . . . . : 10.20.20.2
DNS Servers . . . . . : 64.212.106.84
64.212.106.85

Ethernet adapter Wireless Network Connection 4:

Connection-specific DNS Suffix . : savvis.net
Description . . . . . : Belkin 802.11g Network Adapter

IP Address. . . . . : 10.0.50.77
Subnet Mask . . . . . : 255.255.255.0
IP Address. . . . . : fe80::211:50ff:fe35:8482%7
Default Gateway . . . . . : 10.0.50.4
DHCP Server . . . . . : 10.0.50.4
DNS Servers . . . . . : 209.144.50.113
209.144.50.125

IPv6 Enables Direct Connectivity

- Every node has a global routeable address
- Local Link Neighbor (Peer) Discovery
- Inbound connections possible if firewalls allow
- Remote peer address discovery provided by:
  - Home Agent fixed Home Address using Mobile IPv6
  - Static IP for non-mobile assets w/o Mobile IPv6
  - Dynamic DNS update with current IPv6 address, if allowed, enables name resolution to find current address
  - Still use rendezvous point for remote peer address discovery w/o Mobile IPv6 Home Agent

- AND end-to-end security standard with IPsec
  - Core protocols finalized defined ‘98, and recently improved
  - Work in progress to define scenarios like, “how does home gateway let only your family connect in ?”

IPv6 Network Architecture Protection

(draft-ietf-v6ops-nap-00.txt)

Brian Carpenter, Ralph Droms, Tony Hain, Eric L Klein, Gunter Van de Velde

Network Architecture Protection:

“A set of IPv6 techniques that may be combined on an IPv6 site to simplify and protect the integrity of its network architecture, without the need for Address Translation“

Market Perceived Benefits of NAT & the IPv6 alternatives

Function	*IPv4/NAT*	*IPv6*
Simple Gateway as default router and address pool manager	**DHCP – single address upstream** **DHCP – limited number of individual devices downstream**	**DHCP-PD – arbitrary length customer prefix upstream, SLAAC via RA downstream**
Simple Security	**Filtering due to lack of translation state**	**Context Based Access Control**
Local usage tracking	**NAT state table**	**Address uniqueness**
End system privacy	**NAT transforms device ID bits in the address**	**Temporary use privacy addresses**
Topology hiding	**NAT transforms subnet bits in the address**	**Untraceable addresses using IGP host routes /or MIPv6 tunnels for stationary devices**
Addressing Autonomy	**RFC 1918**	**RFC 3177 & ULA**
Global Address Pool Conservation	**RFC 1918**	**340,282,366,920,938,463,463,374,607,431,768,211,456 addresses**
Renumbering and Multi-homing	**Address translation at border**	**Preferred lifetime per prefix & Multiple addresses per interface**

IPv6 Gap Analysis

- Completion of work on ULAs
- Renumbering procedure
- How to completely hide subnet topology
- Multihoming
- Traceability issues