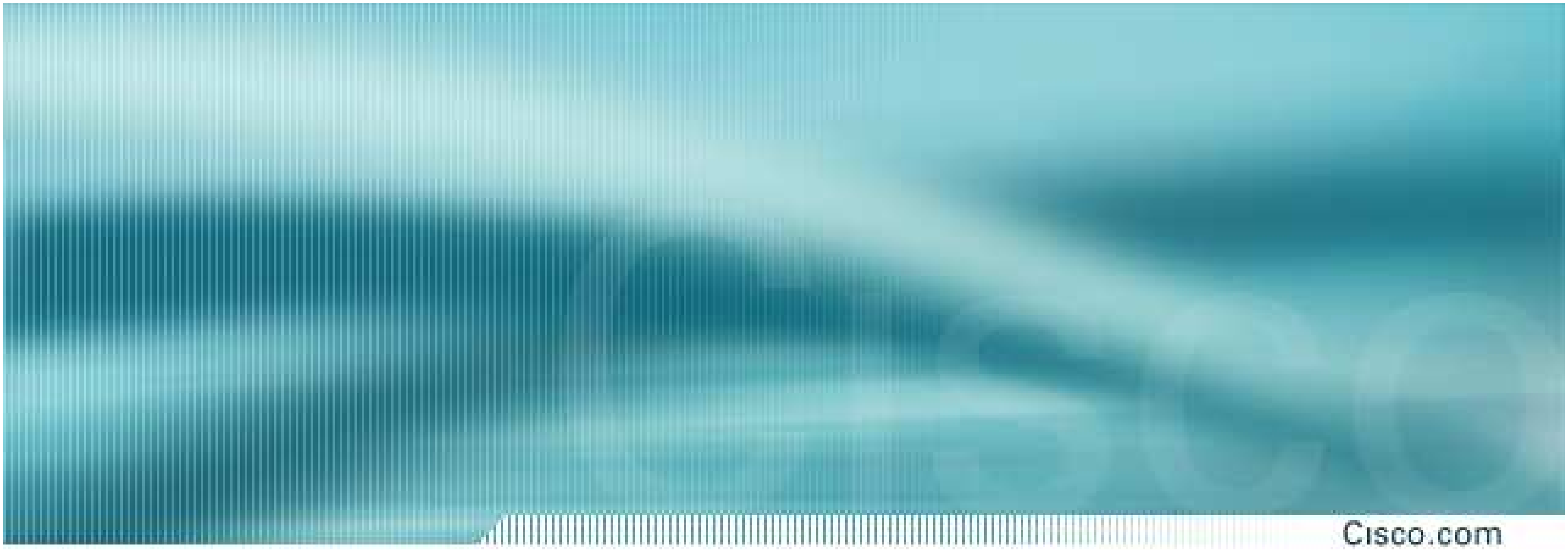
Cisco Systems



Network Architecture Protection

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

Gunter Van de Velde
Cisco Systems

(IETF Draft Editors: Brian Carpenter, Ralph Droms, Tony Hain, Eric L Klein, Gunter Van de Velde)

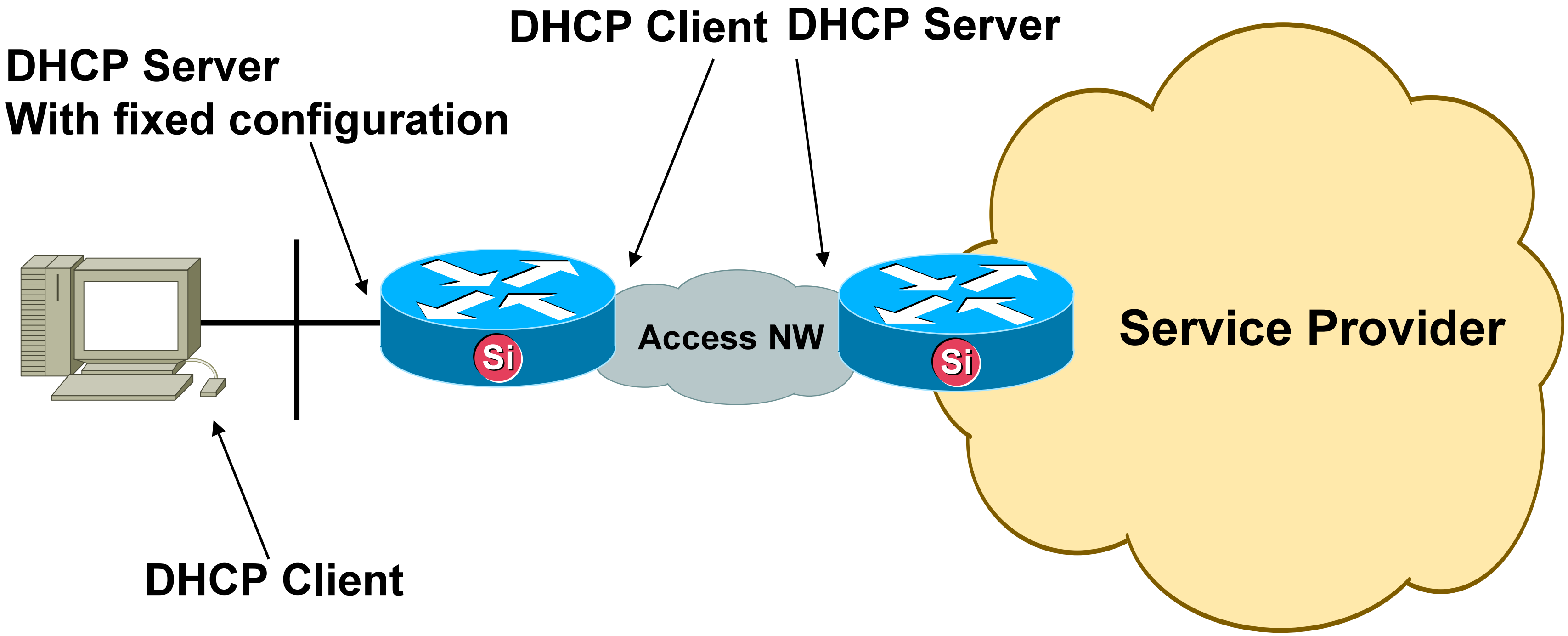
IPv6 Network Architecture Protection

"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

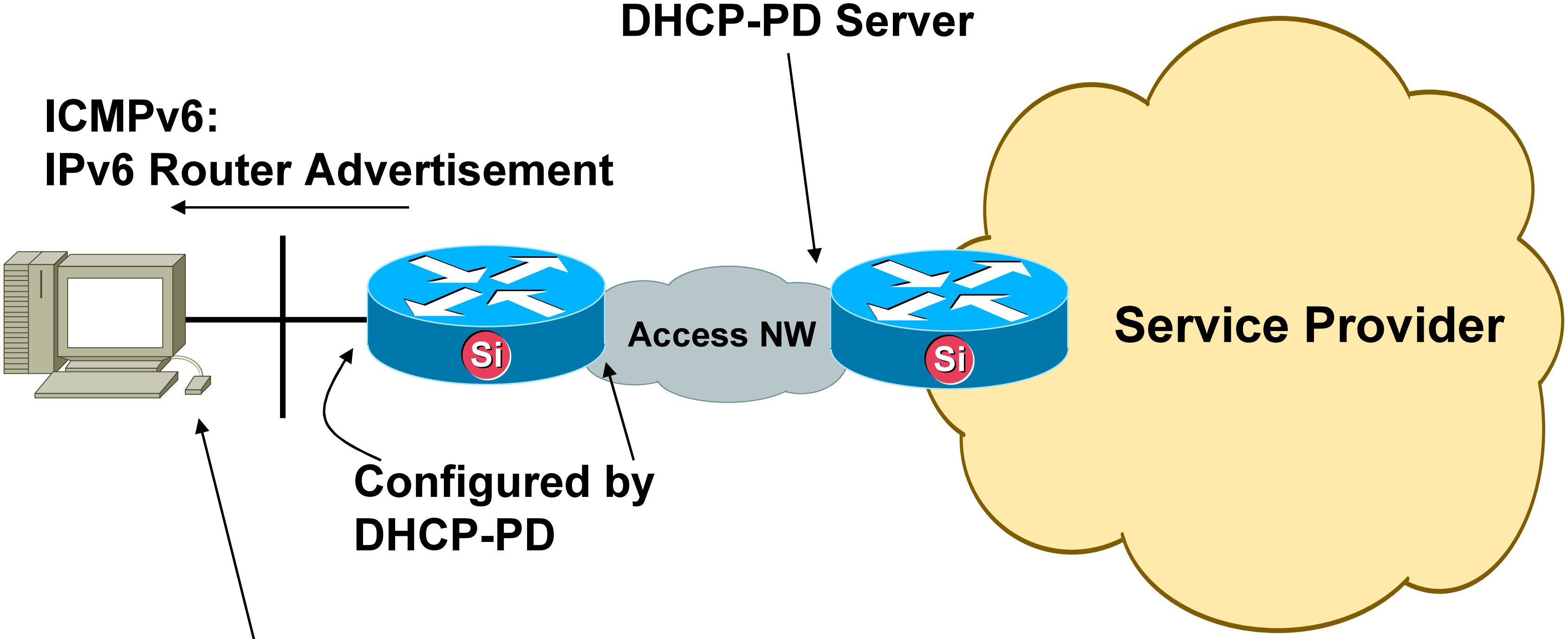
Function	*IPv4/NAT*	*IPv6*
Simple Gateway as default router and address pool manager	DHCP – single address upstream DHCP – limited number of individual devices downstream	DHCP-PD – arbitrary length customer prefix upstream, SLAAC via RA downstream
Simple Security	Filtering due to lack of translation 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

Simple Gateway – IPv4



Conclusion: IPv4 Address Configured Dynamically by DHCP

Simple Gateway – IPv6



DHCP-PD Server

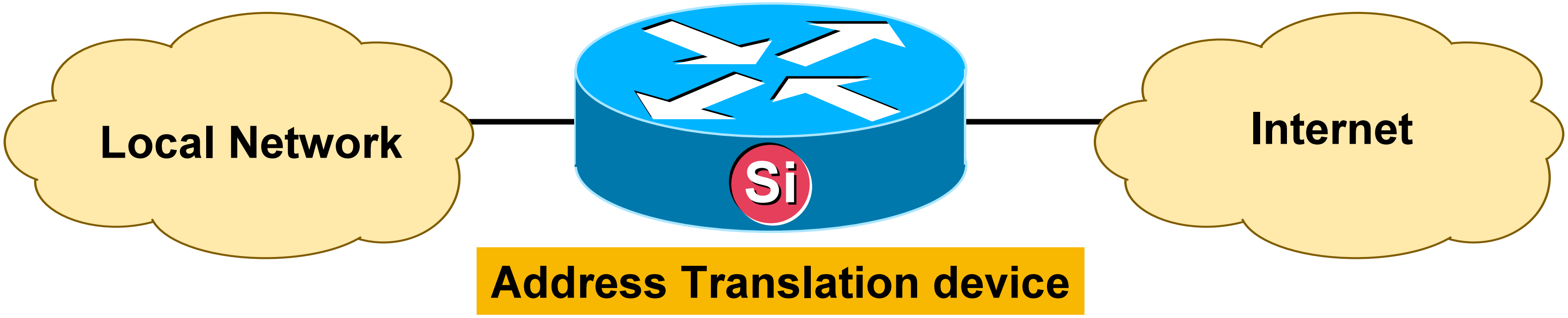
ICMPv6:
IPv6 Router Advertisement

Configured by
DHCP-PD

IPv6 Host configured by
Stateless Auto-configuration

IPv6 Addresses Configured Dynamically by DHCP-PD

Simple Security & Local Usage Tracking by IPv4 Address Translation



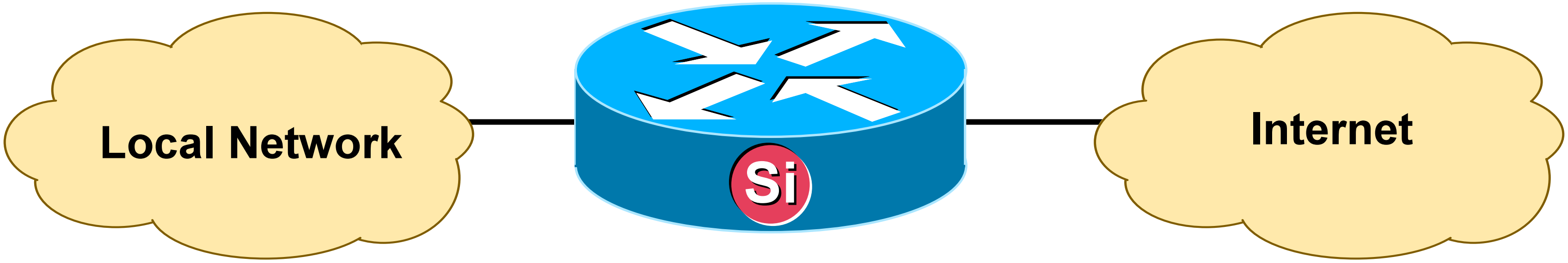
1 Initial outbound Packet →

2 Creation of Statefull Address Translation slot

3 Return Packets allowed ←

This state-database can provide awareness of who requested what at which time

Simple Security & Local Usage Tracking with IPv6



1 Initial outbound Packet

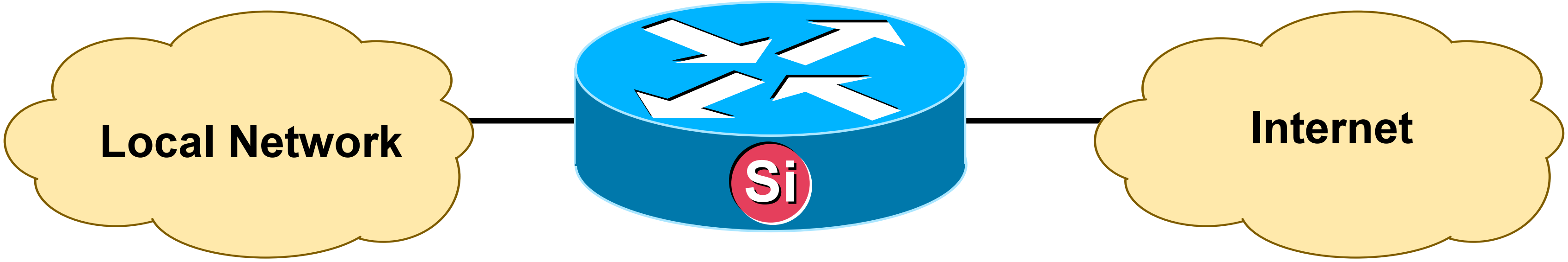
2 Creation of reflexive acceptance slot

3 Return Packets allowed

1. This state-database can provide awareness of who requested what at which time

2. Also addresses inside the local Network are Unique and can be monitored by various means if there is user/address correlation

End System Privacy



Local Network

Internet

IPv4 + NAT

10.10.10.100

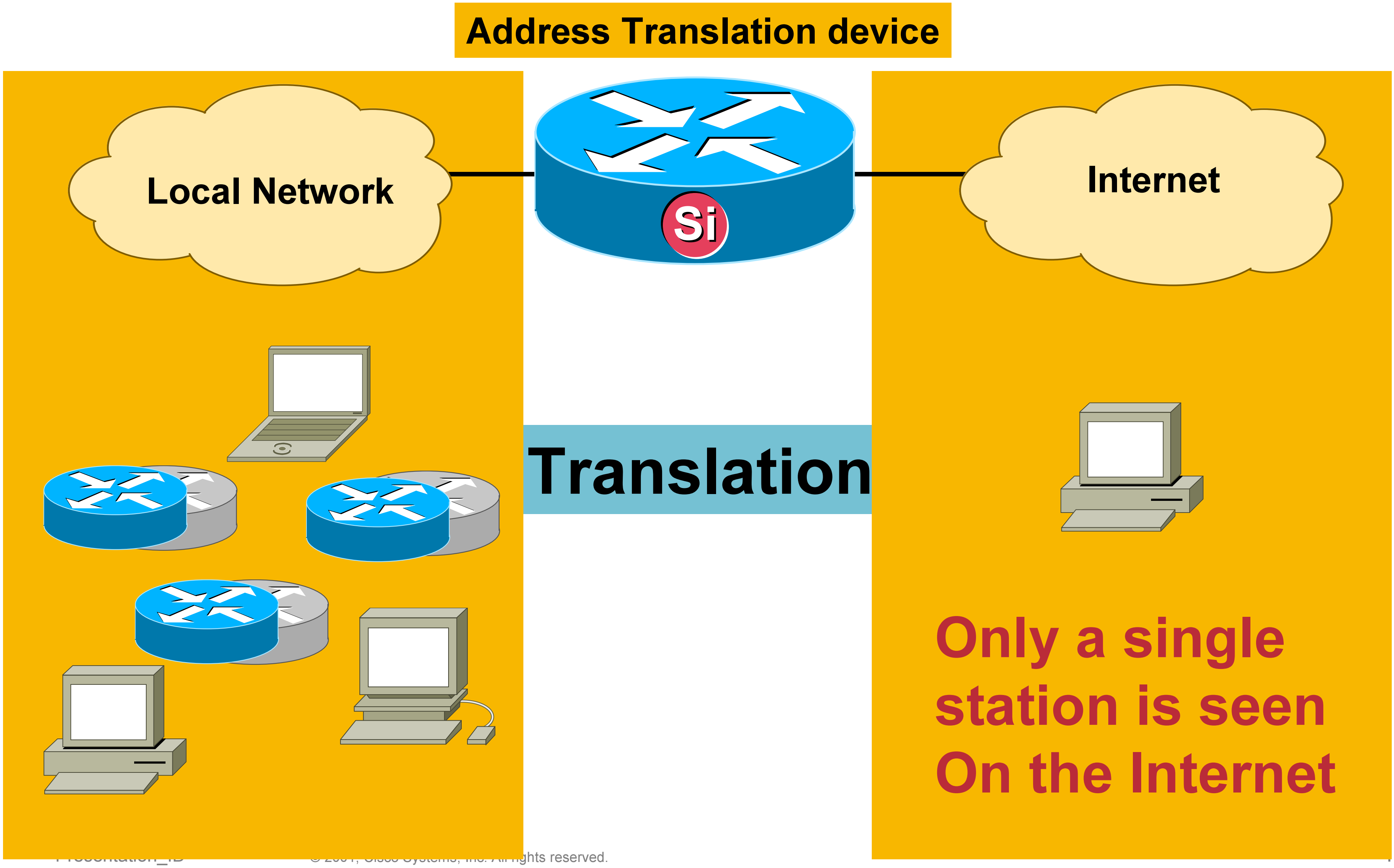
Could be Translated to
After NAT

121.1.1.1

IPv6 & privacy

2001:1:2:3::cafe:213/64	2001:1:2:3::cafe:213
:	:
2001:1:2:3::dead:991/64	2001:1:2:3::dead:991
2001:1:2:3::deaf:321/64	2001:1:2:3::deaf:321
2001:1:2:3::1/64	2001:1:2:3::1

Topology Hiding with Address Translation (IPv4)



Address Translation device

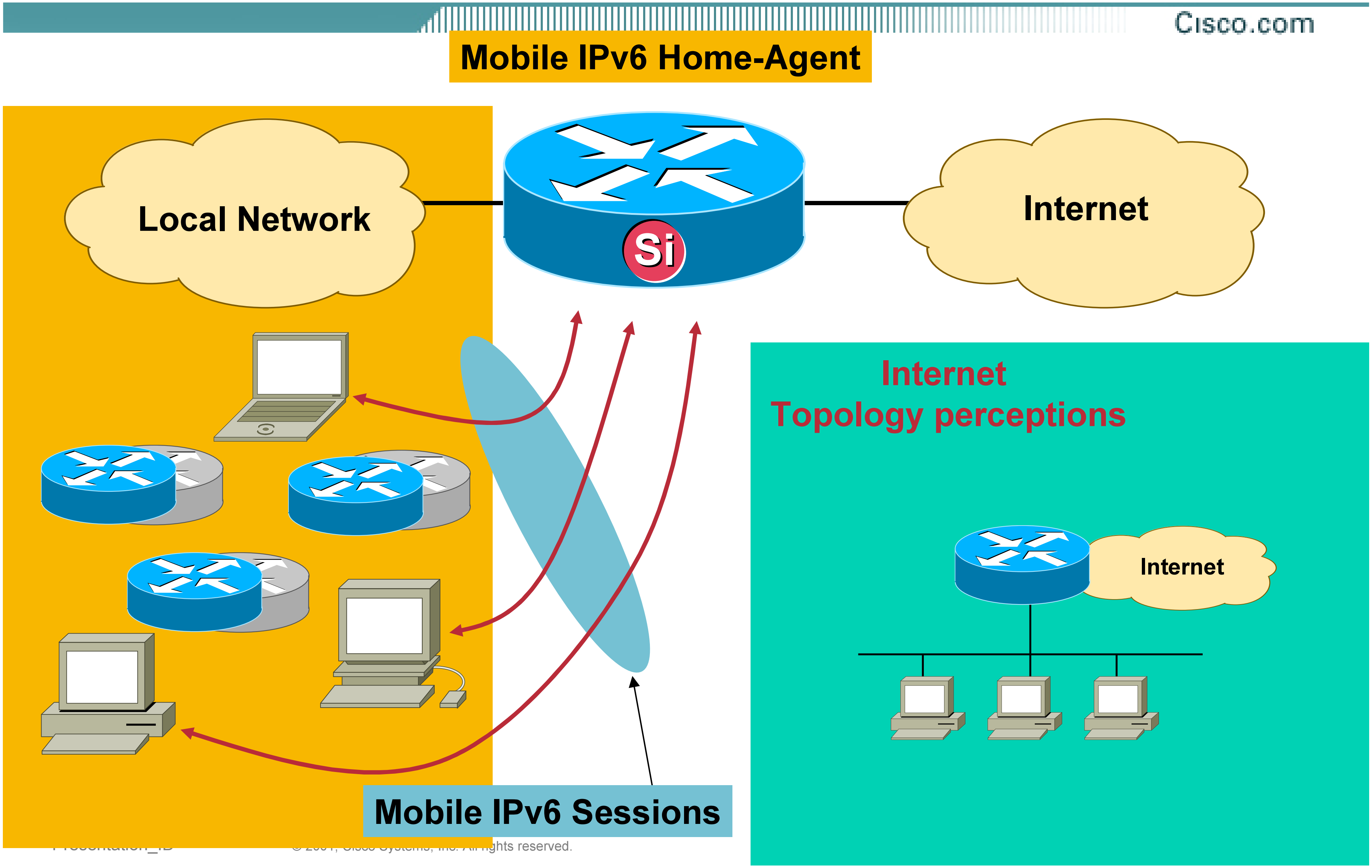
Local Network

Internet

Translation

Only a single station is seen On the Internet

Topology Hiding with IPv6 (1)



Topology Hiding with IPv6 (2)

- Remove the subnet/host correlation by using /128 host routes
- Alternative topology hiding solution:

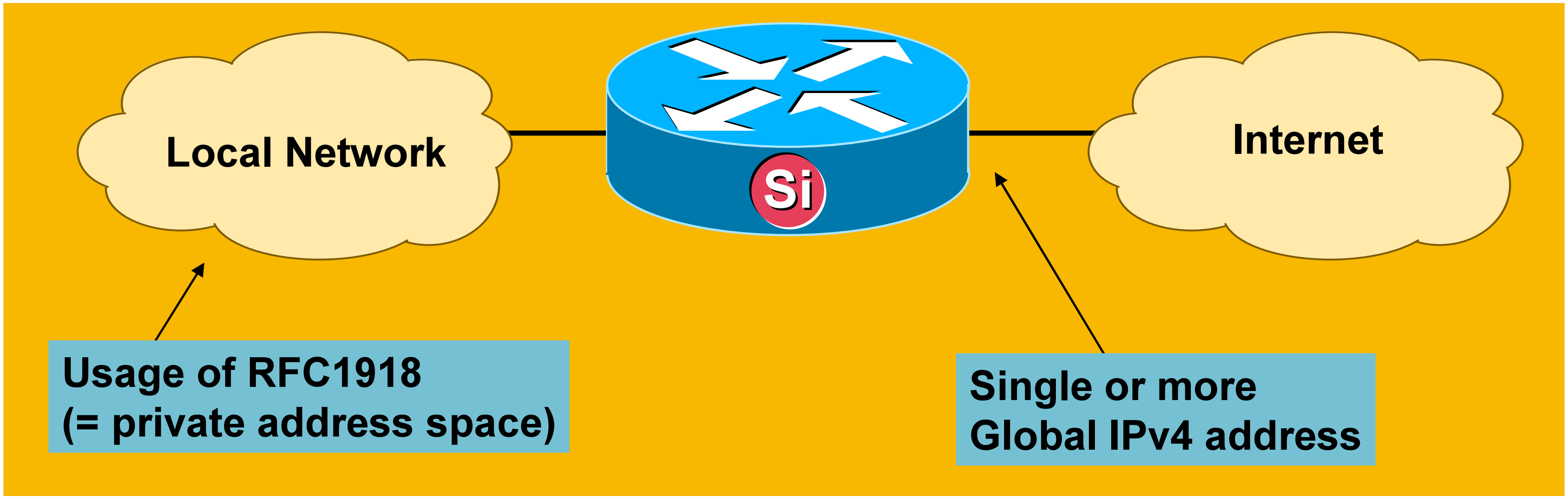
  Usage of multiple IPv6 addresses per host:

    One or more ULA addresses

    One or more Global IPv6 Addresses

  Redistribute the global addresses into the IGP

Address Autonomy



Usage of RFC1918
(= private address space)

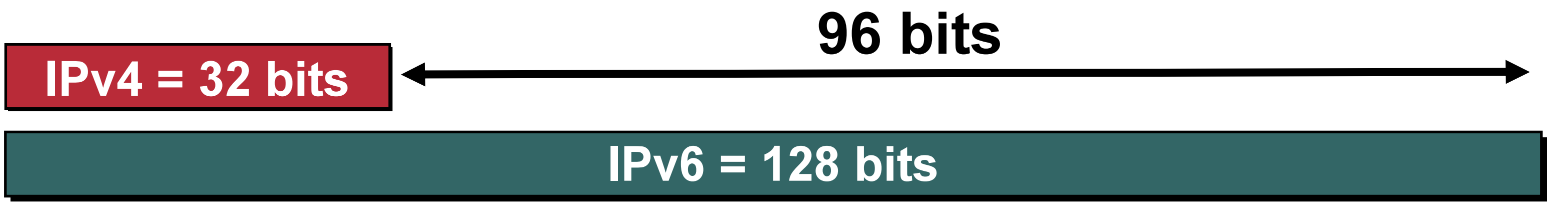
Single or more
Global IPv4 address

For IPv6 however …

there is no problem of address Autonomy:

- Large Address space per site or user (/48)
  - RFC3177 describes the allocation of IPv6 address space
  - Typical site will get /48 (this provides 16 bits for subnets = 65536 networks per site (even for your home-network)
- Unique Local Addresses
  - draft-ietf-ipv6-unique-local-addr-09.txt
  - Provides Unique private address space for internal independent usage

Global Address Pool Conservation



- IPv4

  32 bits

  =~ 4,200,000,000 possible adressable nodes

- IPv6

  128 bits: 4 times the size in bits

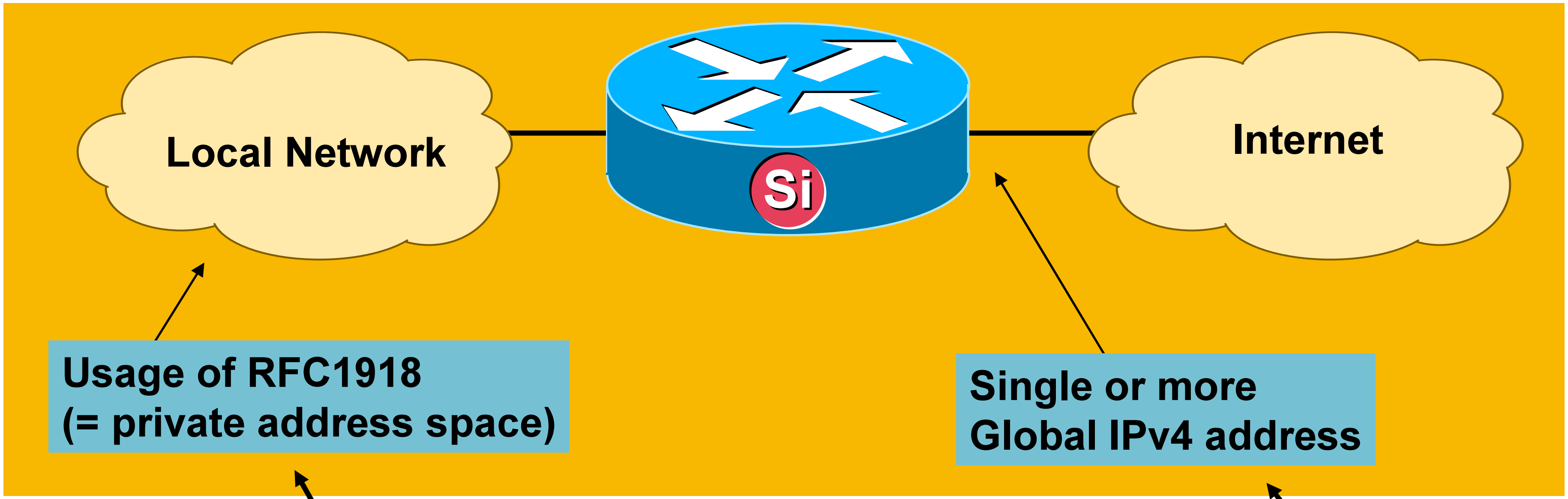
  =~ 3,4 * 10^38 possible addressable nodes

  =~340,282,366,920,938,463,374,607,432,768,211,456

  =~ 10^30 addresses per person on the planet

Conclusion: No need for Global Address Pool Conservation in IPv6 due to a legacy protocol limitation

Renumbering & Multihoming (IPv4)



Usage of RFC1918
(= private address space)

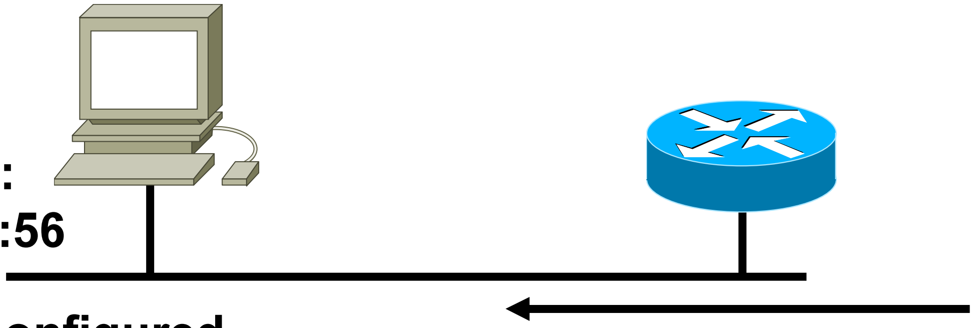
Single or more
Global IPv4 address

Totally independent from
any external renumbering

Only this address needs to change
if the external IP address changes,
and even this happens normally
automatically through DHCPv4

Renumbering & Multihoming (IPv6)

Operational IPv6 environment

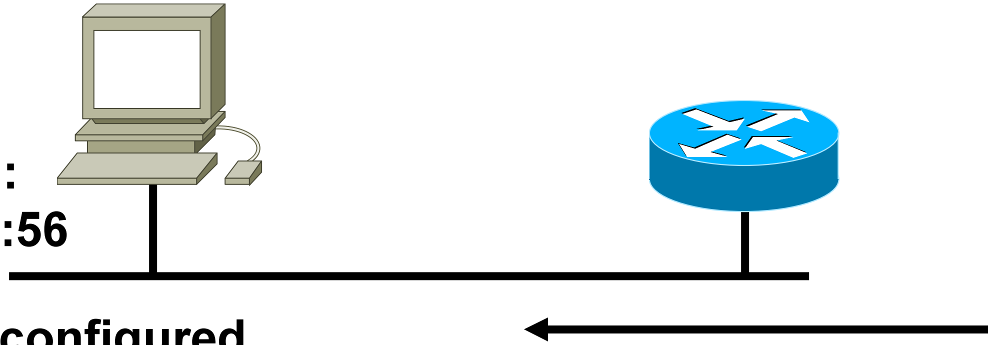


Mac address:
00:2c:04:00:FE:56

Host autoconfigured address is:
prefix received + link-layer address

Sends network-type information
(prefix, default route, …)

Introduction of a new prefix



Mac address:
00:2c:04:00:FE:56

Host autoconfigured address is:
NEW prefix received +
SAME link-layer address

Sends NEW network-type information
(prefix, default route, …)

IPv6 Gap Analysis

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

CISCO SYSTEMS®

EMPOWERING THE
INTERNET GENERATION