Tony Hain

IPv6 Forum Fellow

Cisco Systems Technical Leader

ahain@cisco.com

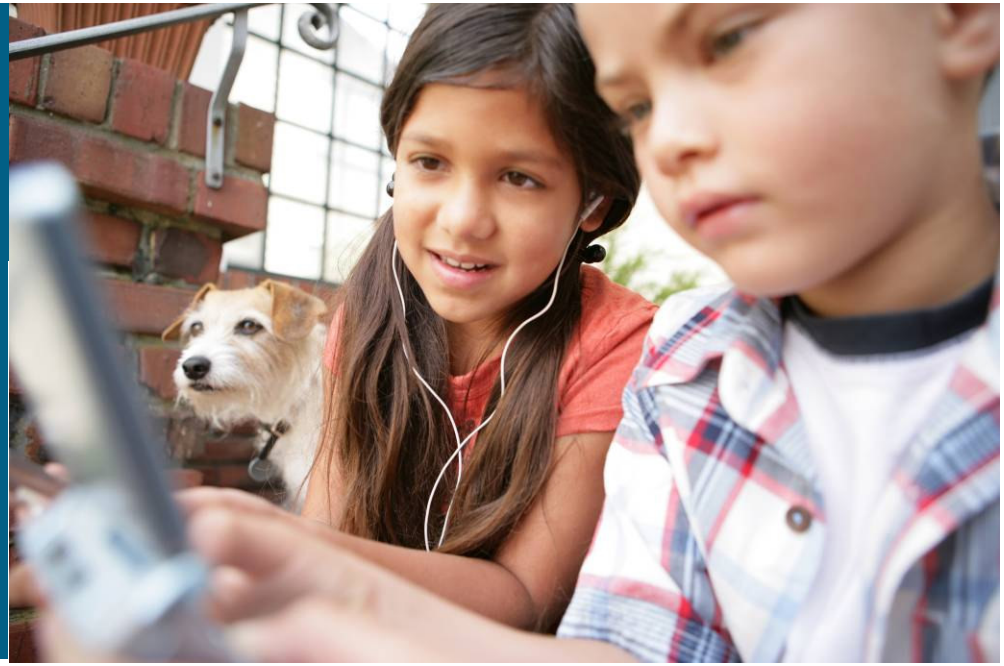
Agenda

- Security for the Complacent
- Security Perspectives
- Security in Evolution
- General policy considerations
- Threats
- Steps to avoid header mangling
- Wrap-up

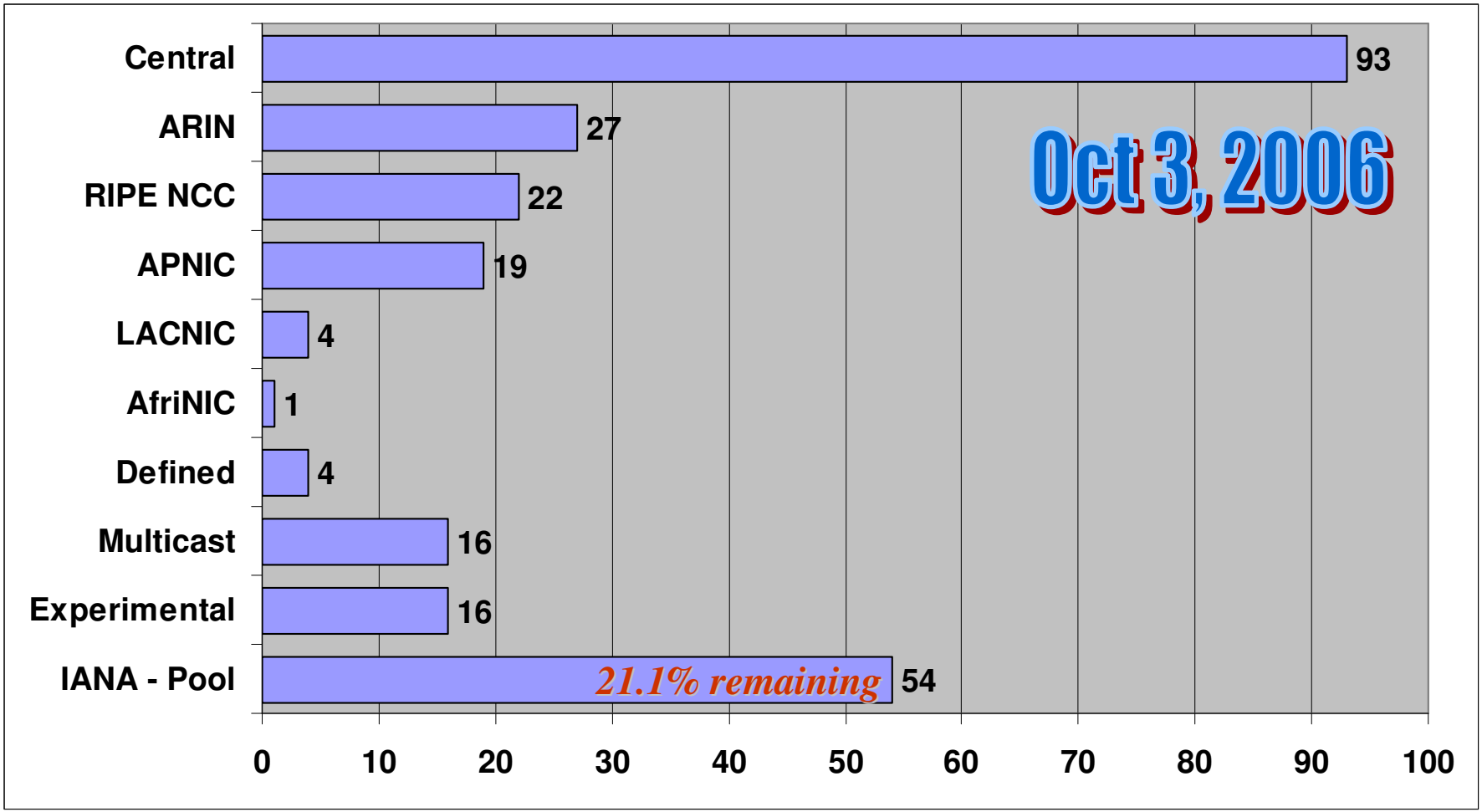
Introduction

- **Discussions around IPv6 security have centered on IPsec**
  - **Though IPsec is mandatory in IPv6, the same issues with IPsec deployment remain from IPv4:**
    - **Configuration complexity & Key management**
- **Security in IPv6 is a much broader topic than just IPsec**
  - **Even with IPsec, there are many threats which still remain issues in IP networking**
- **Marketing has done a good job of convincing consumers to deploy NAT with IPv4 to improve the security of their network.**
  - **Despite that effort, the technology of address translation and header manipulation does not improve security.**
- **IPv6 makes some things better, other things worse, and most things are just different, but no more or less secure**

Security in Complacency



Distribution of IPv4 addresses by /8



IANA allocated 25 /8's between Jan. 1, 2004 and Jan. 5, 2006

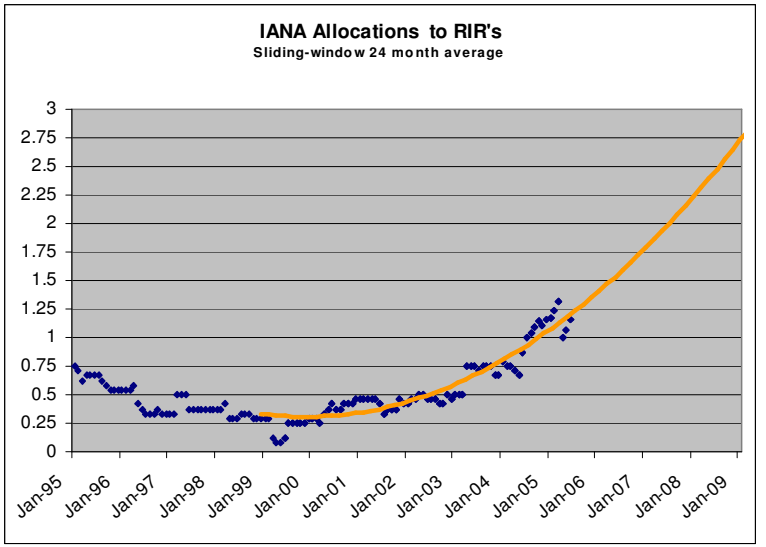
typical RIR re-allocation period 9-12 months

IP Address Allocation History

IP Address Allocation History

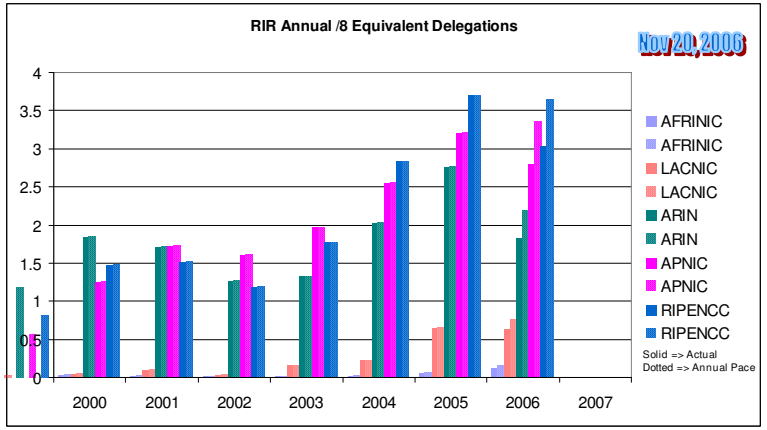
Full discussion at: **www.cisco.com/ipj**
The Internet Protocol Journal
Volume 8, Number 3, September 2005

- Consumption is accelerating despite increasingly intense conservation efforts.
  - **PPP / DHCP (temporal address sharing)**
  - **CIDR (classless inter-domain routing)**
  - **NAT (network address translation)**
  - **plus some address reclamation**



Projection based on IANA* data from 2000

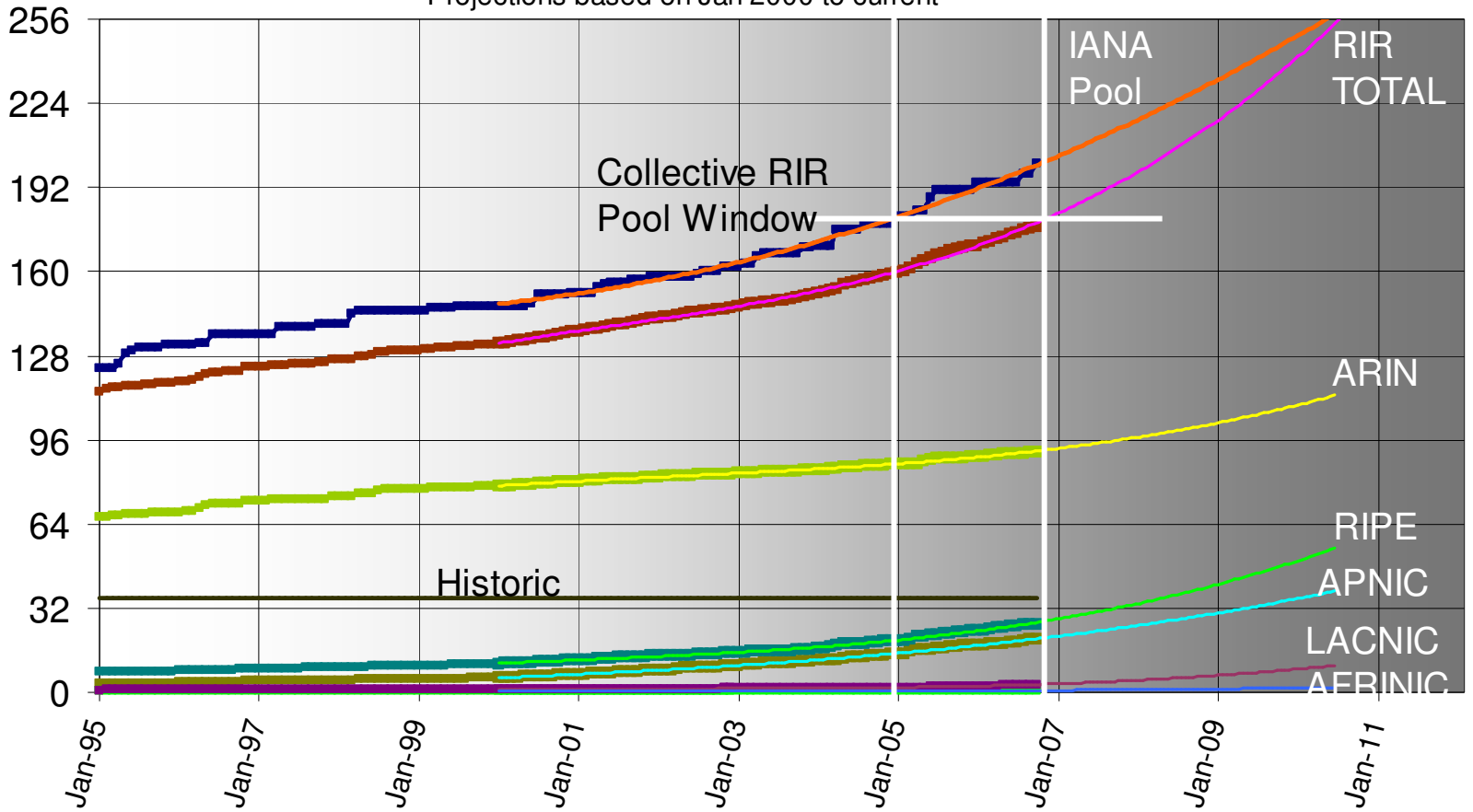
- **Growth is occurring in all regions**
  - **While growth as seen in the routing system is strongest in Asia, the allocation growth is strongest in Europe.**



IPv4 Address Pool

Nov 20, 2006

IANA Policy - RIRs Allocated Pool for 12-24 Months Distribution
Projections based on Jan 2000 to current



Update to: http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_8-3/ipj_8-3.pdf
Exhaustion of the central IANA pool - orange
Exhaustion of the collective RIR pools - magenta
Relative distribution rates between the RIRs
Time depth of collective RIR pools on pub date - white
Time depth between exhaustion events - diff between orange & magenta

Tony Hain

Implications

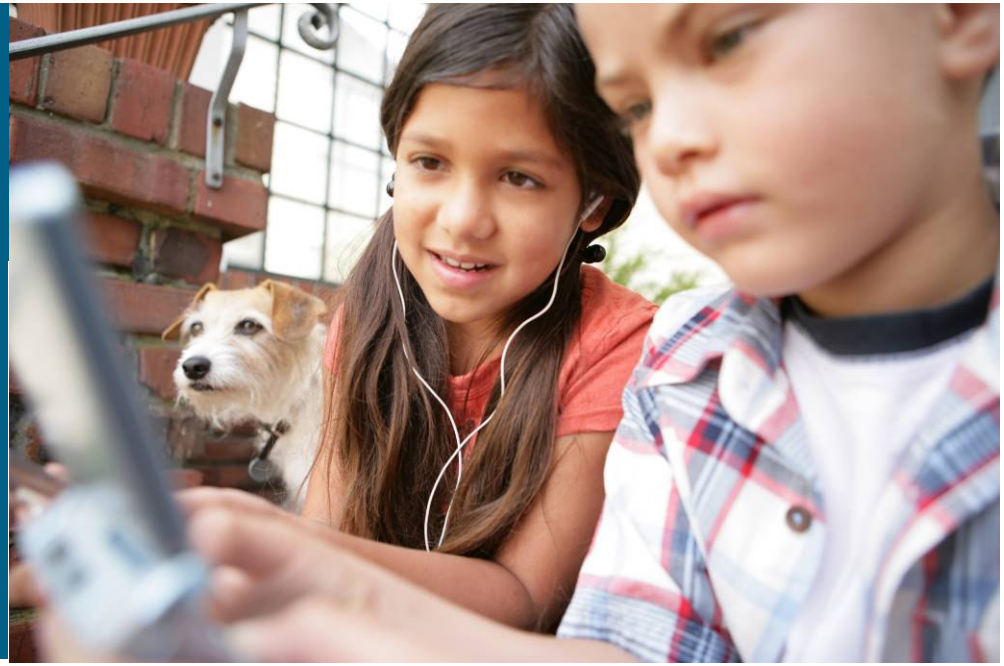
- **Despite the wide-scale deployment of NAT, the consumption of the IPv4 pool continues at an accelerating rate.**
- **When IANA runs out, existing IPv4 networks still work.**

  The only ones that will be immediately impacted are the RIRs when they come back for more space.
- **When any RIR runs out, existing IPv4 networks still work.**

  The only ones that will be immediately impacted are the LIR/ISP/Enterprise's when they come back for more space.
- **When the LIR/ISP runs out, existing IPv4 networks still work.**

  The only ones that will be immediately impacted are the people looking for more or new space.
- **Any specific network will only *need* IPv6 when they attempt to talk to someone that was *unable* to acquire enough IPv4 space, or attempt to expand or add new applications and find themselves *unable* to get enough IPv4 space.**

Security Perspectives



http://www.ipv6forum.com/dl/white/NAv6TF_Security_Report.pdf

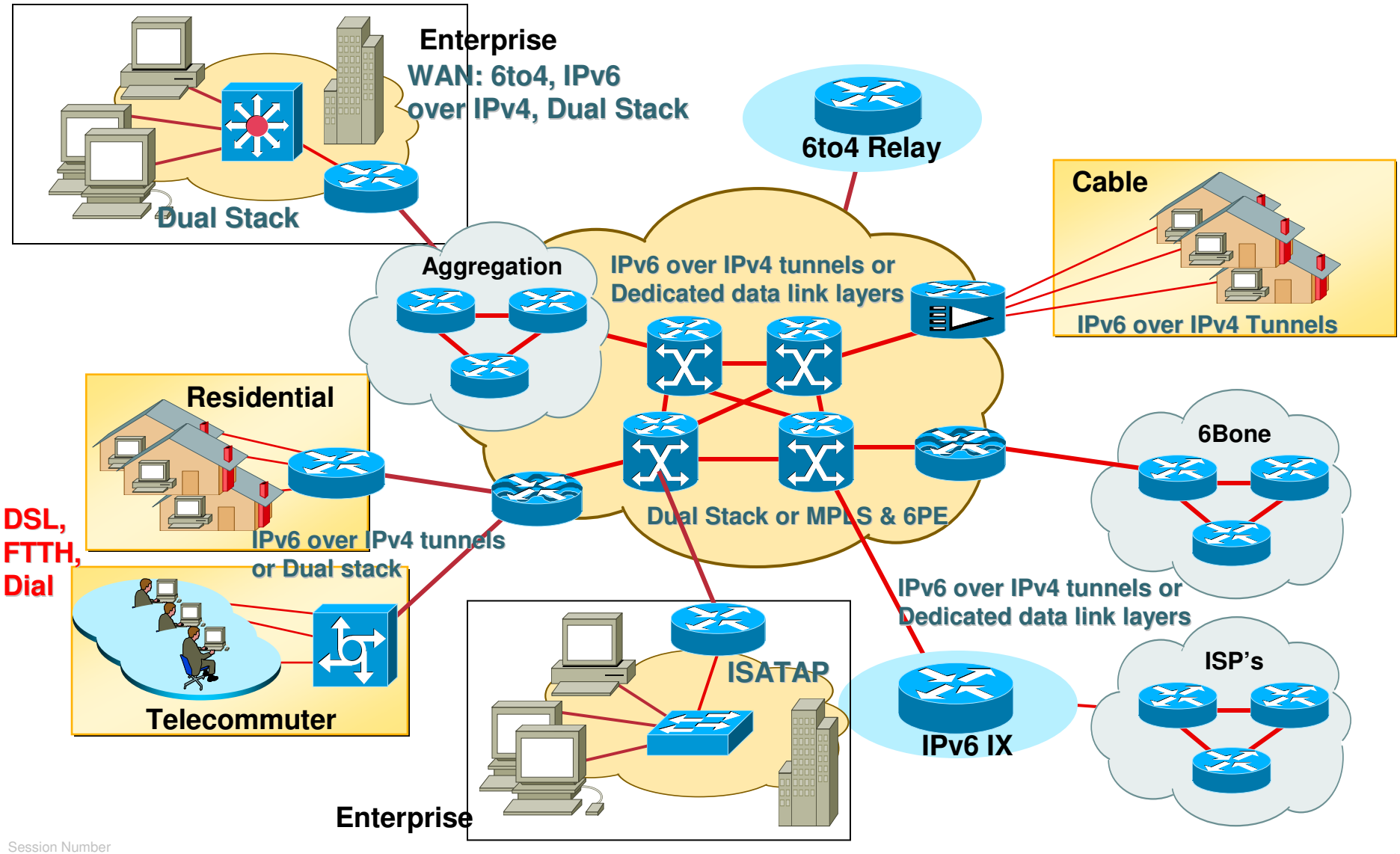
Conflicting views on network security

- Privacy end-to-end eliminates opportunity for a compromised node or shared media segments to be used for man-in-the-middle attacks.
- Traceability is mandatory for both diagnostics and to comply with many laws.

  Privacy Extensions limit the exposure to a security threat that targets a host IPv6 address directly. This is great for making an end host harder to identify to an attacker, but it also makes an end host harder to identify to the network administrator

- Securing at IP layer between the endpoints allows transport flows to obtain or share a security association without requiring application awareness or involvement.
- Firewalls expect visibility to ensure only authorized traffic crosses the border.

Internet Environment Diversity

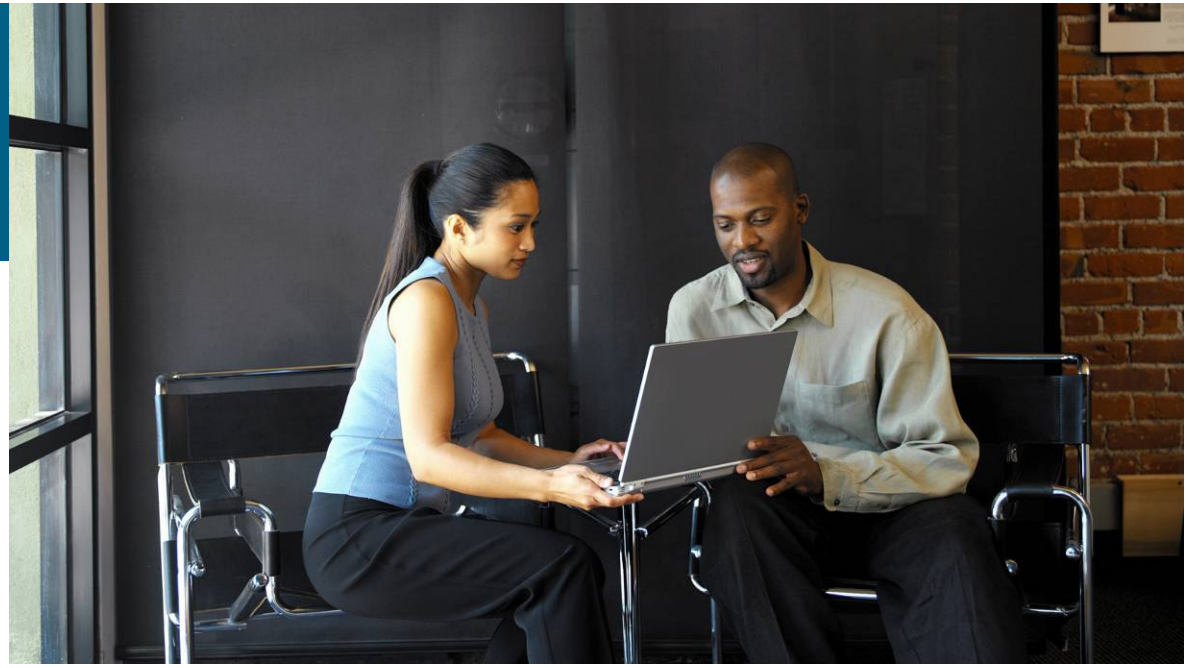


Security at the IP layer

- **In most environments the IP layer is not responsible for security, but stability and uniqueness at the IP layer are relied on by many security functions and mechanisms.**

- **IPsec simply provides a common security mechanism for use by the wide array of transport protocols.**

Security in Evolution



The Internet of 20 years ago

- **Modest capacity**

  1.2 kbps → 45 Mbps
- **Moderate latency**
- **Moderate loss rate**
- **Periodic attachment**
- **Primarily text based applications**

The Internet of today

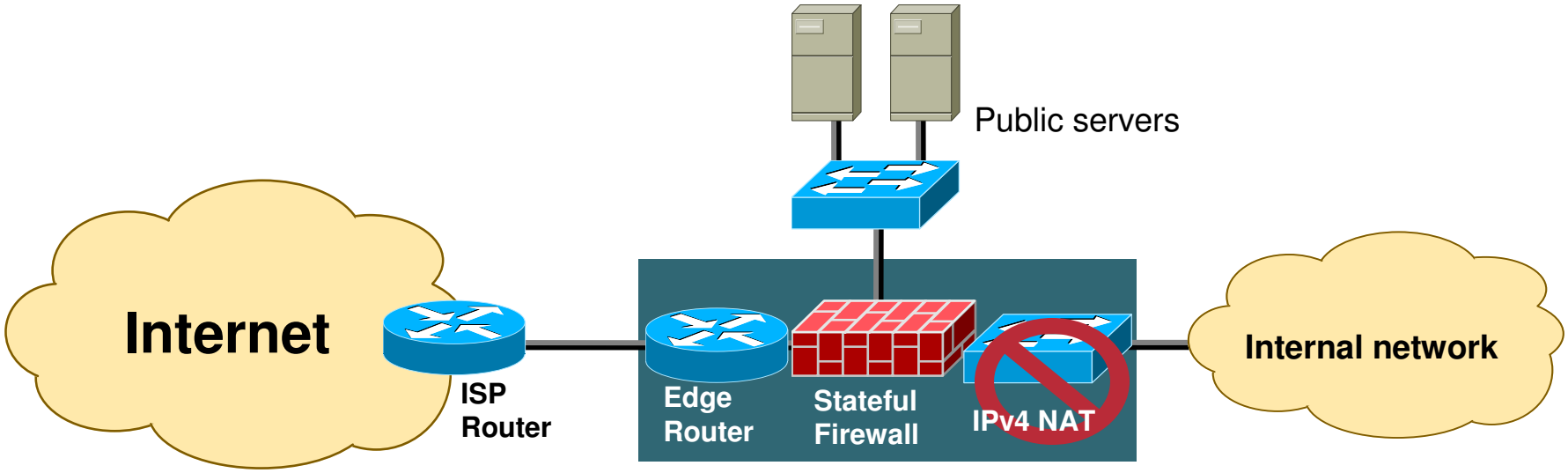
- **Vast range of capacities**
  - **10's kbps → 40 Gbps**
- **Fixed and nomadic attachment**
- **Basic multimedia**
- **Foundation for global e-commerce**

Mobility challenges

Mobility is a natural human trait – even when the technology is not ready

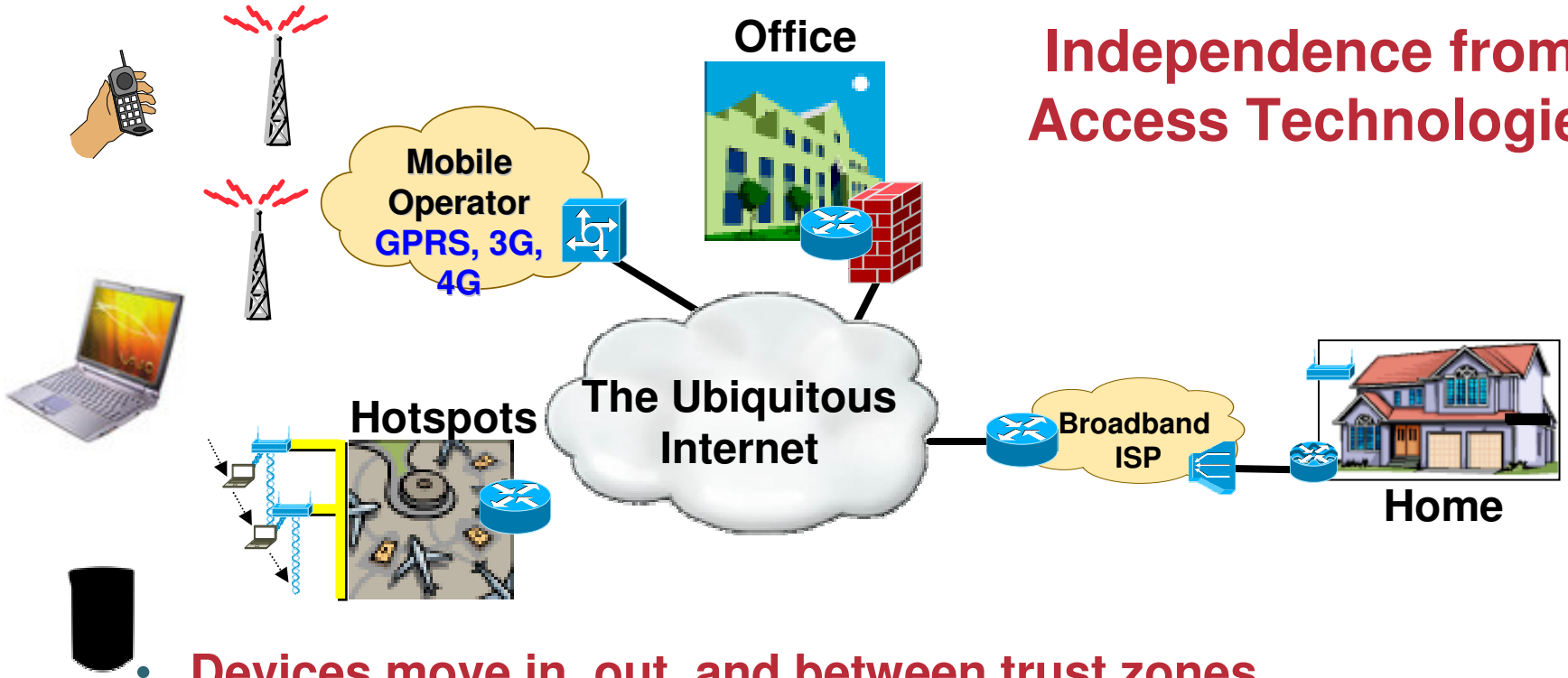
- Modest capacity
- Moderate latency
- Moderate loss rate
- Intermittent attachment
- Limited multimedia

Traditional Edge Security Design (evolved…)



- This design can be augmented with IDS, application proxies, and a range of host security controls
- The 3-interface FW design as shown here is in use at thousands of locations worldwide
- Firewall policies are generally permissive outbound and restrictive inbound
- As organizations expand in size the number of "edges" and the ability to clearly identify them becomes more difficult

Where is the perimeter?



Independence from Access Technologies

- Devices move in, out, and between trust zones
- Simple appliances lack UI to support complex access control
- Applications are generally unaware of topology impediments
- End users expect applications to work from any connection point without significant effort

General policy considerations

Change takes time

- **Translation removes audit trail and creates scaling concerns**
  - **Services should be available via IPv6 before client systems are forced to change protocol versions.**
- **Tunneling tools decouple decisions about application & end system deployment from infrastructure deployment**
- **Tunneling is really just framing a packet in another L3 protocol vs. L2.**
  - **Configured IPv6 tunnels over a closed IPv4 network are no less secure than IPv4 over a closed F/R or ATM fabric. When the IPv4 network is not closed, IPv6 over an IPv4/IPsec connection between edge routers effectively isolates those logical links to the closed part of the network.**
- **Judicious use of secure/managed tunnels allows service delivery while traversing routers that have not reached their natural replacement timeframe.**

Layered access & scope

Addresses are assigned to interfaces

change from IPv4 model :

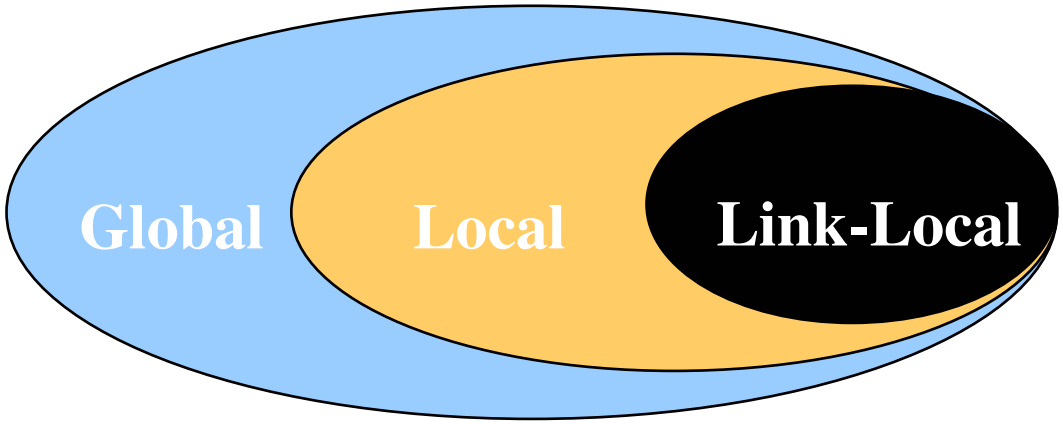
Interface 'expected' to have multiple addresses

Addresses have scope

Link Local

Local

Global

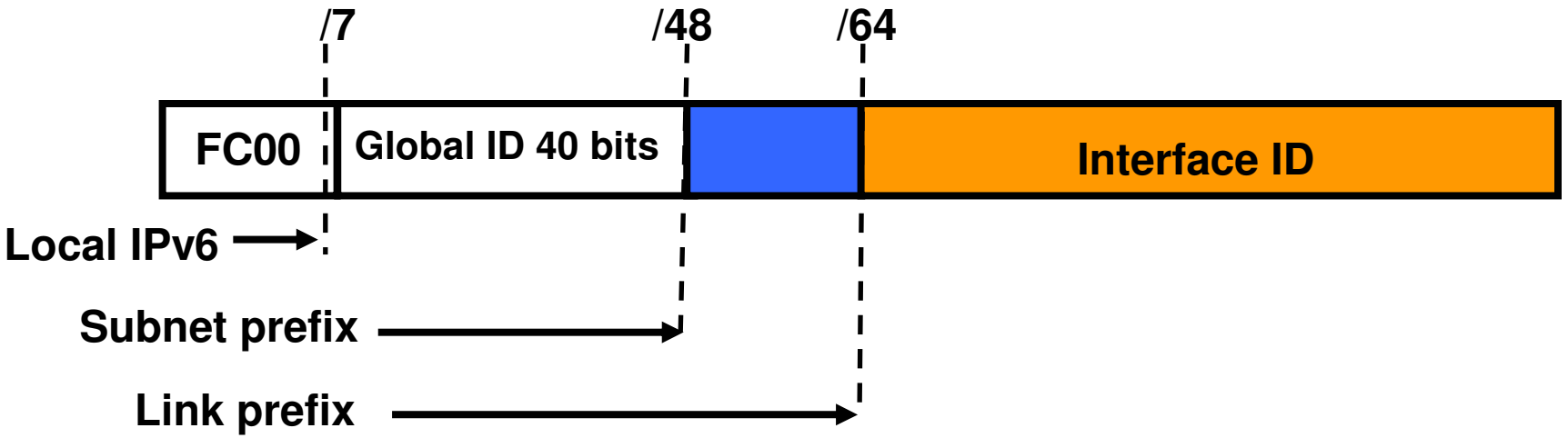


Addresses have lifetime

Valid and Preferred lifetime

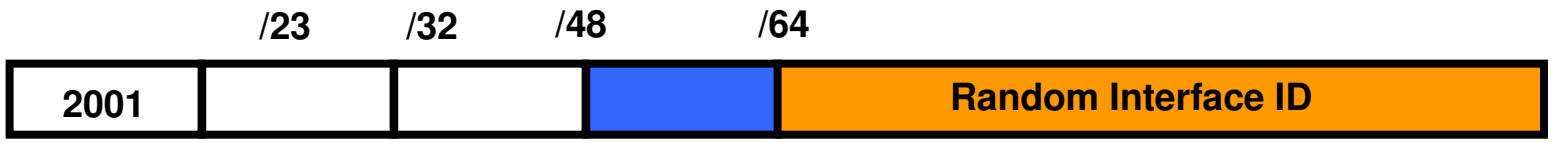
Keeping applications restricted within the scope that meets policy reduces the attack profile in the event that other layers of security fail. Since local prefixes will not be routed in the global Internet, remote attackers will not even see or reach the network edge.

Local IPv6 Unicast Addresses – FC00::/7



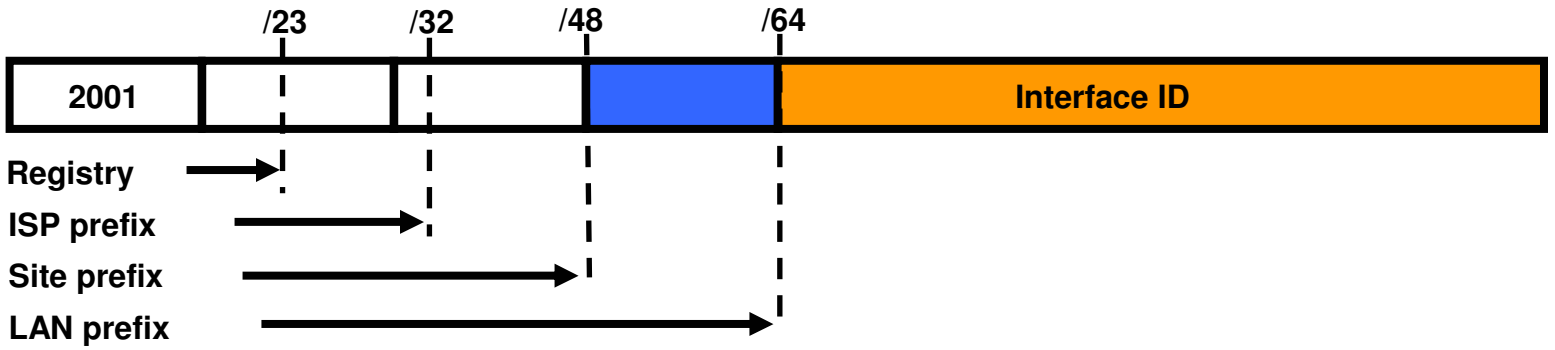
- Prefix FC00::/7 prefix to identify Local IPv6 unicast addresses.
- One bit to identify local generation vs. reserved
- Global ID 40-bit global identifier used to create a globally unique prefix.
- Subnet ID 16-bit subnet ID is an identifier of a subnet within the site.
- Interface ID 64-bit IID

Privacy based addressing



- **Temporary addresses for IPv6 host client application, eg. Web browser / soft-phone**
  - **Inhibit device/user tracking**
    - **From RFC 3041: "[mac derived] interface identifier …facilitates the tracking of individual devices (and thus potentially users)…"**
  - **Random 64 bit interface ID, run DAD before using it**
  - **Rate of change based on local policy**
  - **Reduces attack profile as device stops answering when no longer valid**
- **More general use counters direct attack threats**
  - **Administrators may adopt easy to remember addresses (::10, ::20, ::F00D, IPv4 last octet)**
  - **IPv6 addresses derived from IEEE Organizational Unit Identifier (OUI) designations, allow scanning focus on popular NIC vendor's ranges**

Traceability to the subnet

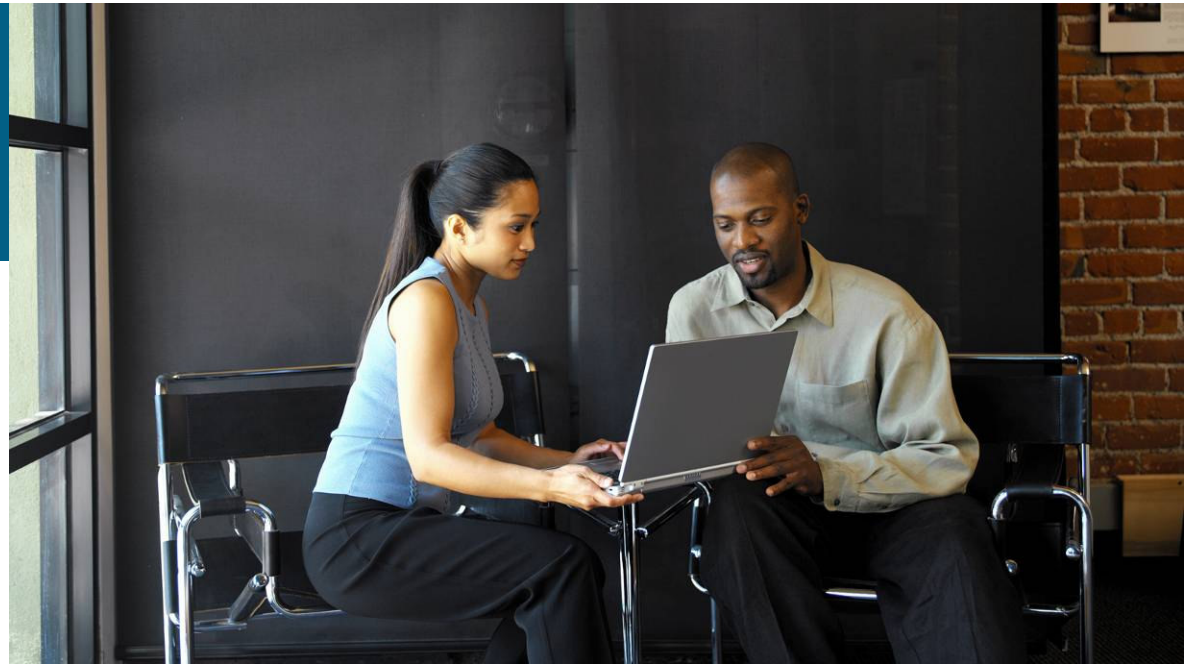


- **The allocation process implemented by the Registries:**
  - **IANA allocates from 2001::/16 to registries**
  - **Each registry gets a /23 prefix from IANA**
  - **Current policy, Registry allocates a /32 or shorter prefix to an IPv6 ISP**
  - **Then the ISP allocates a /48 prefix to each customer (or potentially /64)**

  http://www.apnic.net/docs/policy/ipv6-address-policy.html

- **All packets tracable to the specific subnet**
- **Public servers will still be registered in DNS**

Threats



Types of Threats (1/2)

- **Reconnaissance - Provide the adversary with information enabling other attacks**
- **Unauthorized Access - Exploit the open transport policy inherent in the IPv4 protocol**
- **Header Manipulation and Fragmentation - Evade or overwhelm network devices with carefully crafted packets**
- **Layer 3 – Layer 4 Spoofing - Modify the IP address and port information to mask the intent or origin of the traffic**
- **ARP and DHCP Attacks - Subvert the host initialization process or a device the host accesses for transit**
- **Broadcast Amplification Attacks (smurf) - Amplify the effect of an ICMP flood by bouncing traffic off of a network which inappropriately processes directed ICMP echo traffic**
- **Routing Attacks - Disrupt or redirect traffic flows in a network**

Types of Threats (2/2)

- **Viruses and Worms - Attacks which infect hosts and optionally automate propagation of the malicious payload to other systems**
- **Sniffing - Capturing data in transit over a network**
- **Application Layer Attacks - Broad category of attacks executed at Layer 7**
- **Rogue Devices - unauthorized devices connected to a network**
- **Man-in-the-Middle Attacks - Attacks which involve interposing an adversary between two communicating parties**
- **Flooding - Sending bogus traffic to a host or network designed to consume enough resources to delay processing of valid traffic**

Attacks fundamentally the same between IPv6 & IPv4

- **Sniffing**

  Without IPsec, IPv6 is no more or less likely to fall victim to a sniffing attack than IPv4

- **Application Layer Attacks**

  Even with IPsec, the majority of vulnerabilities on the Internet today are at the application layer, something that IPsec will do nothing to prevent

- **Rogue Devices**

  Rogue devices will be as easy to insert into an IPv6 network as in IPv4

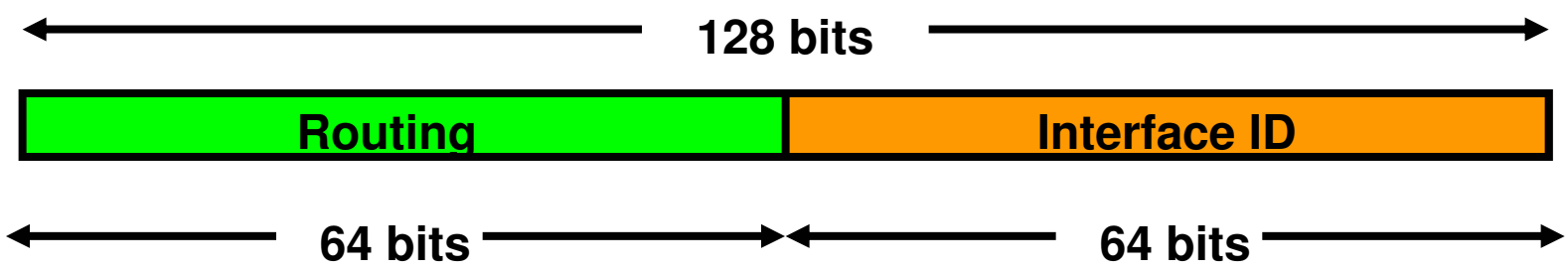
- **Man-in-the-Middle Attacks (MITM)**

  Without IPsec, any attacks utilizing MITM will have the same liklihood in IPv6 as in IPv4

- **Flooding**

  Flooding attacks are identical between IPv4 and IPv6

Reconnaissance



- **At 100M pings / second (40 Gbps fdx), it takes > 5,800 years to scan the address range for just one subnet.**

Worm and virus propagation will fail or will have to find an alternative search path.

So will scanning based network management products…

L3 - L4 Spoofing

- **L3 Spoofing is very common in IPv4, RFC 2827 defines mechanisms to largely eliminate L3 spoofing but this has not seen broad adoption in IPv4 networks.**

  Note that RFC 2827 stops the spoofing of the network portion of an IP address, not the host portion

- **L4 Spoofing can be done in concert with L3 spoofing to attack systems (most commonly running UDP, I.e. SNMP, Syslog, etc.**
- **Nearly 25% of the current IPv4 space has not been allocated, and around 8% more is reserved for special use (RFC3330) making it fairly easy to block at network ingress through bogon filtering.**
- **IPv6 deployments should deploy the filtering discussed in RFC 2827 at every point up the aggregation hierarchy.**

Securing Neighbor discovery RFC 3971

- **IPsec can only be used with a manual configuration of security associations, due to bootstrapping problems in using IKE**

Steps to avoid header mangling

IPv6 Network Architecture Protection

- **NAP – 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**

http://www.ietf.org/internet-drafts/draft-ietf-v6ops-nap-04.txt

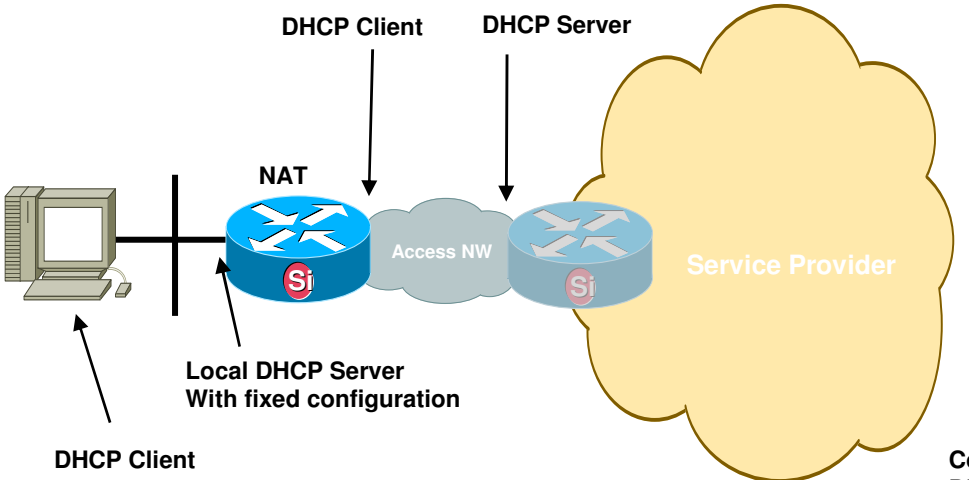
Market perceived benefits of IPv4

http://www.ietf.org/internet-drafts/draft-ietf-v6ops-nap-04.txt

Function	*IPv4*	*IPv6*
Simple Gateway	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 side effect due to lack of translation state	Explicit Context Based Access Control (Reflexive ACL)
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
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 (3.4*10^38) addresses
Renumbering and Multi-homing	Address translation at border	Preferred lifetime per prefix & Multiple addresses per interface

Simple Gateway

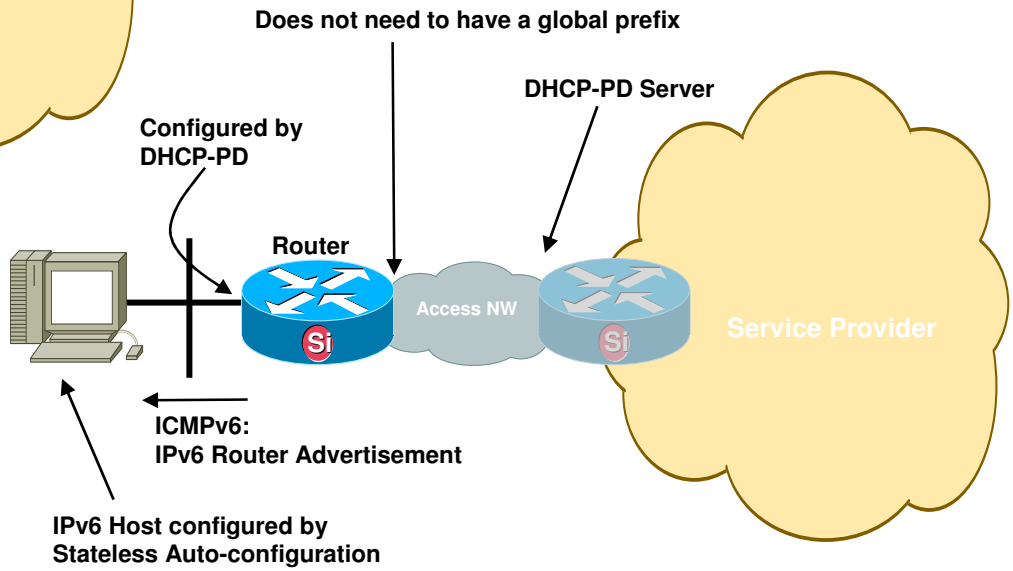
IPv4



- Fixed configuration local DHCP server provides private IPv4 address space to internal hosts.
- NAT function shares across all internal network devices the single IPv4 address acquired from the service provider DHCP.

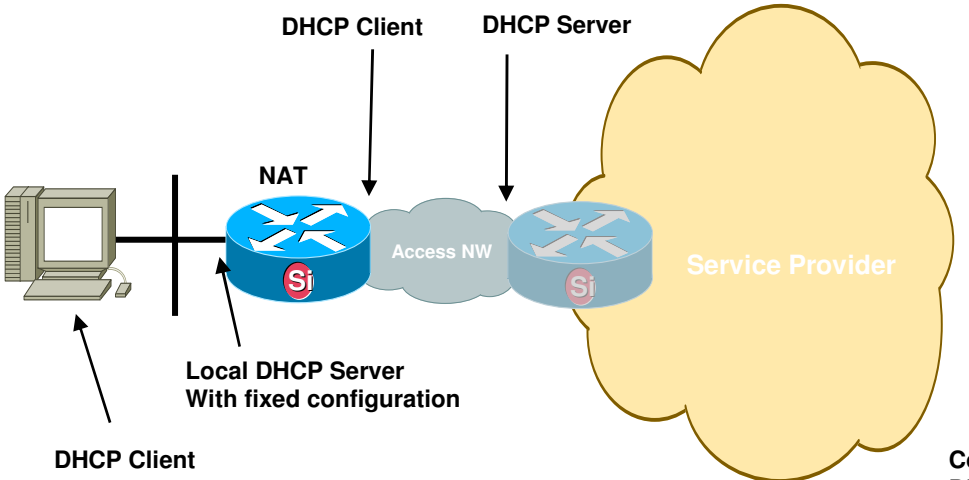
IPv6

- Simple router acquires delegated prefix for use across all internal network devices using DHCP-PD, announcing that internally via a Router Advertisement.
- External interface of the router could function using only the LinkLocal prefix on the interface connecting to the upstream router.



Simple Security

IPv4

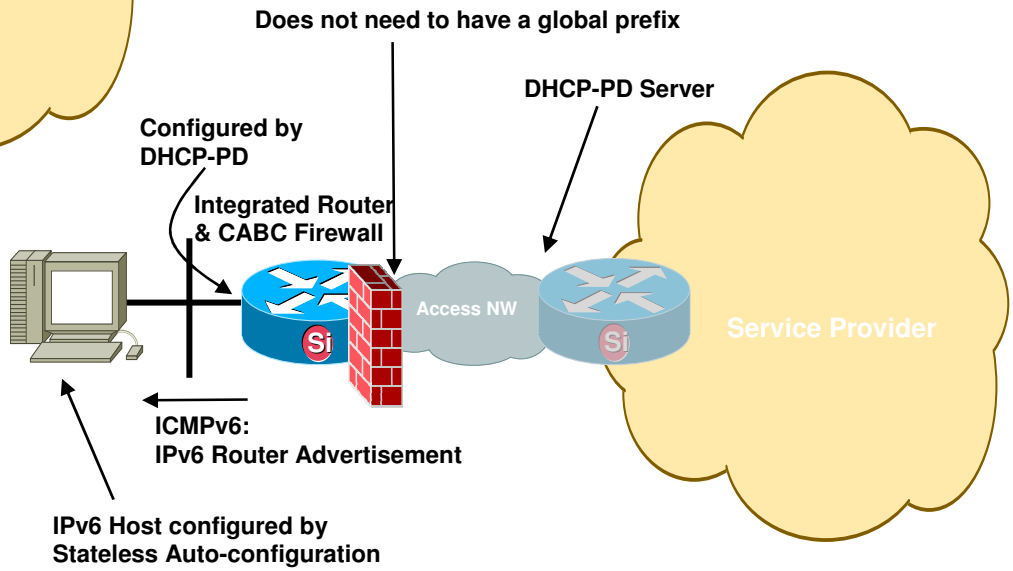


- The filtering side effect in a NAT due to lack of translation state does not provide predictable security.
- The header modifications at the NAT reduce overall security since the receiver can not determine which device originated the packet.

IPv6

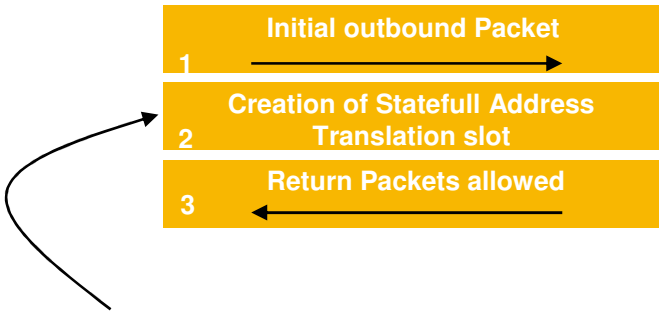
- Explicit Context Based Access Control
- Reverse Path Forwarding (RPF) filter

  Only allow the DHCP-PD prefix out as the source address in any packet.



Local Usage Tracking

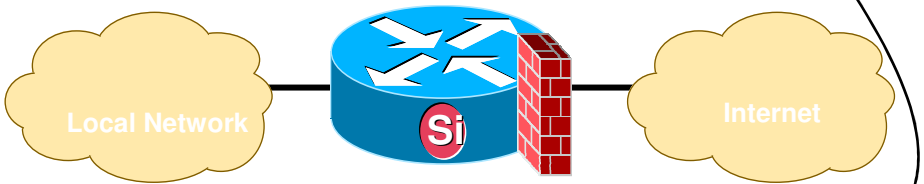
IPv4



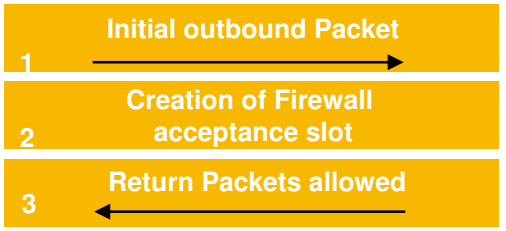
- This state database can be harvested to track which internal node interacted with target external addresses at specified points in time.

IPv6

- This state database can be harvested to track which internal node interacted with target external addresses at specified points in time.

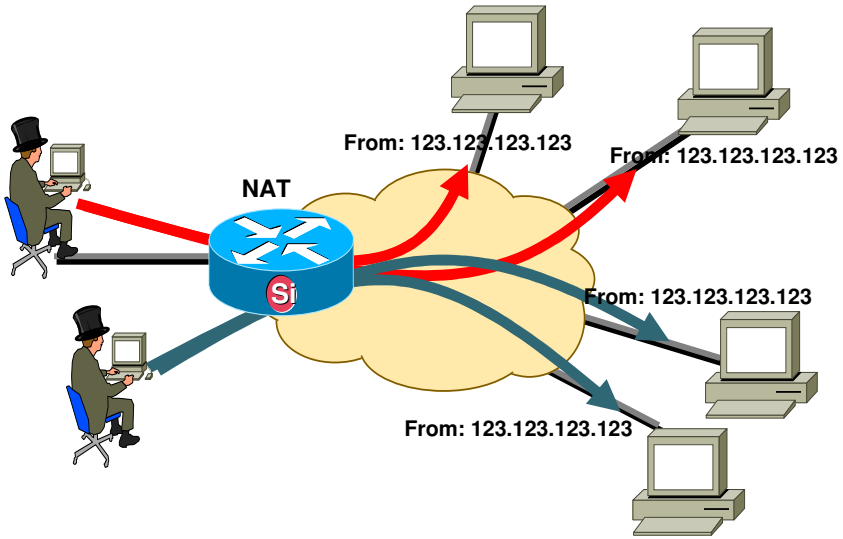


Integrated Firewall / Router



End System Privacy

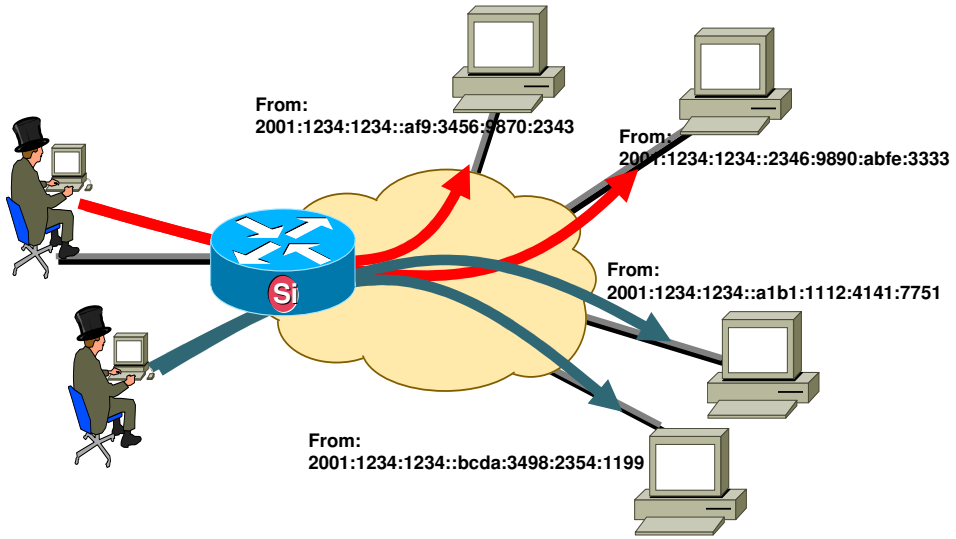
IPv4



- All internal devices appear to be the same from the outside.

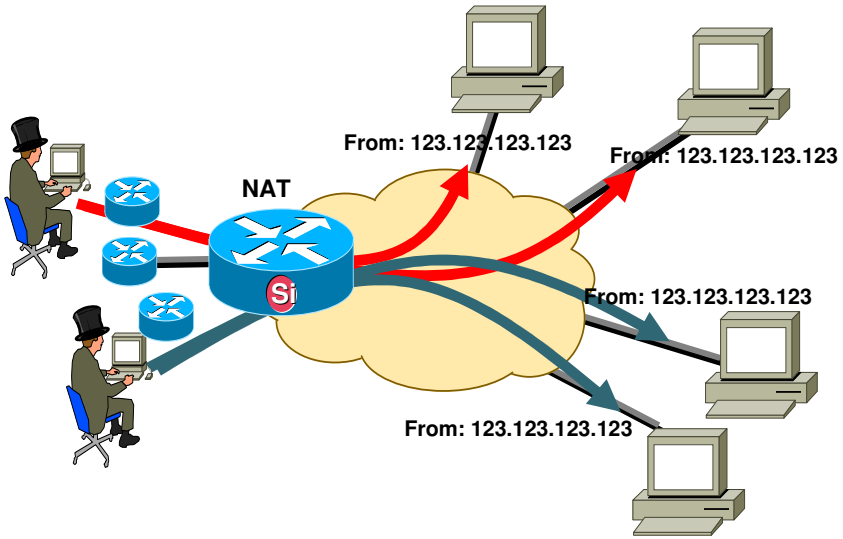
IPv6

- Privacy enabled nodes periodically generate new addresses based on lifetime policy.
- In some situations they might use a different address for each new connection they establish.



Topology Hiding

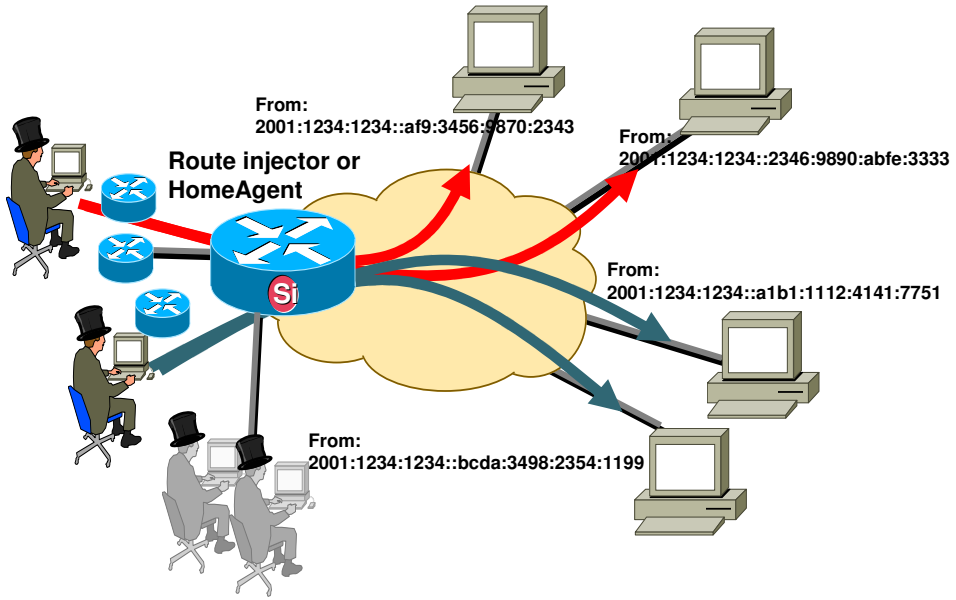
IPv4



- All internal devices appear to be the same from the outside, masking both the host and network topology.

IPv6

- Internal nodes appear to be hosted on a logical subnet attached to the edge router no matter which approach is used.
- In the IGP host routing approach an explicit host entry is injected for hidden nodes (limited due to IGP capacity).
- In the mobile IP approach the HomeAgent tunnels to the CareOfAddress and blocks all path optimization messages.



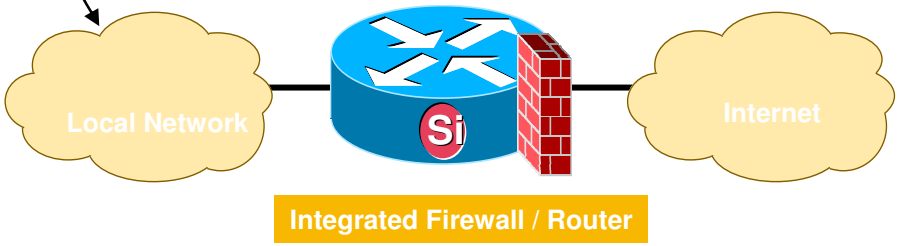
Addressing Autonomy

IPv4

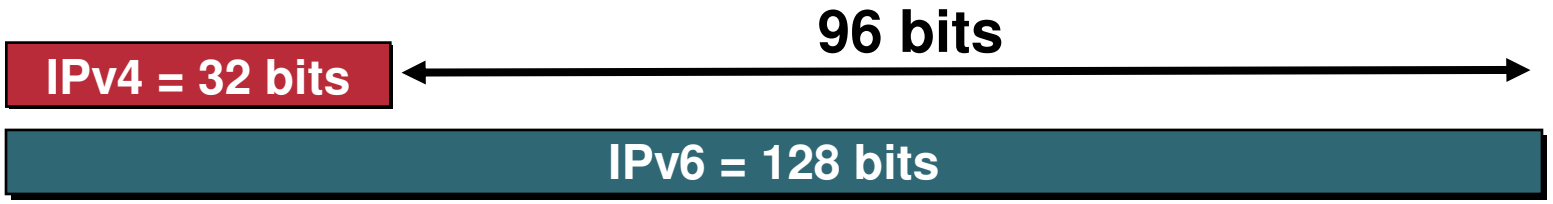
- Private address space defined in RFC 1918. Allows for one /8, one /12, and one /16 to be autonomously managed (some organizations have exceeded these limits).
- Overlapping use creates problems when interconnecting private local networks.
- Provider changes are limited to public edge device.

IPv6

- Private use address space defined as Unique Local Addresses (ULA). Allows each organization to autonomously manage as many /48 prefixes as they need for internal use. (65536 subnets per /48 prefix)
- 40 bit randomized field minimizes the potential for overlap when interconnecting private local networks.
- Router announcement simplifies global use prefix overlay for nodes that need to communicate externally.
- Provider changes can be limited to DHCP-PD server.



Global Address Pool Conservation



- **IPv4 – 32 bits**

  4,294,967,296 addresses

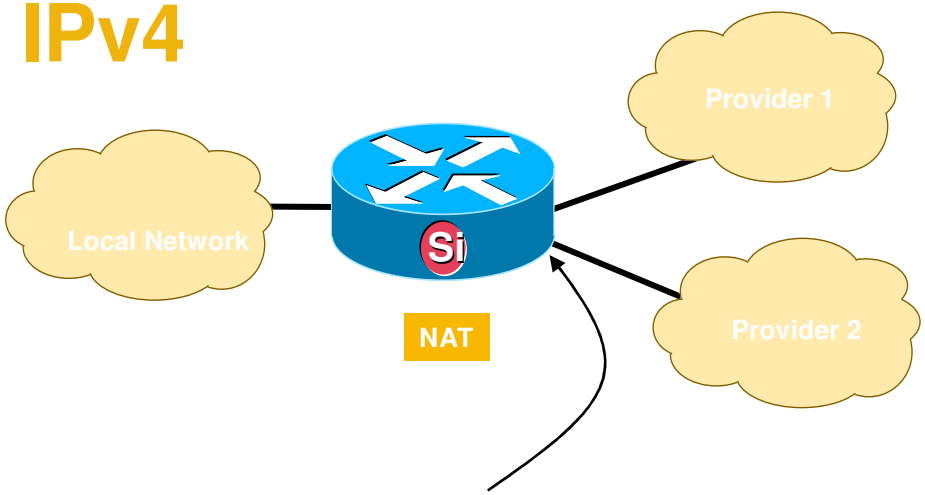
- **IPv6 – 128 bits**

  340,282,366,920,938,463,463,374,607,431,768,211,456

  addresses

Multi-homing & Renumbering

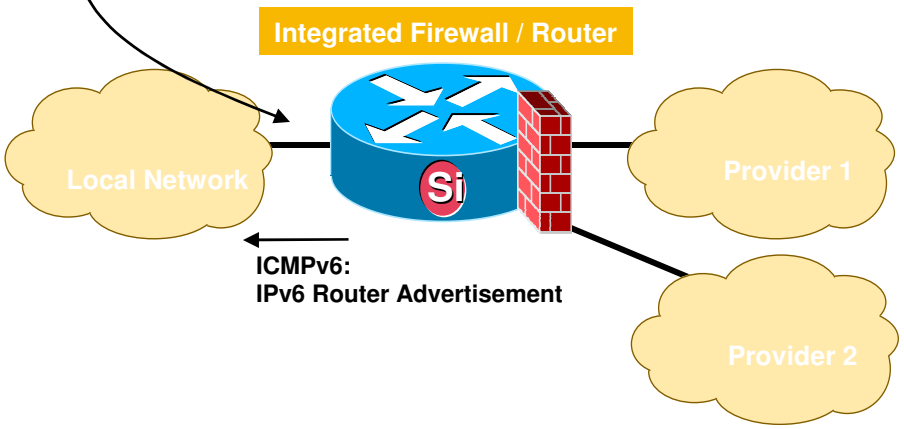
IPv4



- External interfaces on the NAT are the only points aware of the actual public addresses, so they can be changed with minimal effort.

IPv6

- Router Advertisement includes prefixes for any provider(s) the network manager wants that specific subnet to use. Hosts use longest match with dst address to select src.
- Transition between providers simplified as preferred-lifetime is set longer on the new, while the valid is left for the overlap duration on the old.



Wrap up

Security Wrap-up (1/2)

- '***Security***' is a function of perspective:

  content privacy is a security value to the end user

  content inspection is a security value to the network manager tasked with asset protection.

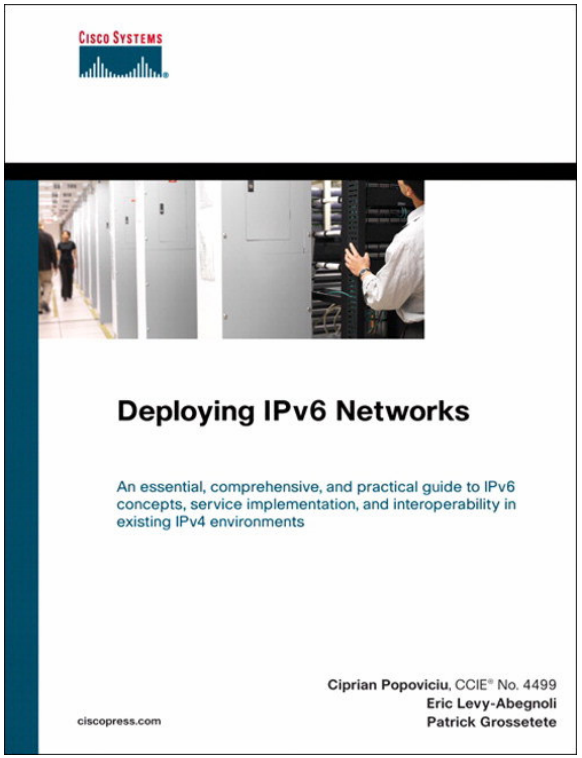
- In most environments the IP layer is not responsible for security, but stability and uniqueness at the IP layer are relied on by many security functions and mechanisms.
- Scanning is a futile effort in IPv6 networks, both for attackers and for network management tools.
- There are native IPv6 alternatives for the perceived beneficial functions of IPv4/NAT that avoid the application failures caused by address translation.

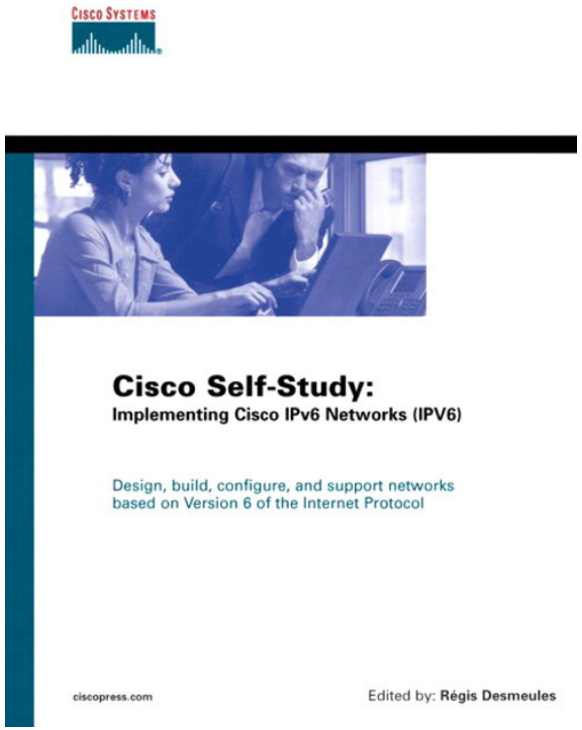
Summary Wrap-up (2/2)

- **IPv6 makes some things better, other things worse, and most things are just different, but no more or less secure:**
  - **Better**
    - **Automated scanning and worm propagation is harder due to huge subnets**
    - **Link-local addressing can limit infrastructure attacks**
    - **IPsec will be routinely available for use where keys exist**
  - **Worse**
    - **Lack of familiarity with IPv6 among operators**
    - **Multiple addresses per interface is a different concept**
    - **Immaturity of software in the next few years**
    - **Improperly deployed transition techniques**

Q and A

Cisco Press Books





More Information

- **CCO IPv6 - http://www.cisco.com/ipv6**
- **The ABC of IPv6**

  http://www.cisco.com/en/US/products/sw/iosswrel/ios_abcs_ios_the_abcs_ip_version_6_listing.html
- **IPv6 Application Notes**

  http://www.cisco.com/warp/public/732/Tech/ipv6/ipv6_techdoc.shtml
- **ICMPv6 Packet Types and Codes TechNote:**

  http://www.cisco.com/warp/customer/105/icmpv6codes.html
- **Cisco IOS IPv6 Product Manager – pgrosset@cisco.com**