North American IPv6 TASK FORCE

Next Generation

IPv6 CYBER-SECURITY & PRIVACY

October 17, BOSTON

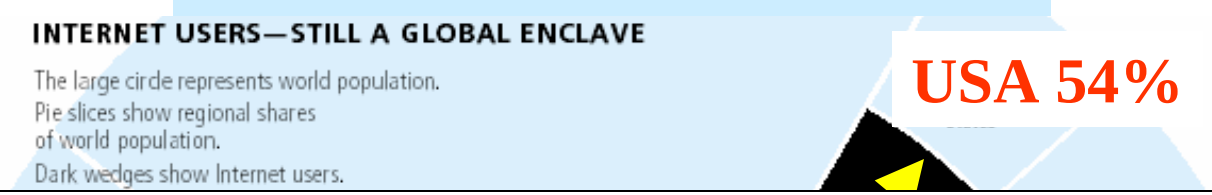
Recommendations of The North American IPv6 Task Force to:

***Richard Clarke**, Special Advisor to the President for Cyberspace Security, Critical Infrastructure Assurance Office (CIAO)*

Internet Generations

1G	2G	3G
NCP	IPv4	???
Pioneers	Innovators	EveryOne Everything
Email, FTP	WWW	Wireless, Streaming Media, P2P, VPN
TOURISTS		RESIDENTS
Gov. Internet	Public Internet	Global Internet
ARPANET	INTERNET	NEW INTERNET

UNEVEN DIFFUSION OF TECHNOLOGY



WORLD
8 %

PHONE NETWORK: 1.2 Billion -> 20%

INTERNET USERS: 0.5 Billion -> 8%

INTERNET HOSTS: 150 M Hosts -> 2%

NO e2e : NOBODY KNOWS !

Source: Human Development Report Office calculations based on data supplied by Nua Publish 2001 and UN 2001c.

COL David Shaddrix

Director, Enterprise Architecture

CIO/G-6

IPv6 Army Needs

For Distributed Networks supporting:

- Soldiers
- Weapons
- Sensors
- Command/Control
- Logistics

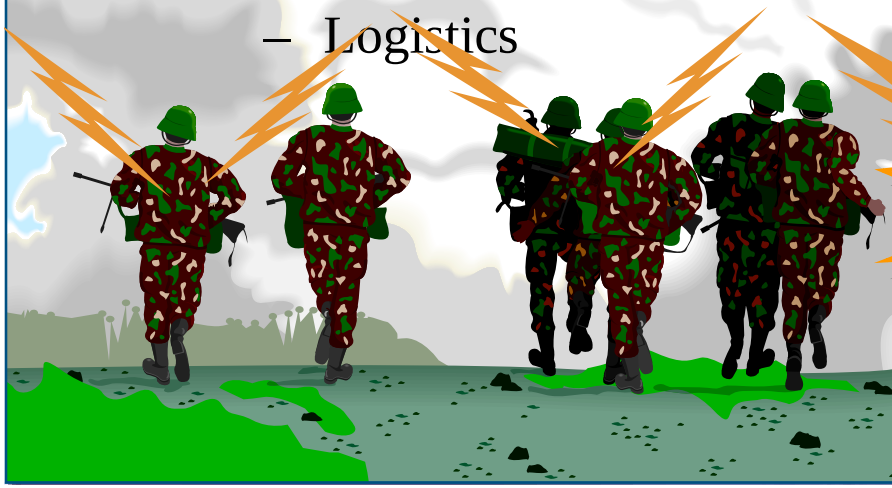
address space

Mobile IP

Security

Simplified Management

Interoperability



So When…?

The Internet

The IETF was divided over the Future of the Internet !

Garage Mentality

Band-Aids & Short-term Fixes!

Becoming Permanent Fixes!

Stovepipe Syndrome!

The Packet Switching Technology is Suffering!

The Future of the Internet

NAT EXPERTS created the NAT Roulette

Digital Divide

Instead of

Digital Ubiquity

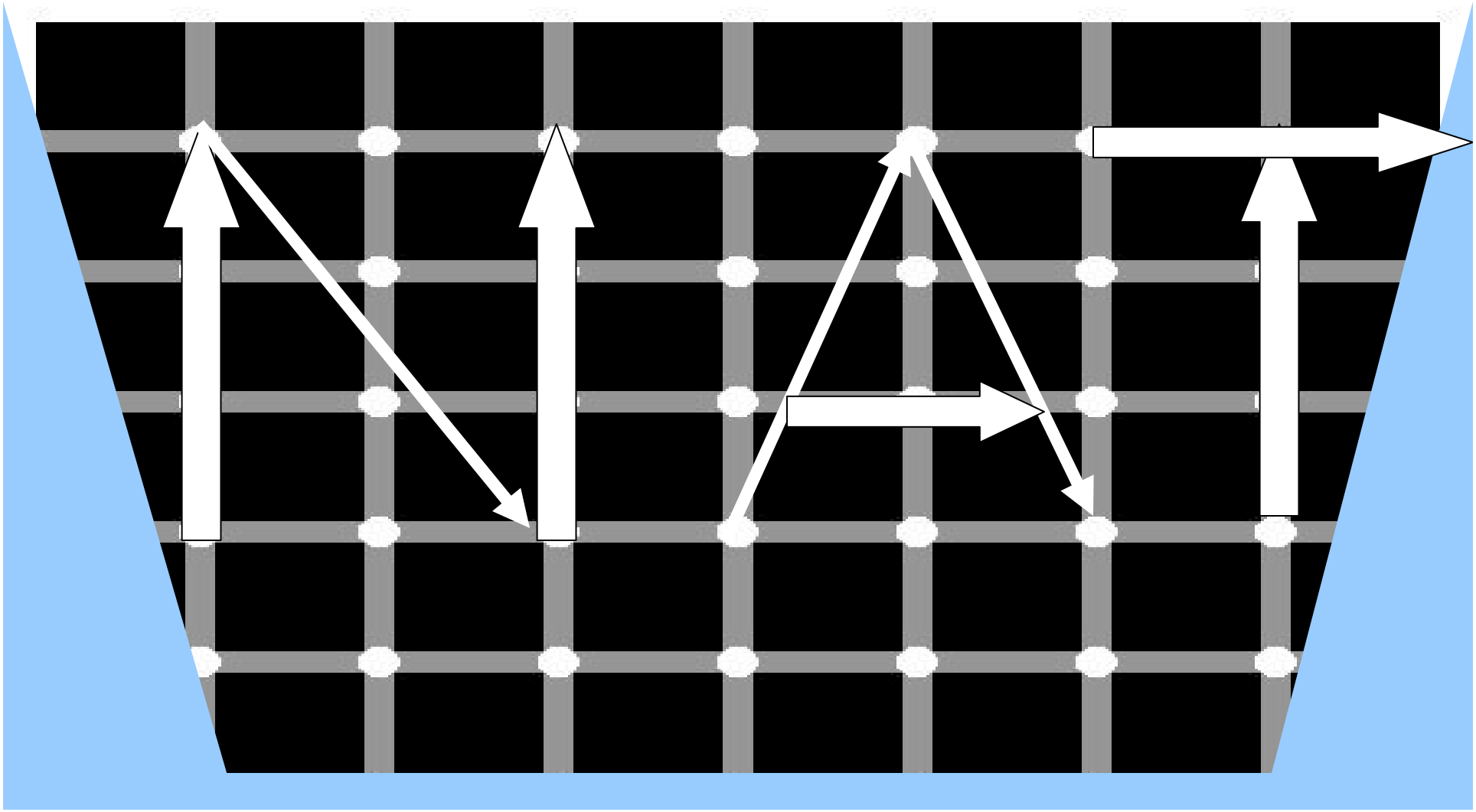
The Future of the Internet

NATs: Peeping Holes

Loss of End-2-End Transparency

The Future Cultlture

NATs: Holes for Shipworm Culture



Security History (Network)

- **None (we are all friends)**
  - **Early Internet users were researchers**
  - **Personal Computing revolution had yet to start**
- **1988: Uh Oh!**
  - **Internet Worm, first time Internet made television... in a bad way**
- **Today**
  - **Security threats abound, but security technology is an add-on**

Security is not Deployed

- **Internet is "edge" centric**
  - **Hard to add security in the middle**
  - **Firewalls attempt to add security "quasi" edge**
- **Security is Hard**
  - **It is a "negative deliverable"**

    You don't know when you have it, only when you have lost it!

Users don't ask for it, so the market doesn't demand it

Attacks Keep Getting Easier

Critical Security Enhancements Built-in in IPv6

!

IPv4 Address Space is Melting!

So, is Identitiy and therefore Security!

Identificate First Then Authenticate !!!

- **Identificate in order to Authenticate**
  - **Before authentification the source has to be identified**
  - **Identification is still done based on the IP Address**
  - **The IP address should be unique and global – Only IPv6 can provide such a critical resource.**
- **IPsec doesn‘t really work with NATs**
  - ***In an* IPv6 world, NATs are no longer needed.**
  - **The ability to get rid of NATs will remove a major current difficulty in deploying secure (encrypted) VPNs. We see many customer scenarios in which NAT traversal by IPSEC is a big issue today.**

Distinct Security Enhancements on IPv6

- **IPsec Mandated in IPv6, meaning ...**
  - **Yes, my peer supports IPsec**
  - **OS, Routers, Hosts have to support IPsec**
  - **New Security Models can be built**
- **Large Address Space for new models**
  - **Assign multiple addresses to a single host**
  - **Local address for local access and global addresse for Internet access.**
  - **Enhanced Filtering: One Application = One IPv6 Address**

Distinct Security Enhancements on IPv6

- More Robust IP Datagram
  - No more Fragmentation as in IPv4
  - More rigorous chaining of datagrams
  - Will better resist to DOS at IP/ICMP/TCP/UDP levels
    - No change at application layer
- Large Addresses, no doubt more routed addresses
  - Search for valid addresses and open services will take longer and will be more complex for the attacker to find.

Distinct Security Enhancements on IPv6

Address Switching

- Hosts can pick new addresses frequently.
  - Prevents tracking of usage.
- Using separate IP address per process group can simplify firewalls.

Distinct Security Enhancements on IPv6

Availability

- Multiple addresses per host help with multihoming.
- Autorenumbering permits switching providers without downtime.
- Autoconfiguration helps prevent mistakes.

Distinct Security Enhancements on IPv6

- **IPsec Encryption End-2-End Is Integrated in IPv6**
  - **Generalising from this, the restoration of end to end addressing will allow not only IPSEC but various other forms of end to end security at session level (more cleanly than with SSL via NAT) and this will allow us to overcome the main problems with the firewall security model of today**

It‘s Acrobatic!

e2e Communication

e2e Security

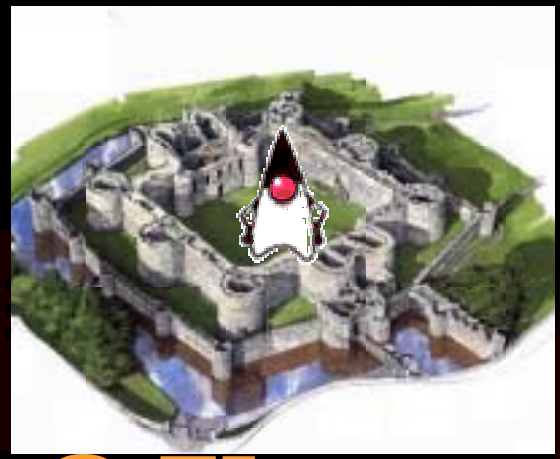
The Road Warrier

Is A Clown!

Internet Security and Privacy with IPv6 -An

Folks, Just Surfing with Random Address for Privacy

IPv6 Firewall



IPv6 Firewall

Steel Pipe

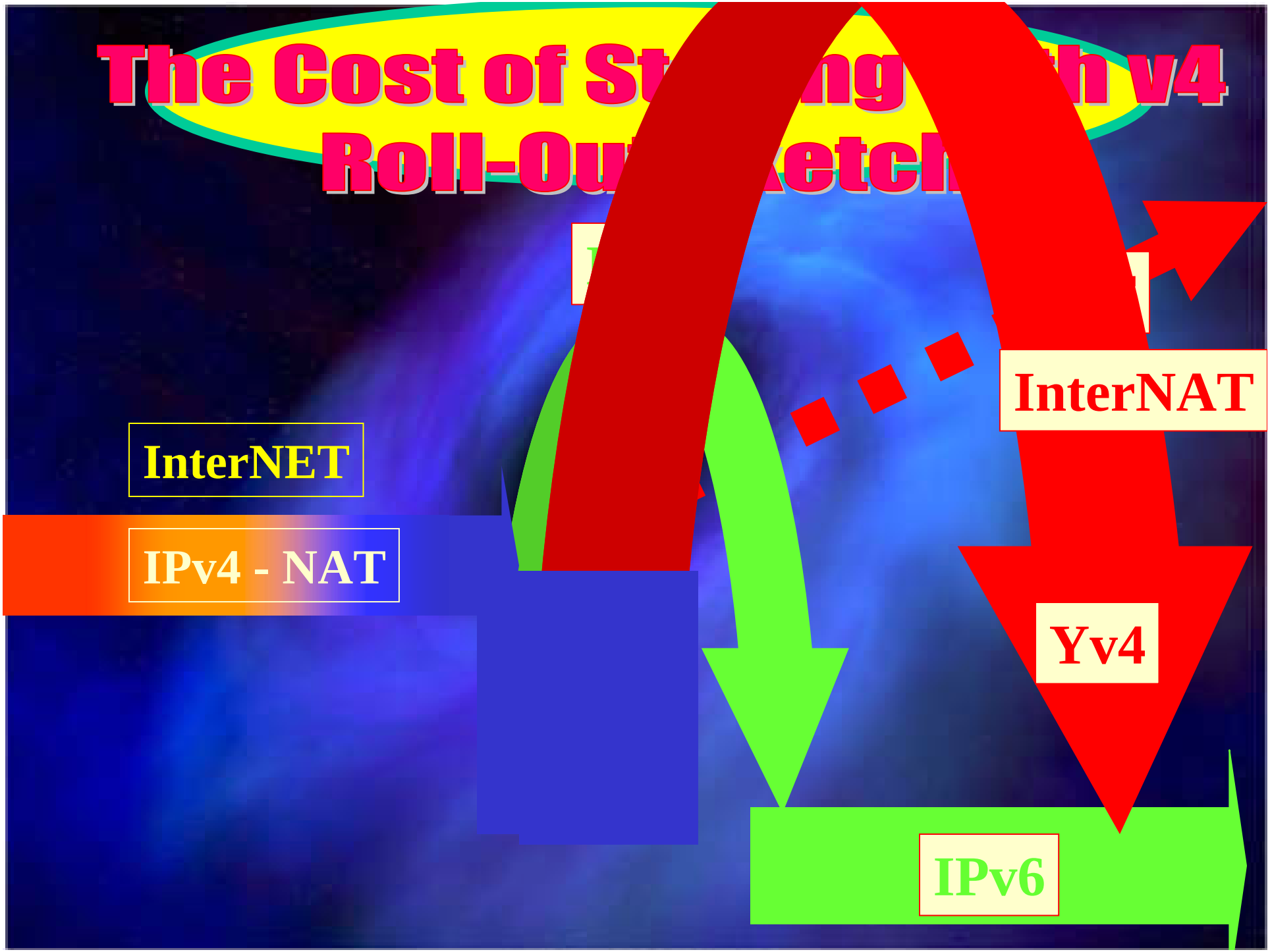
IPsec-o-IPv6

v6 - IPsec Roadmap Scenaria

	Scenario 1	Scenario 2	
IPv6 Deployment	Successful	Complete Failure	
Address Transparency	Restored e-2-e	Recycling IP Addresses	Exhaustion NAT-over-NAT
IPsec	e-2-e works	Limited	Broken
FOG	Clears!	Noticeable Fog	Permanet Thick Fog
Issues	Intranet, Proxies & Firewalls may remain	Generalised use of NAPT, RSIP?	NATs between even ISPs

INTERNET

Largest Man-Made Digital FOG!


InterNAT
InterNET
IPv4 - NAT
Yv4
IPv6

***Richard Clarke**, Special Advisor to the President for Cyberspace Security, Critical Infrastructure Assurance Office (CIAO)*

Recommendations of ISOC/IAB/IETF INET 2002 June 19

Vint Cerf
Scott Bradner
Fred Baker
Lynn St. Amour
Leslie Daigle
Harald Alvestrand
Brian Carpenter

- - the proliferation of NATs makes end to end encryption or authentication difficult, meaning we need to actively deploy IPv6 in routers and end nodes to eliminate that issue. Please specify IPv6 support on all future procurements (shades of GOSIP)

Recommendations of ISOC/IAB/IETF INET 2002 June 19

Richard Clarke

- - while export controls have loosened, Cisco and others are still forced to distinguish between US and non-US versions of code, around crypto.
- It was suggested that USG simply drop all export restrictions on crypto code using the new Advanced Encryption Standard
- - we still don't know how to deploy a global Public Key Infrastructure, making global IPSEC privacy/authentication difficult (research funding)
- - ditto secure/scalable/quickly-converging

Societal Challenges

- **Shift from ISP to .. Personal ISP**
- **Bring Trust to Internet**
  - Banking
  - Government (evoting)
  - E-commerce

- **Security-aware Society**
- **Security Divide! (Security Haves and Have-Nots)**
- **Security for EveryOne & Everything**

Supporting Slides on Security & Privacy Enhancements Built-in in IPv6

Some Internet Security Protocols

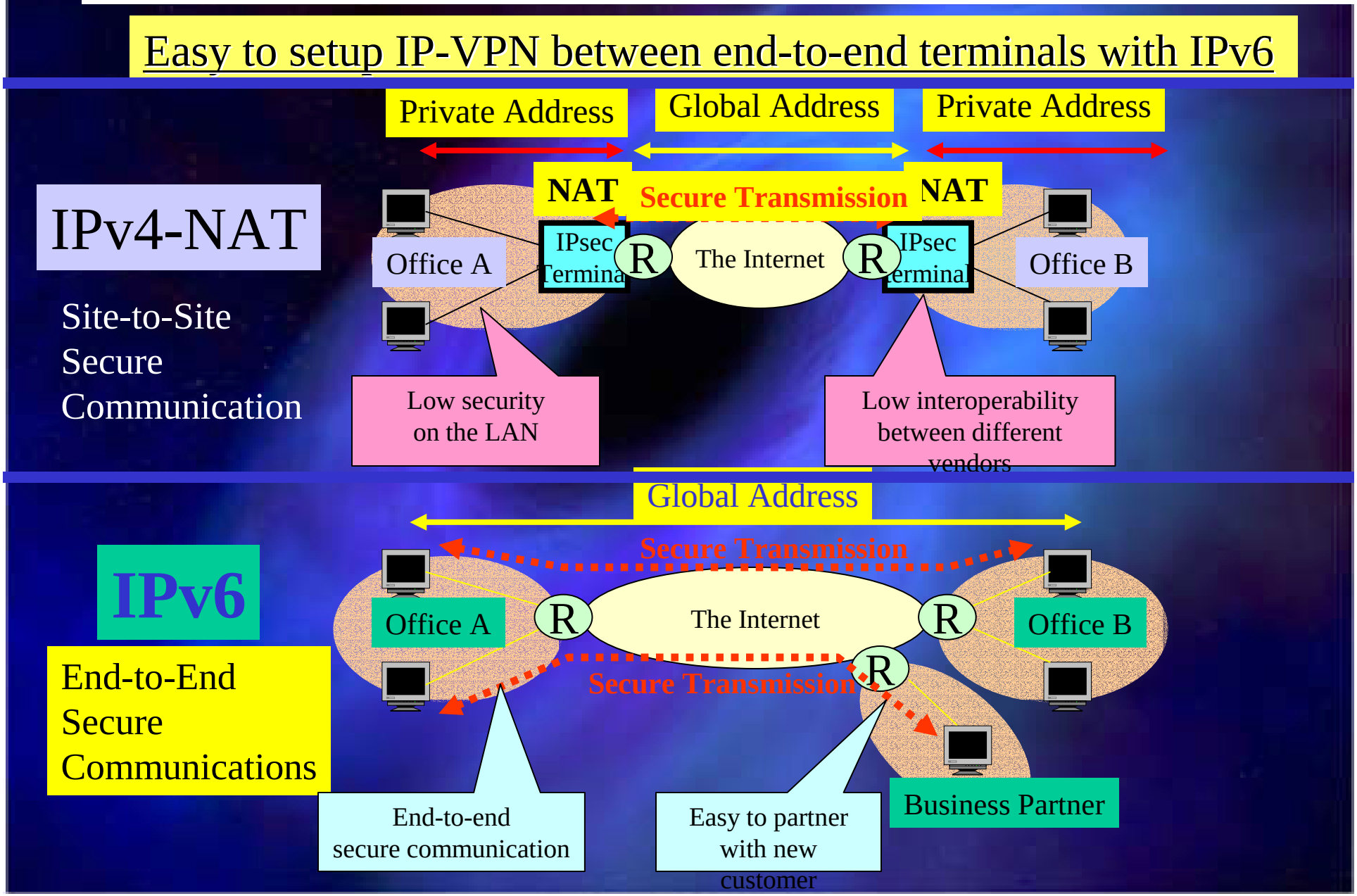
Application	- e-mail + PGP, S/MIME
Transport	- Primarily Web + SSL/TLS + Secure Shell (SSH)
Network	+ IPsec - MIPv6 Routing security
Infrastructure	+ DNSsec - PKI + SNMPv3 security

You are here

- Political
- Economic
- Application
- Presentation
- Session
- Transport
- Network
- Link
- Physical

Large-Scale End-to-End Security

Easy to setup IP-VPN between end-to-end terminals with IPv6



IPsec

- Protects all upper-layer protocols.
- Requires no modifications to applications.
  - But smart applications can take advantage of it.
- Useful for host-to-host, host to gateway, and gateway-to-gateway.
  - Latter two used to build VPNs.

Doesn’t IPsec work with IPv4?

- Yes, but…

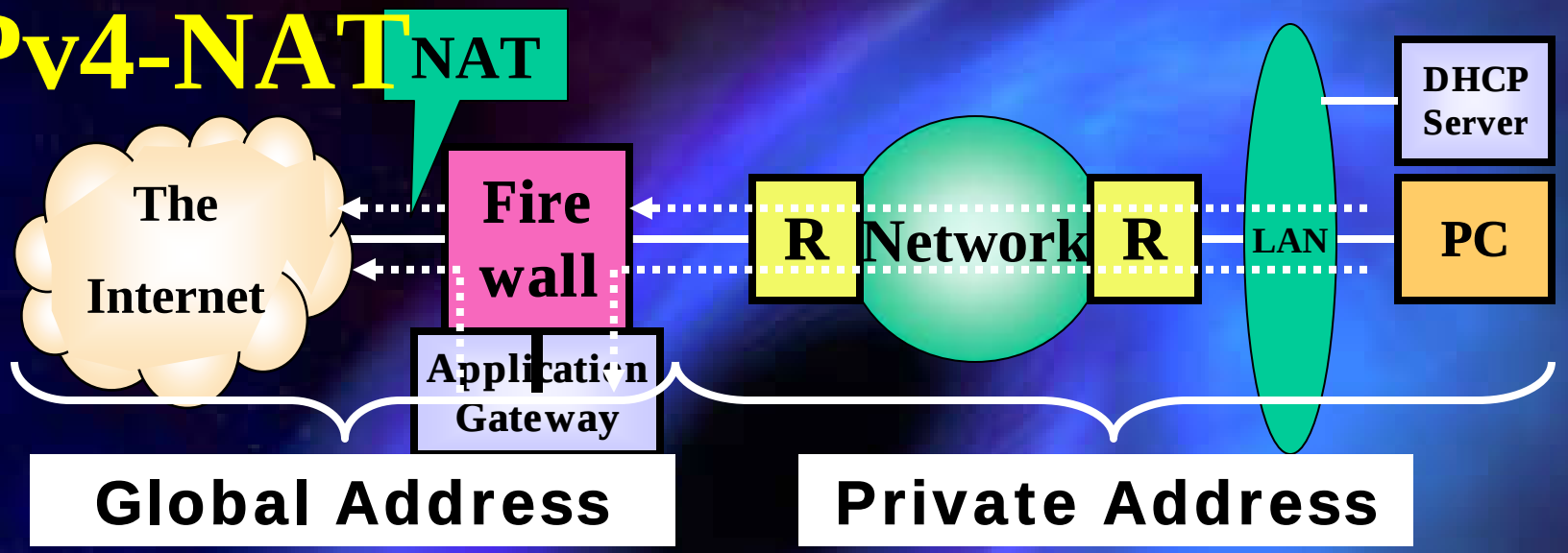
- It isn’t standard with v4.
- Few implementations support host-to-host mode.
  - Even fewer applications can take advantage of it.

No NATs

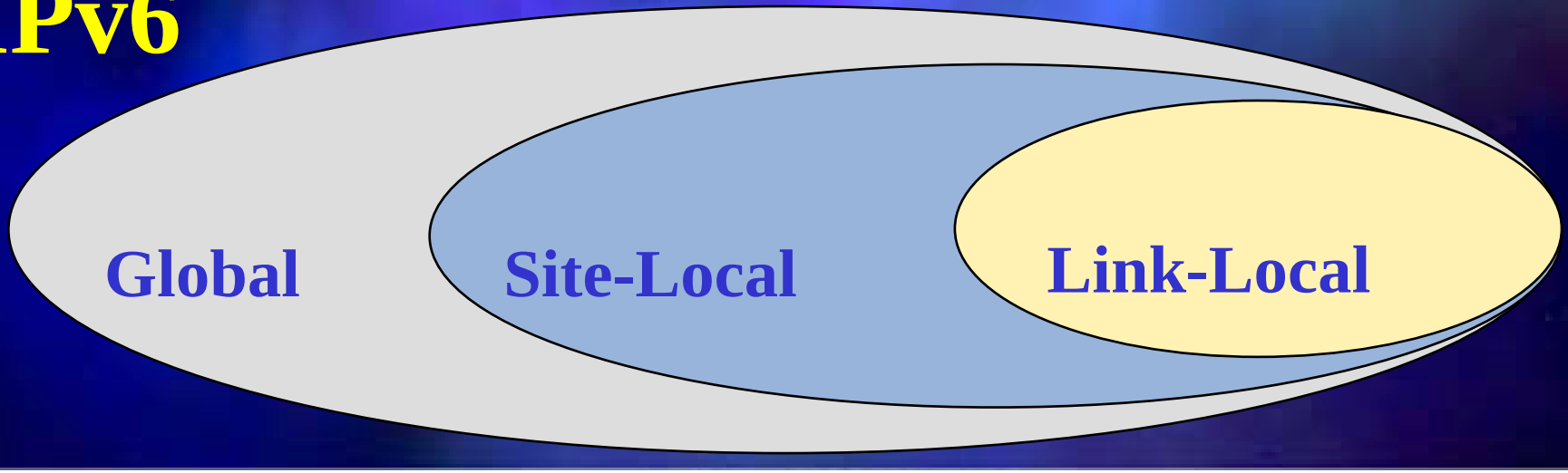
- NATs break IPsec, especially in host-to-host (P2P) mode.
- With no NATs needed, fewer obstacles to use of IPsec.
- Note carefully: NATs provide no more security than an application-level firewall.

PRIVACY: Addressing Model

IPv4-NAT



IPv6



Configuring Interface IDs

Several choices for configuring the interface ID of an address:

- manual configuration (of interface ID or whole addr)
- DHCPv6 (configures whole address)
- automatic derivation from 48-bit IEEE 802 address or 64-bit IEEE EUI-64 address
- pseudo-random generation (for client privacy)

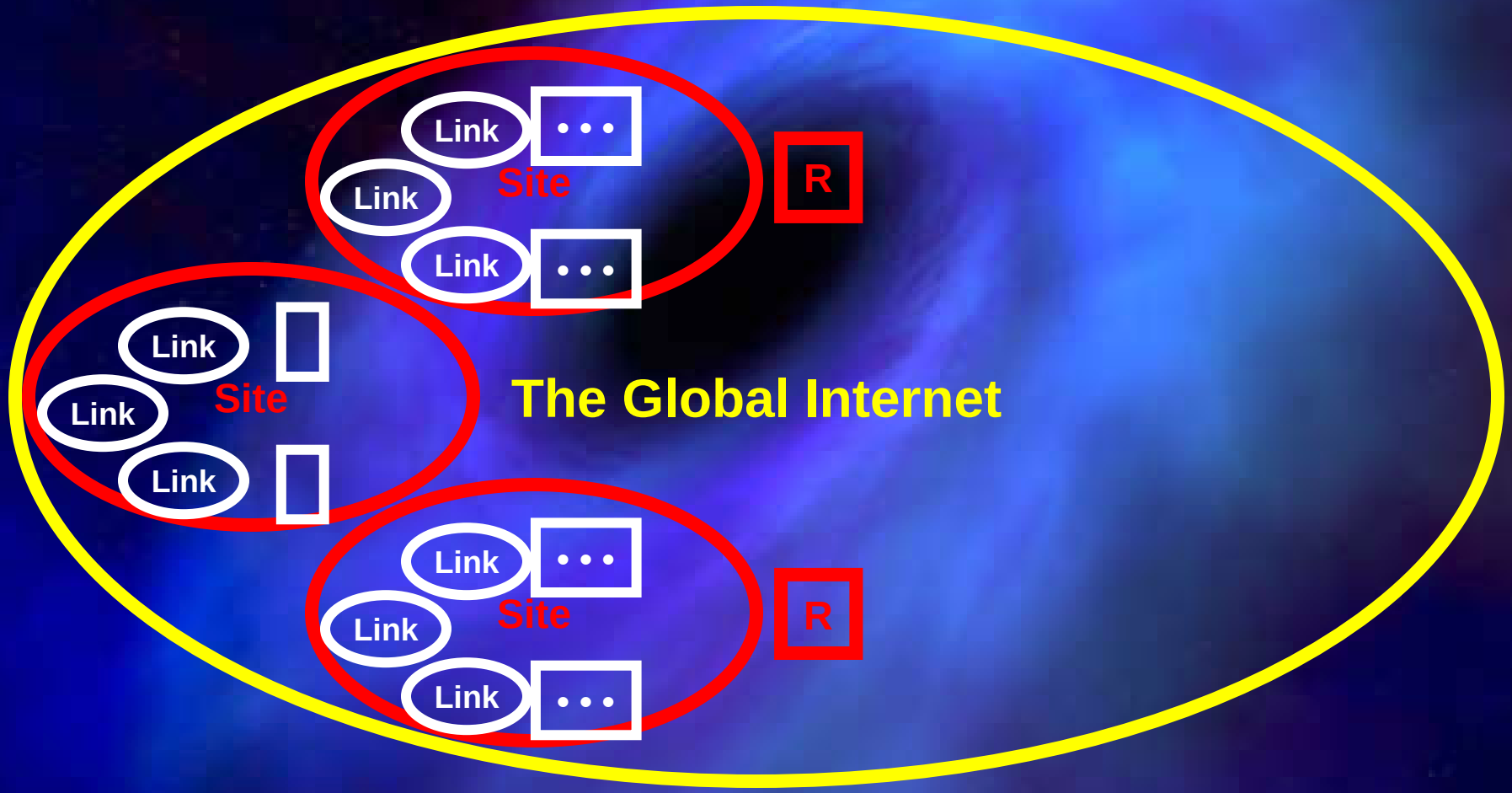
the latter two choices enable “serverless” or “stateless” autoconfiguration, when combined with high-order part of the address learned via Router Advertisements

Non-Global Addresses

- IPv6 includes non-global addresses, similar to IPv4 private addresses (“net 10”, etc.)
- a topological region within which such non-global addresses are used is called a zone
- zones come in different sizes, called scopes (e.g., link-local, site-local,…)
- unlike in IPv4, a non-global address zone is also part of the global addressable region (the “global zone”)

  => an interface may have both global and non-global addresses

Address Zones and Scopes



Each oval is a different zone; different colors indicate different scopes

Authentication Challenges

- **There is username/password**
- **And then there is everything else**
  - SecurID
  - Smart Card
  - ATM Card
  - Biometrics
    - The “password” you cannot change...
    - There are also “safety” hazards...

Recommendations of ISOC/IAB/IETF INET 2002 June 19

Richard Clarke

- - ditto secure/scalable/quickly-converging global and local routing
- - ditto on intrusion detection as a service provider service (detecting and mitigating attacks of various kinds)

Ciphers and Networks

- **Traditional Cipher: Transforms data using a key. Same key is used to "undo" the cipher and obtain original contents**
- **You don't design your own, use available and accepted ciphers**
  - **DES was U.S. National Standard for over 25 years**
    - **DES is still "good" but key length is too short for modern use.**
  - **AES: The new Advanced Encryption Standard**
    - **Longer keys, should be strong for 30 years or so.**
  - **Other alternatives: 3DES,Blowfish, CAST, IDEA, DESX to name a few**