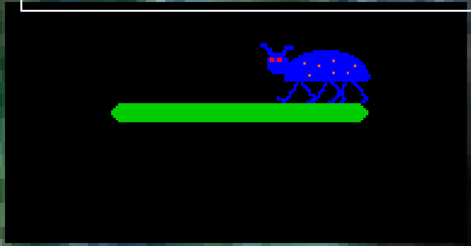
Security & Privacy with IPv6

’’Taming the World ”

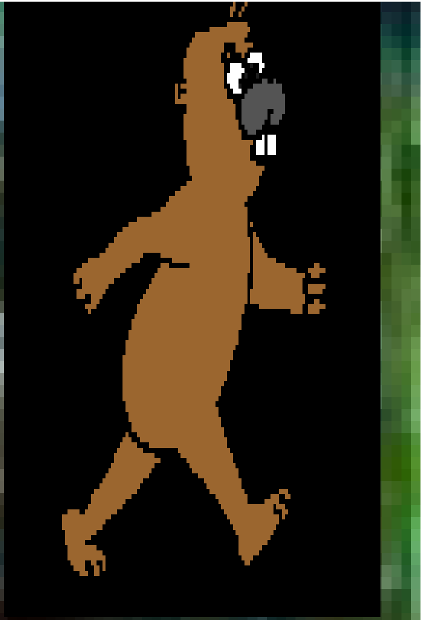
The Internet‘s Serious Enemies

They are called Security,,,, and!

SW Bugs: OS,..



Governments



Privacy

Hackers

Viruses

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

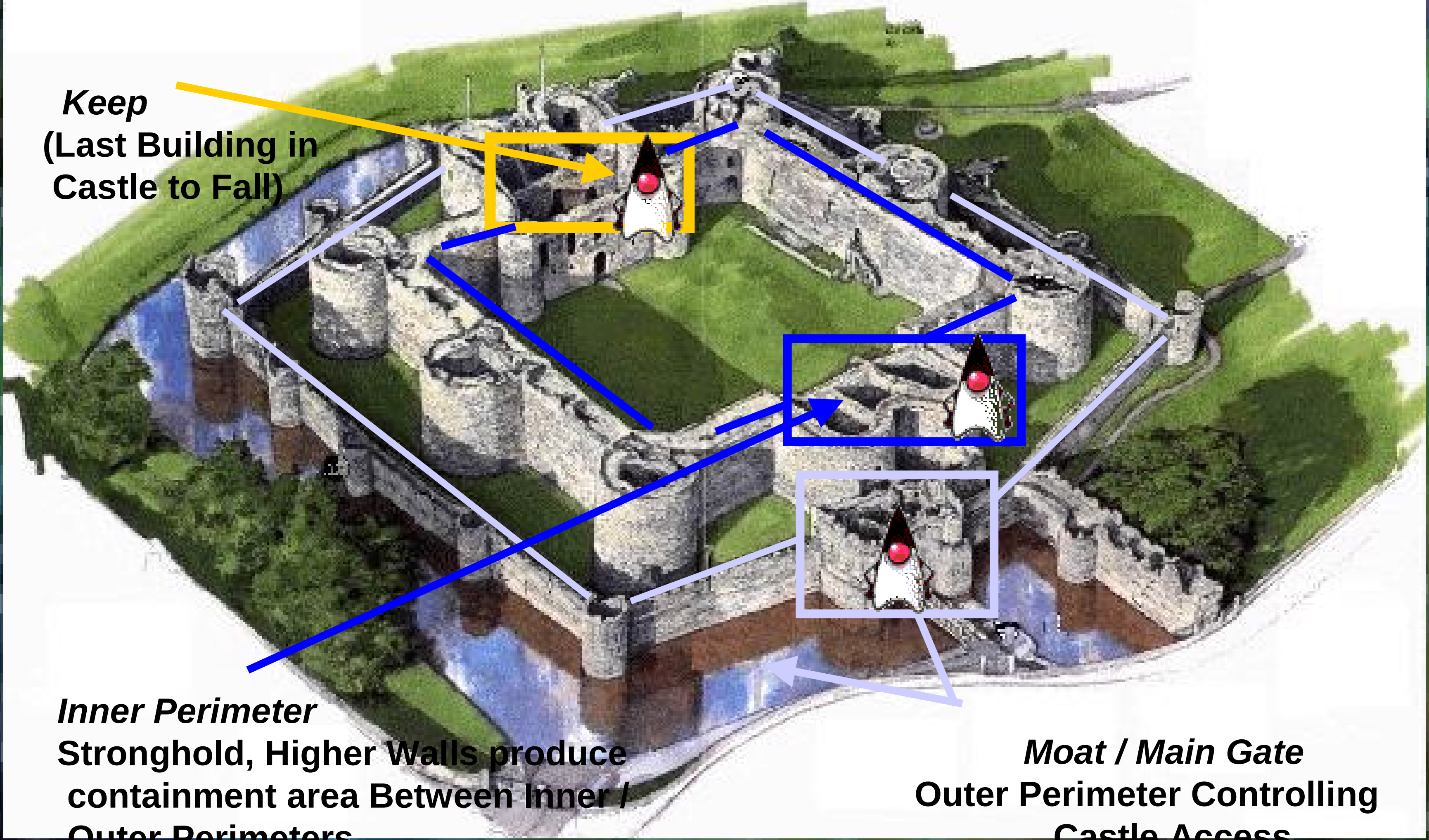
- Internet is “edge” centric
  - Hard to add security in the middle
  - Firewalls attempt to add security “quasi” edge

- 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

Internet Security Analogy

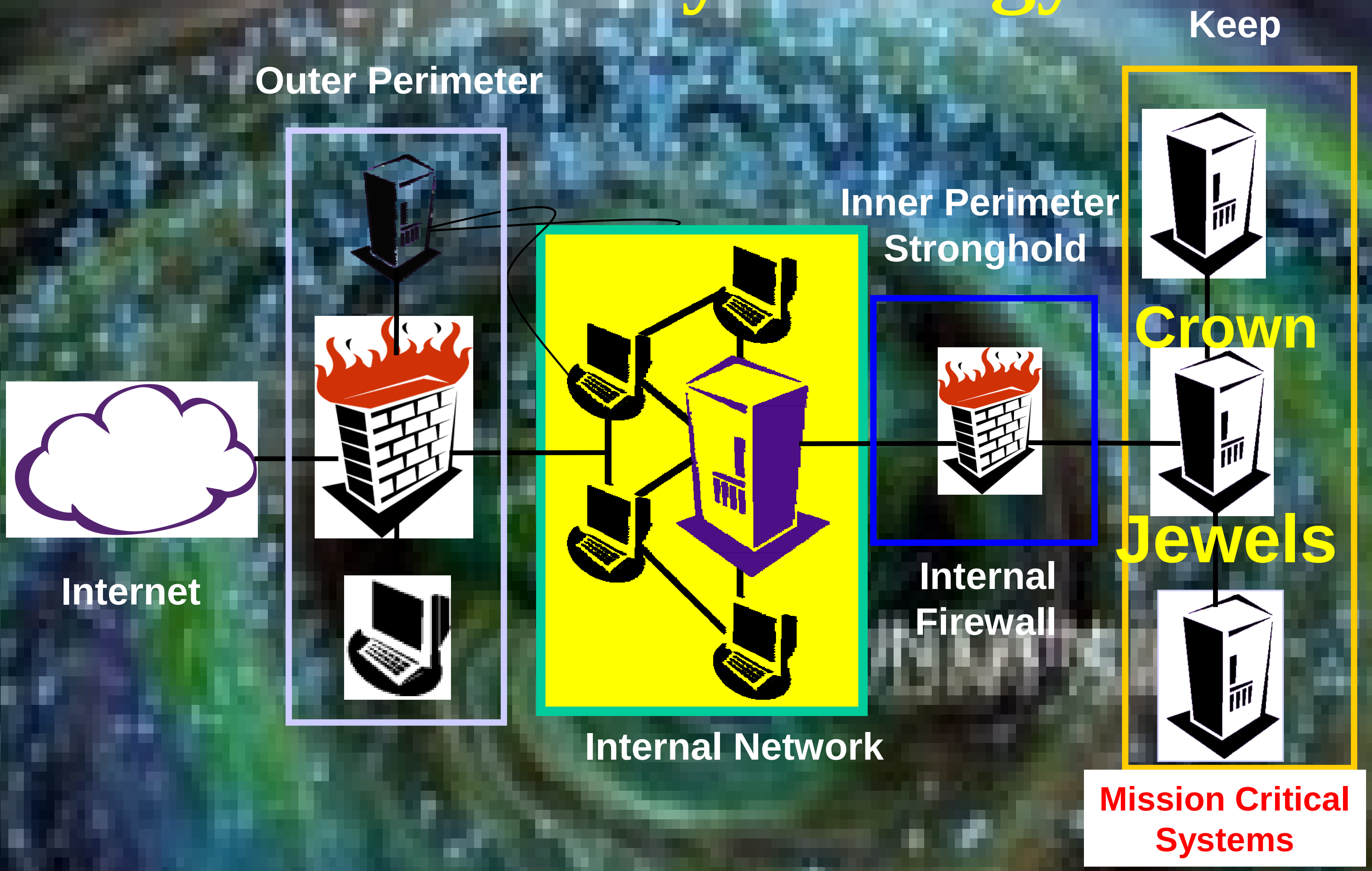


Keep
(Last Building in Castle to Fall)

Inner Perimeter
Stronghold, Higher Walls produce containment area Between Inner / Outer Perimeters

Moat / Main Gate
Outer Perimeter Controlling Castle Access

Internet Security Analogy



Keep

Outer Perimeter

Inner Perimeter Stronghold

Crown Jewels

Internet

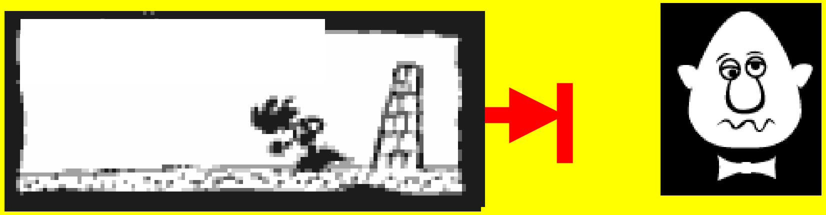
Internal Firewall

Internal Network

Mission Critical Systems

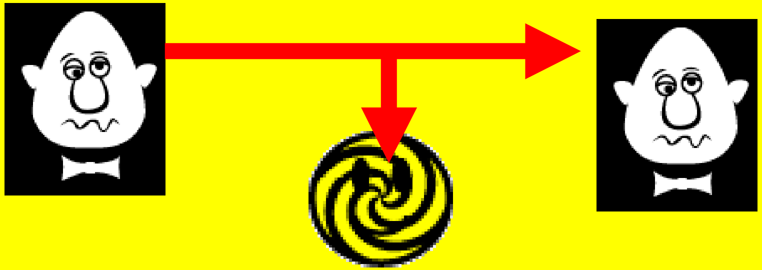
Internet Attacks

Denial of Service



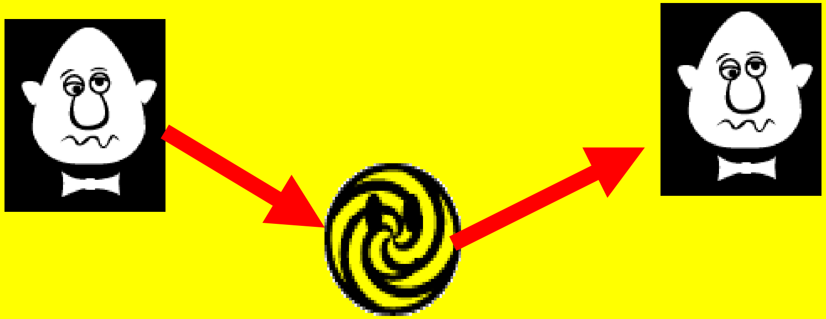
Brute Force, Hidden,...

Eavesdropping (secrecy)



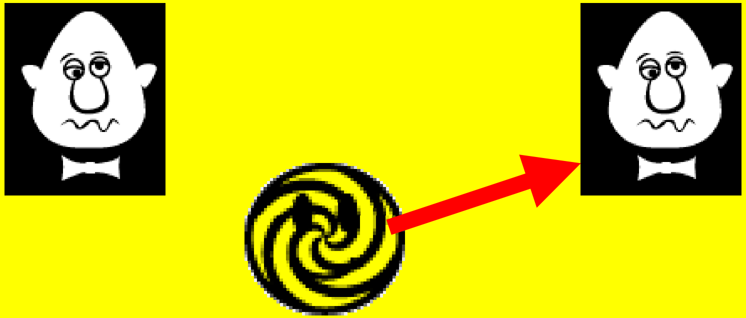
Wiretapping, Trojan Horse

Modification (Integrity)



Man-in-the M., Viruses, ...

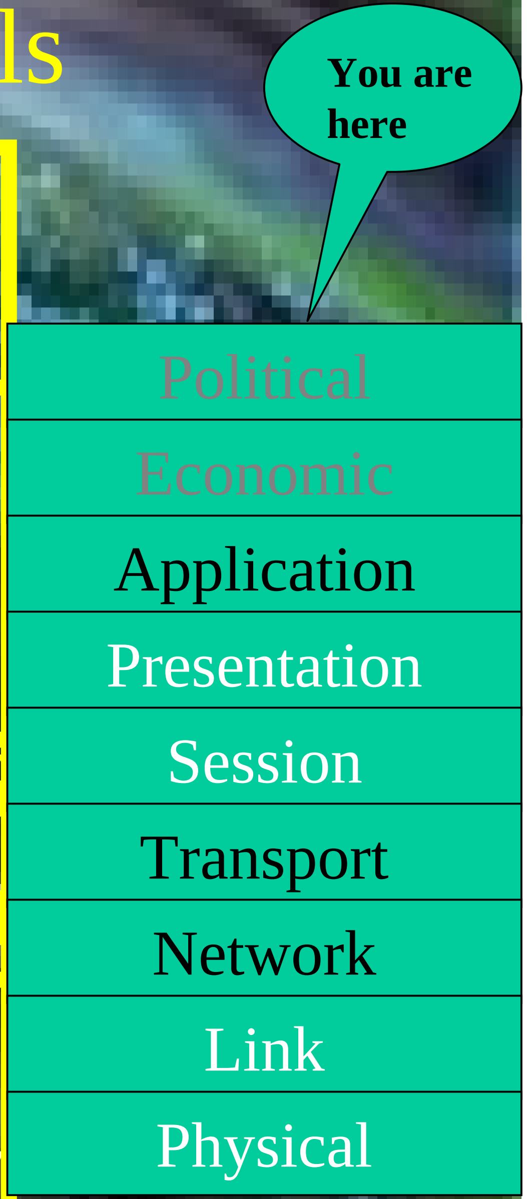
Fabrication (Authentication)



Masquerading,...

Some Internet Security Protocols

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



You are here

Political

Economic

Application

Presentation

Session

Transport

Network

Link

Physical

Internet Security and Privacy with IPv6 -Analogy

Folks, Just Surfing with Random Address for Privacy

Steel Pipe

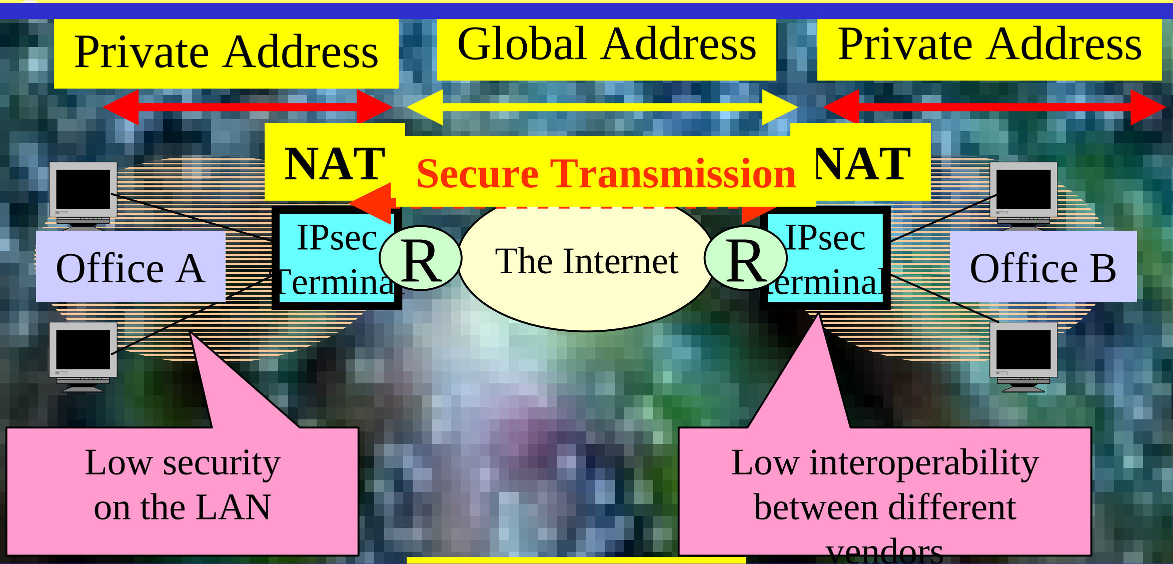
IPsec-o-IPv6

Large-Scale End-to-End Security

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

IPv4-NAT

Site-to-Site
Secure
Communication



Private Address

Global Address

Private Address

NAT

Secure Transmission

NAT

Office A

IPsec
Termina

R

The Internet

R

IPsec
erminal

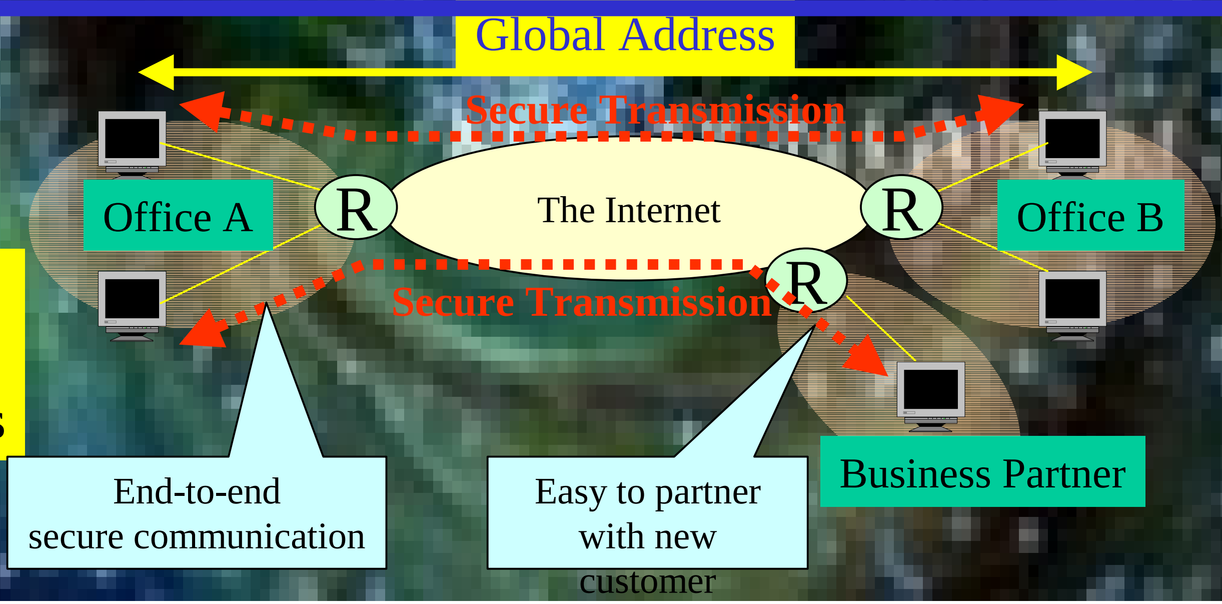
Office B

Low security
on the LAN

Low interoperability
between different
vendors

IPv6

End-to-End
Secure
Communications



Global Address

Secure Transmission

Office A

R

The Internet

R

Office B

R

Secure Transmission

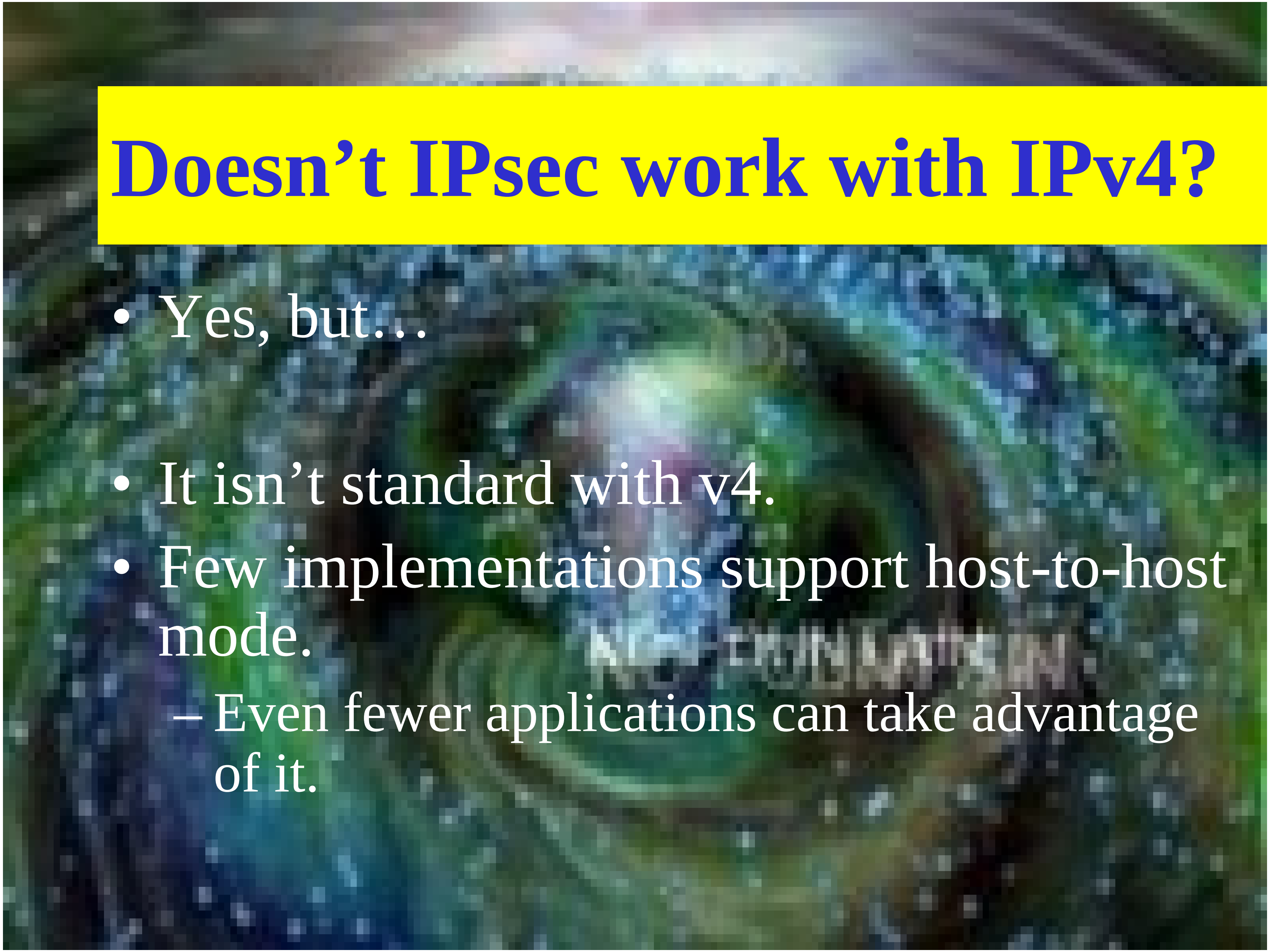
Business Partner

End-to-end
secure communication

Easy to partner
with new
customer

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.**



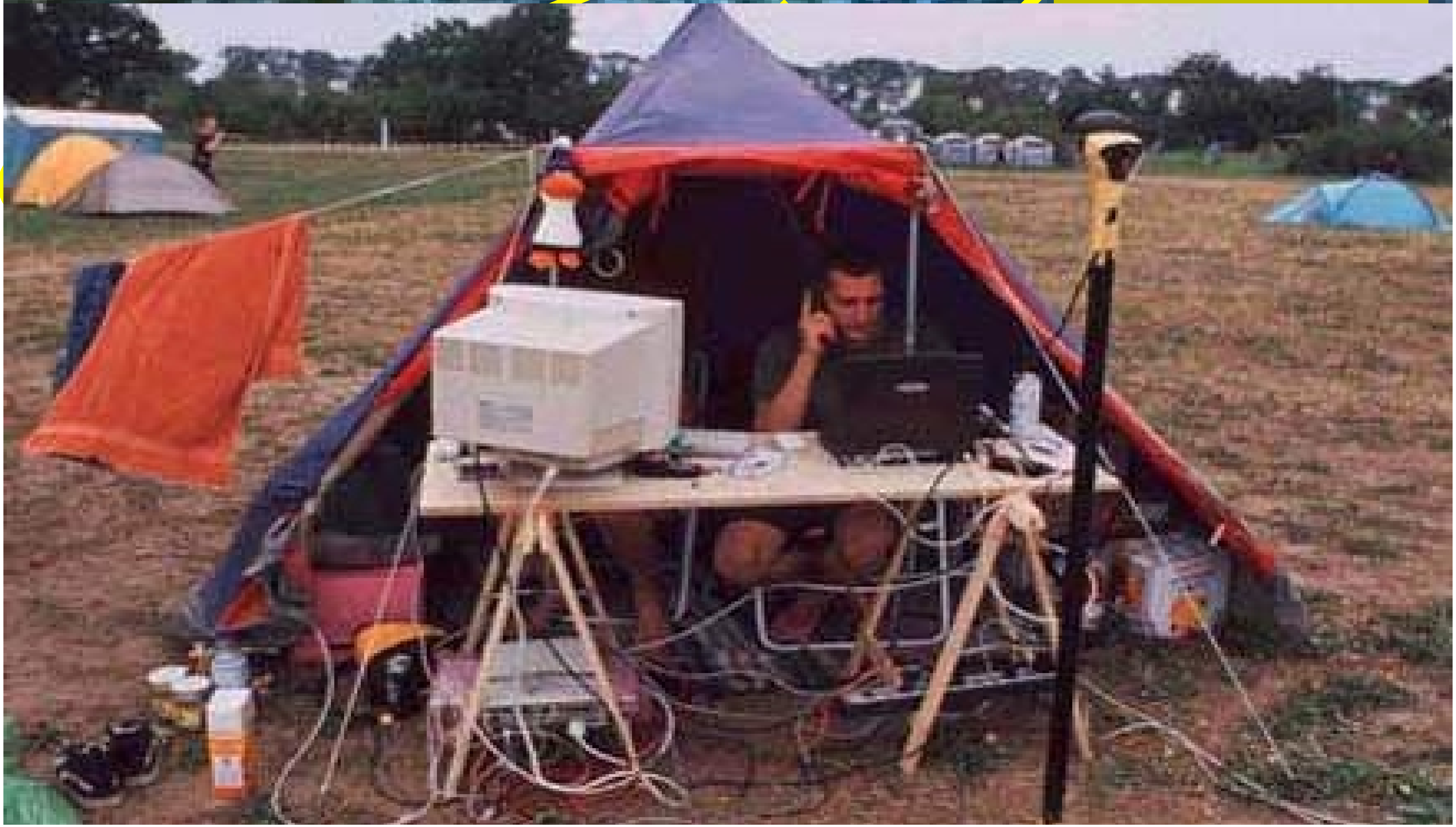
Doesn’t IPsec work with IPv4?

- 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

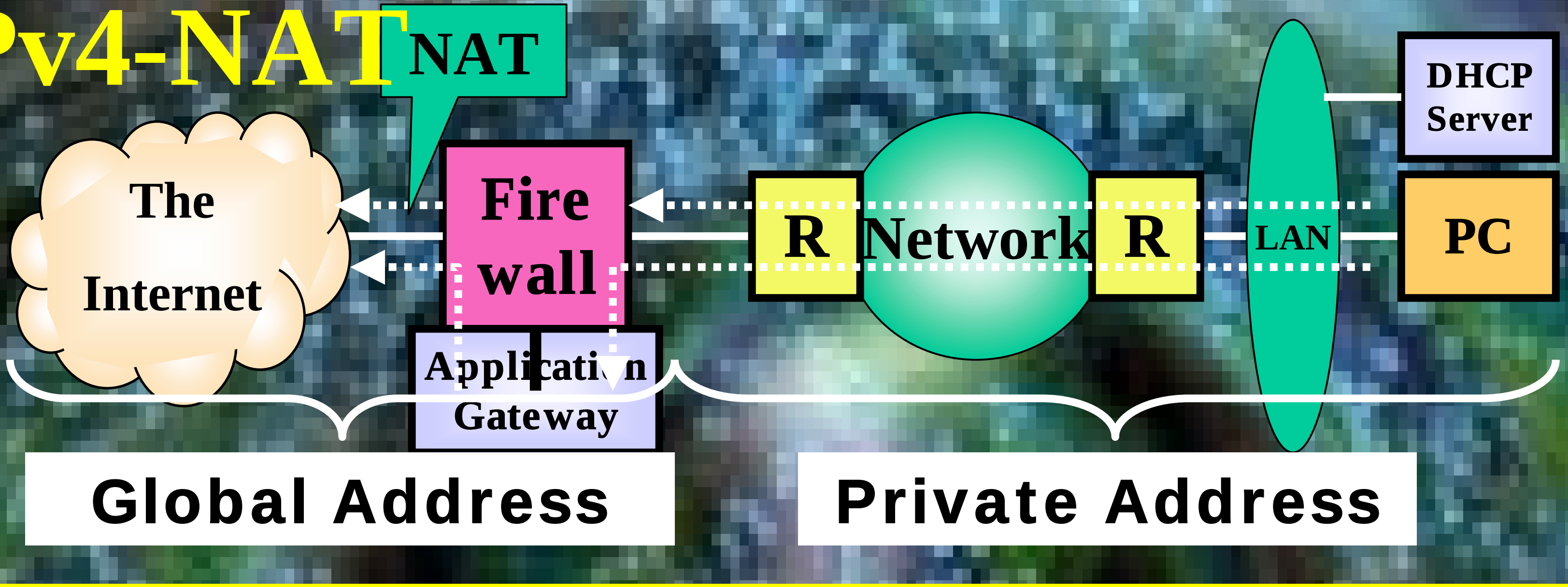
- NATs break IPsec, especially in host-to-host (P2P) mode.
- With no NATs needed, fewer obstacles to use of IPsec.
- Note carefully: NATs provide no more security than an application-level firewall.

It‘s Acrobatic!

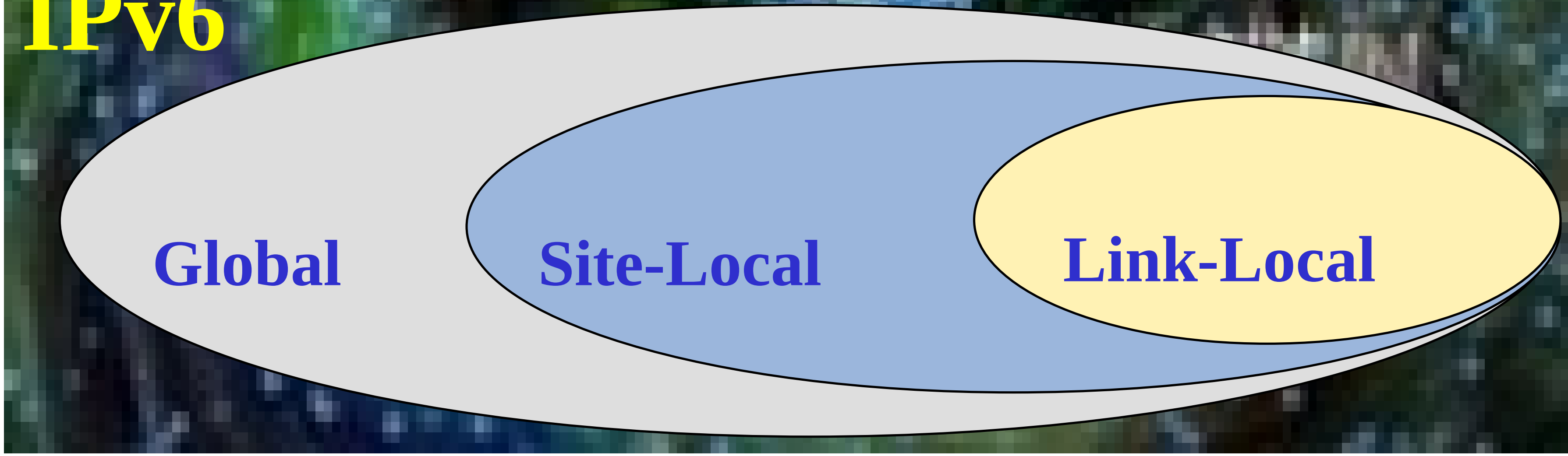


PRIVACY: Addressing Model

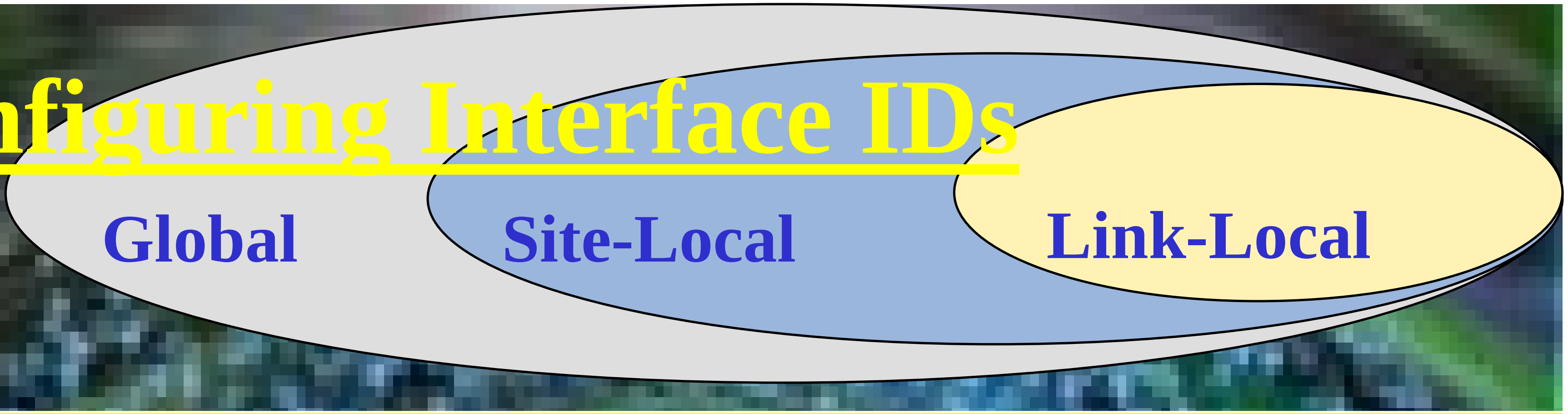
IPv4-NAT



IPv6



Configuring Interface IDs

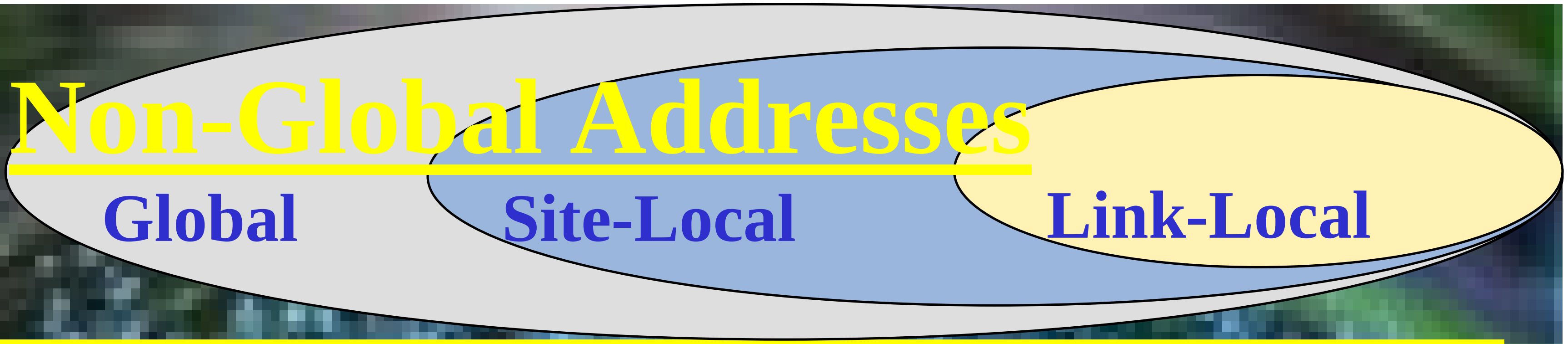


Several choices for configuring the interface ID of an address:

- 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

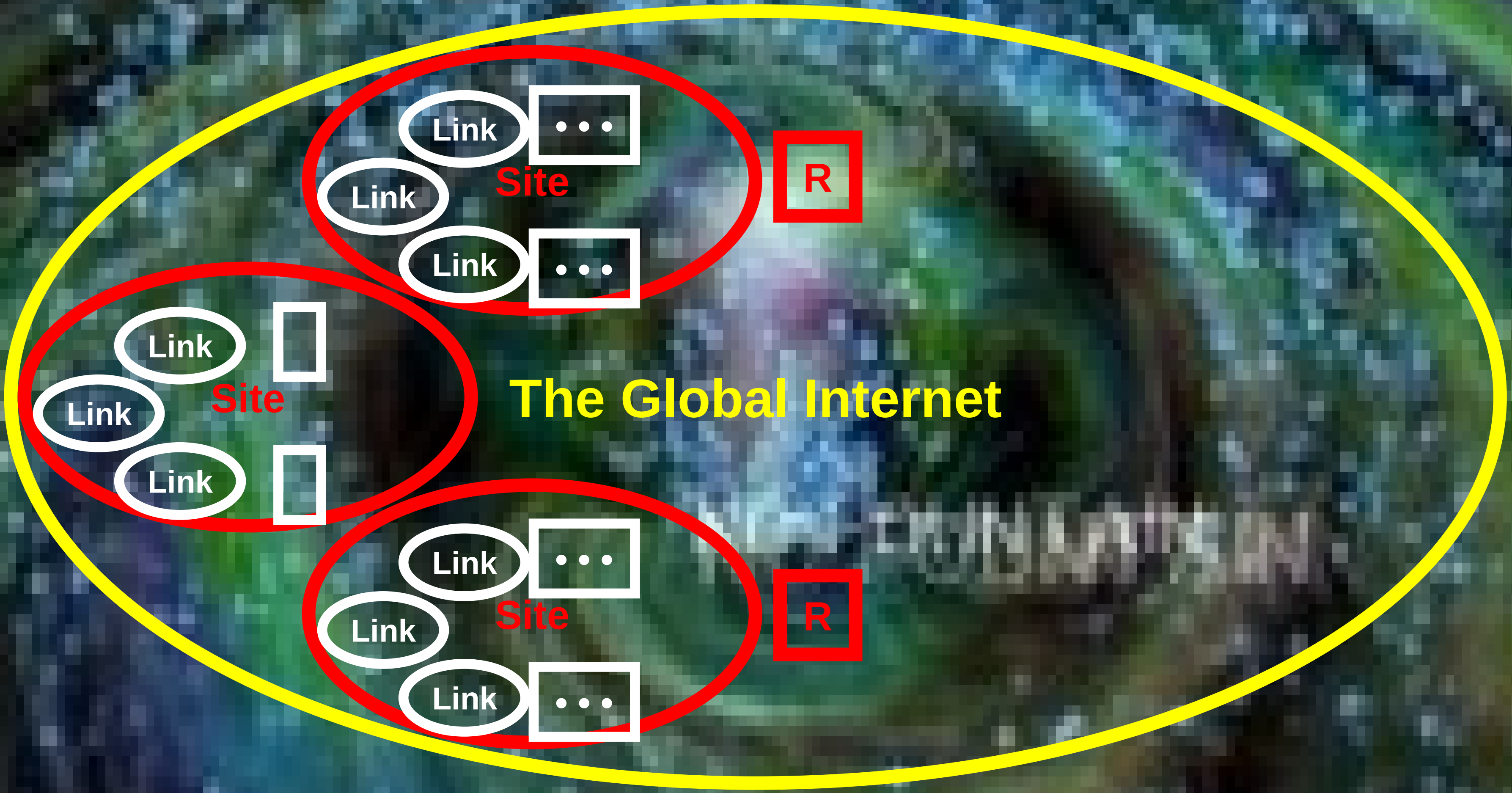
Non-Global Addresses



- 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

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

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

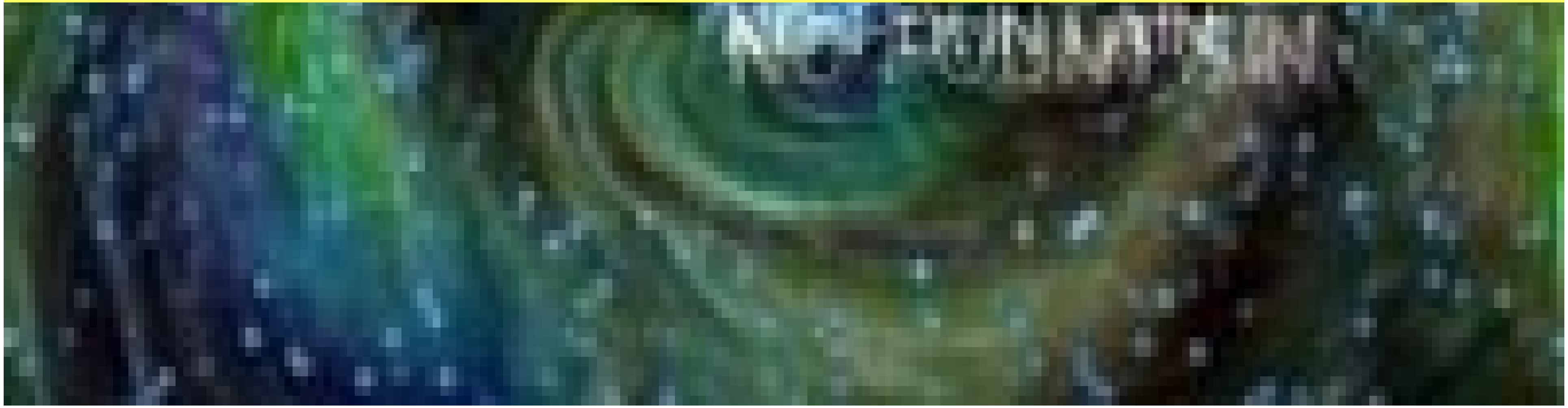
Richard Clarke

- - 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

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)



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**

Conclusions

- IPv6 mandates and enables an important improvement in security.
- Much of the improvement comes from standard, usable, IPsec.
- The very large address space may provide for other, innovative security mechanisms.