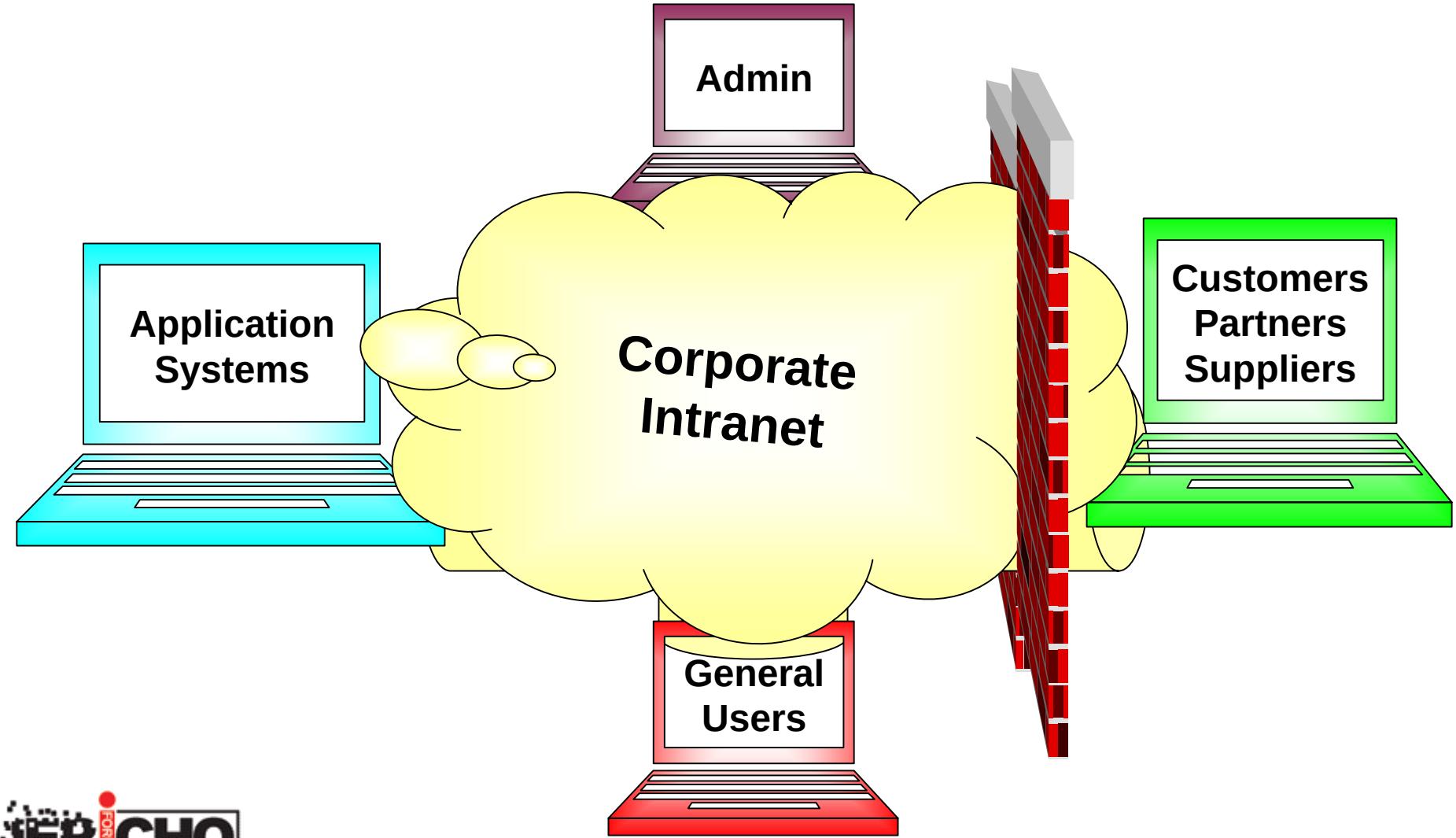
De-Perimeterisation and the Jericho Forum Viewpoint

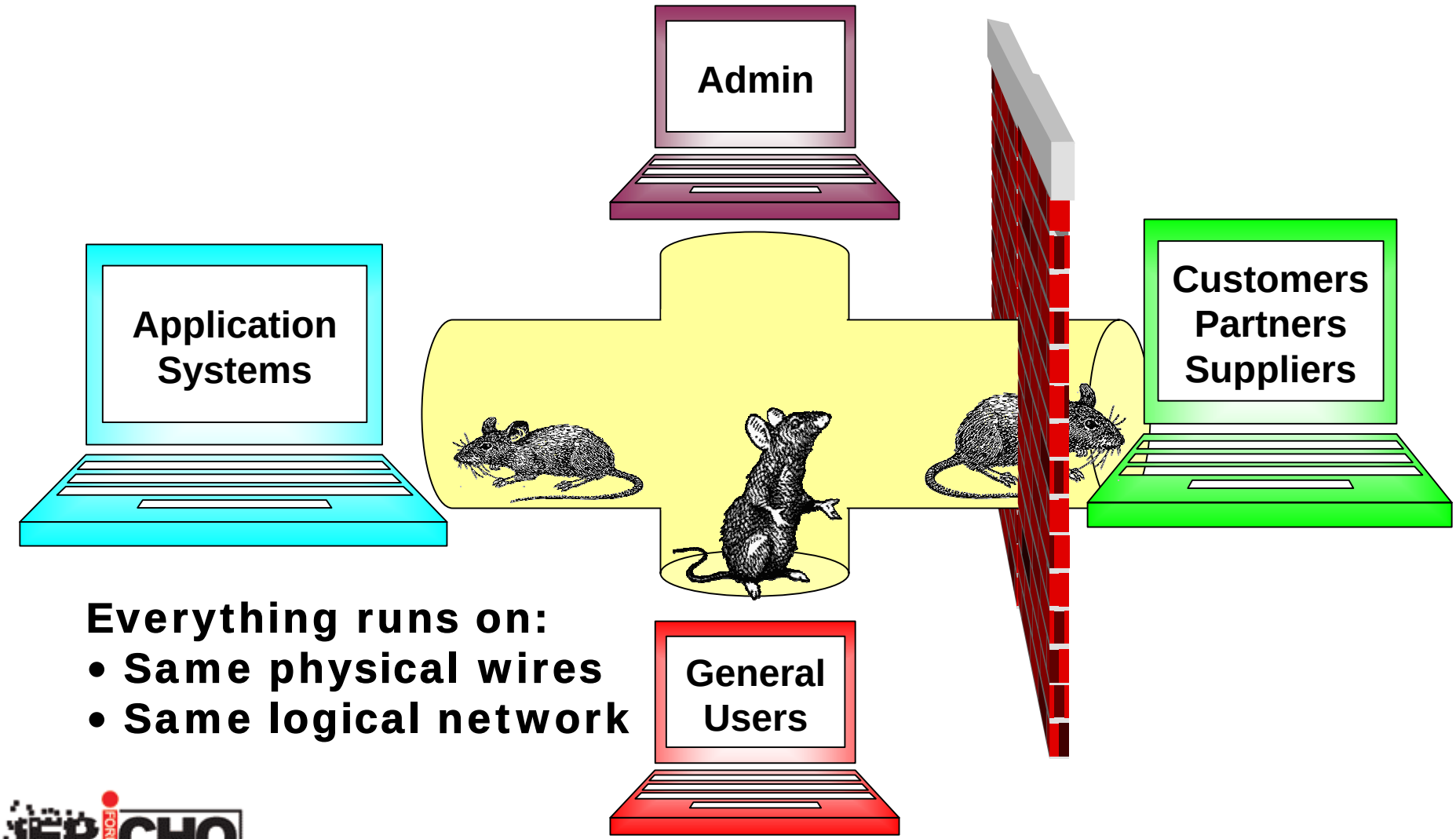
Nick Bleech, Jericho Forum

August 1st 2005

Today's 'Trusted' Network:
Concept



Today's Twisted Network: Reality

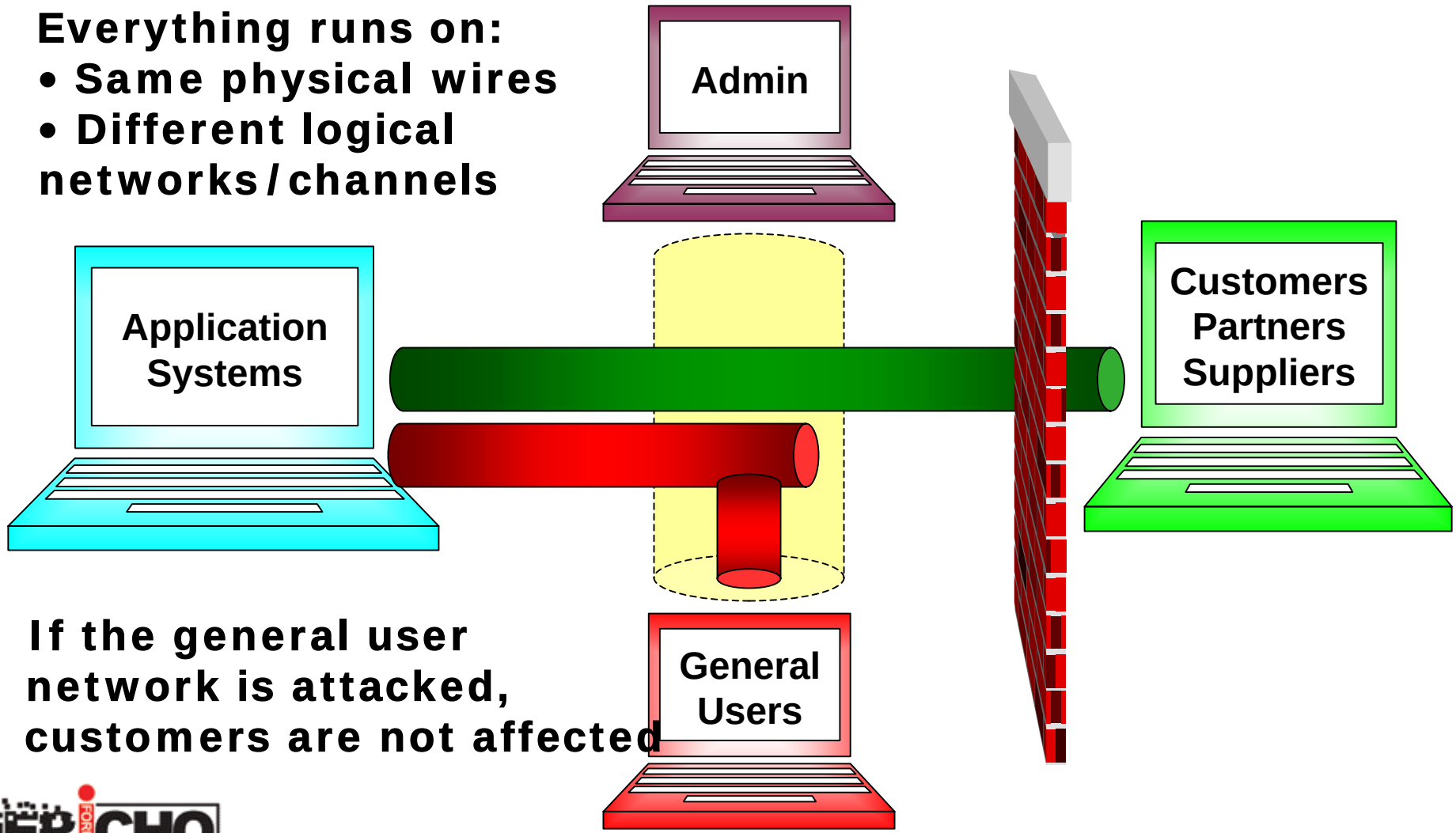


Everything runs on:

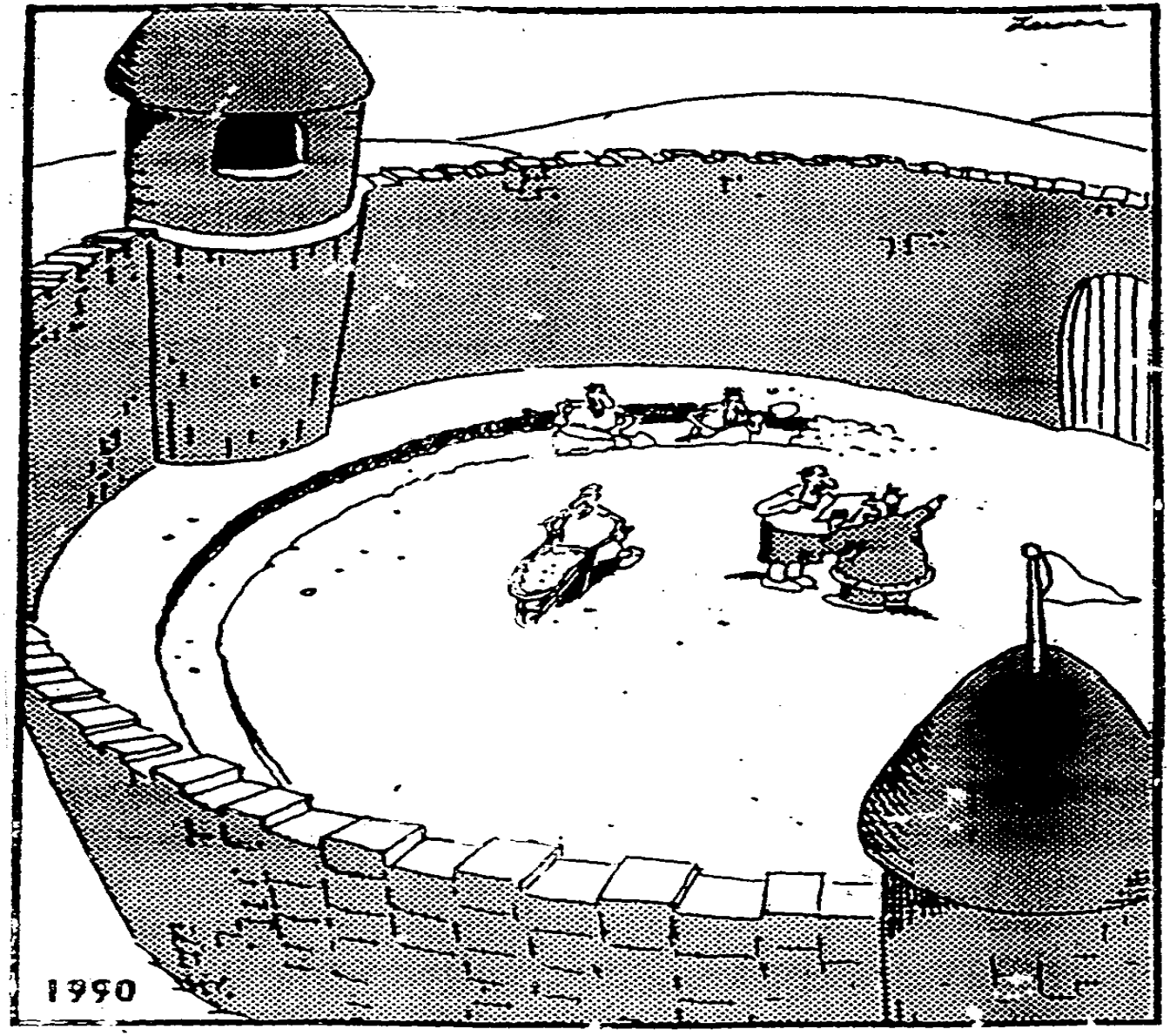
- **Same physical wires**
- **Same logical network**

Tomorrow's Network

Everything runs on:
- **Same physical wires**
- **Different logical networks/channels**



If the general user network is attacked, customers are not affected



Suddenly, a heated exchange took place between the king and the moat contractor.

Trends

Past

- Static, long term business relationships
- Assumption that threats are external – perimeters responsible for protecting all assets from all external attacks
- Traditional client server environment used by an office based workforce
- Operating System and Network based security controls

Future

- ➔ Dynamic, global business partnerships
- ➔ Threats are everywhere – perimeters defend the network, but highly mobile devices must defend themselves
- ➔ Growing use of mobile and wireless devices by an increasingly virtual workforce
- ➔ Protection extended to applications and end user devices

Changing Perimeter Requirements

- The traditional model of a hard perimeter and soft centre is changing as :
  - The workforce moves outside the perimeter
  - Business partners move inside the perimeter
- Policy is out of sync…
  - too restrictive at the perimeter (default deny)
  - lacking in the core (default allow)

Tomorrow's Perimeter

- Why would you still have a perimeter?
  - Block external attacks in network infrastructure
    - IP spoofing
  - Block noise and control intranet
    - Denial of service attacks
    - Protection from random traffic
    - Routing and network address management
  - Legal barrier
    - Evidence of corporate boundary
- …Depending on criticality of the (sub) network / channel / application / service

Security Problem

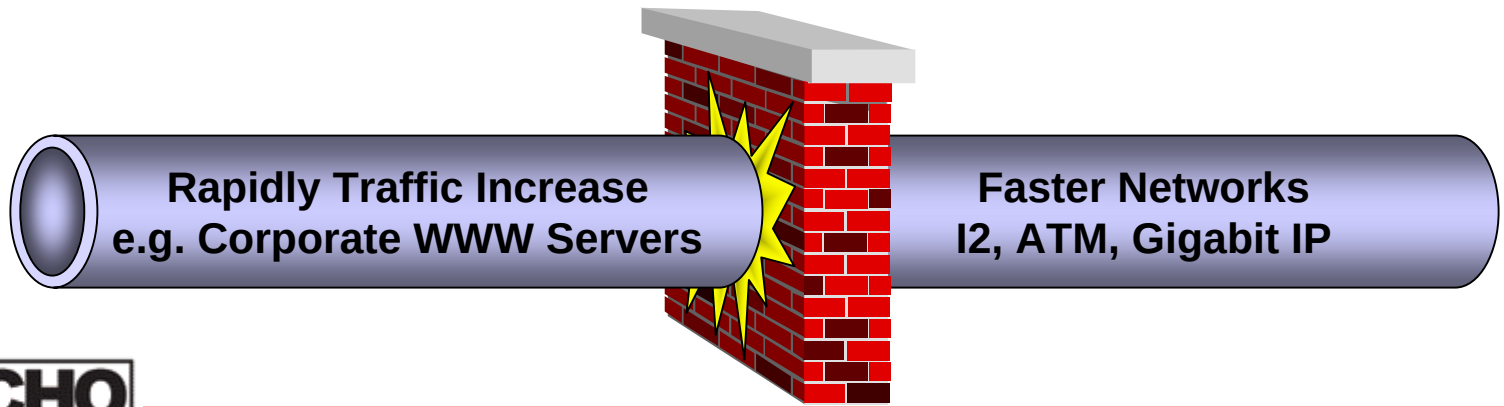
- The Remote PC
  - Is it securely configured? Is it infected with malware?
  - What about data stored locally?
- The network / communication channels
  - How do I establish it easily (transitive trust)?
  - What happens to my data passing over it?
- The island host / applications and services
  - Who do I let in? How do I exclude others?
  - Granularity of services ➔ granularity of controls
- The management
  - How to manage ‘000s of points of control to same standard with robustness.

Business Case Problem

- We want low cost and high security.
  - If aggregate controls costs remain about equal, but redistributed to end point security, business case rests on reducing connectivity costs / enhancing usage and business benefit (e.g. externalize data).
  - If aggregate controls costs reduce, connectivity costs reduce, and usage increases we get a win-win.
- Expect that earlier adopters are seeing the former, later adopters will see the latter.
- Evidence of reduced controls costs include e.g. commoditization of f/w and IDS, market-led distributed trust (eBay model).

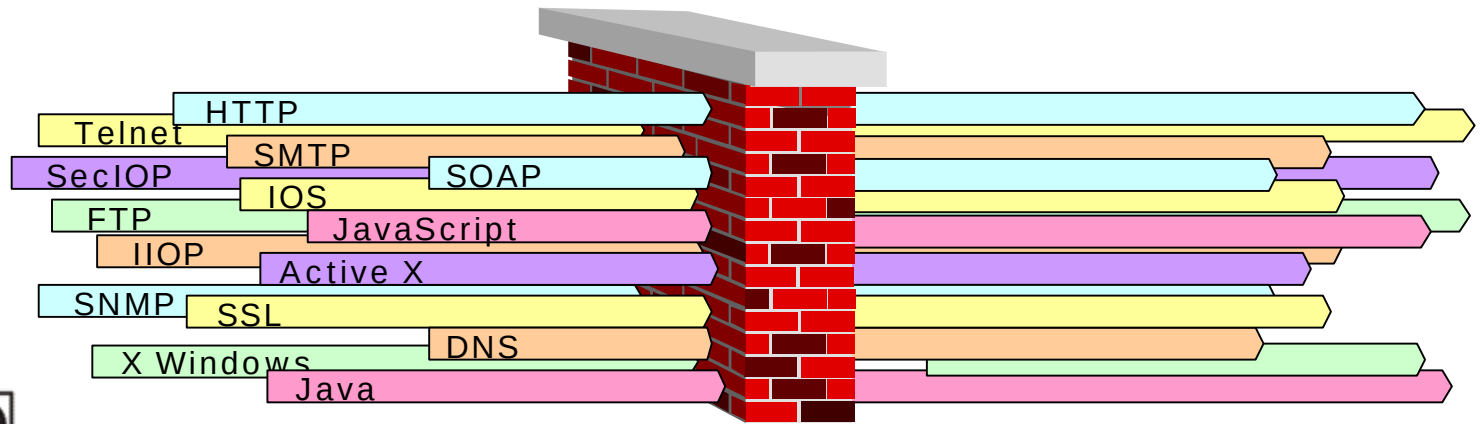
Challenge 1: Traffic Volume

- Demand for services and new technologies generating significant increases in traffic volumes. CPU intensive tasks such as virus checking and intrusion detection sensors will not keep up
  - Can perimeter proxies keep up with gigabit links?
  - Can traffic be decrypted, analyzed, and re-encrypted?
  - Many firewall products, including packet filters, fail by passing all traffic when overloaded



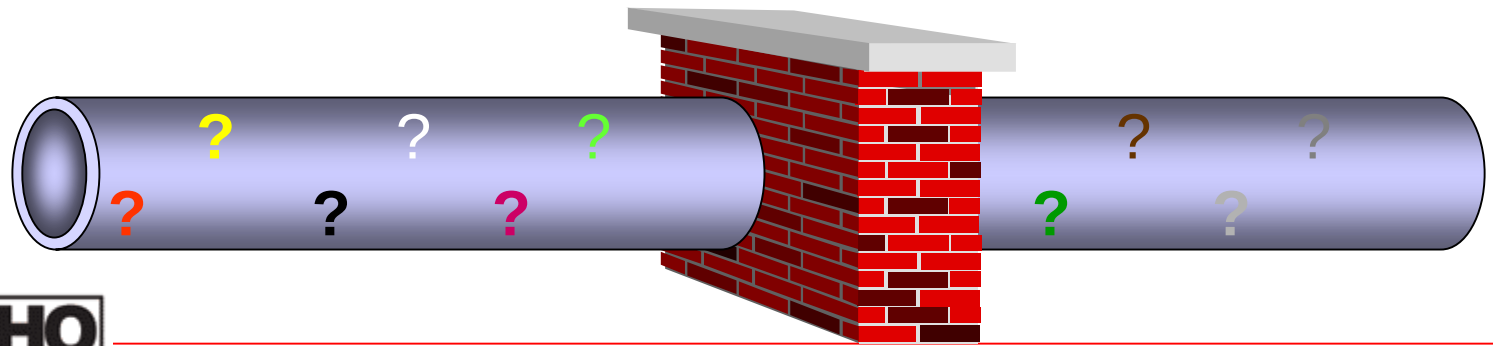
Challenge 2: Increasing Service Variety

- The perimeter now looks like a sieve.
  - Increasing number of new, complex, protocols which require proxies or holes in filters.
  - The practice of sending traffic through the same "firewall friendly" perimeter ports – the web - is rapidly increasing,
    - New protocols often use these ports by design. (SOAP)
    - Older protocols are often wrapped in HTTP/HTTPS.



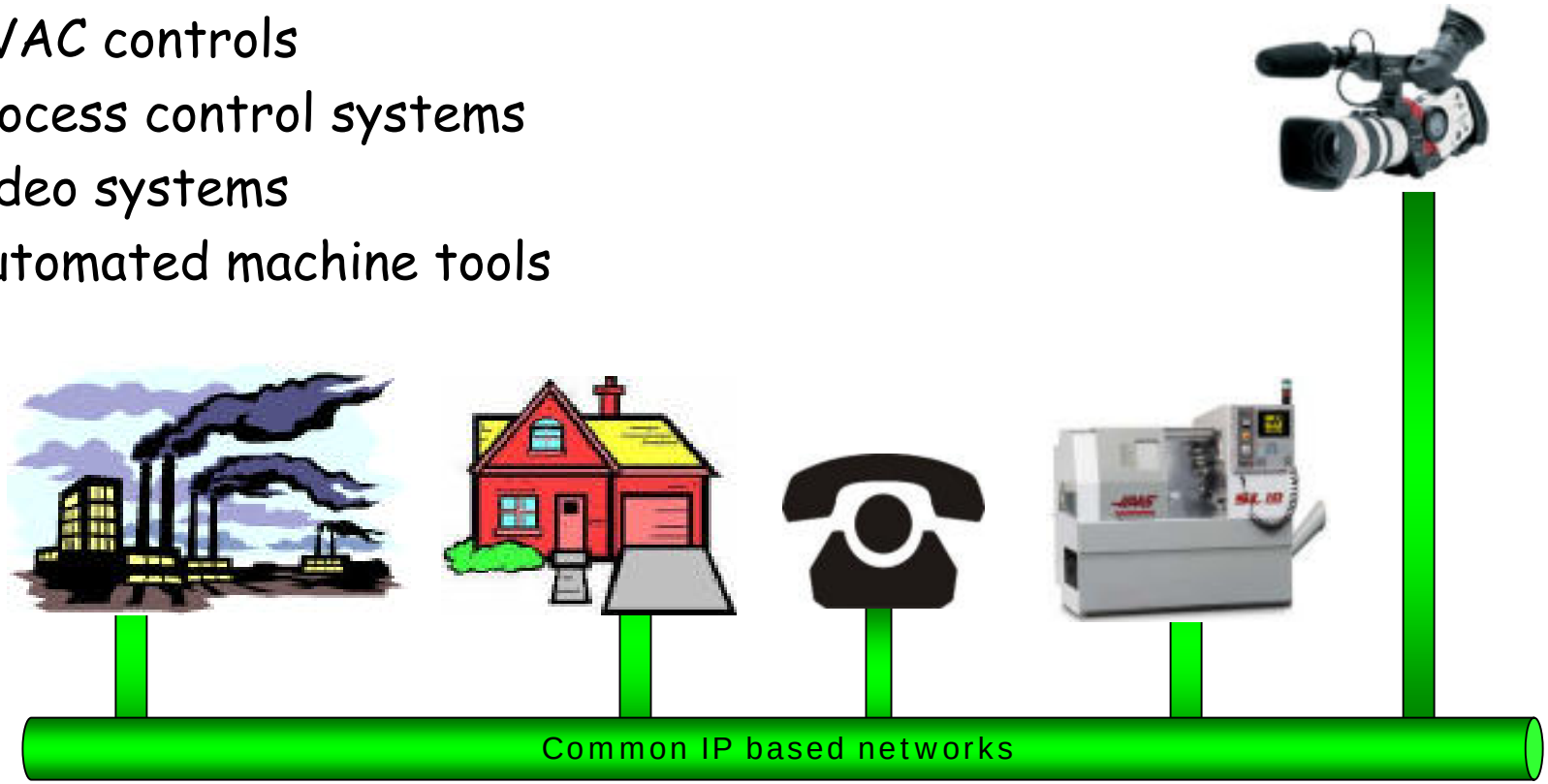
Challenge 3: Encryption

- When packets are passed through encrypted:
  - The firewall is blind, no virus checking
  - TCP port and protocol information unavailable for use in system management, intrusion detection and other tools
- When packets are decrypted at the perimeter:
  - Server SSL certificates "break" at the perimeter
  - Perimeter device is indistinguishable from person in the middle attack
- Industry trend is for end-to-end security
  - Many of these require outbound and inbound encryption.
  - Many do not proxy well
  - Many require advertisement of internal IP addresses



Challenge 4: Application Migration

- Control of non traditional IT applications is migrating to the Internet Protocol
  - Telephones (Voice over IP)
  - HVAC controls
  - Process control systems
  - Video systems
  - Automated machine tools



Strategy: Externalize Trust Models

- **Strongly secure persistent identities:**
  - identity credentials private to the individual.
- **Dynamic roles, attributes, associations**
  - formed on demand / on association.
- **Design for open networks**
  - they are cheaper to run, and 'closed' model is broken anyway.

Strategy: Virtualize to isolate critical business components from general network traffic

- **Partition by service type/criticality:**
  - prevent attacks on one part from taking down entire infrastructure.
- **Partition by sub-organisation/project**
  - protect different user communities from each other.

Strategy: Protect individual users, devices, applications and networks from attack by moving access enforcement down to the end systems

- Devices are highly mobile and must be able to protect themselves. This requires:
  - Hardening the security of end user devices and infrastructure components
    - Improved device firewalls, encryption
  - Improved software solutions and new platform designs
    - NGSCB – Next Generation Secure Computing base
- Servers require additional protection and isolation.
- Uniform trust model to support user identities
- Establish 'citadels' for data of record to support:
  - Information needed for Regulatory Disclosure
  - Master Standing Data, Security Information…
  - Etc.

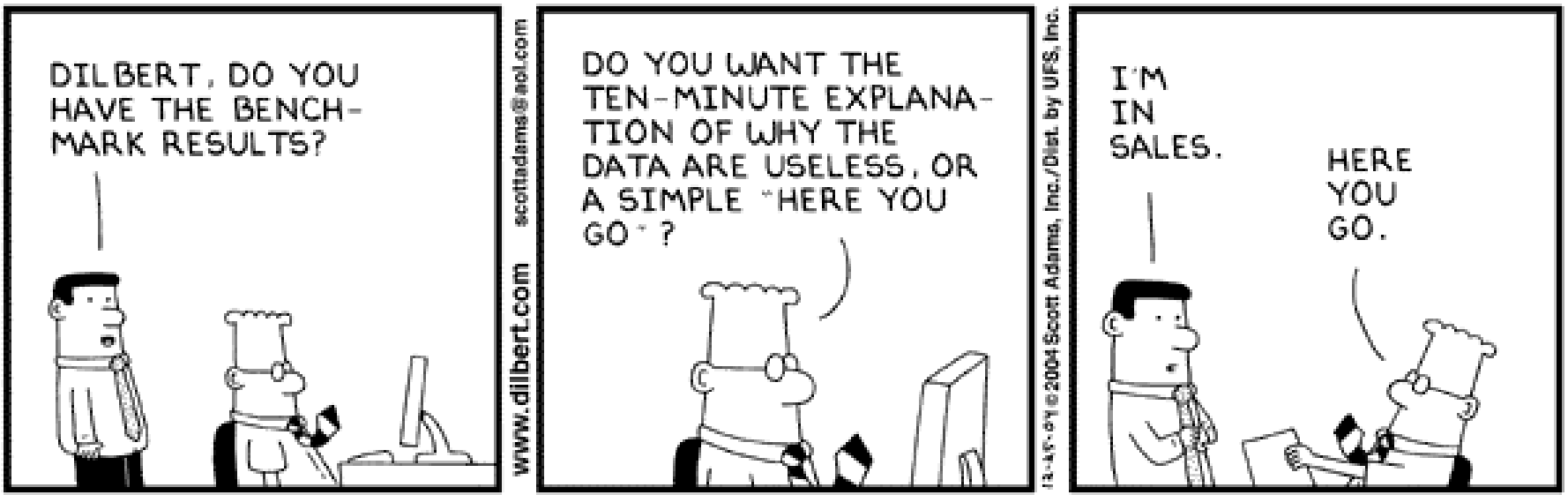
Challenges

- **Network partitioning will add complexity since**
  - Expectation of full access to all IP based services.
  - Trade-off between partitioning and simplicity.
- **Isolation of application components conflicts with server consolidation strategies?**
- **Protecting end devices may hamper central device management and operational support.**
- **Vendors promote solutions favoring product base.**
- **All of the above need standards (preferably, IT customer-led, to counter vendor bias) to:**
  - Avoid having to re-invent the wheel each time
  - Achieve scalability for collaboration and commerce.

Challenges

- **Many existing 'standards' are broken in practice, e.g.:**
  - Certificate/CRL (non) processing in SSL
  - Bug-compatible implementations of X.509 certificate policy/attribute processing in crypto library software
  - Representing collaborating/cooperating organisations in X.500/LDAP; directory interoperability
  - Re-inventing the wheel for security services for XML (Signatures, Encryption, Key Management…)
- **Repeated technical standards initiatives with little or no 'user' / vendor dialogue:**
  - Vendors supposedly understand 'user' requirements
  - 'Users' can't/don't articulate what they want…

Challenges



Jericho Vision/Mission

Vision

- To enable business confidence for collaboration and commerce beyond the constraint of the corporate, government, academic & home office perimeter, through
  - Cross-organizational security processes and services
  - Products that conform to Open security standards
  - Assurance processes that when used in one organization can be trusted by others.

Jericho Vision/Mission

Mission

- Act as a catalyst to accelerate the achievement of the Vision, by
  - Defining the problem space
  - Communicating the collective Vision
  - Challenging constraints and creating an environment for innovation
  - Demonstrating the market
  - Influencing future products and standards

Timetable

- A period of 3-5 years for the achievement of its Vision, whilst accepting that its Mission will be ongoing beyond that.

Thank you

Questions?