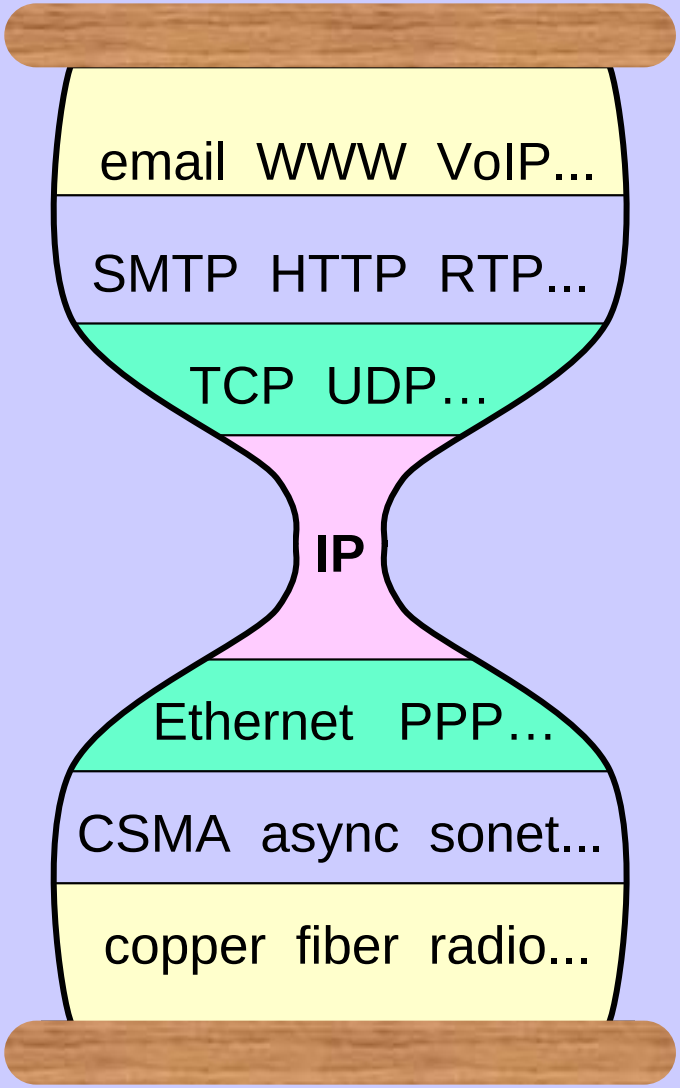
IIJ
Internet Initiative Japan

Tension Between the Innovative Internet and Security

APNIC – Nadi, Fiji
2004.09.01

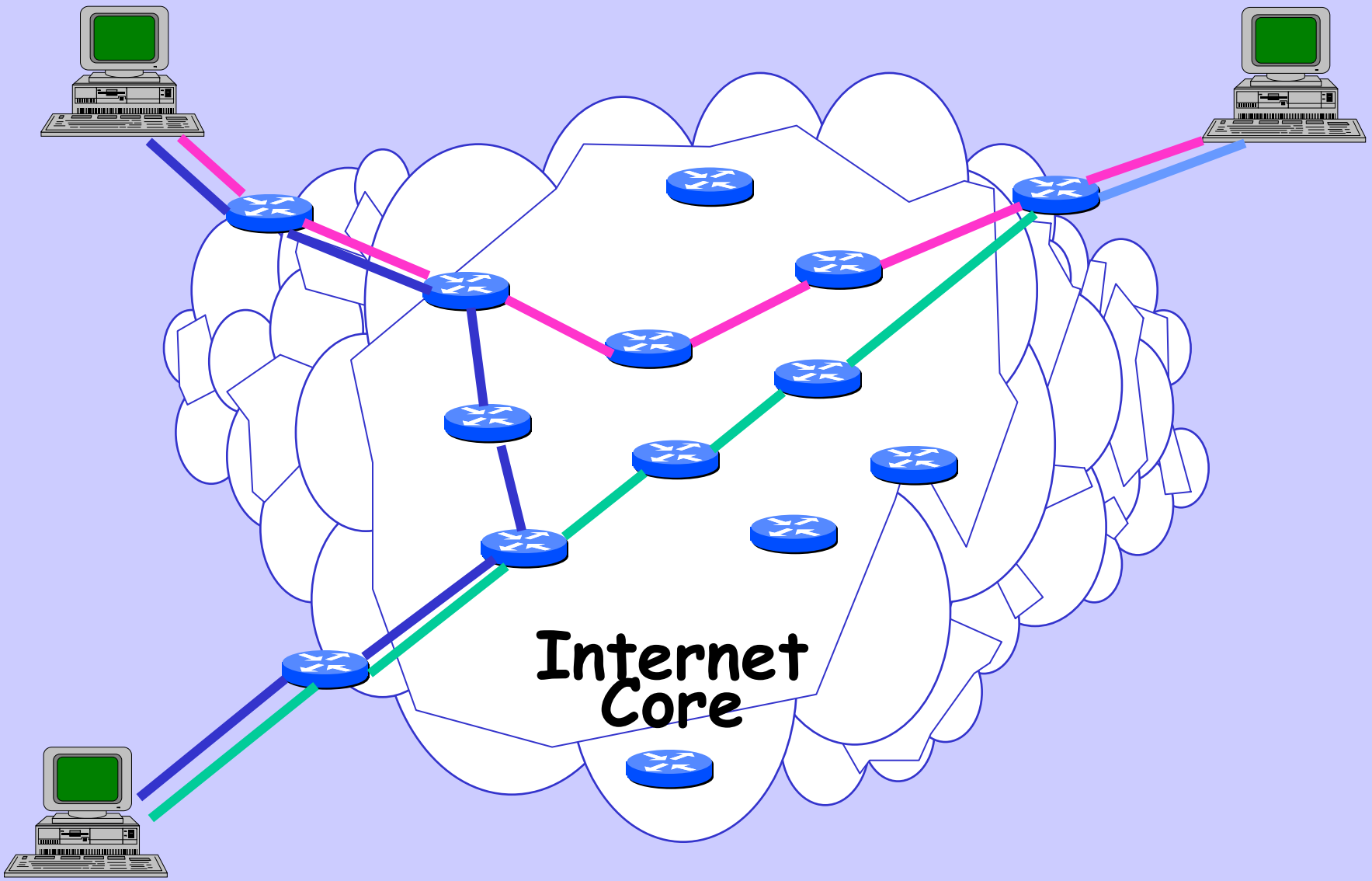
Randy Bush <randy@iij.com>
<http://psg.com/~randy>

Hourglass Model



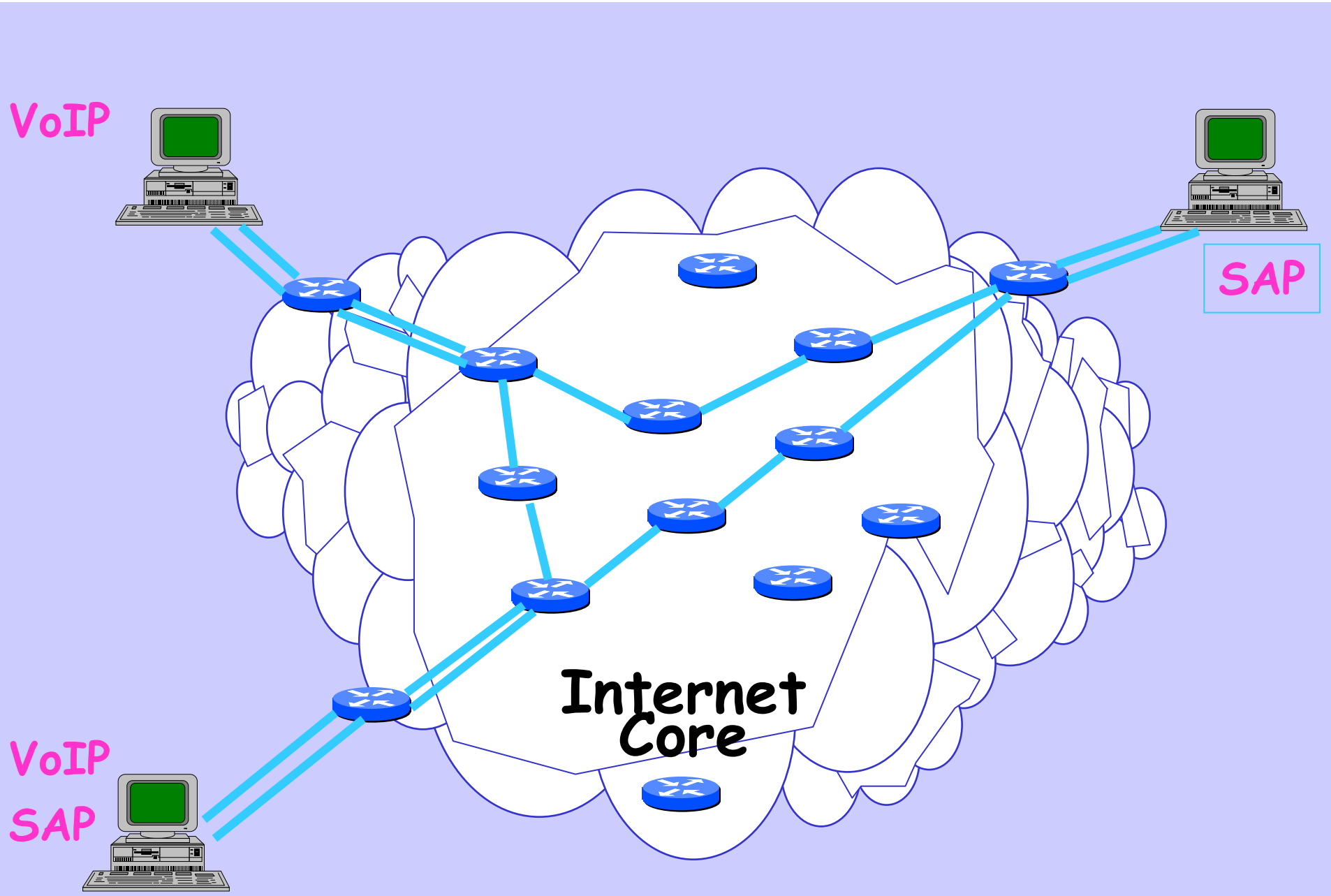
The End to End Model

- Internet has a 'Stupid' Center
- Packets travel *End to End* with Routers only Forwarding, Not Modifying
- The Edge, Hosts, are Smart
- As the Net Scaled, the Cost of a Router has Remained Constant or has Grown
- The Cost of a Host has Fallen as they are Commodity Products



EtoE Fosters Innovation

- To Add a New Internet Service
- Just Distribute the Application to Participating End Hosts
- No Change to the Internet Core
- E-mail was a Service ***Added*** to the ARPANET
- HTTP (the *Web*), VoIP, eSQL, SAP, … were ***Added*** to the Internet



Compare to Telco

- Stupid Edges - Phone Instruments
- Very Smart Core – Massive Switches, 800 Boxes, Voicemail Add-Ons, …
- Adding Services Requires Core Changes and is Very Complex
- Innovation is Very Very Slow
- Innovation is Very Very Expensive
- All Change is Controlled by the Core

Telco Deployment

- How long did it take Telcos to Deploy Rotary Dialing?
- Over a Decade at Massive Expense (when the network was tiny)
- How long did it take the Telcos to Convert to TouchTone Dialing?
- Decades, and they are Still Doing it!

EtoE / Internet Win$

- Internet Applications are Your Customers' Key to Profit
- New Killer Apps will Help Drive Their Future Business
- Without an Open EtoE Internet, Tomorrow's Killer Application will be Difficult to Deploy

But…

- Security was NOT a Design Goal of the Internet, Reliability was, so …
- With no Borders, Bad things Move as Easily as Good Things
- Worms, Viruses, DDoS Attacks, are Possible
- But the Problem is not the EtoE Model
- Horrible Lack of Security in OSs
- Lack of Security in Internet Protocols

Can't Filter in Core

- Difference Between Good Traffic and Bad Traffic is *Intent*
- Did the Sender Intend to Send / Reveal the Data?
- Did the Recipient wish to Receive?
- We Can't Judge in the Core
- For Example, Some Customers are Security Researchers!

What this Means?

- Burden for Security is at the Edges
- The Servers & Users' Computers
- The Site Borders, Overworked IT
- IT Departments are Directed to Manage Cost and Security, not Maximize User's Productivity
- With No Goal for Users to be Early Adopters of the Next Killer App

Site Edge - a Holding Action

- *Hard Crunchy* Edge – Firewalls, NATs, Application Gateways
- *Soft Center* – User Machines
- Worms & Viruses Carried in on Laptops
- Users Open Bad Email, Bad Sites
- DDoS still Takes Out Sites
- But it is All We Have Today

Educated Users

- In a Free Society, the People Must be Educated
- Users Know how to Handle an Obscene Phone Call
- Why not Bad Email?
- Do Not Open that Attachment!
- Do Not Click on that "Please Confirm Your Password" Site (aka Phishing)

But Also …

- Microsoft Really has to Clean Up the Vulnerabilities in their Code
- All 80 Million Lines of it
- Applications must be Cleaned Up of Weak Programming Practice
- Protocols have to be Designed for Security and Secure Deployment

In the Meantime

- This will all Take a Decade Plus
- In the Meantime, You have to Get Your Work Done
- So we Use Edge Security
- We Filter Email
- We Block Sites
- We Mitigate DDoS Attacks

Long Run

- Secure Protocols – the IVTF will take a Decade
- Secure Operating Systems – Microsoft will take a Decade
- Secure Applications – Customers Must Apply Pressure

But…

- Do Not Break the End to End Model of the Internet
- It is Why the Internet is so Successful Today
- It is Why You are $uccessful Using the Internet Today

Questions and Discussion