

# Internet Reliability under Stress

Fred Baker  
Cisco Fellow

## The Internet's principles of reliability

- End to End Principle
- Robustness principle
- Route redundancy
- Fate sharing

## **The End to End Principle: *an argument for simplicity***

**“The function in question can completely and correctly be implemented only with the knowledge and help of the application standing at the end points of the communication system. Therefore, providing that questioned function as a feature of the communication system itself is not possible.”**

**END-TO-END ARGUMENTS IN SYSTEM DESIGN**

**J.H. Saltzer, D.P. Reed and D.D. Clark**

**M.I.T. Laboratory for Computer Science, 1981**

## **Another way to say it: Occam's Razor**

**“Entities should not be multiplied unnecessarily,” or  
“A satisfactory proposition contains no unnecessary complexity.”**

**William of Occam**

**14<sup>th</sup> Century England**

**K.I.S.S.**

## Robustness Principle

**“TCP implementations should follow a general principle of robustness:**

- **Be conservative in what you do**
- **Be liberal in what you accept from others.”**

RFC 761, 791

## Route redundancy

Cisco.com

- **Multiple paths selected by the network**
- **Application/transport resilience to loss**

## Fate sharing

Cisco.com

- **Session seen as shared state between end station processes**
- **Loss of connection implies loss of shared state**

**“If the strength of a chain is its weakest link, then the strength of a net – or a network - is the strength of the path through it that survives.”**

Judy Estrin - 1999

# Threat analysis

Stresses the internet sees

**“The challenge of implementing software that satisfies its specification is well known, and failing to meet that challenge invariably compromises system trustworthiness.”**

**Trust in Cyberspace**

**Fred B. Schneider, Editor;**

**Committee on Information Systems Trustworthiness,**

**National Research Council**

## Threat analysis:

Cisco.com

- **Key security issues outside of software reliability**
- **Physical layer**
- **Link layer**
- **Network layer**
  - Routing issues
  - Operational faults
  - Network reliability and serviceability (RAS)
- **Transport layer**
- **Application functionality**

Quality Week 2002

© 2002, Cisco Systems, Inc. All rights reserved.

11

## Key security issues outside of software reliability

Cisco.com

- **Access control**
- **Authentication of users**
- **Authorization issues**
- **Privacy**

Quality Week 2002

© 2002, Cisco Systems, Inc. All rights reserved.

12

## Physical layer

Cisco.com

- The biggie
- More generally:
  - Physical access
  - Physical damage
  - Wiretap



Quality Week 2002

© 2002, Cisco Systems, Inc. All rights reserved.

13

### portable generator next to Telehouse, 9/15



Photo: Anthony Townsend, Taub Urban Research Center, New York University

renesys

[www.renesys.com](http://www.renesys.com)

Quality Week 2002

© 2002, Cisco Systems, Inc. All rights reserved.

14

## Link layer

Cisco.com

- **LAN/VLAN routing**
  - Security**
  - Correctness**
- **Unauthorized access to traffic**
- **Solutions:**
  - IEEE 802.11f proposing security procedure**

Quality Week 2002

© 2002, Cisco Systems, Inc. All rights reserved.

15

## Network layer

Cisco.com

- **Routing issues**
- **Operational faults**
- **Network reliability and serviceability (RAS)**

Quality Week 2002

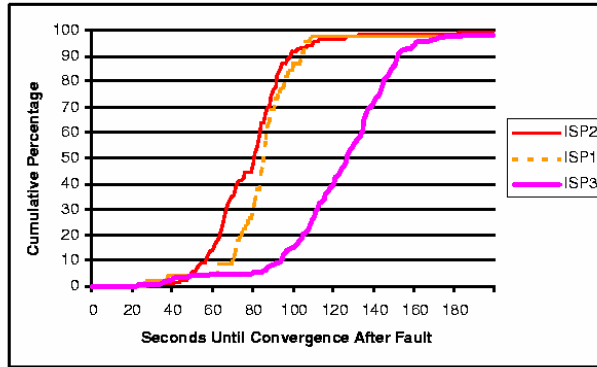
© 2002, Cisco Systems, Inc. All rights reserved.

16



# Comparing ISP Convergence Latencies\*

Cisco.com



- CDF of faults injected into three Mae-West providers and observed at Japanese ISP
- Significant variations between providers
- Not related to geography

\*Data From Abha Ahuja and Craig L. presentation at NANOG20

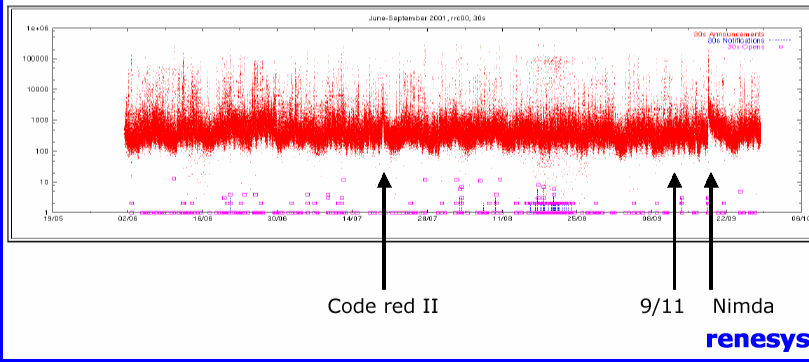
Quality Week 2002

© 2002, Cisco Systems, Inc. All rights reserved.

17

## 9/11 in context

Number of prefix announcements in 30 sec intervals  
 1 June – September 30, 2002  
 Amsterdam (rrc00) all peers aggregate



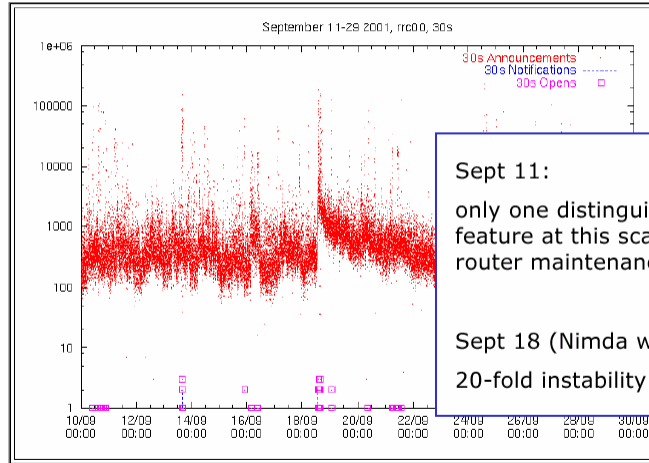
Quality Week 2002

© 2002, Cisco Systems, Inc. All rights reserved.

18

## 9/11 in context: zoom-in

Number of prefix announcements in 30 sec intervals



Sept 11:

only one distinguishable feature at this scale – fewer router maintenance resets

Sept 18 (Nimda worm):

20-fold instability growth.

renesys

www.renesys.com

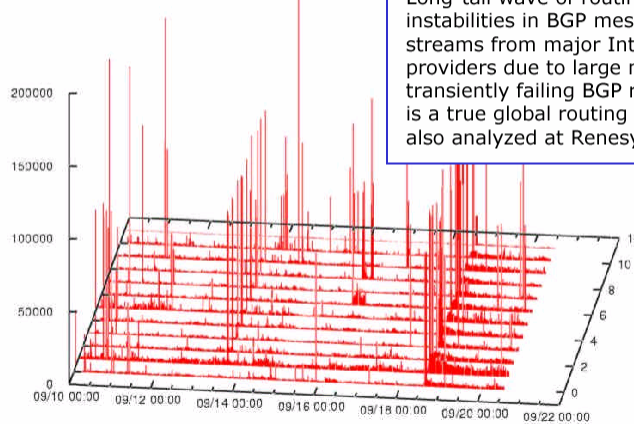
Quality Week 2002

© 2002, Cisco Systems, Inc. All rights reserved.

19

## Appendix: Nimda worm attack

prefix announcements by peer in 15-min intervals  
RIPE rrc00 peering point,  
10 – 22 september



**18 September 2001:**

Long-tail wave of routing instabilities in BGP message streams from major Internet providers due to large numbers of transiently failing BGP routers. This is a true global routing instability, also analyzed at Renesys.

renesys

www.renesys.com

Quality Week 2002

© 2002, Cisco Systems, Inc. All rights reserved.

20

## Network routing issues

Cisco.com

- **Network design**
  - Is there a backup route?
- **Convergence intervals**
- **Snap state loss**
- **Loss detection**
- **Security of communication**
  - IPSEC or HMAC-MD5 neighbor authentication
- **Authorization to originate/change data**
  - Secure BGP proposal and friends

Quality Week 2002

© 2002, Cisco Systems, Inc. All rights reserved.

21

## Network operational faults

Cisco.com

- **Configuration errors**
- **Mis-announcements**
- **Service masquerade**

Quality Week 2002

© 2002, Cisco Systems, Inc. All rights reserved.

22

## Network reliability and serviceability (RAS)

Cisco.com

- **Service overload**
  - Denial of service attacks
  - Server loading issues
- **Database design issues**
- **Firewall design issues**
- **Intrusion management issues**

Quality Week 2002

© 2002, Cisco Systems, Inc. All rights reserved.

23

## Solutions to Network Issues

Cisco.com

- **Security of communication**
  - IPSEC or HMAC-MD5 neighbor authentication
  - Several RFCs apply, but the network must be configured to use them
- **A secure form of BGP (securing information) is called for, and perhaps a next generation BGP**
- **Significant ongoing work in BGP development**

Quality Week 2002

© 2002, Cisco Systems, Inc. All rights reserved.

24

## Transport layer

Cisco.com

- **Session hijack**
- **Spurious session**
  - Port scans
  - Misdirected traffic
- **Man-in-the-middle attacks from middleware**
  - Firewalls
  - Network address translators
  - IPSEC gateways
  - QoS appliances
- **Solutions: hence IPSEC**

Quality Week 2002

© 2002, Cisco Systems, Inc. All rights reserved.

25

## Application functionality

Cisco.com

- **Virus/worm attacks**
- **Encoding issues**
  - Unicode encodings of non-ASCII characters
  - Encodings of DNS names
- **Application vulnerabilities in authentication and authorization**
  - How do I know who you are?
  - How do I know whether you may have certain information?

Quality Week 2002

© 2002, Cisco Systems, Inc. All rights reserved.

26

## Referential integrity

Cisco.com

- **Property:**
  - A name for an object predictably gets you that object
- **Examples**
  - URL gets you a certain file, even if it changes
  - DNS name gets you a consistent set of computers that offer a service
  - IP Address consistently gets you the same computer

## Scaling Issues

**“If you’re not afraid, you don’t understand.”**

Mike O’Dell  
Then Chief Scientist, UUNET

## Solutions in the application layer

Cisco.com

- **The problems, and their solutions, are generally application-specific**
  - Security solutions exist for mail (APOP, IMAP)
  - More secure alternatives exist for many applications (SSH/SFTP for rsh/rcp, for example)
- **Caveat emptor: get your application vendor to**

## Trend analysis

All is not lost

Cisco.com

## The good news

Cisco.com

- **The trend line**
  - Software quality is improving as the Internet gets more widely adopted**
  - Network reliability is improving**
  - Slight acceptance of security as an issue in product design**
- **CERT reports down**

Quality Week 2002

© 2002, Cisco Systems, Inc. All rights reserved.

31

## Internet reliability is not about “more testing”

Cisco.com

- **Testing sure helps**
- **Usually about design and thought**
  - Poorly thought through ideas generally work poorly under stress**

Quality Week 2002

© 2002, Cisco Systems, Inc. All rights reserved.

32



## The Internet's principles of reliability

Cisco.com

- End to End Principle
- Robustness principle
- Route redundancy
- Fate sharing

**K.I.S.S.**

Quality Week 2002

© 2002, Cisco Systems, Inc. All rights reserved.

33

## How you can help

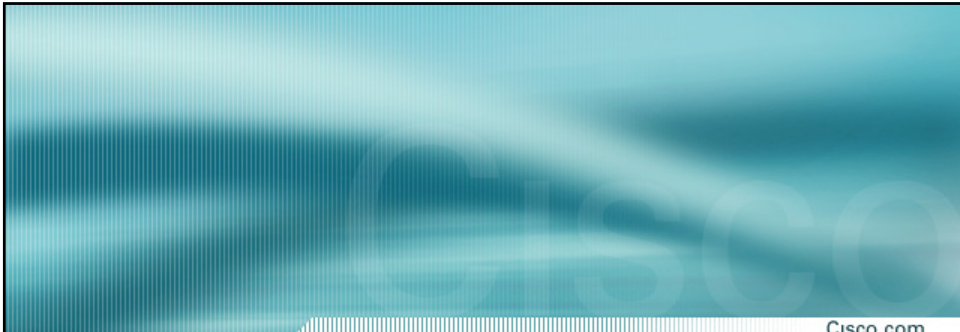
Cisco.com

- Solid network design
- Solid specification of your needs
- **Use** secure versions or security features of applications, stacks, and routing protocols
- Insistence on a threat analysis of any network elements or subsystems as part of their design

Quality Week 2002

© 2002, Cisco Systems, Inc. All rights reserved.

34



Cisco.com

# Internet Reliability under Stress

Fred Baker  
Cisco Fellow

Keynote  
Quality Week 2002

© 2002, Cisco Systems, Inc. All rights reserved.

35