Workshop on Infrastructure Security and Operational Challenges of Service Provider Networks

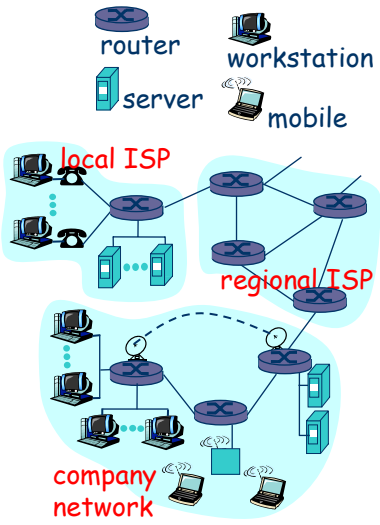
Farnam Jahanian
University of Michigan and Arbor Networks

IFIP Working Group 10.4
June 29-30, 2006

What's the Internet: "nuts and bolts" view

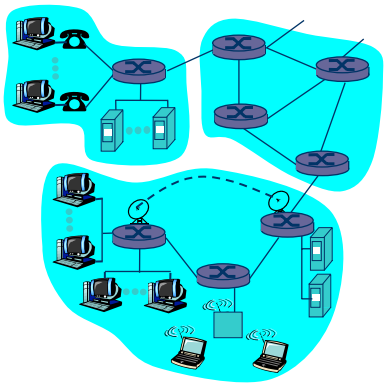
- millions of connected computing devices: *hosts, end-systems*
  - PCs workstations, servers
  - PDAs phones, toasters

  running *network apps*
- *communication links*
  - fiber, copper, radio, satellite
  - transmission rate = ***bandwidth***
- *routers:* forward packets (chunks of data)



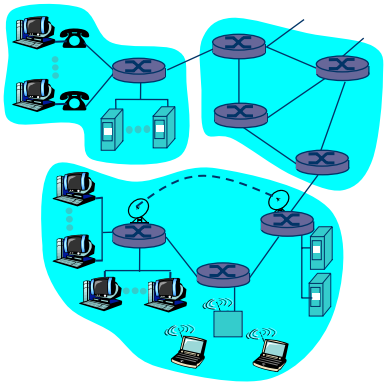
What's the Internet: "nuts and bolts" view

- communication *infrastructure* enables distributed applications:
  - Web, email, games, e-commerce, database., voting, file (MP3) sharing
- communication services provided to apps:
  - connectionless
  - connection-oriented

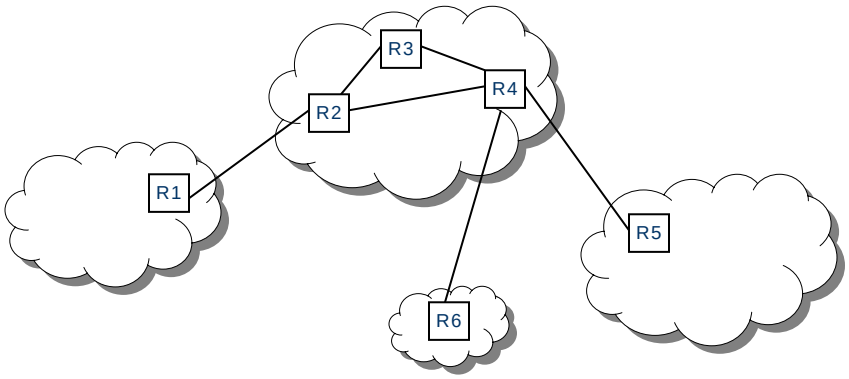


What's the Internet: a service view

- communication *infrastructure* enables distributed applications:
  - Web, email, games, e-commerce, database., voting, file (MP3) sharing
- communication services provided to apps:
  - connectionless
  - connection-oriented



Autonomous Systems (AS)



- The Internet is a collection of autonomous systems.
- AS: A set of routers and networks under the same administrative control.
- Inter-domain vs. intra-domain routing.

- 5 -

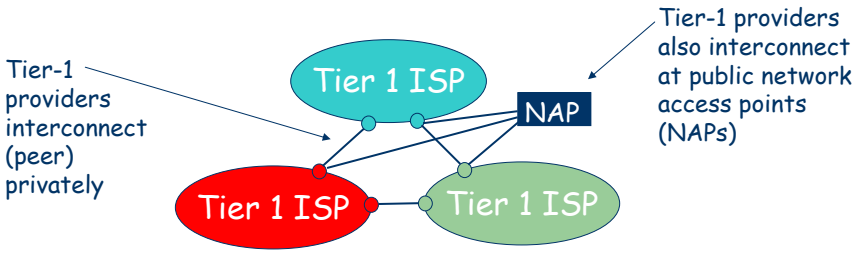
Internet design – End-to-End Principle

- Put the intelligence in the end hosts and keep the network simple
  - Packet switched instead of circuit switched
  - Best effort delivery
  - Force transport layer to deal with delay and loss
- Dynamic routing in the face of failures
  - No session state on routers
  - Allows routers to be added and removed without causing large disturbances

- 6 -

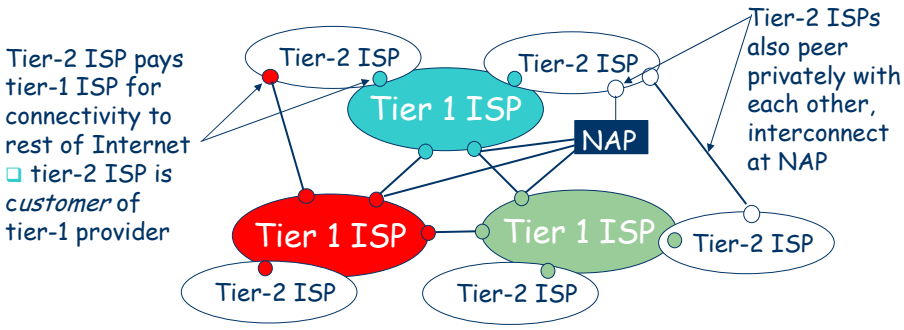
Internet structure: network of networks

- roughly hierarchical
- at center: "tier-1" ISPs (e.g.,AT&T, Verizon, Sprint), national/international coverage
  - treat each other as equals



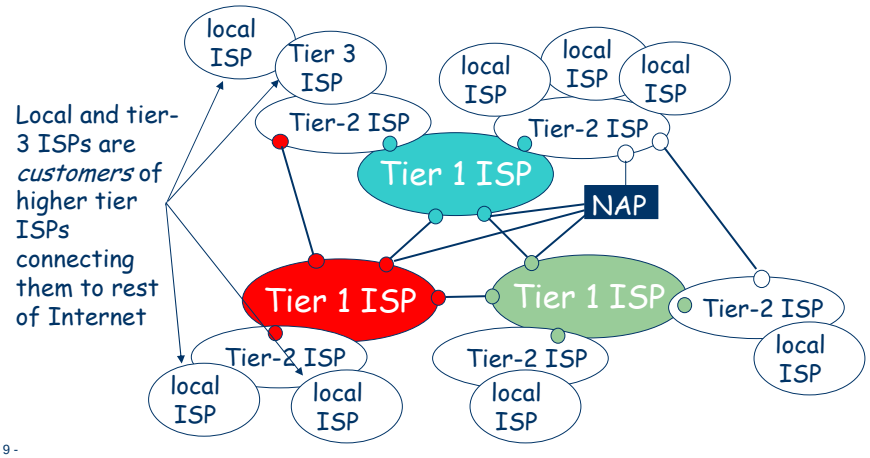
Internet structure: network of networks

- "Tier-2" ISPs: smaller (often regional) ISPs
  - Connect to one or more tier-1 ISPs, possibly other tier-2 ISPs



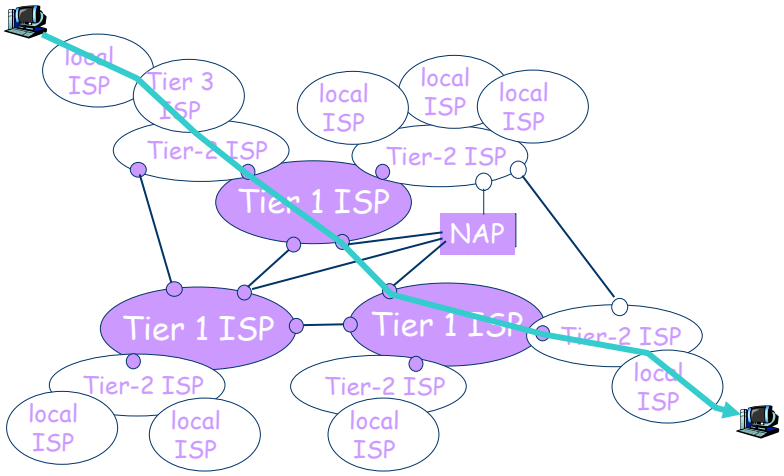
Internet structure: network of networks

- "Tier-3" ISPs and local ISPs
  - last hop ("access") network (closest to end systems)

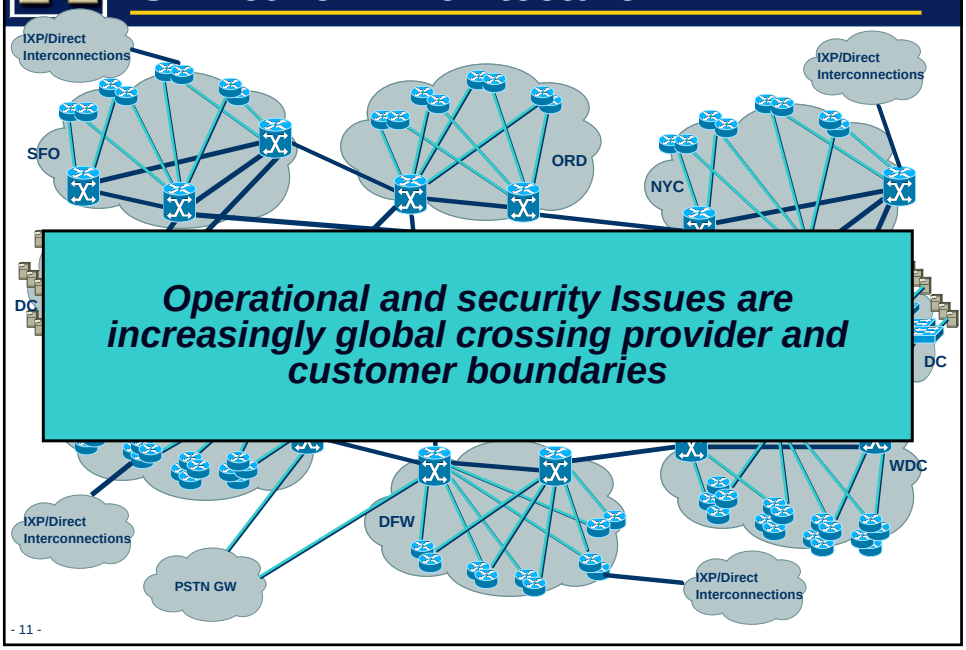


Internet structure: network of networks

- a packet passes through many networks!



ISP Network Architecture



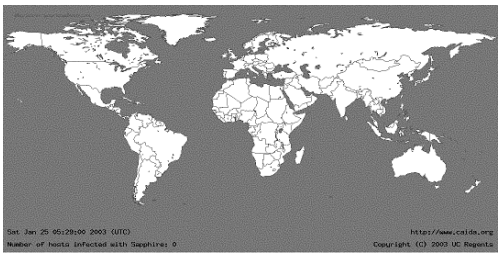
WHY IS IT HARD?

- Requirements of emerging Internet applications
  - VoIP, IPTV, groupware, content delivery & DRM
  - Predictable, reliable and secure services
- Diverse and complex building blocks
  - 10,000 of network elements in a large network
  - Provider edge, customer edge, POP, backbone
- Fragile and vulnerable IP control infrastructure
  - IP is a best-effort service, end-to-end principle
  - Scalability achieved thru highly decentralized protocols/services
- Evolution of security attacks
  - DDoS, worms, botnets, phishing, ...
  - Crumbling network perimeter
- Evolving regulatory and legal issues

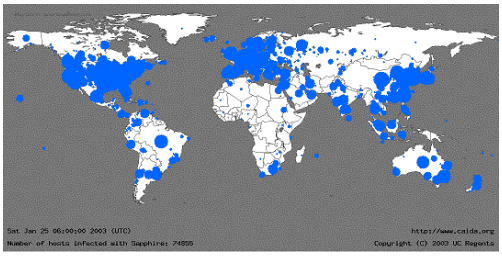
Trends in Internet Security Threats

- ***Globally scoped***, respecting no geographic or topological boundaries.
  - At peak, 5 Billion infection attempts per day during Nimda including significant numbers of sources from Korea, China, Germany, and the US. [Arbor Networks, Sep. 2001]
- Exceptionally ***virulent***, propagating to the entire vulnerable population in the Internet in a matter of minutes.
  - During Slammer, 75K hosts infected in 30 min. [Moore et al, NANOG February, 2003]
- ***Zero-day*** threats, exploiting vulnerabilities for which no signature or patch has been developed.
  - In Witty, "victims were compromised via their firewall software the day after a vulnerability in that software was publicized"

SQL Slammer Attack Propagation



0 hosts infected at the start



75,000 hosts infected in 30 min.

Infections doubled every 8.5 sec.

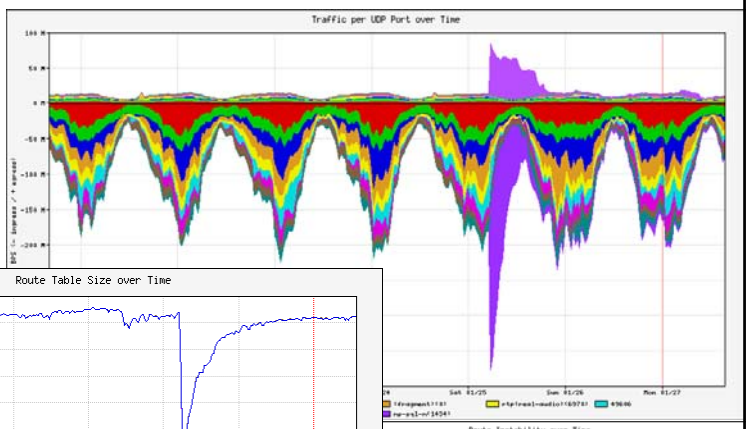
Spread 100X faster than Code Red

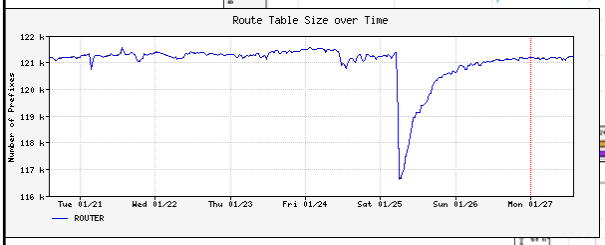
At peak, scanned 55M hosts per sec.

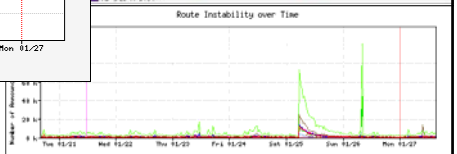
[Moore, Paxson, et al; NANOG February, 2003]

Impact of Slammer on the Internet

No DoS playload!

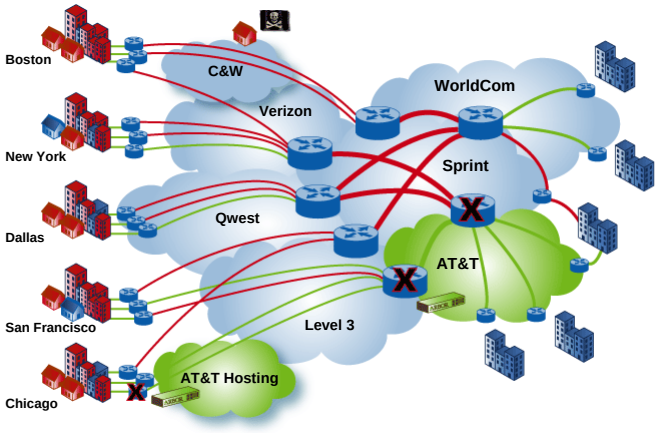




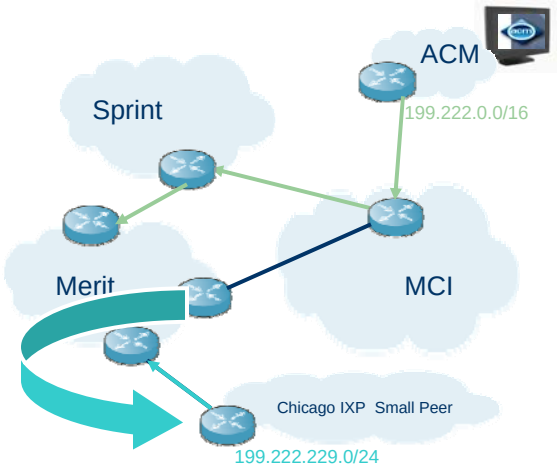


Loss of several thousand routes, mostly /24s

Distributed Denial-of-Service



BGP Address Hijacking



- Though providers filter customer BGP announcements, few filter peers
  - Memory, line-card limitations
  - Maintenance problem
- More specific announcements wins
- Injection attack requires compromised commercial or PC-based router
  - man-in-middle session attacks rare

- 17 -

… Availability Attacks

- 18 -

A Dramatic Transformation and Escalation

- 19 -

Threat Evolution

The evolution of malicious Internet activities primarily motivated by *economic incentives*

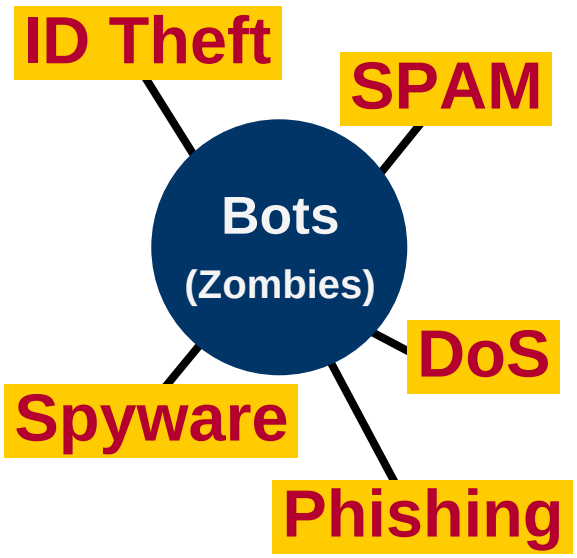
- DoS Extortion
- Identity Theft
- Phishing
- SPAM
- Spyware

Attackers have learned:

1. *A compromised system provides anonymity*
2. *Network of compromised hosts provides a powerful delivery platform*
3. *A compromised system is more useful alive than dead!*

- 20 -

Lurking in the darkness… Bots



How many bots?

- Almost 1 million *bot* infected systems [IEEE04]
- Reports of botnets with 100,000 *Zombies*! [CERT03]
- 1000's of new *bots* each day [Symantec05]

- 21 -

Network Managements & Traffic Engineering

- Inter-domain Traffic Engineering
- Transit / Peering Management
- Backbone Engineering
- Capacity Planning / Provisioning
- Root-cause Analysis / Failure Diagnosis
- Traffic / Routing Anomalies
- Abuse and Misuse

- 22 -

WHY IS IT HARD?

- Requirements of emerging Internet applications
  - VoIP, IPTV, groupware, content delivery & DRM
  - Predictable, reliable and secure services
- Diverse and complex building blocks
  - 10,000 of network elements in a large network
  - Provider edge, customer edge, POP, backbone
- Fragile and vulnerable IP control infrastructure
  - IP is a best-effort service, end-to-end principle
  - Scalability achieved thru highly decentralized protocols/services
- Evolution of security attacks
  - DDoS, worms, botnets, phishing, ...
  - Crumbling network perimeter
- Evolving regulatory and legal issues