ISP Security Issues in today’s Internet

It’s not a nice place anymore ...

Cisco Systems

The Internet Today

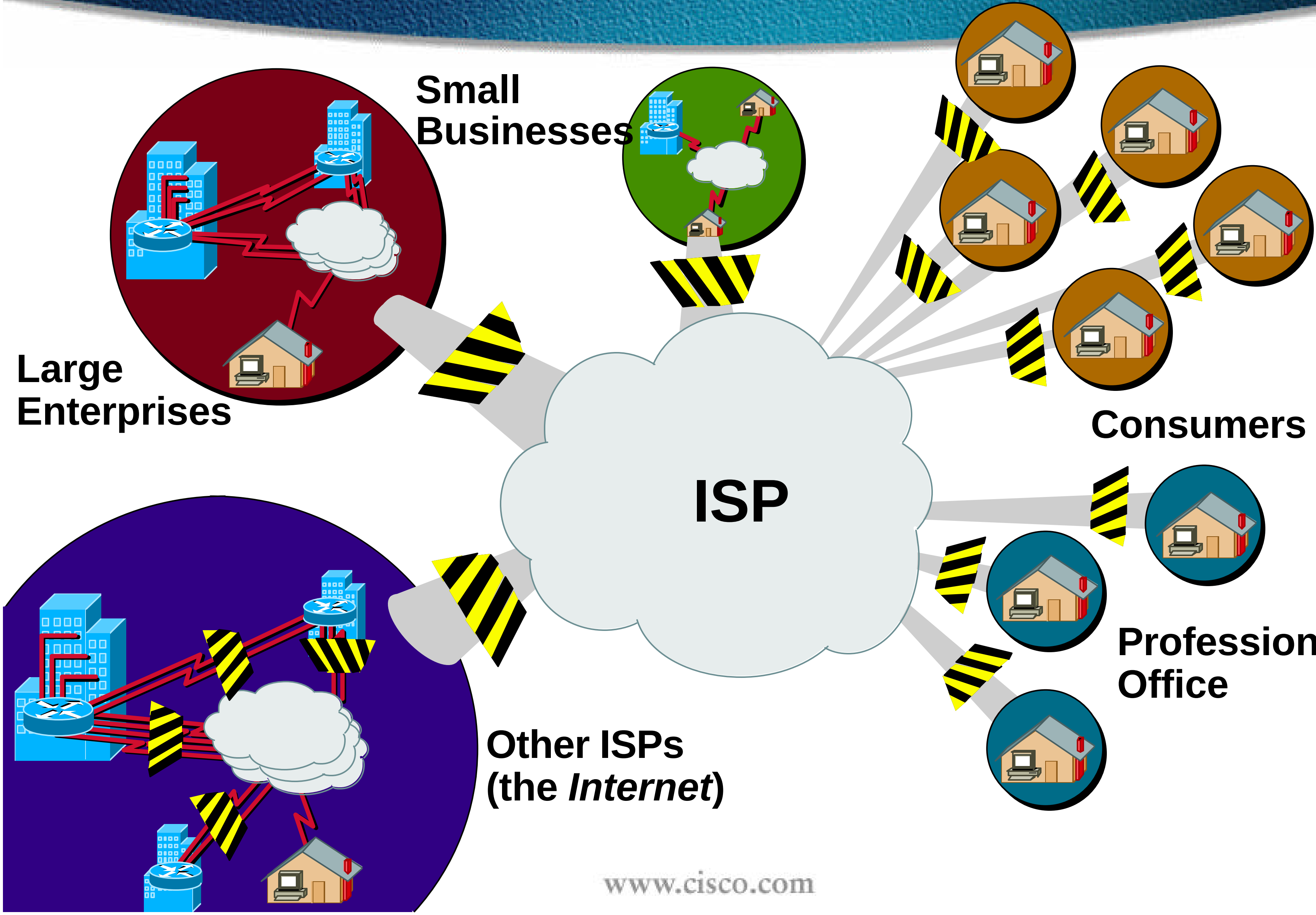
- **NetAid’s October 9th Event**

www.netaid.org

✓ System architected for 60 million hits per hour, one million hits per minute, or just over 16,000 transactions per second to support 50,000,000 users over a multi-day event … *while under constant cyber-probes and attacks.*

✓ NetAid was consistently probed and attacked through out the life of the event. It is an example of how today’s Internet networks need to be built - to ride out attacks, maintain the service, collect information on the attack, and counter the attack.

The ISP's World Today



Small Businesses

Large Enterprises

ISP

Consumers

Professional Office

Other ISPs (the *Internet*)

The ISP’s World Today

- **Changing Threat**
  - ✓ **User Friendly Tools make is easier for the amateur cyberpunks to do more damage**
  - ✓ **E-Commerce provides a monetary motivation**
  - ✓ **Direct attacks on the Internet’s core infrastructure means that the *NET* is not scared anymore.**

Source: Placeholder for Notes, etc. 14 pt., bold

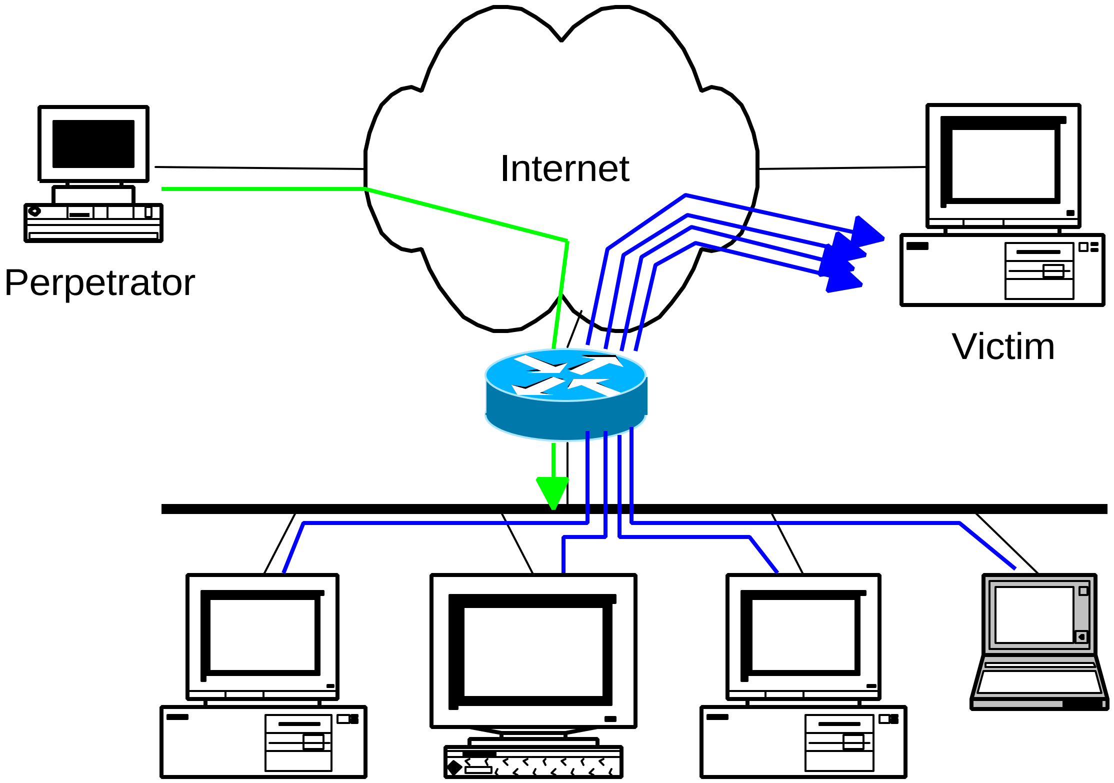
For example - *Smurfing*

- **Newest Denial of Service attack**
  - ✓ **Network-based, fills access pipes**
  - ✓ **Uses ICMP echo/reply packets with broadcast networks to multiply traffic**
  - ✓ **Requires the ability to send spoofed packets**
- **Abuses “bounce-sites” to attack victims**
  - ✓ **Traffic multiplied by a factor of 50 to 200**

For example - *Smurfing*

🟩 ICMP echo (spoofed source address of victim)
Sent to IP broadcast address

🟦 ICMP echo reply



Internet

Perpetrator

Victim

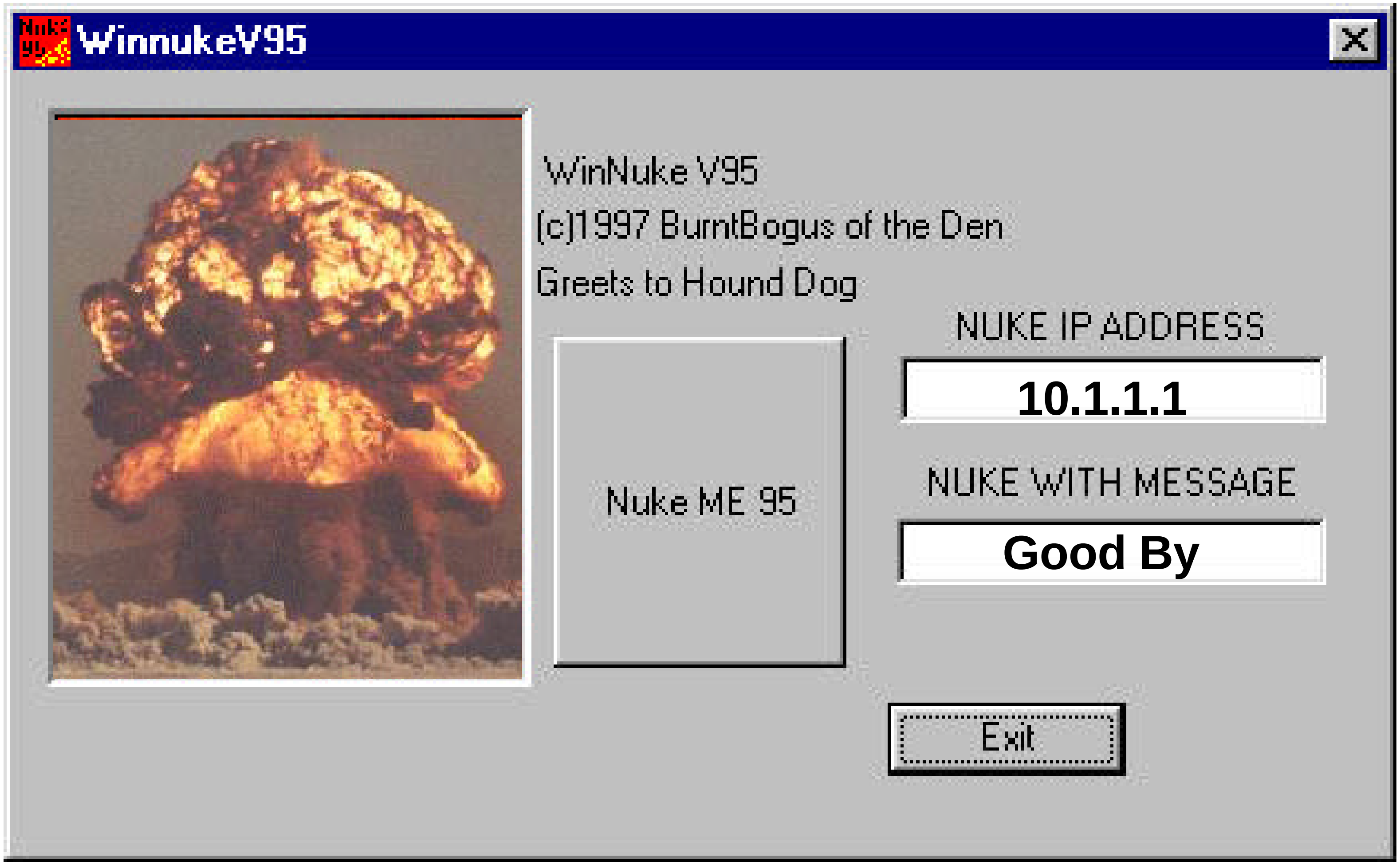
For example - *Smurfing*

- Perpetrator has T1 bandwidth available (typically a cracked account), and uses half of it (768 Kbps) to send spoofed packets, half to bounce site 1, half to bounce site 2
- Bounce site 1 has a switched co-location network of 80 hosts and T3 connection to net
- Bounce site 2 has a switched co-location network of 100 hosts and T3 connection to net

For example - *Smurfing*

- **(384 Kbps * 80 hosts) = 30 Mbps outbound traffic for bounce site 1**
- **(384 Kbps * 100 hosts) = 37.5 Mbps outbound traffic for bounce site 2**
- **Victim is pounded with 67.5 Mbps (!) from half a T1!**
- **Warning!** The newest source of high speed connections are in people’s homes. How many home’s with xDSL and Cable access have any sort of security?

Attack Methods—WinNuke



WinnukeV95

WinNuke V95

(c)1997 BurntBogus of the Den

Greets to Hound Dog

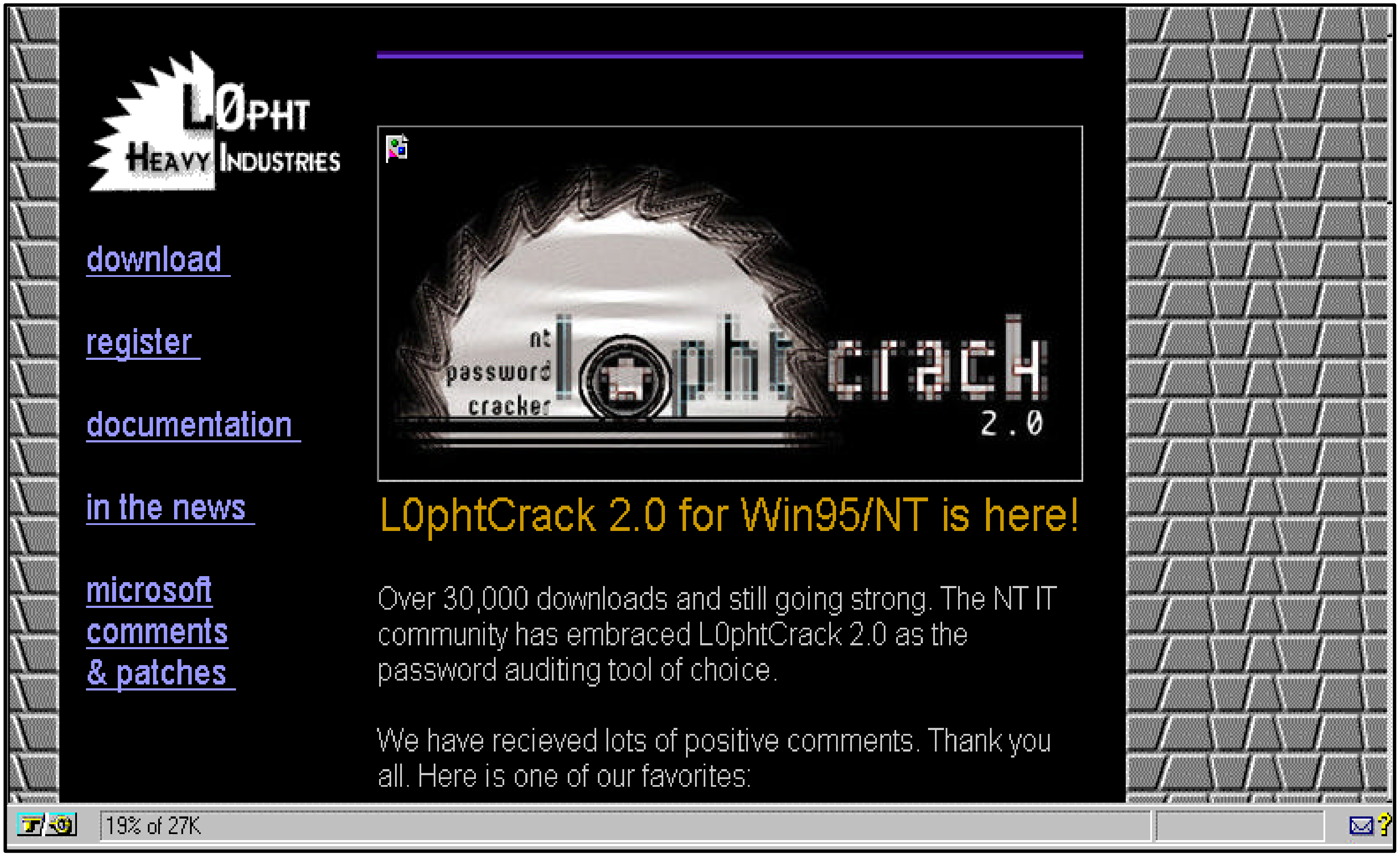
NUKE IP ADDRESS

10.1.1.1

NUKE WITH MESSAGE

Good By

Attack Methods—Crack Shareware



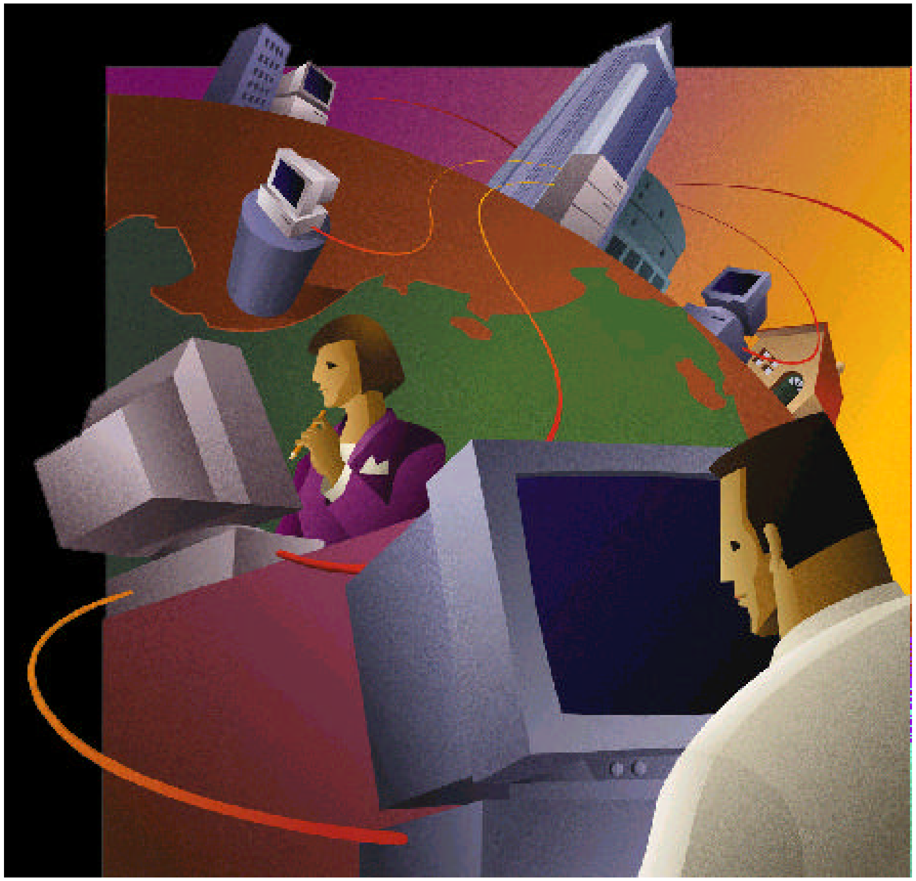
L0phtCrack 2.0 for Win95/NT is here!

Over 30,000 downloads and still going strong. The NT IT community has embraced L0phtCrack 2.0 as the password auditing tool of choice.

We have recieved lots of positive comments. Thank you all. Here is one of our favorites:

What do ISPs need to do?

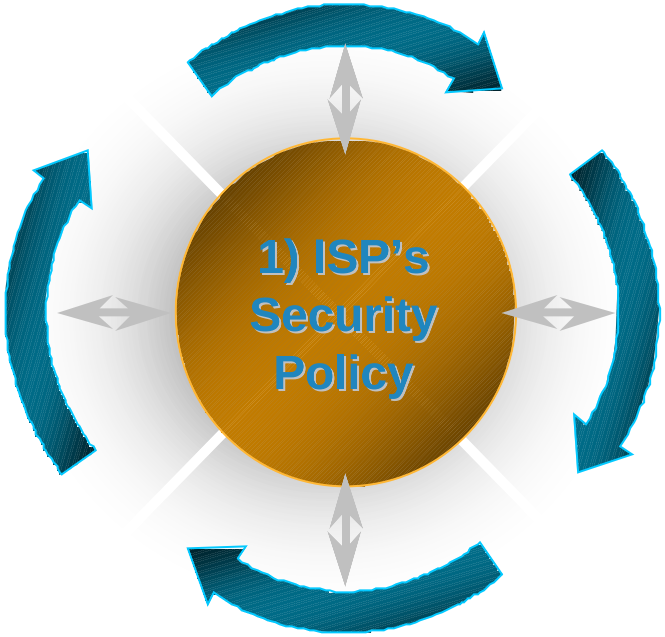
- ISPs need to:
  - ✓ Protect themselves
  - ✓ Help protect their customers from the Internet
  - ✓ Protect the Internet from their customers



What do ISPs need to do?

Security in a is not optional!

2) Secure
Firewall, Encryption, Authentication
(PIX, Cisco IOS, FW, IPSEC, TACACS+Radius)



3) Monitor and Respond
Intrusion Detection
(i.e. NetRanger)

4) Test
Vulnerability Scanning
(i.e. NetSonar, SPA)

5) Manage and Improve
Network Operations and Security Professionals

What do ISPs need to do?

- Implement Best Common Practices (BCPs)
  - ✓ ISP Infrastructure security
  - ✓ ISP Network security
  - ✓ ISP Services security
- Work with Operations Groups, Standards Organisations, and Vendors on new solutions

BCP Examples

- System Architecture
  - ✓ Use AAA for staff
  - ✓ Modular Network Design with Layered Security
  - ✓ Transaction Logging (SNMP, SYSLOG, etc.)
  - ✓ Peering, Prefix, and Route Flap Filters
  - ✓ Premises Security

- Features
  - ✓ Turn off unnecessary features
  - ✓ Routing Protocol MD5
  - ✓ Route Filters
  - ✓ Anti-Spoof filters or Unicast RPF
  - ✓ Rate Limiting filters on ICMP (active or scripts)

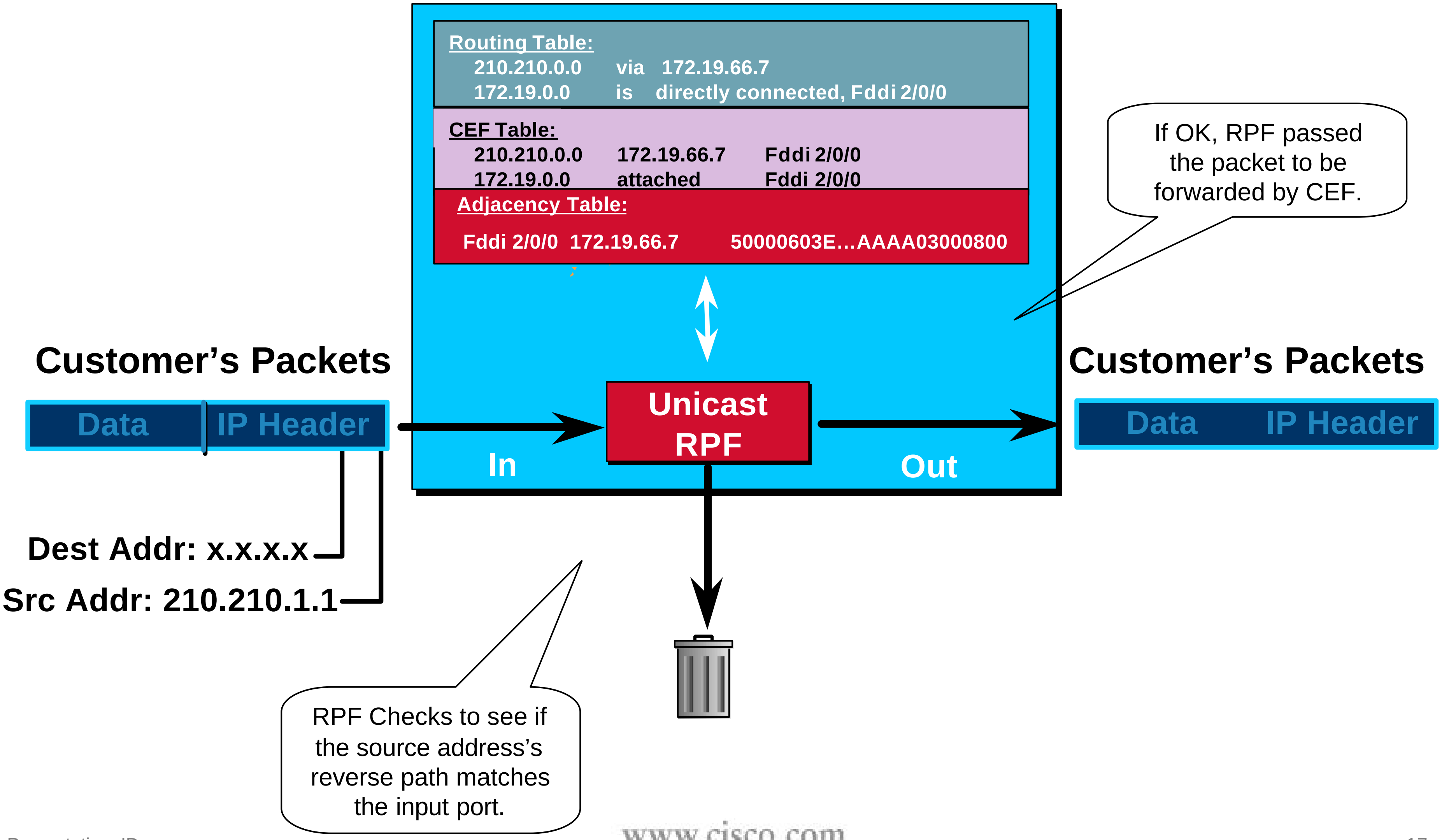
Hardware Vendor's Responsibilities

The roll of the hardware vendor is to support the network's objectives. Hence, there is a very synergistic relationship between the ISP and the hardware vendor to insure the network is resistant to security compromises.

Hardware Vendor's Responsibilities

- Cisco System's Example:
  - ✓ Operations People working directly with the ISPs
  - ✓ Emergency Reaction Teams (i.e. PSIRT)
  - ✓ Developers working with customers on new features
  - ✓ Security Consultants working with customers on attacks, audits, and prosecution.
  - ✓ *Individuals* tracking the hacker/phracker communities

For Example ...
CEF Unicast RPF



<u>Routing Table:</u>

```
    210.210.0.0     via   172.19.66.7
    172.19.0.0      is    directly connected, Fddi 2/0/0
```

<u>CEF Table:</u>

```
    210.210.0.0     172.19.66.7      Fddi 2/0/0
    172.19.0.0      attached         Fddi 2/0/0
```

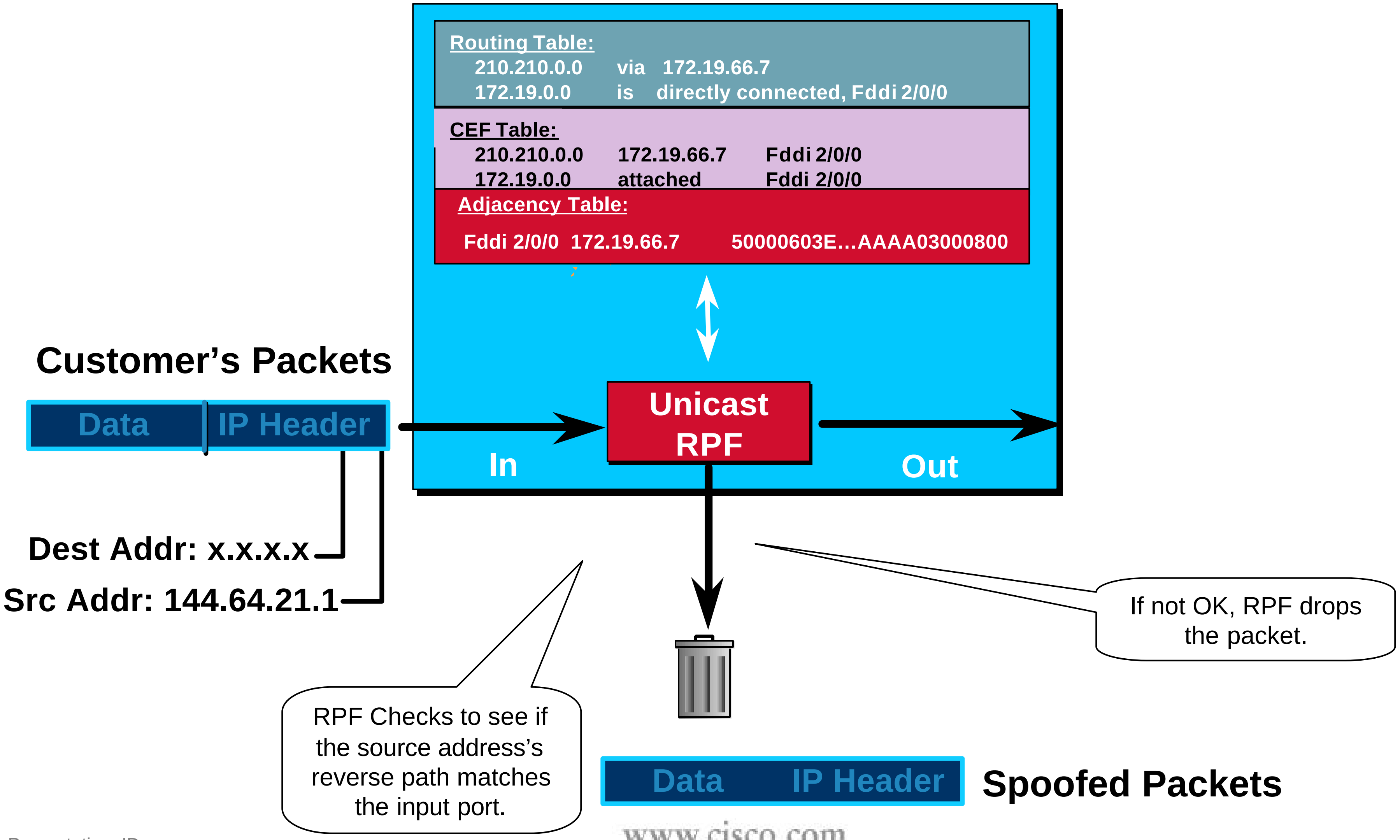
<u>Adjacency Table:</u>

```
   Fddi 2/0/0  172.19.66.7        50000603E…AAAA03000800
```

If OK, RPF passed the packet to be forwarded by CEF.

RPF Checks to see if the source address's reverse path matches the input port.

For Example ...
CEF Unicast RPF



Routing Table:

```
210.210.0.0     via   172.19.66.7
172.19.0.0      is    directly connected, Fddi 2/0/0
```

CEF Table:

```
210.210.0.0     172.19.66.7     Fddi 2/0/0
172.19.0.0      attached        Fddi 2/0/0
```

Adjacency Table:

```
Fddi 2/0/0  172.19.66.7       50000603E…AAAA03000800
```

RPF Checks to see if the source address’s reverse path matches the input port.

If not OK, RPF drops the packet.

For More Information…

URLs Referenced in the Presentation

- This presentation
  - ✓ http://www.cisco.com/public/cons/isp/document/Hoover-Security.pdf
- BCPs for ISPs - Essentials IOS Features Every ISP Should Consider
  - ✓ http://www.cisco.com/public/cons/isp/documents/
- Product Security Incident Response Team (PSIRT)
  - ✓ http://www.cisco.com/warp/public/707/sec_incident_response.shtml
- Improving Security on Cisco Routers
  - ✓ http://www.cisco.com/warp/public/707/21.html

For More Information…

Industry Resources

- http://www.icsa.net/library
  - ✓ Many security articles by National Computer Security Assoc., and great tutorial on firewalls
- ftp://info.cert.org
  - ✓ Published warnings and downloadable files of solutions for defeating various types
    of attacks that have been reported to Computer Emergency Response Team
- http://www-ns.rutgers.edu/www-security/reference.html
  - ✓ Llinks to Web sites, mailing lists, standards documents, etc., related to WWW and/or Internet security

Cisco Systems®

Empowering the Internet Generation℠