CISCO SYSTEMS

© 2003, Cisco Systems, Inc. All rights reserved.

Cisco.com

Quo Vadis Network Security?

Warsaw, Feb 26th 2003

Franjo Majstor
fmajstor@cisco.com

© 2003, Cisco Systems, Inc. All rights reserved.

Agenda

Cisco.com

- **Intro & Security Myths**
- **Security trends**
  - **Security Architecture**
  - **Integrated Security**
  - **Intelligent Secure Information Networks**
- **Summary**

© 2003, Cisco Systems, Inc. All rights reserved.

Introduction

There's No Longer a Question of Need
The Question Is How To Secure

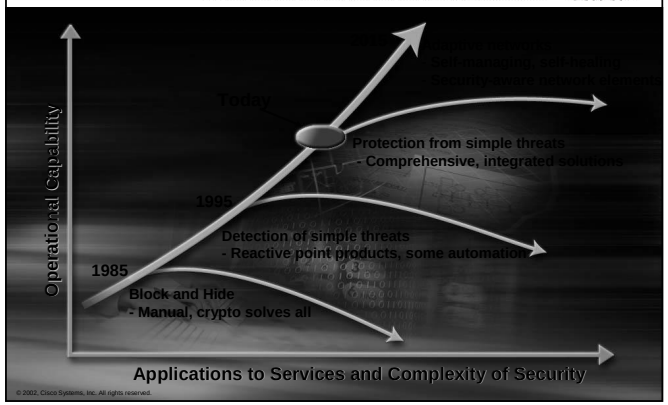
Cisco.com

	# of Organizations Reporting Breaches	% Suffering Breaches	Average Days Lost / Year	Average US$ Lost / Year	Highest Reported US$ Lost / Year
Virus Incident	390	81%	68	$162,000	$10,000,000
Email Intrusion (eg Spamming)	188	29%	12	$16,000	$200,000
Loss of s/w	102	16	19	$104,000	$3,000,000
Website Intrusion (eg Hacking)	70	12	34	$32,000	$200,000
Critical System Failure	70	12	30	$155,000	$4,000,000
Loss of Confidential Data	35	5	18	$197,000	$1,500,000
Tampering on I/O	23	4	14	$14,000	$100,000

Source: KPMG 2002 Information Security Survey

Network Security Evolution
From Simple Detection to Simple Protection

Cisco.com



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

Cisco Commitment to Security

Cisco.com

"Security threatens network availability which directly effects productivity"

John Chambers
President and CEO

"security is our single most important differentiator…our largest revenue opportunity over the next few years…"

Mario Mazzola
Chief Development Officer

© 2003, Cisco Systems, Inc. All rights reserved. 7

Comprehensive Security Integration

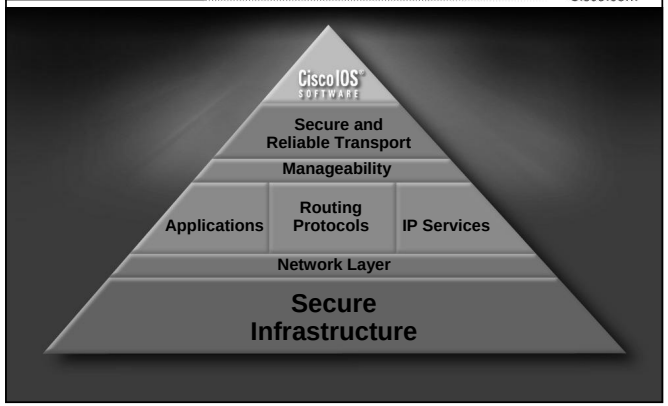
Cisco.com

"Networks have evolved from closed to more open, sophisticated systems. As a result, security threats have grown exponentially both at the network perimeter and from within. **Cisco is the first with an articulated strategy to integrate security services into the network infrastructure**. This is the most logical, cost-effective approach to secure today's extended network in a comprehensive fashion."

Zeus Kerravala
Vice President, Enterprise Computing
The Yankee Group

Cisco IOS® Software hardened by Secure Infrastructure

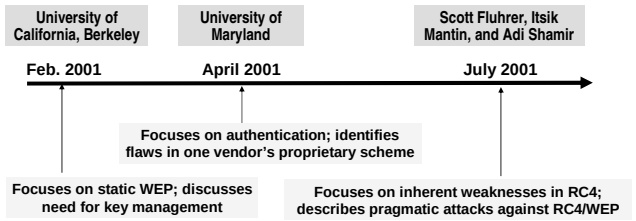
Cisco.com



Security Myths

Solved on a another layer - eg. WLAN?

Cisco.com

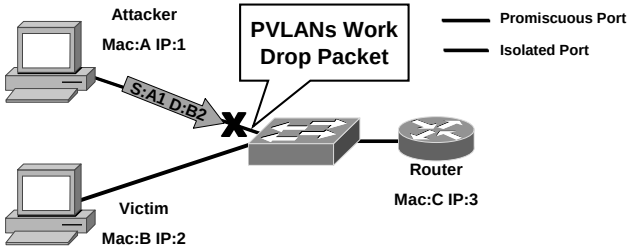


* "In practice, most installations use a single key that is shared between all mobile stations and access points. More sophisticated key management techniques can be used to help defend from the attacks we describe…"
– University of California, Berkeley report on WEP security, http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

© 2003, Cisco Systems, Inc. All rights reserved. 11

Solved with a single feature or product?

Cisco.com

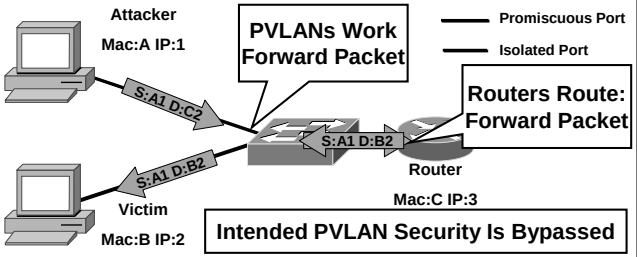


Independent security research firm @stake conducted a Security Review of the virtual LAN (VLAN) technology:
http://Cisco.com/en/US/products/hw/switches/ps708/products_white_paper09186a008013159f.shtml

© 2003, Cisco Systems, Inc. All rights reserved. 12

Private VLAN Attacks

Cisco.com



- Only allows unidirectional traffic (Victim will ARP for A and fail)
- If both hosts were compromised, setting static ARP entries for each other via the router will allow bi-directional traffic
- Most firewalls will not forward the packet like a router
- Note: this is not a PVLAN vulnerability as it enforced the rules!

© 2003, Cisco Systems, Inc. All rights reserved. 13

Solved with a new protocol - eg. IPv6?

Cisco.com

- Security & IPv6:
  - Nothing IP4 doesn't do - IPsec runs in both
  - Does a lot dynamically on L3 (via ICMP), hence remove all of L2 problems, right?
  - Autoconfiguration

ICMP w/o IPsec AH⇔ gives exactly same level of security as ARP for IPv4 (none)

Bootstrap security problem!

Security mechanisms built into discovery protocol ⇔ None.

Bootstrap security problem!

From RFC 2462:

« If a duplicate @ is discovered … the address *cannot* be assigned to the interface…»

⇔ What if: Use MAC@ of the node you want to DoS and fabricate its IPv6 @

© 2003, Cisco Systems, Inc. All rights reserved. 14

Layer above - Port 80: The Battleground

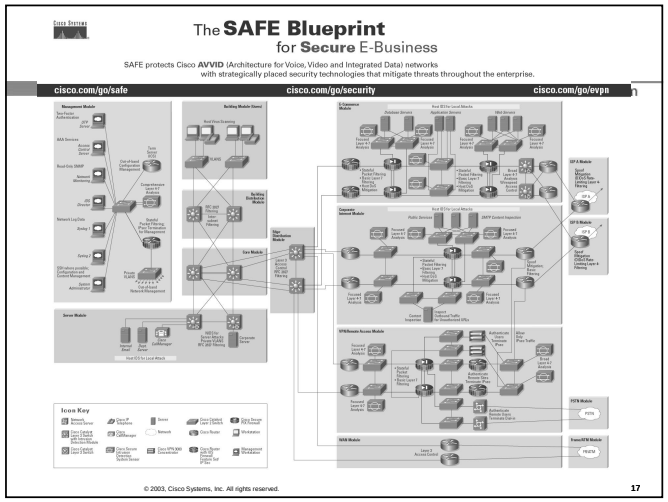
Cisco.com

- Typically opened through firewalls
- It can be used to attack other hosts through
- Tunneling through the SSL port also hides the activity from IDS

http://www.nocrew.org/software/httptunnel.html

© 2003, Cisco Systems, Inc. All rights reserved. 15

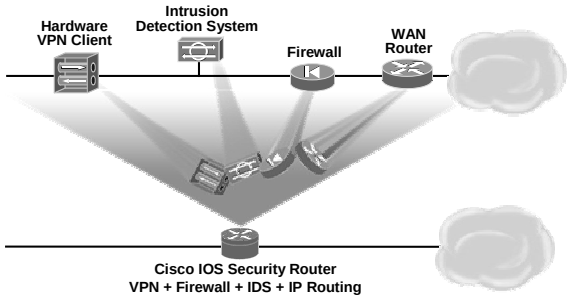
Security Architecture & Integrated Security



Convergence of embedded Security Functions

Cisco.com

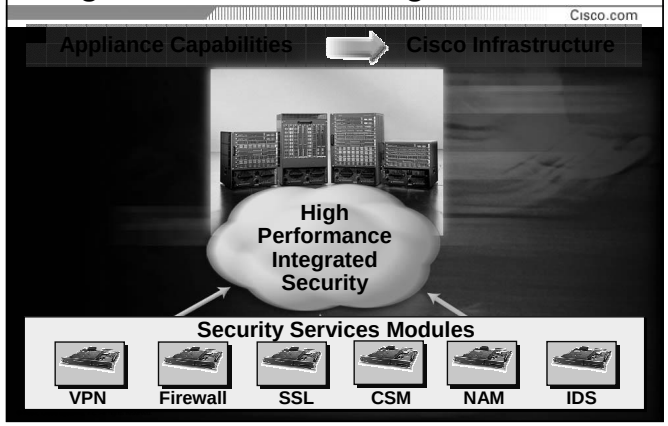
- IPsec VPN, Inline Stateful Firewall, IDS, and IP Routing
- Eases management burden, reduces cost of ownership



© 2003, Cisco Systems, Inc. All rights reserved. 18

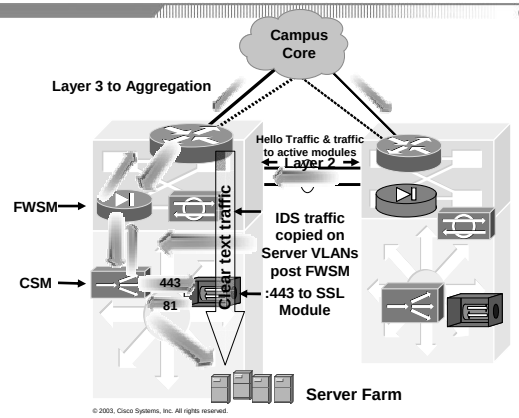
Integration into Switching Infrastructure

Cisco.com



SAFE Architecture: CSM SSLSM FWSM IDSM

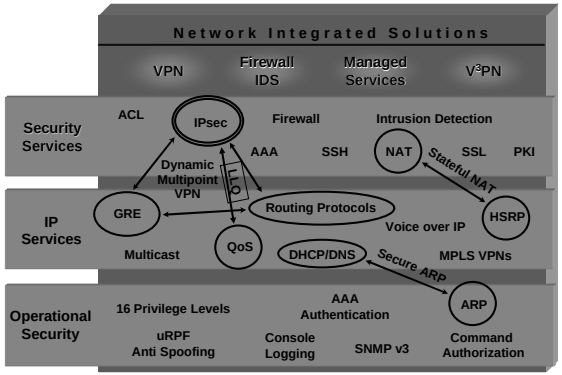
Cisco.com



© 2003, Cisco Systems, Inc. All rights reserved. 20

Leading-Edge IP Services Integration
Integrating Security With IP Services

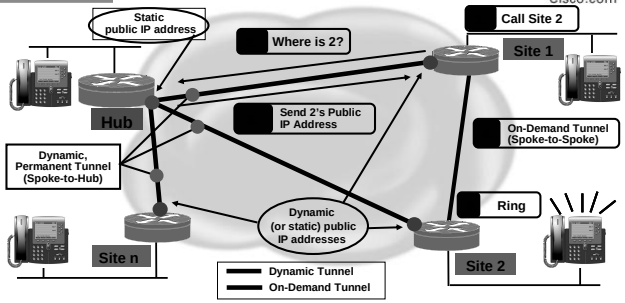
Cisco.com



© 2003, Cisco Systems, Inc. All rights reserved. 21

P2P & Cisco IOS IPsec VPN Integration
Dynamic Multipoint VPN

Cisco.com

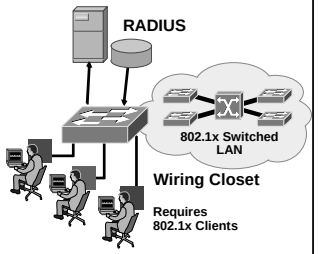


- Reduced latency and jitter
- Improved performance
- Increased scalability
- Easy to deploy and maintain

© 2003, Cisco Systems, Inc. All rights reserved. 22

Integrated Network Identity Services

Cisco.com



802.1x

Protects network access by allowing RADIUS server to authenticate user allowing/disallowing access to the network.

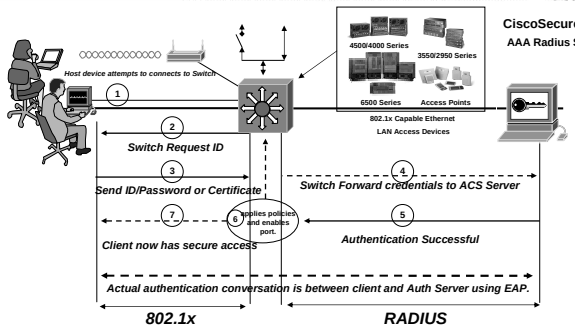
DHCP Interface Tracker (option 82)

Tracks where a user is physically connected on a network by providing both switch and port ID to a DHCP Server.

© 2003, Cisco Systems, Inc. All rights reserved. 23

Secure Identity-Based Network Access

Cisco.com



The switch detects the 802.1x compatible client, forces authentication, then acts as a middleman during the authentication, Upon successful authentication the switch sets the port to forwarding, and applies the designated policies.

© 2003, Cisco Systems, Inc. All rights reserved. 24

Critical Infrastructure Assurance Group

Cisco.com

"Assuring critical services in the Information Age" ***through***

- ***Communications & Awareness***
- ***Incident Response***
- ***Education & Training***
- ***Research***
- ***Product Enhancement***

http://Cisco.com/go/ciag

© 2003, Cisco Systems, Inc. All rights reserved. 25

Intelligent Secure Information Networks

Cisco Security Agent: Accelerating the Endpoint Transition

Cisco.com

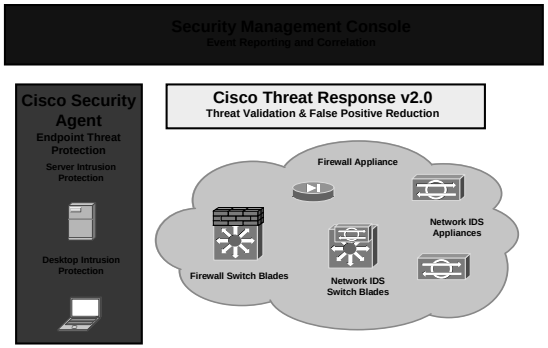
Security at network endpoints is changing…

- **From Intrusion Detection to Protection**
  - At the desktop and server
  - Extending to PDAs and other devices
- **From Signature-based to Policy-Based**
  - Stops new attacks that attempt malicious activity
  - Policies allow "good" behavior and prevent "bad" behavior
- **From Data-Heavy to Highly Accurate**
  - Automatic Correlation + Defense in depth = Near-zero false positives
- **From Updates to Zero-Update Protection**
  - Behavior-based architecture changes desktop paradigm

© 2003, Cisco Systems, Inc. All rights reserved. 27

Cisco Intrusion Protection Solutions

Cisco.com



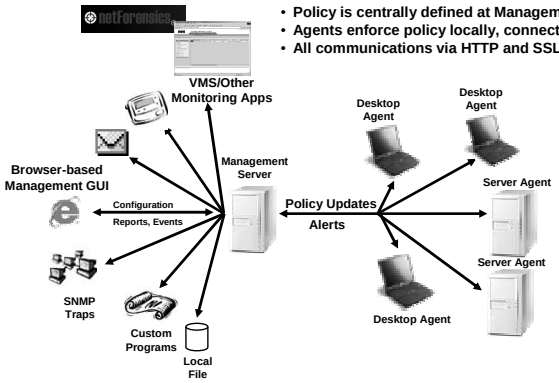
© 2003, Cisco Systems, Inc. All rights reserved. 28

fmajstor@cisco.com, Quo Vadis Network Security, Warsaw Feb 16th 2003, Copyright © 2003, Cisco Systems, Inc. All rights reserved.

Cisco Security Agent: Solution Architecture

Cisco.com

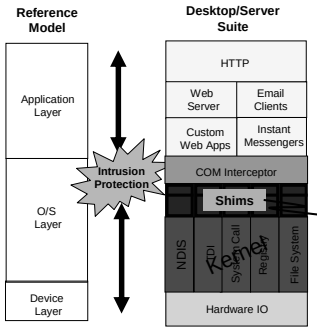
- Policy is centrally defined at Management Server
- Agents enforce policy locally, connected or not
- All communications via HTTP and SSL



© 2003, Cisco Systems, Inc. All rights reserved. 29

Cisco Security Agent: The Conceptual View

Cisco.com



Product Features:

- Host Intrusion Protection
- Distributed Firewall
- OS Hardening
- Malicious Code Sandbox
- Buffer Overflow Protection
- Web Server Protection
- Instant Messenger security

Architectural Features:

- Comprehensive *Kernel Shims*
- Low Computational Overhead
- *Virtual Bus* that can be extended to other applications

© 2003, Cisco Systems, Inc. All rights reserved. 30

Cisco Security Agent Aggregates Multiple Endpoint Security Functions

Cisco.com

	Cisco Secure Agent	Conventional Distributed Firewall	Conventional Host-based IDS
Desktop/Laptop Protection	X	X	
Block Incoming Network Requests	X	X	
Block Outgoing Network Requests	X	X	
Stateful Packet Analysis	X	X	
Detect /Block Port Scans	X	X	
Detect /Block Network DoS Attacks	X	X	
Detect /Prevent Malicious Applications	X		X
Detect/Prevent Known Buffer Overflows	X		X
Detect/Prevent Unknown Buffer Overflows	X		X
Detect/Prevent Unauthorized File Modification	X		X
Operating System Lockdown	X		X

© 2003, Cisco Systems, Inc. All rights reserved. 31

Cisco Security Agent Complements Traditional Desktop Anti-Virus SW

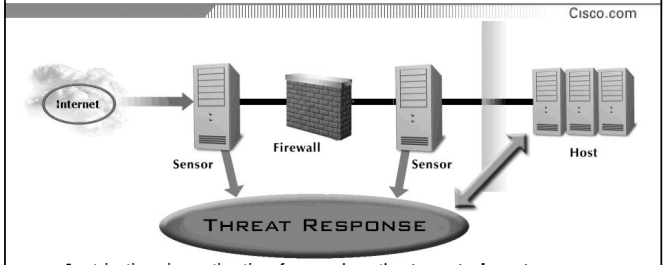
Cisco.com

	Cisco Secure Agent	Anti-Virus
Malicious Code Protection		
Stop Known Virus/Worm Propagation	X	X
Stop Unknown Virus/Worm Propagation	X	
Scan/Detect Infected Files		X
"Clean" Infected Files		X
Identify Viruses/Worms by Name		X
No Signature Update Required	X	
Distributed Firewall Functionality	X	
Operating System Lockdown	X	
Correlates Events Across Endpoints	X	

© 2003, Cisco Systems, Inc. All rights reserved. 32

Intelligent Network Intrusion Protection

Cisco.com



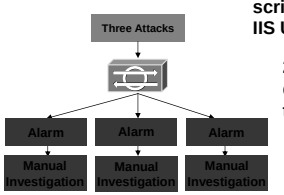
Just-in-time investigation focused on the **targeted system**

- **Based on processes taught at SANS and CSI and used by expert network security professionals**
- **No broad based scanning of network for use hours or days later**
- **Not an event correlation solution**
- **No need for deployment of software across the enterprise**

© 2003, Cisco Systems, Inc. All rights reserved. 33

Network Intrusion Protection without Intelligent Investigation

Cisco.com



15 minutes manually investigating each alarm

Total elapsed time = 45 minutes

1. An attacker launches auto-scanner script to search for a common Microsoft IIS Unicode vulnerability

2. The IDS sensor reports a number of detected attacks against systems in the network

3. The security administrator sees several real attack events on their IDS and correlation screens. Time is wasted investigating each one.

© 2003, Cisco Systems, Inc. All rights reserved. 34

Cisco Threat Response

Cisco.com

Was the attack successful? (Eliminate & Escalate)

- **Target OS or Device Vulnerability Check (Level 1)**
- **Patch Level Check (Level 1)**
- **Detailed System Investigation (Level 2)**
  - **Includes analysis of registry files, web logs, file system, etc.…**

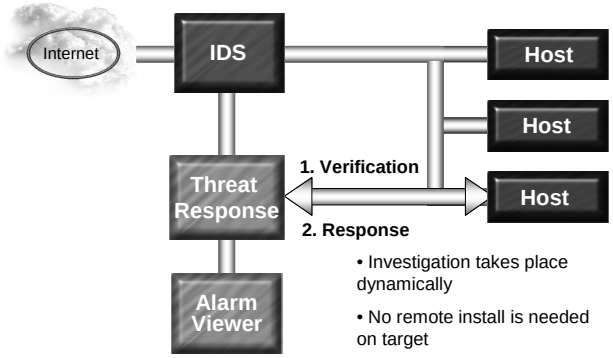
What can de done about it? (Remediate)

- **Forensic Evidence Retrieval**
  - **Includes capture of impacted files and logs**

5

Cisco Threat Response in Action

Cisco.com

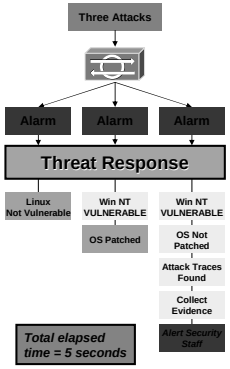


- Investigation takes place dynamically
- No remote install is needed on target

© 2003, Cisco Systems, Inc. All rights reserved. 36

Intrusion Protection with Intelligent Investigation - Cisco Threat Response

Cisco.com



1. **An attacker launches auto-scanner script to search for a common Microsoft IIS Unicode vulnerability**
2. **The IDS sensor reports a number of detected attacks against systems in the network**
3. **Threat Response technology quickly assesses the target in real-time without prior network knowledge or installed remote agent software.**

- **Investigation steps for successful IIS Unicode Attack:**
  1. Does the attack target this OS type?
  2. Is the OS vulnerable?
  3. Are there traces of a successful attack?
  4. Copy and secure forensic evidence
  5. Alert administrator to real and confirmed attack

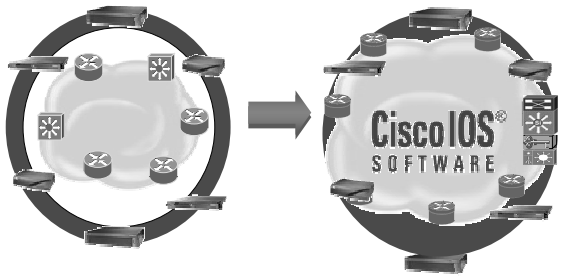
© 2003, Cisco Systems, Inc. All rights reserved.
37

Evolution of Network Security

Cisco.com

Additional Layers of Defense within the Network

Before **Now**



Increasing role of Security-Integrated Cisco IOS devices

© 2003, Cisco Systems, Inc. All rights reserved.
38

Instead of a Summary

Cisco.com

"Only two things are infinite, the universe and a human stupidity, and I'm not sure about the former."

Albert Einstein

"If you think technology can solve your security problems, than you don't understand the problems and you don't understand the technology."

Bruce Schneier, Secrets & Lies - Digital Security in a Networked World

"...the human factor is truly security's weakest link."

Kevin D. Mitnick, The Art of Deception

Thank you!

Cisco.com

Quo Vadis Network Security?

fmajstor@cisco.com

CISCO SYSTEMS

EMPOWERING THE
INTERNET GENERATION℠

www.cisco.com

41

 Copyright © 2003, Cisco Systems, Inc. All rights reserved.