Network Security

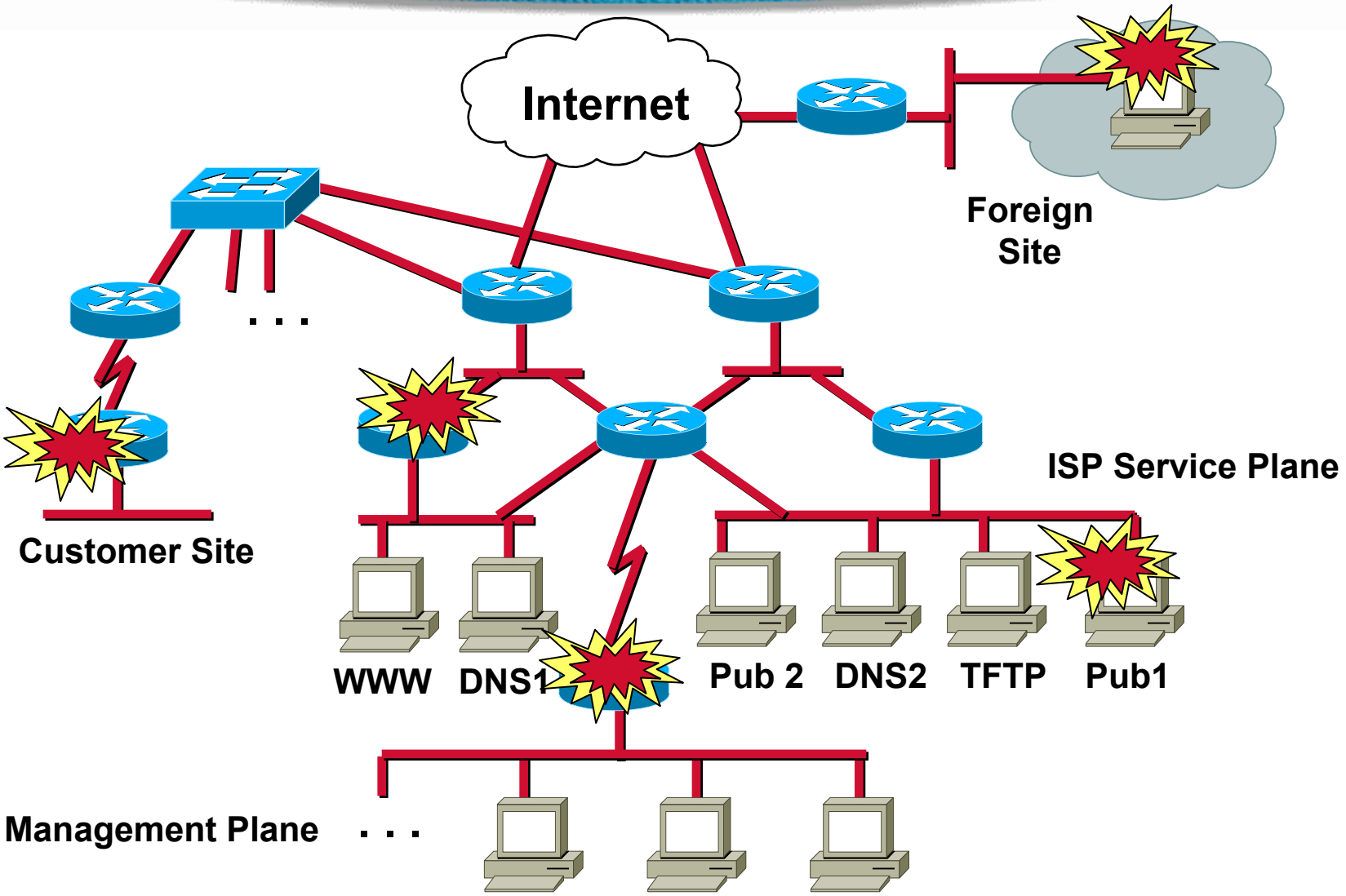
ISOC NTW 2000

Cisco Systems

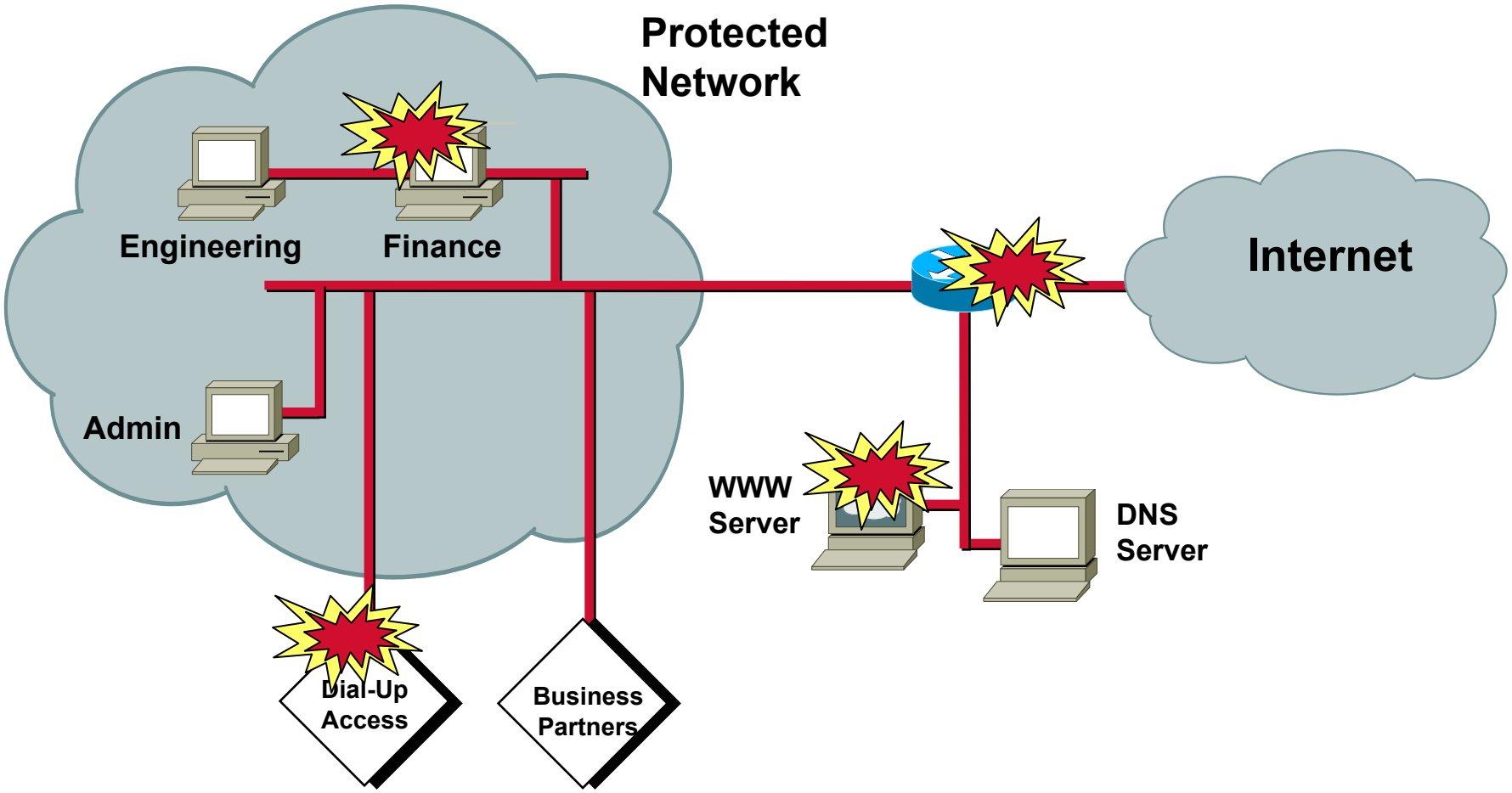
Introduction

Network Security Components

ISP Example



Enterprise Example

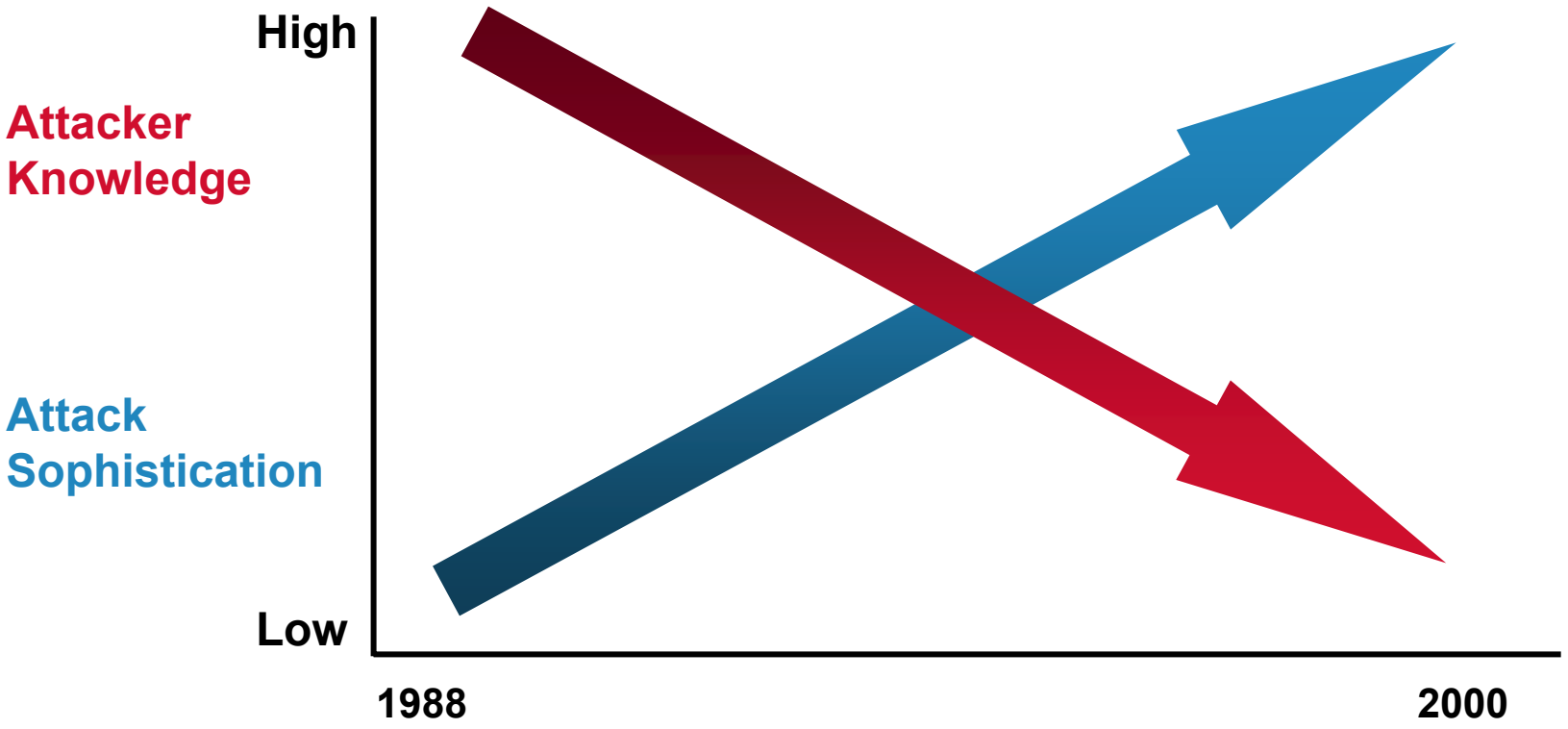


Current Threats and Attack Methods

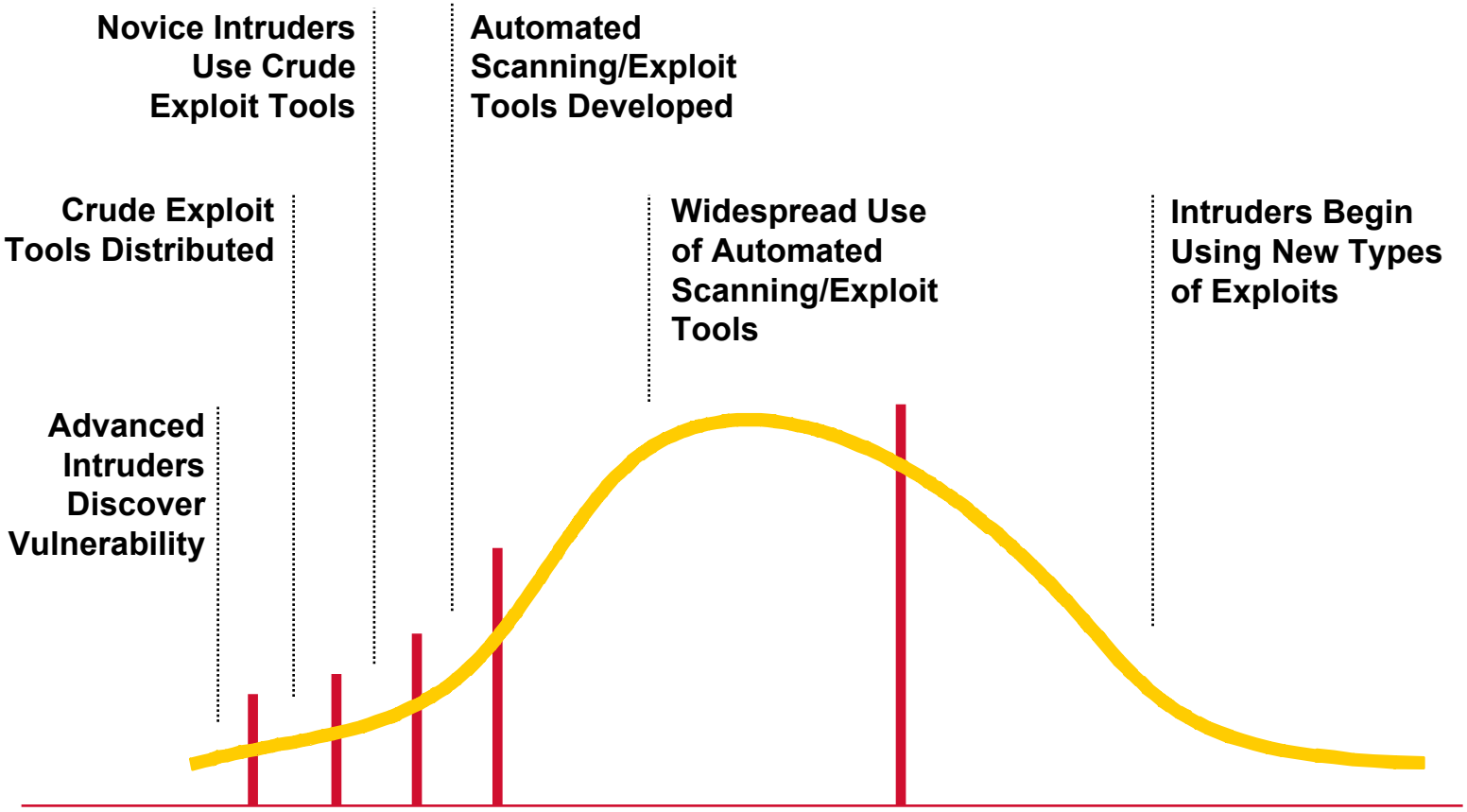
Attack Trends

- Exploiting passwords and poor configurations
- Software bugs
- Trojan horses
- Sniffers
- IP address spoofing
- Toolkits
- Distributed attacks

Attack Trends



Vulnerability Exploit Cycle



Source: CERT Coordination Center

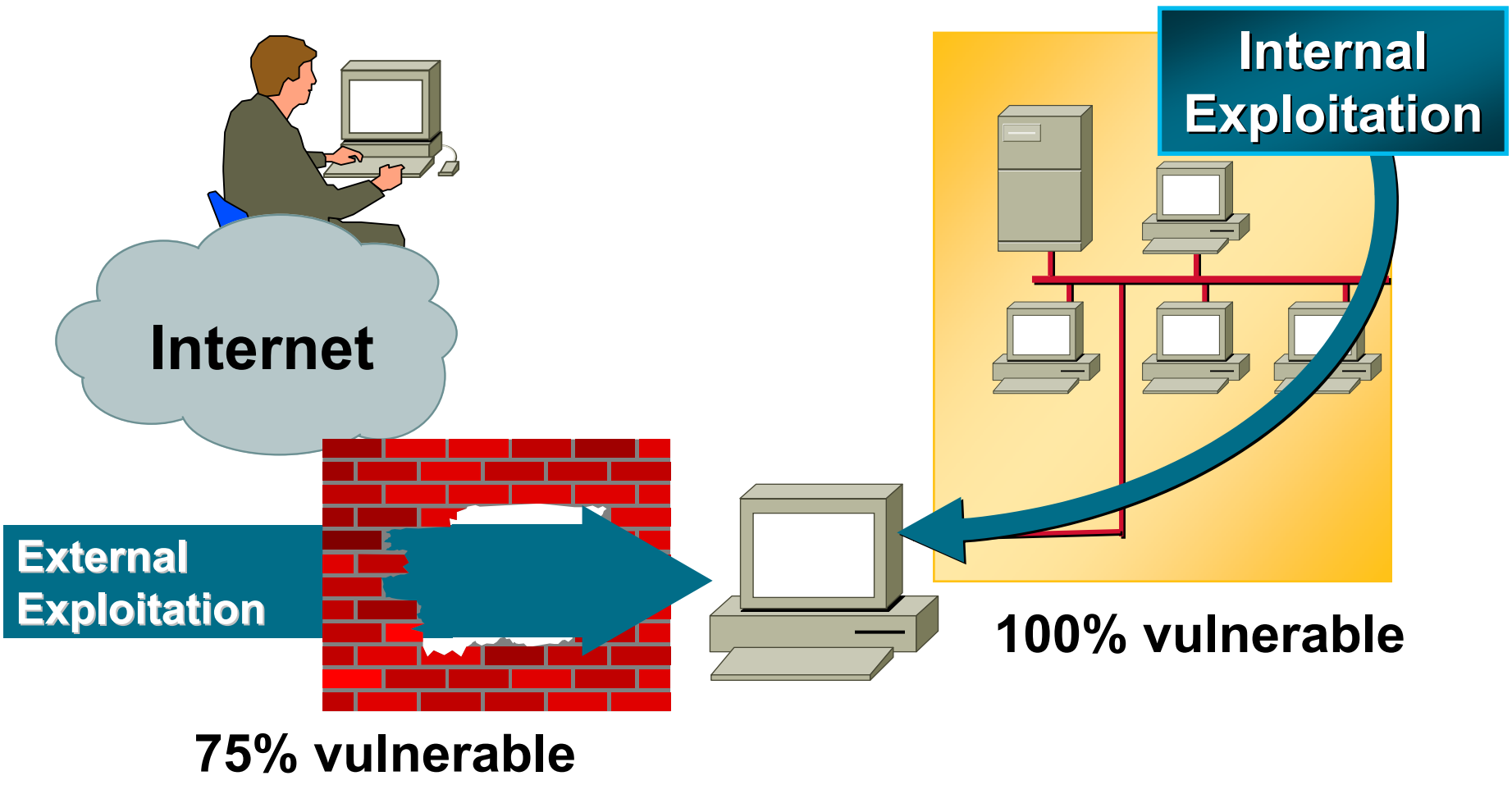
Increasingly Serious Impacts

- $10M transferred out of one banking system
- Loss of intellectual property - $2M in one case, the entire company in another
- Extensive compromise of operational systems - 15,000 hour recovery operation in one case
- Alteration of medical diagnostic test results
- Extortion - demanding payments to avoid operational problems

Evolving Dependence

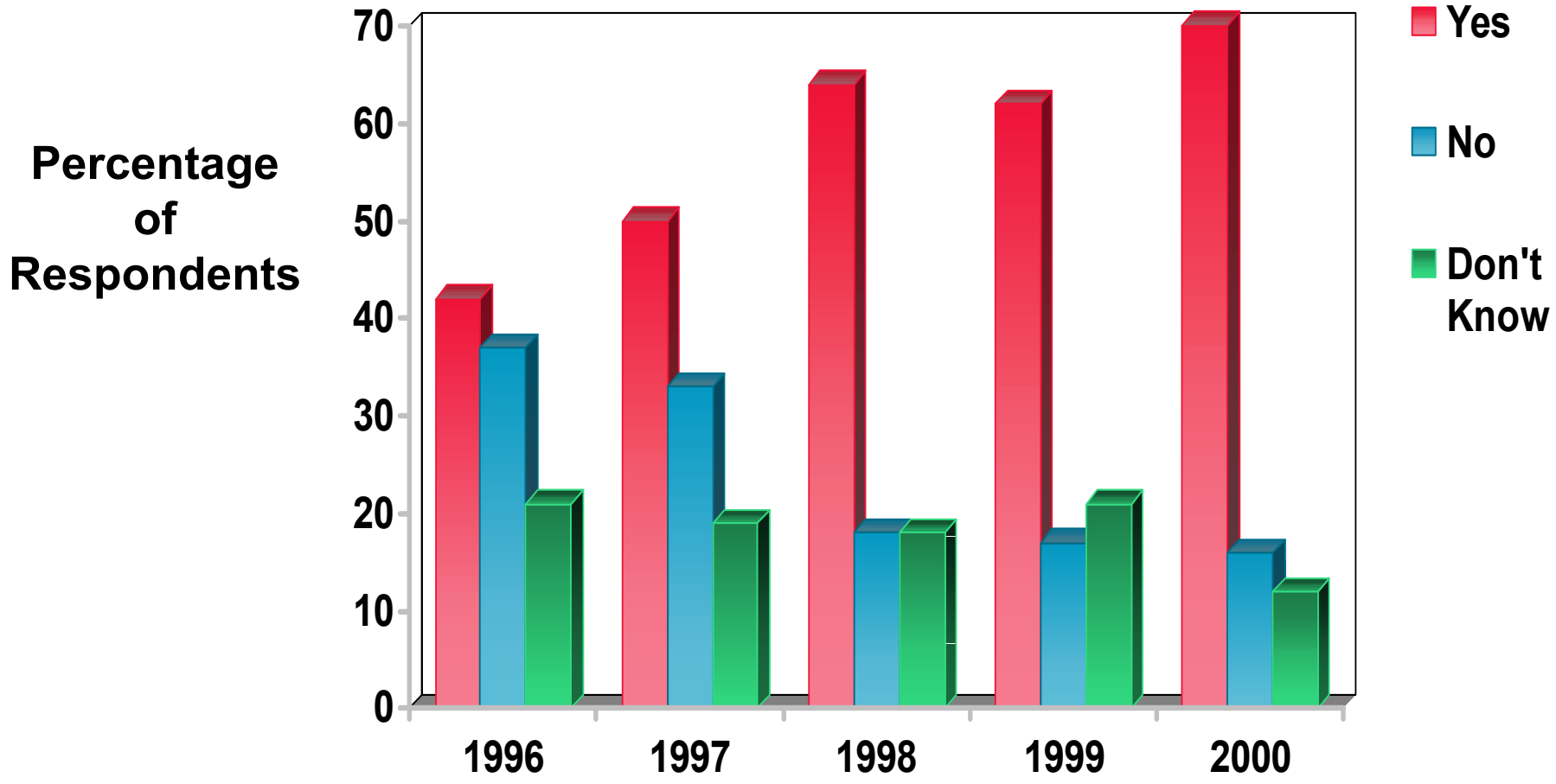
- Networked appliances/homes
- Wireless stock transactions
- On-line banking
- Critical infrastructures
- Business processes

The Community's Vulnerability



Source: Cisco Security Posture Assessments 1996-1999

Unauthorized Use



Source: 2000 CSI/FBI Computer Crime and Security Survey

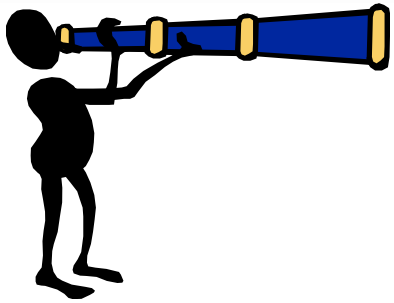
Conclusion

Sophisticated attacks
+
Dependency
+
Vulnerability

Classes of Attacks

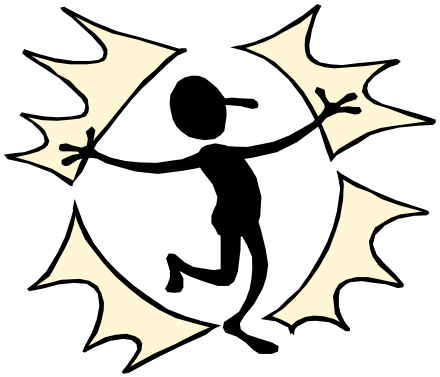
- **Reconnaisance**

  Unauthorized discovery and mapping of systems, services, or vulnerabilities



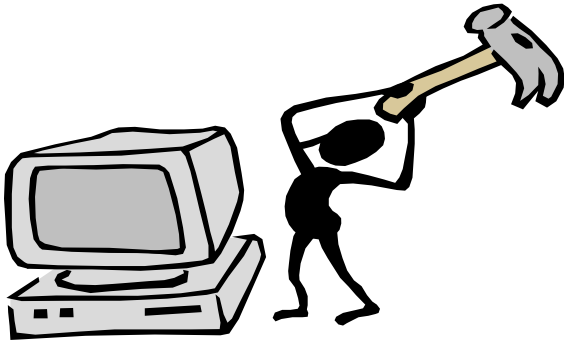
- **Access**

  Unauthorized data manipulation, system access, or privilege escalation

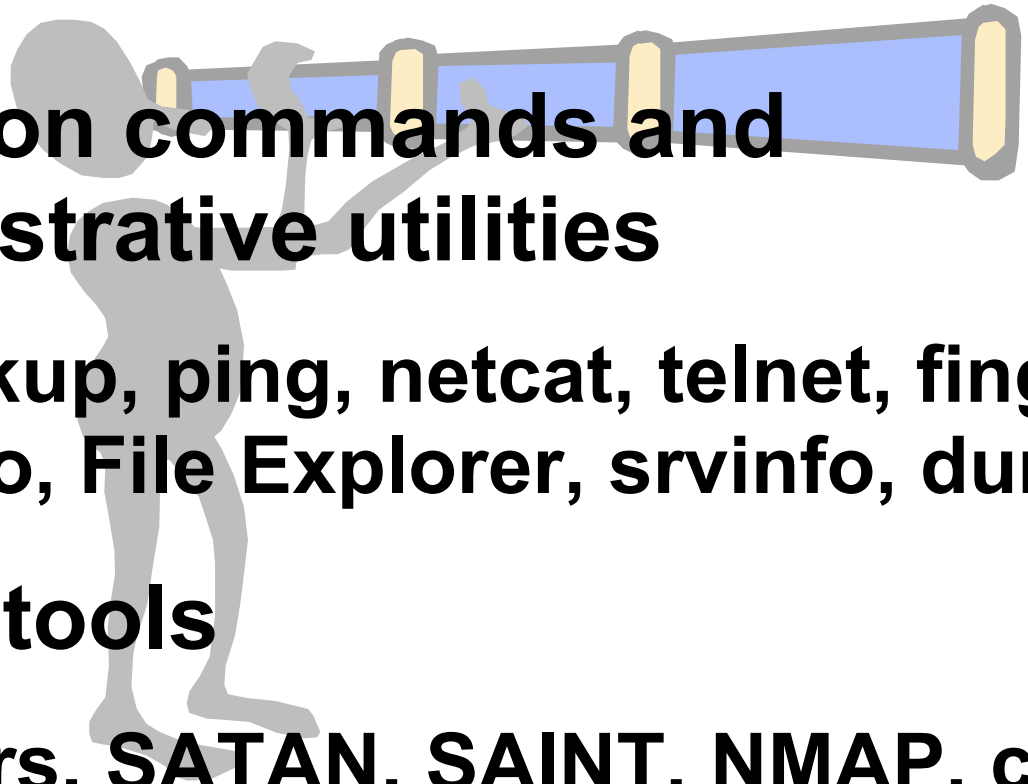


- **Denial of Service**

  Disable or corrupt networks, systems, or services



Reconnaissance Methods



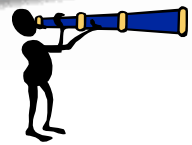
- **Common commands and administrative utilities**

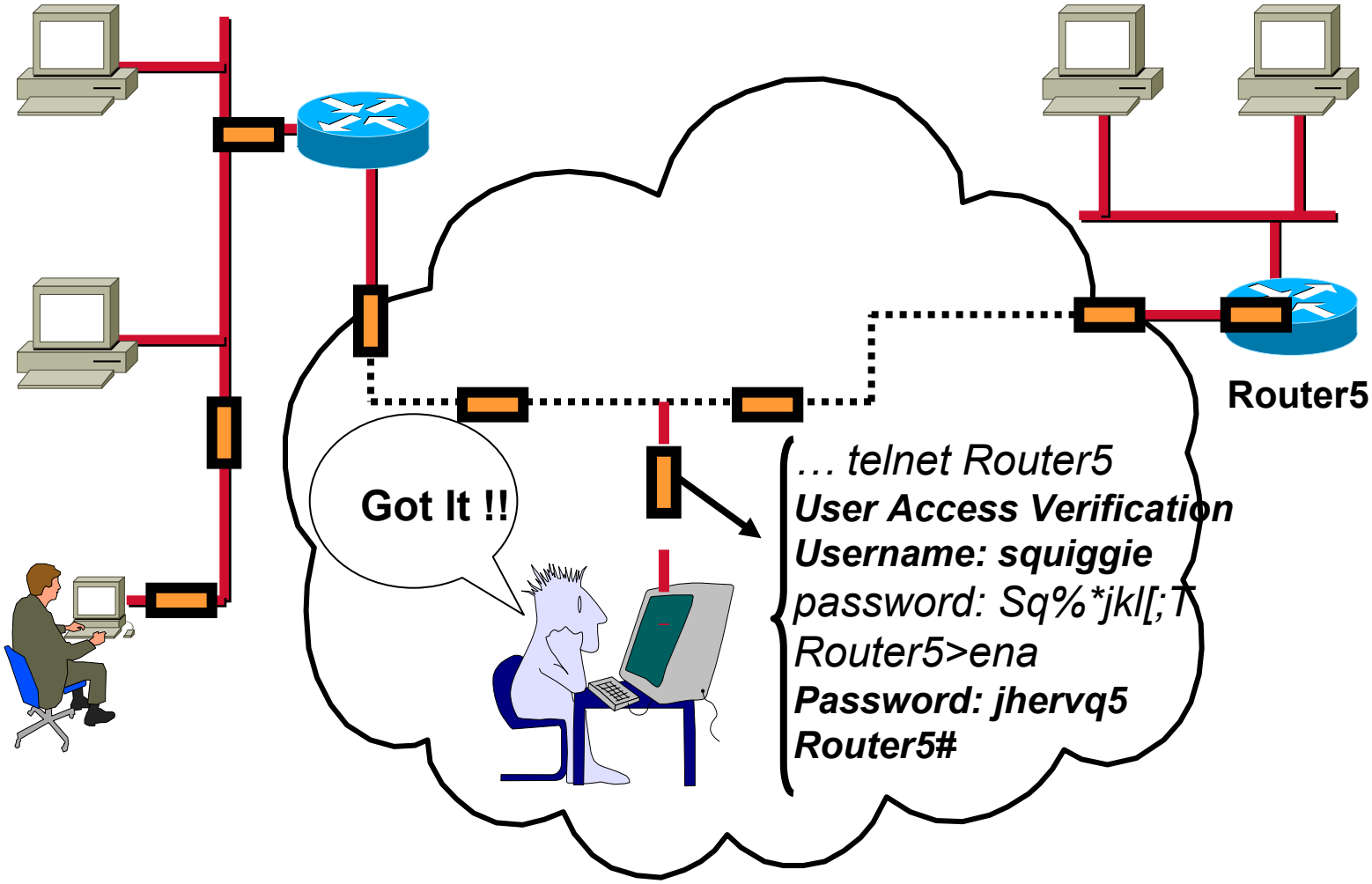
  nslookup, ping, netcat, telnet, finger, rpcinfo, File Explorer, srvinfo, dumpacl

- **Public tools**

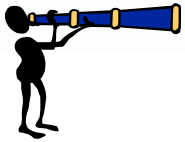
  Sniffers, SATAN, SAINT, NMAP, custom scripts

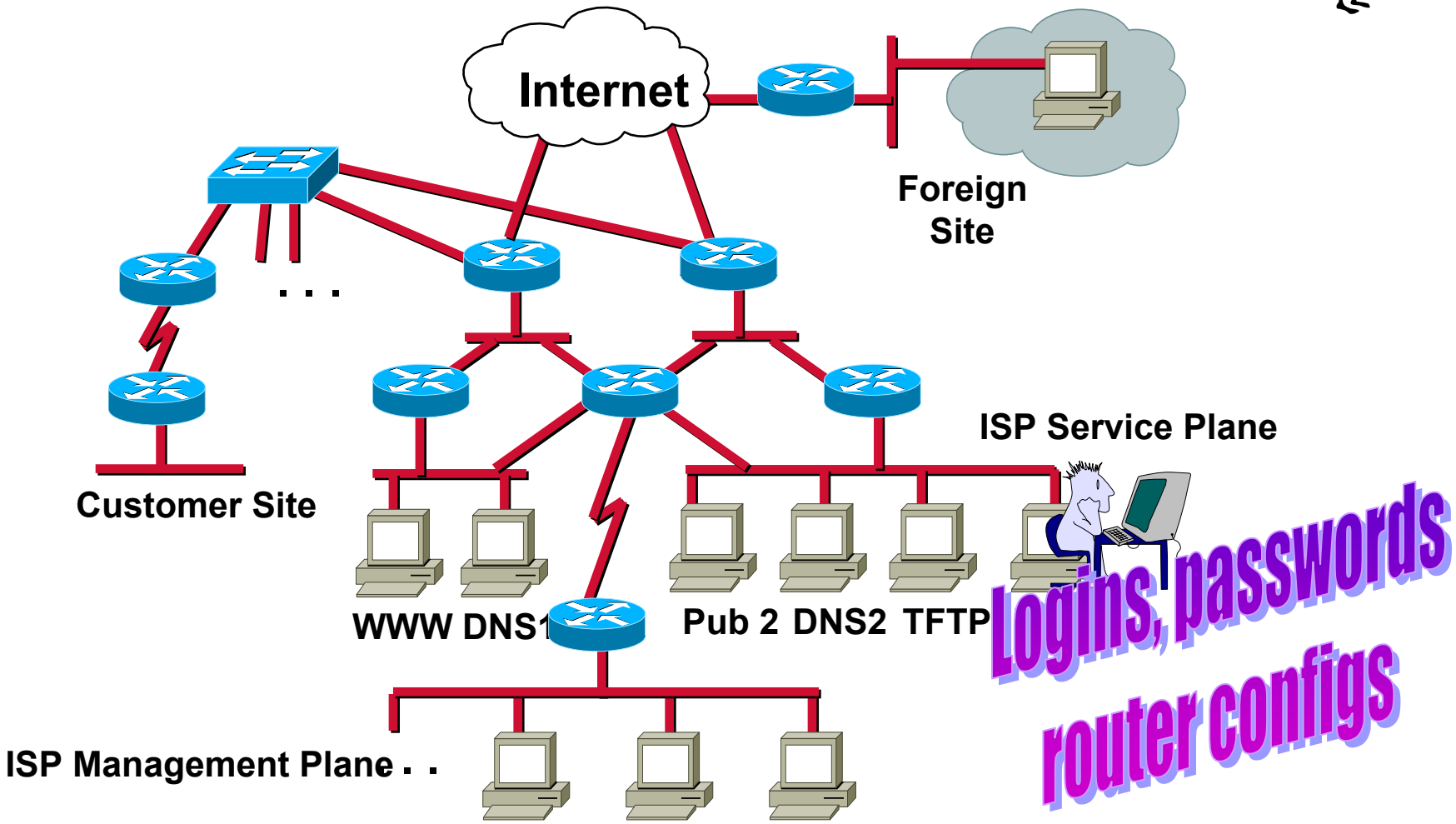
Network Sniffers



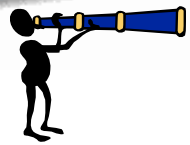


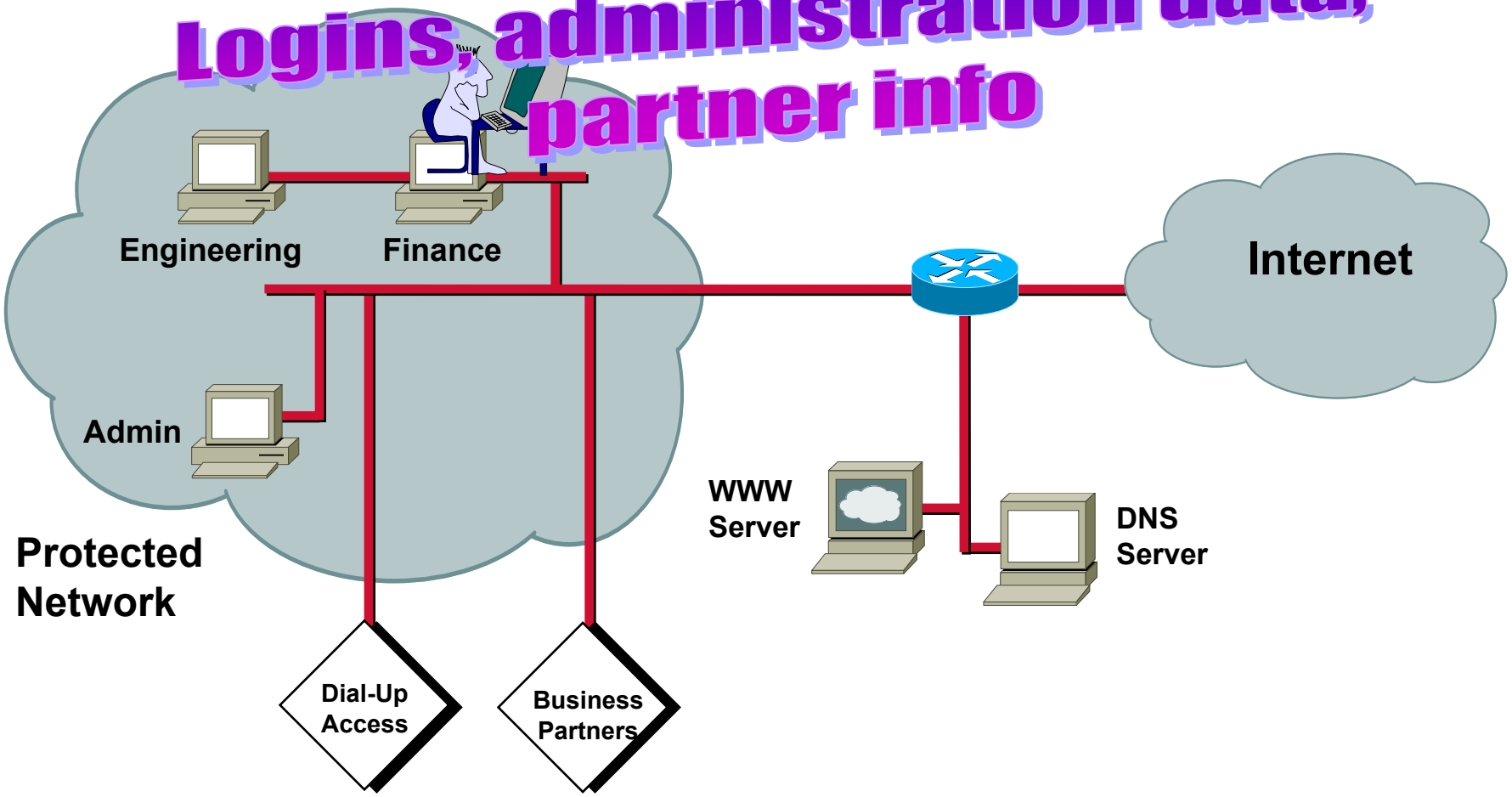
ISP Example



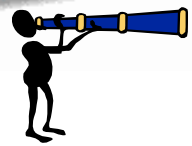


Enterprise Example



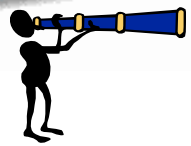


nmap



- **network mapper is a utility for port scanning large networks:**
  - **TCP connect() scanning,**
  - **TCP SYN (half open) scanning,**
  - **TCP FIN, Xmas, or NULL (stealth) scanning,**
  - **TCP ftp proxy (bounce attack) scanning**
  - **SYN/FIN scanning using IP fragments (bypasses some packet filters),**
  - **TCP ACK and Window scanning,**
  - **UDP raw ICMP port unreachable scanning,**
  - **ICMP scanning (ping-sweep)**
  - **TCP Ping scanning**
  - **Direct (non portmapper) RPC scanning**
  - **Remote OS Identification by TCP/IP Fingerprinting (nearly 500)**
  - **Reverse-ident scanning.**

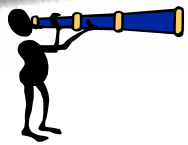
nmap



- nmap {Scan Type(s)} [Options] <host or net list>
- Example:

```
my-unix-host% nmap -sT my-router
Starting nmap V. 2.53 by fyodor@insecure.org ( www.insecure.org/nmap/ )
Interesting ports on my-router.example.com (10.12.192.1)
(The 1521 ports scanned but not shown below are in state closed)
Port       State       Service
21/tcp     open        ftp
22/tcp     open        ssh
23/tcp     open        telnet
25/tcp     open        smtp
37/tcp     open        time
80/tcp     open        http
110/tcp    open        pop-3
```

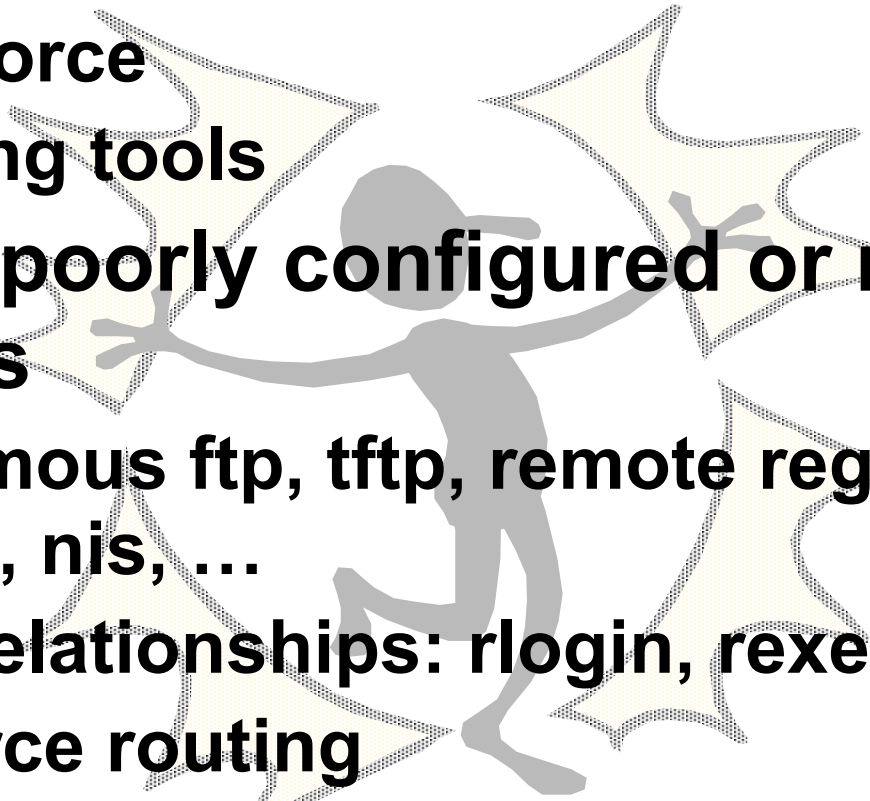
Why Do You Care?



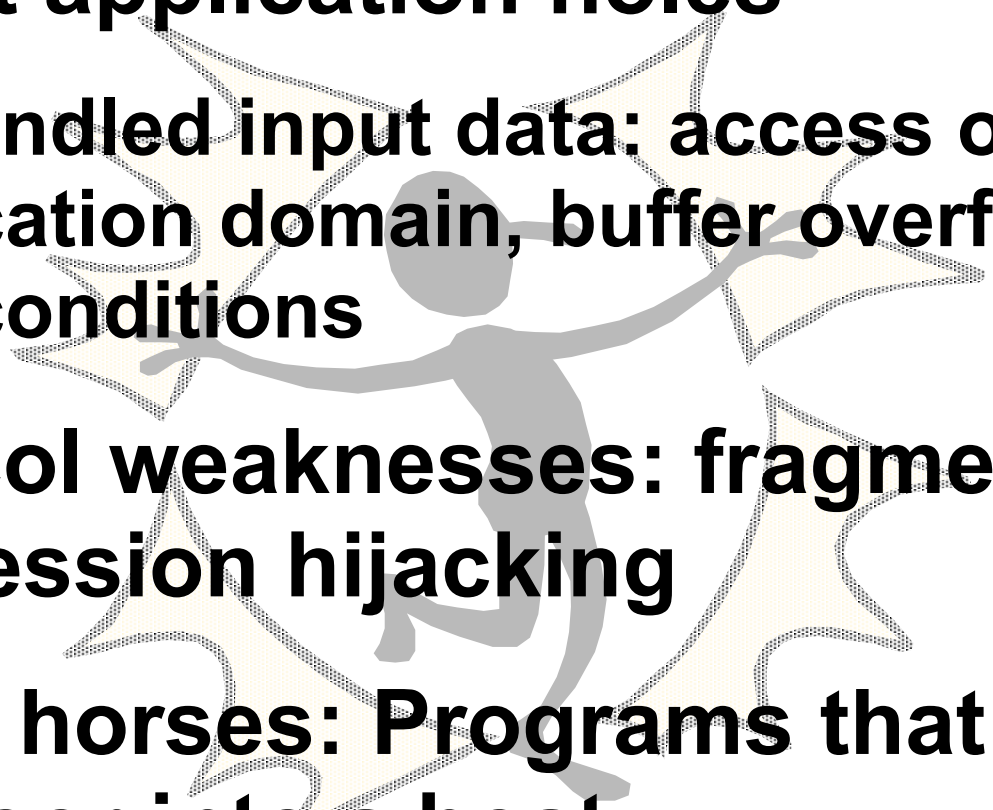
- **The more information you have, the easier it will be to launch a successful attack:**
  - **Map the network**
  - **Profile the devices on the network**
  - **Exploit discovered vulnerabilities**
  - **Achieve objective**

Access Methods

- Exploiting passwords
  - Brute force
  - Cracking tools
- Exploit poorly configured or managed services
  - anonymous ftp, tftp, remote registry access, nis, …
  - Trust relationships: rlogin, rexec, …
  - IP source routing
  - File sharing: NFS, Windows File Sharing



Access Methods cont'd



- **Exploit application holes**

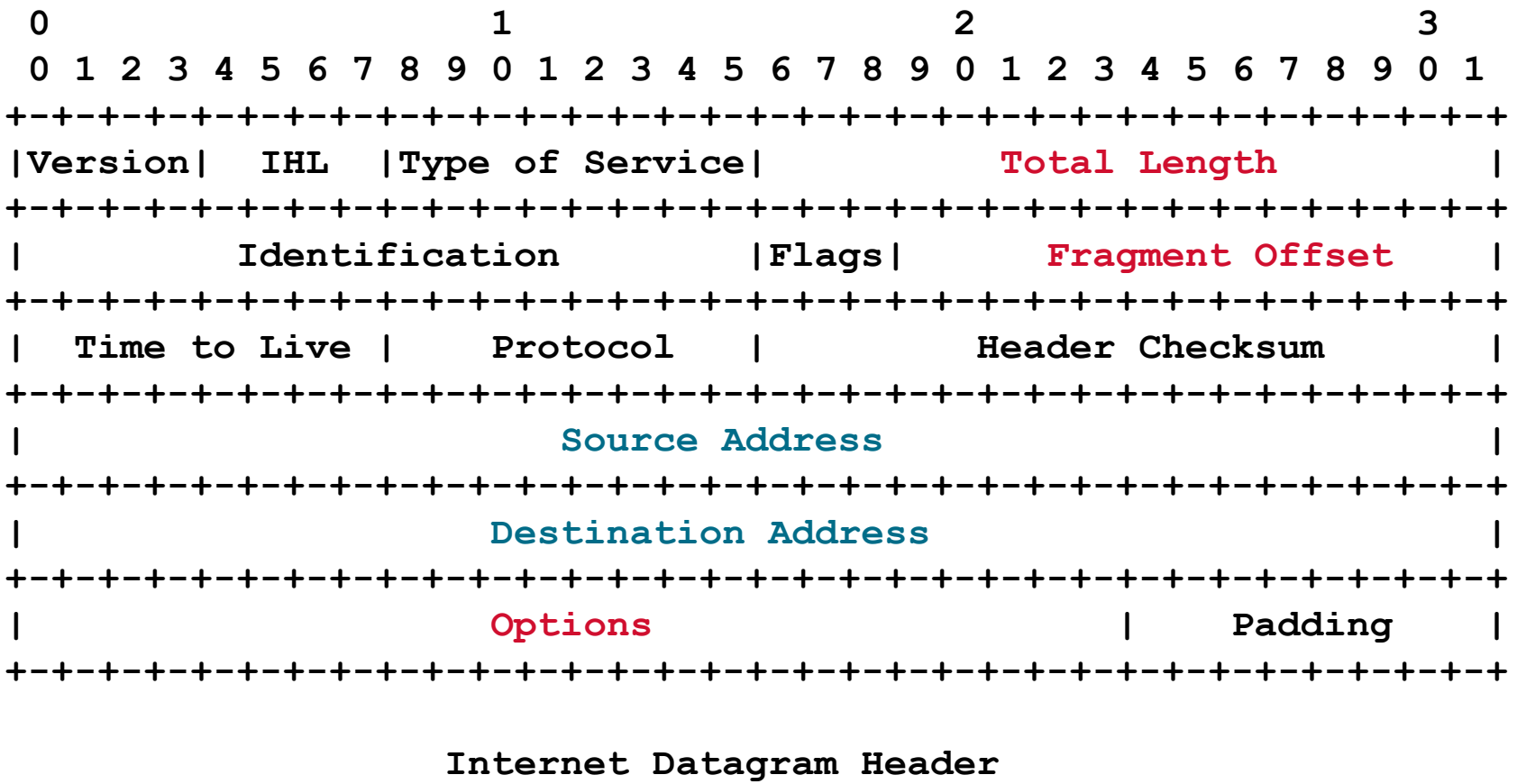
  Mishandled input data: access outside application domain, buffer overflows, race conditions

- **Protocol weaknesses: fragmentation, TCP session hijacking**
- **Trojan horses: Programs that plant a backdoor into a host**

IP Packet

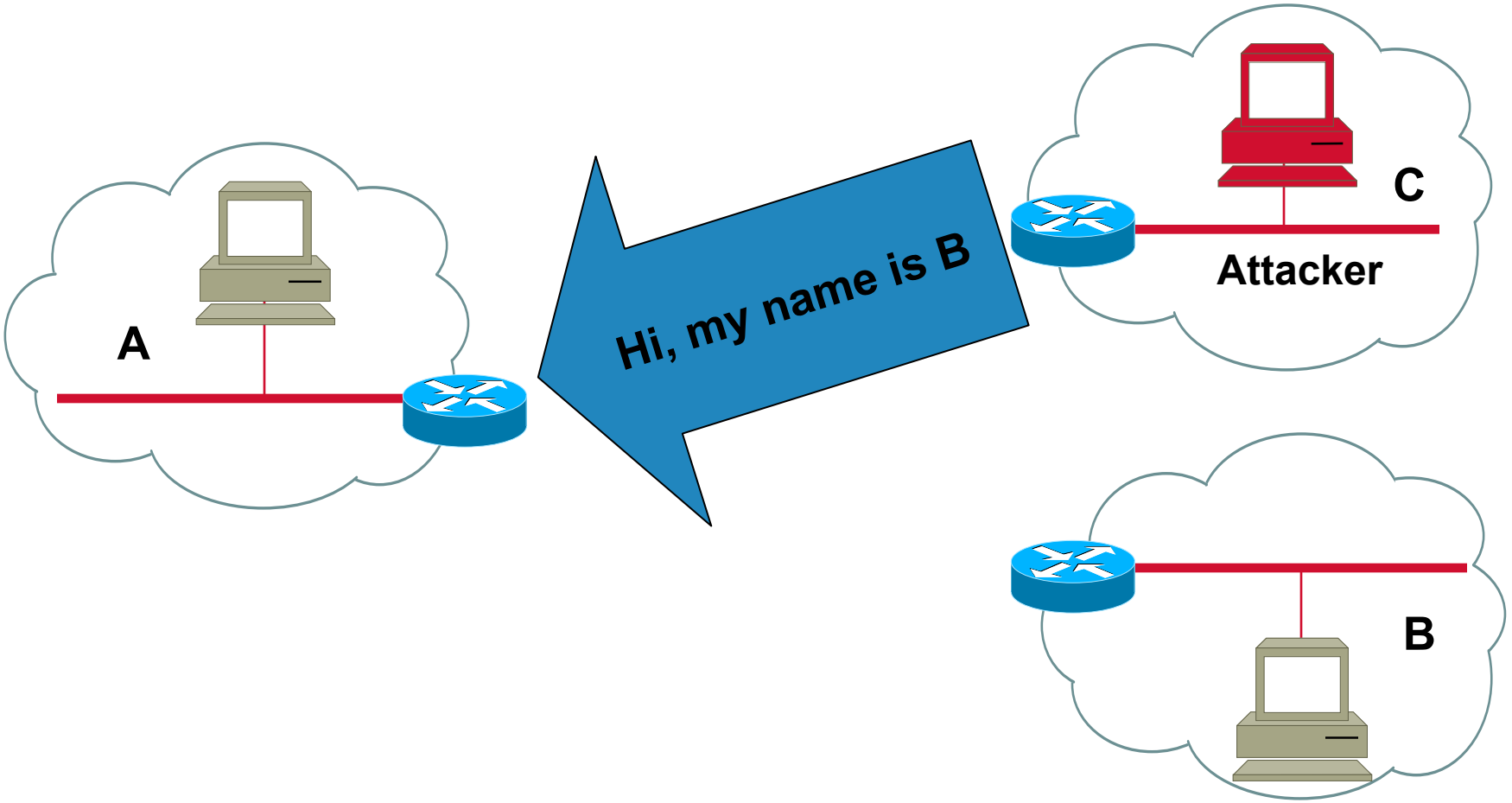
- **Internet Protocol**
  - **IP = connectionless network layer**
  - **SAP = 32 bits IP address**
  - **RFC 791, Sep 1981**

IP: Packet Format

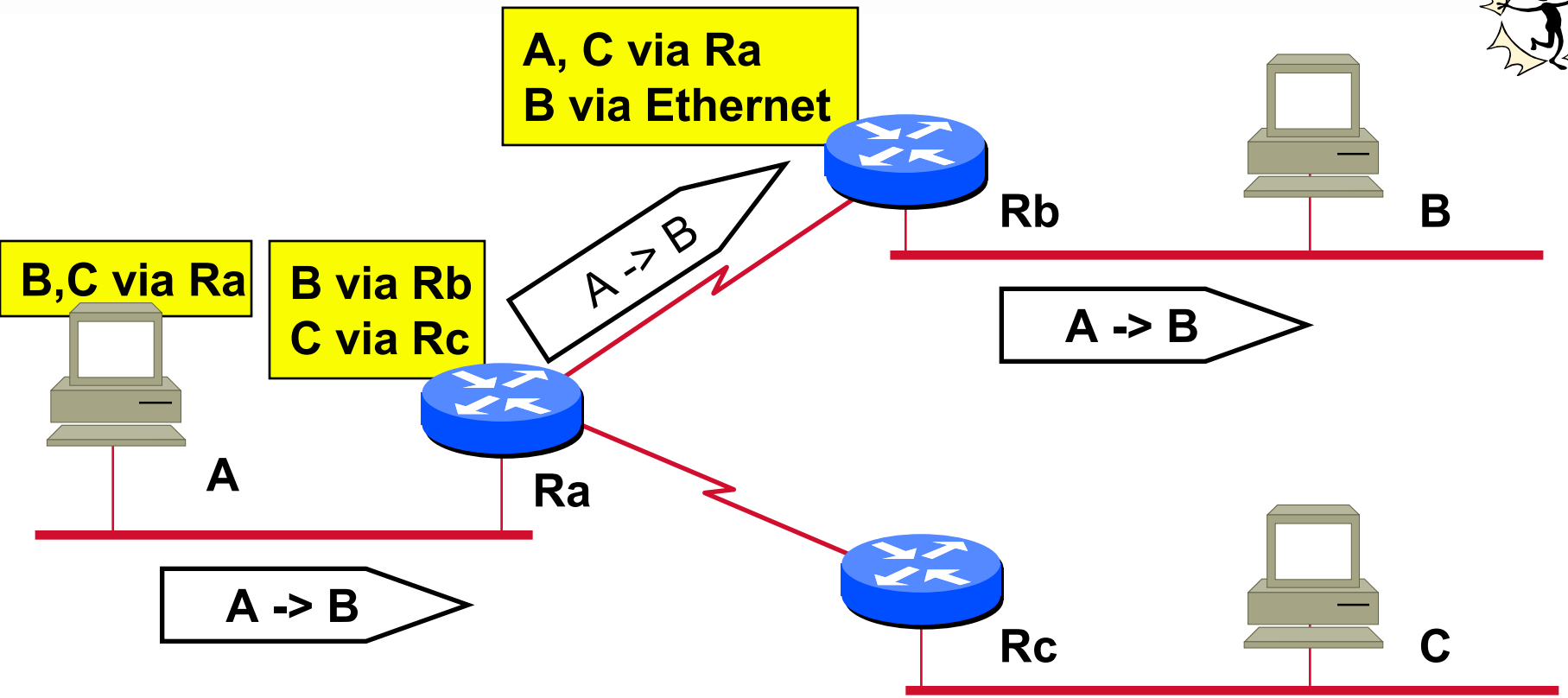


Internet Datagram Header

IP Spoofing

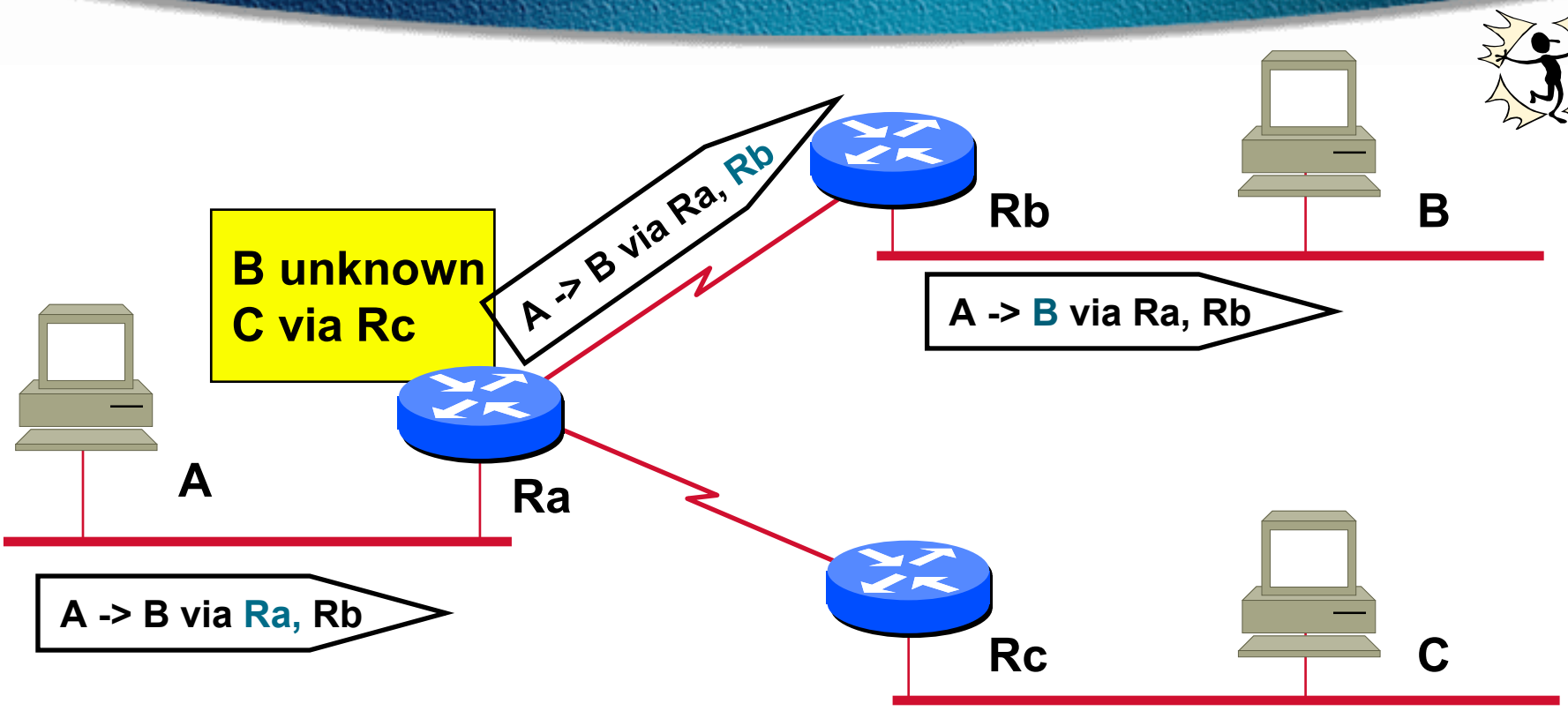


IP: Normal Routing



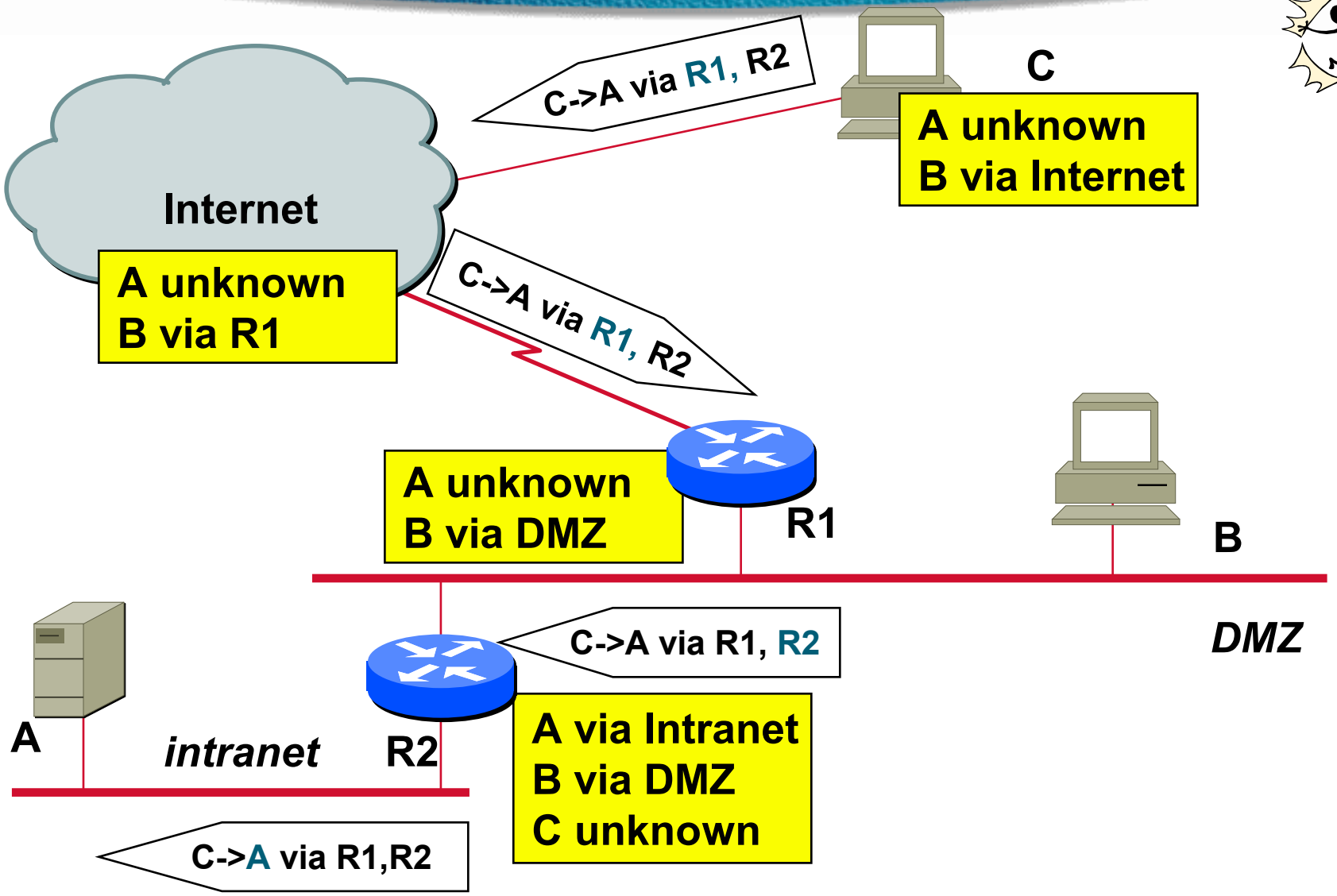
Routing based on routing tables

IP: Source Routing

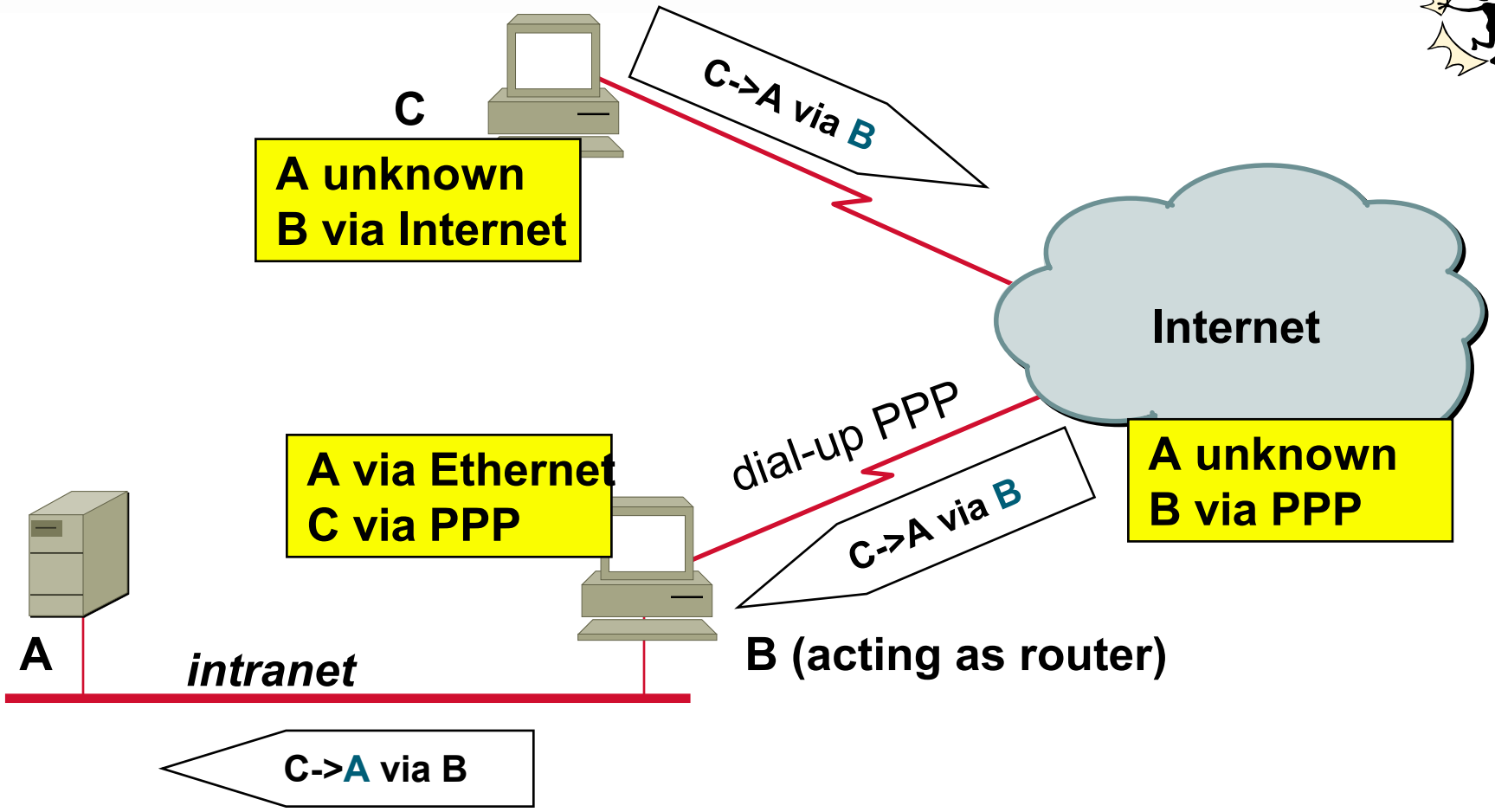


Routing based on IP datagram option

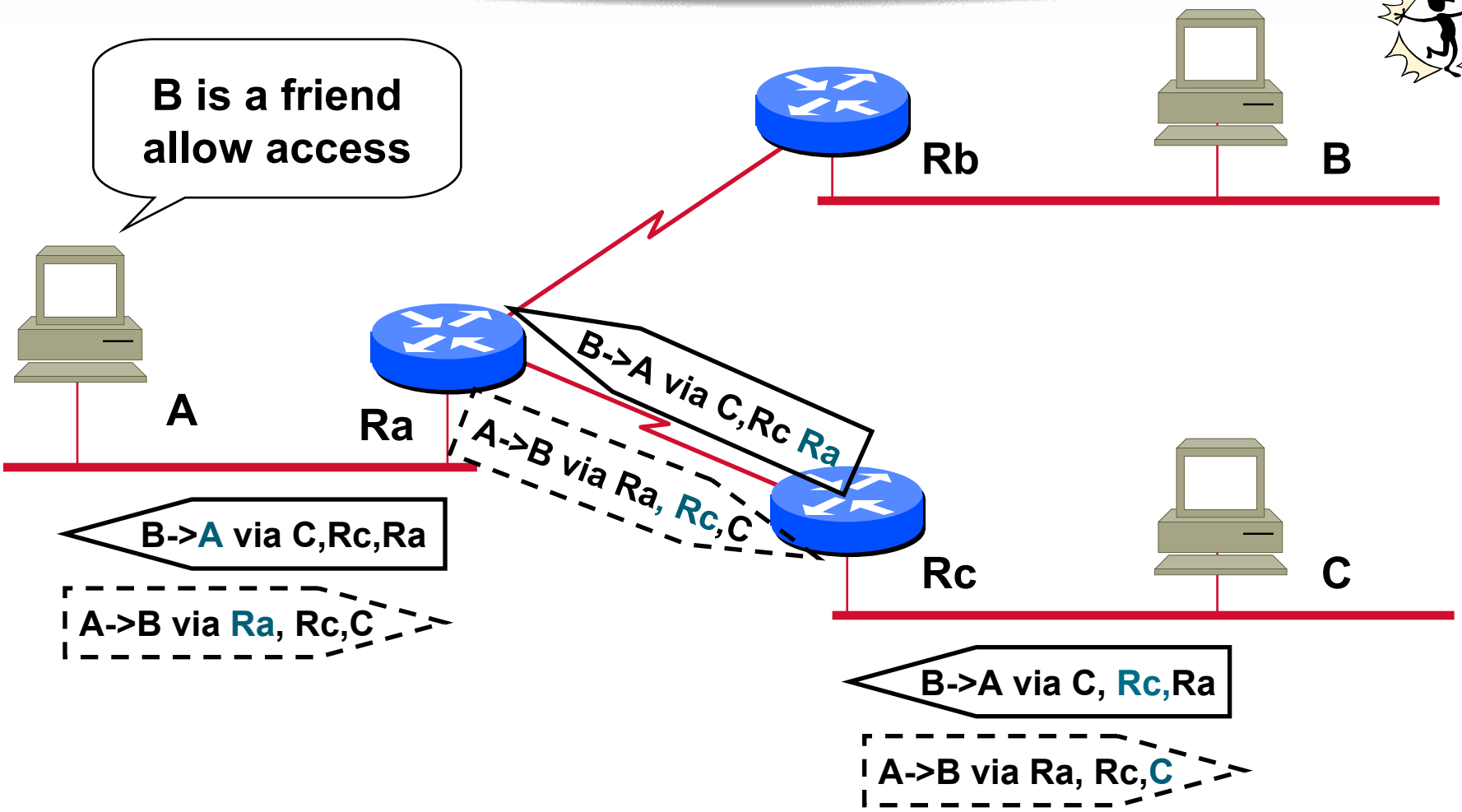
IP Unwanted Routing



IP Unwanted Routing (Cont.)



IP Spoofing Using Source Routing



Back traffic uses the same source route

Transport Control Protocol

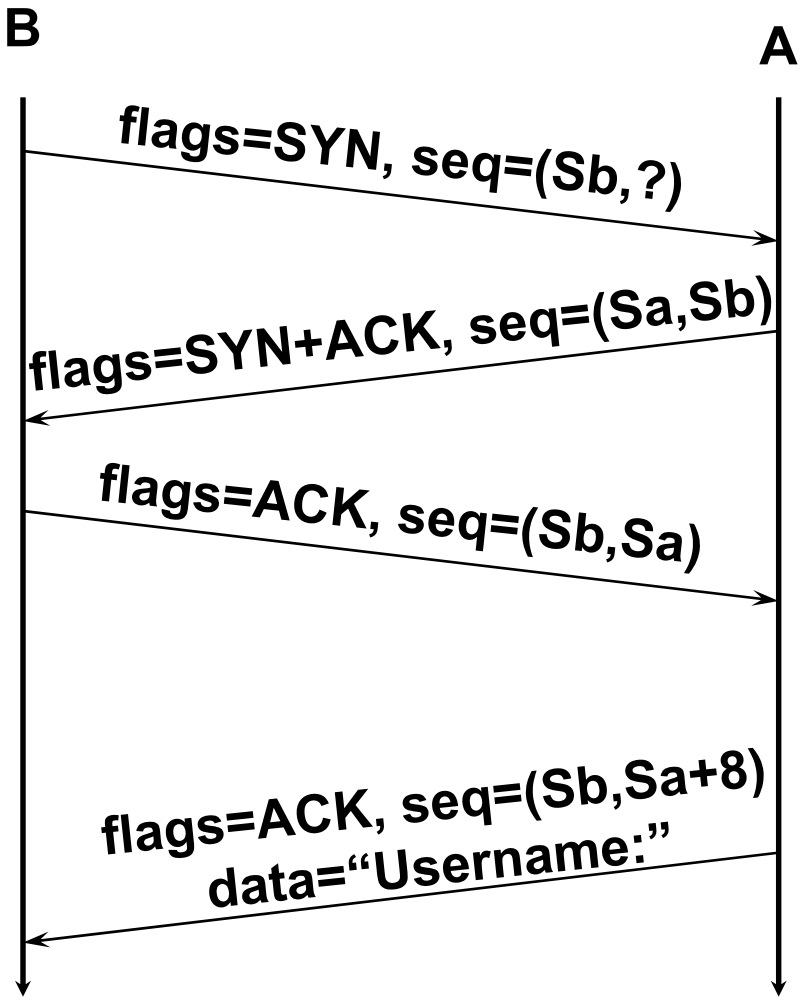
- TCP = connection oriented transport layer
- RFC 793, Sep 1981
- SAP= 16 bits TCP ports

TCP Packet Format

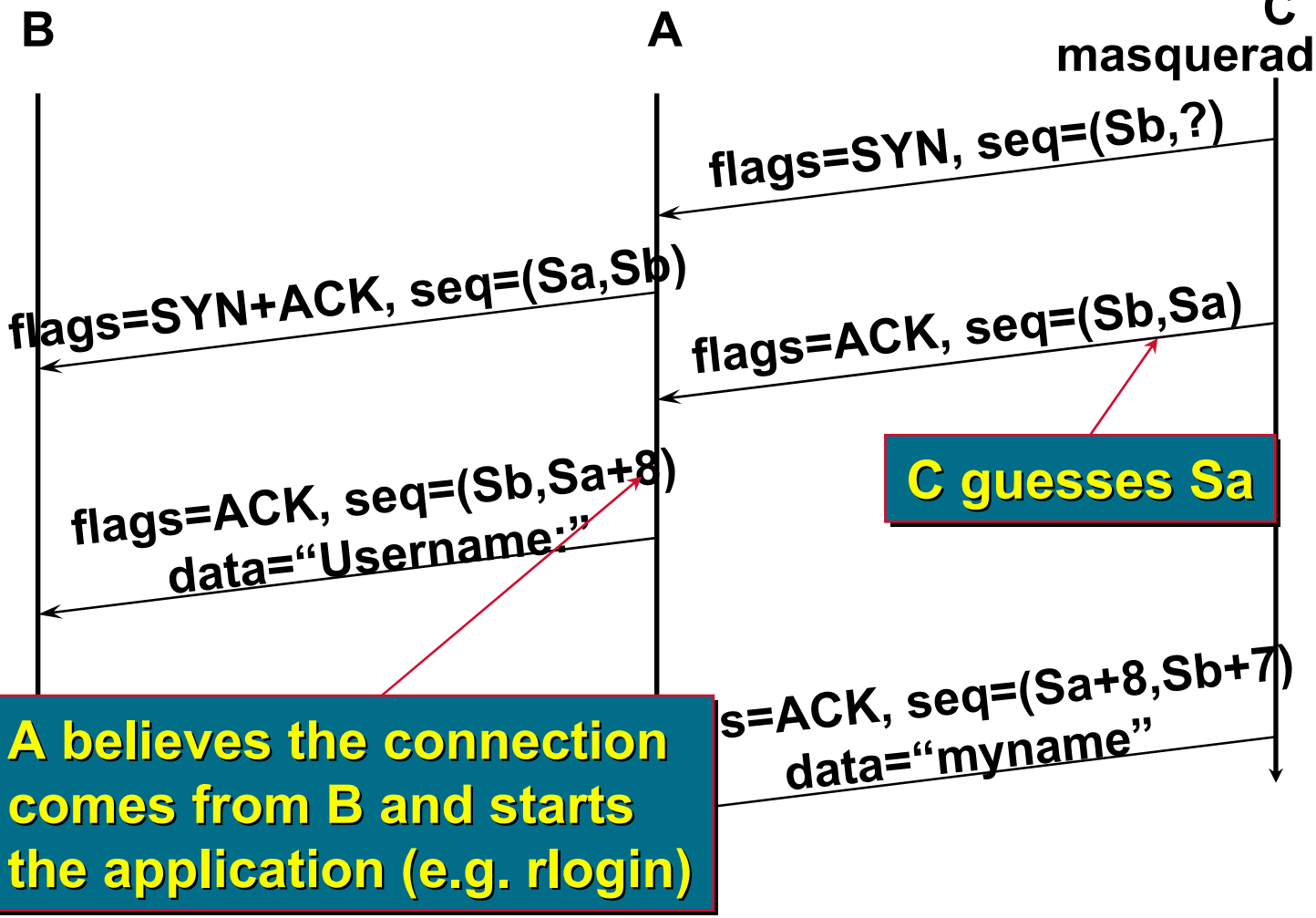
```
 0                   1                   2
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          Source Port          |       Destination Port        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                        Sequence Number                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Acknowledgment Number                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Data |           |U|A|P|R|S|F|                               |
| Offset| Reserved  |R|C|S|S|Y|I|            Window             |
|       |           |G|K|H|T|N|N|                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           Checksum            |         Urgent Pointer        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Options                    |    Padding    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                             data                              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

TCP Header Format

TCP connection establishment



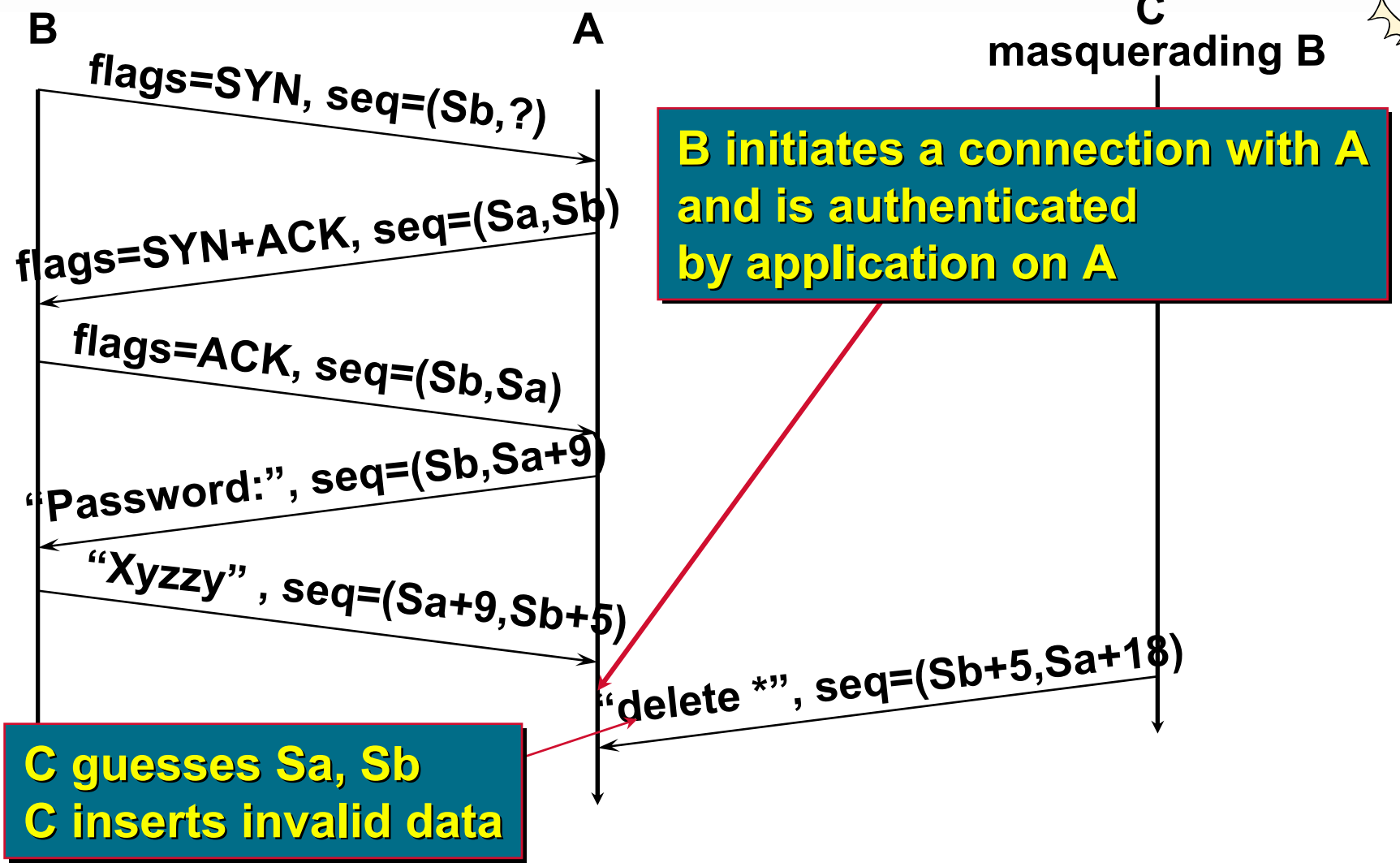
TCP blind spoofing



TCP blind spoofing (Cont.)

- C masquerades as B
- A believes the connection is coming from trusted B
- C does not see the back traffic
- For this to work, the real B must not be up, and C must be able to guess A's sequence number

TCP session hijacking



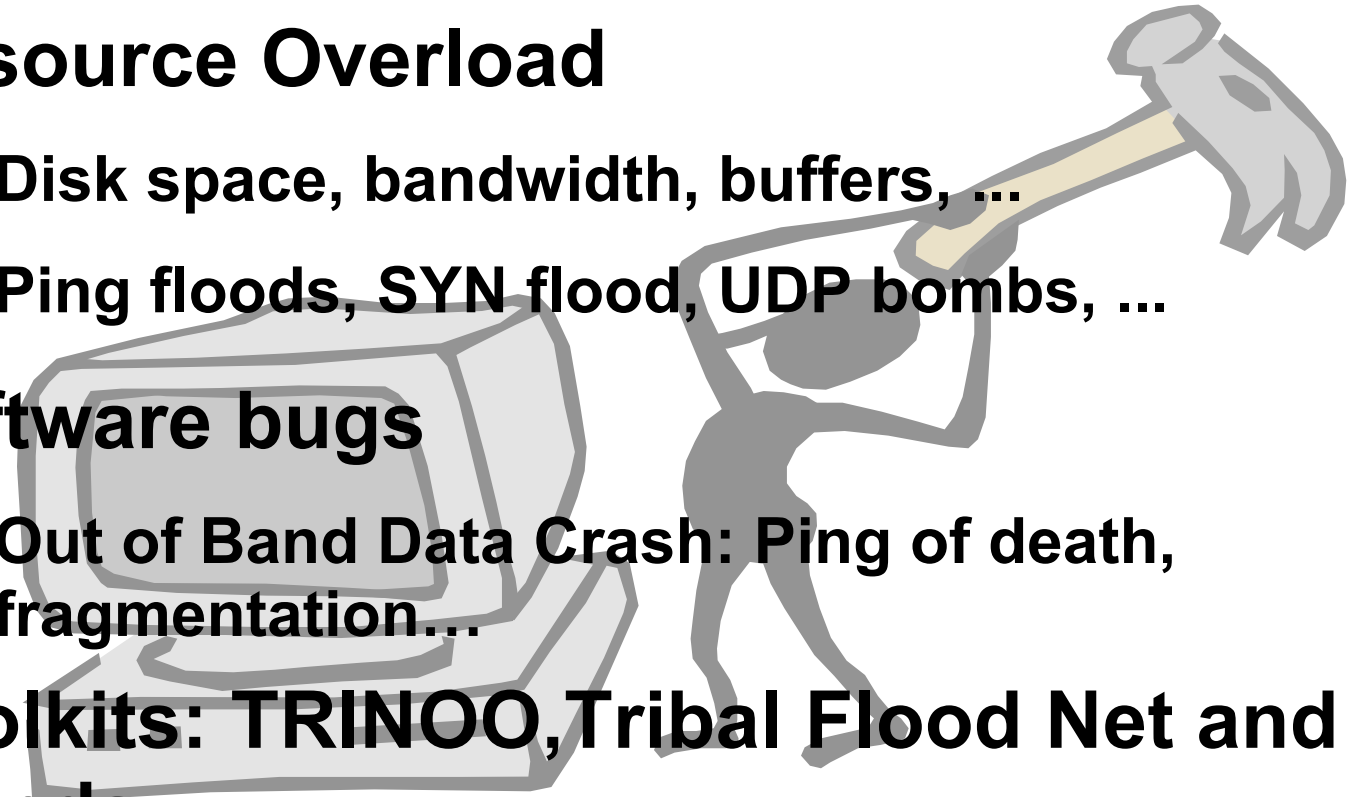
It Never Ends

Latest FTP Vulnerability

“Because of user input going directly into a format string for a *printf function, it is possible to overwrite important data, such as a return address, on the stack. When this is accomplished, the function can jump into shell code pointed to by the overwritten eip and execute arbitrary commands as root. While exploited in a manner similar to a buffer overflow, it is actually an input validation problem. Anonymous ftp is exploitable making it even more serious as attacks can come anonymously from anywhere on the internet.”

Source: SecurityFocus.Com, 2000

Denial of Service Methods



- **Resource Overload**
  - Disk space, bandwidth, buffers, ...
  - Ping floods, SYN flood, UDP bombs, ...
- **Software bugs**
  - Out of Band Data Crash: Ping of death, fragmentation…
- **Toolkits: TRINOO,Tribal Flood Net and friends**
- **Distributed attacks for amplification**

IP Normal Fragmentation

- IP largest data is 65.535 == 2^16-1
- IP fragments a large datagram into smaller datagrams to fit the MTU
- fragments are identified by *fragment offset* field
- destination host *reassembles* the original datagram

IP Normal Fragmentation (Cont.)

Before fragmentation:

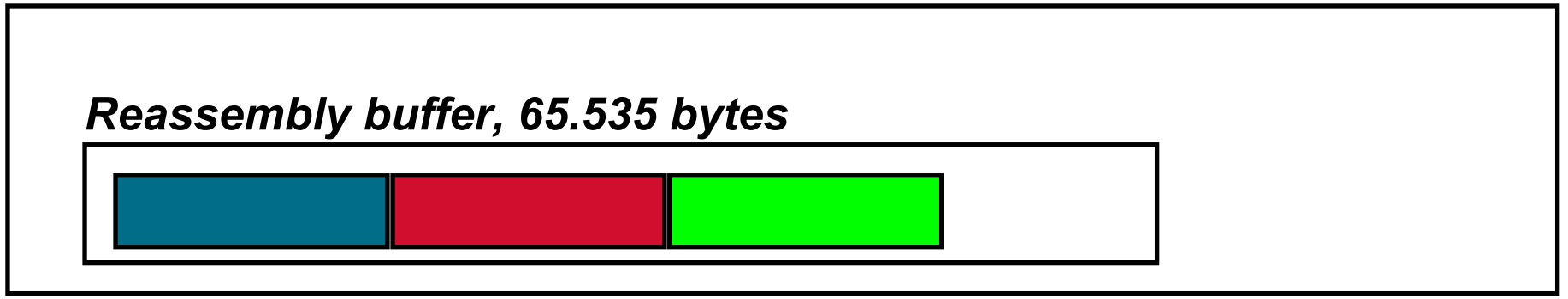
After fragmentation (MTU = 500):

TL=500, FO=0	data length 480
TL=500, FO=480	data length 480
TL=360, FO=960	data length 340

IP Normal Reassembly

Received from the network:

TL=500, FO=0	data length 480
TL=360, FO=960	data length 340
TL=500, FO=480	data length 480



Kernel memory at destination host

IP Reassembly Attack

- send invalid IP datagram
- *fragment offset* + fragment size > 65.535
- usually containing ICMP echo request (ping)
- not limited to *ping of death* !

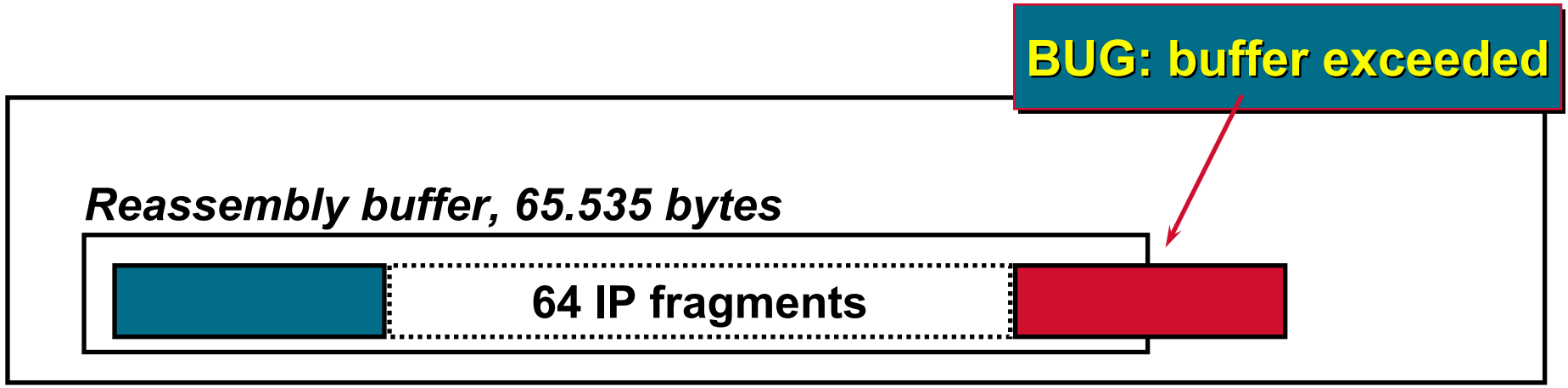
IP Reassembly Attack (Cont.)

Received from the network:

TL=1020, FO=0	data length 1000

… 64 IP fragments with data length 1000 ...

TL=1020, FO=65000	data length 1000



Kernel memory at destination host

SYN attack

B

A

C
masquerading as B

flags=SYN, seq=(Sb,?)

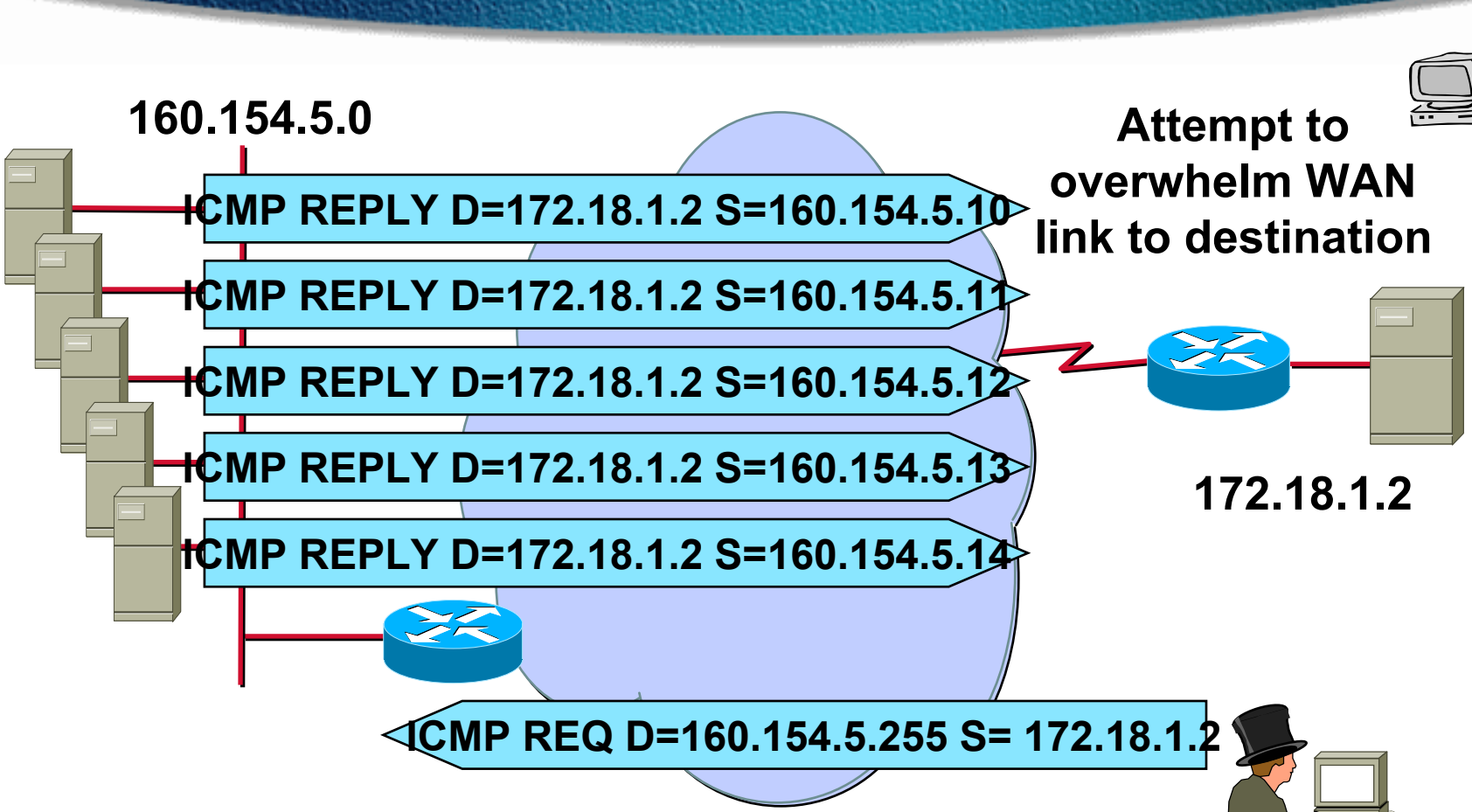
flags=SYN+ACK, seq=(Sa,Sb)

A allocates kernel resource
for handling the starting connection

No answer from B…
120 sec timeout
Free the resource

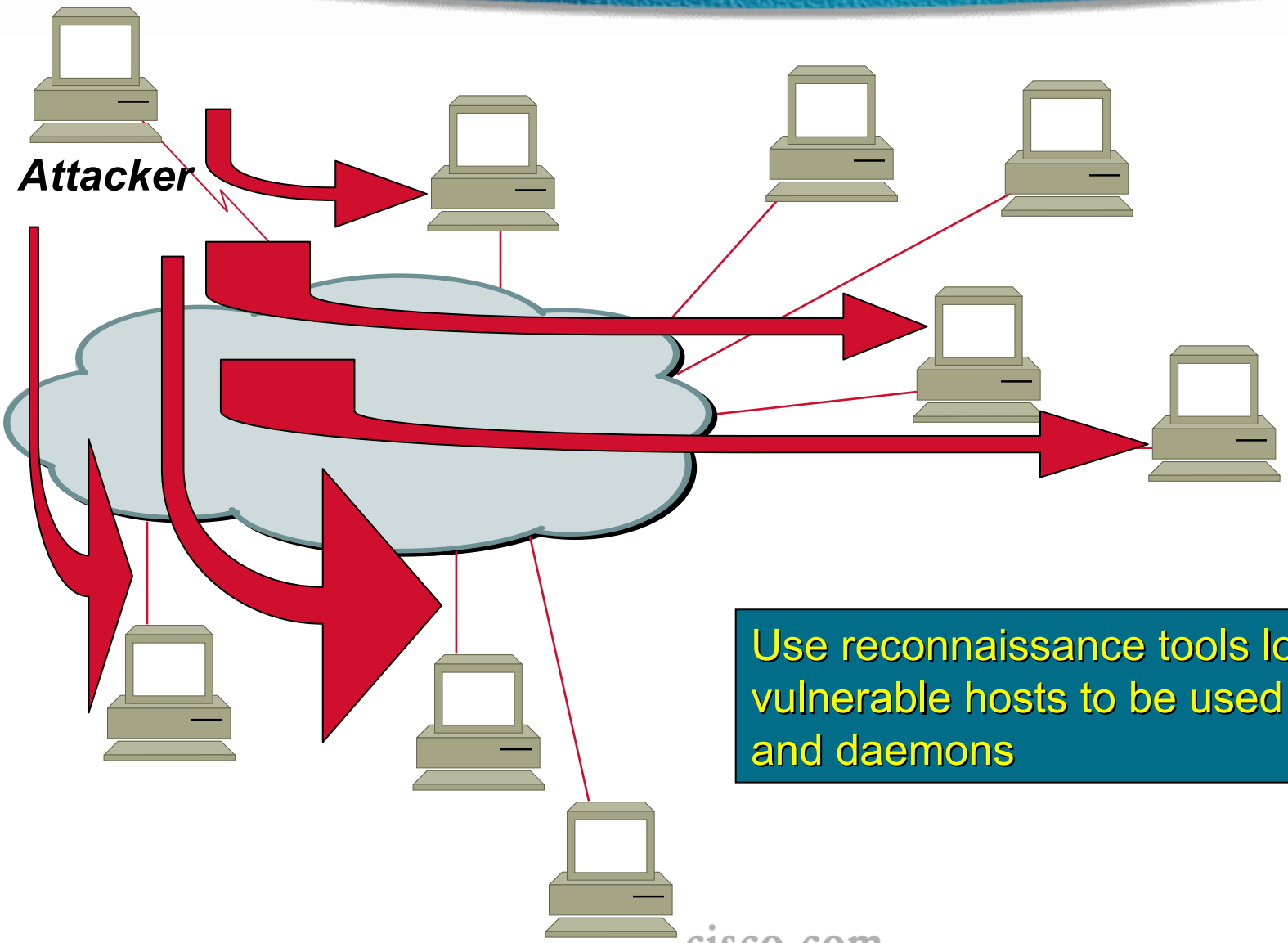
Denial of Services
kernel resources exhausted

SMURF Attack



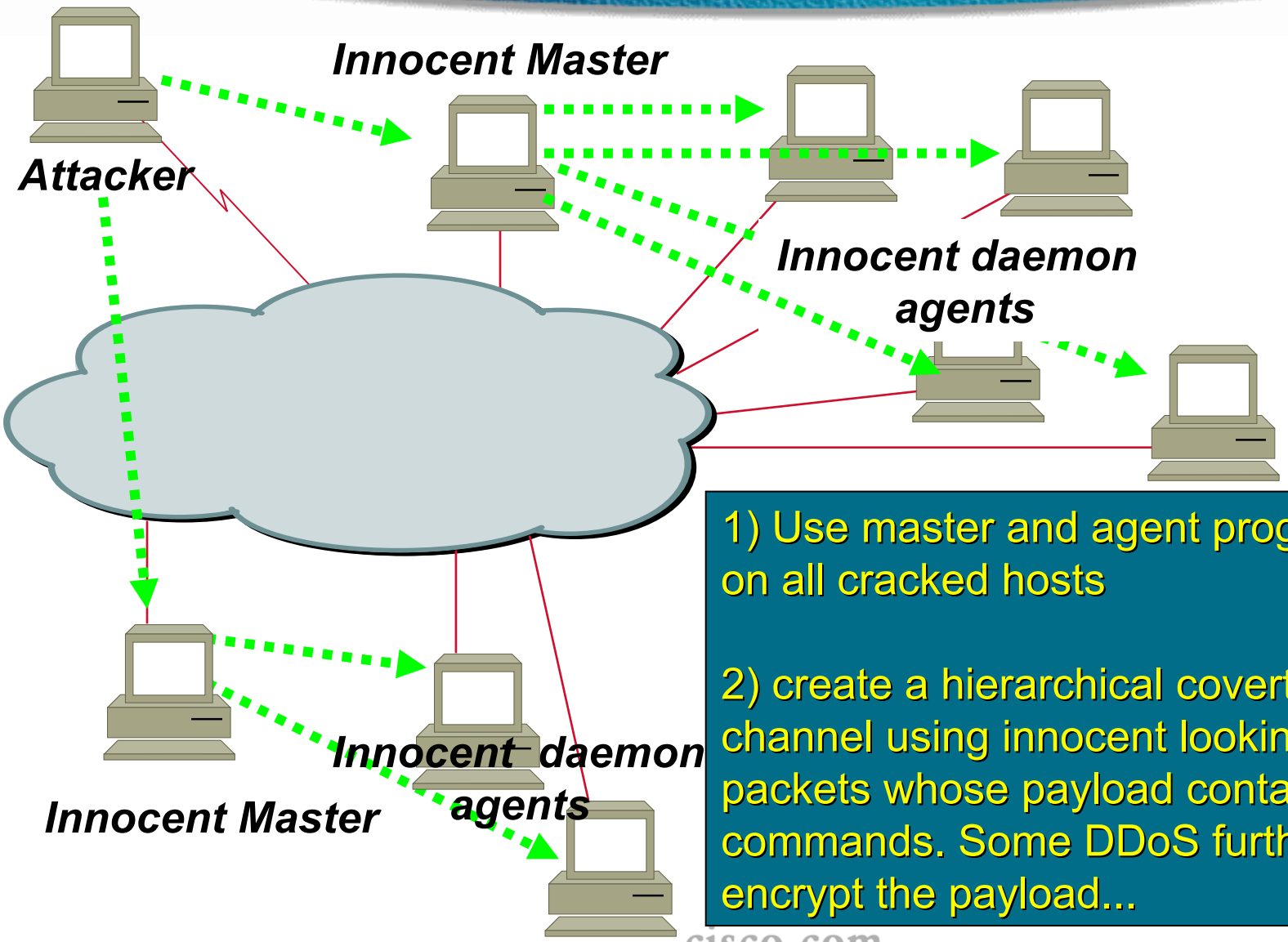
- Directed Broadcast PING

DDoS Step 1: Find Vulnerable Hosts



Use reconnaissance tools locate vulnerable hosts to be used as masters and daemons

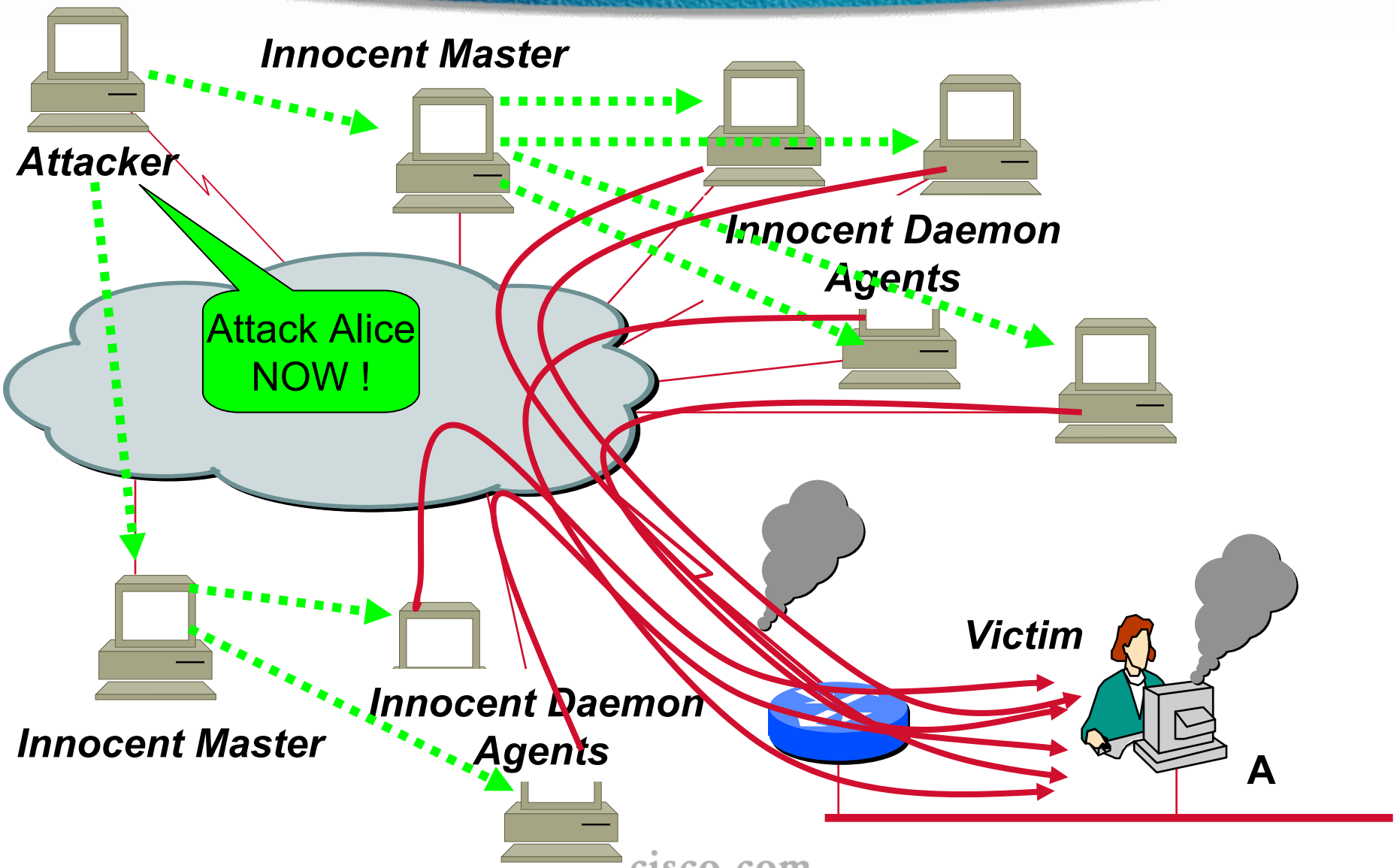
DDoS Step 2: Install Software on Masters and Agents



1) Use master and agent programs on all cracked hosts

2) create a hierarchical covert control channel using innocent looking ICMP packets whose payload contains DDoS commands. Some DDoS further encrypt the payload...

DDoS Step 3: Launch the attack



Today

- New agent software has been created for Windows hosts…
- No longer a problem for just Unix systems
- Target may be a router!

Why Should You Care

- Protect your own operational environment
- Protect your customer's data
- Protect the services you offer to your customers
- In other words….to protect your business !!

What Should You Do?

- **Develop security policy**
  - **for your organization**
  - **for your customers**
- **Develop your security plan**
- **Secure your network**
- **Develop an incident response procedure**

Security Policy

Why a Site Security Policy?

- To protect assets
- To help prevent security incidents
- To provide guidance when incidents occur

Security Policy Topics

- Access
- Authentication
- Accountability
- Privacy
- Violations handling
- Supporting information
- others...

Site Security Policy Resources

- http://secinf.net/info/policy/AusCERT.html written by Rob McMillan
- RFC 2196 - Site Security Handbook
- RFC 1281 - Guidelines for the Secure Operation of the Internet
- RFC 2504 - Users' Security Handbook

Policies Affecting Your Customers

- Service expectations
- Access policies for customers
  - what type of access is allowed and under what circumstances
- Authentication policy for customers
  - what type of authentication must they use when connecting to your site
- Protection of your customers' traffic
- Incident handling policies
  - inbound incidents
  - outbound incidents

Policies Affecting Your Customers -2

- **Notification of vulnerabilities and incidents**
  - who is coordinating response to the incident
  - the vulnerability
  - how service was affected
  - what is being done to respond to the incident
  - whether customer data may have been compromised
  - what is being done to eliminate the vulnerability
  - the expected schedule for response, assuming it can be predicted
- **Sanctions for policy violations**
- **See IETF draft-ietf-grip-isp-expectations-03.txt**

Security Plan

Your Security Plan

- **Describe the assets you want to protect**
  - **data**
  - **hardware and software**
  - **services**
- **Describe how you will protect the assets**
  - **access restrictions and authentication**
  - **redundancy**
  - **encryption**

Your Security Plan -2

- **Describe disaster recovery plans**
  - **physical disasters**
  - **equipment failures**
  - **intrusions**
  - **employee or customer mistakes**
- **Regularly test your security plan**
- **Update plan based on results of testing**

Securing Your Network

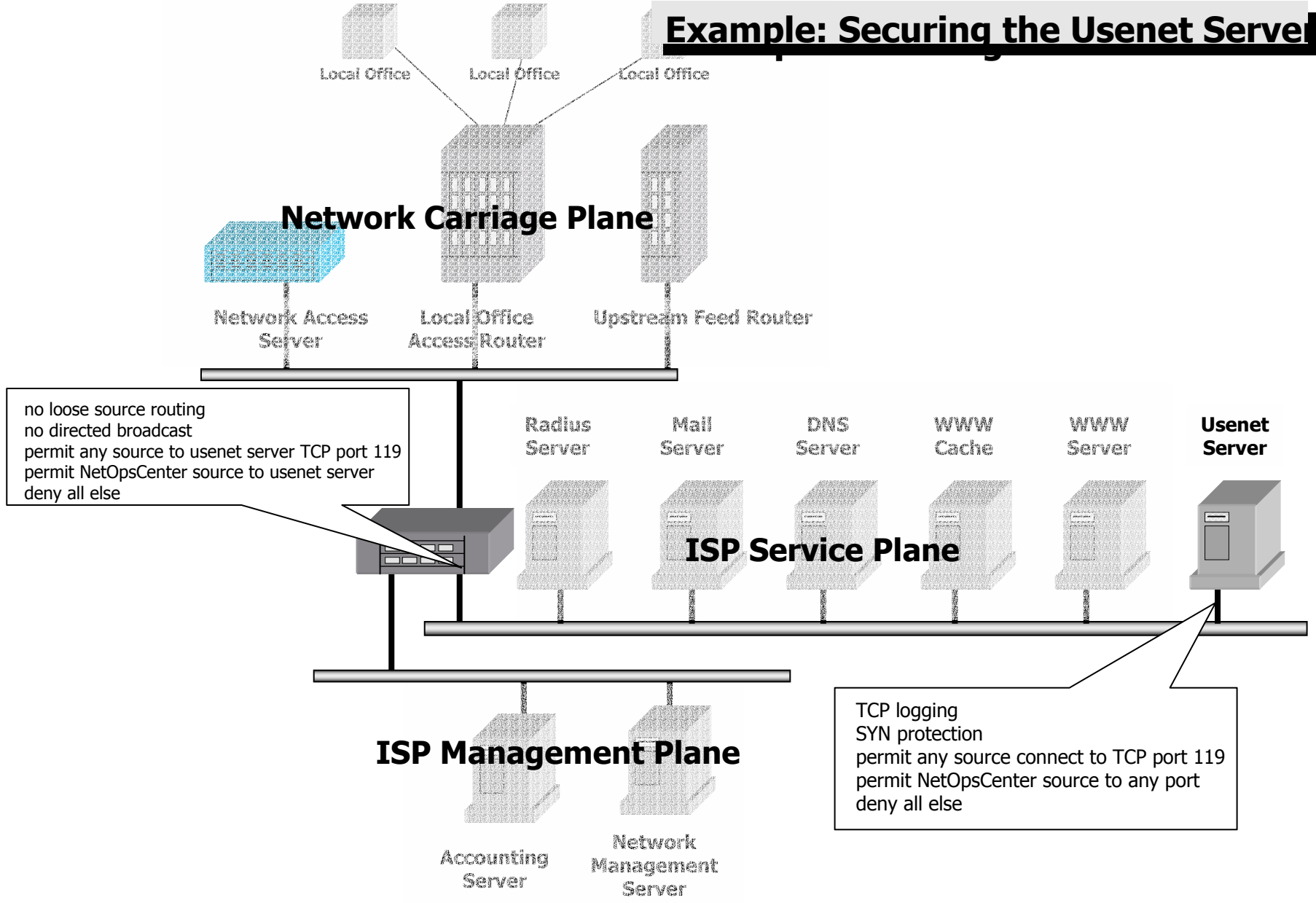
Securing Your Network

- Securing your operational network
- Securing services offered to your customers

Securing Your Operational Network

- Separate your operational networks from your service networks
- Restrict services to your organization's network/hosts
- Protect services that are allowed to internal network

Example: Securing the Usenet Server



Source: *ISP Survival Guide*, 1999

Secure Initial System Setup - 1

- Build off-line
- Set or disable passwords for all existing accounts
- Review account groups and privileges
- Review CERT Advisories and VIBs
- Install all applicable security patches
- Minimize system and network services
- Remove unnecessary software

  compilers, shells, servers, daemons, etc.
- Fix file permissions

Secure Initial System Setup - 2

- Configure logging and quota mechanisms
- Install and configure system monitoring tools
- Replace weak access mechanisms with more secure ones
  - UNIX - e.g., replace telnet, r-commands with SSH
- Configure file system integrity tools
  - UNIX - e.g., Tripwire
- Make a Backup!
- Deploy on network only when prepared for exposure

Domain Name Servers

- **Intruders target domain name servers**
  - **exploit services that trust host names**
  - **masquerade as another host**
- **Consider using internal and external servers**
  - **external servers provide information regarding hosts serving the Internet: email, FTP, WWW...**
  - **internal servers provide information about internal hosts to internal hosts**
- **Use latest version of bind**

Protecting System Password Information

- **Unix**
  - **password aging**
  - **16-character passwords**
  - **freely available shadow password suite**
- **NT - configure to protect SAM database**
  - **Registry settings and protections**
  - **Use NTFS file system instead of FAT, set permissions**

Manage Networks Securely

- Restrict access to routers and servers
- Require strong authentication when accessing any critical system
- Use SSH to tunnel through firewalls to access network

Configuring Public Servers -1

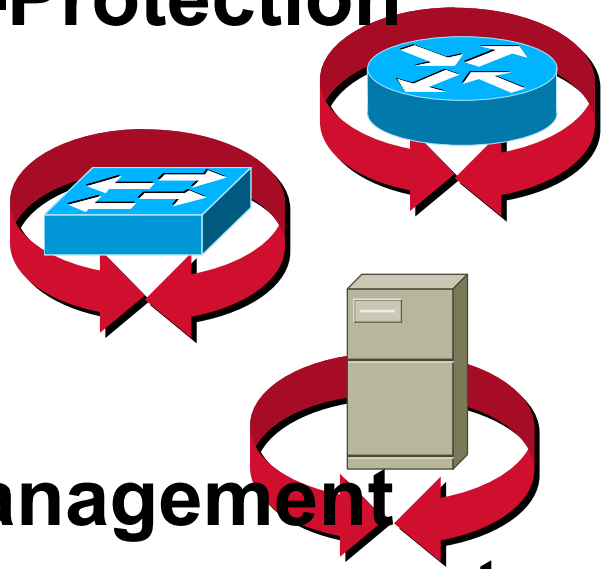
- Turn on logging of all outside access (using TCP-Wrappers or other tools)
- Use Tripwire or other cryptographic checksums to verify the integrity of information and system configuration
- Locate the public servers on a separate network segment
- Keep a copy of the information on another system for fast backup
- Consider CD-ROM for information and system files that rarely change

TFTP

- Disable tftpd if it isn’t absolutely necessary
- Otherwise, restrict tftpd access

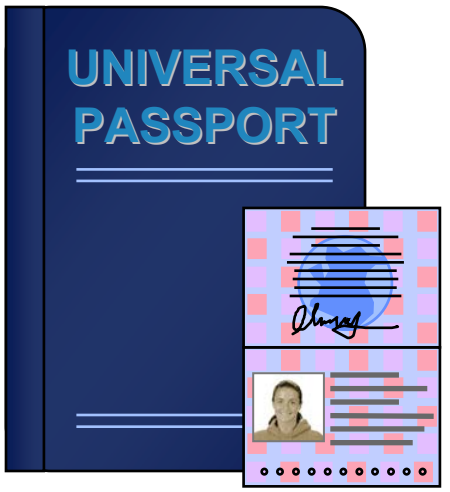
Securing the Network

- Router/Switch/Server Self-Protection
  - Use good access controls
  - Limit SNMP access
  - Disable unused services
  - Implement privilege levels
- Resource Protection
- In-band vs Out-of-band Management
- Good network design and management
  - Redundancy, Logging
- Audit

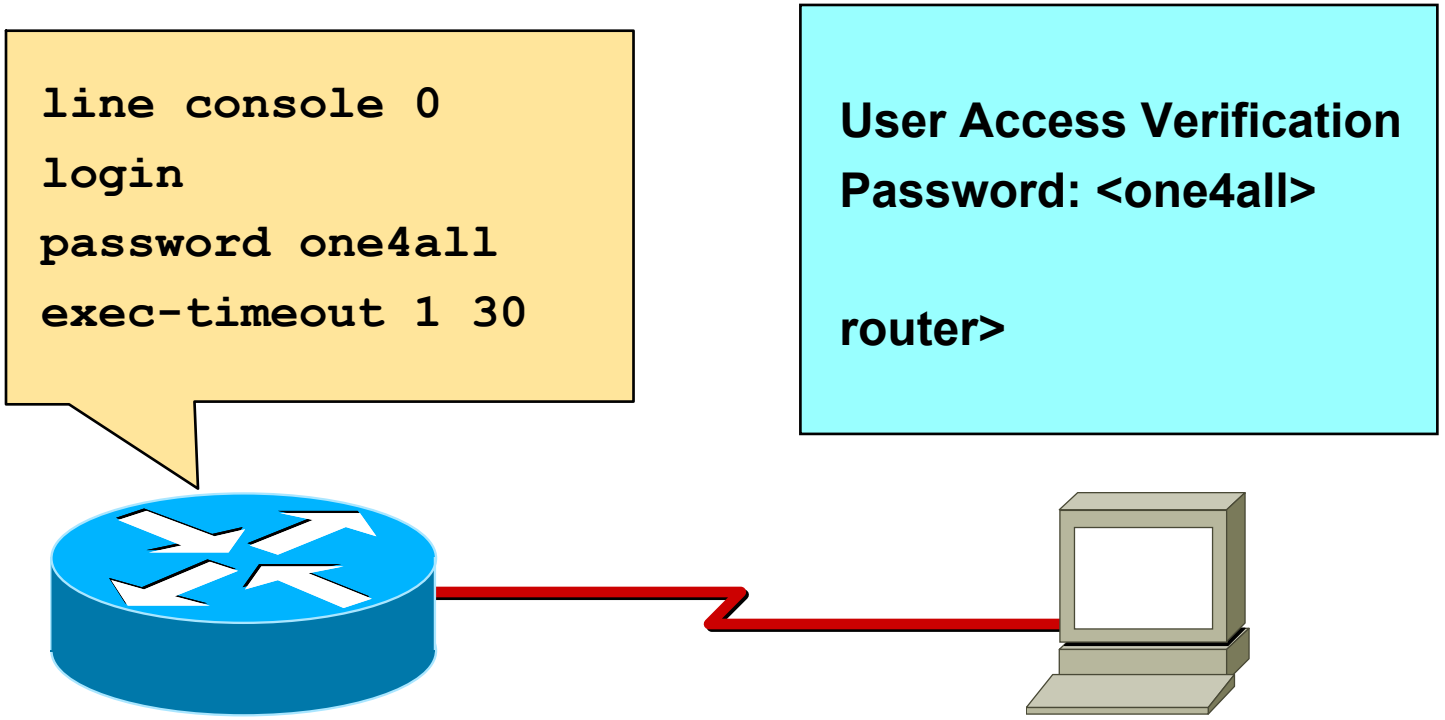


Authentication Mechanisms

- Console, Telnet
- Local passwords
  - Username based
- External Authentication
  - TACACS+, RADIUS, Kerberos, SSH
- One-time passwords



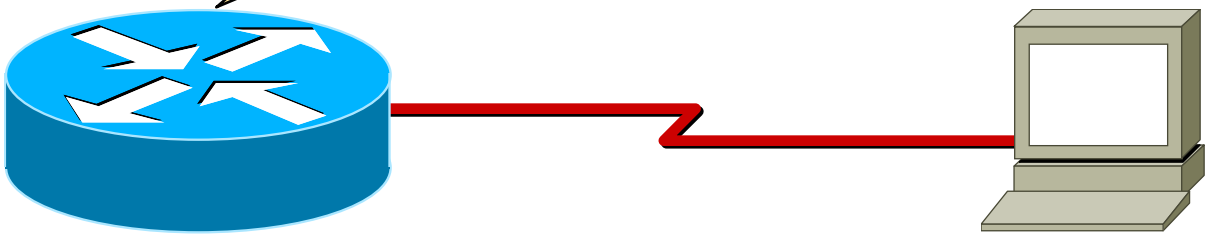
Local Passwords



- Password in every device
- Viewable in plain text in configuration

Service Password-Encryption

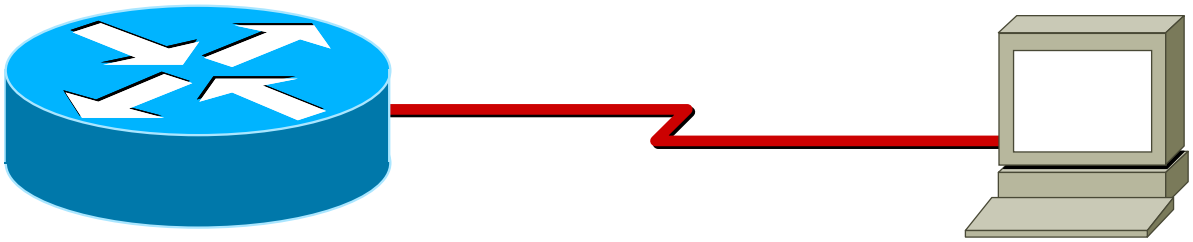
```
service password-encryption
!
hostname Router
!
enable password 7 15181E020F
```



- Encrypts password in configuration
- Easily reversible

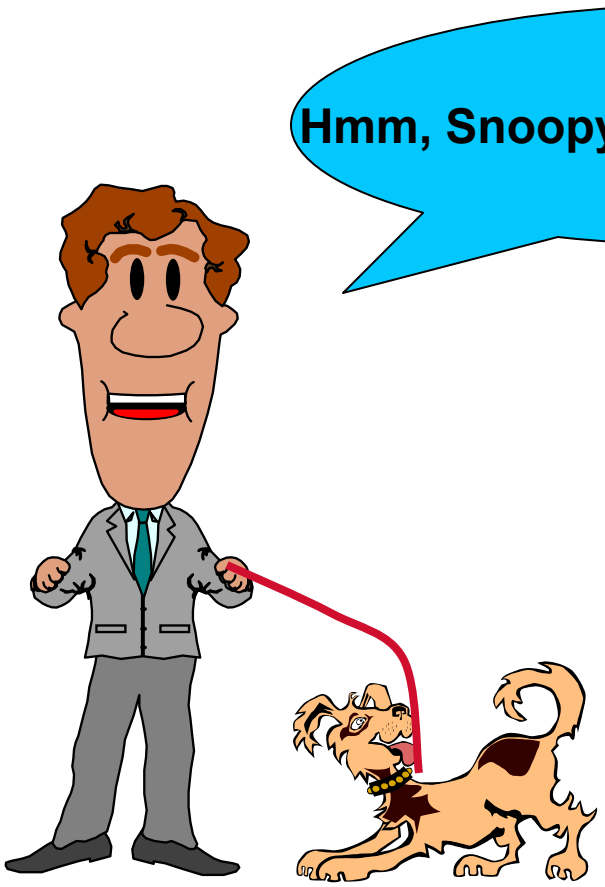
Enable Secret

```
!
hostname Router
!
enable secret 5 $1$hM3l$.s/DgJ4TeKdDkTVCJpIBw1
```



- Uses MD5 one-way hash to encrypt **enable** password in configuration

Use Good Passwords

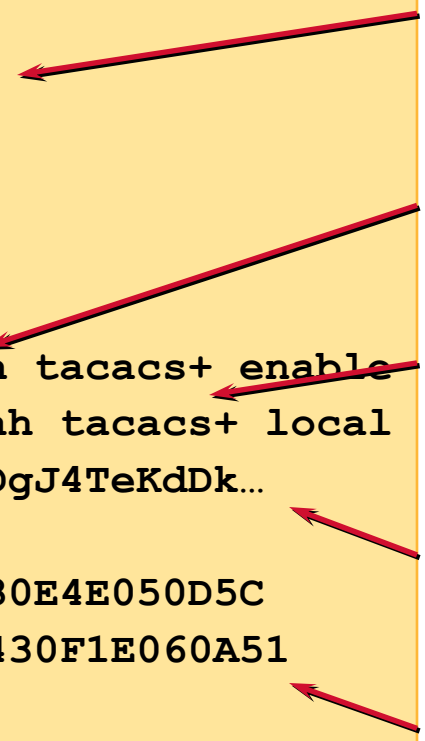


- Don’t use easily guessed passwords
- Centralize password management

  RADIUS, TACACS+

Cisco IOS TACACS+ Login Authentication

```
version 12.0
!
service password-encryption
!
hostname Router
!
aaa new-model
aaa authentication login ruth tacacs+ enable
aaa authentication login sarah tacacs+ local
enable secret 5  $1$hM3l$.s/DgJ4TeKdDk…
!
username john password  7  030E4E050D5C
username bill password  7  0430F1E060A51
!
```



Encrypts Passwords with Encryption (7)

Define List "Ruth" to Use TACACS+ then the Enable Password

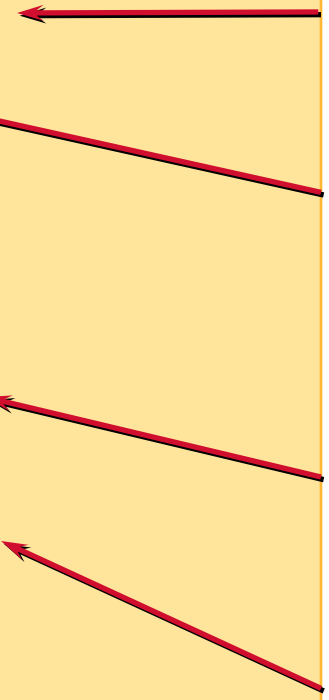
Define List "Sarah" to Use TACACS+ then the Local User and Password

"Enable Secret" Overrides the (7) Encryption

Define Local Users

Cisco IOS TACACS+ Login Authentication

```
tacacs-server host 10.1.1.2
tacacs-server key <key>
!
line con 0
 login authentication ruth
line aux 0
 login authentication ruth
line vty 0 4
 login authentication sarah
!
end
```



Defines the IP Address of the TACACS+ Server

Defines the "Encryption" Key for Communicating with the TACACS+ Server

Uses the Authentication Mechanisms Listed in "Ruth"—TACACS+ then Enable Password

Uses the Authentication Mechanisms Listed in "Sarah"—TACACS+ then a Local User/Password

PIX TACACS+ Login Authentication

```
PIX Version 4.3(1)
enable password BjeuCKspwqCc94Ss encrypted
passwd nU3DFZzS7jF1jYc5 encrypted
tacacs-server host 10.1.1.2 <key>
aaa authentication any console tacacs+
no snmp-server location
no snmp-server contact
snmp-server community notpublic
no snmp-server enable traps
telnet 10.1.1.2 255.255.255.255
…
Cryptochecksum:a21af67f58849f078a515b177df4228
: end
[OK]
```

Enable Password

Telnet Password

Define TACACS+ Server and Encryption Key

Use TACACS+ for Telnet or Console (Enable) Access

Defines the Device that Can Telnet into the PIX

Catalyst TACACS+ Login Authentication

```
set enablepass
$1$CBqb$j53diREUitkHDGKfAqFpQ
set authentication login tacacs enable
set authentication enable tacacs enable
set tacacs key secretkey
set tacacs server 144.254.5.9
```

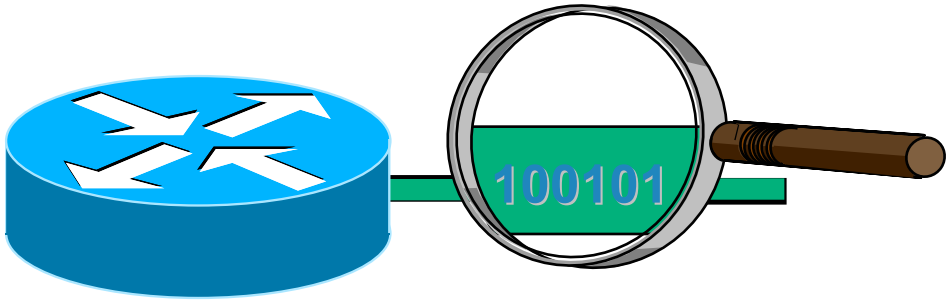
Enable Password

Use TACACS+ for Telnet or Console (Enable) Access

Define TACACS+ Server and Encryption Key

PassWord of Caution

- **Even passwords that are encrypted in the configuration are not encrypted on the wire as an administrator logs into the router**

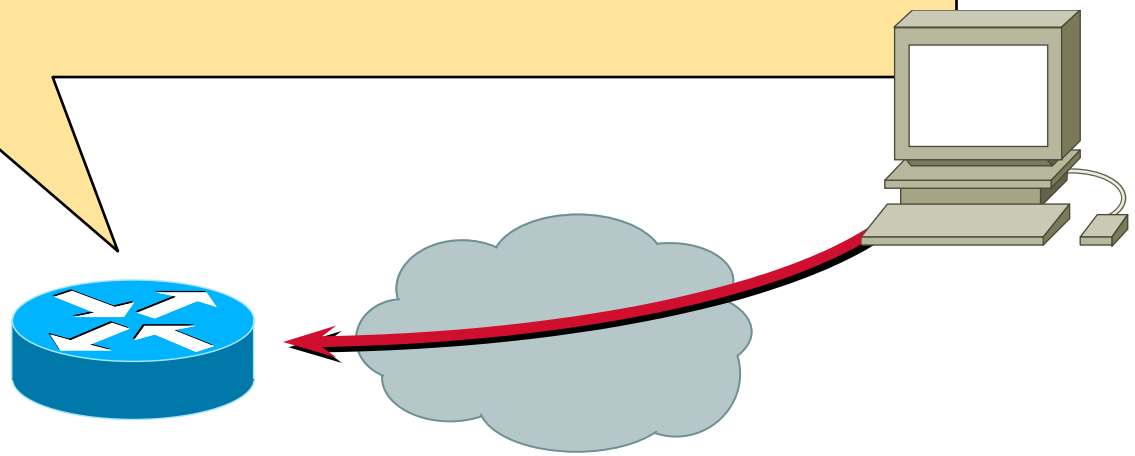


One-Time Passwords

- May be used with TACACS+ or RADIUS
- The same “password” will never be reused by an authorized administrator
- Key Cards—CryptoCard token server included with CiscoSecure
- Support for Security Dynamics and Secure Computing token servers in Cisco Secure

Restrict Telnet Access

```
access-list 12 permit 172.17.55.0 0.0.0.255
line vty 0 4
access-class 12 in
```



SSH

- SSH can be used for secured Command and Control sessions to routers.
- Full SSH has three components

  a terminal session with a secure transport

  the ability to handle “r-commands” similar to rsh

  the ability to “forward” other TCP-based protocols

SSH Authentication

- **There are two levels of Authentication required for an SSH session**
  - **Host (or ‘device’) Authentication**
  - **User Authentication**

Host Authentication

- Each IOS host has its' own unique RSA key with a user selectable key length up to 2048 bytes.
- The RSA authentication will transfer the session key.
- This authentication will establish the encrypted session.

Host Authentication

- IOS will store its' own RSA key and will accept all other keys.
- In the "full" implementation, keys of other hosts should be kept in permanent storage and a warning will be presented to the user if the hostname/key do not match.

User Authentication

- After the encrypted session is established, user authentication is still required.
- Since the SSH feature is tied to the vty's, user authentication is associated with some of the authentication mechanisms available to the vty's: RADIUS, TACACS+ and local.
- The username and password will pass between the workstation and the router inside of the encrypted session.

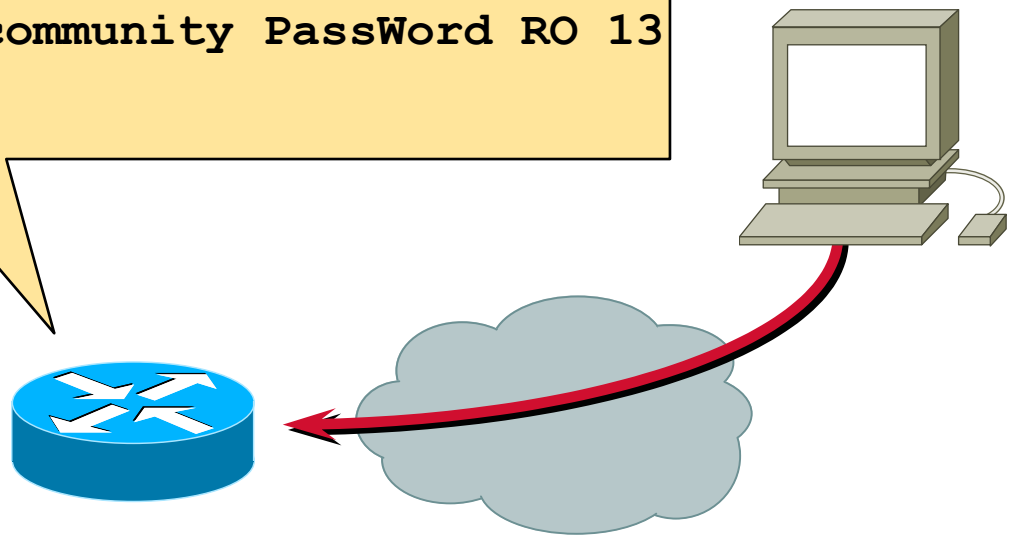
User Authentication

- The session will be terminated if authentication fails, or if the authentication mechanism fails (e.g.- a router cannot establish a session with a TACACS+ server, etc.).
- If authentication succeeds, a session is opened using the encryption algorithm selected.

SNMP Access Control

RO—Read Only
RW—Read + Write

```
access-list 13 permit 192.85.55.12
access-list 13 permit 192.85.55.19
snmp-server community PassWord RO 13
```



SNMP

- **Change your community strings! Do not use *public, private, secret!***
- **Use different community strings for the RO and RW communities.**
- **Use mixed alphanumeric characters in the community strings: SNMP community strings can be *cracked*, too!**

Transaction Records

- **How do you tell when someone is attempting to access your router?**

  ip accounting

  ip accounting access-violations

  logging 127.0.3.2

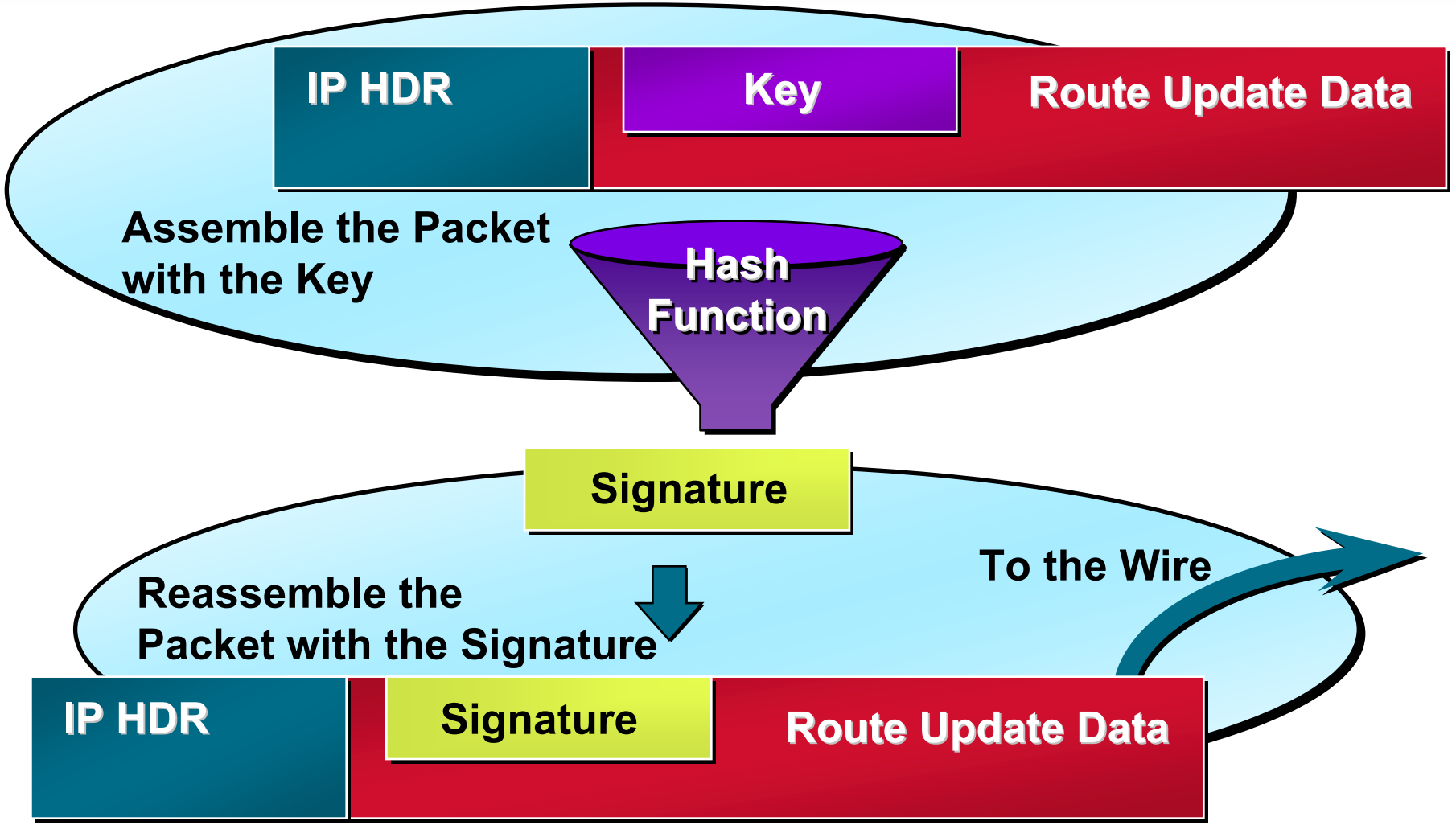
- **Consider some form of audit trails:**

  Using the *syslog* feature.

  SNMP Traps and alarms.

  Implementing TACACS+, Radius, Kerberos, or third party solutions like *One-Time Password* token cards.

Route Update Authentication and Integrity

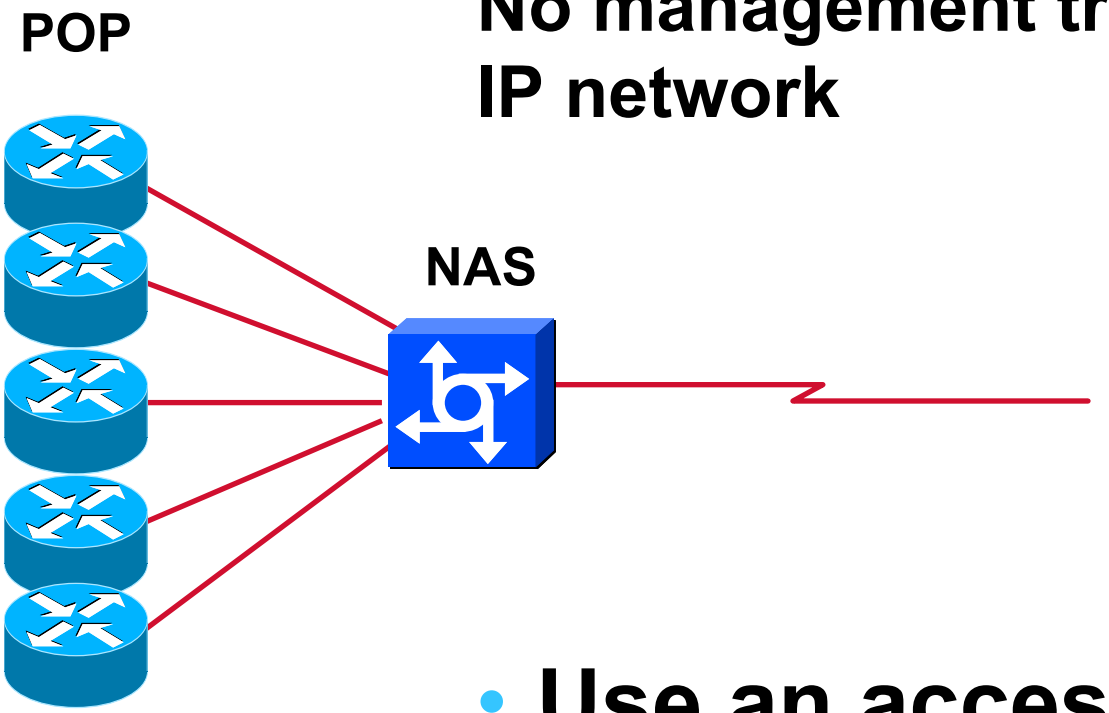


Route Filtering

```
router rip
 network 10.0.0.0
 distribute-list 1 in
!
access-list 1 deny   0.0.0.0
access-list 1 permit 10.0.0.0  0.255.255.255
```

```
Router# sho ip proto
Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 12 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is 1
  Redistributing: rip
```

Out-of-band Management



No management traffic in primary IP network

- Use an access server to connect console ports through reverse Telnet

In-band Management

- Use private addresses for backbone routers
- Ingress filter at the Edge: SNMP, ICMP, anti-spoofing, your IP@ as source or destination addresses
- Encryption and integrity

In-band vs Out-of-band

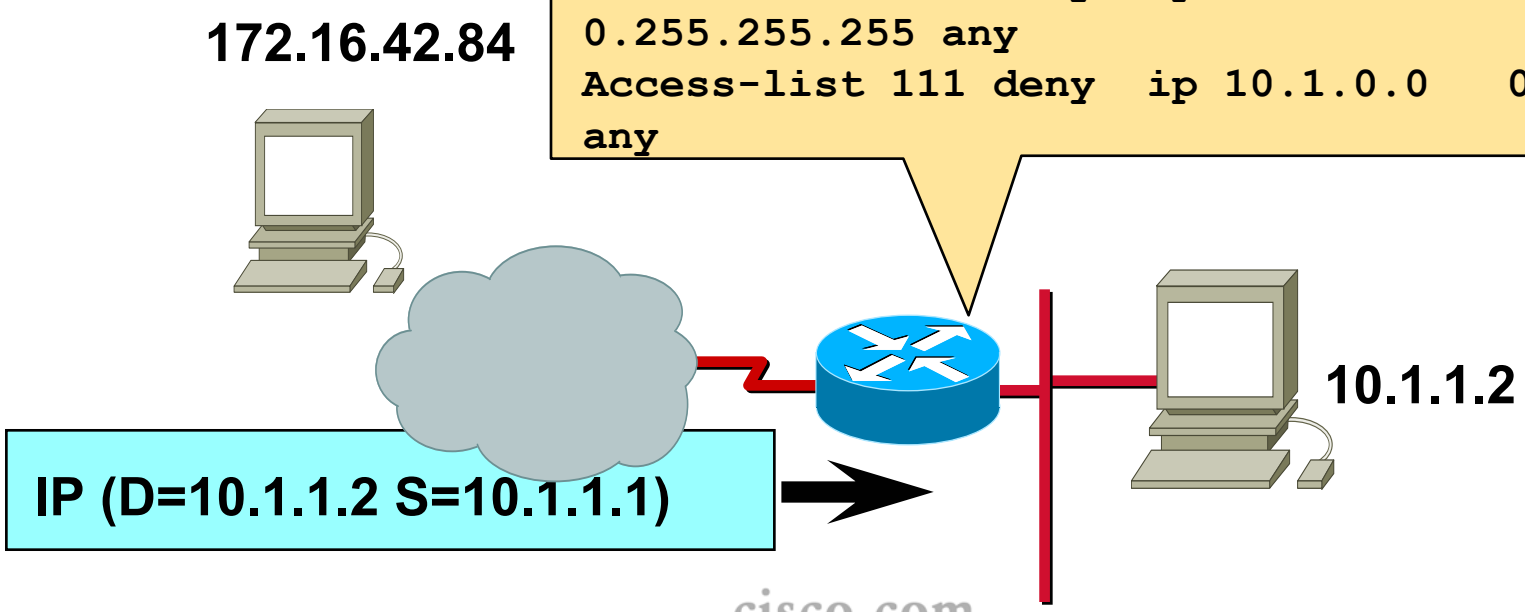
- Console or Aux ports do not allow SNMP
- IOS software upgrade may be easier with console port
- Outbound needs a dedicate connection: cost

Protect Resources

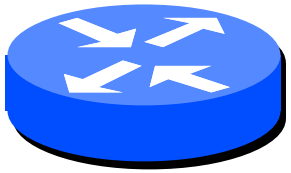
- Spoofing
- Source routes
- Resource consumption

Spoofing

```
interface Serial 1
ip address 172.26.139.2 255.255.255.252
ip access-group 111 in
no ip directed-broadcast
!
interface ethernet 0/0
ip address 10.1.1.100   255.255.0.0
no ip directed-broadcast
!
Access-list 111 deny  ip 127.0.0.0
0.255.255.255 any
Access-list 111 deny  ip 10.1.0.0   0.0.255.255
any
```

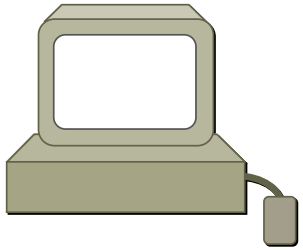


Preventing IP spoofing



Cisco routers, disable source routing (on by default)

```
no ip source route
```



Hosts, disable:

1) IP forwarding, usually easy

2) source routing, usually impossible *(Windows had to wait until Win NT4 SP5 May 99)*

3) applications check for IP options via `getsockopt(...)`

Ingress & Egress Route Filtering

Your customers should not be sending *any* IP packets out to the Internet with a source address other then the address you have allocated to them!

Including Private Addresses

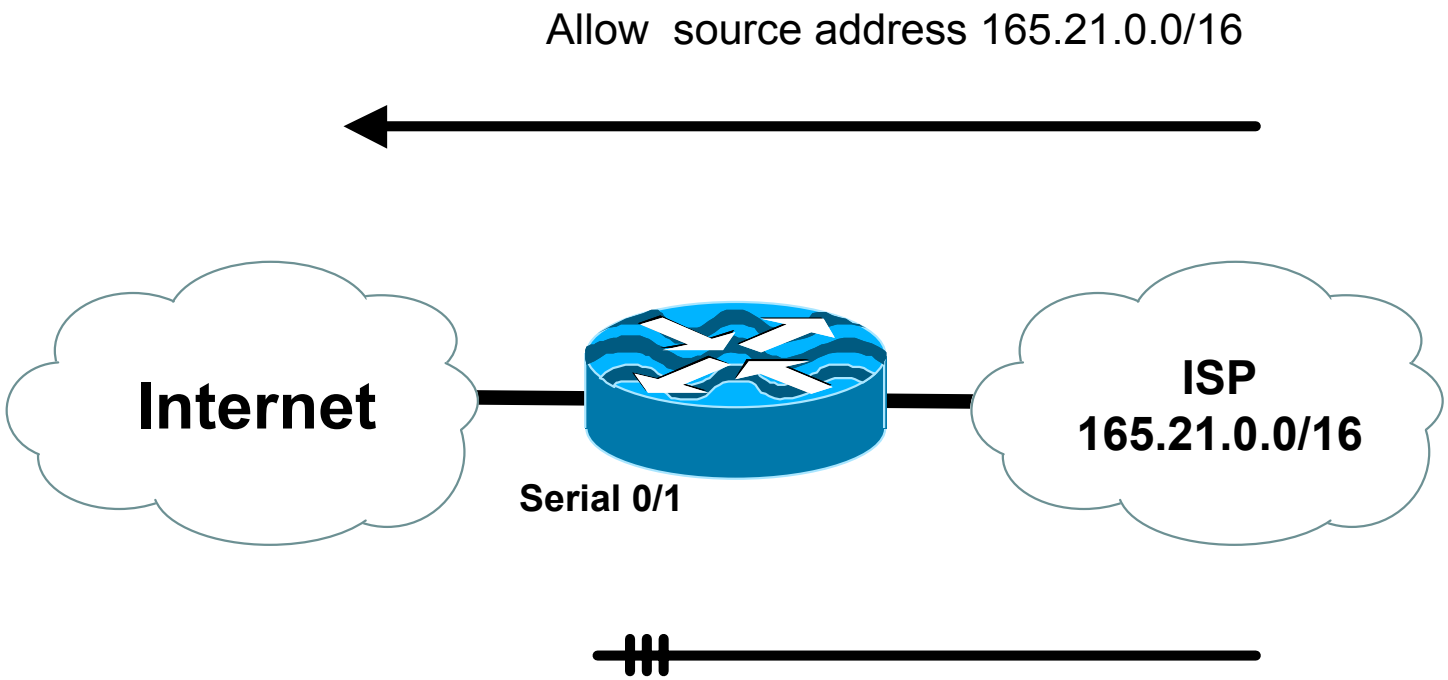
10.0.0.0 - 10.255.255.255 (10/8 prefix)

172.16.0.0 - 172.31.255.255 (172.16/12 prefix)

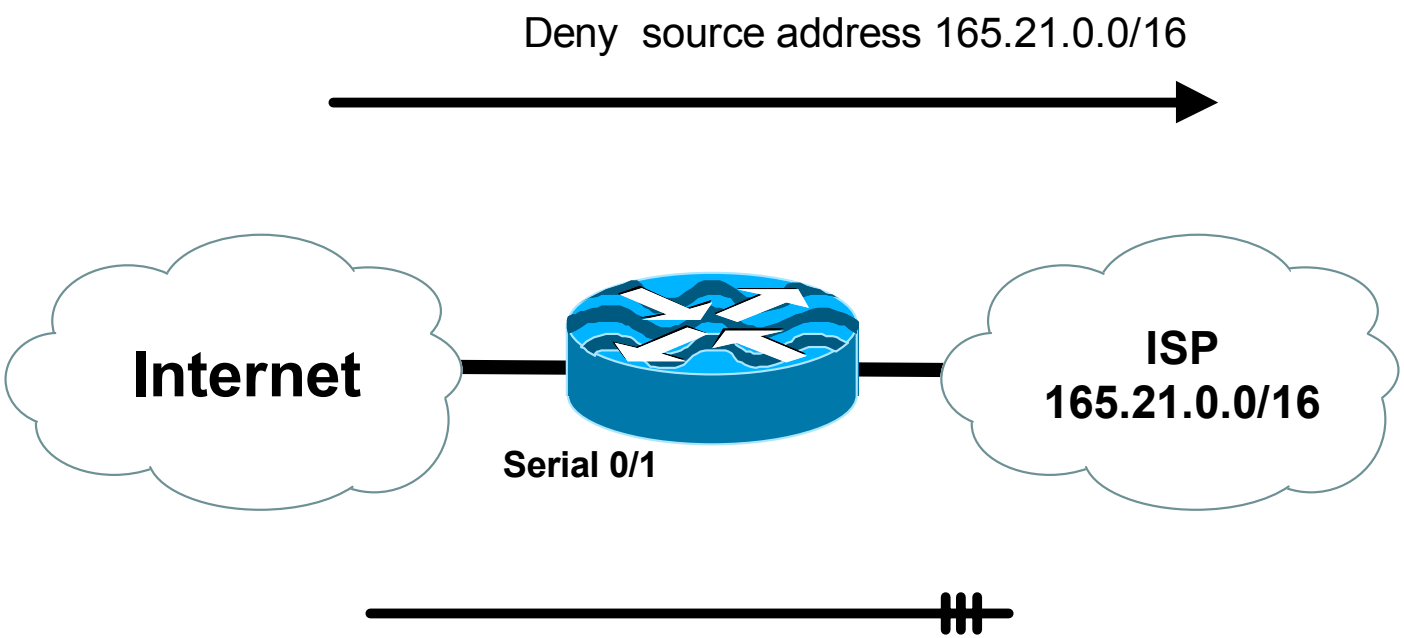
192.168.0.0 - 192.168.255.255 (192.168/16 prefix)

Source: RFC 1918

Ingress Route Filtering

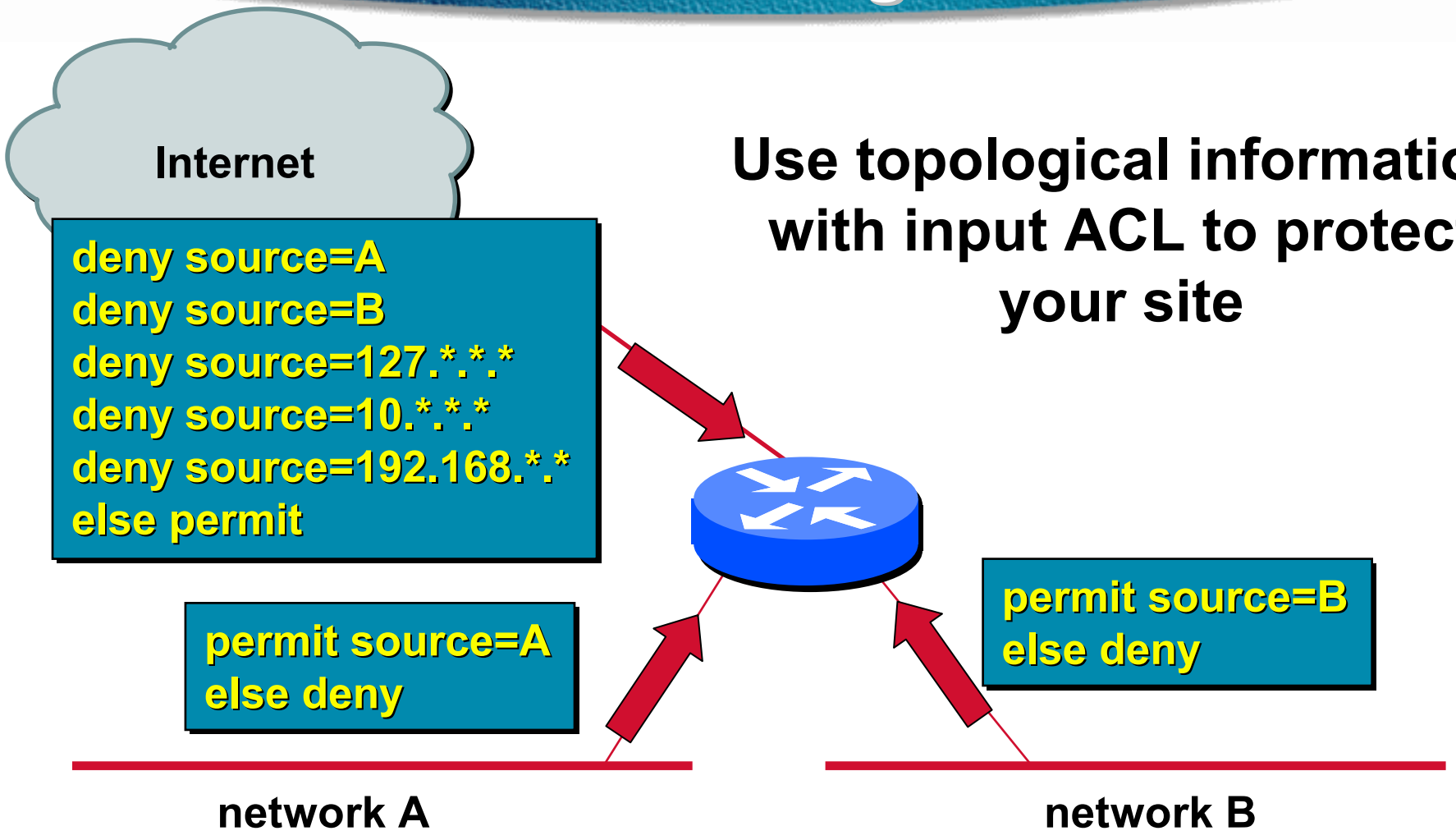


Egress Route Filtering



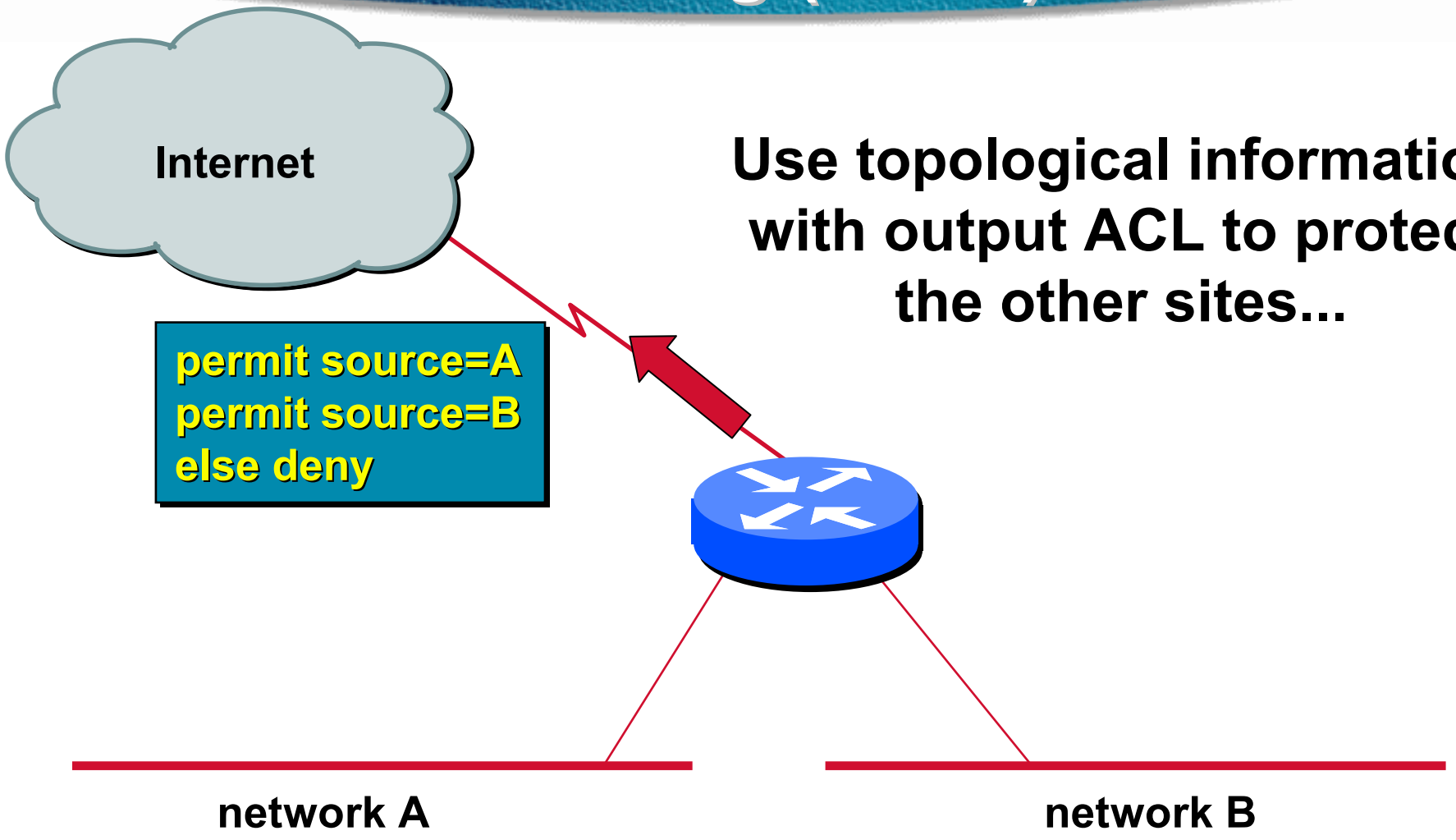
Ex. IP addresses with a source of 10.1.1.1 would be blocked

Enterprise Ingress and Egress Filtering



Use topological information with input ACL to protect your site

Enterprise Ingress and Egress Filtering (Cont.)



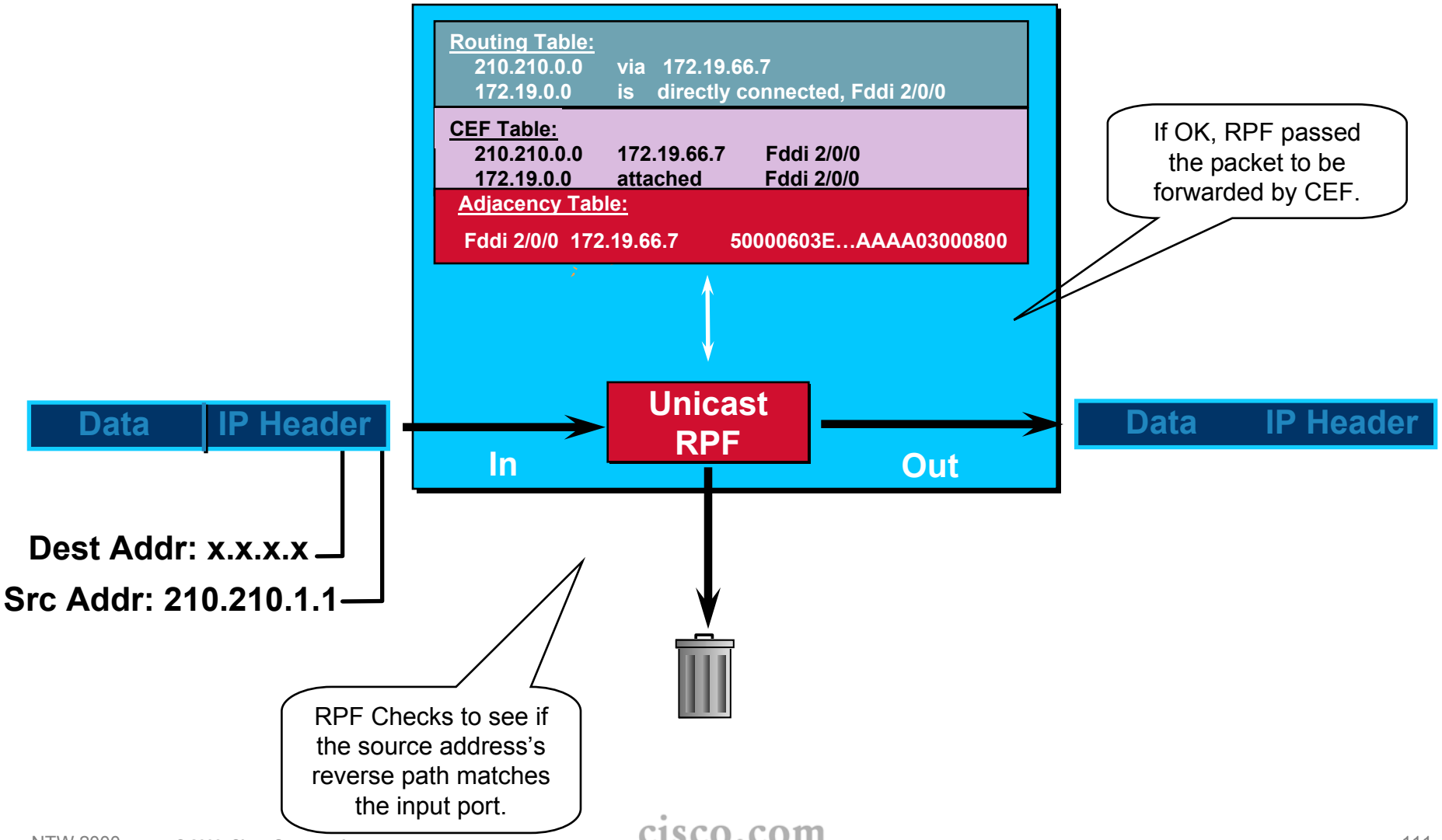
Use topological information with output ACL to protect the other sites...

Source: RFC 2167

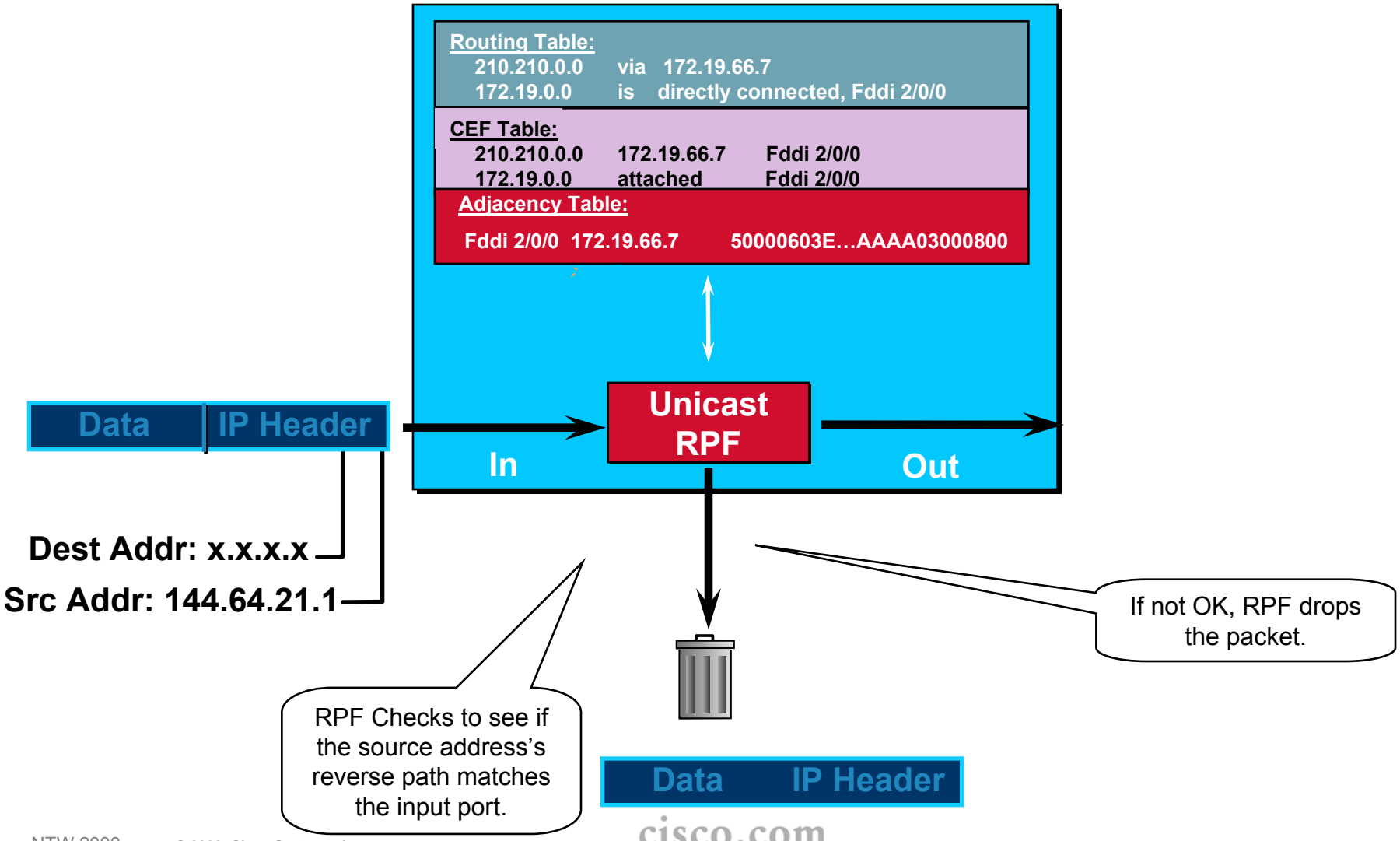
Reverse Path Forwarding

- Supported from 11.1(17)CC images
- CEF switching must be enabled
- Source IP packets are checked to ensure that the route back to the source uses the same interface
- Care required in multihoming situations

CEF Unicast RPF

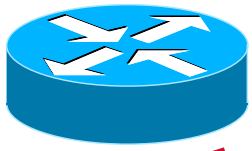


CEF Unicast RPF



Resource Deprivation Attacks

```
version 11.2
!
no service finger
no service udp-small-servers
no service tcp-small-servers
!
```



- Echo (7)
- Dis[illegible]
- Finger (79)
- Daytime (13)
- Chargen (19)

Eliminate unneeded services!!

Addressing DoS Attacks

- ISPs can create an AUP that clearly states how they intend to handle the customer's traffic
- ISP's can craft SLA's, and peering & transit agreements, to include who is responsible for ingress filtering

ICMP Filtering

Extended Access List:

Summary of Message Types

- 0 Echo Reply
- 3 Destination Unreachable
- 4 Source Quench
- 5 Redirect
- 8 Echo
- 11 Time Exceeded
- 12 Parameter Problem
- 13 Timestamp
- 14 Timestamp Reply
- 15 Information Request
- 16 Information Reply

access-list 101 permit icmp any any <type> <code>

no ip unreachables (IOS will not send)

no ip redirects (IOS will not accept)

ICMP Codes are not shown

Source: RFC 792, Internet Control Message Protocol

ICMP Filtering

- **General Case:**

```
access-list 101 permit icmp any any <type> <code>
no ip unreachables      (IOS will not send)
no ip redirects                 (IOS will not accept)
```

- **Example: Control the direction of a ping**

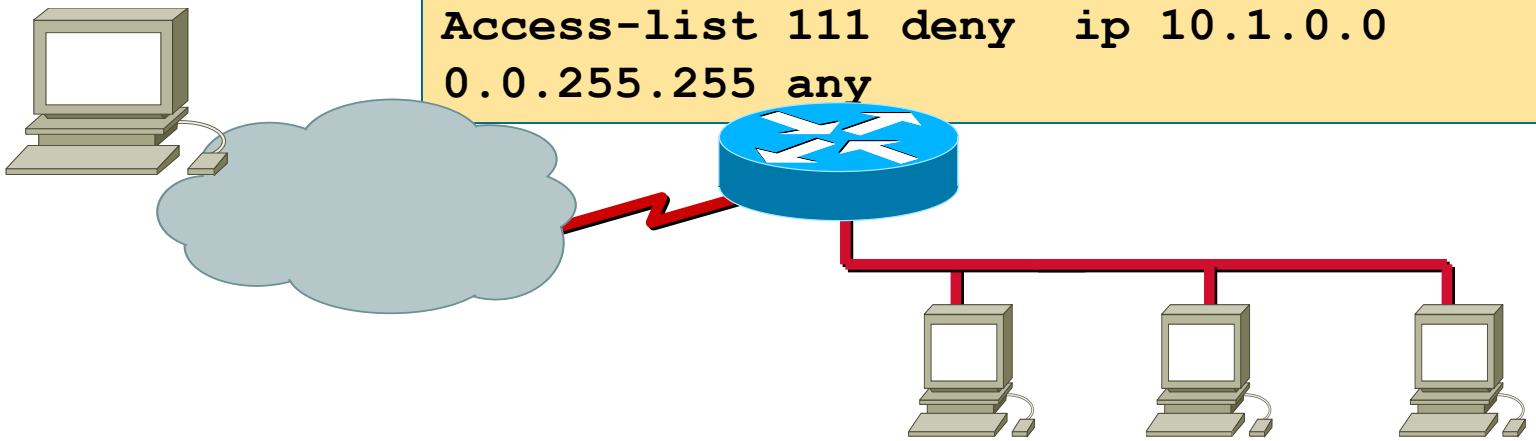
```
access-list 101 permit icmp any any 0
!
Interface Serial 0
Access-group 101 out
```

Summary of ICMP Message Types

- 0 Echo Reply
- 3 Destination Unreachable
- 4 Source Quench
- 5 Redirect
- 8 Echo
- 11 Time Exceeded
- 12 Parameter Problem
- 13 Timestamp
- 14 Timestamp Reply
- 15 Information Request
- 16 Information Reply

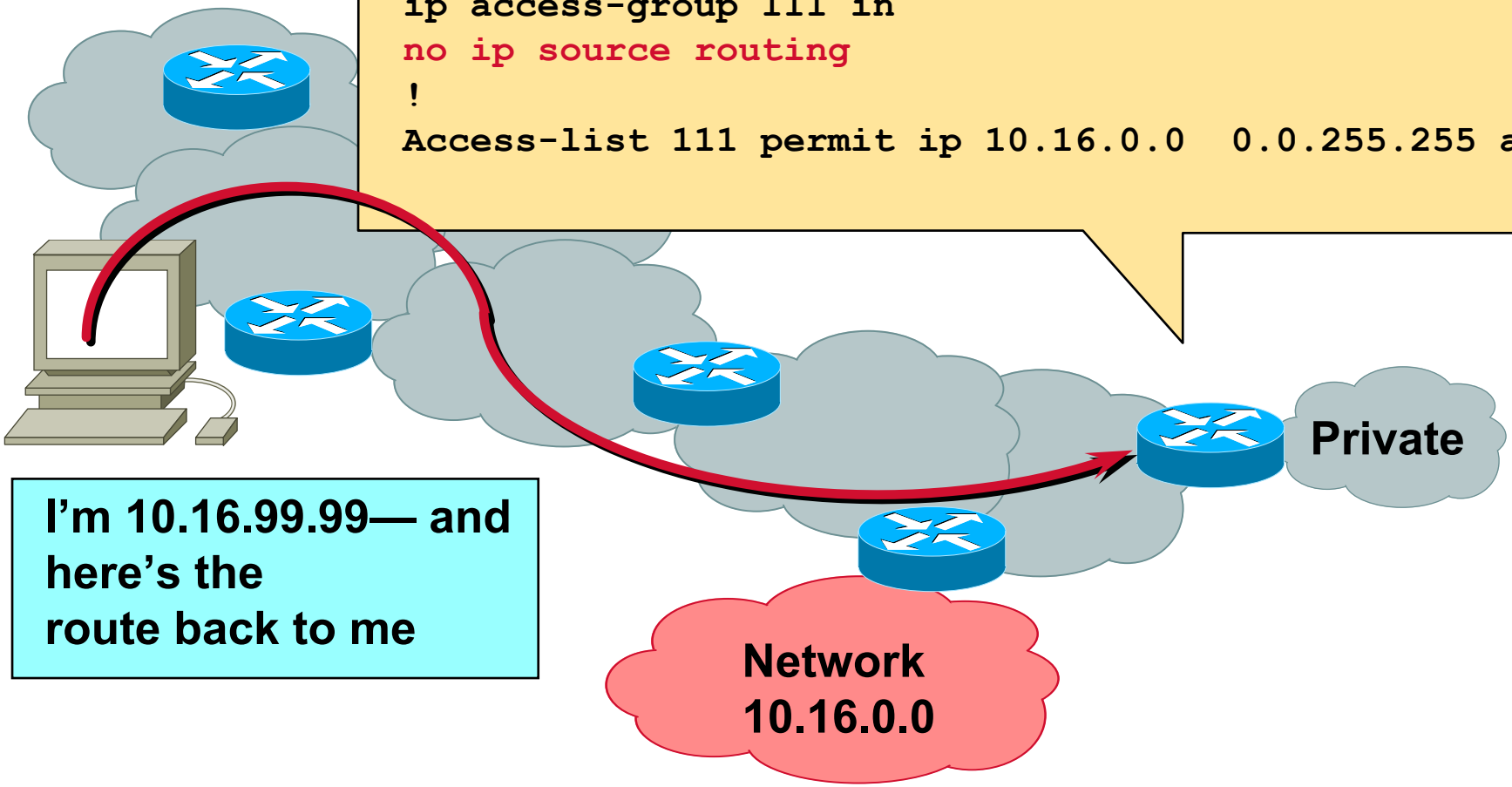
No IP Directed Broadcast

```
interface Serial 1
ip address 172.26.139.2 255.255.255.252
ip access-group 111 in
no ip directed-broadcast
!
interface ethernet 0/0
ip address 10.1.1.100   255.255.0.0
no ip directed-broadcast
!
Access-list 111 deny  ip 127.0.0.0
0.255.255.255 any
Access-list 111 deny  ip 10.1.0.0
0.0.255.255 any
```



No Source Routing

```
interface Serial 1
ip address 172.16.139.2  255.255.255.252
ip access-group 111 in
no ip source routing
!
Access-list 111 permit ip 10.16.0.0  0.0.255.255 any
```



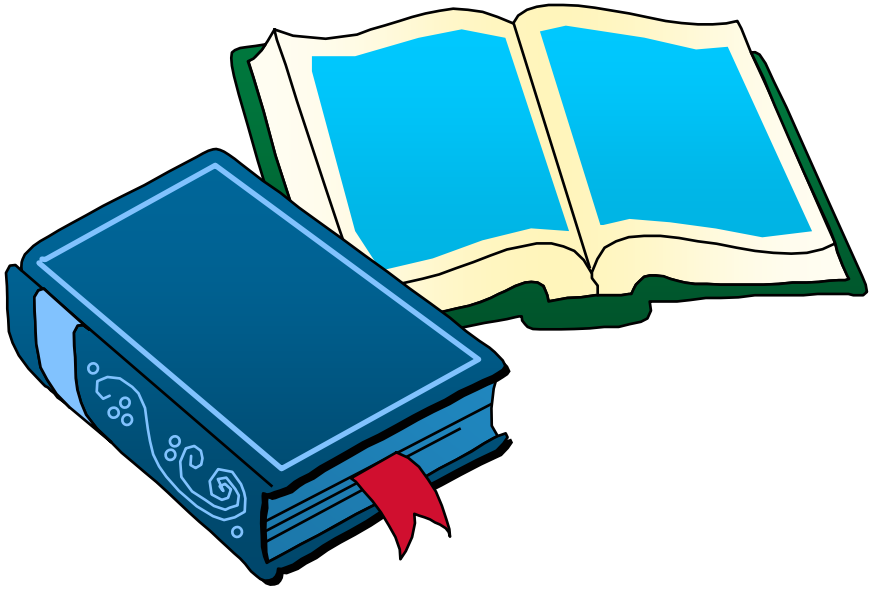
RFC 792: Internet protocol

A Word About Sniffers

- Encrypt sensitive information
- Use one-time authentication or smart cards
- Use switched networks instead of bridges
- Ensure good host security

Audit

- Don’t assume everything is ok
- Actively watch the network
- Investigate any unusual event

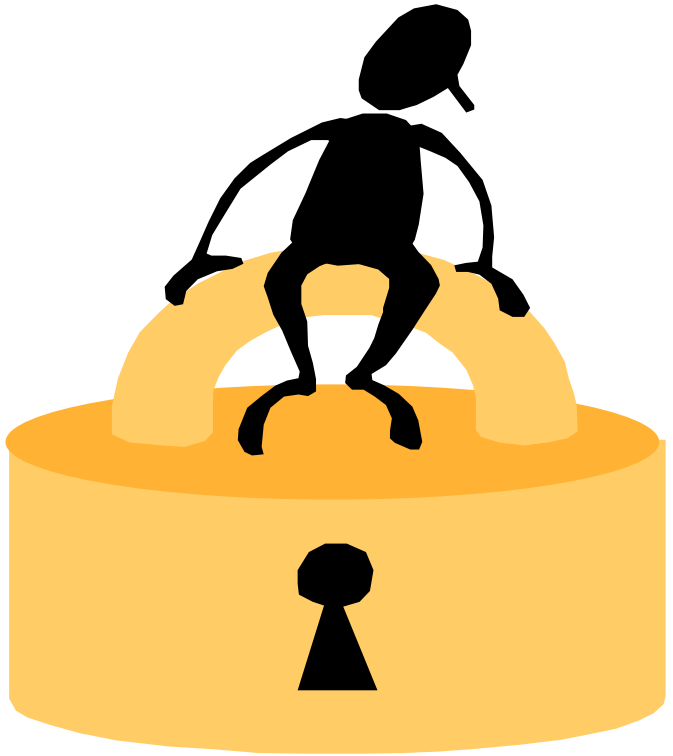


Other Potholes and Chicken Nests

- Avoid segmentation attacks, and other software bugs, by staying up to date with software versions and patches
- Prevent session hijacking through use of encryption and strong random numbers
- Dampened TCP syn attacks through use the “TCP Intercept” feature of IOS 11.2F or PIX firewall

Intrusion Detection

- **To detect individuals attempting attacks against your network, such as the following:**
  - **Reconnaissance**
  - **Access**
  - **Denial of Service**



Profile-Based Detection

- **Anomaly**
  - **Behavior departs from known profile of normal activity**
  - **Requires creation of statistical user profiles**

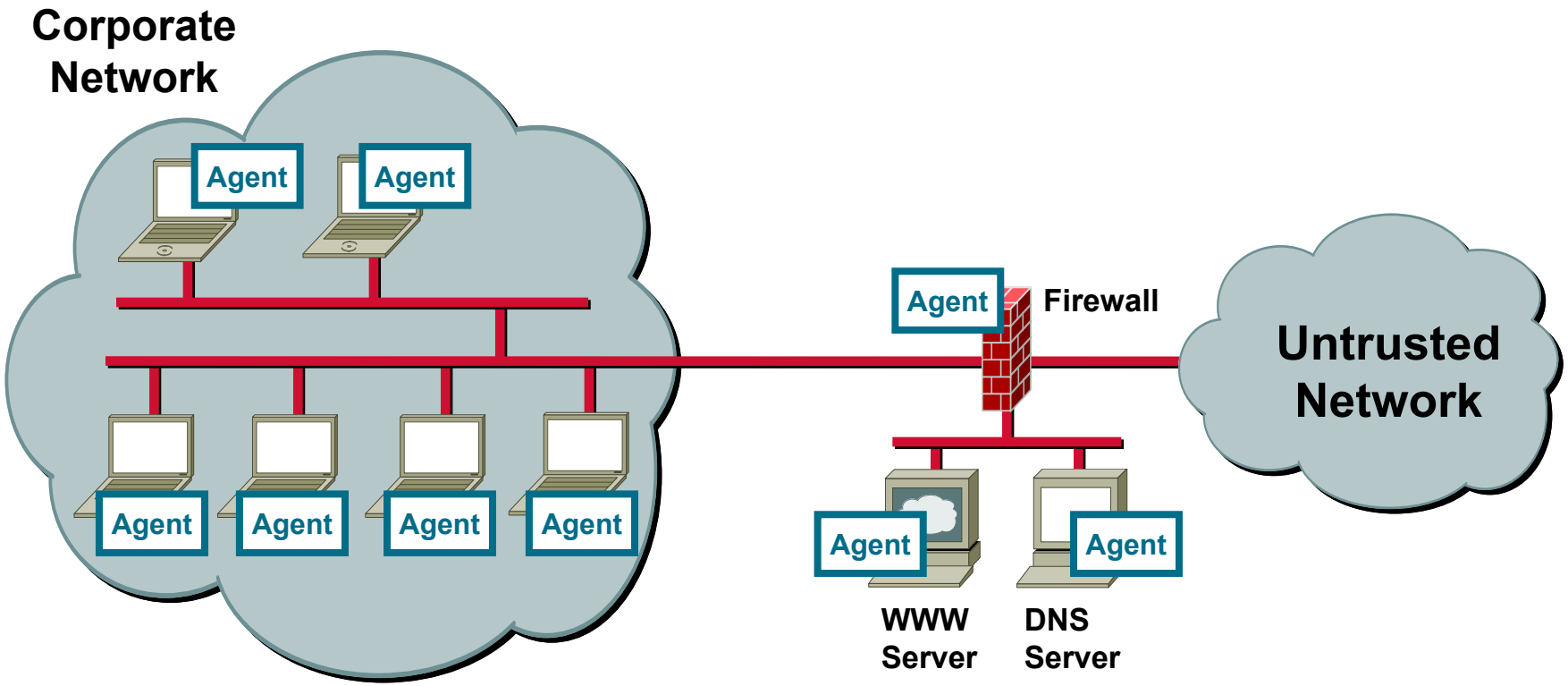
Signature-Based Detection

- **Misuse**

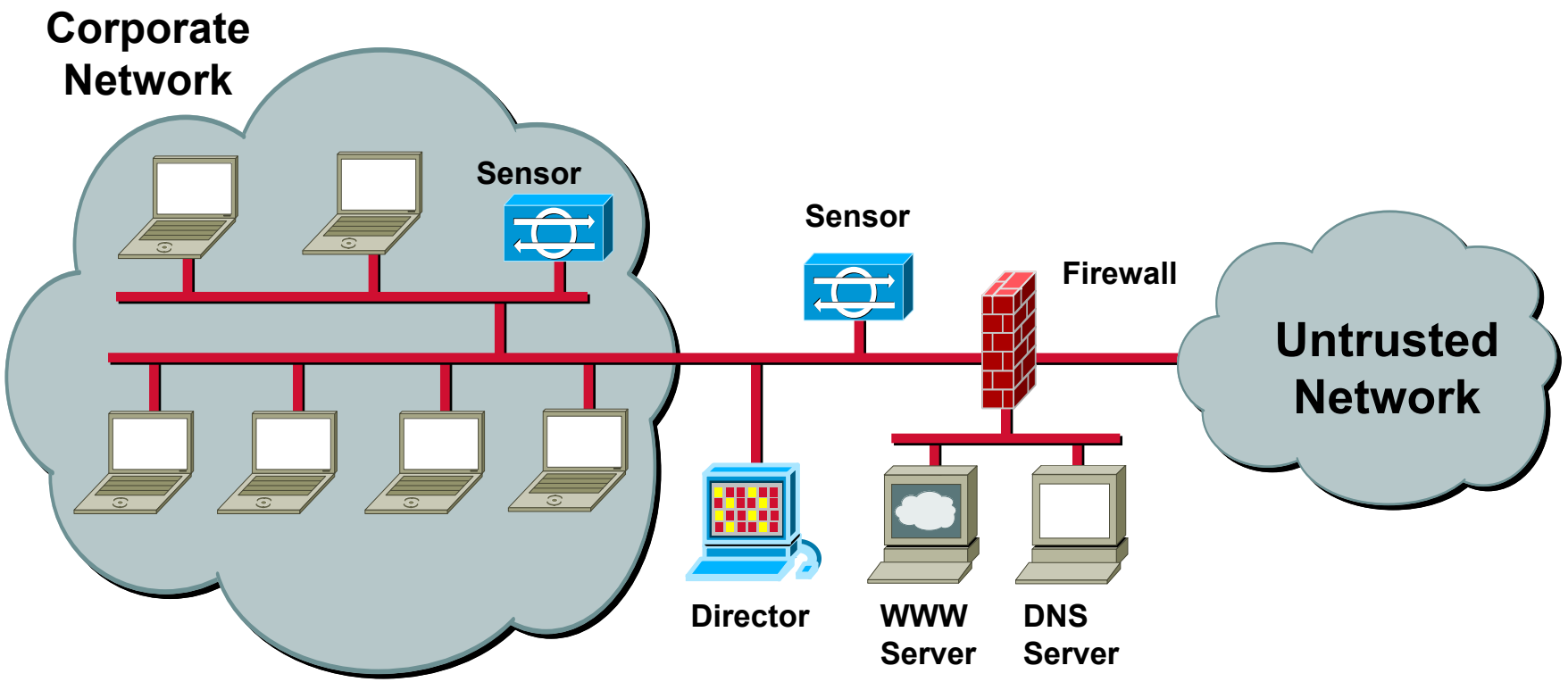
  Behavior matches known patterns of malicious activity

  Requires creation of misuse signatures

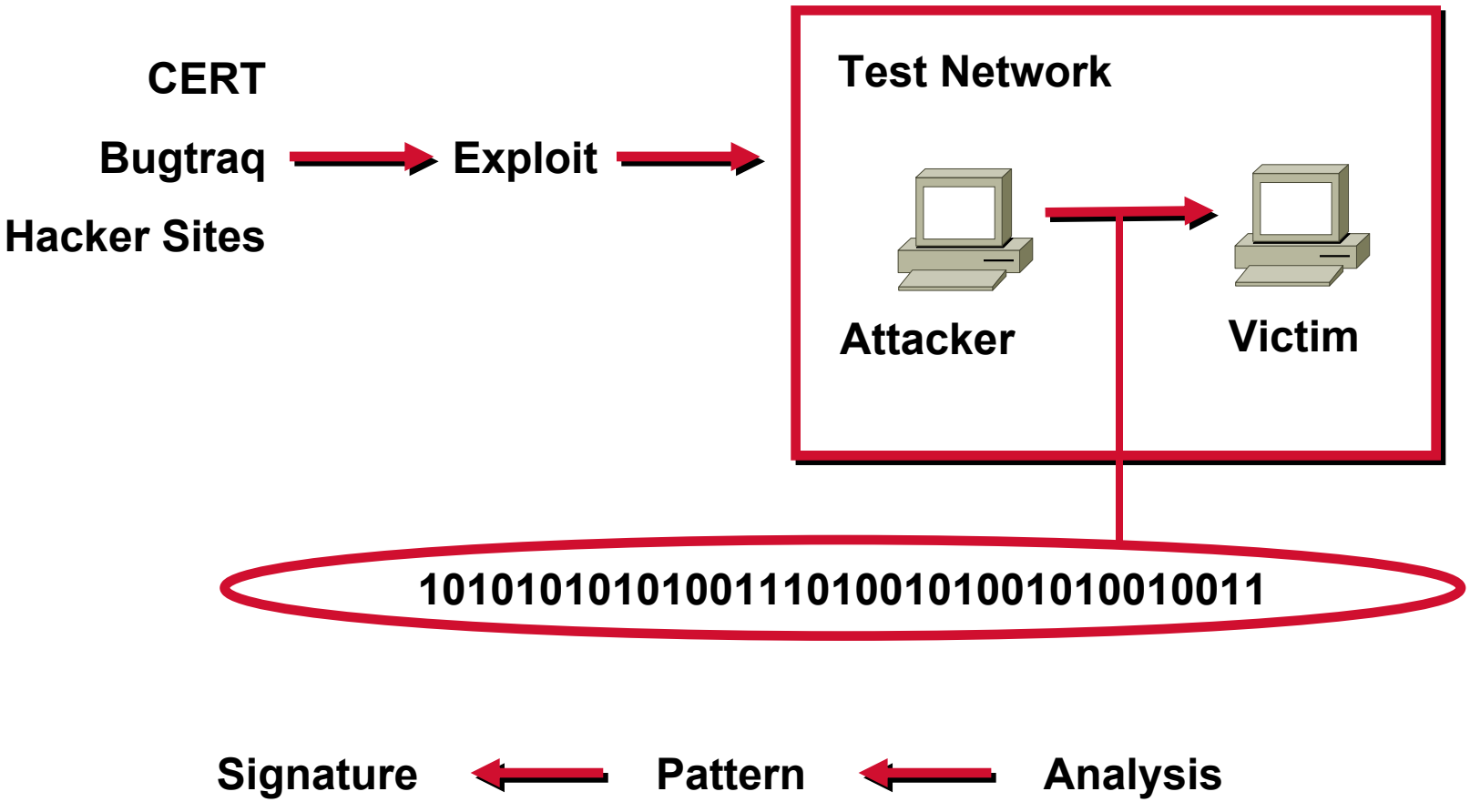
Host-Based Intrusion Detection



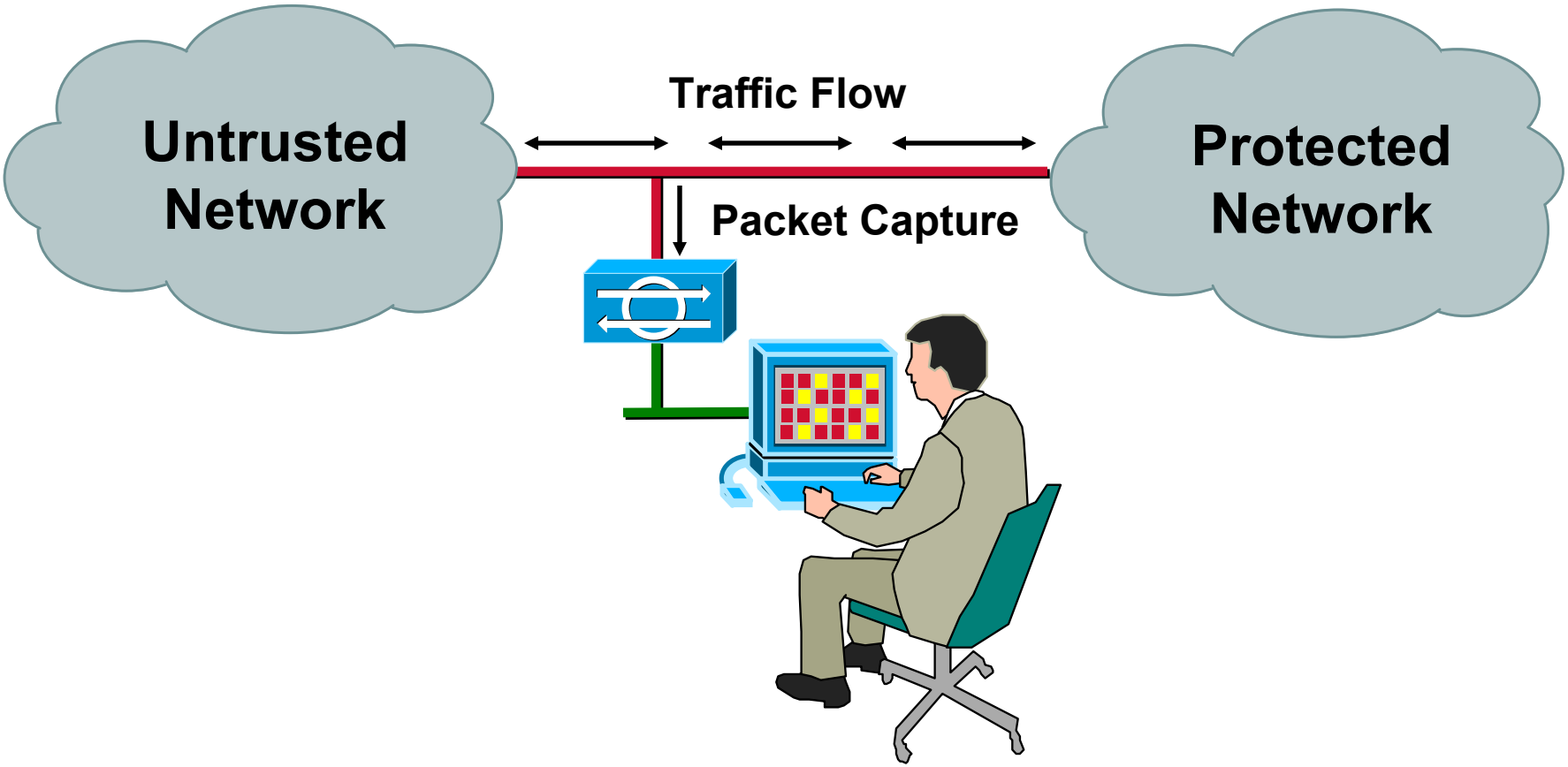
Network-Based Intrusion Detection



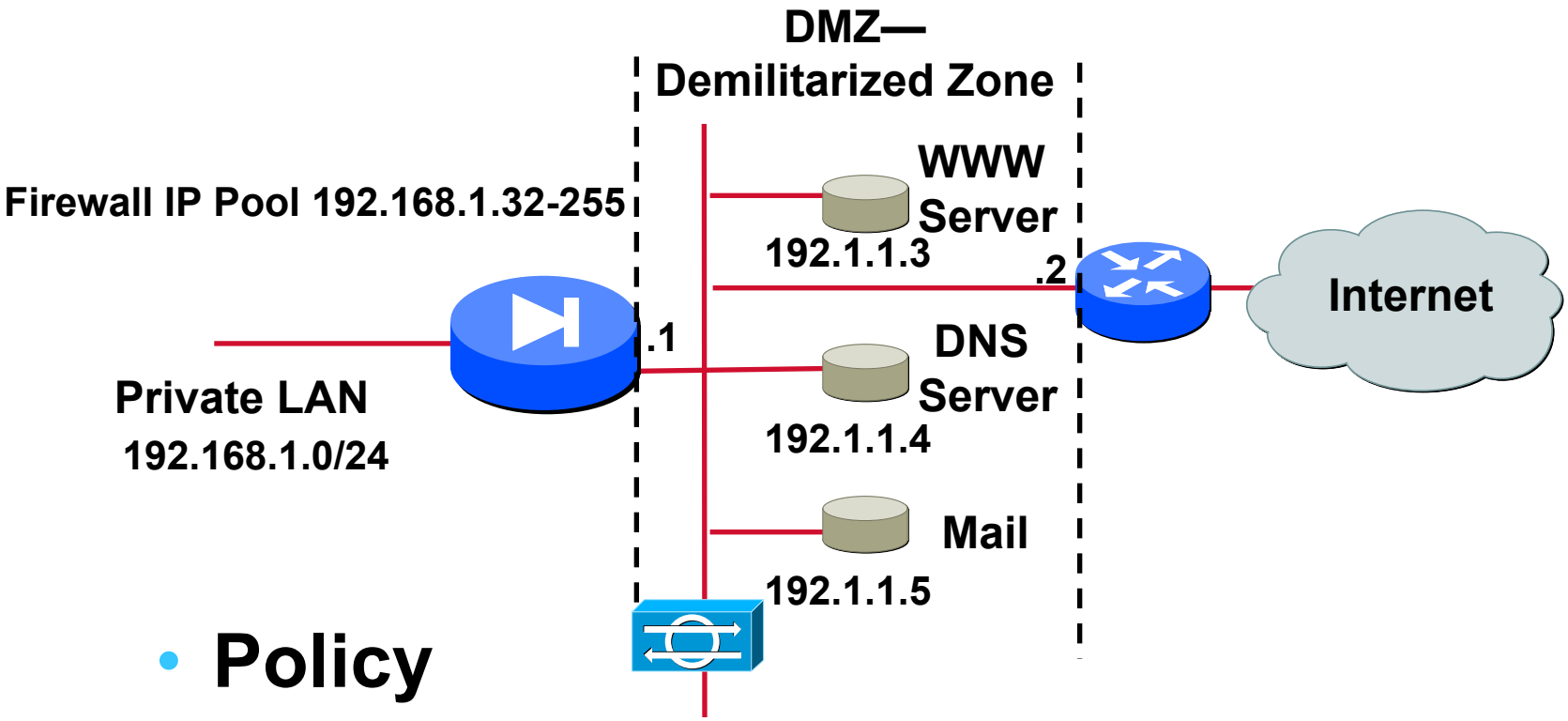
Intrusion Detection Signatures



Intrusion Detection



Firewall For The Internet Access



- **Policy**

  All users can access the Internet

  Servers on DMZ are public

Firewall For The Internet Access

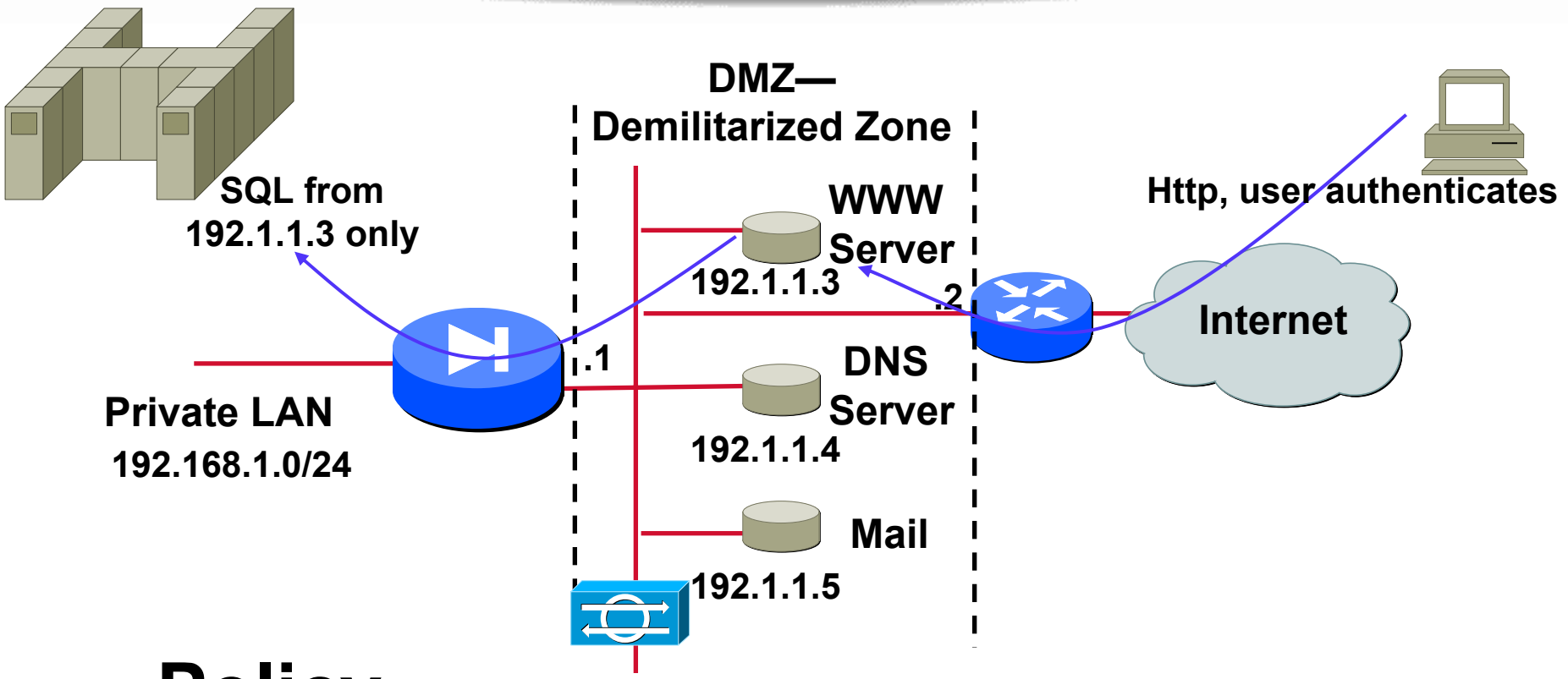
- On the router
  - deny all traffic with your own addresses as source
  - authorize any traffic to the DNS, Web or Mail servers
  - authorize returning traffic to the firewall (NAT Pool)
- On the firewall
  - statefully allow returning traffic

Access-Group ACL On The Router

```
access-list 101 deny ip 192.168.1.0 0.0.0.255 any
access-list 101 deny ip 192.1.1.0 0.0.0.255 any
access-list 101 permit ip any host 192.1.1.3 eq www
access-list 101 permit ip any host 192.1.1.4 eq dns
access-list 101 permit ip any host 192.1.1.5 eq smtp
access-list 101 permit ip any 192.1.1.32 0.0.0.31
access-list 101 permit ip any 192.1.1.64 0.0.0.63
access-list 101 permit ip any 192.1.1.127 0.0.0.127

Interface Serial 0
  access-group 101 in
```

Opening Holes Through The Firewall



- **Policy**

After authentication, external user may have access to their bank account

Opening Holes Through The Firewall

```
static (inside,outside) 192.1.1.6 10.0.1.6
access-list acl_outside permit tcp any host 192.1.1.3
eq sql
access-group acl_outside in interface outside
```

- **To hack the inside host you would first need to hack the web server and then you could use only SQL through the FW**

Good Practices

- To limit OS/Application weaknesses, dedicate one task per public server
- No unnecessary services
- Use Intrusion Detection Software probes in the DMZ
- Remember that opening holes through a FW means stateless


Tools

SSL

- SSL = secure socket layer
- SSL sits between the HTTP application and TCP and was developed by Netscape to protect web traffic.
- SSL is supported by all the major web browsers
- Two components of SSL:
  - SSL record layer
  - SSL handshake layer

How It Works

- A customer contacts a site, accessing a secured URL (indicated by a URL that begins with "https:" instead of just "http:" or by a message from the browser).
- The server responds, automatically sending the customer the server site's digital certificate, which authenticates the server's site.
- Your customer's web browser generates a unique "session key" to encrypt all communications with the site.

How It Works -2

- The user's browser encrypts the session key itself with the site's public key so only the site can read the session key.
- A secure session is now established. It all takes only seconds and requires no action by the user. Depending on the browser, the user may see a key icon becoming whole or a padlock closing, indicating that the session is secure.
- If your site doesn't have a digital certificate, visitors will see a warning message when they attempt to offer credit card or personal information.

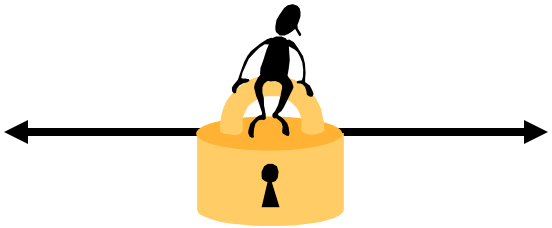
Source: Netscape Communications, Inc.

How It Works -3

request

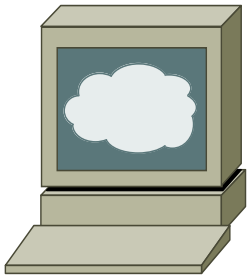
Server's digital certificate

Session Key encrypted with server site's public key



Secure communication

Web server



SSH -1

- Secure Shell was designed to replace the UNIX r* commands: rsh, rlogin, and rcp (ssh, scp, and slogin)
- Added features:
  - strong end-to-end encryption
  - improved user and host authentication
  - TCP and X11 forwarding
- The r* commands depend on the IP address, or the name-to-IP address translation and IP address to be trustworthy. But we know that security based on IP addresses is not very good. SSH uses RSA for host authentication

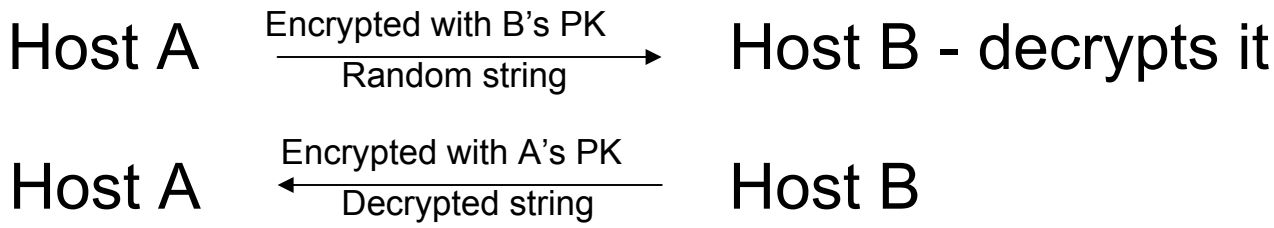
SSH -2

- When installed on a host, a public and private key pair is generated for that host and stored on the host. These are used to authenticate the host to another host with whom a connection is being established.

  The public key of the local host will need to be added to to the ssh_known_hosts file on all remote hosts that the current host wants to access. Or, a user can add the remote host's public key to a similar file in her home directory. Issue: key management/directory services

- Public key cryptography is used for the host-host authentication.

SSH -3



SSH -4

- Once the host to host authentication has taken place, the user can authenticate. The strongest available way:

  The user can generate a public-private key pair and distribute the public key to the remote hosts to which authentication will be needed.

SSH -5

- SSH also provides for encrypted tunnels by using the public private key pairs. A symmetric session key is encrypted using the remote host's public key and sent to the remote host. All transmissions, including the user's authentication information will then be encrypted.
- SSH can also forward TCP ports over the secure connection. For example, e-mail can be configured to go across the encrypted channel.

Responding to Security Incidents

Incident Response

Typical Network Intrusion

- Locate or identify a target host
- Gain regular user-level access to the host
- Obtain elevated privileges on the host
- Conduct unauthorized activity
- Cover tracks
- Jump to another host on the network and continue

Scope and Impact

- **Scope of an incident: the number of systems, networks, data, and other resources affected or accessed during the intrusion**
- **Impact of an incident: the resulting effects of the intrusion on the organization.**
- **The scope and impact of the incident will influence the actions you and your staff will take in response to the intrusion**

Why Should You Care?

- Avoid extensive damage to data, systems, and networks due to not taking timely action to contain an intrusion
- Minimize the possibility of an intrusion affecting multiple systems both inside and outside an organisation because staff did not know who to notify and what actions to take.
- Avoid negative exposure in the news media that can damage an organisation's public image and reputation.
- Avoid possible legal liability and prosecution for failure to exercise due care when systems are inadvertently or intentionally used to attack others.

Who Should Be Involved?

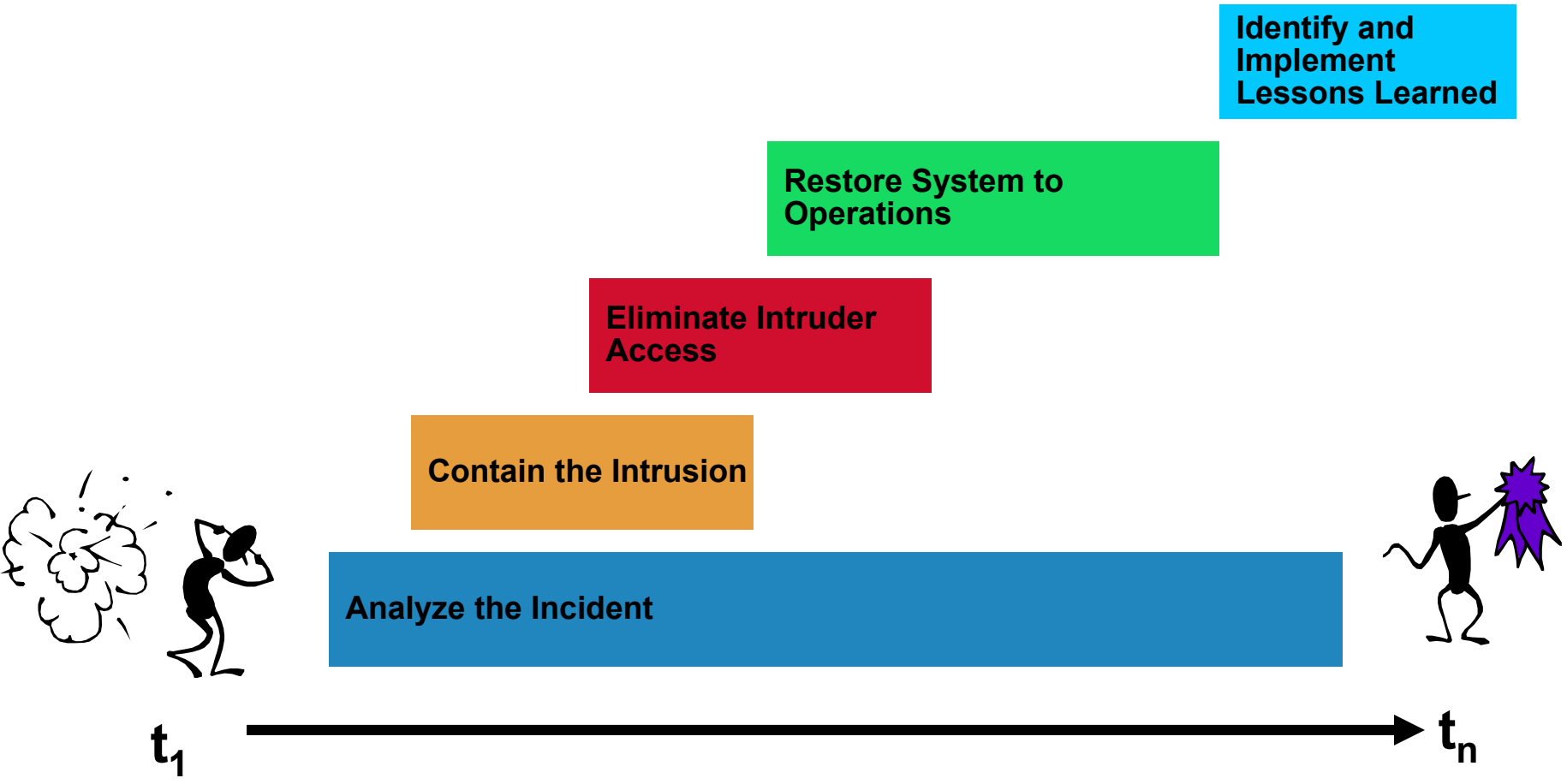
- Management
- Legal
- Network Admin
- Users
- Security
- System Admin

- Top management (CTO, CIO)
- Public Relations
- HR
- Incident Response Teams

Components of Response

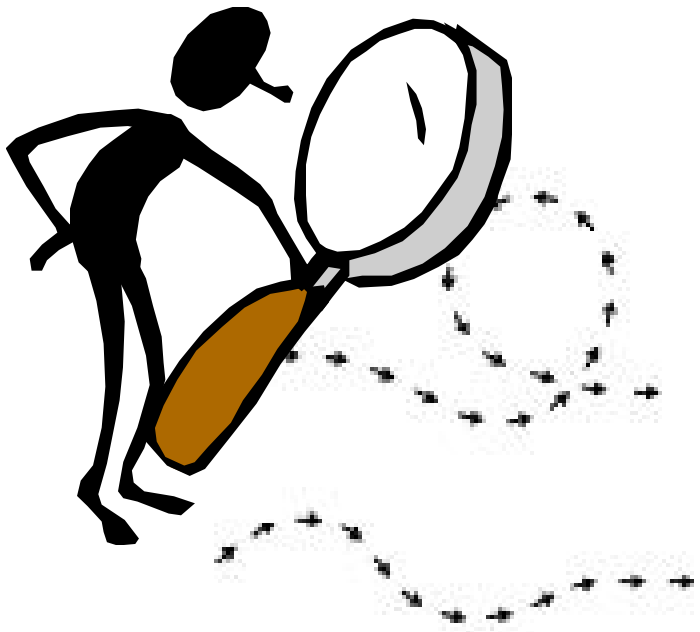
- Analyze the event
- Contain the incident
- Eliminate intruder access
- Restore operations
- Update procedures based on lessons learned

Timing



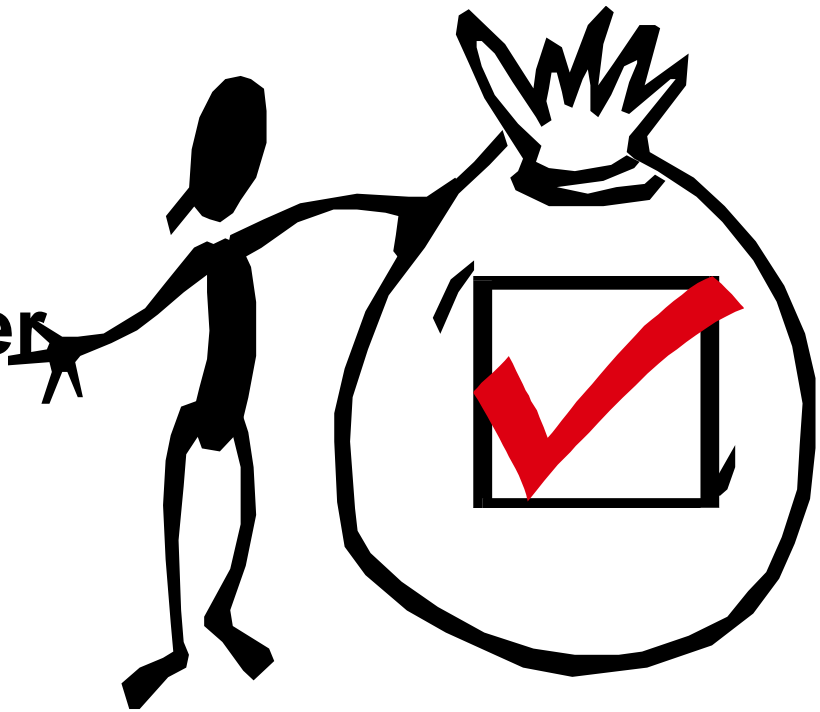
Analyze Event

- What systems were used to gain access
- What systems were accessed by the intruder
- What information assets were available to those systems?
- What did the intruder do after obtaining access?
- What is the intruder currently doing?



Contain the Intrusion

- Gain control of the systems involved
- Attempt to deny the intruder access in order to prevent further damage
- Monitor systems and networks for subsequent intruder access attempts

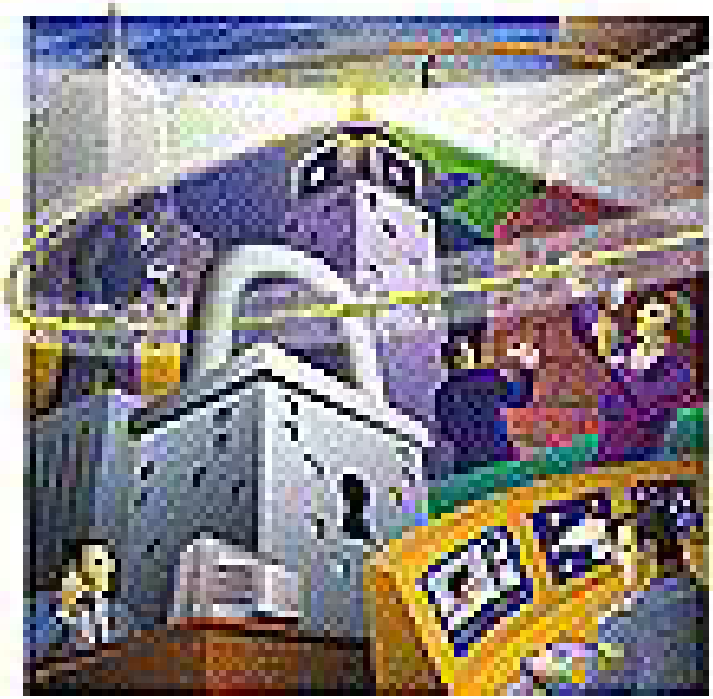


Eliminate Intruder Access

- Change all passwords on all systems accessed
- Restore system and application software and data, as needed
- What other systems might be vulnerable?

Restore Operations

- Validate the restored system
- Monitor systems and networks
- Notify users and management that systems are again operational



Preparing to Respond

- Create an archive of original media, configuration files, and security-related patches for all router and host operating systems and application software versions
- Ensure that backup tools and procedures are working
- Create a database of contact information
- Select and install tools to use when responding to intrusions

Preparing to Respond (Cont.)

- Develop a plan and process to configure isolated test systems and networks when required
- Keep response plans, procedures and tools up to date
- Consider performing a practice drill to test tools and procedures

Responding to Security Incidents

Forming an Incident Response Team

Incident Response Team

A Computer Security Incident Response Team (CSIRT) is a team that performs, coordinates, and supports the response to security incidents that involve sites within a defined constituency.

RFC 2350 "Expectations for Computer Security Incident Response"

Purpose

To facilitate efficient and effective handling of security incidents in order to minimize their impact on the organization

Elements of a CSIRT

- Constituency
- Sponsorship or Affiliation
- Authority

Elements of a CSIRT (Cont.)

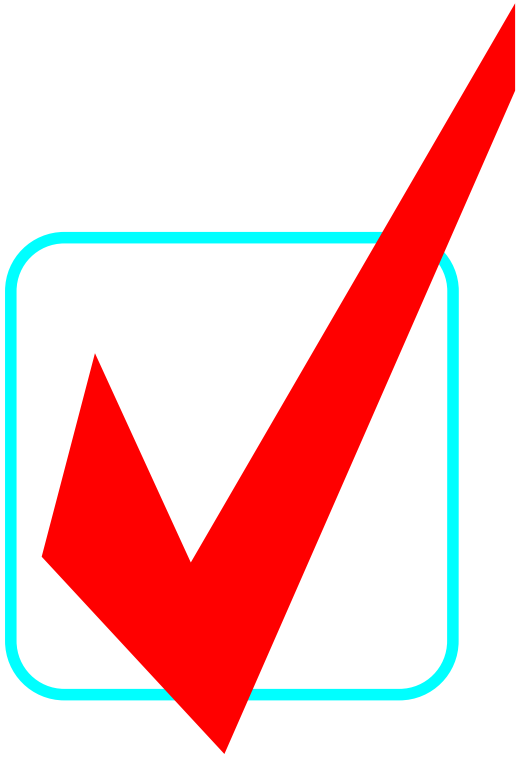
- Types of incidents handled
- Level of service
- Cooperation and disclosure of information
- Protected communications

ISP Issues

- Will you provide incident response service for your subscribers?
- If not, what role will you play in helping your customers with security incidents?
- Alerting customers of security incidents that affect them.

ISP Issues (Cont.)

- Alerting customers when the ISP's infrastructure has been breached
- Providing accurate contact information for the reporting of security problems



In Summary

- The question isn't if you'll have to handle a significant security incident…
- It's WHEN and HOW BAD will it be!


The Hacker News Network
www.hackernews.com
HOPE
August 13-14, 1994
Hotel Pennsylvania
New York City
Celebrating 10 years of 2600
2600
Magazine
The HACKER Quarterly
Are
You
Ready?
phrack
v0.56
http://www.phrack.com
Authorization failed.
Authorization failed.
Authorization failed
ABORT

Resources

- Distributed Systems Intruder Tools Workshop Report

  http://www.cert.org/reports/dsit_workshop.pdf

- Denial of Service Information Page

  http://www.denialinfo.com/

- IOS Essentials - Features Every ISP Should Consider

  http://www.cisco.com/public/cons/isp/documents/IOSEssentialsPDF.zip

- CERT Advisories

  http://www.cert.org/

- FIRST

  http://www.first.org/

More information

- **Improving Security on Cisco Routers**

  http://www.cisco.com/warp/public/707/21.html

- **Cisco Product Security Incident Response (PSIRT)**

  http://www.cisco.com/warp/public/707/sec_incident_response.shtml

- **Cisco Security Advisories**

  http://www.cisco.com/warp/public/707/advisory.html

- **Characterizing and Tracing Packet Floods Using Cisco Routers**

  http://www.cisco.com/warp/public/707/22.html

- **Strategies to Protect Against Distributed Denial of Service Attacks**

  http://www.cisco.com/warp/public/707/newsflash.html