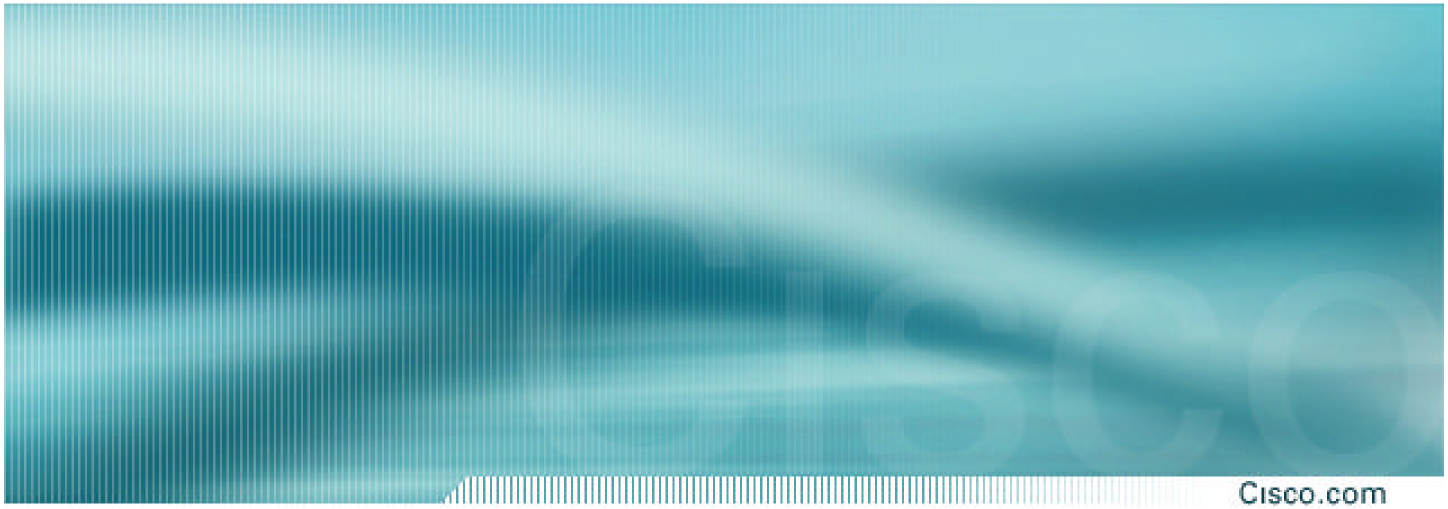


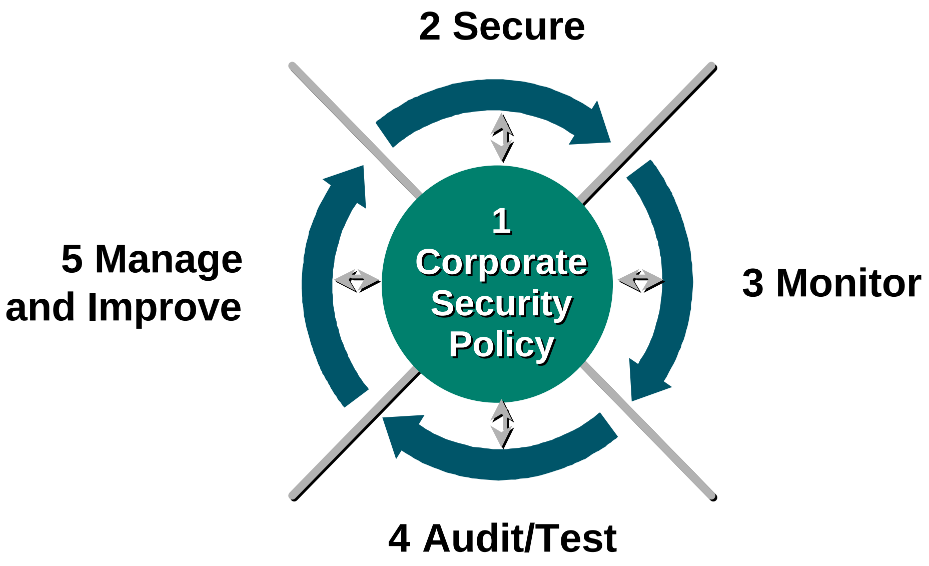
Designing Secure Networks: Dos and Don'ts

Session PS-550

Introduction

- Security lifecycle
- A word about physical security and network and system administration practices
- Today's course

The Security Lifecycle



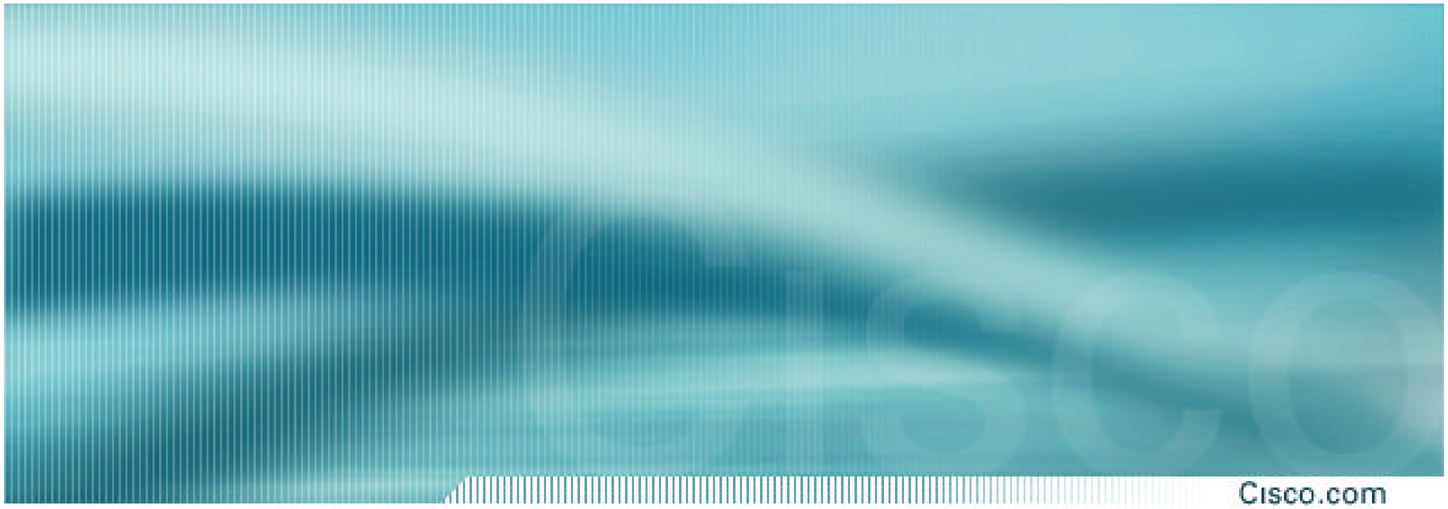
A Word about Physical Security

Cisco.com

- Secure your physical plant
- Dispose of sensitive information carefully
- Teach employees to be on the lookout for social engineering

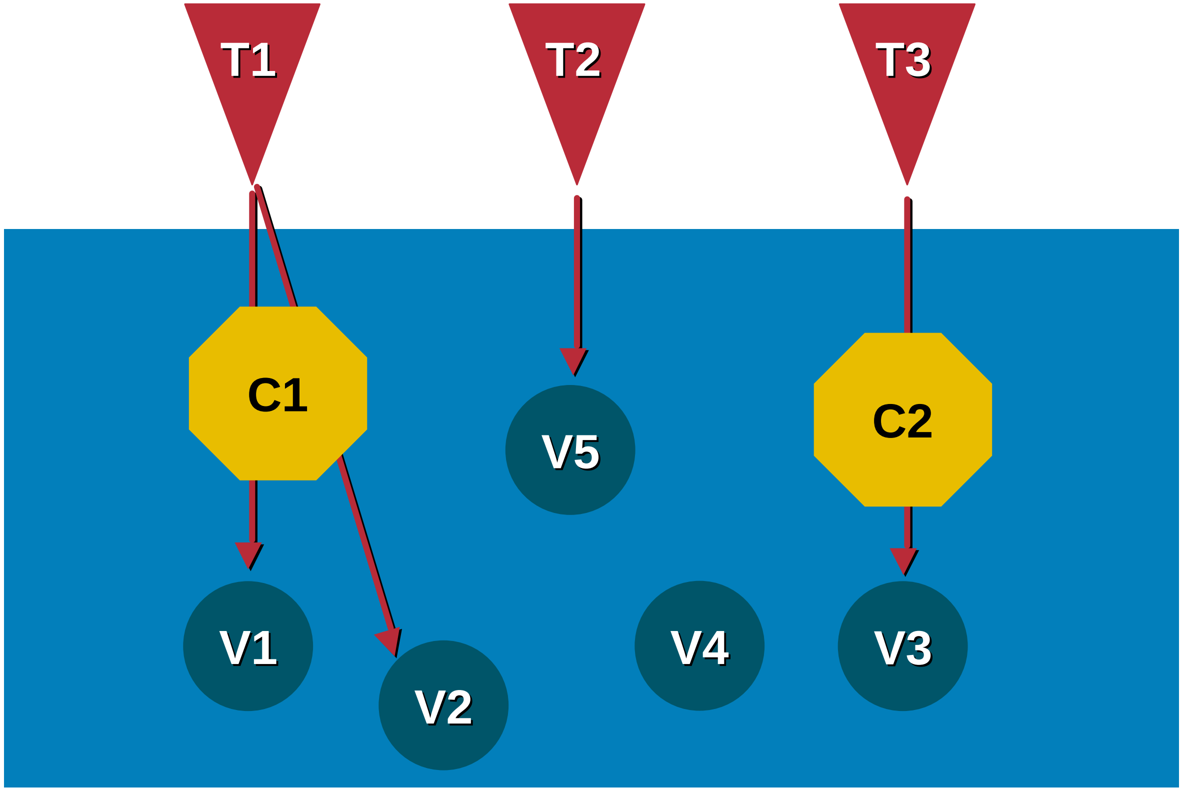
Today's Course Outline

- Understanding Threats and Vulnerabilities
- Securing Network Devices
- Securing the Corporate Internet Connection
- Securing E-Commerce Services
- Securely Connecting Remote Offices and Users
- Wireless and LAN Switch Security
- Resiliency Techniques



Understanding Today’s Threats and Vulnerabilities

Threats,Vulnerabilities, and Countermeasures



Threats

Threats

Guns for Hire

Governments

Script Kiddies

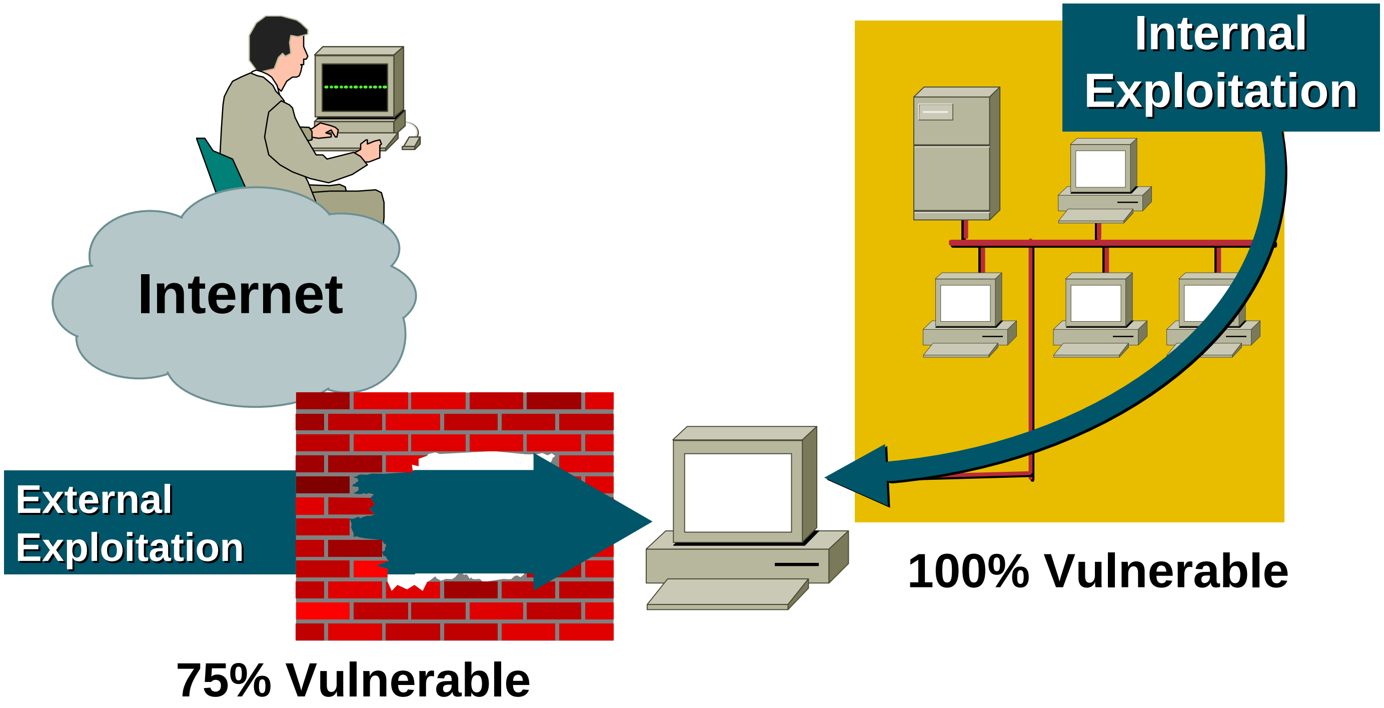
Disgruntled Employees

Terrorists

Vulnerabilities

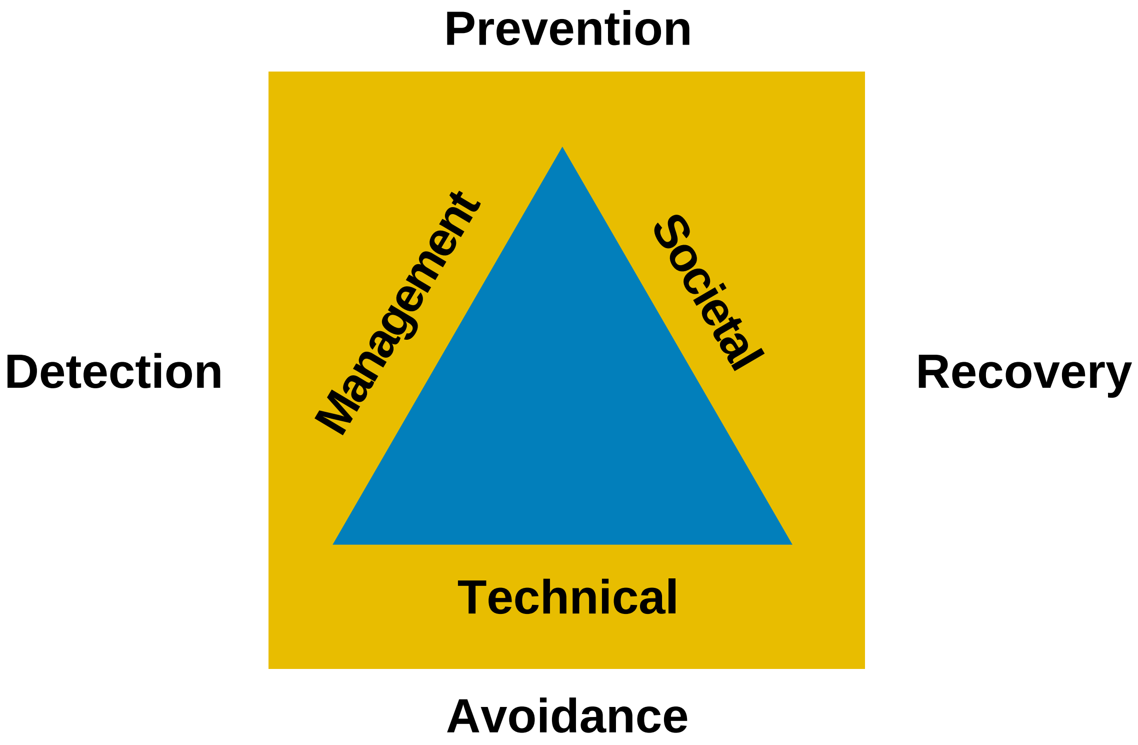
- Designs
- Configurations
- Management
- Software and hardware bugs

The Community's Vulnerability



Source: Cisco Security Posture Assessments 1996–1999

Countermeasures



Prevention

Detection

Management

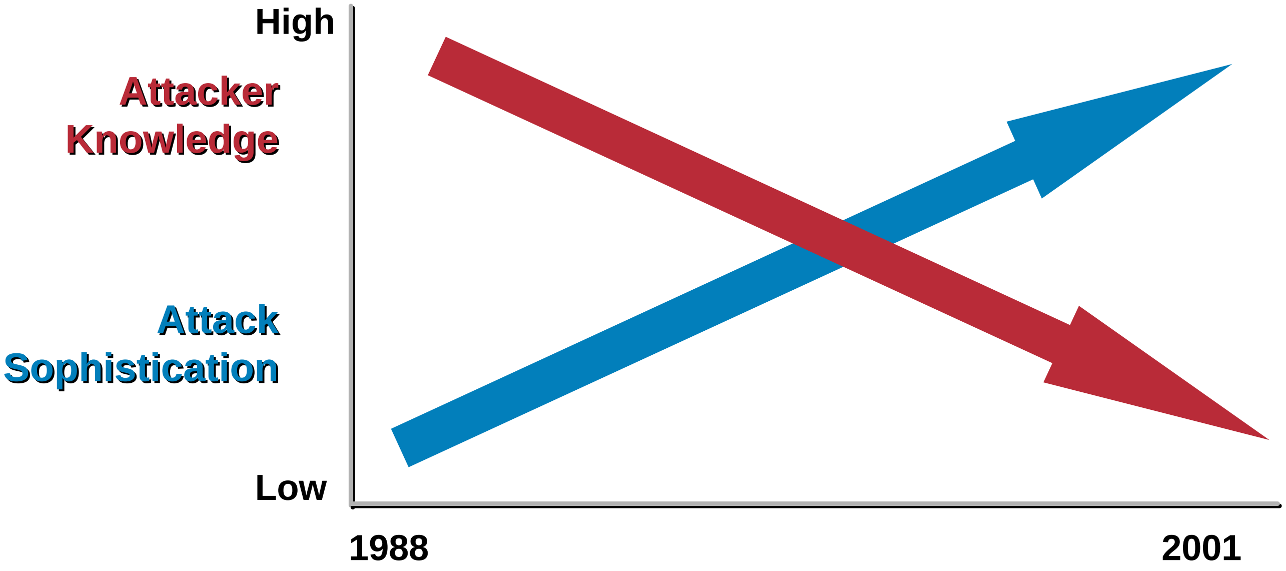
Societal

Recovery

Technical

Avoidance

Attack Trends



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

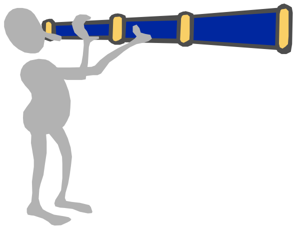
Evolving Dependence

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

Classes of Attacks

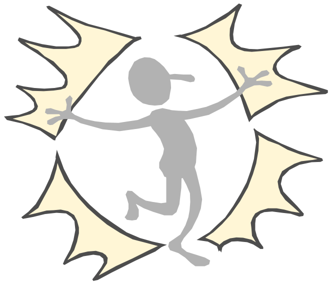
- **Reconnaissance**

  Unauthorized discovery and mapping of systems, services, or vulnerabilities



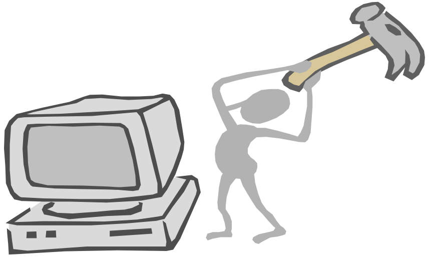
- **Access**

  Unauthorized data manipulation, system access, or privilege escalation

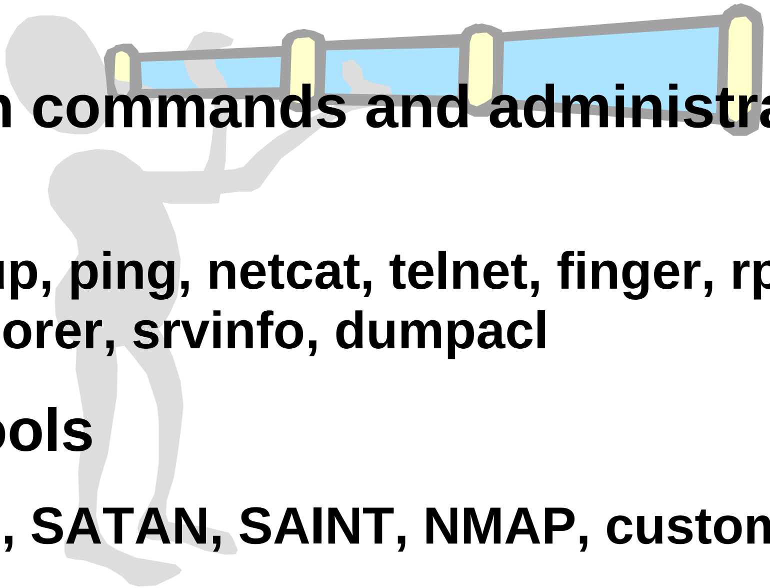


- **Denial of Service**

  Disable or corrupt networks, systems, or services



Reconnaissance Methods



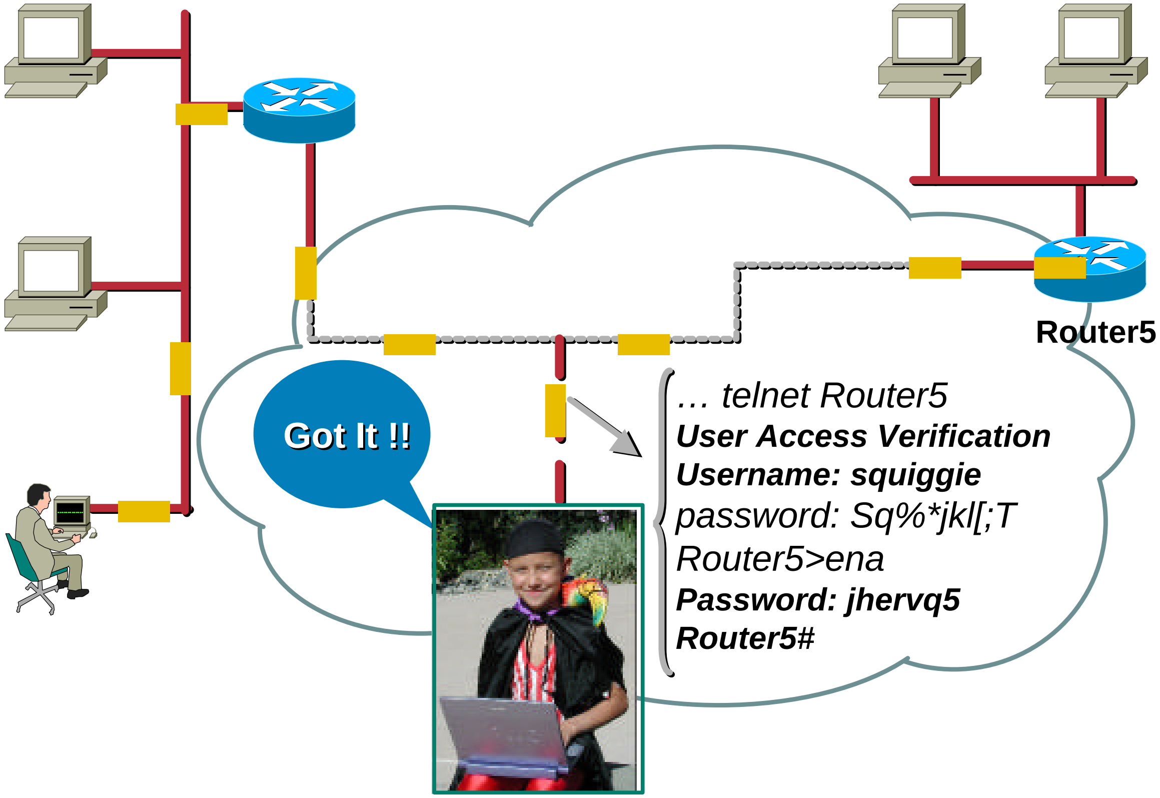
- **Common commands and administrative utilities**

  nslookup, ping, netcat, telnet, finger, rpcinfo, file explorer, srvinfo, dumpacl

- **Public tools**

  Sniffers, SATAN, SAINT, NMAP, custom scripts

Network Sniffers



```
… telnet Router5
User Access Verification
Username: squiggie
password: Sq%*jkl[;T
Router5>ena
Password: jhervq5
Router5#
```

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
```

Attacking Switched Networks

- **ARP spoofing**
- **MAC flooding**

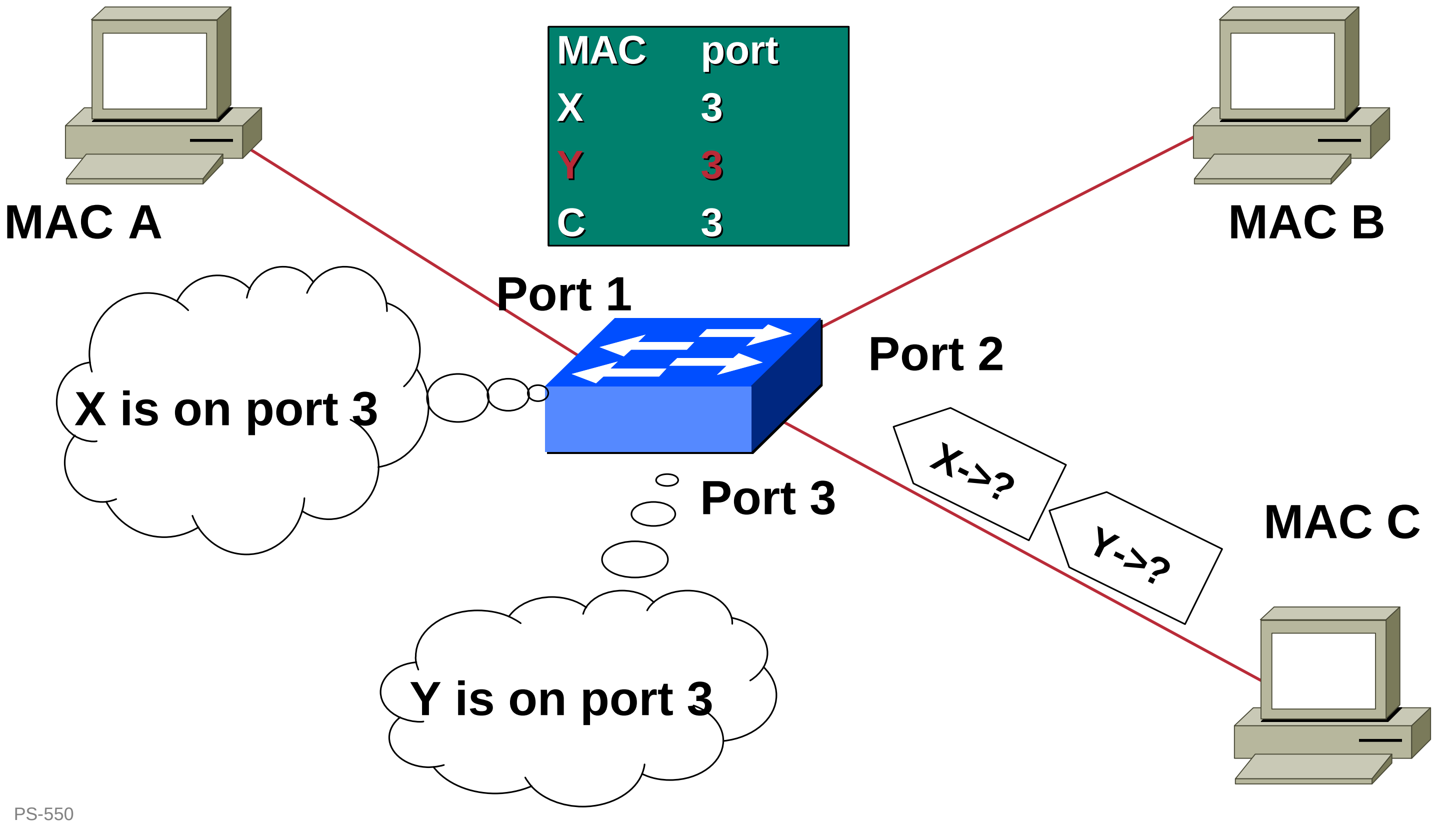
ARP Spoofing

- A send a broadcast ARP request
- C responds with ARP reply with MAC address
- Or…Node B can craft and send an unsolicited, fake ARP reply to Node A
- Node A will unwittingly send the traffic to node B since it professes to have the intended MAC address
- Dsniff and other tools specialize in sending fake ARP requests and in sniffing for specific types of traffic

MAC Flooding

- Switches keep a translation table that tracks which MAC addresses are on which physical port
- The amount of memory for this translation table is limited
- Once all the memory is consumed and all legitimate table entries have been replaced, some switches will begin to flood all frames to all ports, reverting to a hub behavior
- Traditional sniffers will now work

CAM Overflow Example



MAC	port
X	3
Y	3
C	3

MAC A

MAC B

MAC C

Port 1

Port 2

Port 3

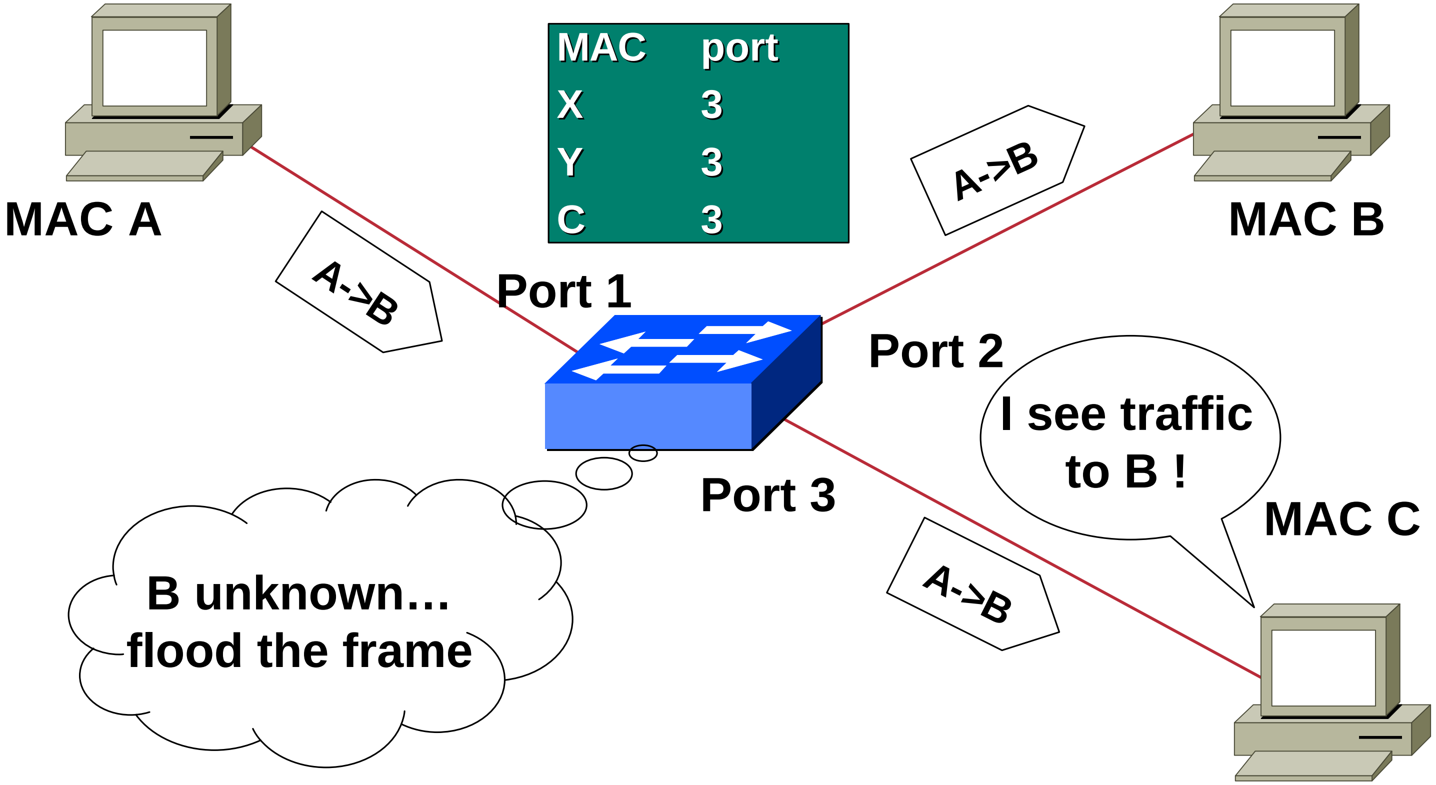
X is on port 3

Y is on port 3

X->?

Y->?

CAM Overflow Example



MAC	port
X	3
Y	3
C	3

Why Do You Care?

- **The more information you have, the easier it will be to launch a successful attack:**

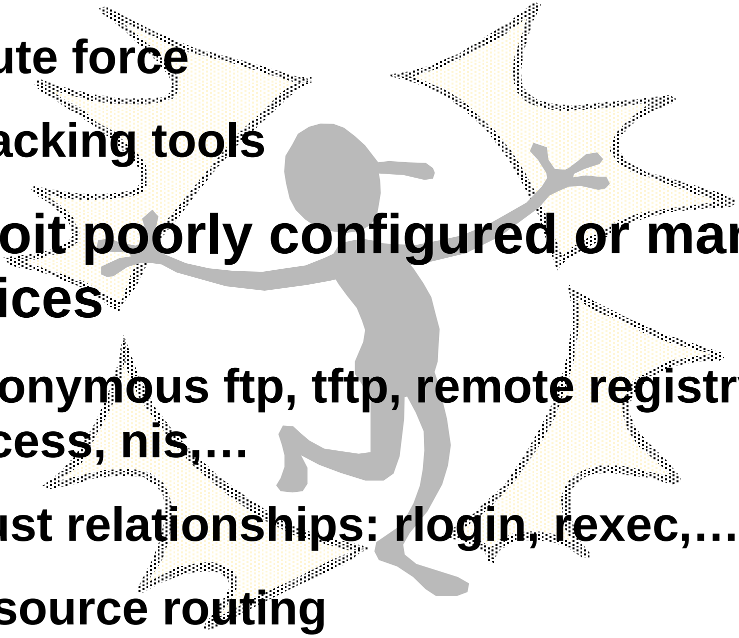
  Map the network

  Profile the devices on the network

  Exploit discovered vulnerabilities

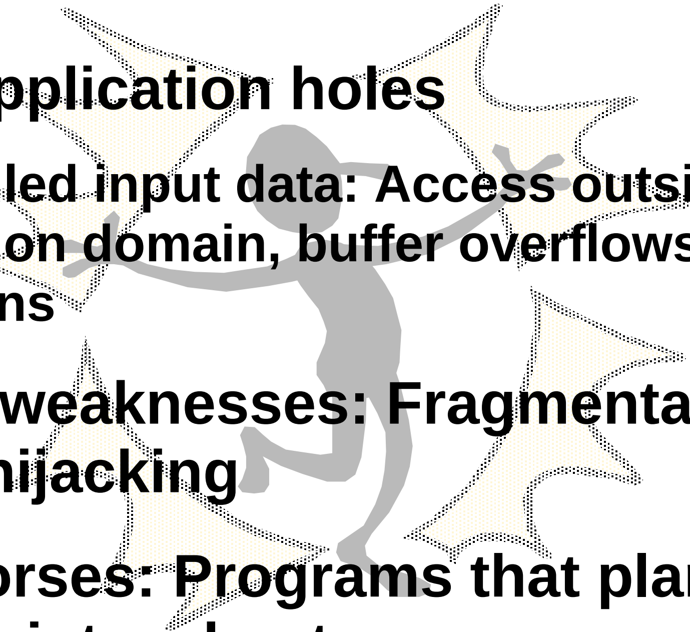
  Achieve objective

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.)

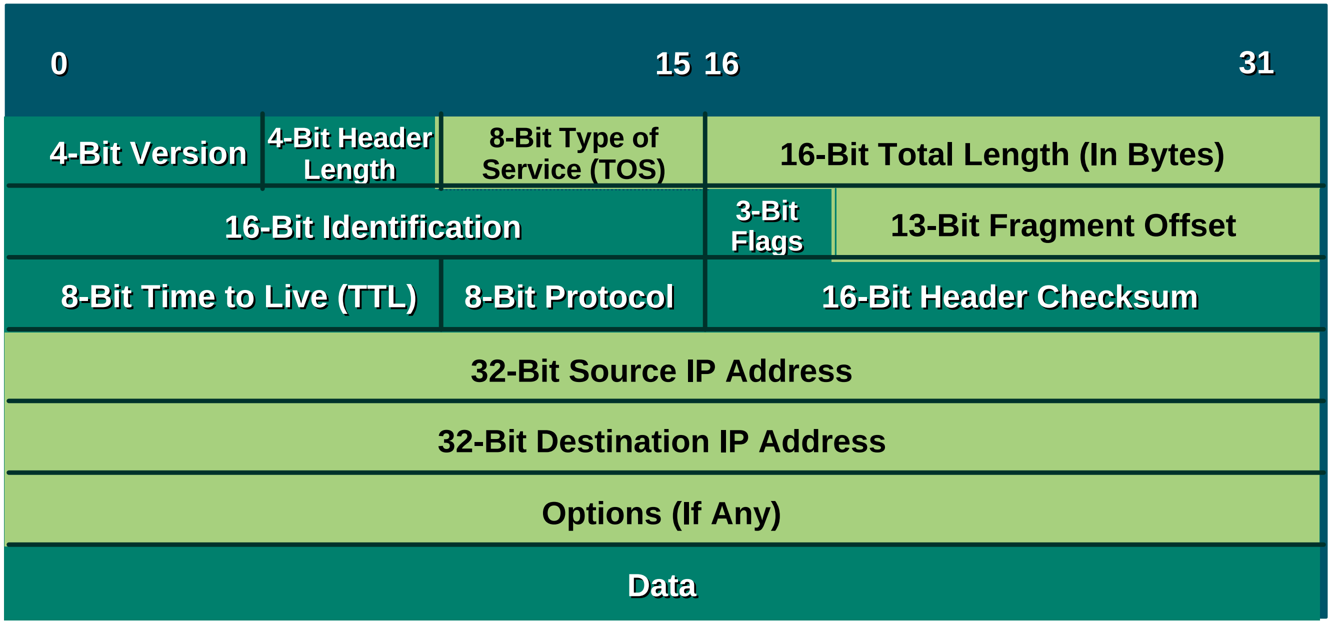


- **Exploit application holes**

  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 Format



0 15 16 31

4-Bit Version | 4-Bit Header Length | 8-Bit Type of Service (TOS) | 16-Bit Total Length (In Bytes)

16-Bit Identification | 3-Bit Flags | 13-Bit Fragment Offset

8-Bit Time to Live (TTL) | 8-Bit Protocol | 16-Bit Header Checksum

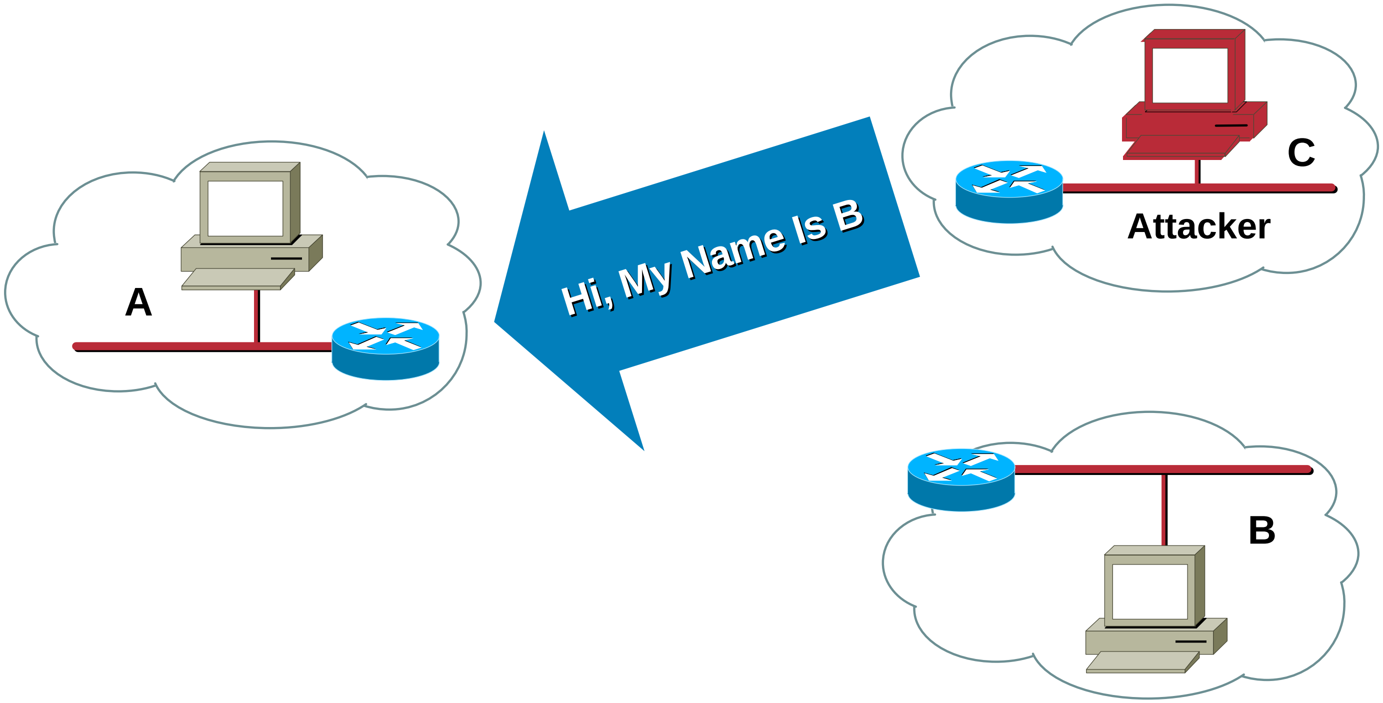
32-Bit Source IP Address

32-Bit Destination IP Address

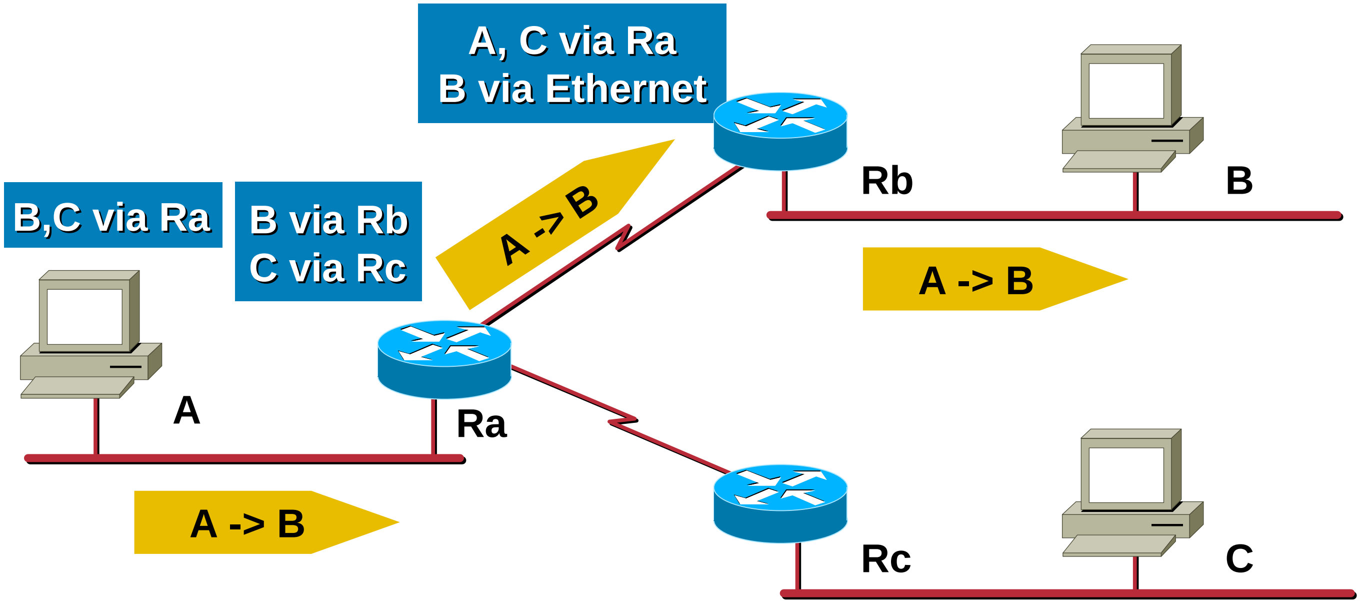
Options (If Any)

Data

IP Spoofing

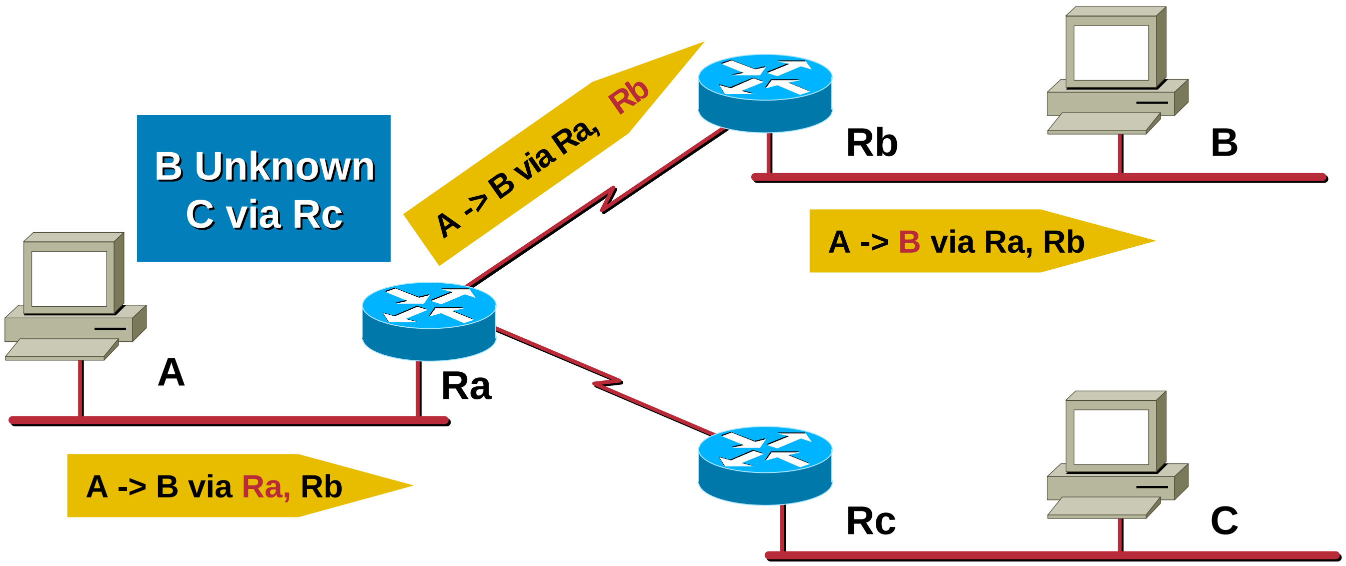


IP: Normal Routing



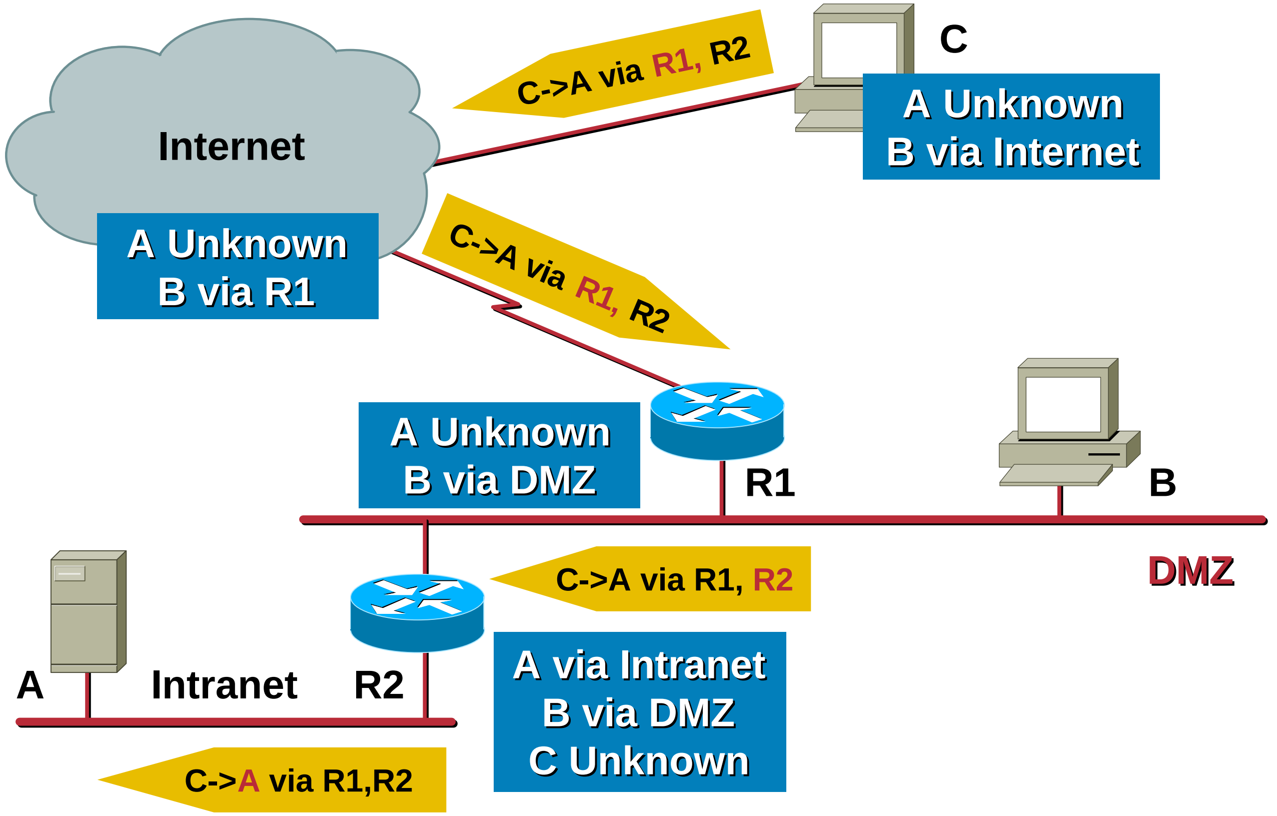
Routing Based on Routing Tables

IP: Source Routing

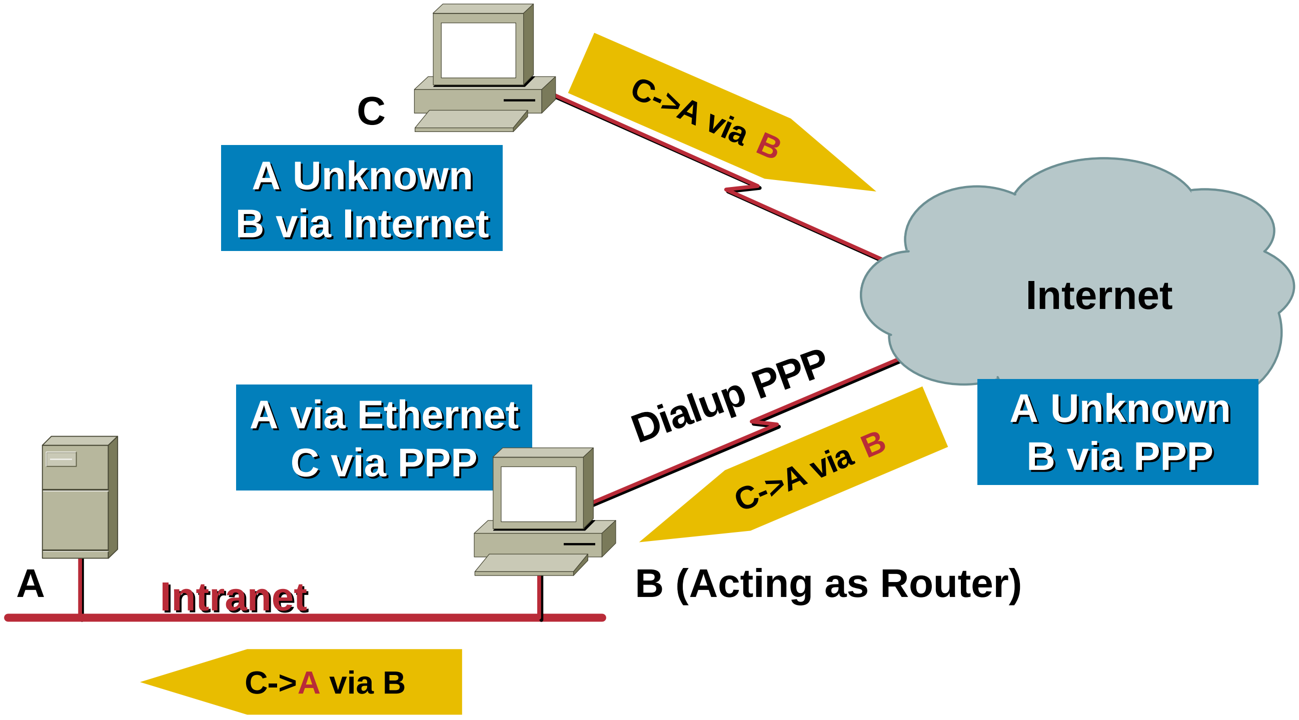


Routing Based on IP Datagram Option

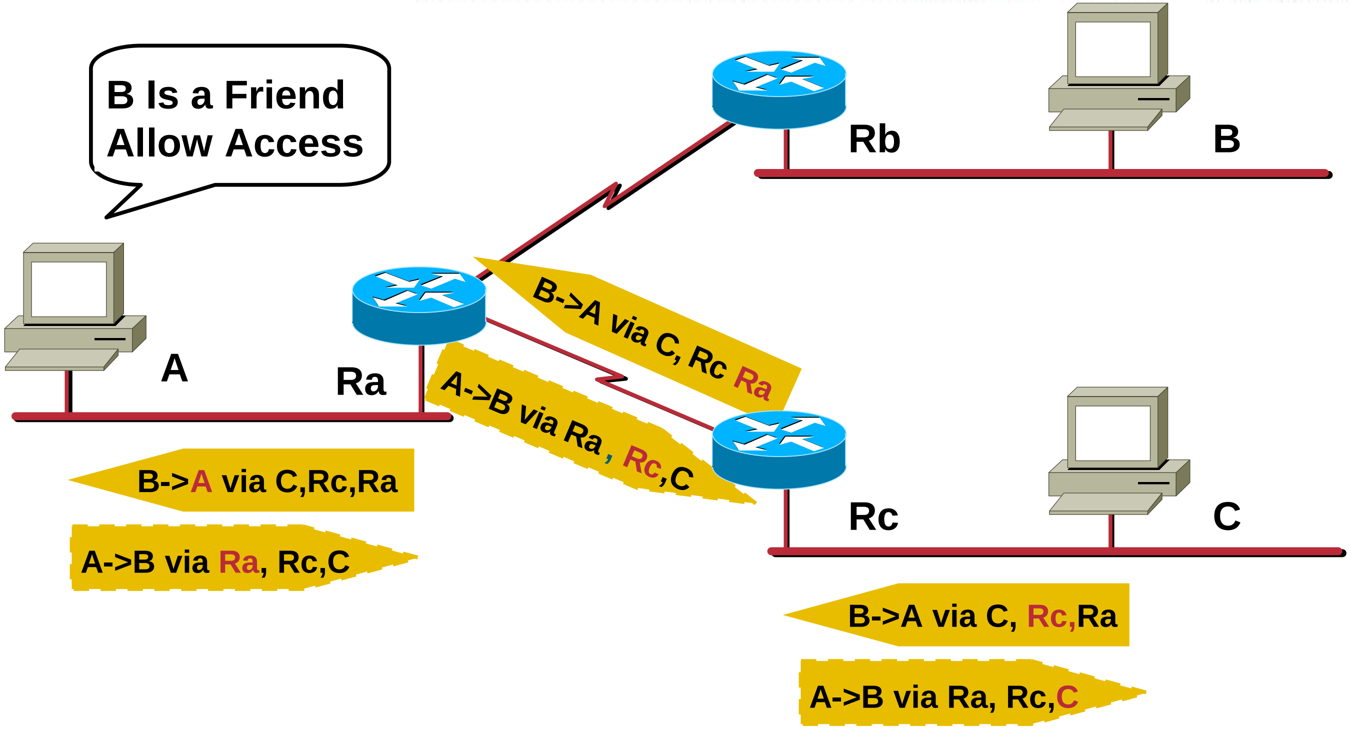
IP Unwanted Routing



IP Unwanted Routing (Cont.)



IP Spoofing Using Source Routing



B Is a Friend
Allow Access

B->A via C,Rc,Ra

A->B via Ra, Rc,C

B->A via C, Rc Ra

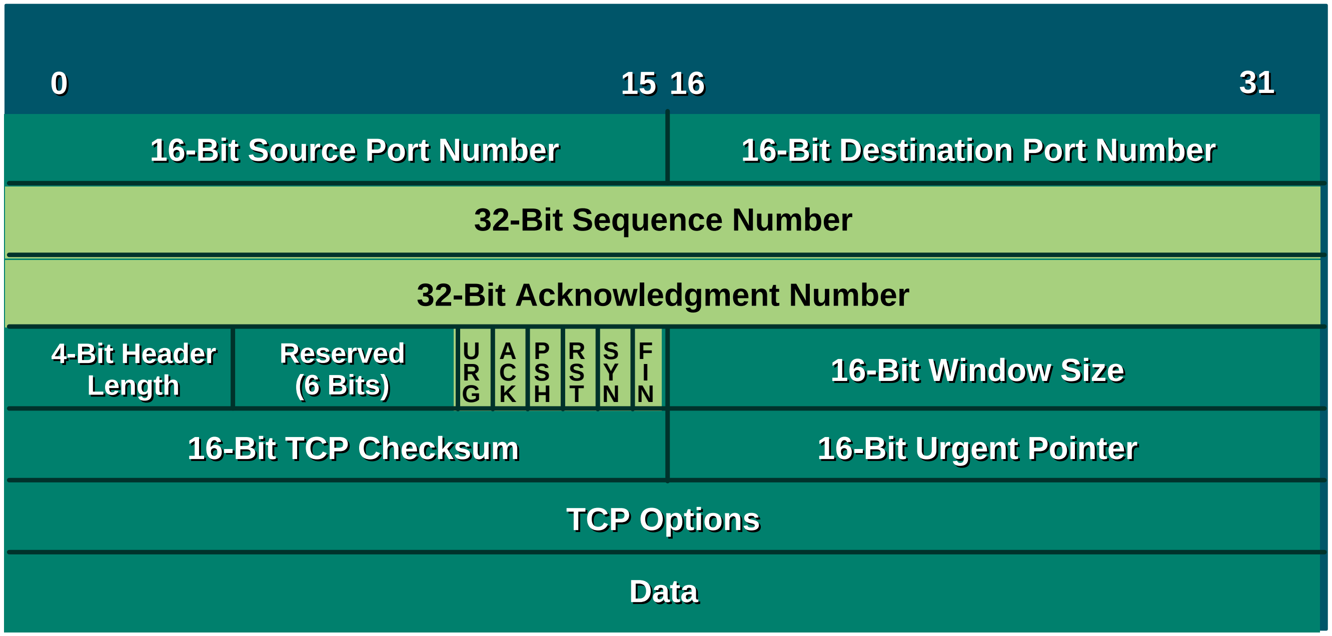
A->B via Ra , Rc,C

B->A via C, Rc,Ra

A->B via Ra, Rc,C

Back Traffic Uses the Same Source Route

TCP Packet Format



0 15 16 31

16-Bit Source Port Number | 16-Bit Destination Port Number

32-Bit Sequence Number

32-Bit Acknowledgment Number

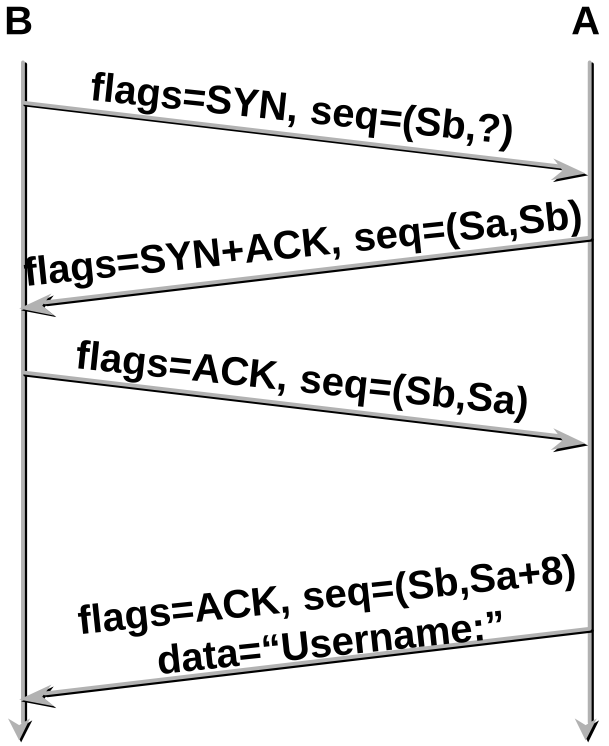
4-Bit Header Length | Reserved (6 Bits) | URG | ACK | PSH | RST | SYN | FIN | 16-Bit Window Size

16-Bit TCP Checksum | 16-Bit Urgent Pointer

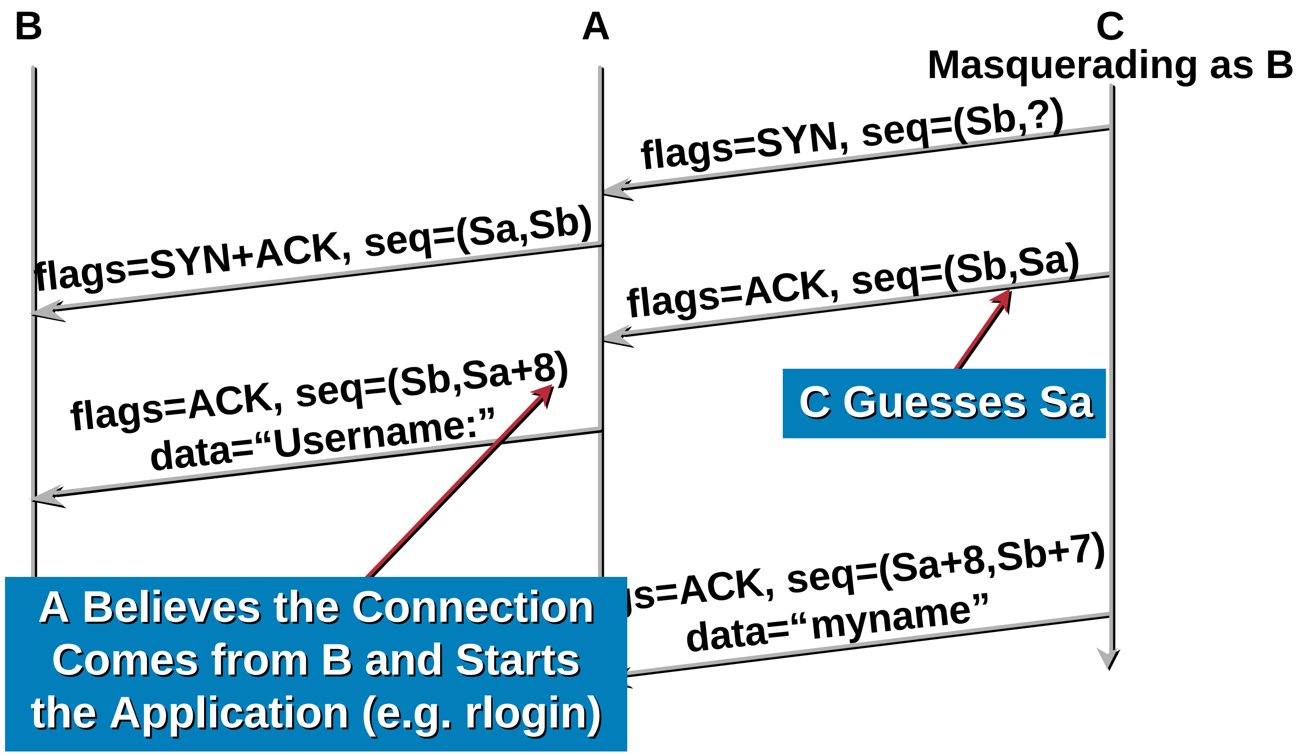
TCP Options

Data

TCP Connection Establishment



TCP Blind Spoofing



B

A

C

Masquerading as B

flags=SYN, seq=(Sb,?)

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

flags=ACK, seq=(Sb,Sa)

C Guesses Sa

flags=ACK, seq=(Sb,Sa+8)
data="Username:"

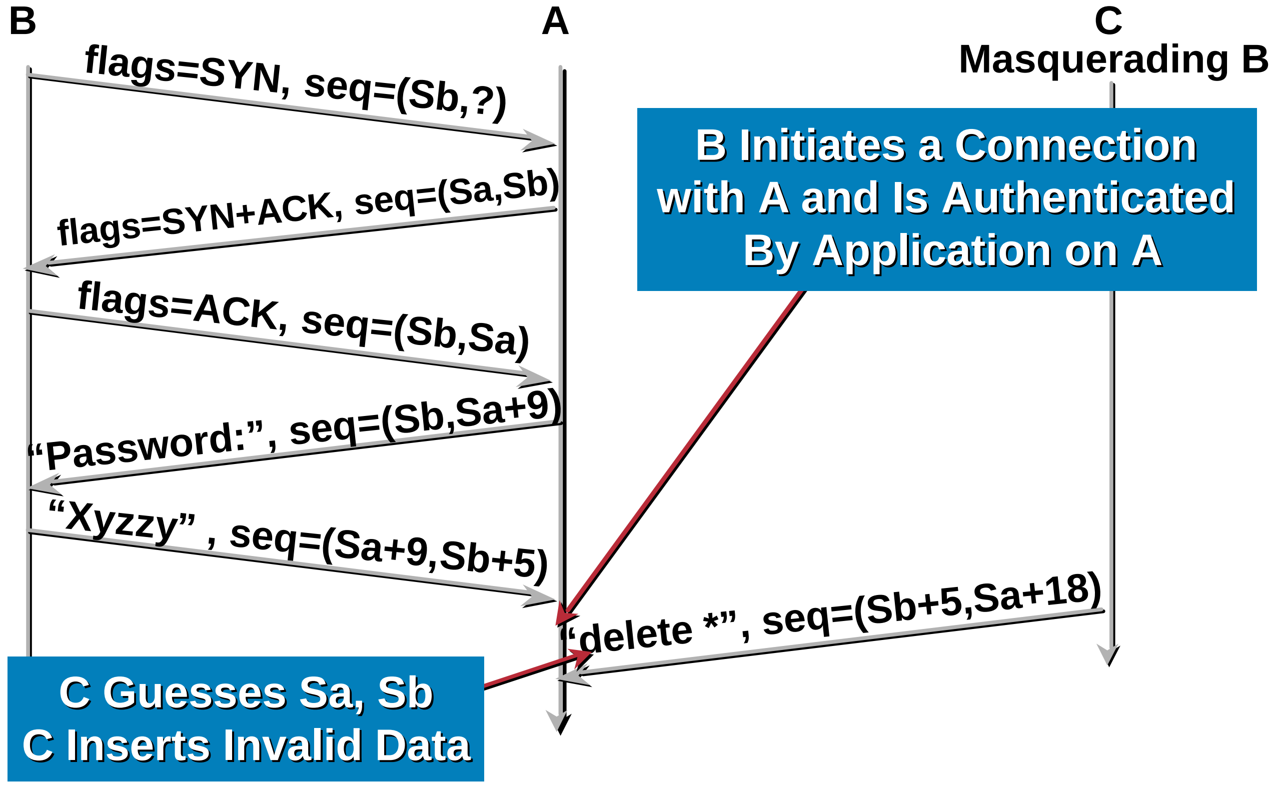
s=ACK, seq=(Sa+8,Sb+7)
data="myname"

A Believes the Connection Comes from B and Starts the Application (e.g. rlogin)

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

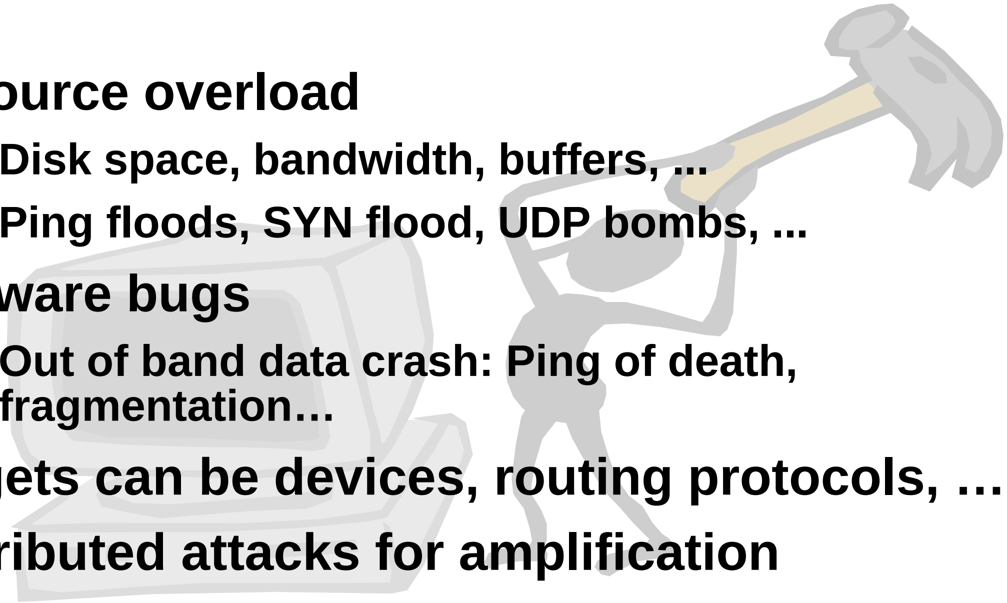
TCP Session Hijacking


B
A
C
Masquerading B
flags=SYN, seq=(Sb,?)
flags=SYN+ACK, seq=(Sa,Sb)
flags=ACK, seq=(Sb,Sa)
"Password:", seq=(Sb,Sa+9)
"Xyzzy" , seq=(Sa+9,Sb+5)
"delete *", seq=(Sb+5,Sa+18)

B Initiates a Connection with A and Is Authenticated By Application on A

C Guesses Sa, Sb
C Inserts Invalid Data

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…
- Targets can be devices, routing protocols, …
- Distributed attacks for amplification

Normal Spanning Tree

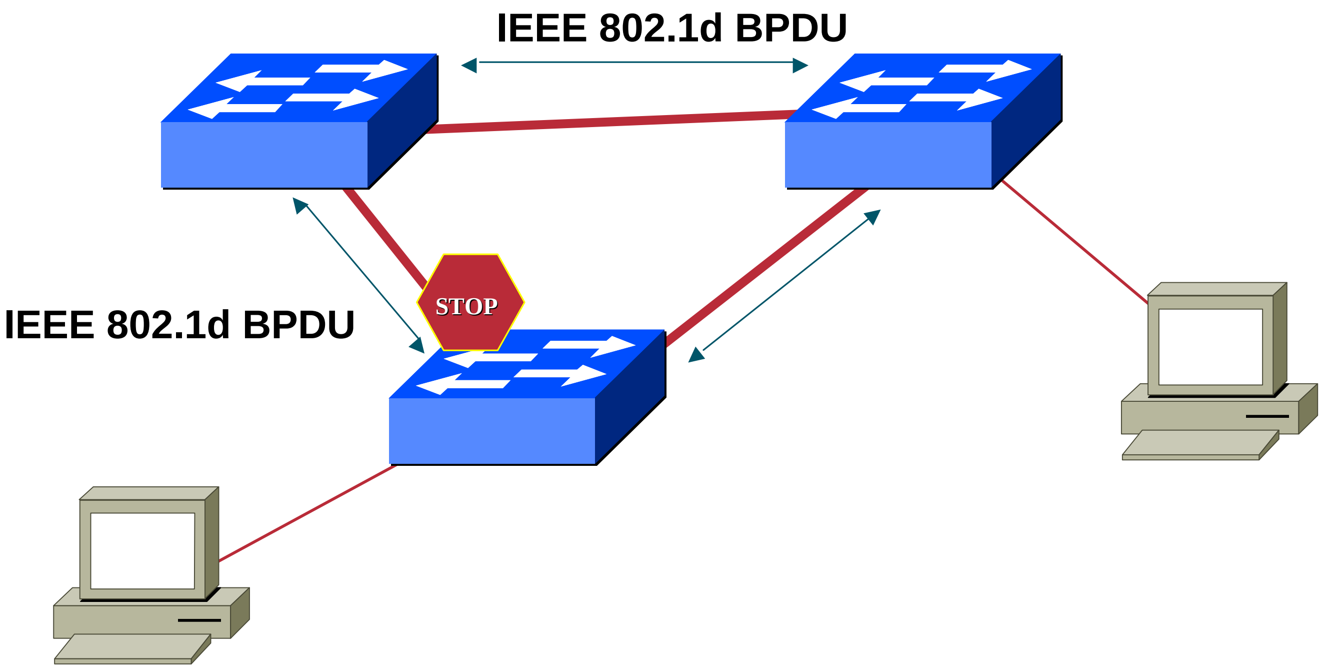
- IEEE 802.1d Spanning Tree is used to prevent loops
- BPDU are sent to:

  elect the root switch (based on priority and MAC address) at start-up and on topology changes

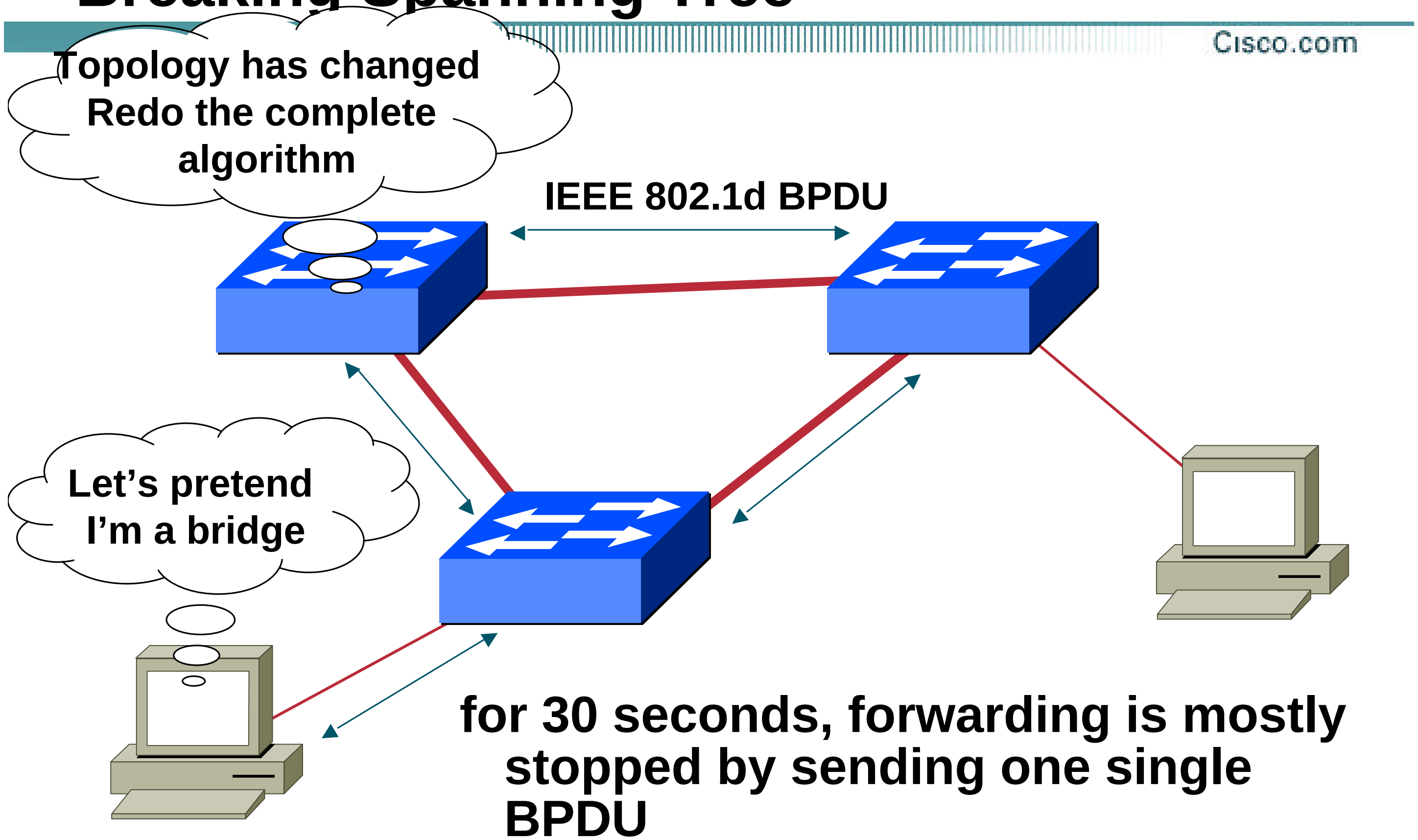
  dynamically block frame forwarding on some switches to prevent loops

- the protocol is not authenticated
- convergence is real slow: ~30 seconds

Spanning Tree in Action



Breaking Spanning Tree



Topology has changed
Redo the complete algorithm

IEEE 802.1d BPDU

Let’s pretend I’m a bridge

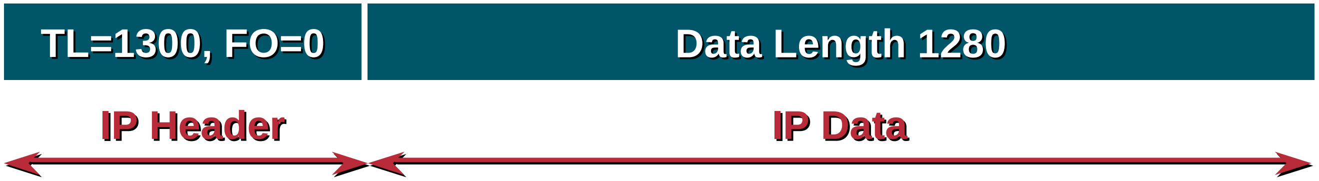
for 30 seconds, forwarding is mostly stopped by sending one single BPDU

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:

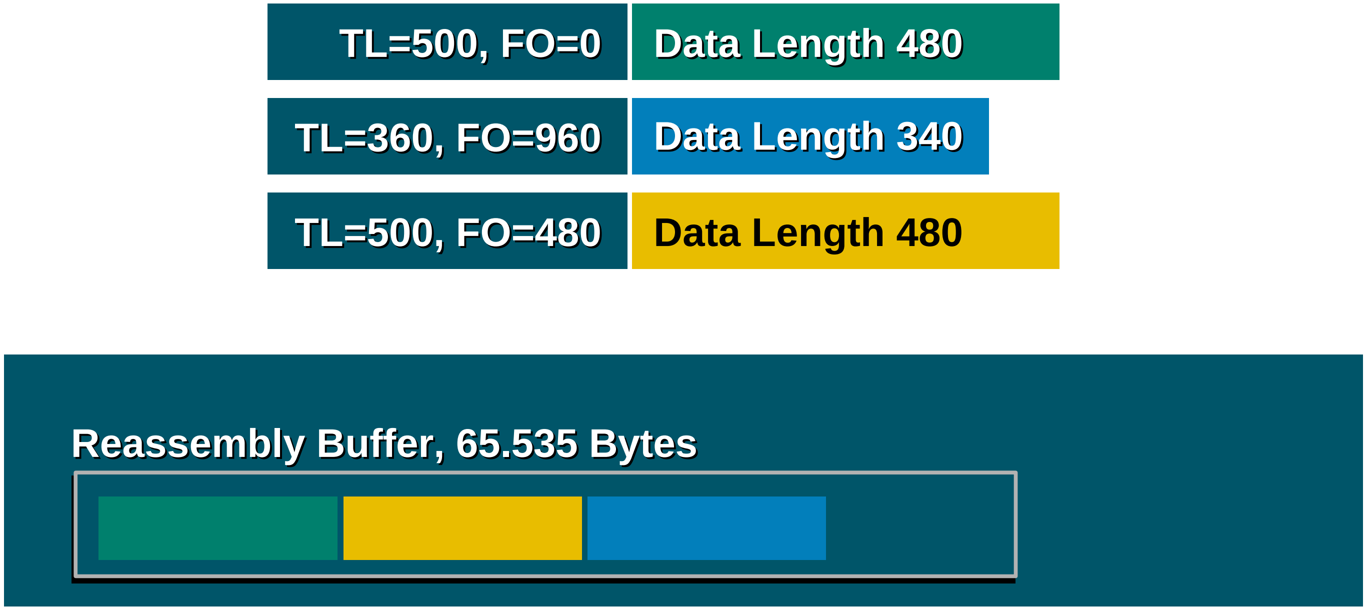


After Fragmentation (MTU = 500):

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

Reassembly Buffer, 65.535 Bytes

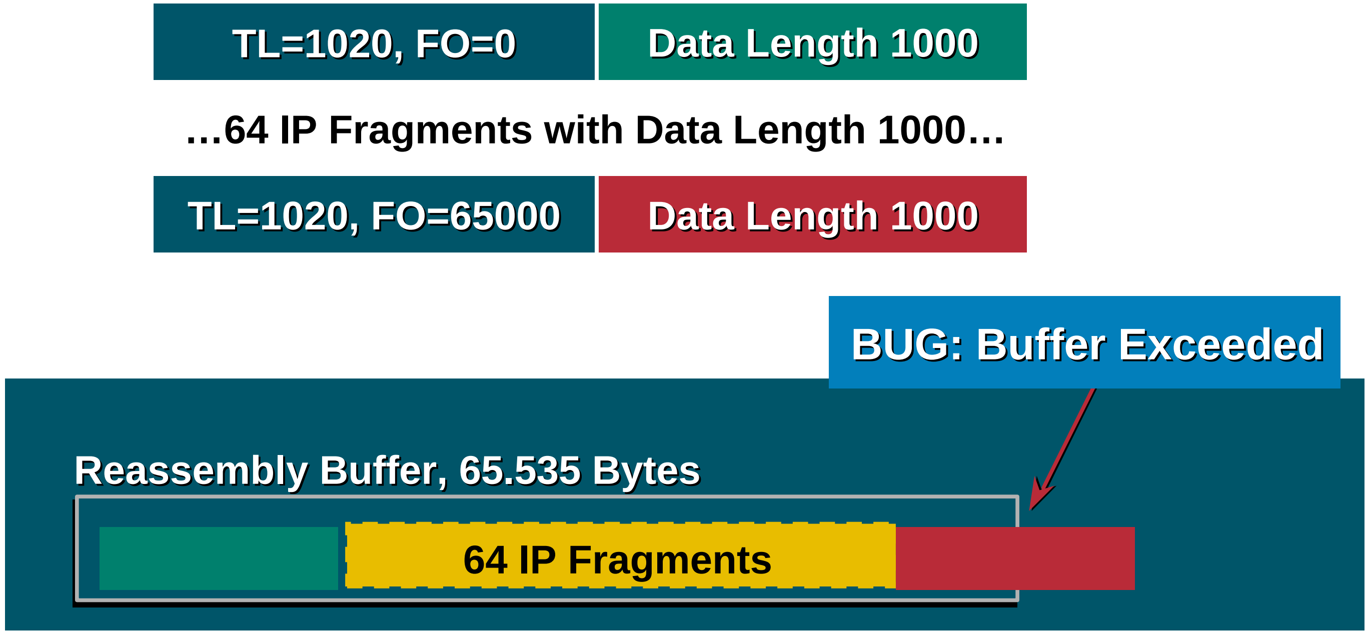
Kernel Memory at Destination Host

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

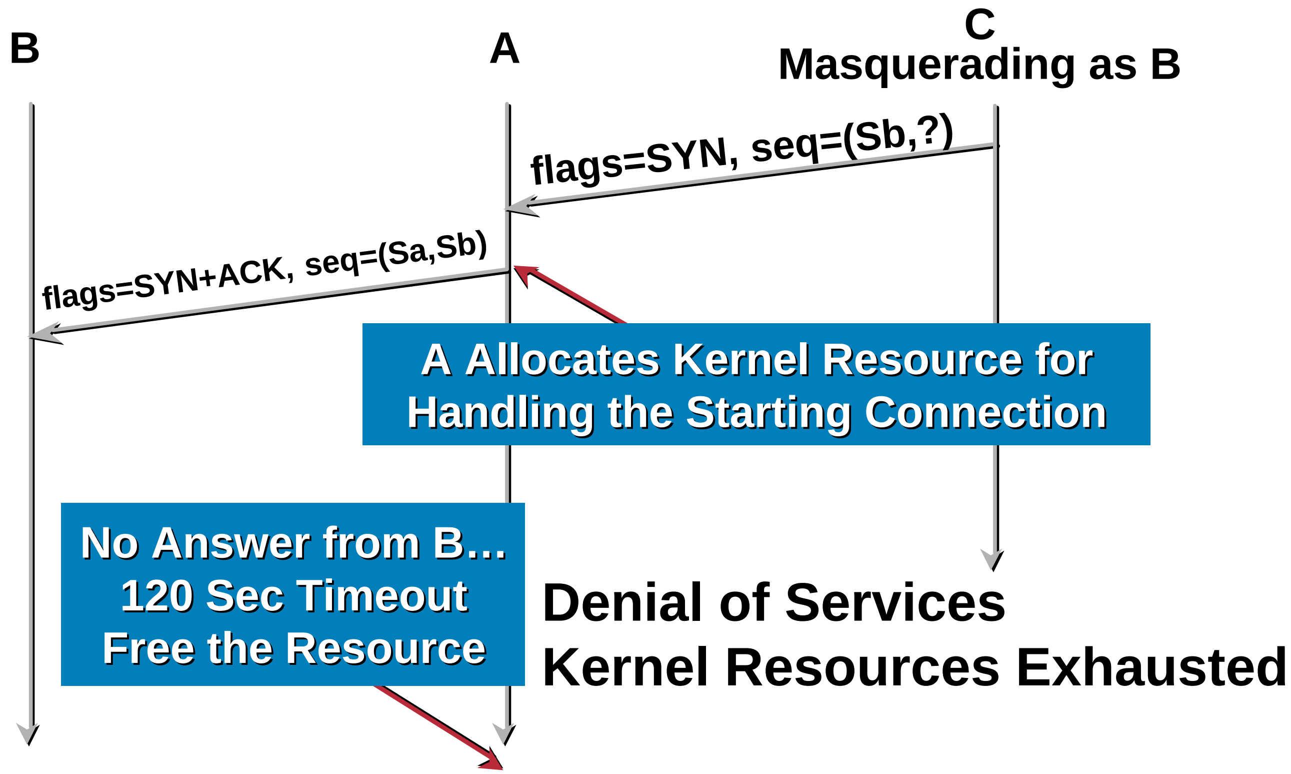
BUG: Buffer Exceeded

Reassembly Buffer, 65.535 Bytes

64 IP Fragments

Kernel Memory at Destination Host

SYN Attack

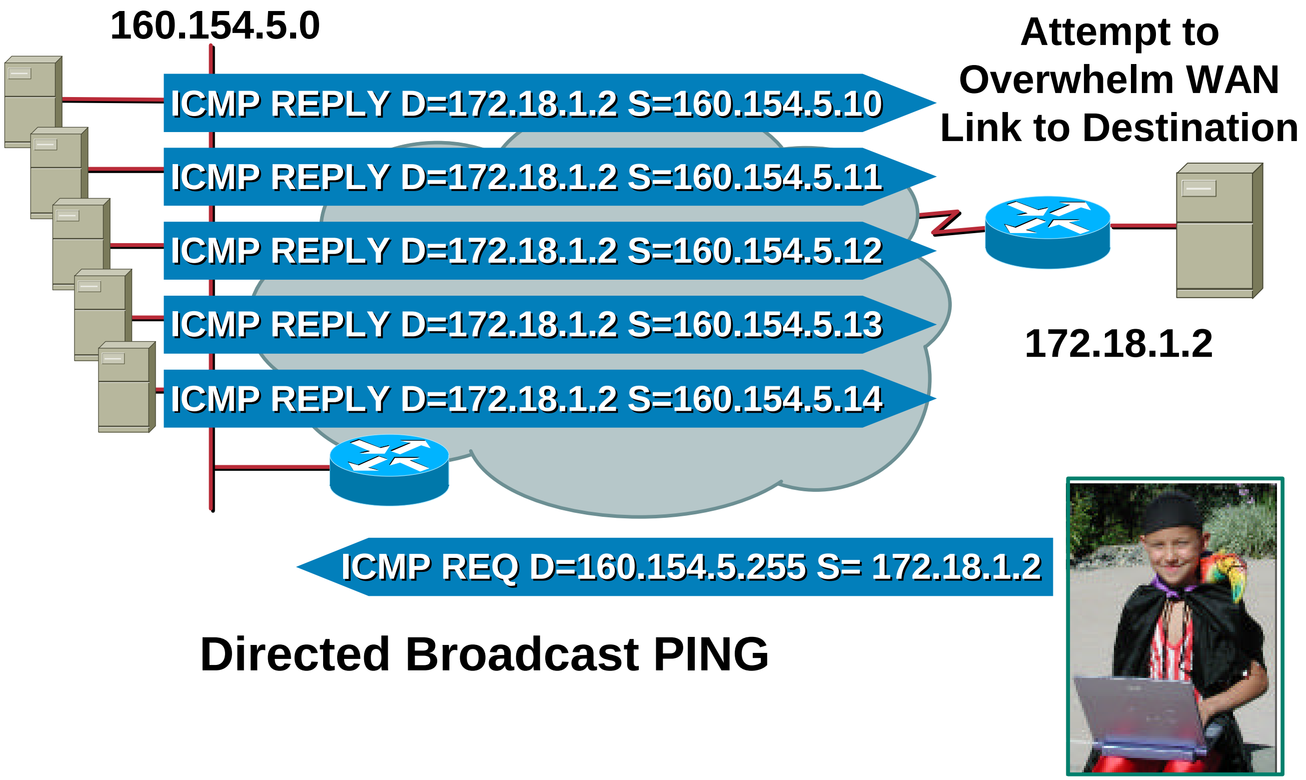


A Allocates Kernel Resource for Handling the Starting Connection

No Answer from B…
120 Sec Timeout
Free the Resource

Denial of Services
Kernel Resources Exhausted

SMURF Attack



160.154.5.0

ICMP REPLY D=172.18.1.2 S=160.154.5.10

ICMP REPLY D=172.18.1.2 S=160.154.5.11

ICMP REPLY D=172.18.1.2 S=160.154.5.12

ICMP REPLY D=172.18.1.2 S=160.154.5.13

ICMP REPLY D=172.18.1.2 S=160.154.5.14

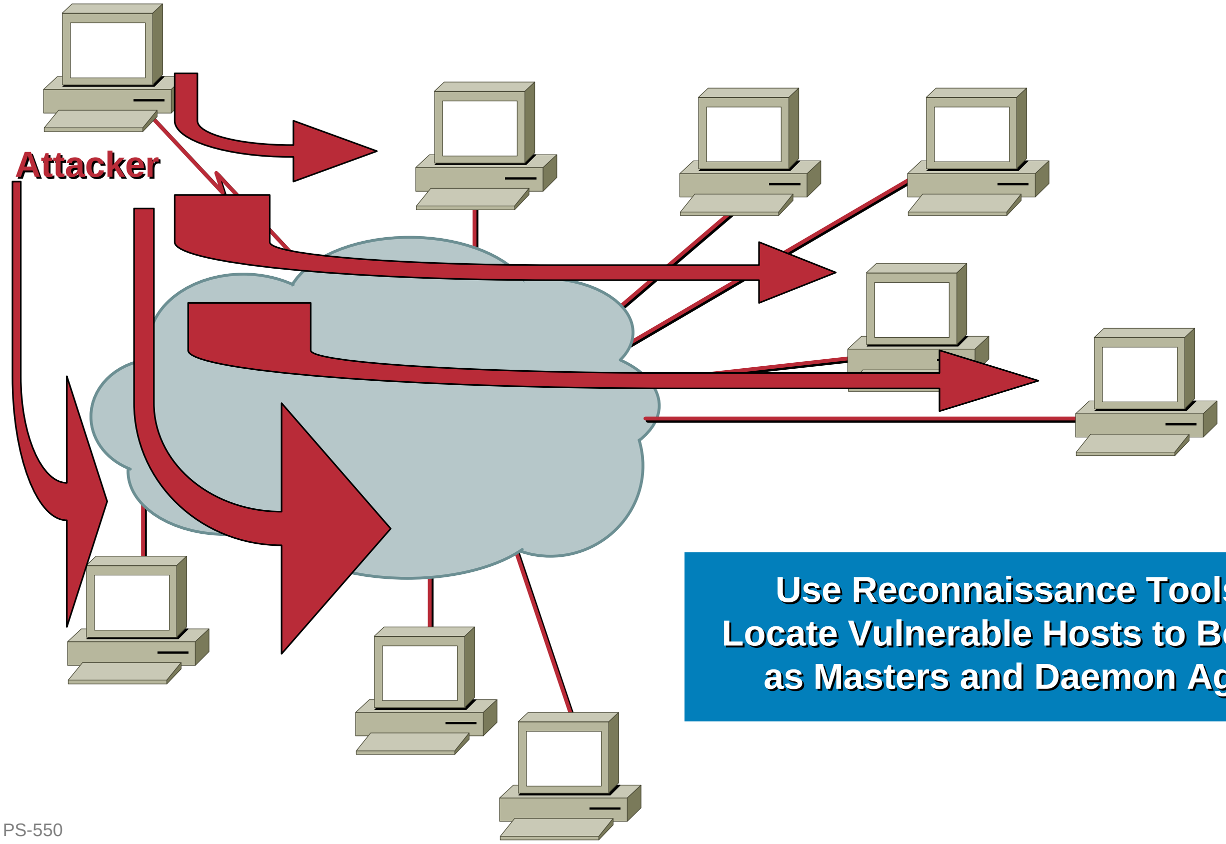
Attempt to
Overwhelm WAN
Link to Destination

172.18.1.2

ICMP REQ D=160.154.5.255 S= 172.18.1.2

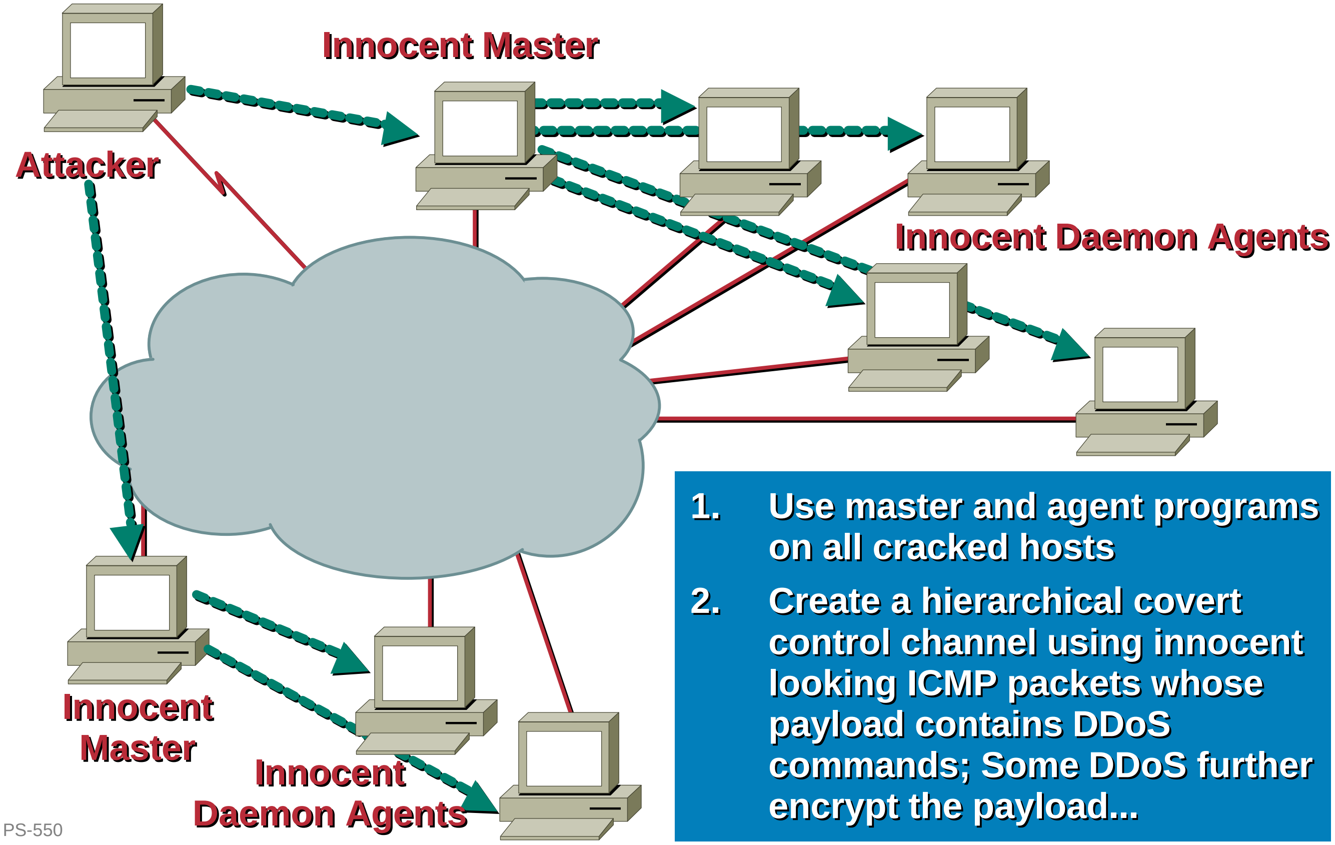
Directed Broadcast PING

DDoS Step 1: Find Vulnerable Hosts



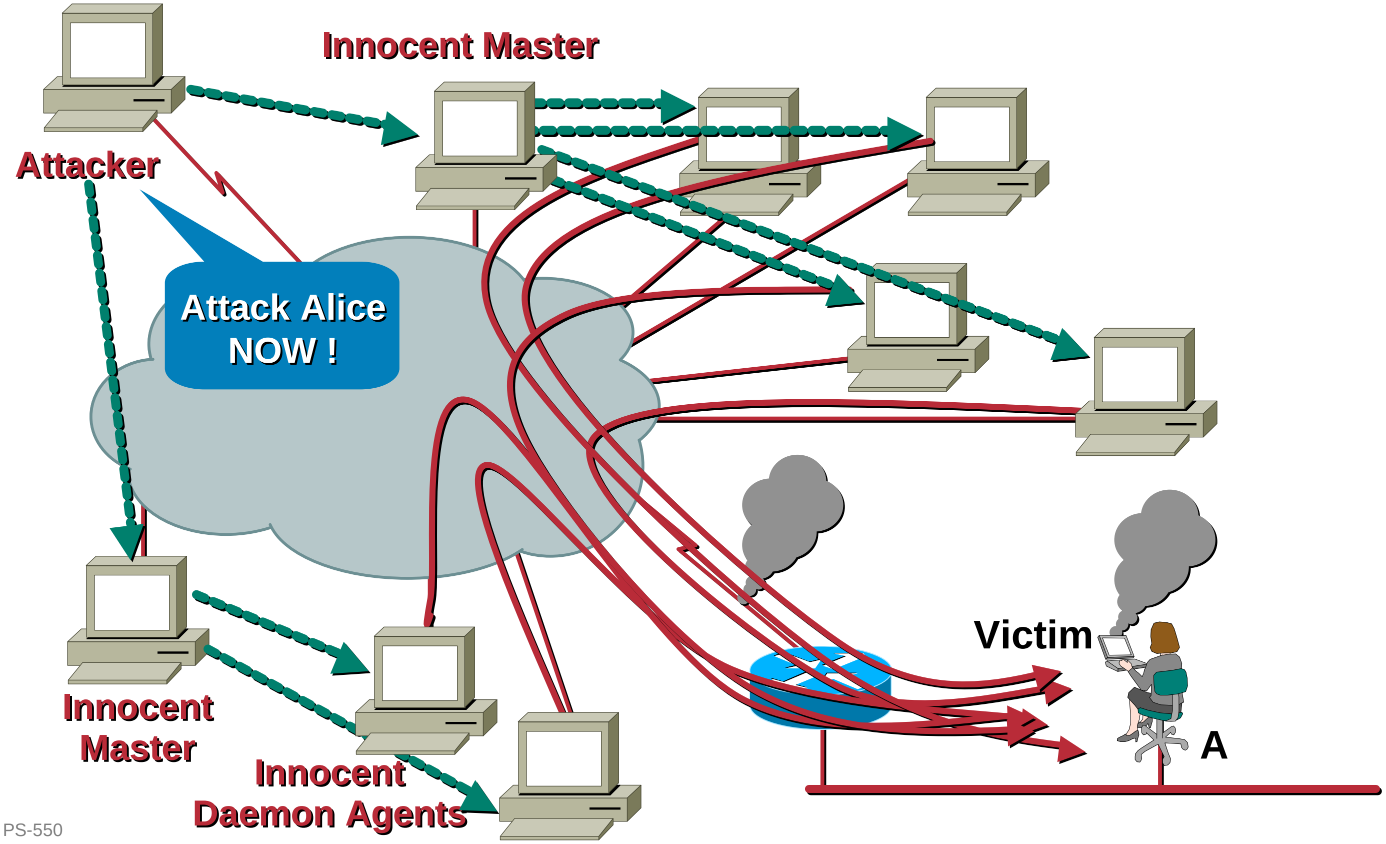
Use Reconnaissance Tools to Locate Vulnerable Hosts to Be Used as Masters and Daemon Agents

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



Underlying Causes for Vulnerability

- Poor administration
- Poor configurations and designs
- Poor authentication
- Poor data protection
- Poor design management
- Poor incident detection and response

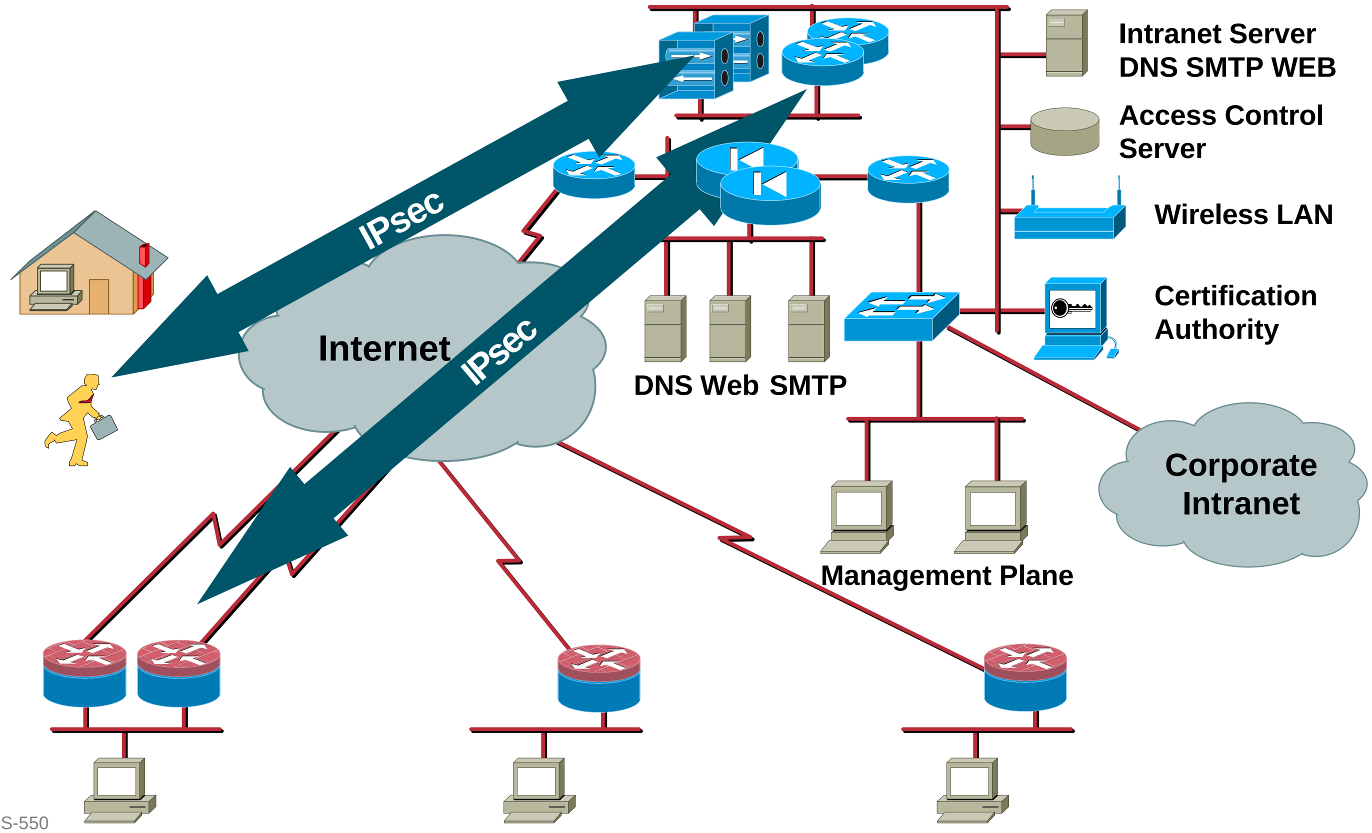
More Causes

- **Misunderstanding attack origin or mechanism**

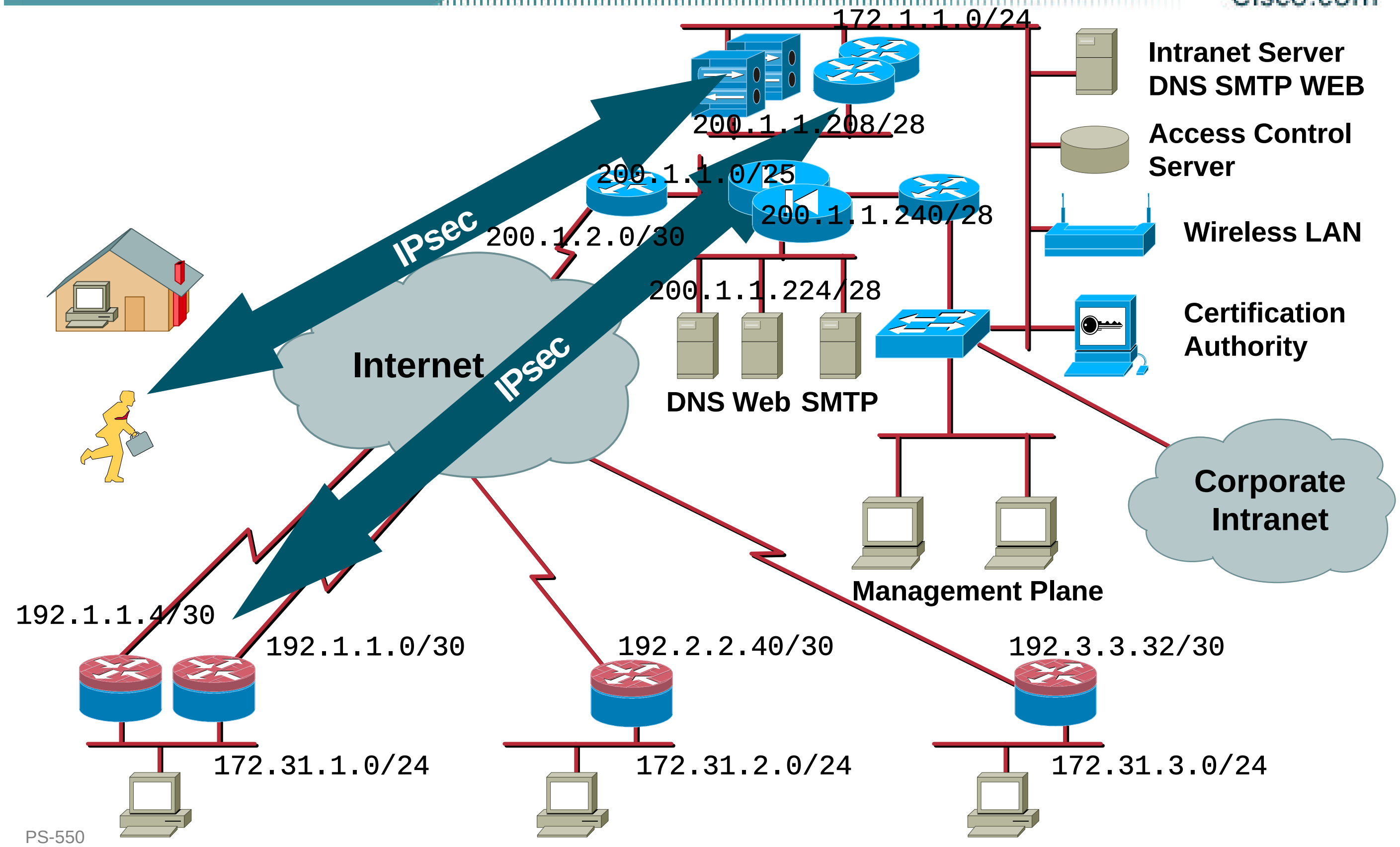
  Apply wrong countermeasure

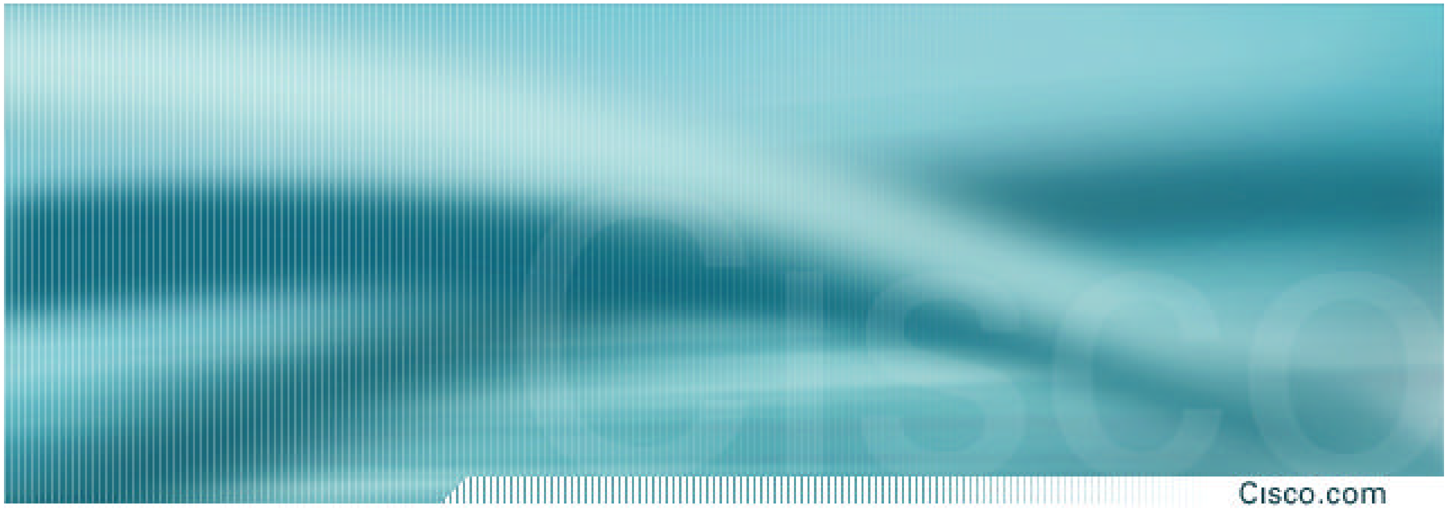
  Apply countermeasure at the wrong place

Introduction to the Target Topology



Address Space





Securing the Devices

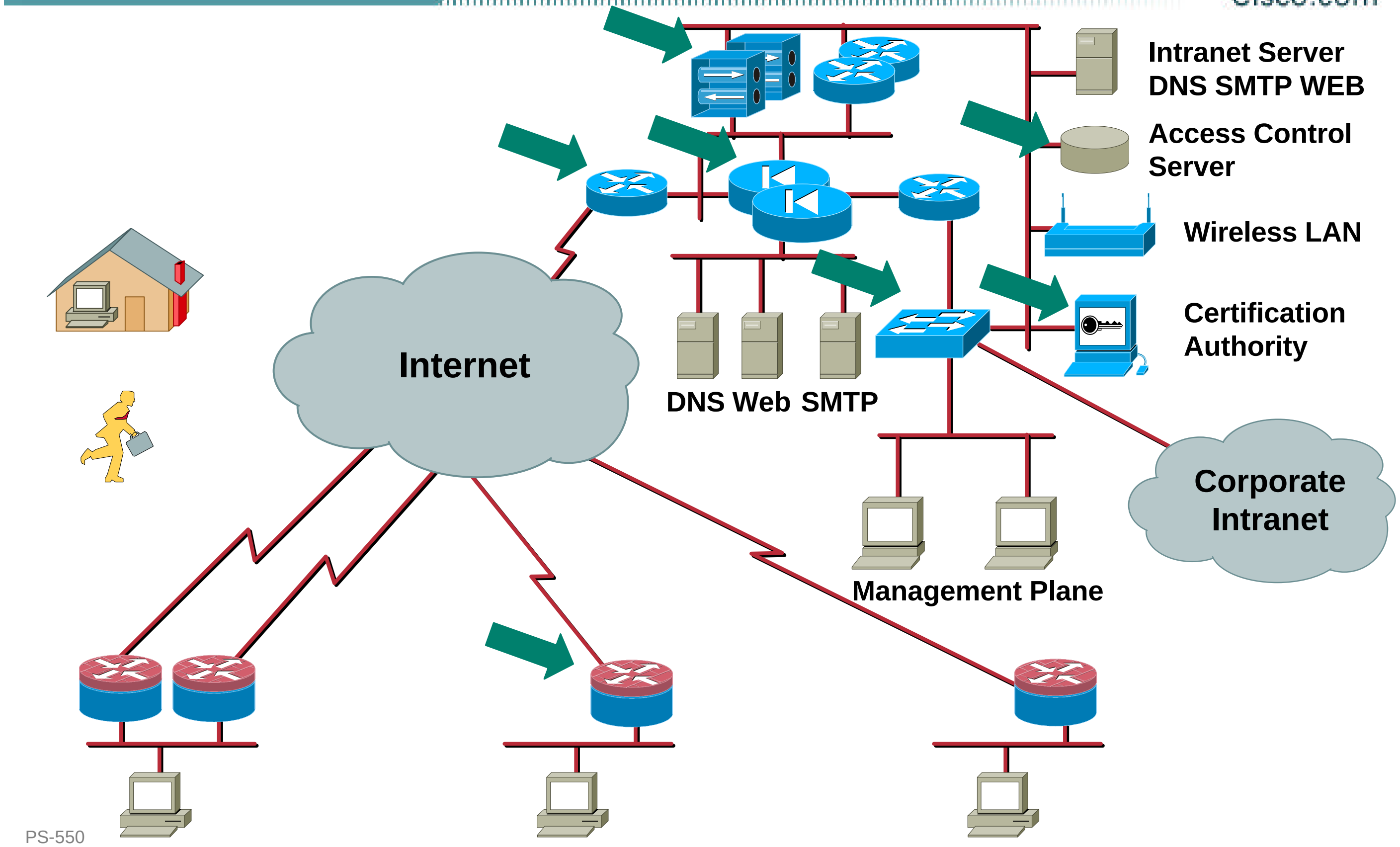
Requirements

- All devices must be up to date with security patches
- All users must be authenticated
- Only required services should be available on devices
- Network connections for administrative purposes should be accepted only from the management subnet
- Detect and handle security incidents

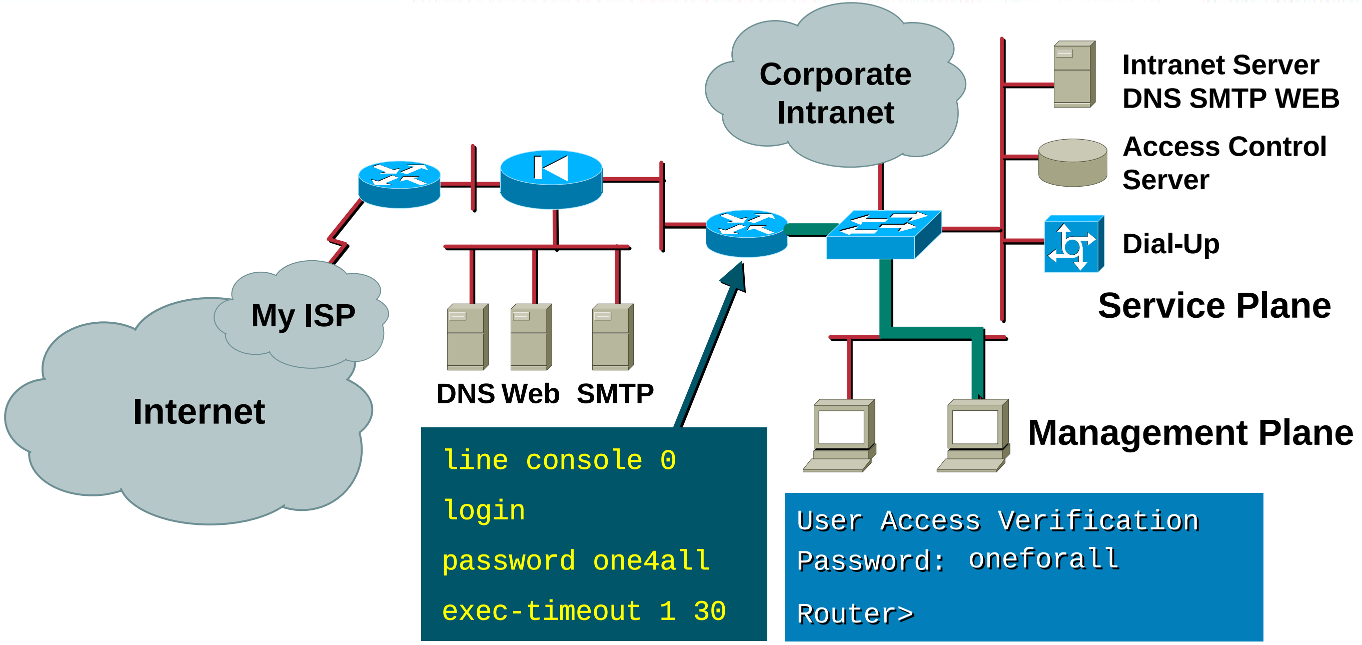
Tool Kit

- Monitor bugtraq and other security information sources
- Configure authentication and authentication server
- Remove unnecessary services and features
- Restrict access to the administrative interface
- Configure time
- Use logging, intrusion detection, and auditing

Devices To Be Protected



Local Passwords

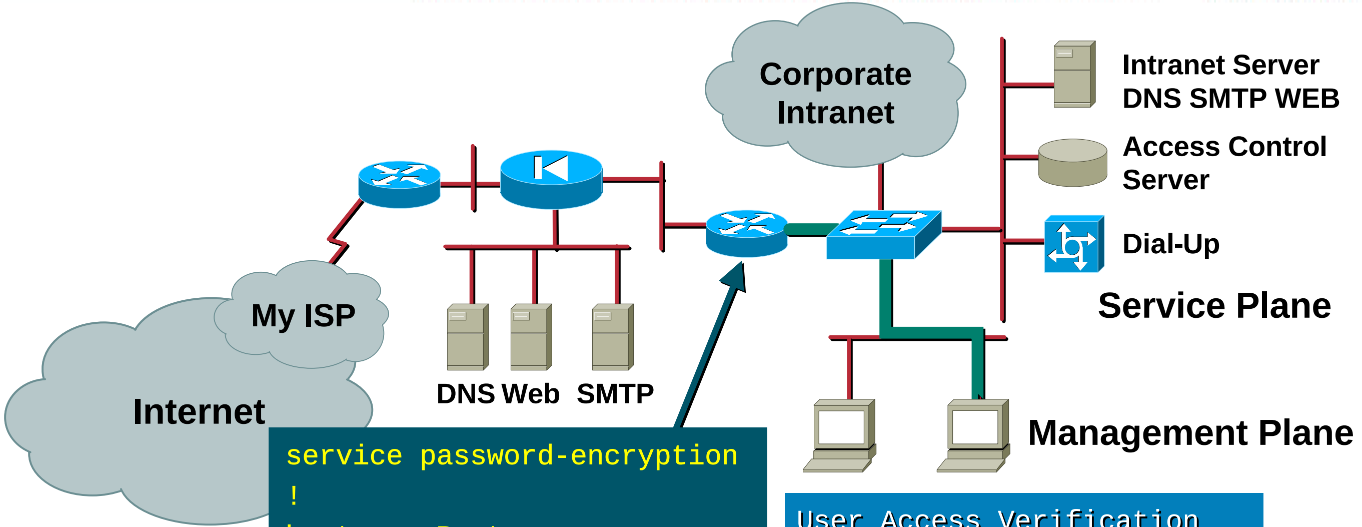


```
line console 0
login
password one4all
exec-timeout 1 30
```

```
User Access Verification
Password: oneforall
Router>
```

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

Service Password Encryption

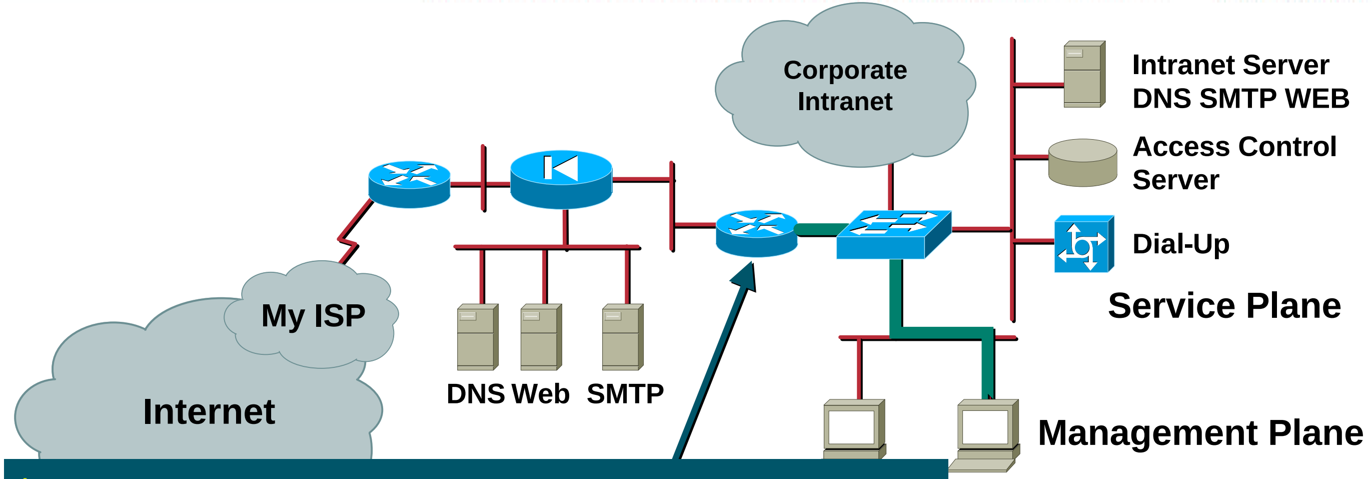


```
service password-encryption
!
hostname Router
!
enable password 7 15181E020F
```

```
User Access Verification
Password:  oneforall

Router>
```

- Encrypts password in configuration
- Easily reversible

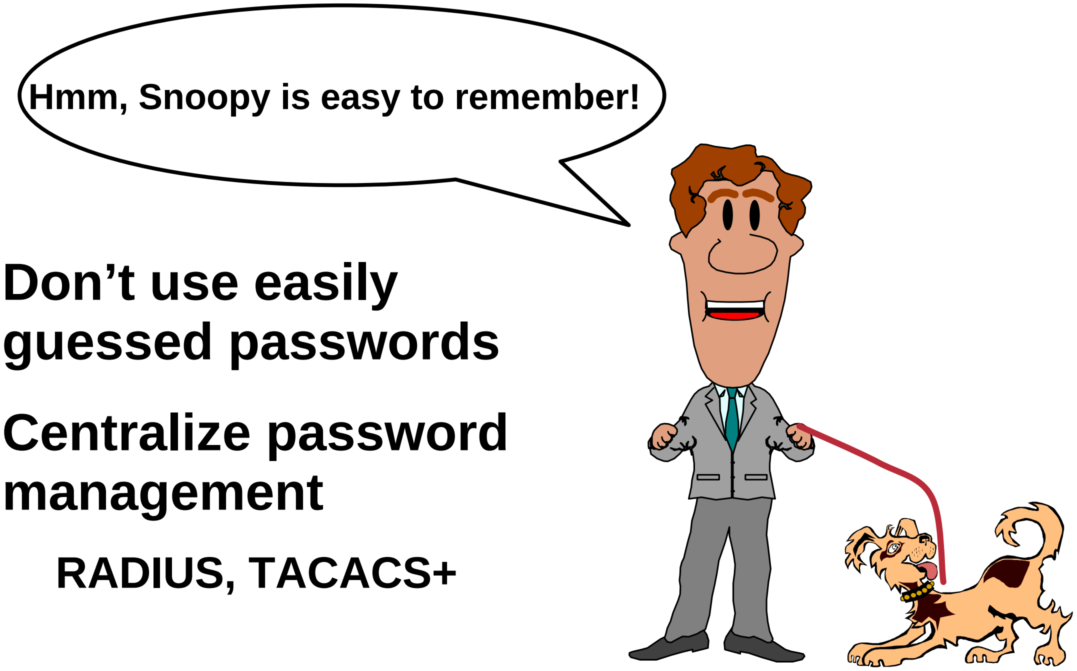
Enable Secret



```
!
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

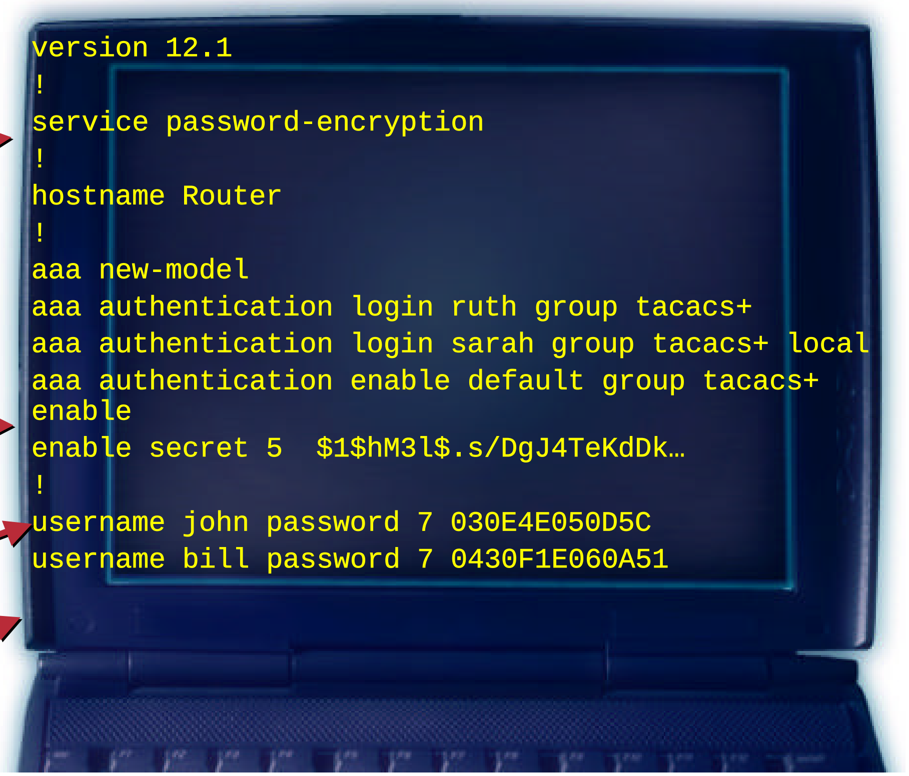
Encrypts Passwords with Encryption (7)

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

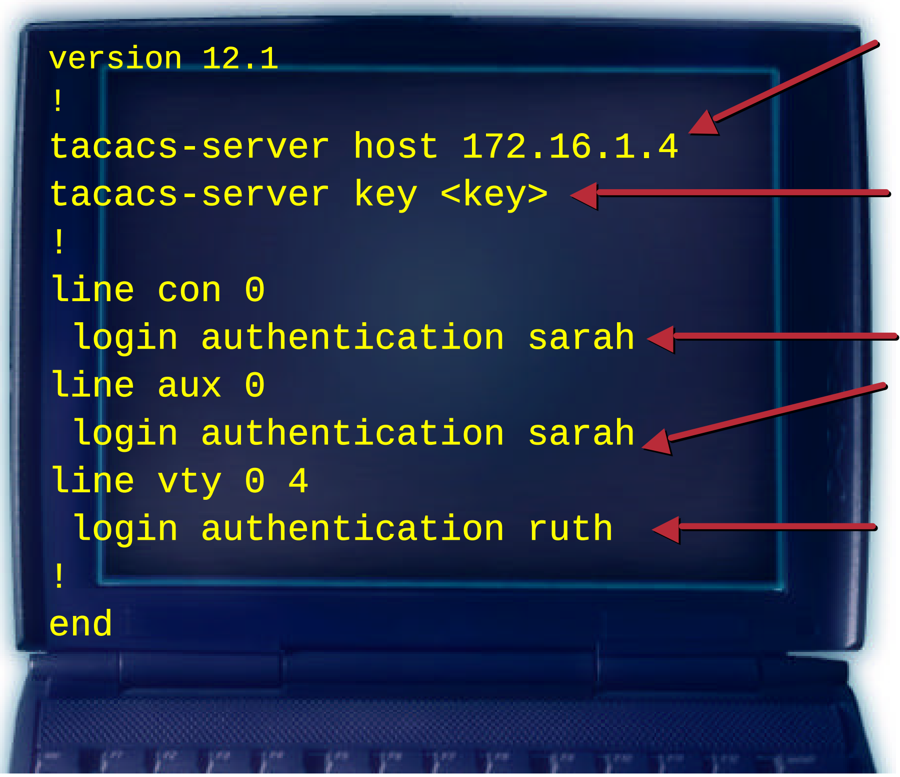
Define Local Users



```
version 12.1
!
service password-encryption
!
hostname Router
!
aaa new-model
aaa authentication login ruth group tacacs+
aaa authentication login sarah group tacacs+ local
aaa authentication enable default group tacacs+
enable
enable secret 5  $1$hM3l$.s/DgJ4TeKdDk…
!
username john password 7 030E4E050D5C
username bill password 7 0430F1E060A51
```

Cisco IOS TACACS+ Login Authentication

Cisco.com



```
version 12.1
!
tacacs-server host 172.16.1.4
tacacs-server key <key>
!
line con 0
 login authentication sarah
line aux 0
 login authentication sarah
line vty 0 4
 login authentication ruth
!
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

Cisco.com

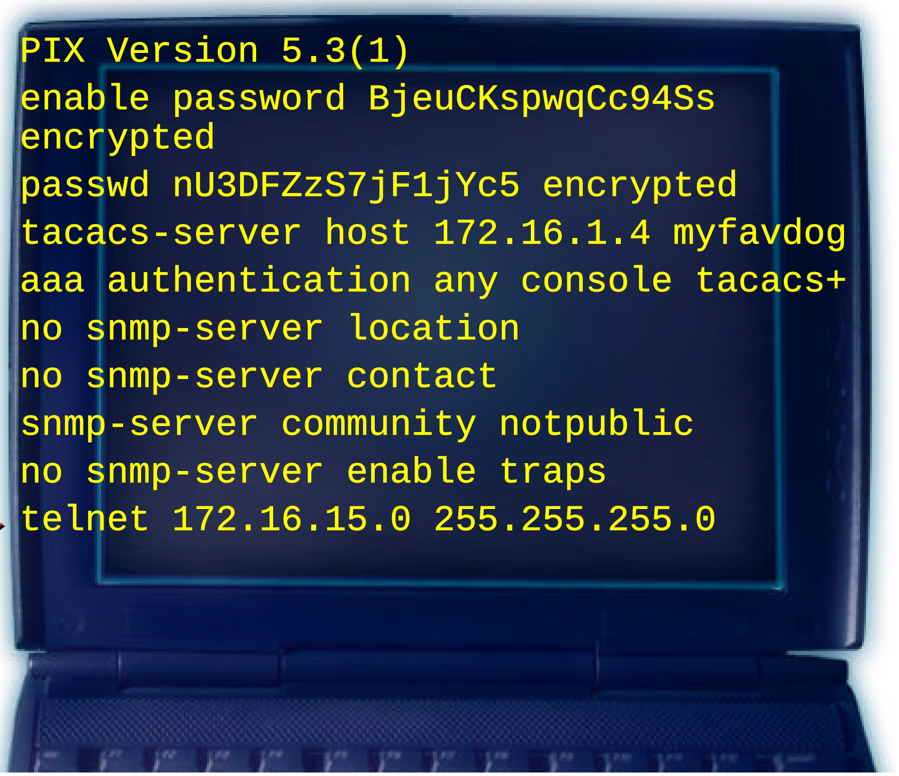
Enable Password

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



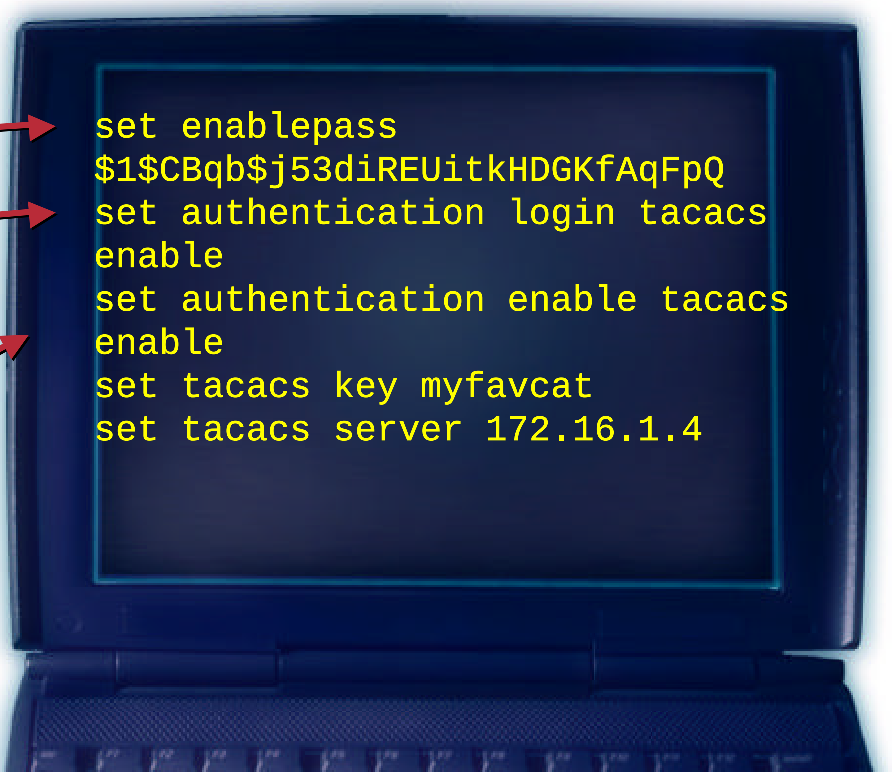
```
PIX Version 5.3(1)
enable password BjeuCKspwqCc94Ss
encrypted
passwd nU3DFZzS7jF1jYc5 encrypted
tacacs-server host 172.16.1.4 myfavdog
aaa authentication any console tacacs+
no snmp-server location
no snmp-server contact
snmp-server community notpublic
no snmp-server enable traps
telnet 172.16.15.0 255.255.255.0
```

Catalyst TACACS+ Login Authentication

Enable Password

Use TACACS+ for Telnet or Console (Enable) Access

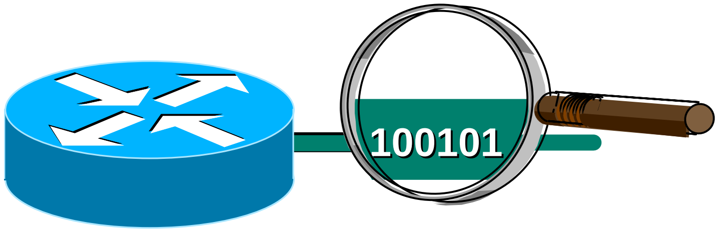
Define TACACS+ Server and Encryption Key



```
set enablepass
$1$CBqb$j53diREUitkHDGKfAqFpQ
set authentication login tacacs
enable
set authentication enable tacacs
enable
set tacacs key myfavcat
set tacacs server 172.16.1.4
```

PassWord of Caution

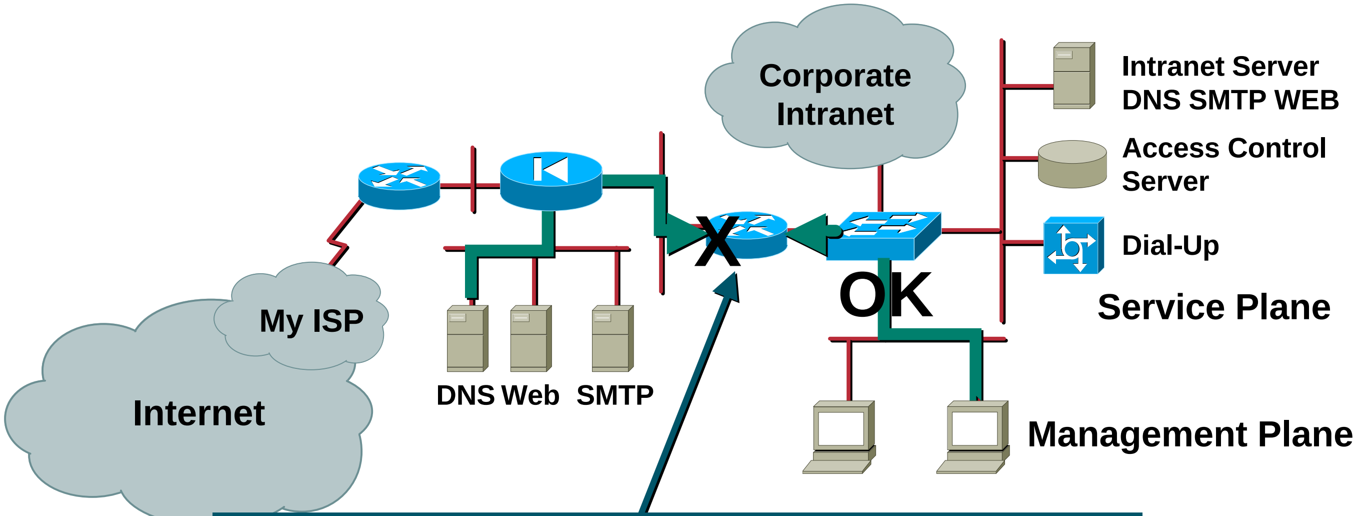
- Even passwords that are encrypted in the configuration are not encrypted on the wire as an administrator logs into the router



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 Cisco Secure ACS**
- **Support for security dynamics and secure computing token servers in Cisco Secure ACS**

Restrict Telnet



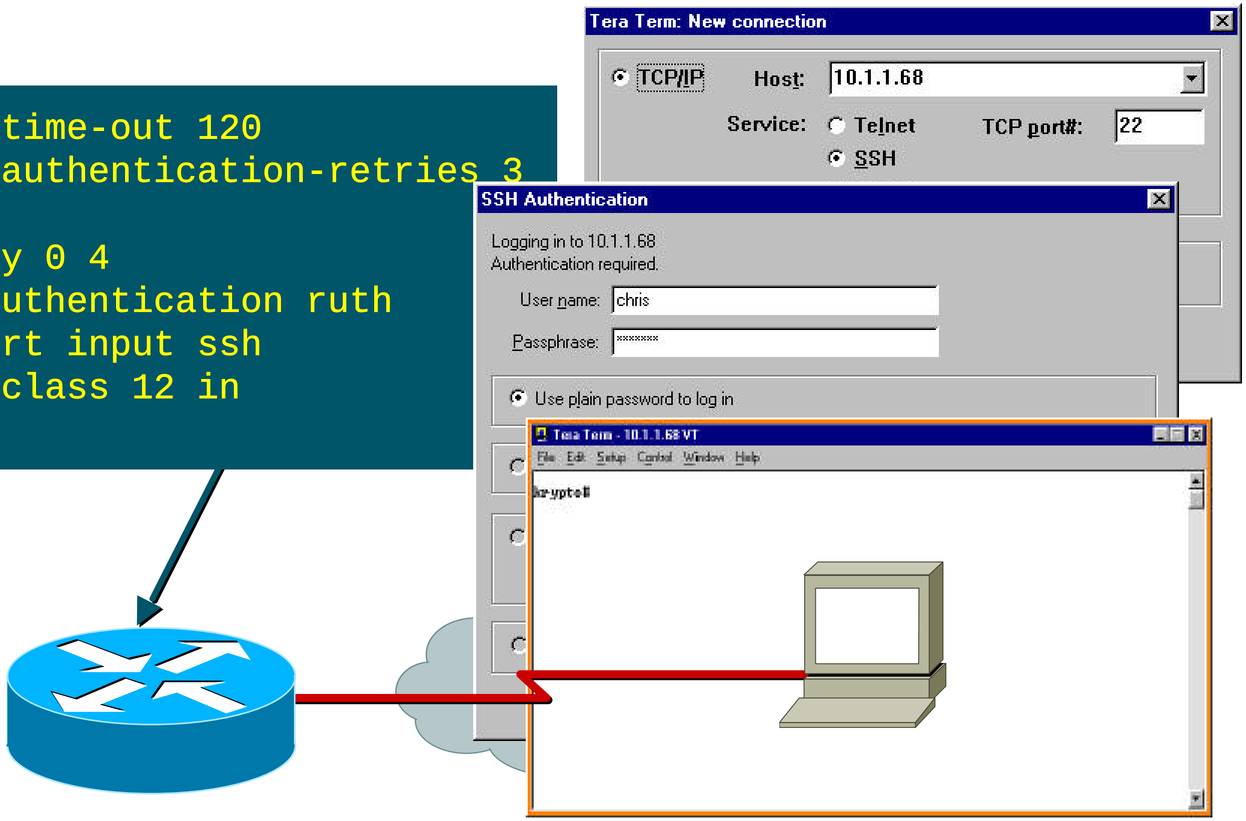
```
access-list 12 permit 172.16.2.0 0.0.0.255
line vty 0 4
access-class 12 in
```

SSH

- Replaces telnet for a protected command and control communication channel
- Strong Authentication provided by RSA key storage and comparison.
- Privacy and integrity provided through the use of strong cryptographic algorithms.

Cisco IOS SSH Configuration

```
ip ssh time-out 120
ip ssh authentication-retries 3
!
line vty 0 4
login authentication ruth
transport input ssh
access-class 12 in
```



Tera Term: New connection

● TCP/IP Host: 10.1.1.68

Service: ○ Telnet ● SSH TCP port#: 22

SSH Authentication

Logging in to 10.1.1.68
Authentication required.

User name: chris

Passphrase: *******

● Use plain password to log in

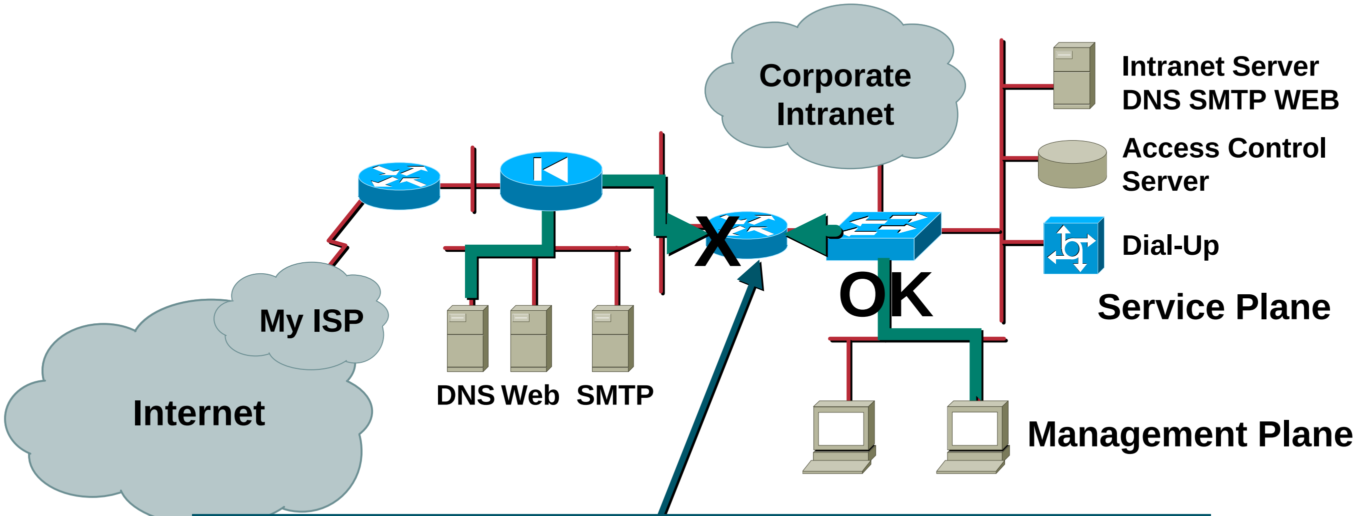
Tera Term - 10.1.1.68 VT

```
krypto#
```

SSHv1 in Cisco Products

Train / Product	Started In
S	Server – 12.0(5)S, Client 12.0(10)S
T	Server – 12.1(1)T, Client 12.1(3)T
Mainline	Server and Client - 12.2(1)
PIX	Server - 5.2
Catalyst Switches	Server - 6.1.1 Release for Catalyst 5000 and 6000 Supervisor
VPN 3000	Server and Client – Release 3.0

SNMP Access Control



```
access-list 13 permit 172.16.2.0 0.0.0.255

snmp-server community NOTpublicORprivate 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

Configuring Syslog on a Router

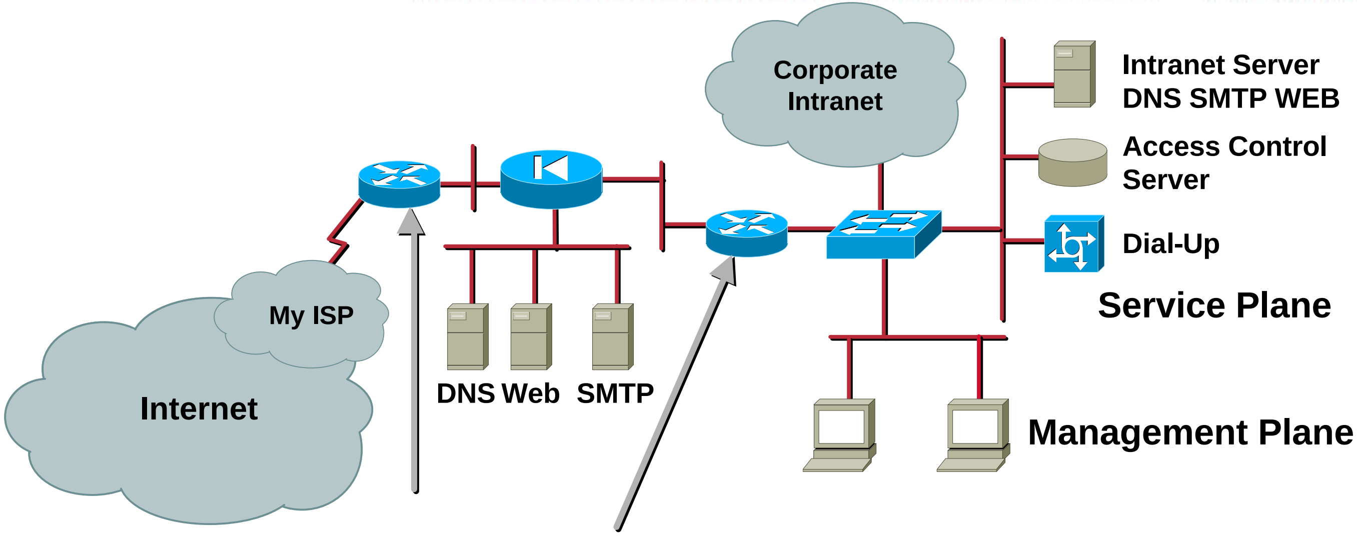
- **To log messages to a syslog server host, use the logging global configuration command**

```
logging host

logging trap level
```

- **To log to internal buffer use:**

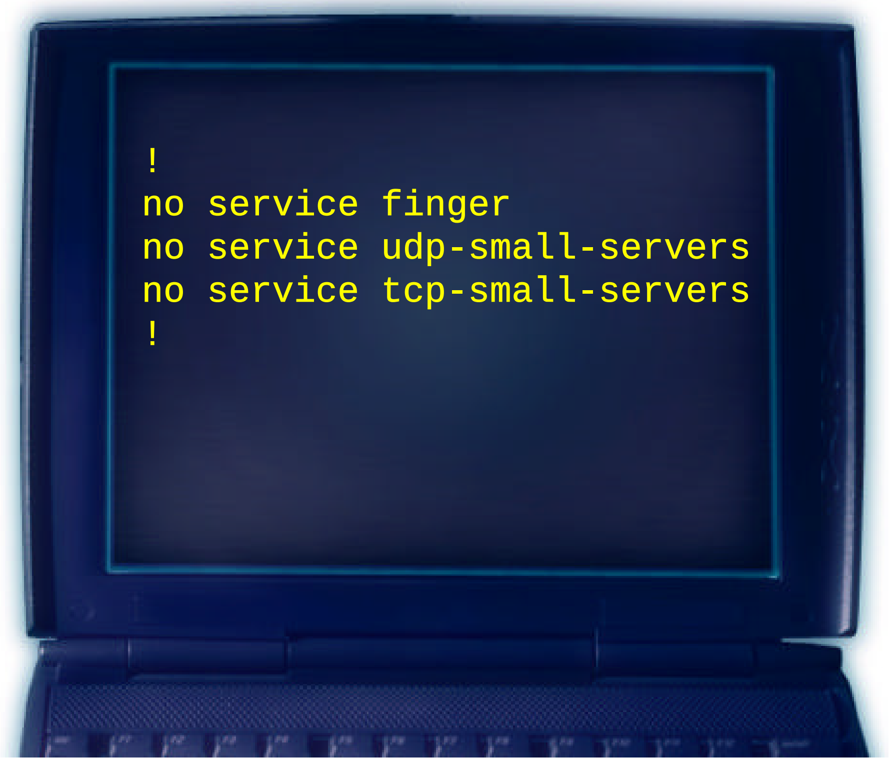
```
logging buffered size
```

Eliminate Unneeded Services



- Echo (7)
- Discard (9)
- Finger (79)
- Daytime (13)
- Chargen (19)

Eliminating Unneeded Services



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

Cisco Discovery Protocol

- CDP can be used to learn information about neighboring devices that are running CDP

  IP address, software version, …

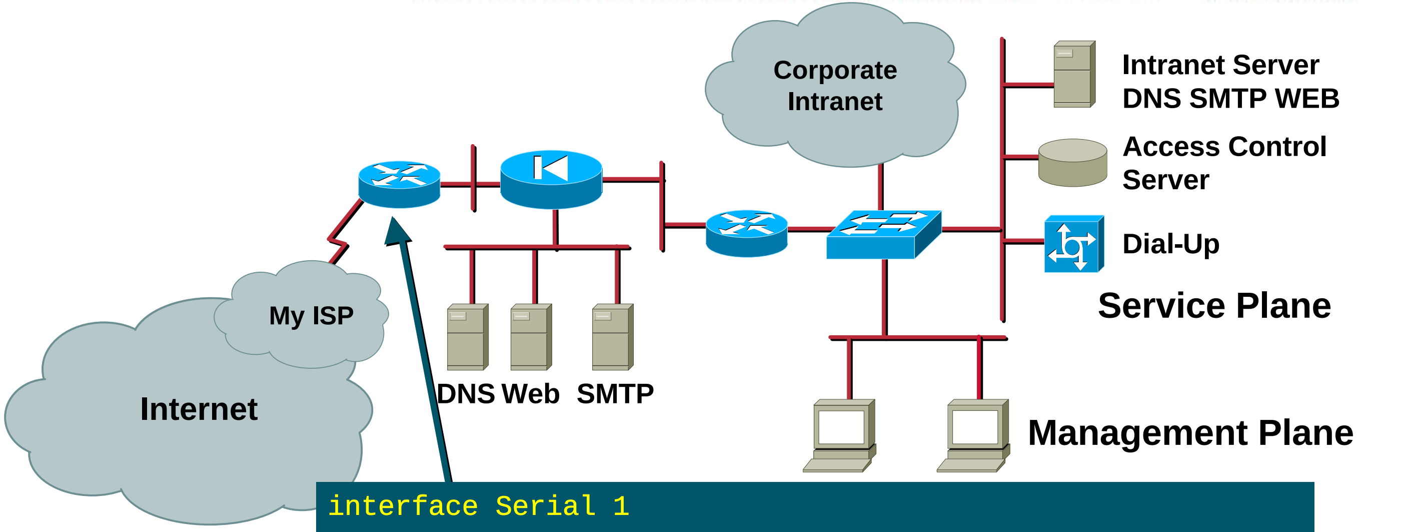
- CDP is configured per interface

- Disable CDP when it isn't needed

  ALL non-trunk ports on switches

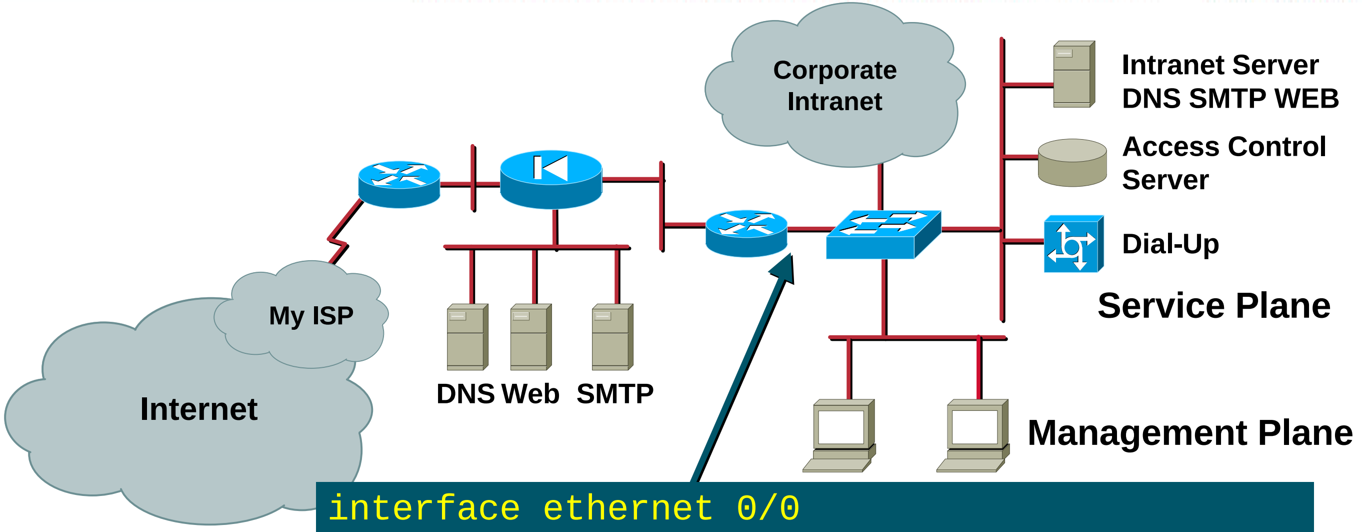
  Case by case on router ports

No IP Directed Broadcasts



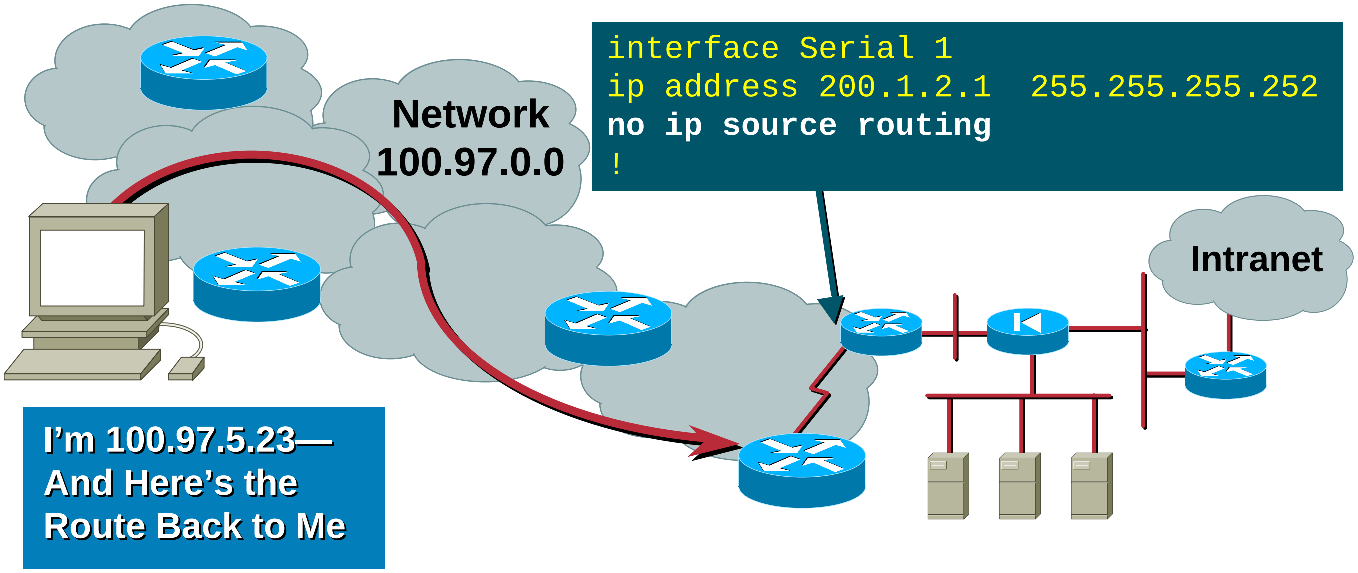
```
interface Serial 1
ip address 200.1.2.1 255.255.255.252
ip access-group 111 in
no ip directed-broadcast

Access-list 111 deny  ip 127.0.0.0    0.255.255.255 any
Access-list 111 deny  ip 172.16.0.0   0.0.255.255 any
```

No IP Directed Broadcasts



```
interface ethernet 0/0
ip address 172.16.1.1   255.255.255.0
no ip directed-broadcast
```

No Source Routing



```
interface Serial 1
ip address 200.1.2.1  255.255.255.252
no ip source routing
!
```

I’m 100.97.5.23— And Here’s the Route Back to Me

RFC 792: Internet Protocol

Verify Configurations

- Use network auditing tools to check configurations

Network Scanning

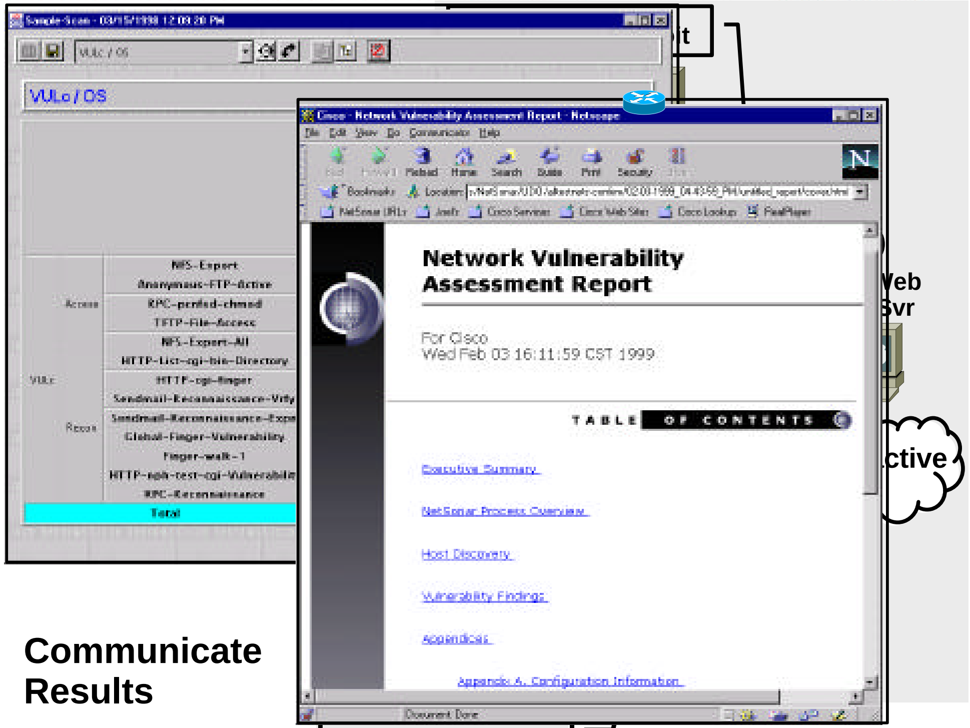
Network Discovery

Passive Vulnerability Analysis

Active Vulnerability Analysis

Presentation and Reporting

Communicate Results



Sample-Scan - 03/15/1999 12:03:20 PM

VULc / OS

VULc	Access	NFS-Export
		Anonymous-FTP-Active
		RPC-pcnfsd-chmod
		TFTP-File-Access
		NFS-Export-All
		HTTP-List-cgi-bin-Directory
		HTTP-cgi-finger
		Sendmail-Reconnaissance-Vrfy
	Recon	Sendmail-Reconnaissance-Expn
		Global-Finger-Vulnerability
		Finger-walk-1
		HTTP-nph-test-cgi-Vulnerability
		RPC-Reconnaissance
Total		

Cisco - Network Vulnerability Assessment Report - Netscape

Network Vulnerability Assessment Report

For Cisco
Wed Feb 03 16:11:59 CST 1999

TABLE OF CONTENTS

Executive Summary

NetSonar Process Overview

Host Discovery

Vulnerability Findings

Appendices

Appendix A. Configuration Information

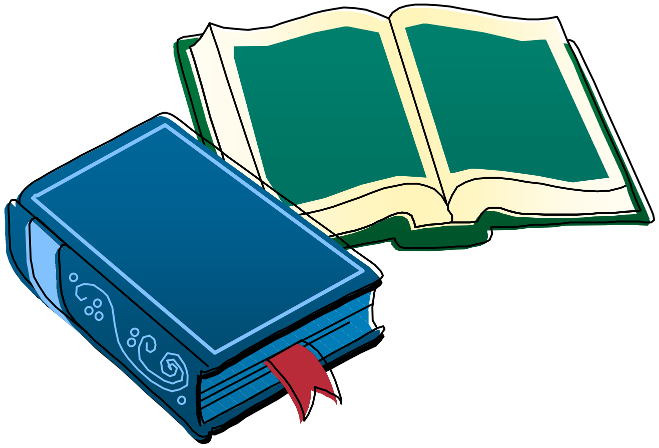
Document: Done

File Edit View Go Communicator Help
Back Forward Reload Home Search Guide Print Security Stop
Bookmarks Location:
NetSonar URLs Jeefs Cisco Services Cisco Web Sites Cisco Lookup RealPlayer
t
Web Svr
ctive

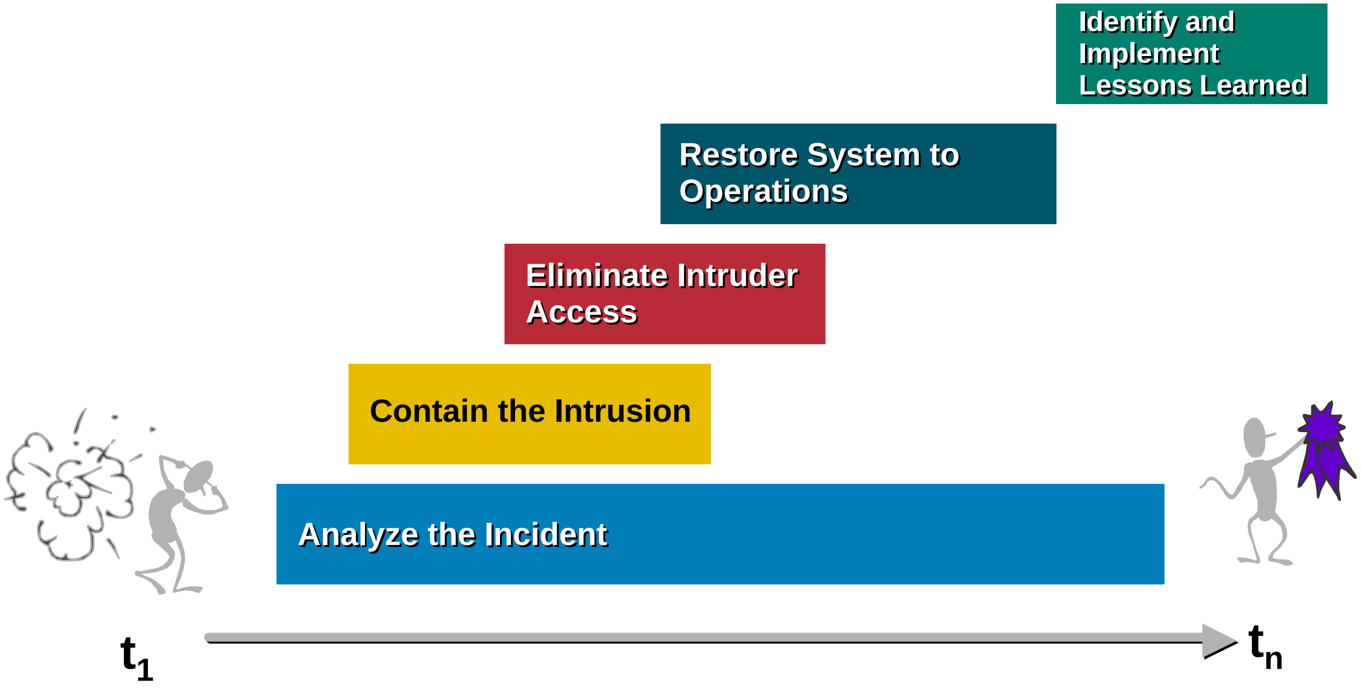
Workstation:
Windows NT 4.0
- **SMB Redbutton**
- **Anonymous FTP**

Audit

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



Handling Incidents



Identify and Implement Lessons Learned

Restore System to Operations

Eliminate Intruder Access

Contain the Intrusion

Analyze the Incident

Cooperating with ISPs

- Will you provide incident response service for your users or subscribers?
- If not, what role will you play in helping your customers with security incidents?
- Work with your ISP to resolve security problems
- Establish a list of contacts at the enterprise and at the ISP
- Define how each organization will respond to given scenarios

Performance

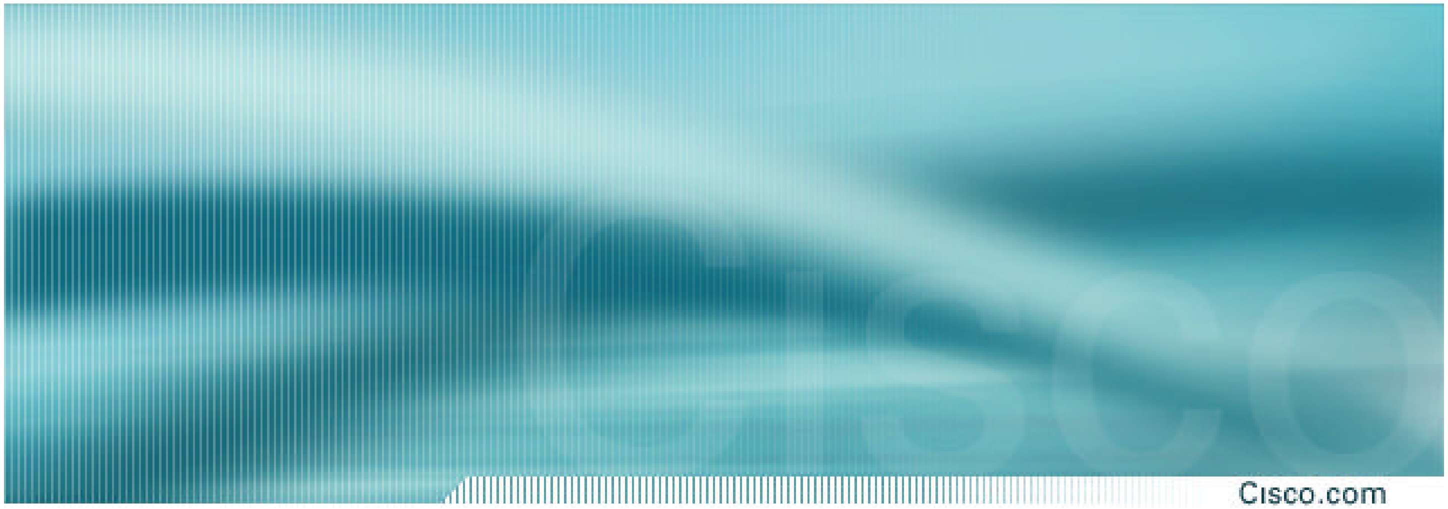
- No bandwidth performance impact
- Slight increased time required when using token card authentication
- Setup time for radius and/or TACACS+

Just Remember…

- All network devices should be protected
- Management access should be restricted
- Don’t assume default configurations meet your security requirements
- Sniffers are everywhere

How Does this Protect Me?

- Reduces the opportunity for unauthorized access
- SSH will protect against capture of authentication information or data by sniffers
- Removal of unneeded services reduces data available to reconnaissance attacks

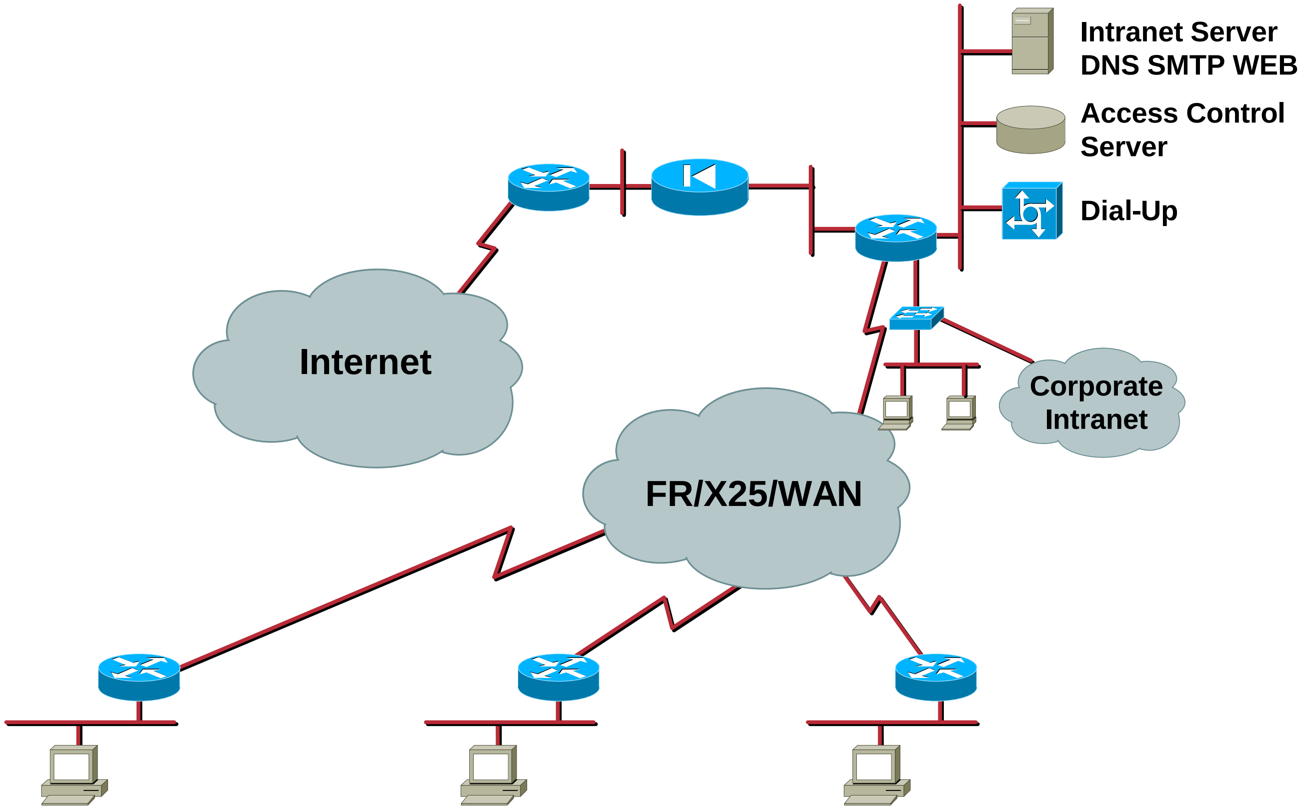


Securing the Corporate Internet Connection

Requirements

- Secure the Internet access
  - Employees have full Internet access
- Protect inside network
  - Allow outbound traffic and associated returning traffic
  - Deny arbitrary inbound traffic
- Verify that the packet header information is reasonable for the topology
- Limit DOS attack bandwidth
- Detect attacks

Connecting Corporate Headquarters to the Internet



Tool Kit

- **Access control list**
- **Stateful packet inspection**
- **Control access rate**
- **Intrusion detection**
- **Logging**

Access Control Lists Are about Packet Classification

- **If <test> Then <action>**
- **<test> is about Layer 3/4 matches**
- **<action> can be**
  - **permit/deny**
  - **prioritize**
  - **trigger dial-up interface**
  - **encrypt, etc…**

ACL: Apply the Test

- access-group # in/out

  permit means can be forwarded

- dialer-list #

  permit means can bring up a dial-up interface

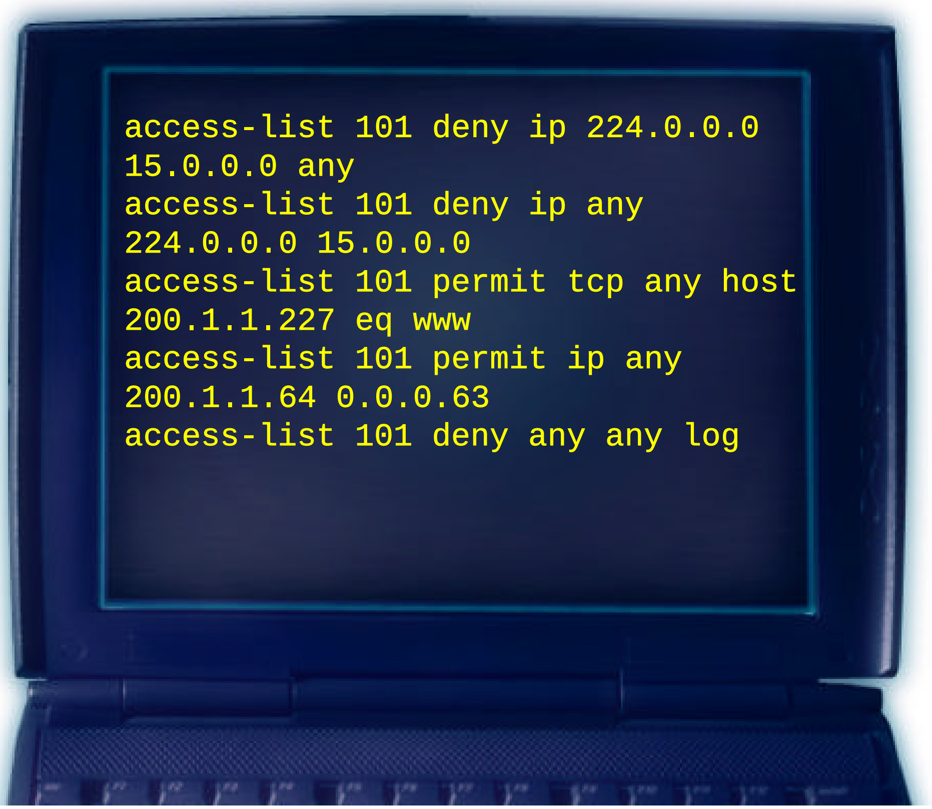
- match address #

  permit means encrypt

ACL: Create a Test

The Last Deny Any Any Is Implicit If You Don’t Put “log”

“log” Is Very Useful to Debug an ACL and Find Out Your Are Missing Some Permit Statements



```
access-list 101 deny ip 224.0.0.0
15.0.0.0 any
access-list 101 deny ip any
224.0.0.0 15.0.0.0
access-list 101 permit tcp any host
200.1.1.227 eq www
access-list 101 permit ip any
200.1.1.64 0.0.0.63
access-list 101 deny any any log
```

ACL Are Stateless

- Check the headers against a static rule
- Execute the action, forget about it, and deal with the next packet

Flow Control with Stateless ACLs

- **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

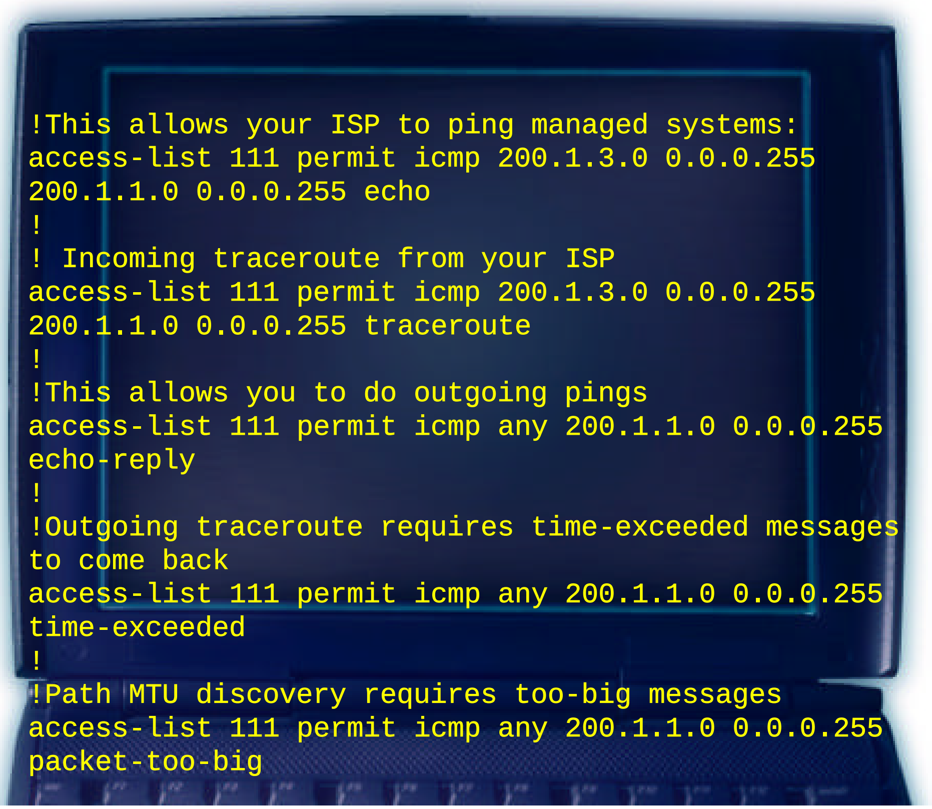
0 Echo Reply
3 Destination Unreachable
4 Source Quench
5 Redirect
8 Echo
11 Time Exceeded
12 Parameter Problem
13 Timestamp
14 Timestamp Reply
15 Information Request
16 Information Reply

Use “Established” to Deny Inbound TCP SYN

Don’t Reply to Ping or Traceroute

Apply This ACL to Inbound Traffic on the Outside Interface of the Most External Router

Based on Your Service Agreement With Your ISP, You May Want to Allow Some Inbound Pings or Traceroutes: Limit the Source to a Range of Addresses Used by Your ISP



```
!This allows your ISP to ping managed systems:
access-list 111 permit icmp 200.1.3.0 0.0.0.255
200.1.1.0 0.0.0.255 echo
!
! Incoming traceroute from your ISP
access-list 111 permit icmp 200.1.3.0 0.0.0.255
200.1.1.0 0.0.0.255 traceroute
!
!This allows you to do outgoing pings
access-list 111 permit icmp any 200.1.1.0 0.0.0.255
echo-reply
!
!Outgoing traceroute requires time-exceeded messages
to come back
access-list 111 permit icmp any 200.1.1.0 0.0.0.255
time-exceeded
!
!Path MTU discovery requires too-big messages
access-list 111 permit icmp any 200.1.1.0 0.0.0.255
packet-too-big
```

Enforce RFC 2827 and RFC 1918 Filters

- RFC 2827 tells us no packet should leave a network if the source address doesn't belong to its address space

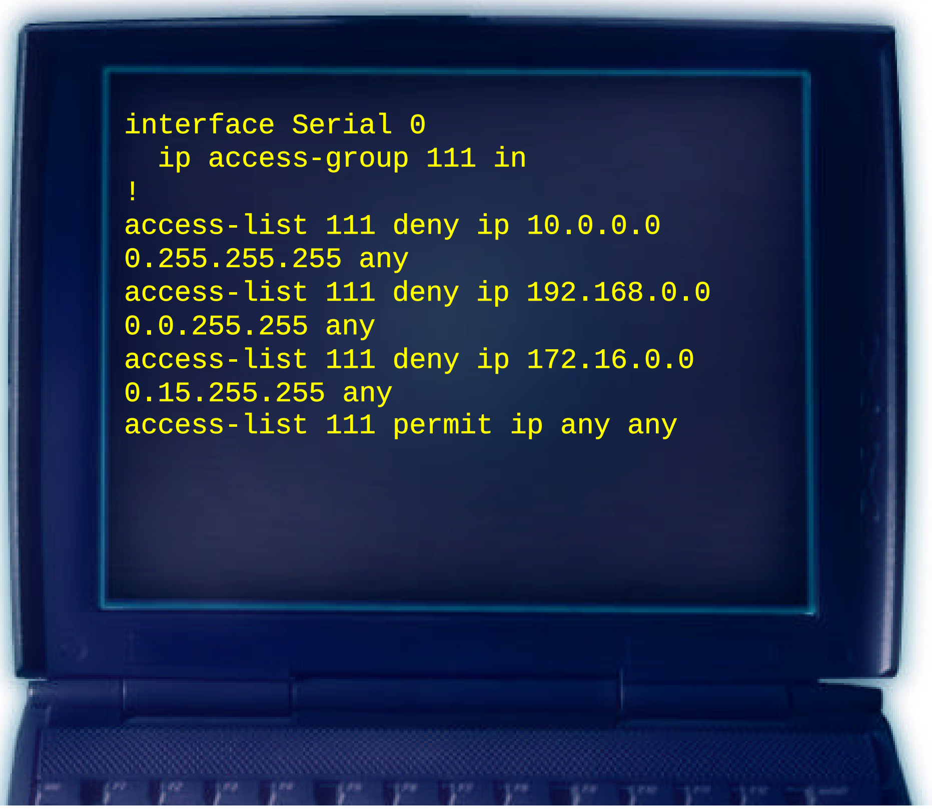
  Should be enforced at both the ISP and customer equipments

- RFC 1918 lists addresses known as private; no packet with such addresses should be on the Internet

RFC 1918 Filtering

Apply This ACL to Inbound Traffic on the Outside Interface of the Most External Router

You Should Also Add the Reverse Statements, Where the Destination Is a Private Address; However, This Should Also Be Taken Care of by the ISP



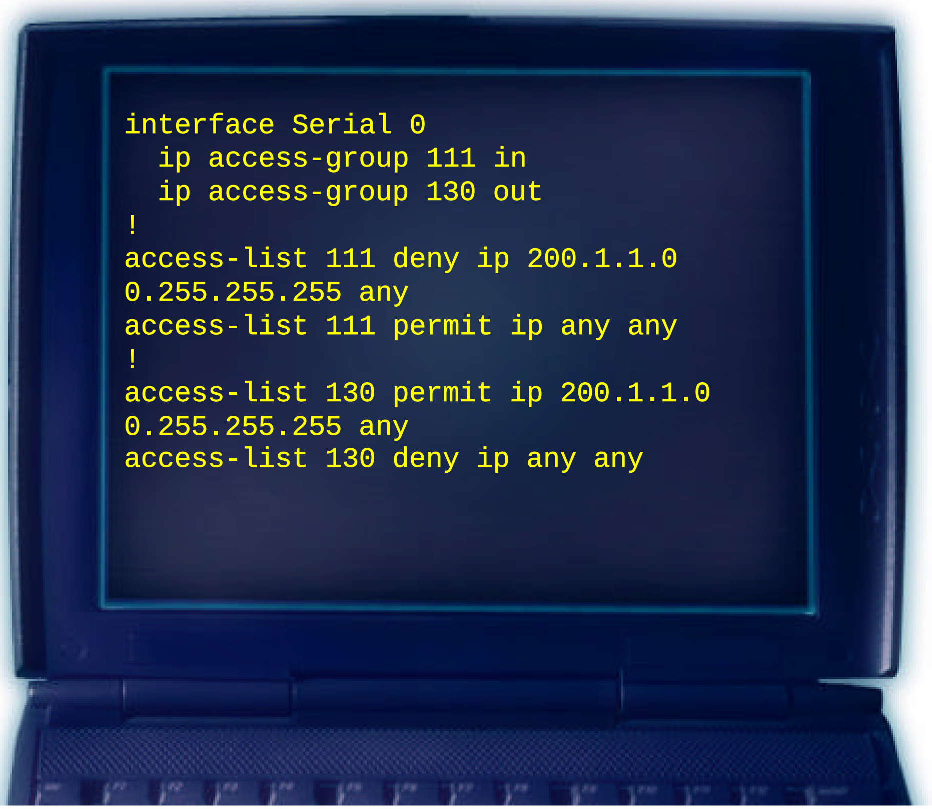
```
interface Serial 0
  ip access-group 111 in
!
access-list 111 deny ip 10.0.0.0
0.255.255.255 any
access-list 111 deny ip 192.168.0.0
0.0.255.255 any
access-list 111 deny ip 172.16.0.0
0.15.255.255 any
access-list 111 permit ip any any
```

RFC 2827 Filtering

Serial 0 Is the Outside Interface of the Most External Router

ACL 120 Ensures That No One Sends You Traffic Masquerading With Your Own Addresses

ACL 130 Ensures That None of Your Users Change Their Addresses to One Not Belonging to Your Network Address Space (Makes Traceability Easier)



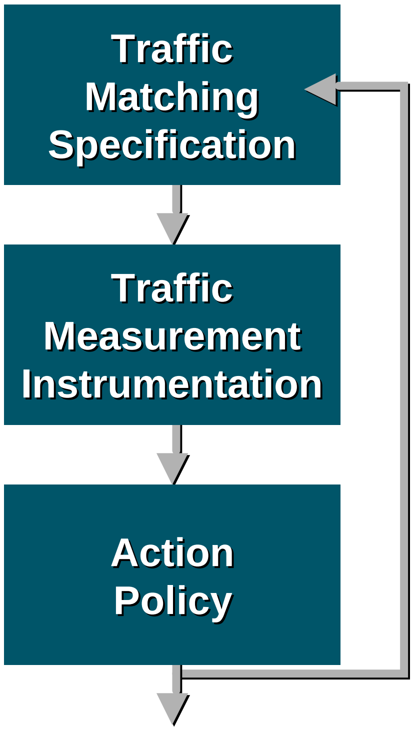
```
interface Serial 0
  ip access-group 111 in
  ip access-group 130 out
!
access-list 111 deny ip 200.1.1.0
0.255.255.255 any
access-list 111 permit ip any any
!
access-list 130 permit ip 200.1.1.0
0.255.255.255 any
access-list 130 deny ip any any
```

Another Option: Unicast Reverse-Path Forwarding Checks

- Mitigates source address spoofing by checking that a packet’s return path uses the same interface it arrived on
- Best implemented at your ISP
- Requires CEF
- Not appropriate where asymmetric paths exist

```
ip cef distributed
!
interface Serial 0
  ip verify unicast reverse-path
```

Limit the Impact of DOS Attacks: Committed Access Rate



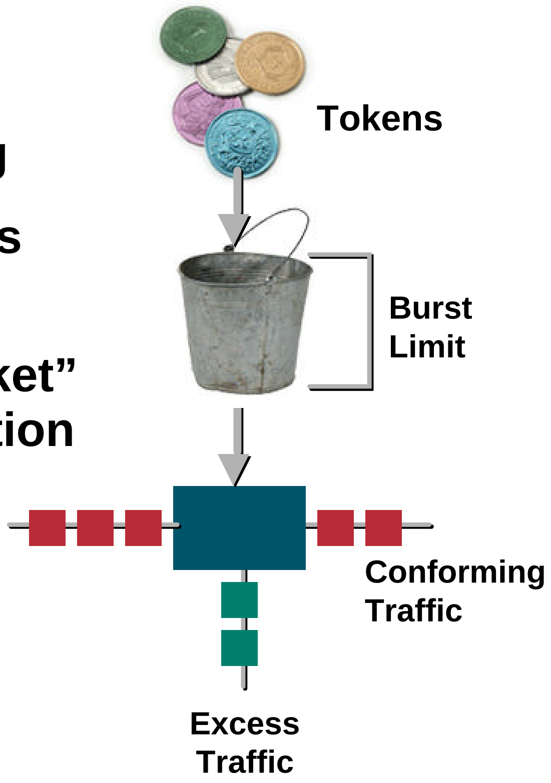
Traffic Matching Specification

Traffic Measurement Instrumentation

Action Policy

Next Policy

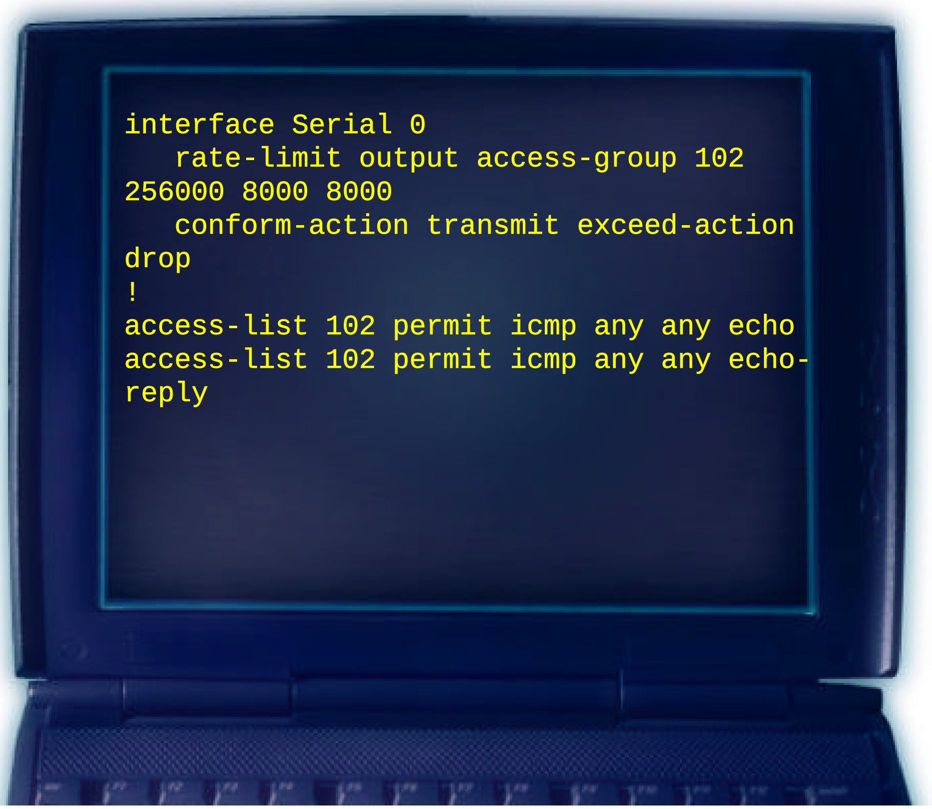
- Rate limiting
- Several ways to filter
- “Token bucket” implementation



Don’t Be Part of a DDOS Attack

This Allows You to Generate Some ICMP Traffic for Management, While Limiting It to 1/32 of You Bandwidth

You May Still Be Used As a Source for a DDoS, but With Less Amplification



```
interface Serial 0
   rate-limit output access-group 102
256000 8000 8000
   conform-action transmit exceed-action
drop
!
access-list 102 permit icmp any any echo
access-list 102 permit icmp any any echo-
reply
```

Stateless vs. Stateful

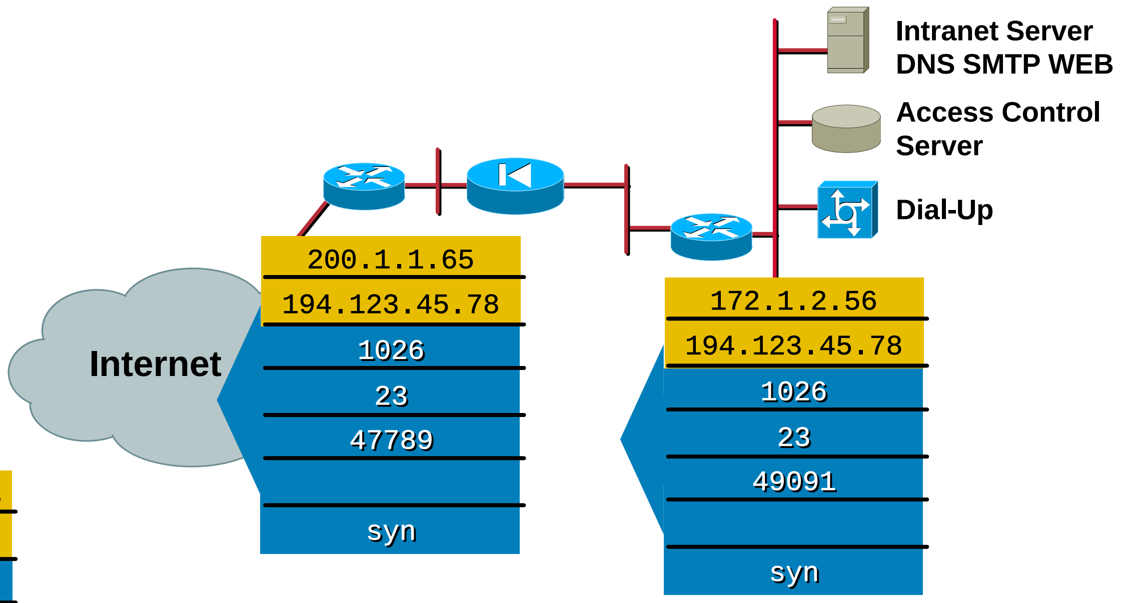
- Stateless is OK authorize specific flows on a permanent basis
- Stateful packet inspection binds inbound traffic to conversations initiated from the inside

Stateful

- Analyze one packet header
- Dynamically create a rule to test the next packet

  In the same direction or for the returning packet

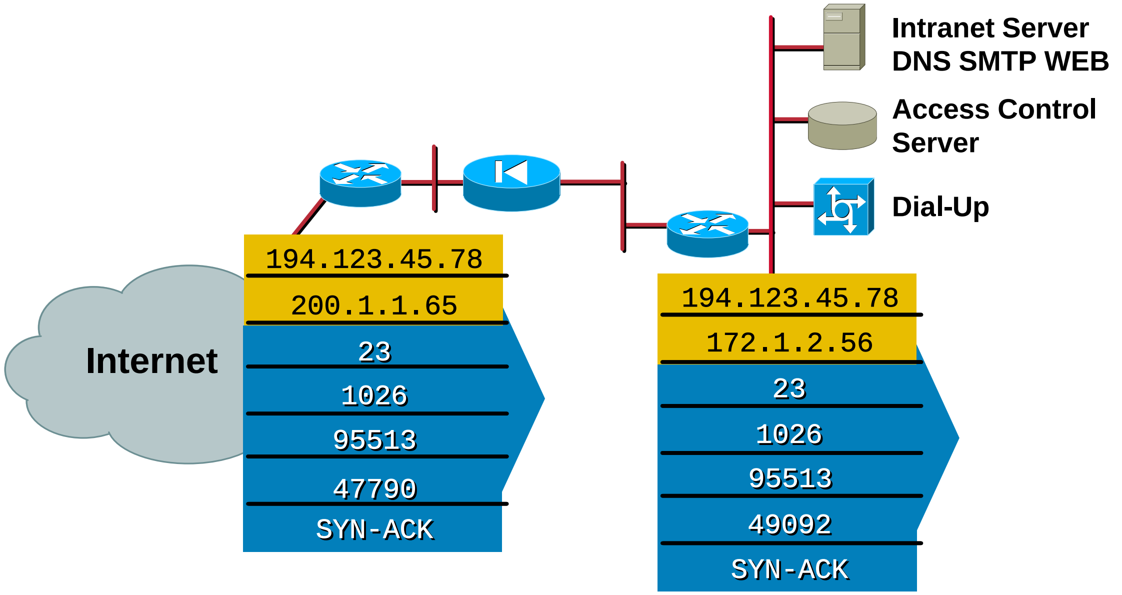
NAT and Stateful Algorithm for TCP



Source address	200.1.1.65	172.1.2.56
Dest. address	194.123.45.78	194.123.45.78
Source Port	1026	1026
Dest. address	23	23
Source Sequence	47789	49091
Dest. Sequence		
Flag	syn	syn

- **Create inbound rule by reversing addresses, port, sequence and updating flag**

NAT and Stateful Algorithm for TCP



- Check inbound packet against the dynamic rule, remove it after there is a match (or time out)

NAT and Stateful Algorithm for UDP

- Similar process
- No flags or sequence number means less state
- Requires shorter time-out

NAT and Stateful Algorithm for Complex Applications

- Some protocols carry addresses in the payload section (netbios, H.323, etc.)
- Most multimedia applications open server to client connections (also FTP)
- Need to open more dynamic inbound rules

Configuring the Stateful Firewall

- Choose an IP pool inside the address space provided by the ISP

  NAT pool: 200.1.1.64 - 200.1.1.127

- Update the router ACL to authorize inbound traffic to the IP pool

  ```
  Access-list 111 permit ip any 200.1.1.64 0.0.0.63
  ```

Configuring the Stateful Firewall

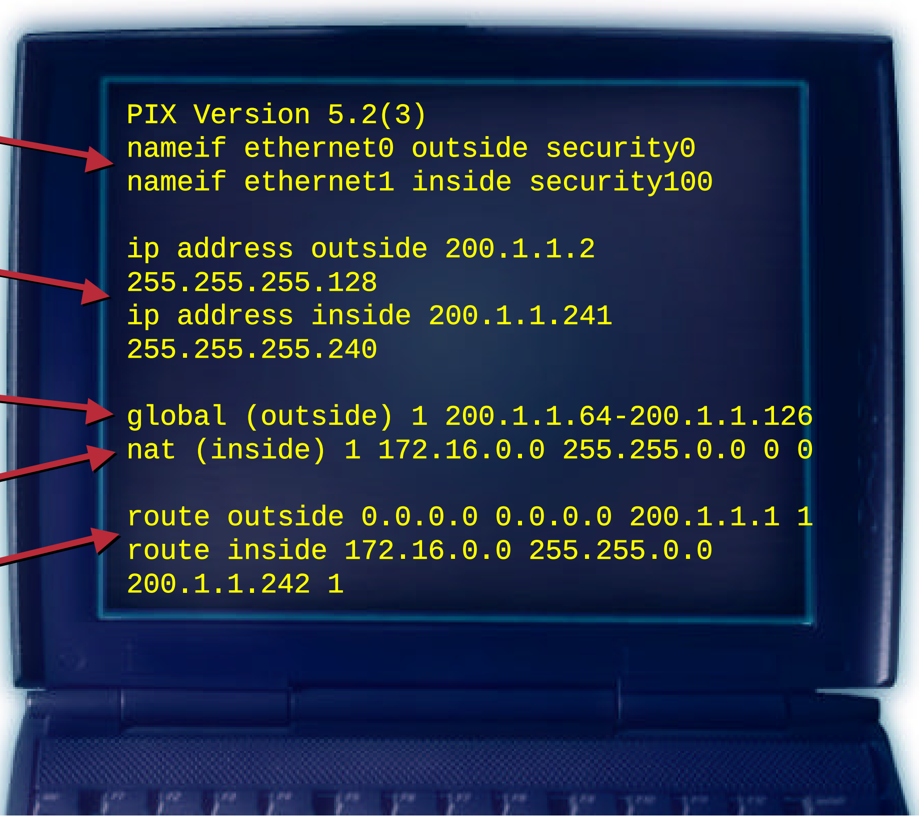
Assign a Security Level to Each Interface

Configure Interface Addresses

Create an Address Pool for Nat

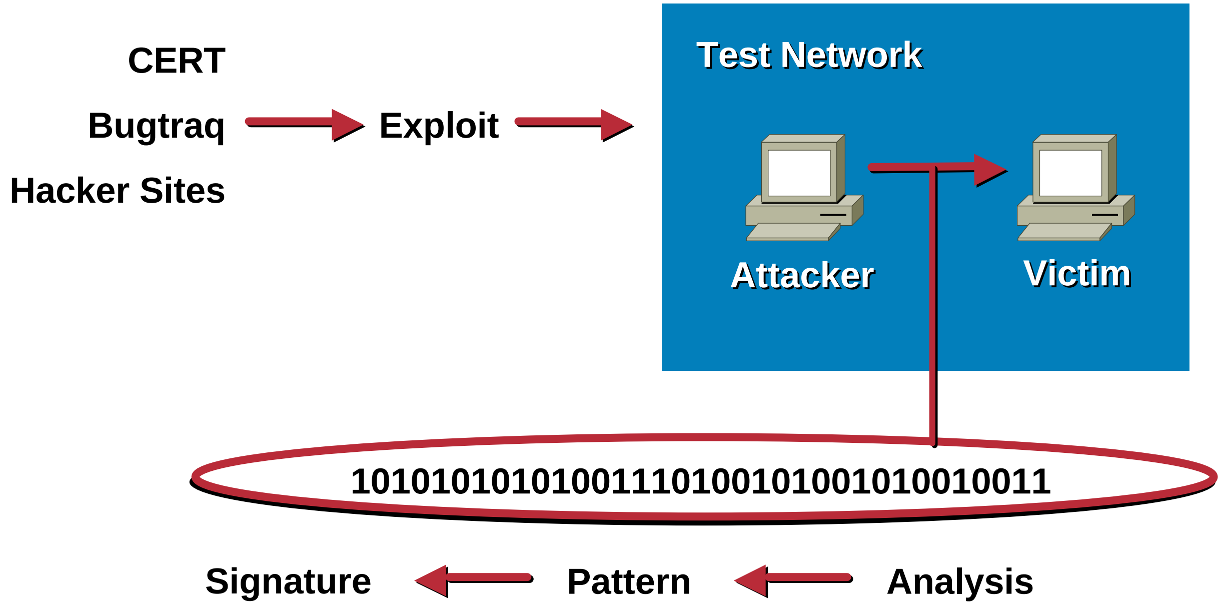
List Inside Addresses to Be Translated

Configure Static Routing



```
PIX Version 5.2(3)
nameif ethernet0 outside security0
nameif ethernet1 inside security100

ip address outside 200.1.1.2
255.255.255.128
ip address inside 200.1.1.241
255.255.255.240

global (outside) 1 200.1.1.64-200.1.1.126
nat (inside) 1 172.16.0.0 255.255.0.0 0 0

route outside 0.0.0.0 0.0.0.0 200.1.1.1 1
route inside 172.16.0.0 255.255.0.0
200.1.1.242 1
```

Intrusion Detection Signatures



CERT

Bugtraq → Exploit →

Hacker Sites

Test Network

Attacker

Victim

10101010101001110100101001010010011

Signature ← Pattern ← Analysis

- Behavior matches known patterns of malicious activity
- Requires creation of misuse signatures

Signature Implementations and Structures

- Signature implementation

  Context—Trigger data contained in packet header

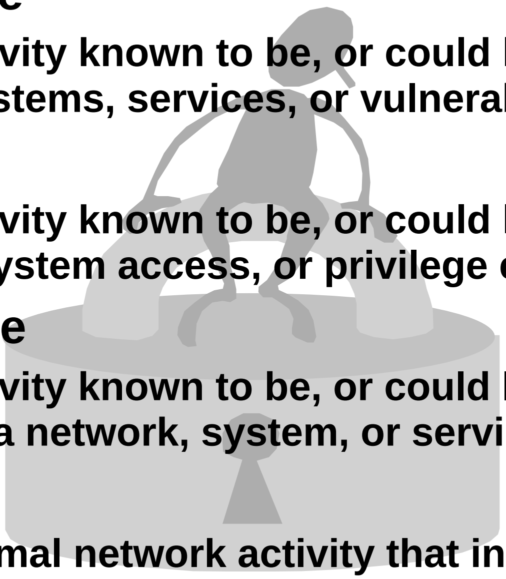
  Content—Trigger data contained in packet payload

- Signature structure

  Atomic—Trigger contained in a single packet

  Composite—Trigger contained in a series of multiple packets

Signature Classes



- **Reconnaissance**

  Triggers on activity known to be, or could lead to, unauthorized discovery of systems, services, or vulnerabilities

- **Access**

  Triggers on activity known to be, or could lead to, unauthorized data retrieval, system access, or privilege escalation

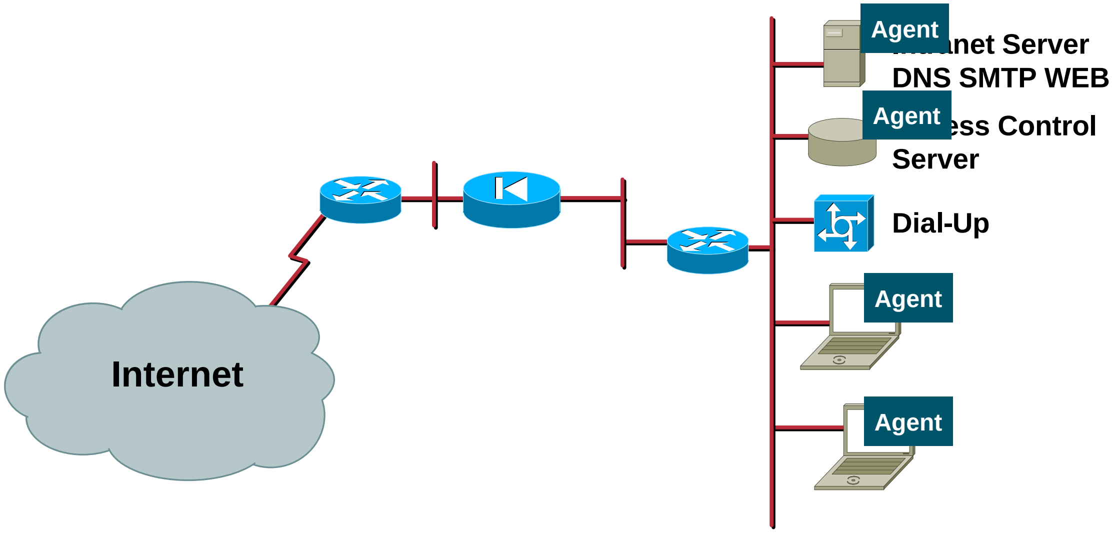
- **Denial of service**

  Triggers on activity known to be, or could lead to, the disablement of a network, system, or service

- **Information**

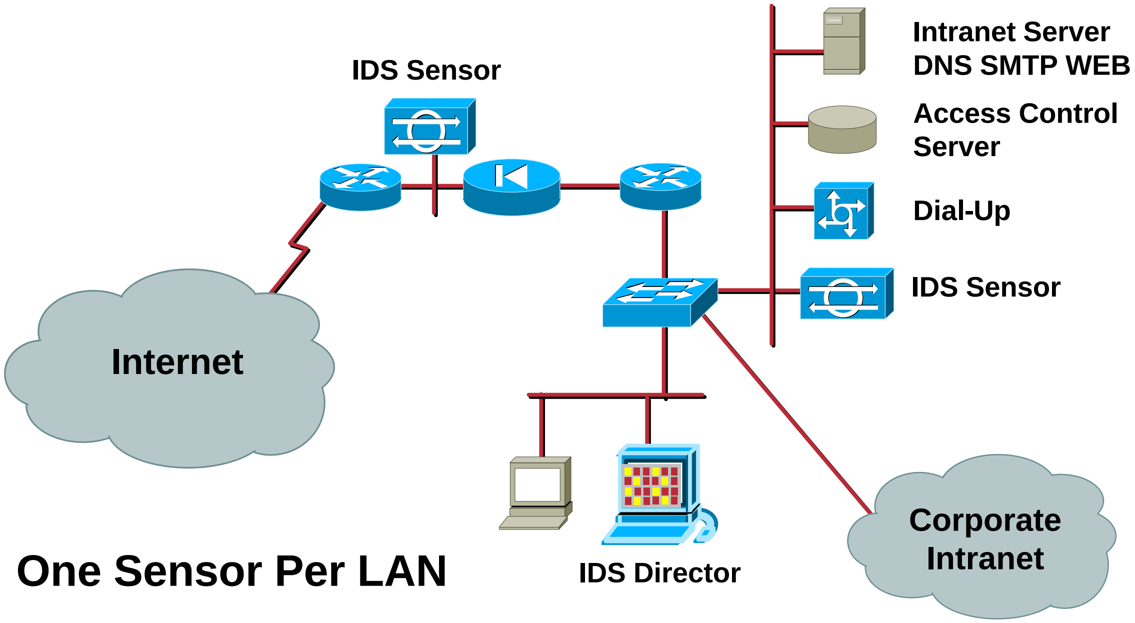
  Triggers on normal network activity that in itself is not considered to be malicious, but can be used to determined the validity of an attack or for forensic purposes

Host-Based Intrusion Detection



- Every host needs to be equipped
- Lack of central management

Network-Based Intrusion Detection



- One Sensor Per LAN
- Allows Response to Attacks
- Central View of Alarms

Configuring Cisco IOS Firewall IDS

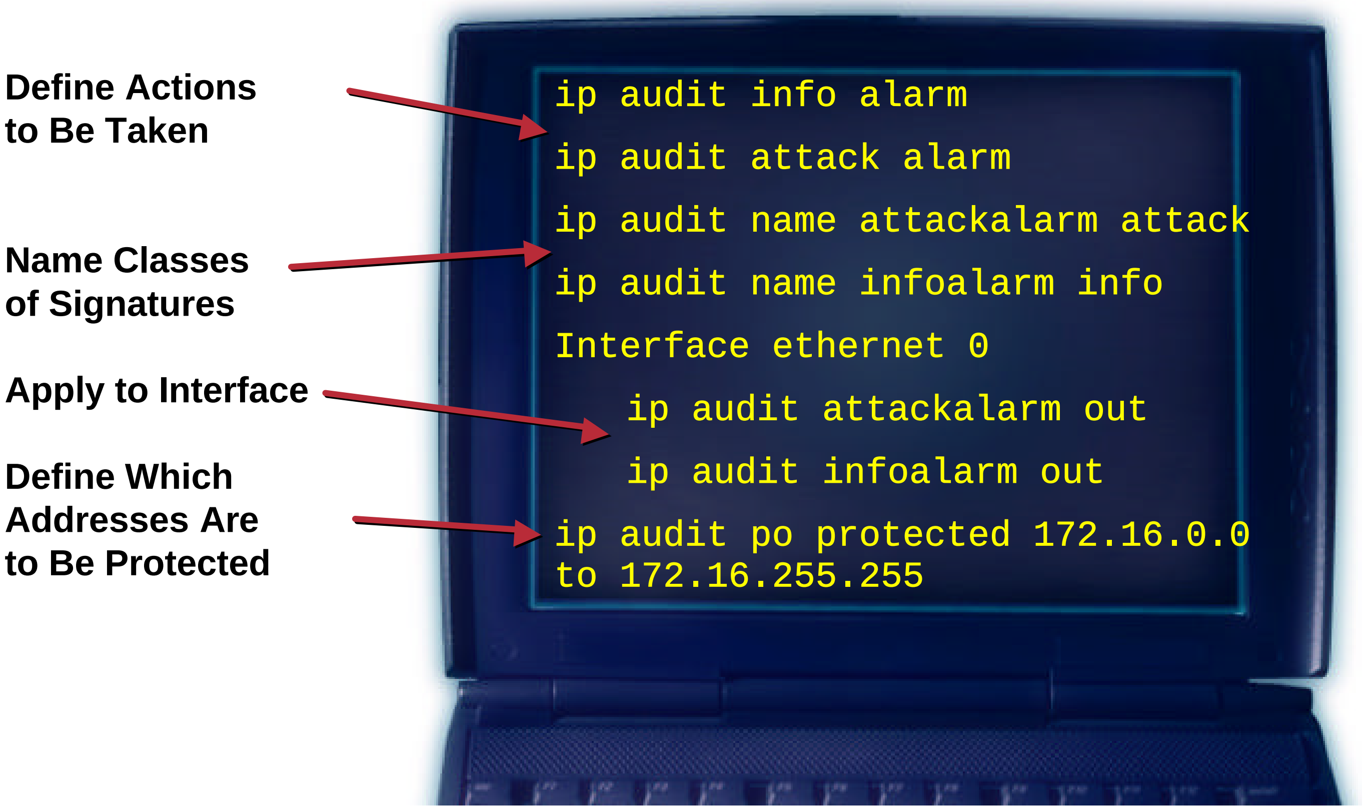
- **Initializing the Cisco IOS FW IDS**

```
router(conf)#ip audit smtp spam 250

router(conf)#ip audit po max-events 100
```

- **Initializing the post office**

```
router(conf)# ip audit notify nr-director

router(conf)# ip audit po local hostid 25 orgid 1

router(conf)# ip audit po remote hostid  25 orgid 1
rmtaddress 172.16.2.10 localaddress 172.16.1.1 port
45000 preference 1 timeout 5 application director
```

Configuring and Applying Audit Rules



Define Actions to Be Taken

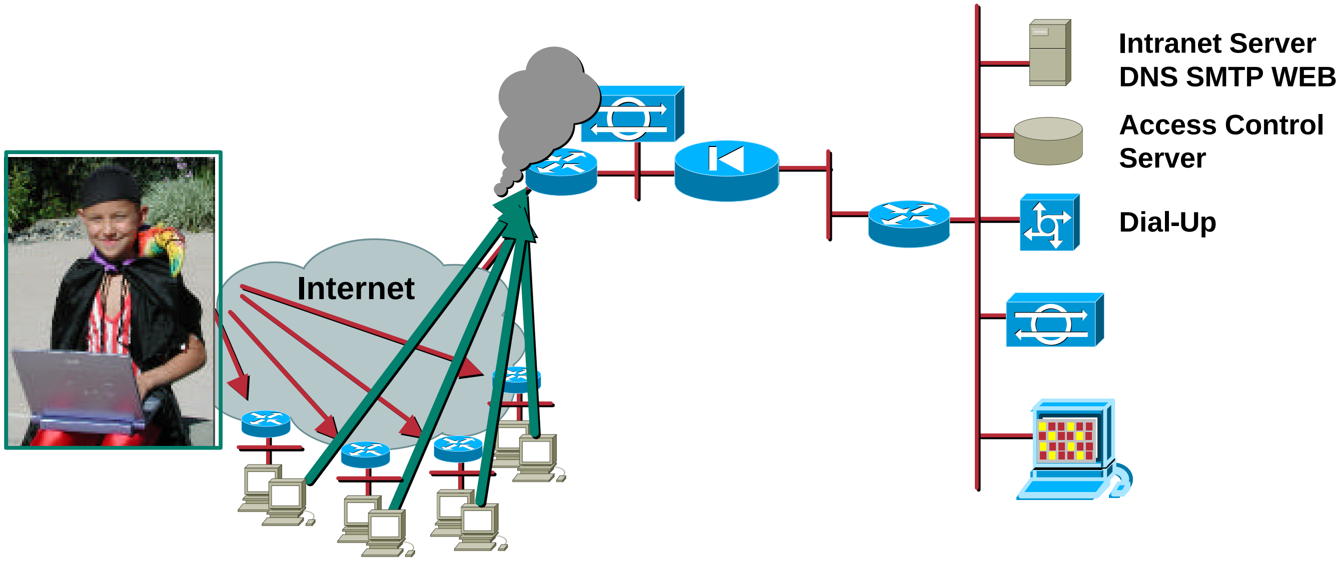
Name Classes of Signatures

Apply to Interface

Define Which Addresses Are to Be Protected

```
ip audit info alarm
ip audit attack alarm
ip audit name attackalarm attack
ip audit name infoalarm info
Interface ethernet 0
   ip audit attackalarm out
   ip audit infoalarm out
ip audit po protected 172.16.0.0
to 172.16.255.255
```

Network under Fire



- All inbound bandwidth is used
- CAR needs to be configured at the ISP edge

Just Remember…

- Be careful when defining ACLs—The order of the lines is very important
- "Deny any any log" as the last ACL line will show you the header of all denied packet
- Ensure that you are applying ACLs on the proper interface and in the correct direction
- Don't filter traffic, such as routing protocols, that should be authorized
- Don't shut yourself out when using IDS shunning

Performance

- Access lists in these configurations have almost no impact on performance
- Denying large numbers of packets on a high bandwidth segment can result in a bottleneck (70k pps dropped on OC-3)
- PIX stateful engine can handle huge numbers of simultaneous connections and very large bandwidth (250k+/1GB)
- IDS on a sensor is not an issue, IDS on a router will consume considerable CPU if all signatures are turned on

Securing the Public Web Service

Requirements

- **Internet visibility**

  Servers on DMZ are public

- **Protect public services**

  Web, DNS, SMTP, FTP,…

- **Limit trust between various DMZ**

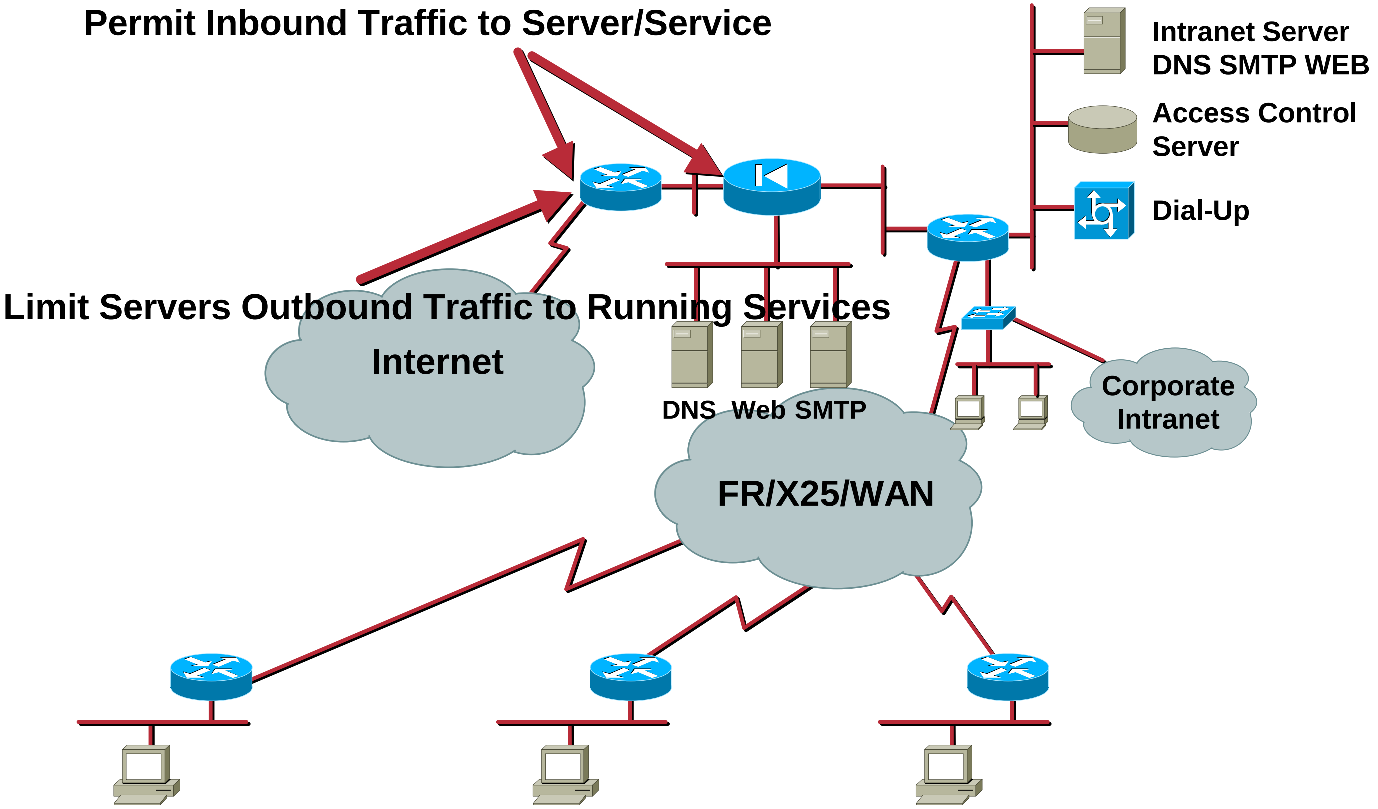
  Control traffic from servers to back end database

- **Don’t be the source of an attack**

Tool Kit

- Use static rules to allow inbound flow
  - Binding a destination address to one service
- Limit access rate to servers
  - SYN flood attack
- Good administrative practice
  - Dedicated servers
  - Up-to-date patches
- Filter outbound traffic from servers
  - Check source port number

Adding E-Commerce Services



Permit Inbound Traffic to Server/Service

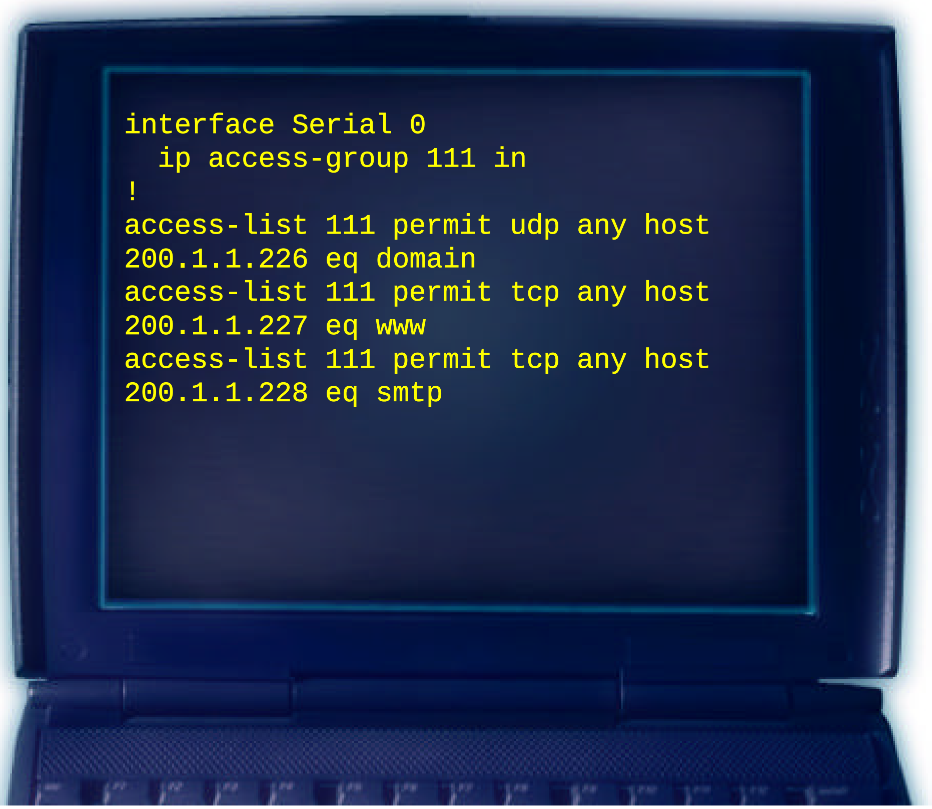
Limit Servers Outbound Traffic to Running Services

External Router: Permit Inbound Traffic to Public Servers

Apply This ACL to Inbound Traffic on the Outside Interface of the Most External Router

Keep in Mind That Lines Are Added at the End of an Existing ACL; Beware of an Explicit `deny any any` Statement!

If You Do Zone Transfers With a Secondary DNS You Need to Permit tcp=domain for This Host



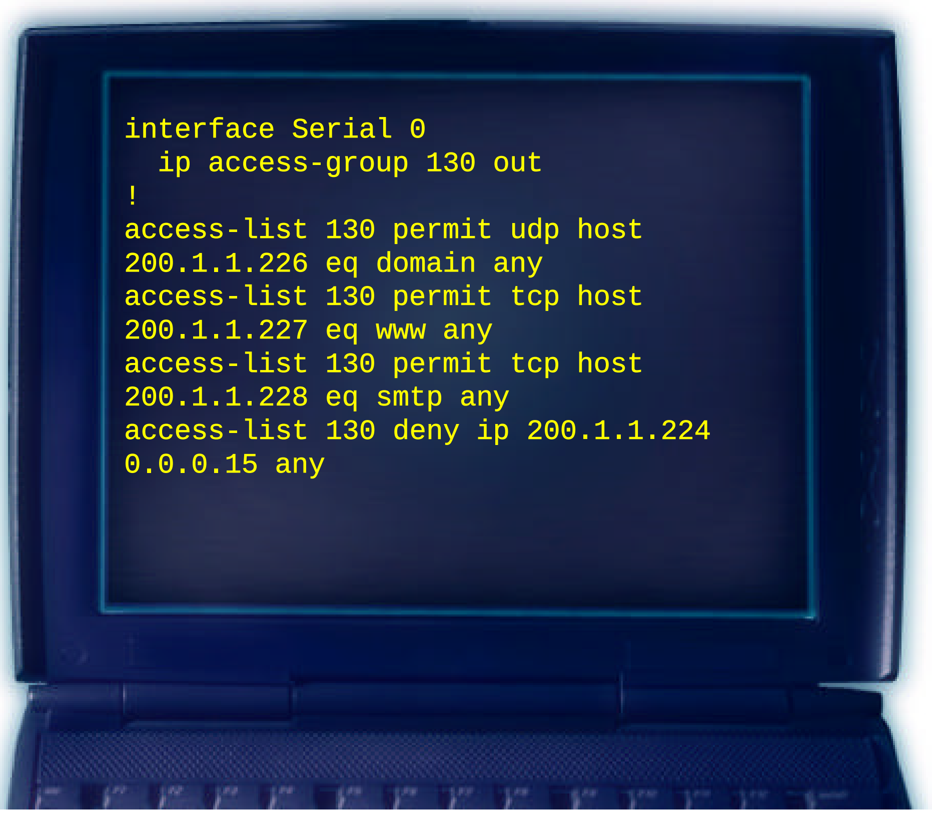
```
interface Serial 0
  ip access-group 111 in
!
access-list 111 permit udp any host
200.1.1.226 eq domain
access-list 111 permit tcp any host
200.1.1.227 eq www
access-list 111 permit tcp any host
200.1.1.228 eq smtp
```

External Router: Verify Traffic Type from Servers

Apply This ACL to Outbound Traffic on the Outside Interface of the Most External Router

Keep in Mind That Lines Are Added at the End of an Existing ACL

By Permitting Very Specific Flows and Then Denying All Traffic for the Public Servers Addresses You Can Control That No Other Services Generate Packets Should the Host Be Compromised



```
interface Serial 0
  ip access-group 130 out
!
access-list 130 permit udp host
200.1.1.226 eq domain any
access-list 130 permit tcp host
200.1.1.227 eq www any
access-list 130 permit tcp host
200.1.1.228 eq smtp any
access-list 130 deny ip 200.1.1.224
0.0.0.15 any
```

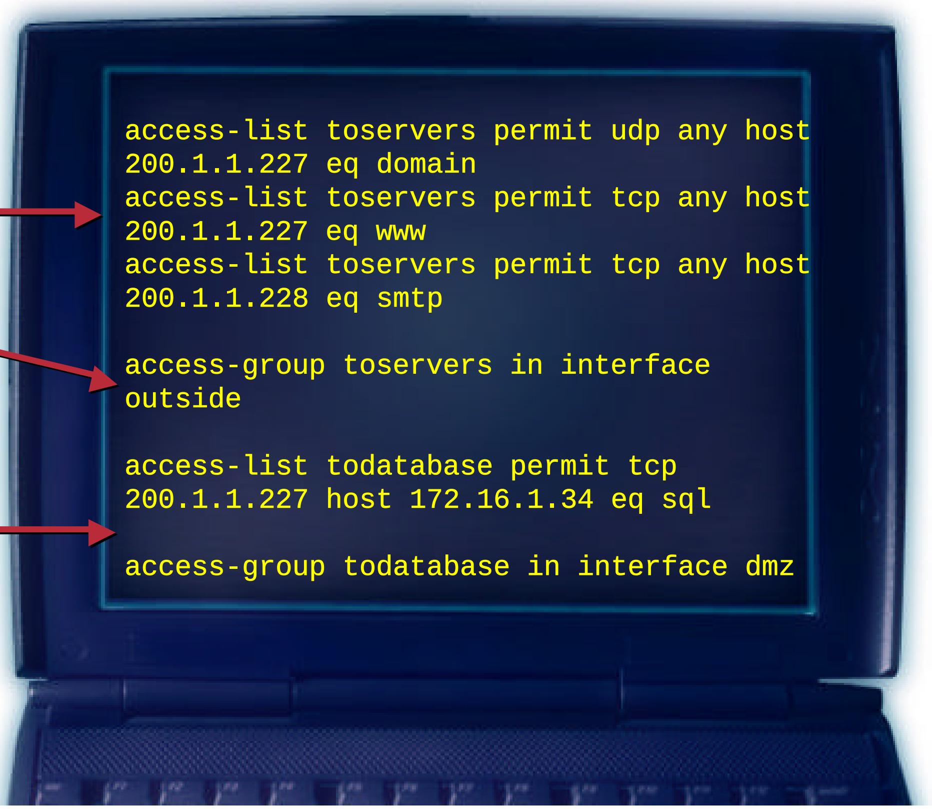
Stateful Firewall: Permit Inbound Traffic to Public Servers

Syntax Is Very Much Identical to Router

Create Test

Apply Filter

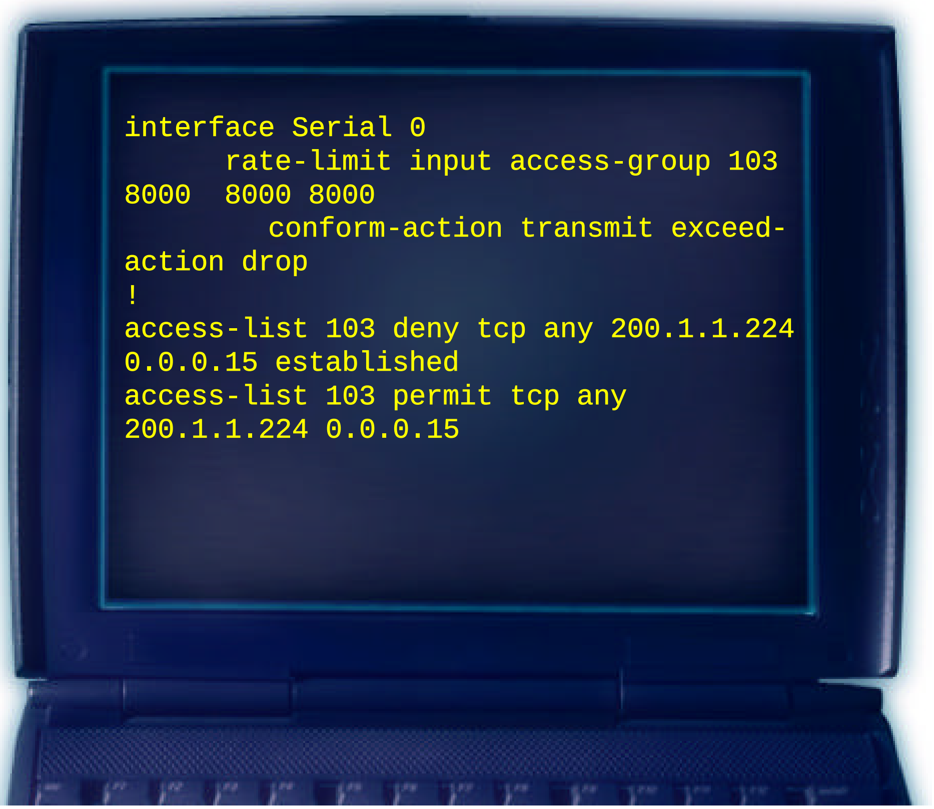
Create a Rule to Authorize Traffic from Web Server to Back End Database



```
access-list toservers permit udp any host
200.1.1.227 eq domain
access-list toservers permit tcp any host
200.1.1.227 eq www
access-list toservers permit tcp any host
200.1.1.228 eq smtp

access-group toservers in interface
outside

access-list todatabase permit tcp
200.1.1.227 host 172.16.1.34 eq sql

access-group todatabase in interface dmz
```

CAR Rate Limiting: Protect Server from SYN Floods

Limit Inbound TCP SYN Packets to 8 Kbps

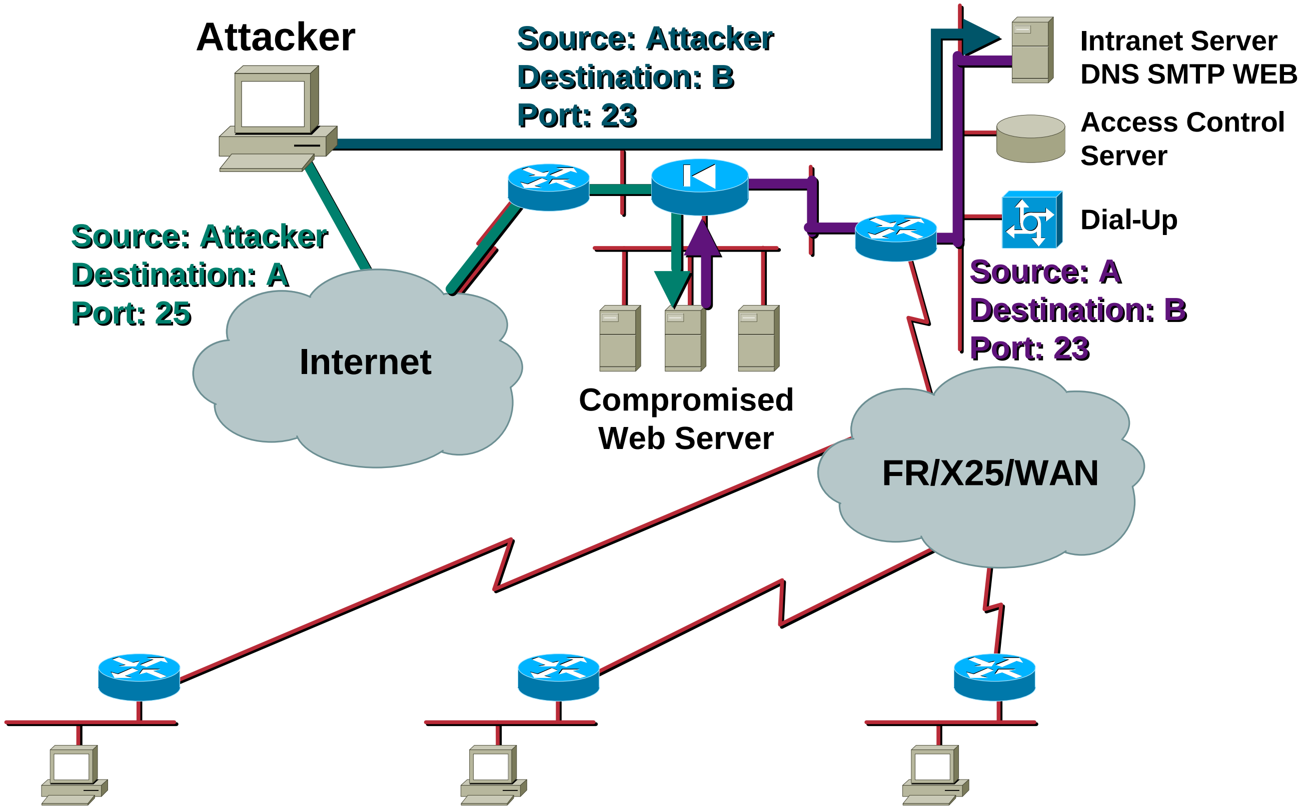


```
interface Serial 0
      rate-limit input access-group 103
8000  8000 8000
         conform-action transmit exceed-
action drop
!
access-list 103 deny tcp any 200.1.1.224
0.0.0.15 established
access-list 103 permit tcp any
200.1.1.224 0.0.0.15
```

Just Remember…

- Many DOS attacks will use ICMP which is needed for management
- Run only one service per server
  - Install minimum kernel
  - Keep up-to-date with security patches
- Be very restrictive when applying rules
  - Limit source and destination addresses when possible

Port Redirection Attack: Avoid It!



Typical Errors

- Allowing all DMZ types of traffic to all DMZ hosts
- Allowing connections from DMZ hosts to the inside
- Missing permit statements in ACL for complex protocols

  Application ports are not always easily predictable

  Use debug or log in your ACL to find out those port numbers

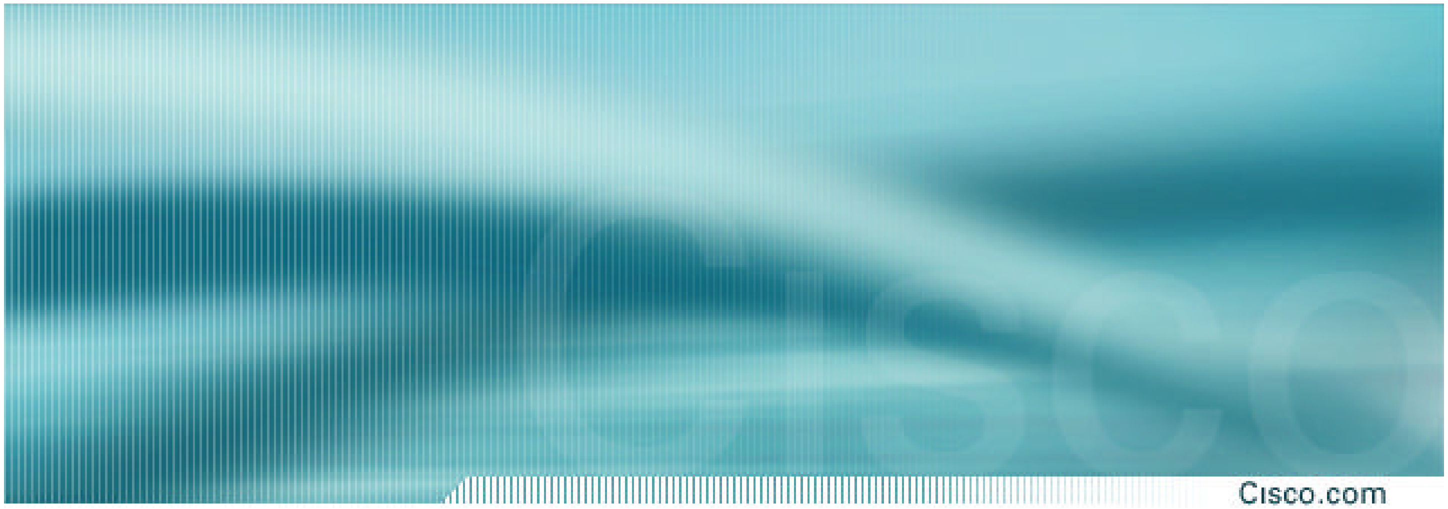
How Does This Protect Me?

- Someone compromising a single host on the DMZ will not be able to leverage that access
- If someone installs an agent for a DDOS attack, the output from your network will be limited to a very small amount
- If you’re the target for a DDOS attack, you will limit the bandwidth consumed by either ICMP or new sessions to a small percentage of your total bandwidth

Performance

Cisco.com

- Increased performance on your server hosts
- No additional impact on the router
- Access lists on PIX rely on its stateful engine which is very efficient



Securely Connecting Branch Offices

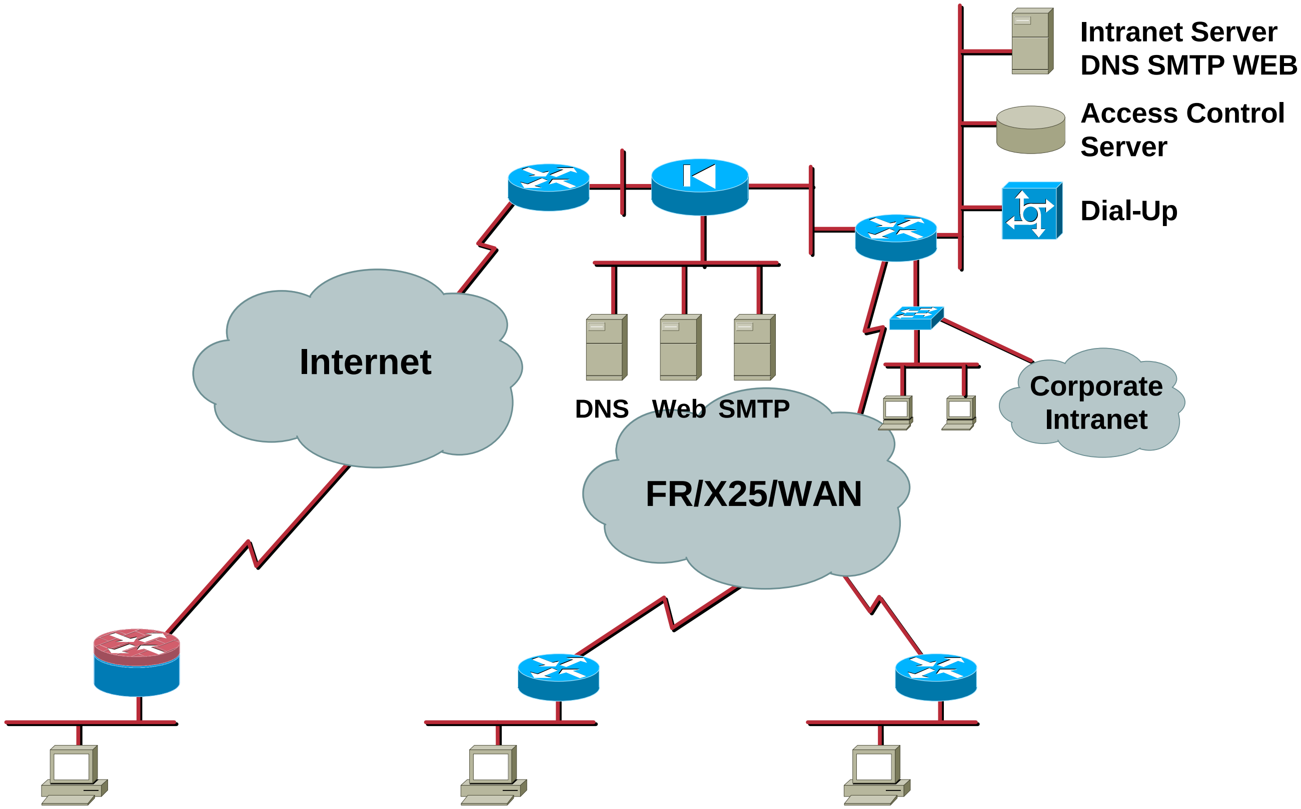
Requirements

- Use the Internet as alternative to expensive leased lines
- Protect networks of the branch offices from Internet attacks
- Protect corporate traffic across the Internet
- No direct branch to branch traffic

Tool Kit

- Stateful firewall for router
- LAN to LAN IPsec
- Dynamic tunnel settings

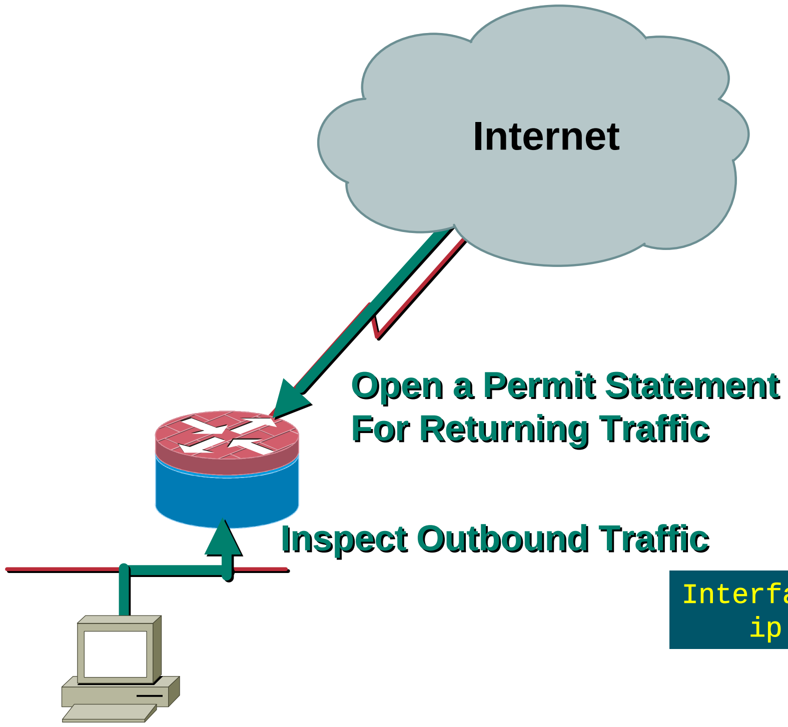
Connecting Remote Branches to the Internet: Configuring the Firewall



A Stateful Firewall on a Router

- Cisco IOS has a similar stateful engine as the PIX
- Unlike on the PIX, it is a binding between two interfaces
- Keep in mind a router was initially design to forward packets without restrictions

How Does It Work?



Open a Permit Statement For Returning Traffic

Inspect Outbound Traffic

```
interface Serial 0
    ip access-group 111 in
```

```
Interface Ethernet0/0
    ip inspect branchfirewall in
```

How Does It Work?

- Create an inspect rule for outbound flow
- Create an ACL denying all opposite direction traffic
- Every outbound packet is screen and dynamic inbound rule is “inserted” in the ACL

Where to Test? Where to Enforce? (Policy Is: Inside Secure, Outside Unsafe)

- If inbound ACL is applied outside:

  Inspect inbound traffic on the inside

  Or, inspect outbound traffic on the outside

- If outbound ACL is applied inside

  Inspect inbound traffic on the inside

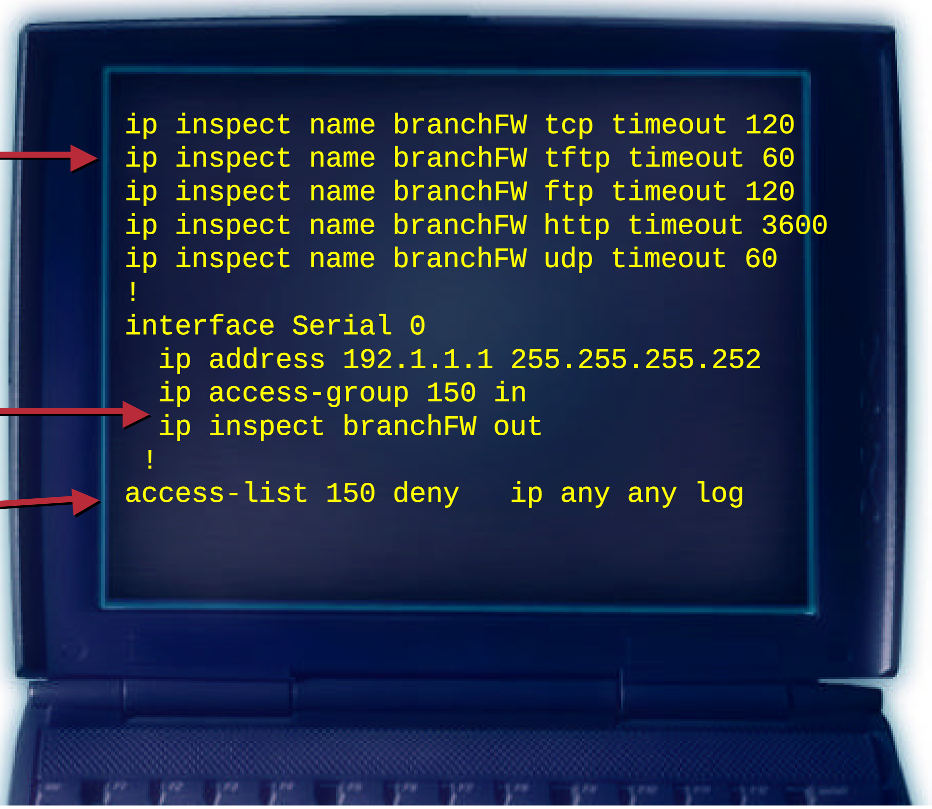
  Or, inspect outbound traffic on the inside

Branch Office Stateful Firewall Configuration

Create an Inspect Rule to Screen Outbound Traffic

Apply the Inspect Rule and the ACL on Opposite Flows (on the Same Interface, or on Separate Interfaces

Create a Very Restrictive ACL

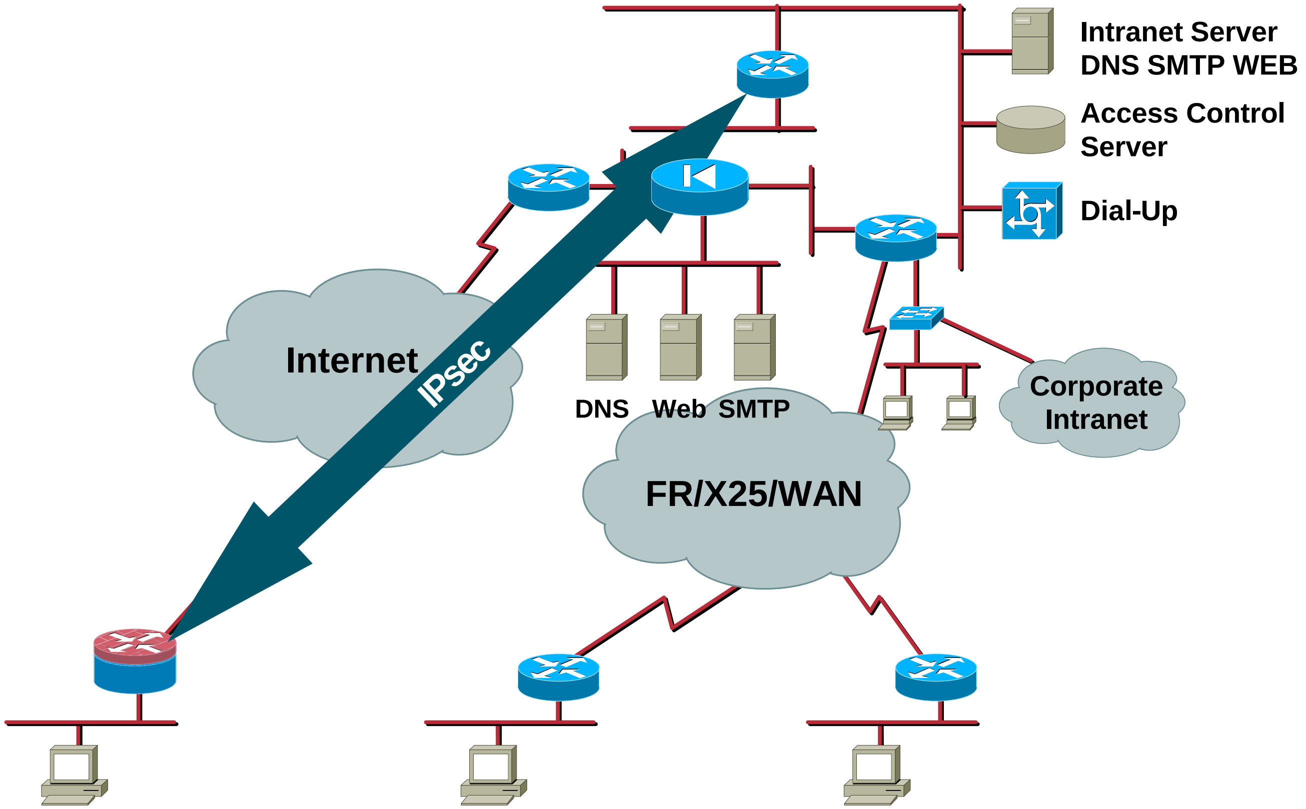


```
ip inspect name branchFW tcp timeout 120
ip inspect name branchFW tftp timeout 60
ip inspect name branchFW ftp timeout 120
ip inspect name branchFW http timeout 3600
ip inspect name branchFW udp timeout 60
!
interface Serial 0
  ip address 192.1.1.1 255.255.255.252
  ip access-group 150 in
  ip inspect branchFW out
 !
access-list 150 deny   ip any any log
```

Just Remember…

- Apply the inspect rule or the ACL on the appropriate interface
- Make sure you have the correct permits in the inbound access list for all non-inspected traffic you want to accept

Connecting Remote Branches to the Internet: Configuring VPN



Requirements

- Route all corporate traffic through the IPsec VPN
- Internet traffic goes directly out
- IPsec traffic should go through firewalls at branches and headquarters
- Route branch to branch traffic via headquarters

Challenges

- IPsec is supported on firewalls, routers, and specialized gateways
- Reuse existing equipment or introduce a dedicated system
- Where in the firewall system should you terminate the IPsec VPNs

Terminating IPsec on the External Router

- **Pros**

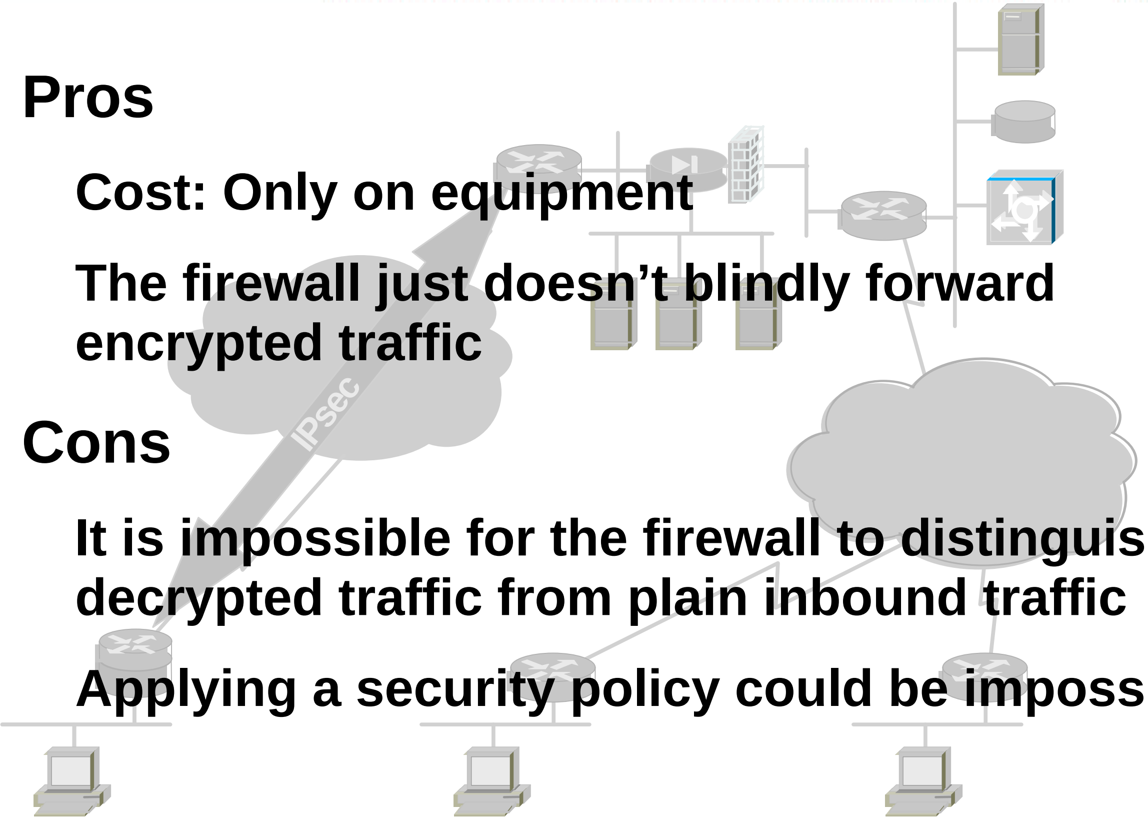
  Cost: Only on equipment

  The firewall just doesn’t blindly forward encrypted traffic

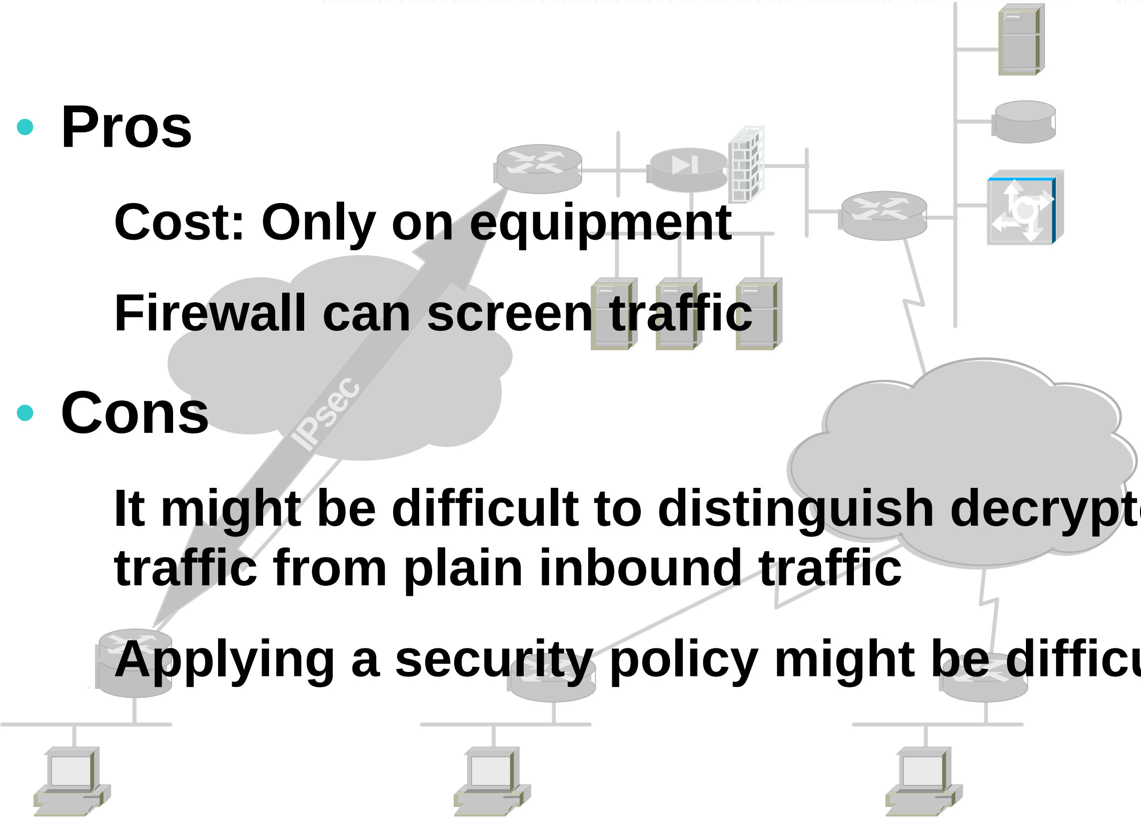
- **Cons**

  It is impossible for the firewall to distinguish decrypted traffic from plain inbound traffic

  Applying a security policy could be impossible



Terminating IPsec on the Firewall



- **Pros**

  Cost: Only on equipment

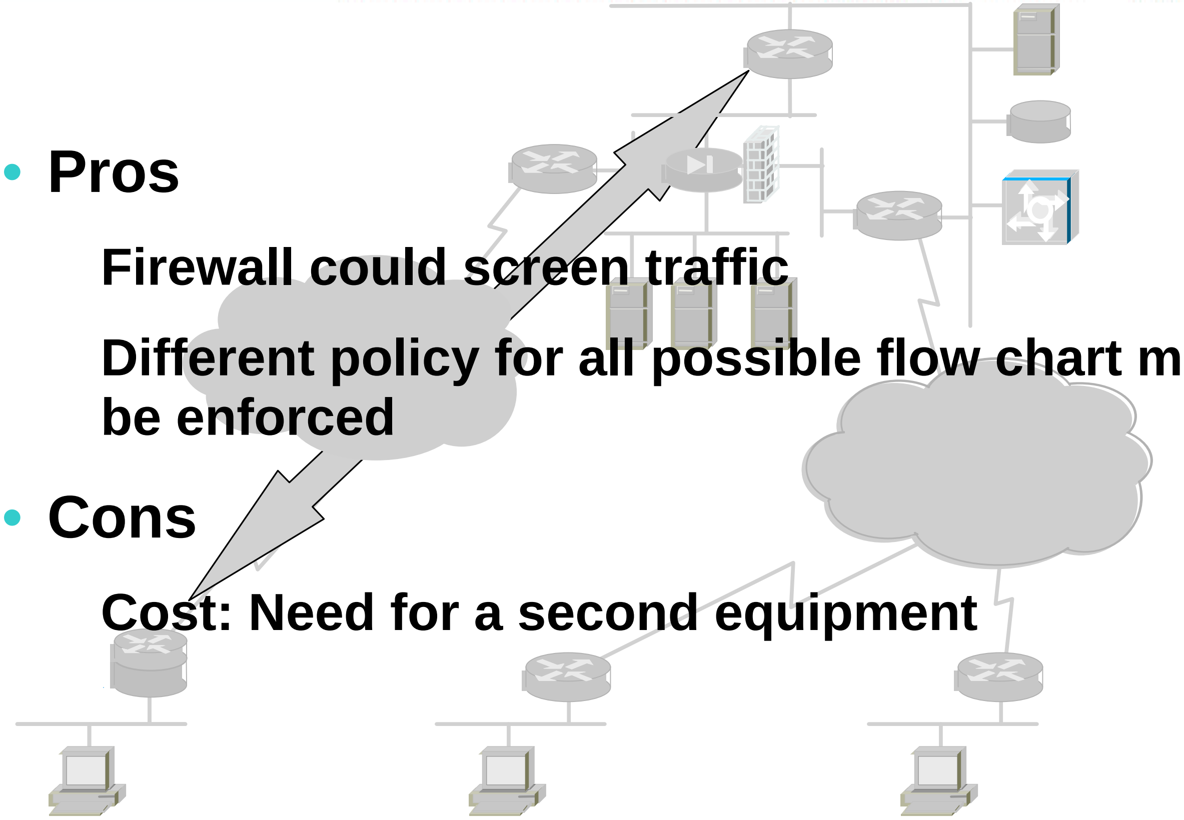
  Firewall can screen traffic

- **Cons**

  It might be difficult to distinguish decrypted traffic from plain inbound traffic

  Applying a security policy might be difficult

Terminating IPsec on a Dedicated Gateway Behind the Firewall



- **Pros**

  Firewall could screen traffic

  Different policy for all possible flow chart may be enforced

- **Cons**

  Cost: Need for a second equipment

IPsec Refresher

- Authentication

  Pre-shared key or PKI like

- Session management

  IKE (Internet Key Exchange), UDP port 500

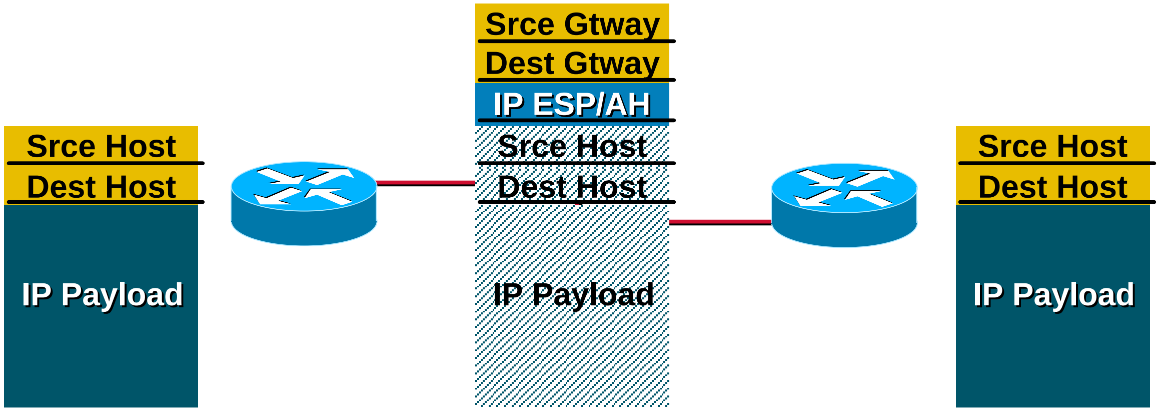
- Integrity services

  AH (Authentication Header), IP protocol 51

- Encryption services

  ESP (Encryption Security Payload), IP protocol 50

Identify Packet Headers Changes



- Depending where you test, you may:

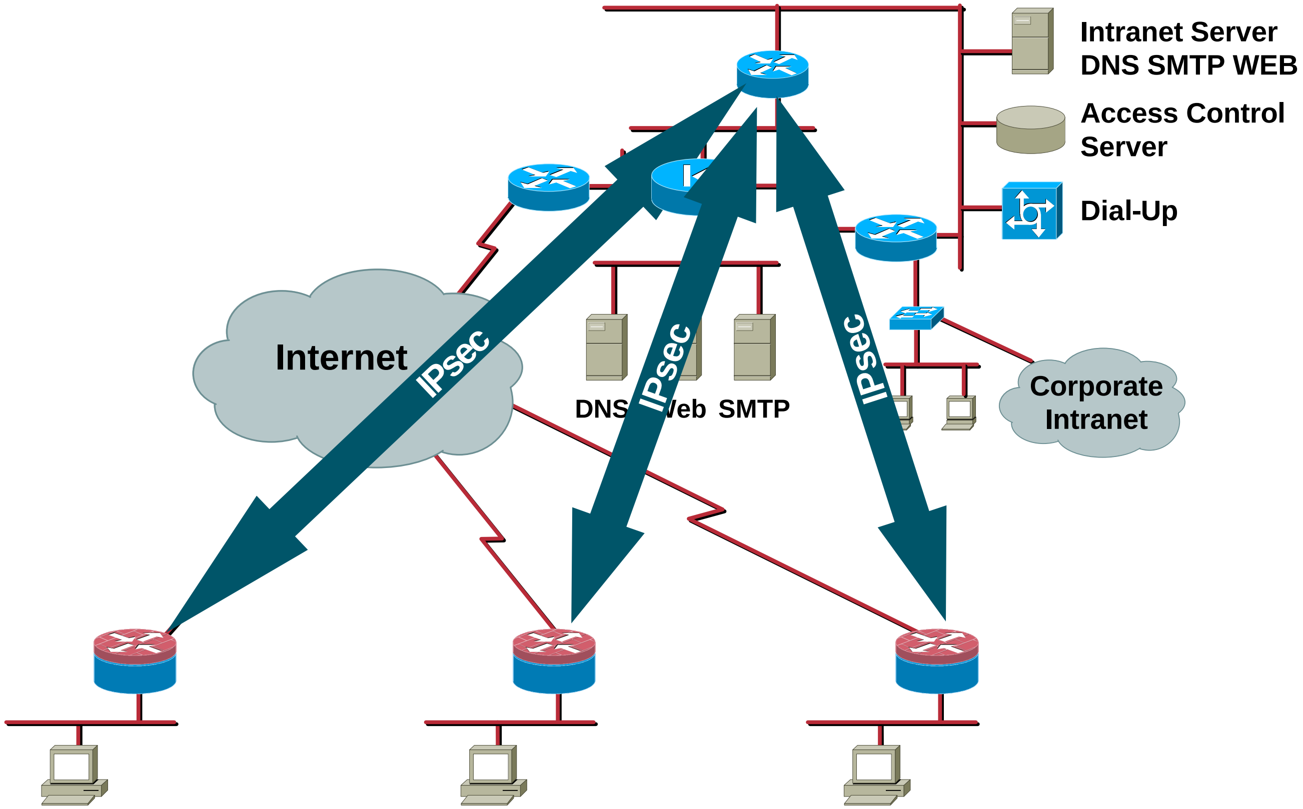
  Use host addresses and layer 4 protocol

  Use gateway addresses and layer 3 protocol

IPsec Is a Contract between Two Gateways

- Need to know who your peers are
- Agree on how to protect data
- Be able to link packets to peers

Hub and Spoke Topology



Key Points

Cisco.com

- Enable IOS FW on branch router
- Traffic direction
  - Both directions
  - Branch to corporate
- Device authentication
  - Pre-shared key with/without central DB
  - Certification authority

Traffic Flow

- Conversations can be initiated from branch office or from headquarters

  Require static crypto map on all routers

- Direct branch to branch encrypted traffic is not possible

  Goes via headquarters gateway

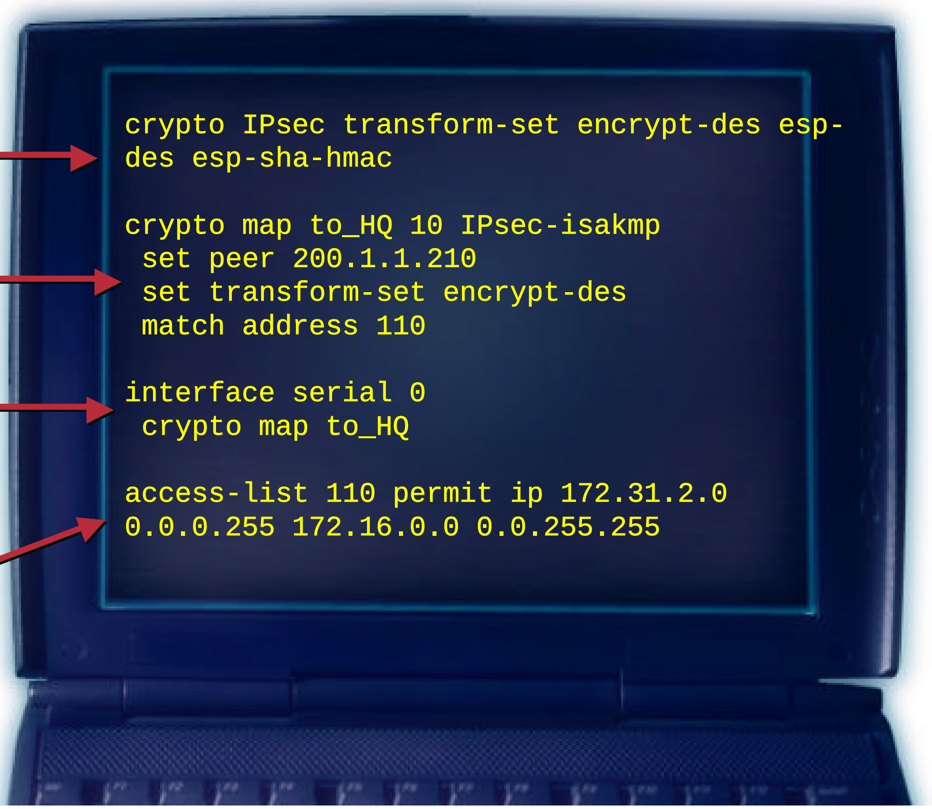
Branch Office Crypto Configuration

Create a Confidentiality/ Integrity Rule

Create a Crypto Map That Binds a Specific Flow to One Peer

Apply the Crypto Map to the Outbound Interface

Create an ACL to Select the Traffic to Be Encrypted

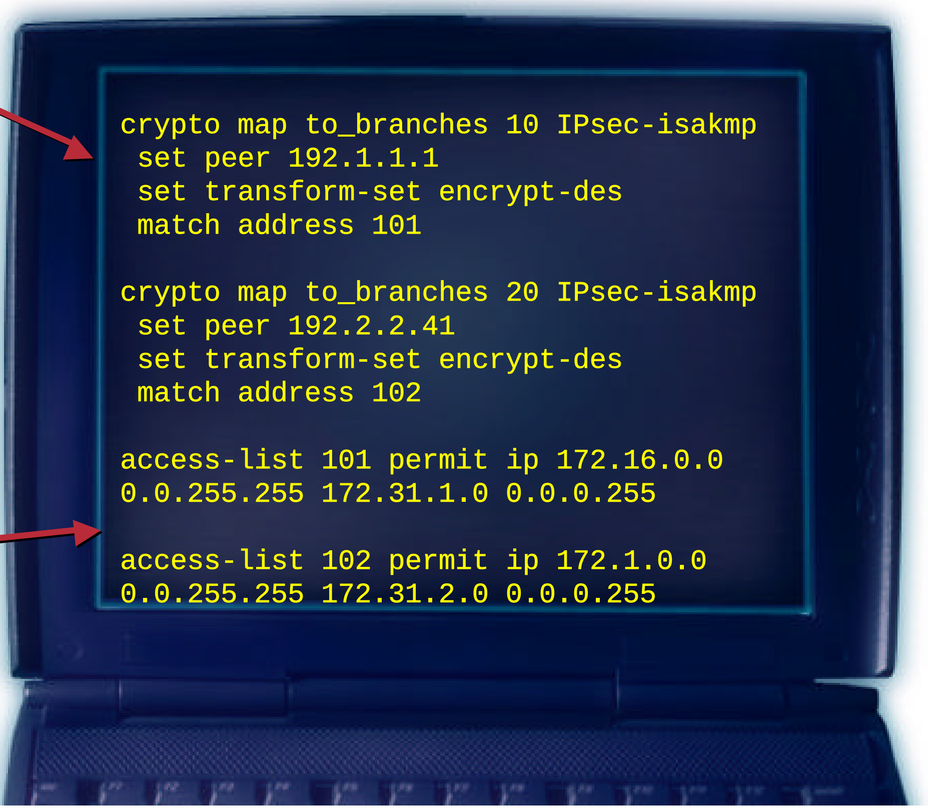


```
crypto IPsec transform-set encrypt-des esp-
des esp-sha-hmac

crypto map to_HQ 10 IPsec-isakmp
 set peer 200.1.1.210
 set transform-set encrypt-des
 match address 110

interface serial 0
 crypto map to_HQ

access-list 110 permit ip 172.31.2.0
0.0.0.255 172.16.0.0 0.0.255.255
```

Headquarters Crypto Configuration

Create a Crypto Map with Multiple Sequence Number That Binds a Specific Flow to One Specific Peer

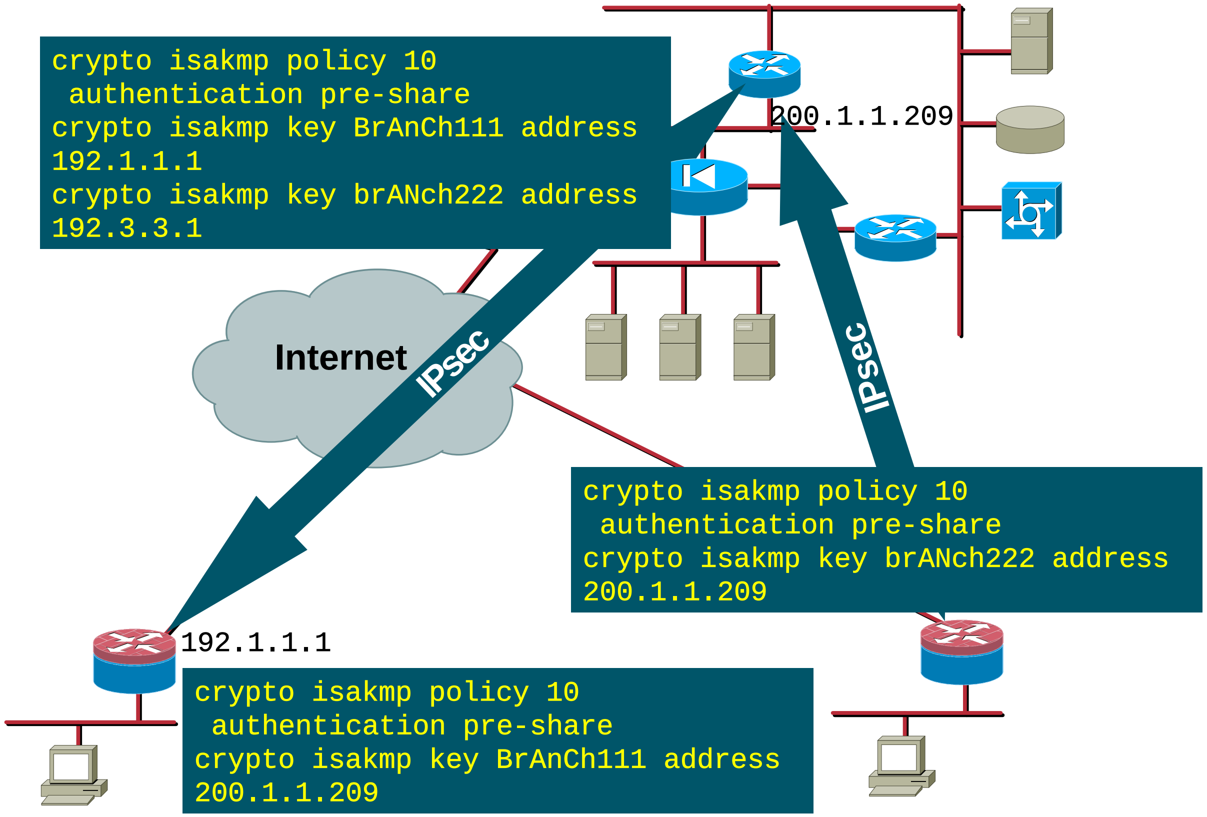
Create ACL to Select the Traffic to Be Encrypted for Each Possible Flows



```
crypto map to_branches 10 IPsec-isakmp
 set peer 192.1.1.1
 set transform-set encrypt-des
 match address 101

crypto map to_branches 20 IPsec-isakmp
 set peer 192.2.2.41
 set transform-set encrypt-des
 match address 102

access-list 101 permit ip 172.16.0.0
0.0.255.255 172.31.1.0 0.0.0.255

access-list 102 permit ip 172.1.0.0
0.0.255.255 172.31.2.0 0.0.0.255
```

Configure Authentication: Pre-Shared Keys

Cisco.com

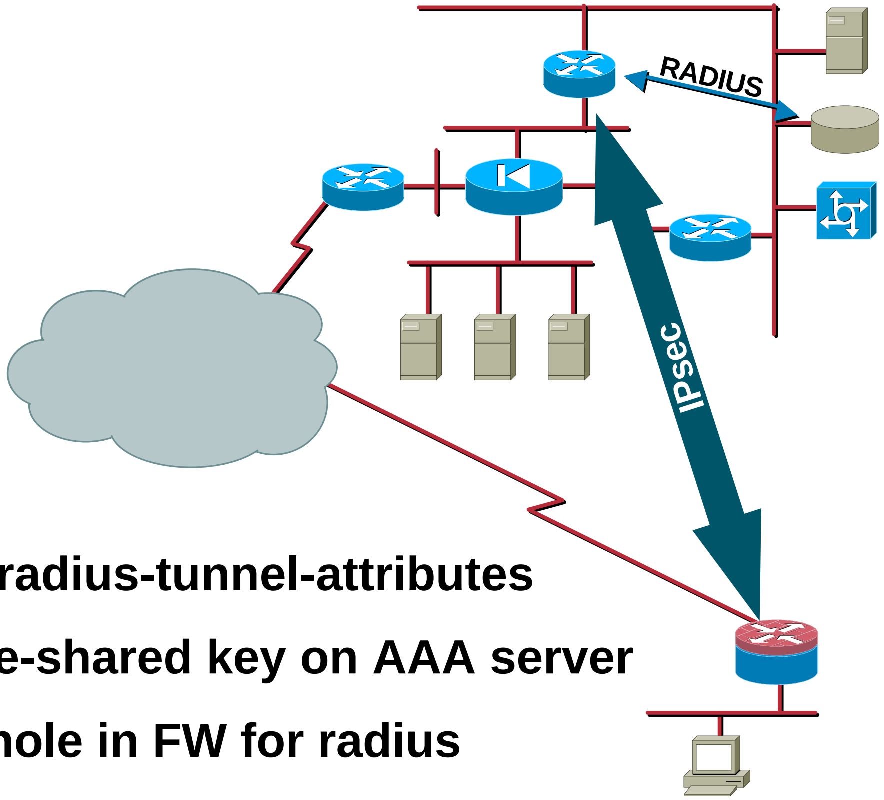


```
crypto isakmp policy 10
 authentication pre-share
crypto isakmp key BrAnCh111 address
192.1.1.1
crypto isakmp key brANch222 address
192.3.3.1
```

```
crypto isakmp policy 10
 authentication pre-share
crypto isakmp key brANch222 address
200.1.1.209
```

```
crypto isakmp policy 10
 authentication pre-share
crypto isakmp key BrAnCh111 address
200.1.1.209
```

IKE Pre-Shared Secret via AAA



- Use the radius-tunnel-attributes
- Store pre-shared key on AAA server
- Open a hole in FW for radius

Crypto Configuration Summary

- Each branch as the same template but the source address in the ACL
- Headquarters need one crypto map entry per branch
- Any change at a branch (new address space, new branch) requires an update on headquarters router
- Crypto map ACL need to be symmetric

What about Routing?

- Current rules are default static routes
- Packet is routed to outside interface regardless of the destination
- If packet matches the crypto map it is encapsulated in a new packet with peer address
- IPsec packet is routed out
- True from headquarters as well as from branches

Typical Errors

- **Branch to branch traffic does not trigger ACL**
- **Multiple ACL overlap**
- **Decrypting/re-encrypting packet on same interface**

  Cisco IOS SADB does not keep track of ACL srce/dest order

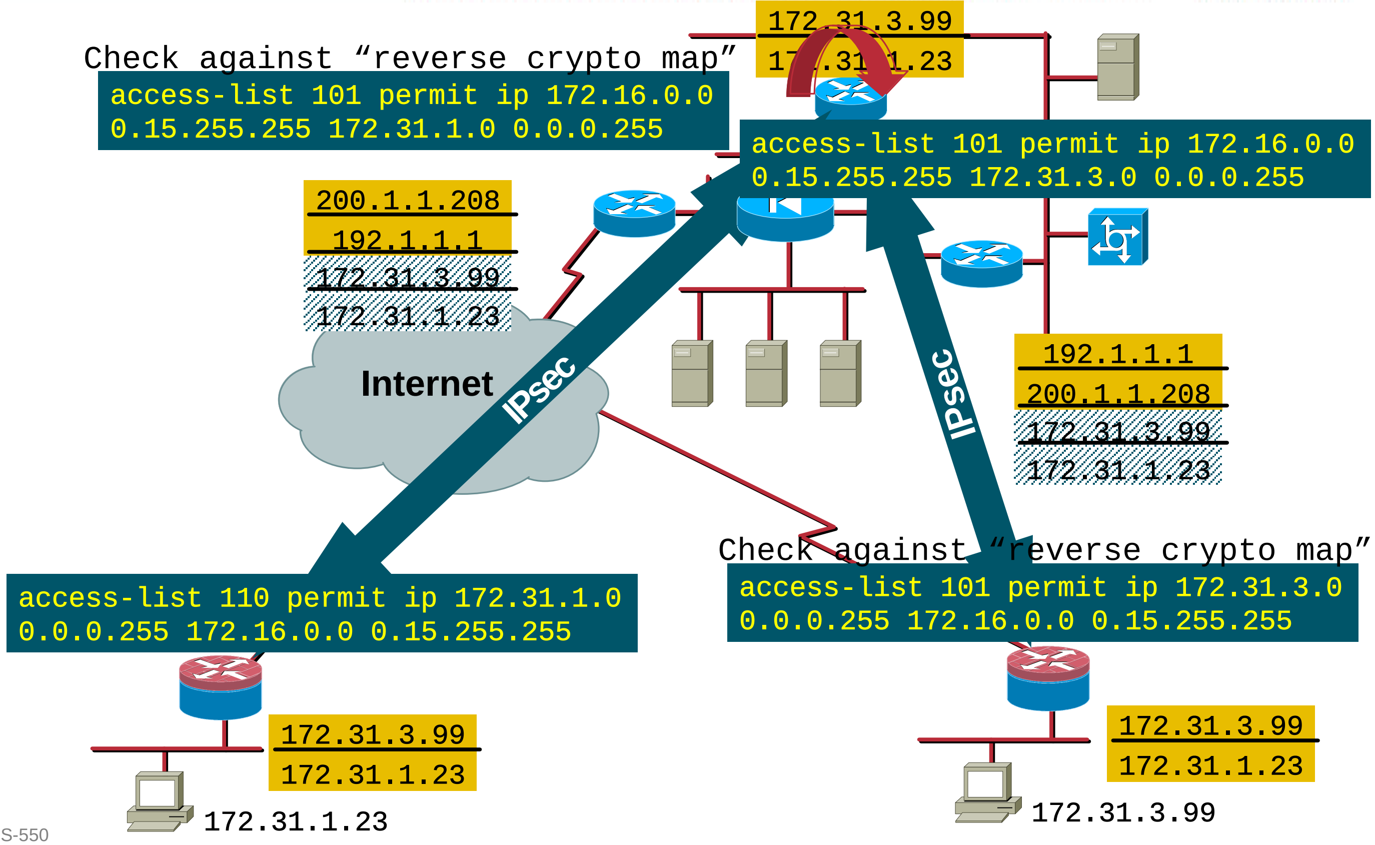
Typical Errors (Cont.)

- Wrong peer address for pre-shared keys or tunnels
- Transform-set or IKE policy mismatch
- Forget to update Ingress ACL to allow encrypted traffic in
- Incomplete Ingress ACL
  - Allow IPsec from specific source
  - Allow decrypted traffic in

Branch to Branch Does Not Trigger ACL

- **172.16.0.0/16 is restrictive to headquarters**
- **Change it to 172.16.0.0/12 which includes all branches address space**
- **Keep in mind ACL cannot overlap**

Branch to Branch Traffic



Check against “reverse crypto map”

```
access-list 101 permit ip 172.16.0.0
0.15.255.255 172.31.1.0 0.0.0.255
```

```
access-list 101 permit ip 172.16.0.0
0.15.255.255 172.31.3.0 0.0.0.255
```

Check against “reverse crypto map”

```
access-list 101 permit ip 172.31.3.0
0.0.0.255 172.16.0.0 0.15.255.255
```

```
access-list 110 permit ip 172.31.1.0
0.0.0.255 172.16.0.0 0.15.255.255
```

Update Your ACL: Headquarters External Router

Cisco.com

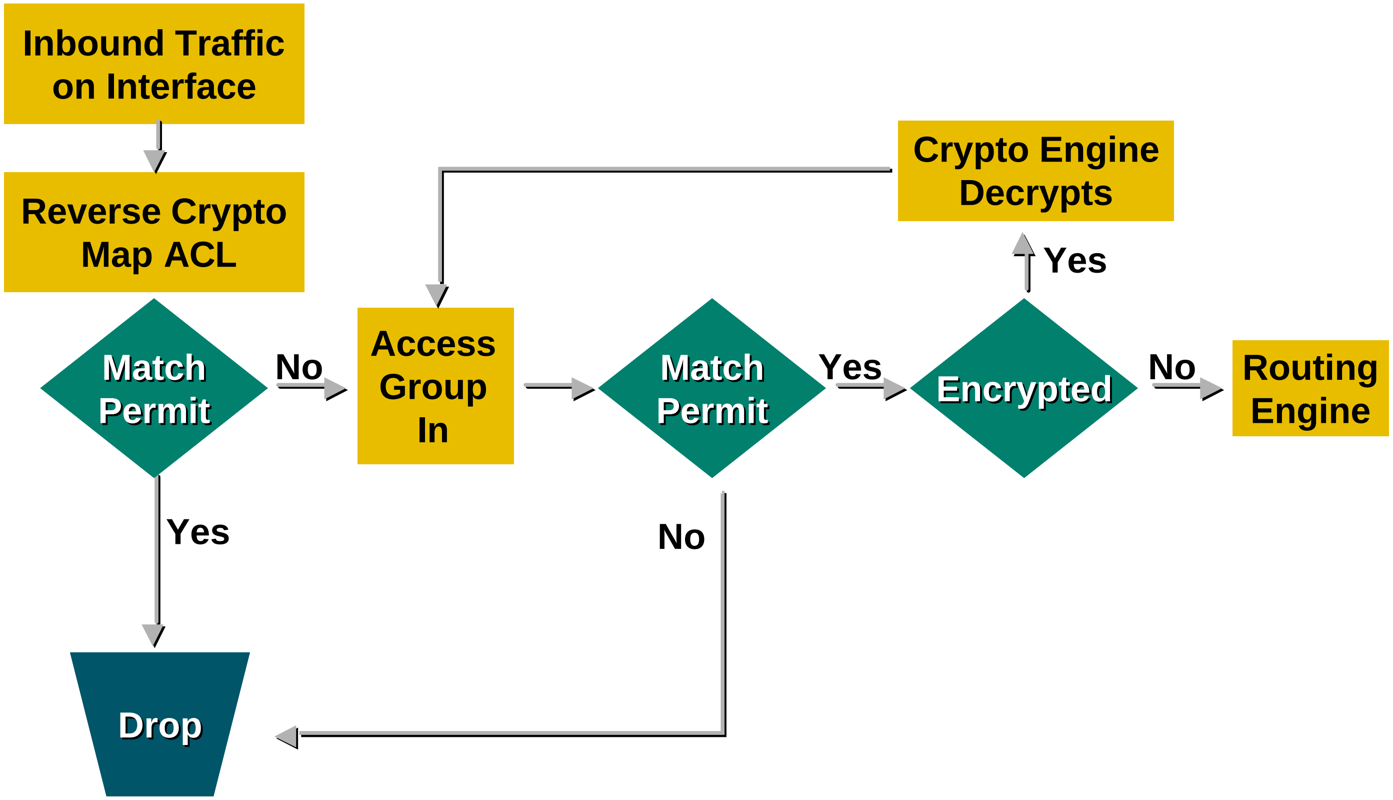
- **Filtering inbound IPsec packets with IOS ACLs**

ISAKMP

```
access-list 111 permit udp any eq 500 host 200.1.1.208 eq 500
access-list 111 permit esp any host 200.1.1.208
```

- **For increased security you may replace “any” by the peers exact addresses**
- **Make sure to insert those line before the “deny any any” statement**

ACL and Crypto Packet Flow



Update Your ACL: Headquarters External Router

- Add all “reverse crypto maps” to the ingress ACL

```
access-list 111 permit ip 172.31.1.0 0.0.0.255 172.16.0.0 0.15.255.255
access-list 111 permit ip 172.31.2.0 0.0.0.255 172.16.0.0 0.15.255.255
access-list 111 permit ip 172.31.3.0 0.0.0.255 172.16.0.0 0.15.255.255
...
```

- There is no security issue since if such a packet comes in, it will be discarded by the first crypto test
- Make sure to insert those lines before the “deny any any” statement

Update Your ACL: Stateful Firewall

- **Filtering inbound IPsec packets with PIX ACLs**

```
access-list toservers permit udp any eq 500 host 200.1.1.208 eq 500
access-list toservers permit 50 any host 200.1.1.208
```

ESP

- **For increased security you may replace "any" by the peers exact addresses**

Update Your ACL: Branch Office Routers

- Add all “reverse crypto maps” to the ingress ACL
- Allow IPsec and IKE through

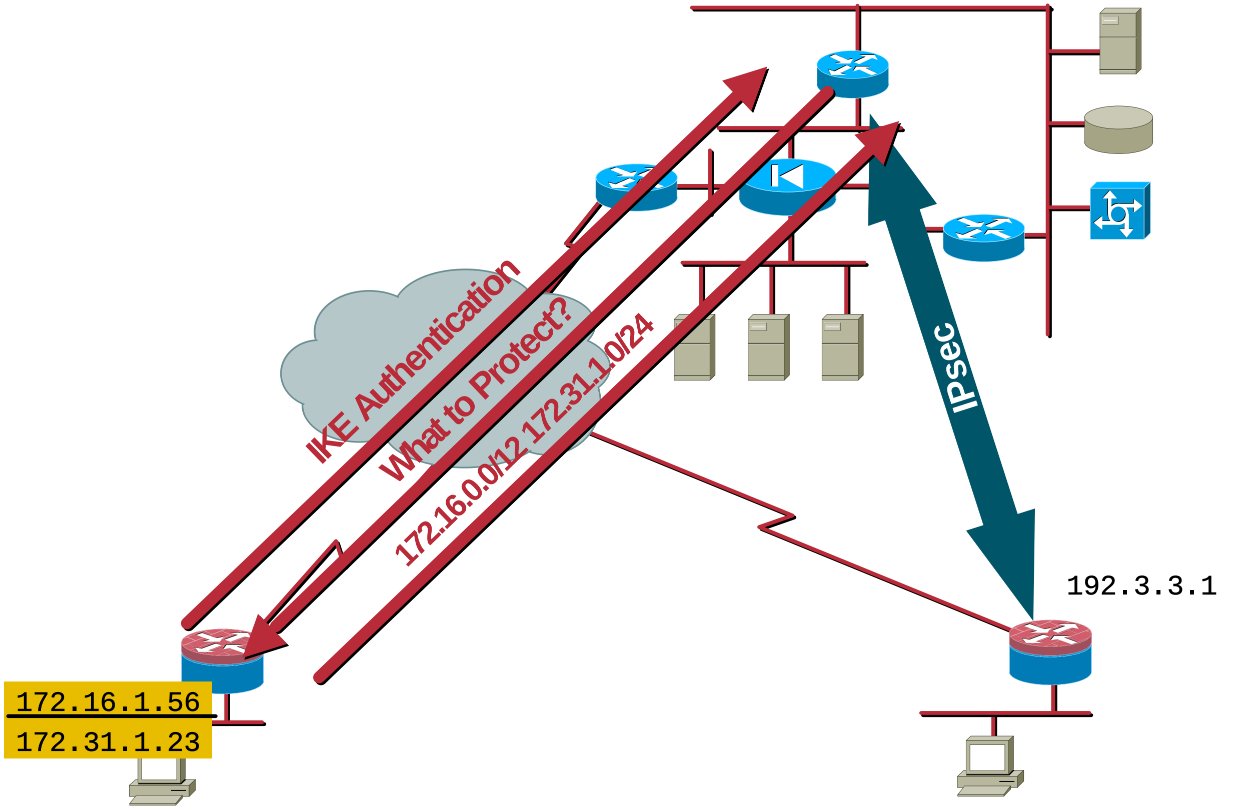
```
access-list 150 permit ip 172.16.0.0 0.15.255.255  172.31.1.0 0.0.0.255
access-list 150 permit esp host 200.1.1.208 host 192.1.1.1
access-list 150 permit udp host 200.1.1.208 eq isakmp host 192.1.1.1 eq isakmp
```

- Make sure to insert those line before the “deny any any” statement

Simplifying the Headquarters Configuration

- On headquarters router, one static crypto map per branch doesn't scale
- Branch office configuration is OK as it is the same template for all of them
- Dynamic crypto map allows an IPsec to learn its settings from its peer if authentication is successful

Hub and Spoke: Upstream Traffic Only



Headquarters Crypto Configuration

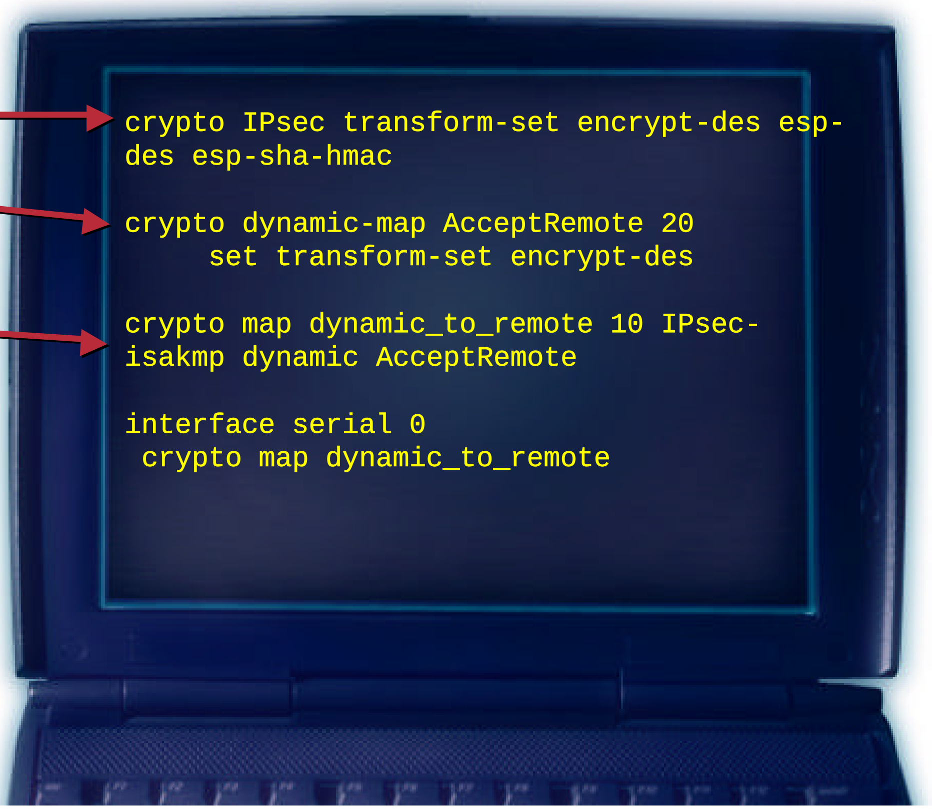
Transform-Set Must Exist on Both Ends

Create a Dynamic Crypto Map Template

Create a Crypto Map Using This Template

Only Remote Routers Can Establish IPsec

Remote Routers Configuration Remains the Same



```
crypto IPsec transform-set encrypt-des esp-
des esp-sha-hmac

crypto dynamic-map AcceptRemote 20
     set transform-set encrypt-des

crypto map dynamic_to_remote 10 IPsec-
isakmp dynamic AcceptRemote

interface serial 0
 crypto map dynamic_to_remote
```

Performance

- Maximum number of tunnels
- Maximum encrypted bandwidth
- IKE start up latency
- Concurrent IKE negotiation

Just Remember…

- IOS inspect must be applied to the correct interface—Access list combination
- Make sure to authorize IPsec through various firewalling devices
- IKE parameters must be exactly the same on both endpoints
- Access lists must be symmetrical on both endpoints

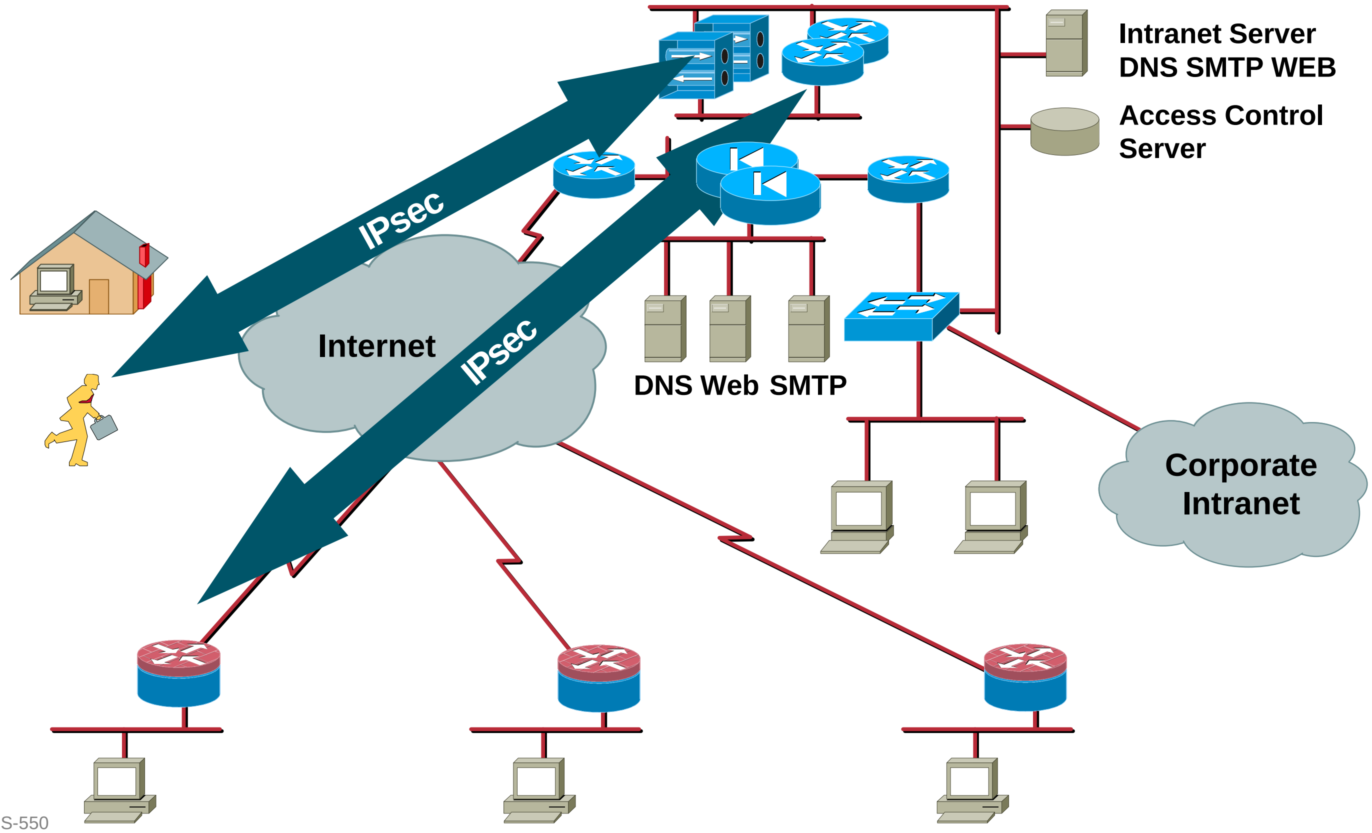
How Does This Protect Me?

- Sensitive traffic is encrypted and safe from sniffers
- Stateful firewall controls clear text traffic
- It is ok to let the IPsec traffic through the firewall because the protocol provides us enough assurance of its origin and integrity

Securely Connecting Mobile Users

Connecting Mobile Users

Cisco.com



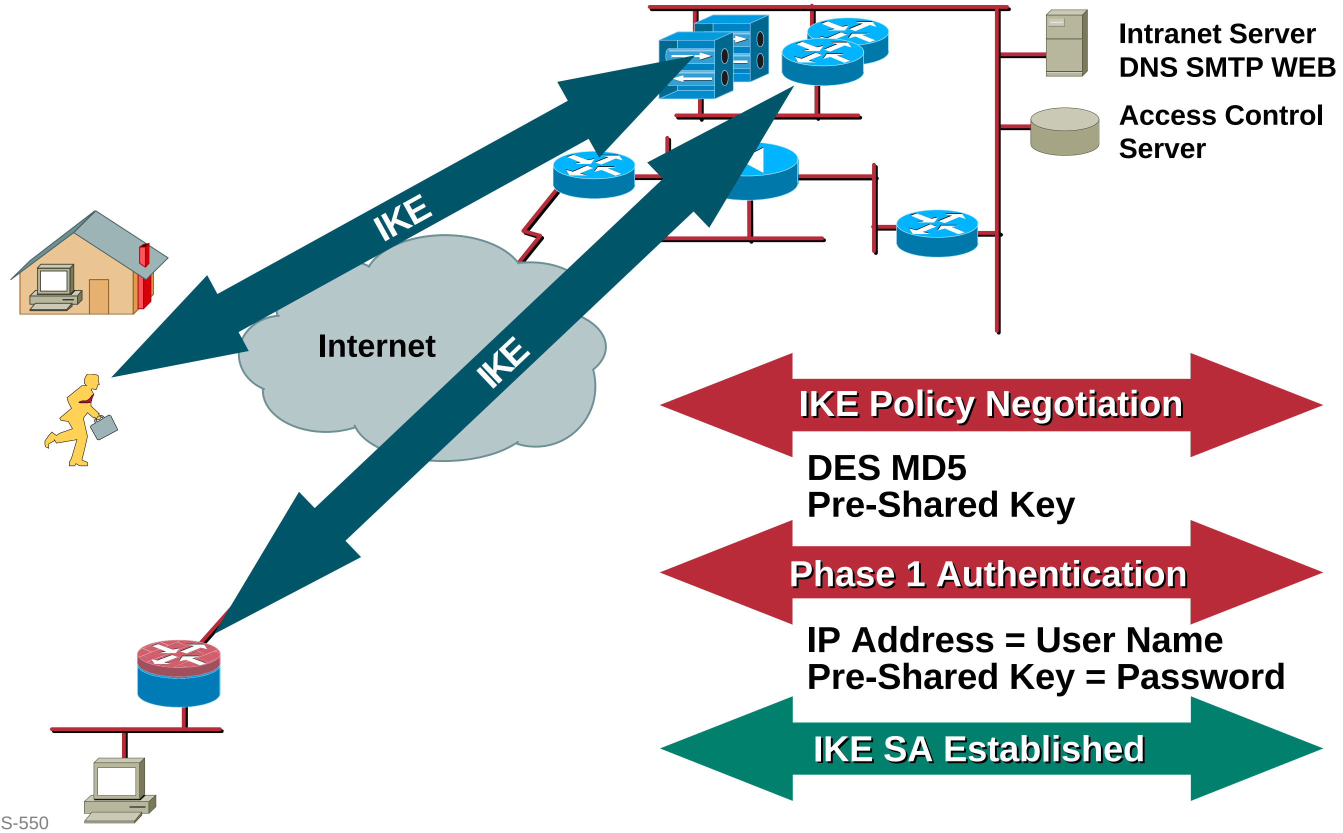
Requirements

- Provide world-wide mobility securely
  - Hotels, tradeshows, Internet café, wireless airport LANs
- Enforce strong user authentication
- Secure the corporate traffic across the Internet
- Support on-demand and always-on access
  - xDSL, cable, ISDN, wireless

Tool Kit

- Client or LAN initiated IPsec VPN
- IPsec user authentication
- Wildcard pre-shared keys or certification authority
- SOHO device with or without routing capabilities

IPsec Phase 1: IPsec Main Mode Authentication



IKE Policy Negotiation

DES MD5
Pre-Shared Key

Phase 1 Authentication

IP Address = User Name
Pre-Shared Key = Password

IKE SA Established

IPsec Main Mode Authentication

Cisco.com

- Authenticates a device

  Not the PC users!

- Authentication is based on one of the following:

  IP address or fully qualified domain name (FQDN) and pre-shared key

  IP address or FQDN and public/private key

  Digital certificate

- Pre-shared or private keys are never transmitted

IPsec Phase 1: Weakening IKE Main Mode

- RFC 2409 requires a unique IP address to be associated with each pre-shared key

    This is for good security

    But prevents the use of dynamic IP addresses

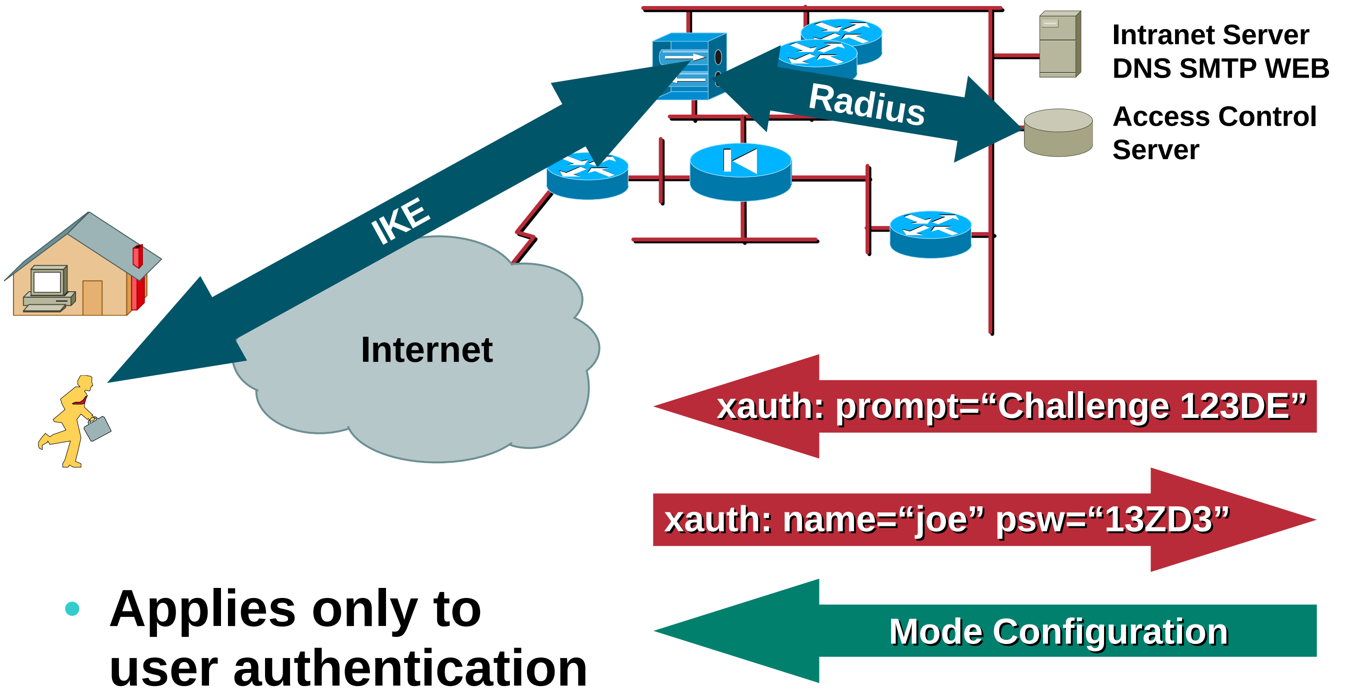
    Hence cannot use a dial client

Weakening IKE (Cont.)

- It is possible to use the same pre-shared key for a large range of IP addresses
- The most unsecured would be to use the same password for all IP addresses:

```
crypto isakmp key sameFORall address 0.0.0.0 255.255.255.255
```

IPsec Phase 1 (optional): IPsec Extended Authentication



xauth: prompt="Challenge 123DE"

xauth: name="joe" psw="13ZD3"

Mode Configuration

IP Address, DNS, WINS

- Applies only to user authentication

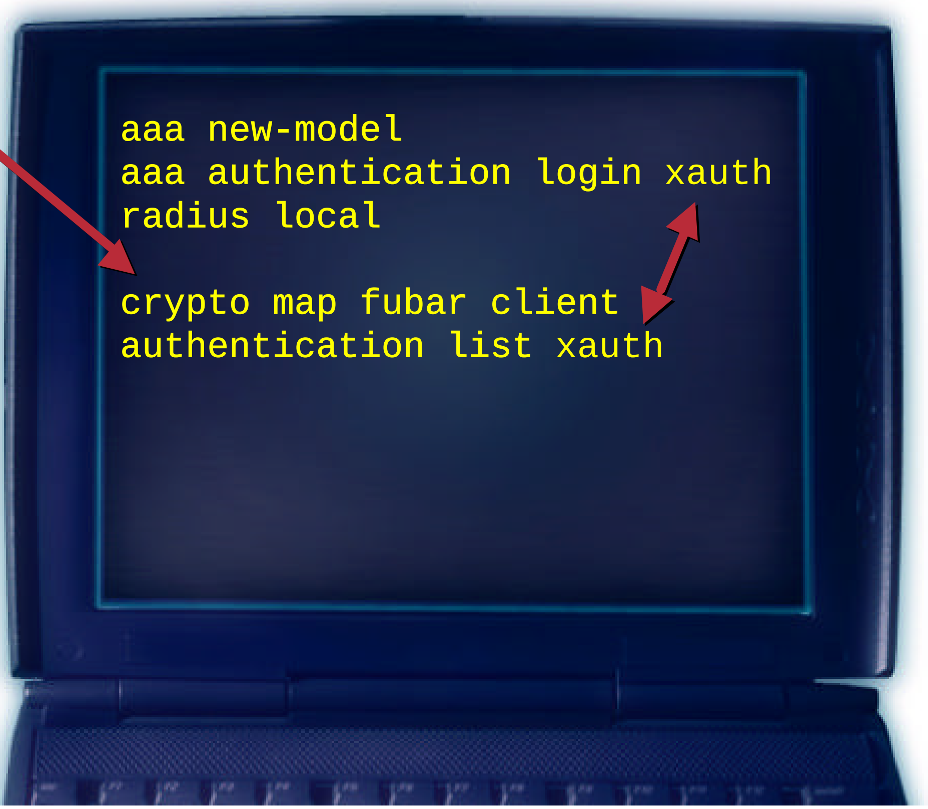
IPsec User Authentication (xauth)

- Allows authenticating a user after authenticating the gateway (e.g. the PC)
- Provides good authentication where certificates cannot be used
- Solves the issue of not knowing the IP address in advance

IPsec Extended Authentication with Radius

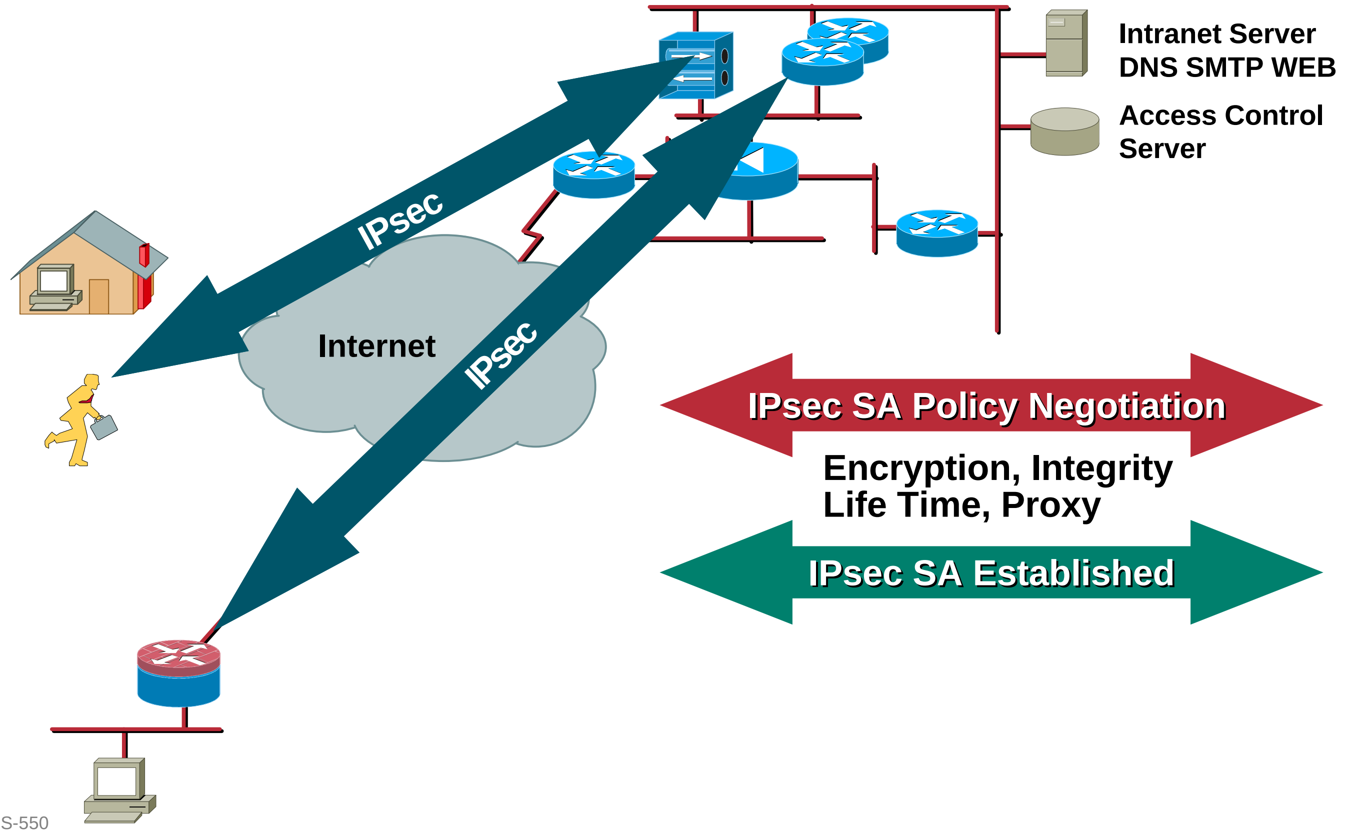
Crypto Map Is for Client Authentication

Beware That If a Remote Router Running Older Versions of IOS Tries to Connect, It Might Refuse xauth and therefore IPsec Will Not Come up



```
aaa new-model
aaa authentication login xauth
radius local

crypto map fubar client
authentication list xauth
```

IPsec Phase 2: IPsec Quick Mode

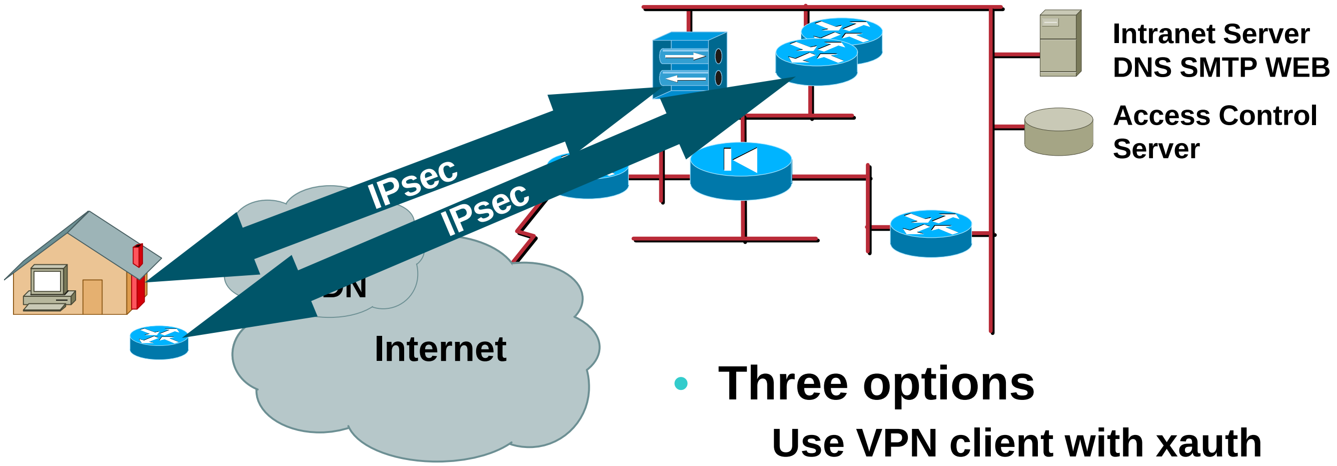


IPsec SA Policy Negotiation

Encryption, Integrity
Life Time, Proxy

IPsec SA Established

Connect Home Office



- Three options
  - Use VPN client with xauth
  - Use a local VPN hardware
  - Use a local router for LAN to LAN VPN
- Internet traffic
  - All through the tunnel
  - Split tunneling

Home VPN Termination

- Using a PC is identical to Internet cafe access
- For multiple home PC use a “VPN hardware client”
- For more complex scenarios, specifically dial, use a VPN router

Complex Home Office Connections: ISDN

- Keep link down when no traffic!
- Dynamic addresses
- SA life time must be equal to connection duration

  Need to use IKE keepalive to reset SPI after ISDN went down

  IKE keepalive must not keep ISDN up and cannot be filtered

- Time source with digital certificates

Keep Alive for Dialup

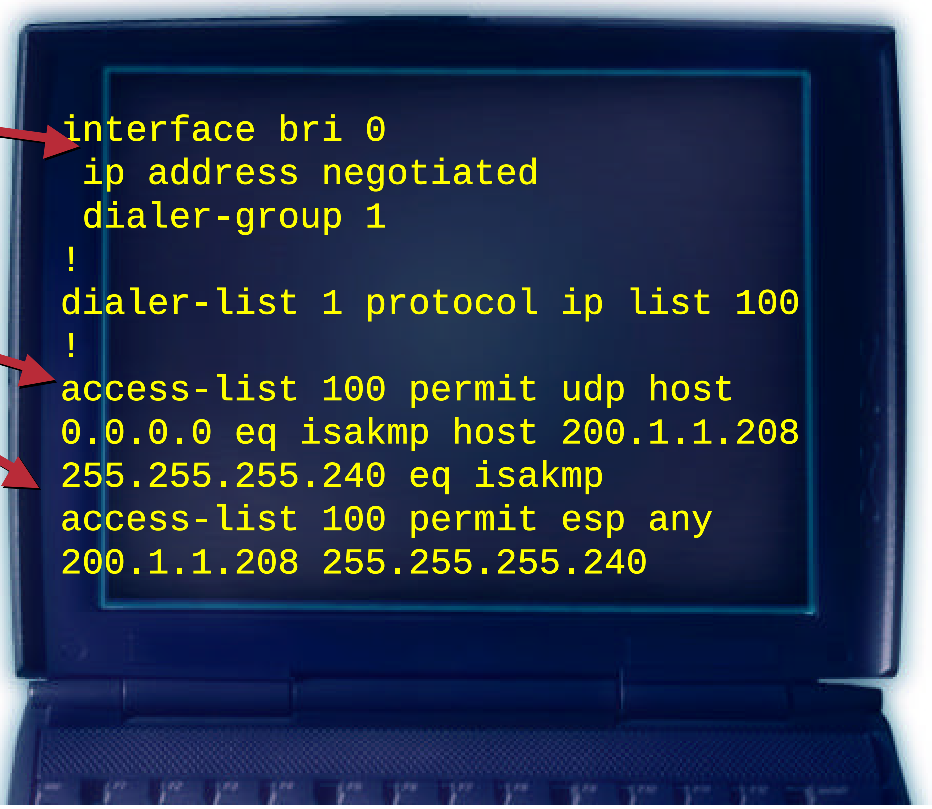
- IKE must be able to trigger the link
- Keep alive cannot be separated from other IKE packets
- Plain IKE keepalive will keep ISDN/DDR line up
- Work-around for negotiated address dial on demand routing (DDR)
    - The first packet of IKE phase 1 has a source IP address of 0.0.0.0
    - All other IKE packets have a real IP address

DDR and IKE Keep Alive

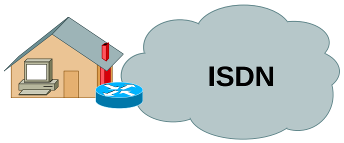
IP Address for the ISDN Interface Is Allocated by ISP

Interesting traffic that can trigger dial is:

- Either first packet of IKE
- Or ESP encrypted data traffic



```
interface bri 0
 ip address negotiated
 dialer-group 1
!
dialer-list 1 protocol ip list 100
!
access-list 100 permit udp host
0.0.0.0 eq isakmp host 200.1.1.208
255.255.255.240 eq isakmp
access-list 100 permit esp any
200.1.1.208 255.255.255.240
```



Other Issues with DDR

- Digital authentication (CERT) requires the router to know the date
- Must use NTP to re-sync after power cycle (some device don’t have permanent time)
- NTP cannot maintain the dial link up ==> use time-based ACL

Small Routers and CERTs

- Small routers have no clock and lose time on power reset/reload
- IOS checks its own X.509 certificates validity at start-up while the clock is still at 1993 => own certificate is rejected
- ==> work around is needed

Configure NTP over Dialup Interfaces

- Configure NTP
- Use time-based ACL to define NTP as interesting traffic when year is 1993
- Denied NTP traffic to be encrypted

  No need for confidentiality: UTC is public!

  Integrity and authentication built-in NTP
- Store the router certificate on the CA (CERT will not be valid at start time)

```
crypto ca certificate query
```

Time-Based ACL

```
interface bri 0
   dialer-group 1
!
dialer-list 1 protocol ip list 101
!
Time-range NTP_startup end 12:00 1 January 2000
!
access-list 101 permit ip any time-range NTP_startup
```

- **At start-up, date is Jan 1st 1993**
- **NTP can trigger the ISDN link**
- **After 3 NTP packets the clock will be in sync and NTP won’t trigger ISDN again**

Internet Traffic

- All traffic goes into the IPsec tunnel
  - Doubles traffic at headquarters (gets in encrypted and out to the Internet)
  - Increase CPU impact
  - Single point of control
- Split tunneling
  - Corporate traffic goes into VPN, Internet traffic goes to local ISP
  - Home office may be used to redirect traffic into VPN

Performance

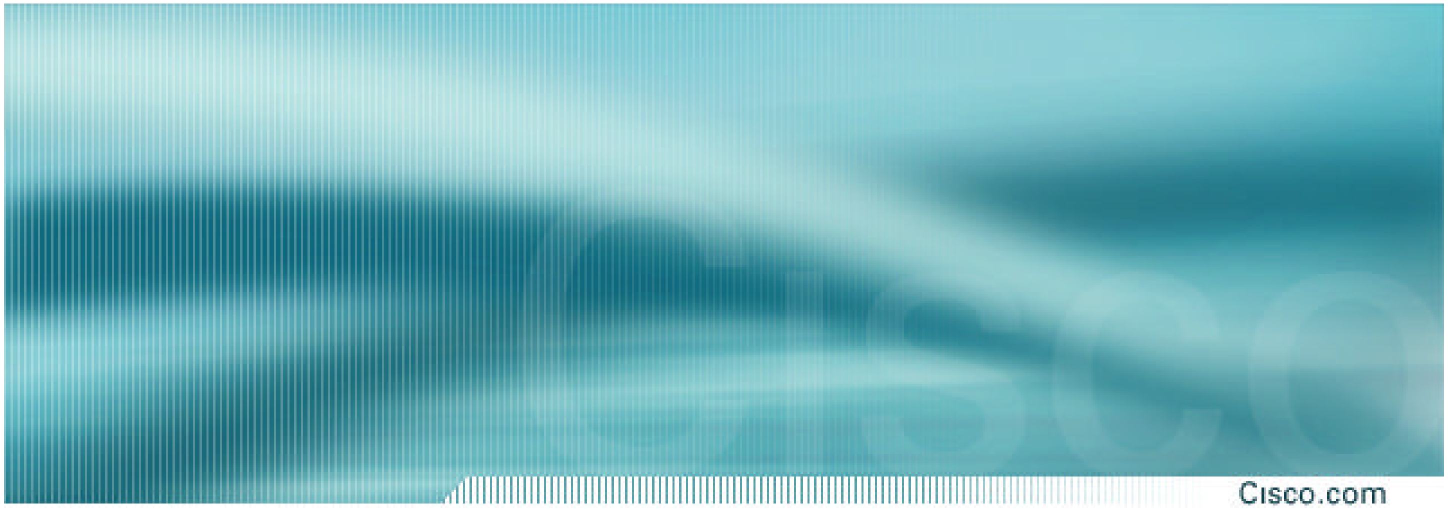
- On the remote system performance is not affected
- On the central termination device, there may be 1000+ VPNs
  - Must provide adequate bandwidth per user
  - May need hardware acceleration

Just Remember…

- Make sure you authorize NTP traffic on your inbound access lists
- IKE keepalives cannot be filtered if you are using fixed BRI interface addresses
- When using split tunneling, make sure you have good firewalling either on the PC or on the IPsec termination device

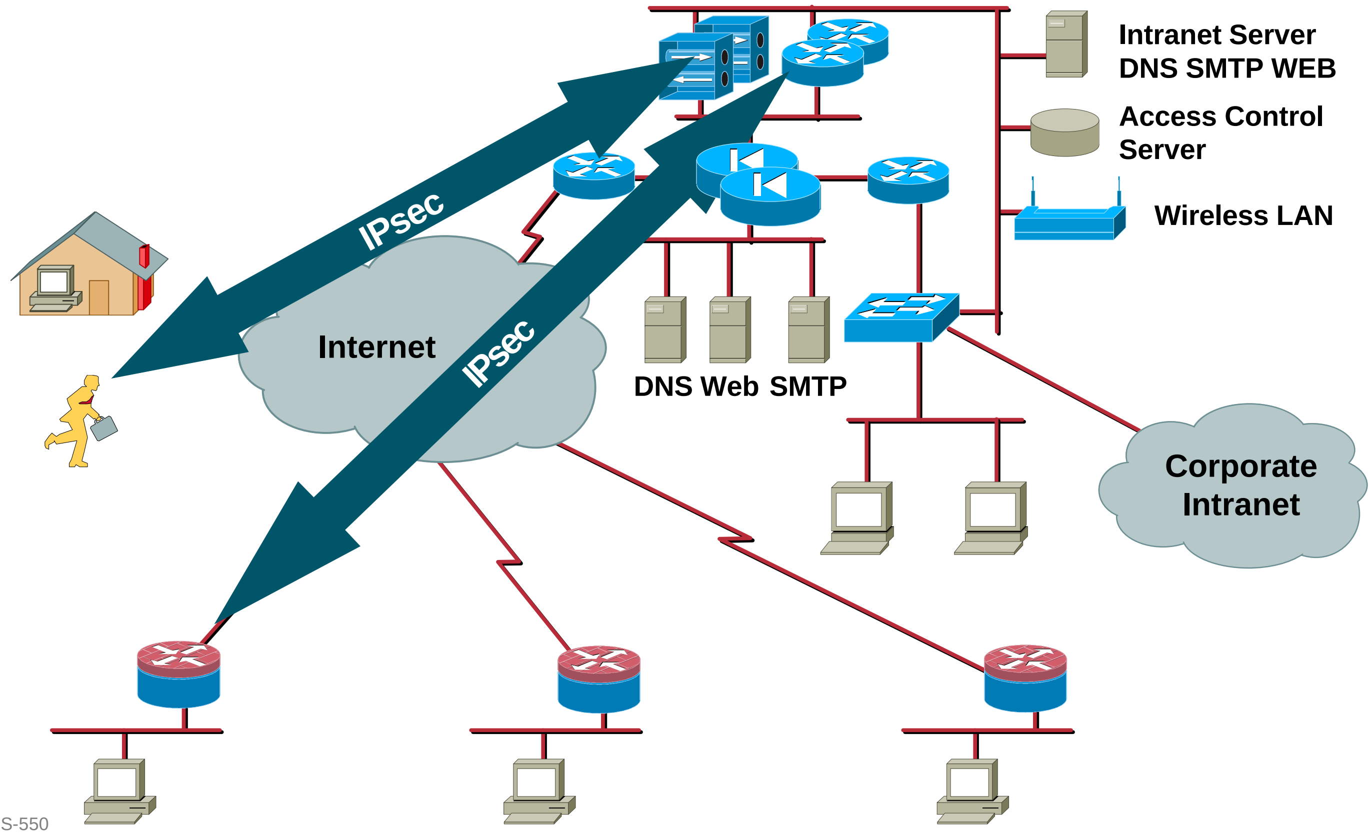
How Does This Protect Me?

- Strong authentication is possible
- Network traffic is secured from sniffers on foreign LANs



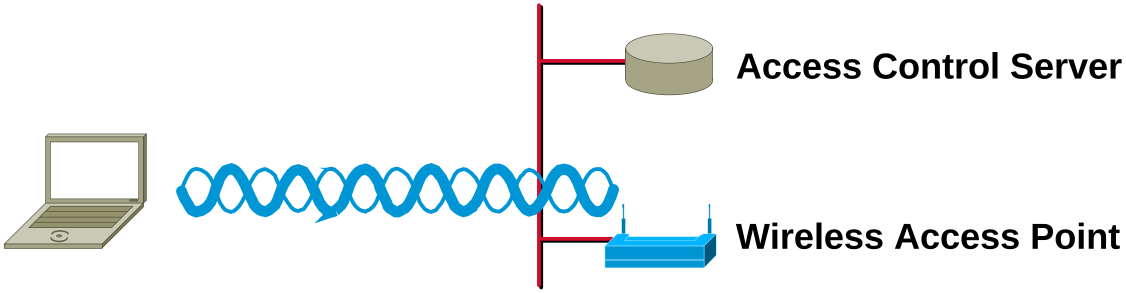
Wireless LAN Security

Wireless and LAN Switch Security



Wireless LAN Security

Cisco.com



- Want to avoid the parking lot wireless scanners

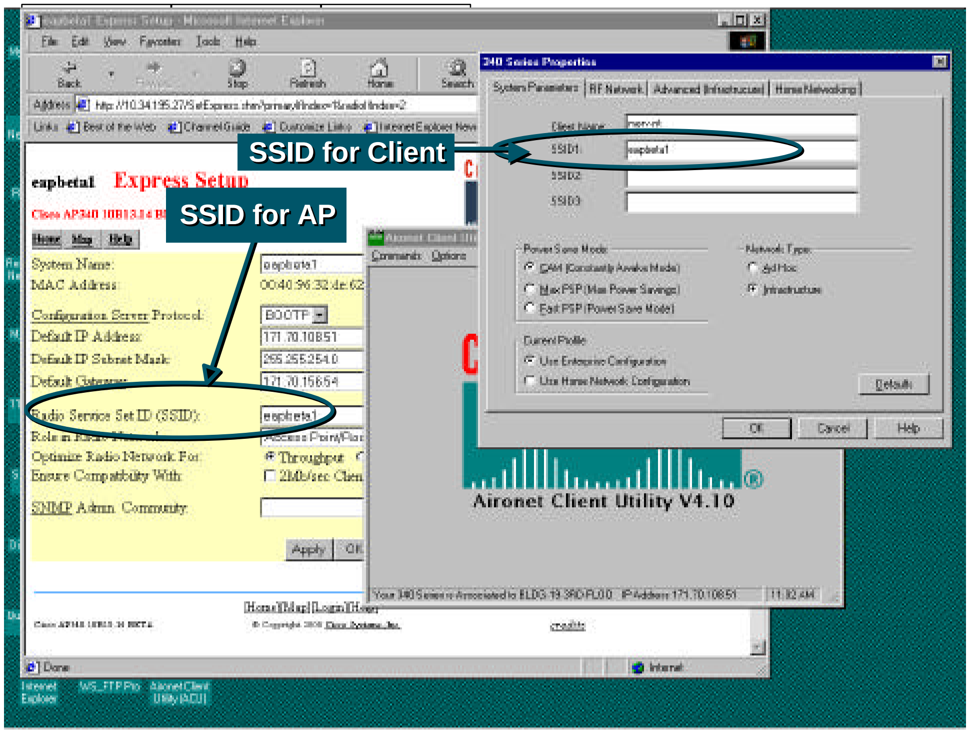
Requirements

- Restrict access to wireless network to only authorized users
- Encrypt the wireless network traffic

First Generation Wireless Security

- Service Set Identifier (SSID)
  - Provisioning and load-balancing mechanism
  - Transmitted in the clear
- Manual Wired Equivalent Privacy (WEP) key management
  - Key itself is never transmitted
  - Often everyone has the same key
  - Not manageable

SSIDs in 802.11



System Name: eapbeta1
MAC Address: 00:40:96:32:de:62
Configuration Server Protocol: BOOTP
Default IP Address: 171.70.108.51
Default IP Subnet Mask: 255.255.254.0
Default Gateway: 171.70.156.54
Radio Service Set ID (SSID): eapbeta1
Role in Radio Network: Access Point/Root
Optimize Radio Network For: ● Throughput
Ensure Compatibility With: □ 2Mb/sec Clients
SNMP Admin. Community:

Client Name: meow-nt
SSID1: eapbeta1
SSID2:
SSID3:

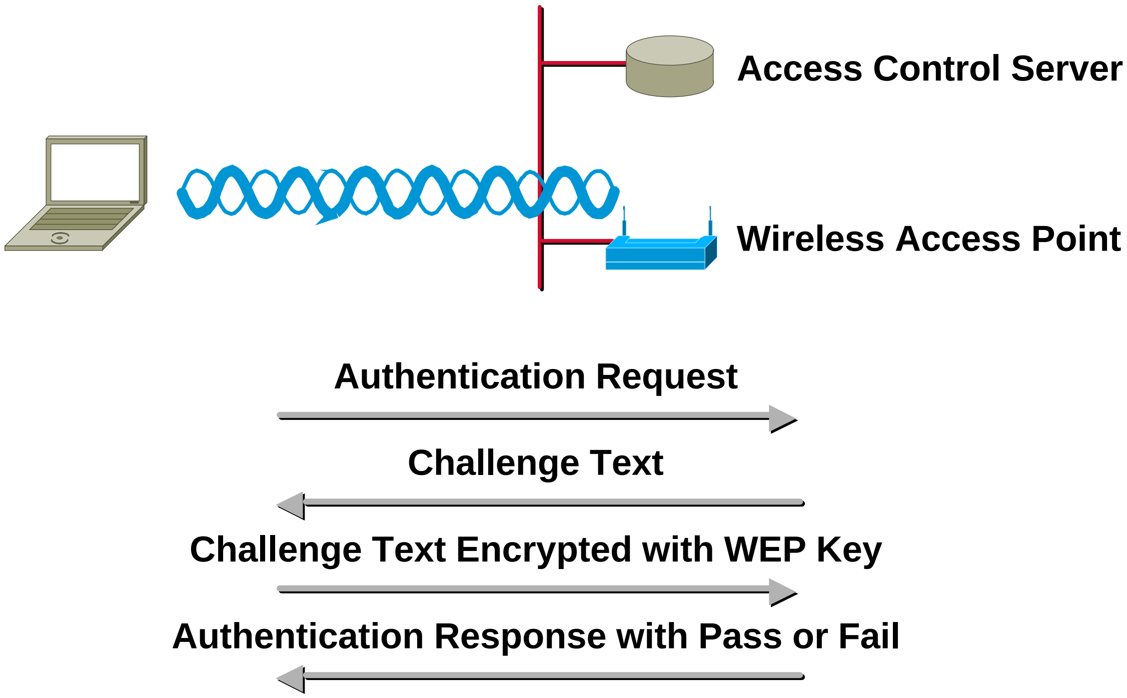
Power Save Mode:
● CAM (Constantly Awake Mode)
○ Max PSP (Max Power Savings)
○ Fast PSP (Power Save Mode)

Network Type:
○ Ad Hoc
● Infrastructure

Current Profile:
● Use Enterprise Configuration
○ Use Home Network Configuration

Your 340 Series is Associated to ELDG 19 3RD FL0.0 IP Address 171.70.108.51 11:02 AM

Manual Shared WEP



Access Control Server

Wireless Access Point

Authentication Request

Challenge Text

Challenge Text Encrypted with WEP Key

Authentication Response with Pass or Fail

Encryption

- **Encryption options**

  No encryption

  40-bit encryption

  128-bit encryption

- **Hardware-based encryption**

  3% performance hit (@128 bit)

- **Encryption choices (defined at access point)**

  No encryption

  Allow client to specify (optional)

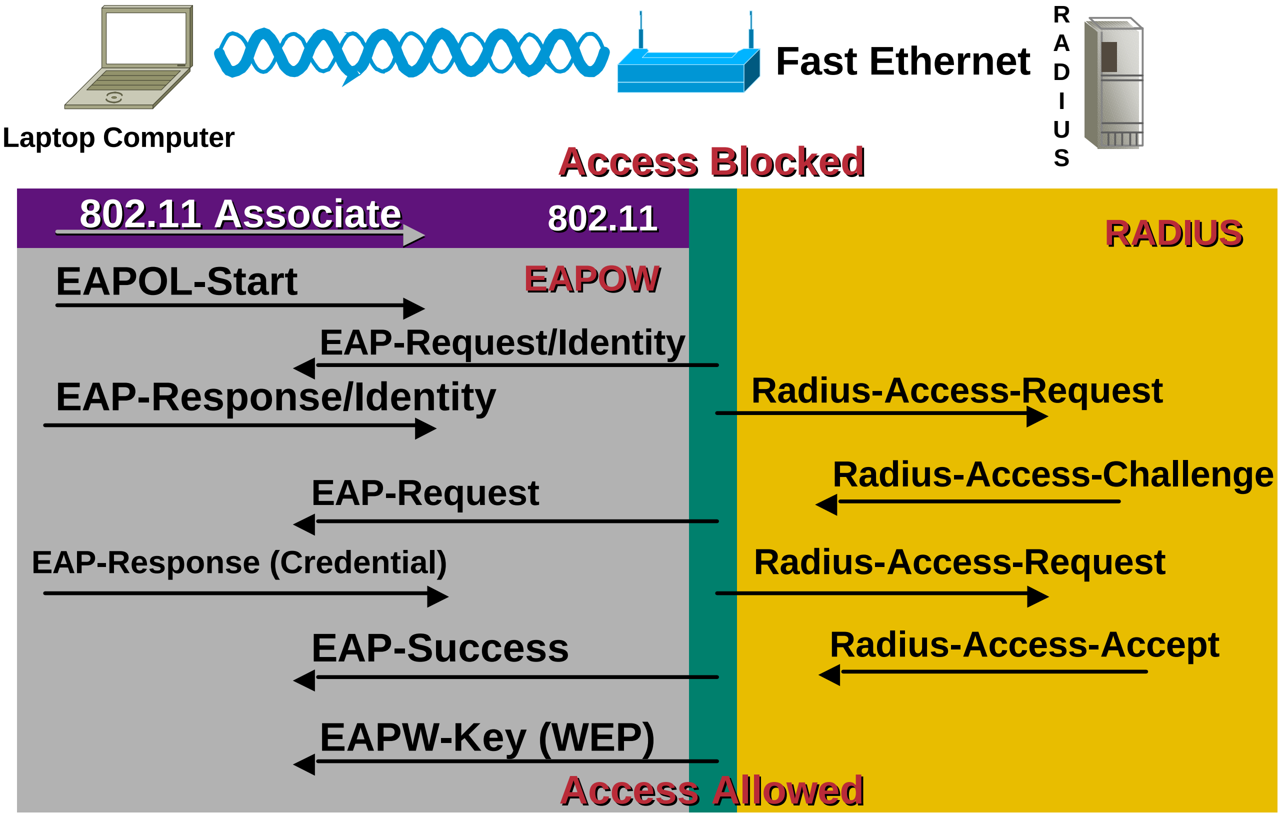
  Forced (required)

Improvements: User Authentication

- **802.1x standard is an extensible security framework**

  Extensible Authentication Protocol (EAP) services that provide centralized, user-based authentication for hassle-free security administration and user-based privacy EAP-enabled Remote Access Dial-In User Service (RADIUS) servers

Dynamic WEP Key Management



Authentication Granted/Denied

- Radius server checks response against it own calculated hash
- If it matches, then authentication is acknowledged to AP and client
- If authentication is not achieved, the AP will not permit any traffic for that client to pass

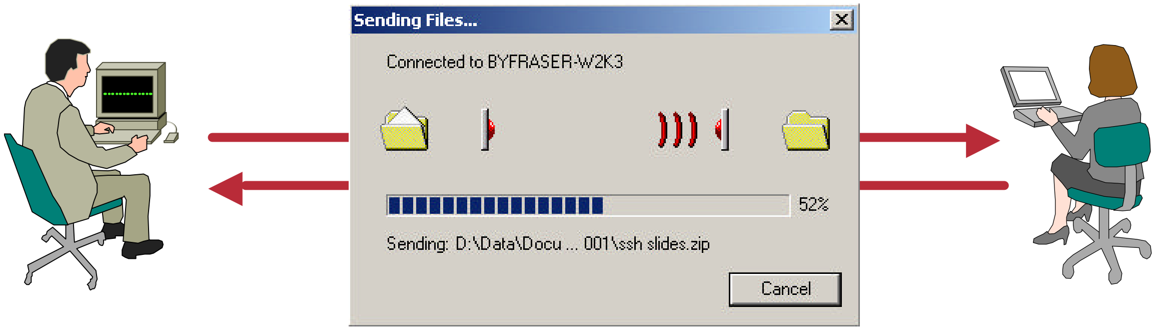
WEP Keys

- WEP key is calculated by the Radius server, only after the authentication is completed
- The key is passed to access point for THAT single authenticated client; this is a session key
- Client calculates the same WEP key
- Key is never transmitted over RF

How Often Does the Key Change?

- Every time a client roams to a new AP, it will go through the same authentication and session WEP key exercise
- The radius server will also require a new authentication/key at a timed interval (programmable)
- This provides different WEP keys often, and totally unique keys to each client

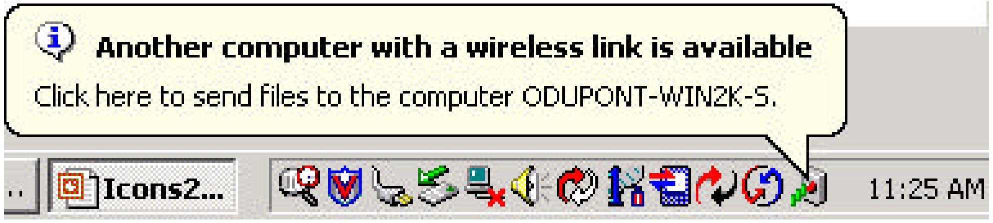
Infrared Communications



Connected to BYFRASER-W2K3

52%

Sending: D:\Data\Docu ... 001\ssh slides.zip

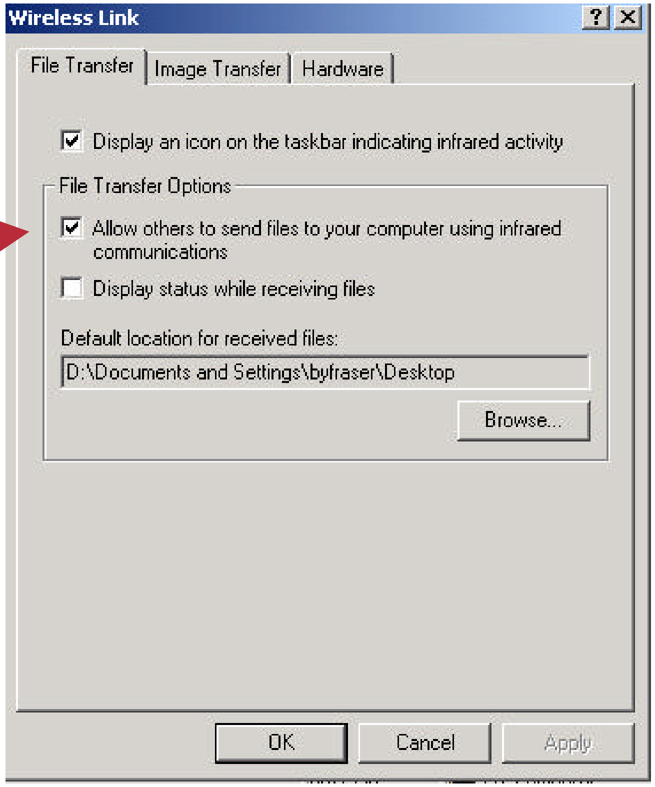


Another computer with a wireless link is available

Click here to send files to the computer ODUPONT-WIN2K-S.

Securing Your Infrared Link

- Disallow file transfers



Wireless Link

☑ Display an icon on the taskbar indicating infrared activity

File Transfer Options

☑ Allow others to send files to your computer using infrared communications

□ Display status while receiving files

Default location for received files:

D:\Documents and Settings\byfraser\Desktop

IR Ports

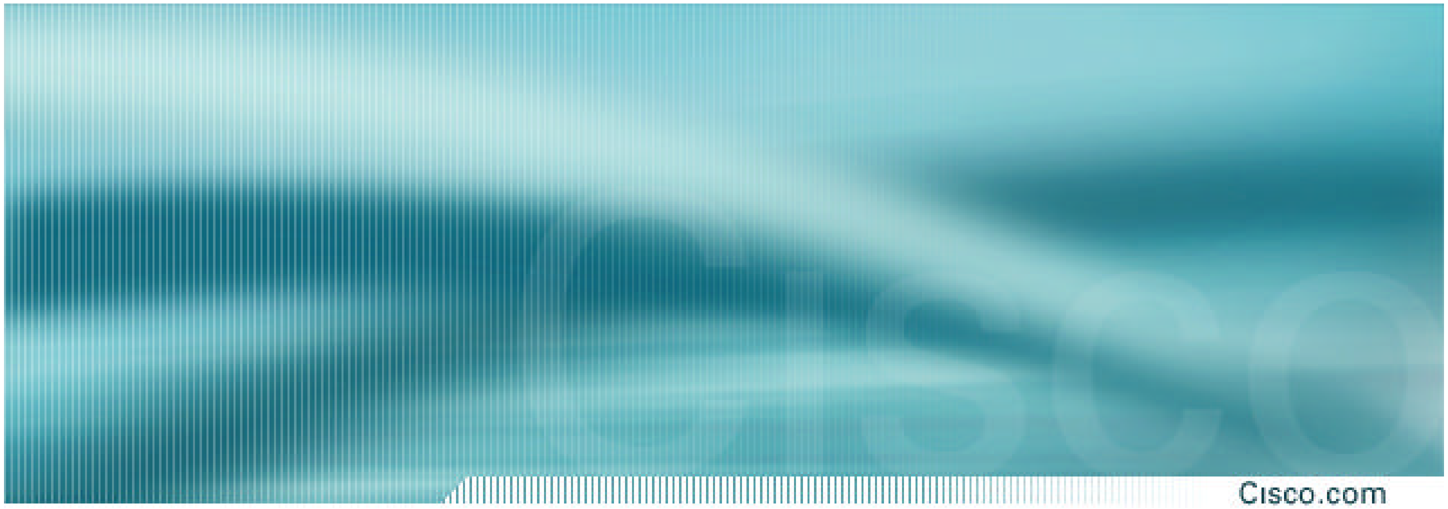
- Infrared ports have a range of 50cm to 100cm, but amplifying systems can increase the range threefold
- Notsync is new software that can capture passwords off targeted Palm Pilots by taking advantage of the PDA's hotsync function.

How Does This Protect Me?

- Strong per user authentication
- Wireless network traffic is encrypted
- EAPW-key provides unique keys per user overcoming the weak shared single key of WEP
- Ability to change encryption keys often overcomes the weakness of WEP

Just Remember

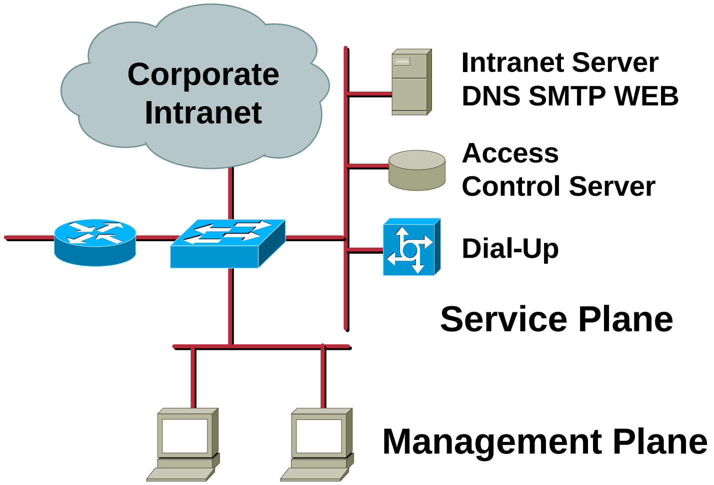
- Change defaults
- Use encryption
- Wireless sniffers are prevalent
- Ensure you aren’t allowing IR communications by default!



LAN Switch Security

LAN Switch Security

- Hacking tools exist that allow for network sniffing and other attacks on switched networks
- Defaults are not always appropriate depending the how you are using a port



The Basics

- A switch learns where MAC addresses are connected by scanning the traffic and updating it’s tables
- A switch will forward a frame to only one port if the destination MAC address is associated with that port in his table
- If no entry exists for the destination MAC address in the switch table, the frame is flooded to all ports
- A switch does not flood most frames, beyond layer 2 broadcasts
- VLANs will contain layer 2 broadcasts, except on trunk ports

Protections

- Use port filtering

  Like with layer 3 access lists you can limit the source/destination MAC address for each port

- Use VLANs to limit the size of the broadcast domain

- VLAN will enable IP filtering

  Directly specify which traffic is allowed to flow to and from each port

- Disable trunking on station ports

- Disable spanning tree on ports connected to PCs

  That is, unless you know there is another switch connected on the same port.

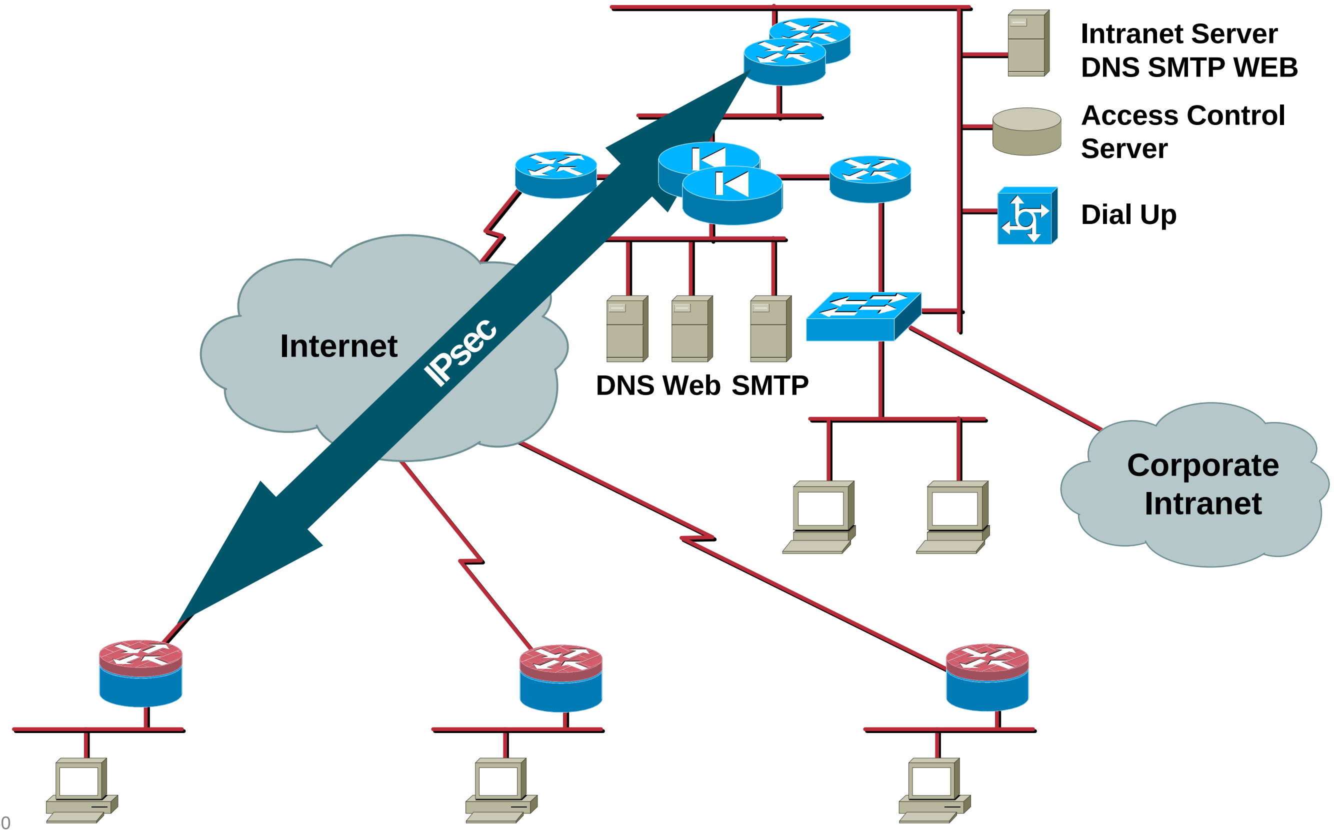
Just Remember…

- **Never use a switch with different VLANs to separate the different DMZs behind your firewall**

Providing Resiliency

Adding Headquarters IPsec and Firewalls Redundancy

Cisco.com

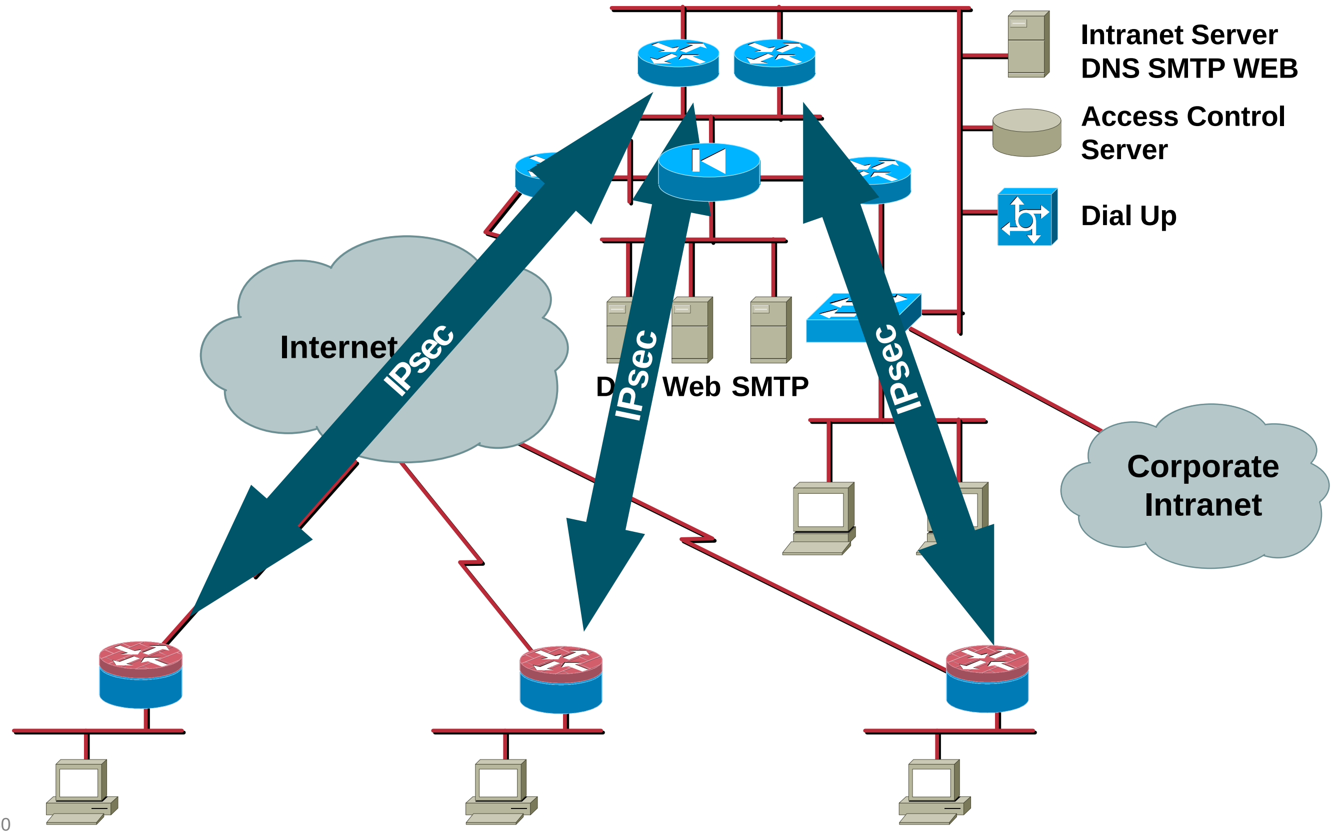


PS-550
3027_05_2001_c2

IPsec Redundancy Requirements

- Provide multiple IPsec termination points at headquarters
- Be able to detect a failure and reconnect to backup gateway
- Re-establish initial topology when primary gateway is back on line
- Maintain routing in all scenarios

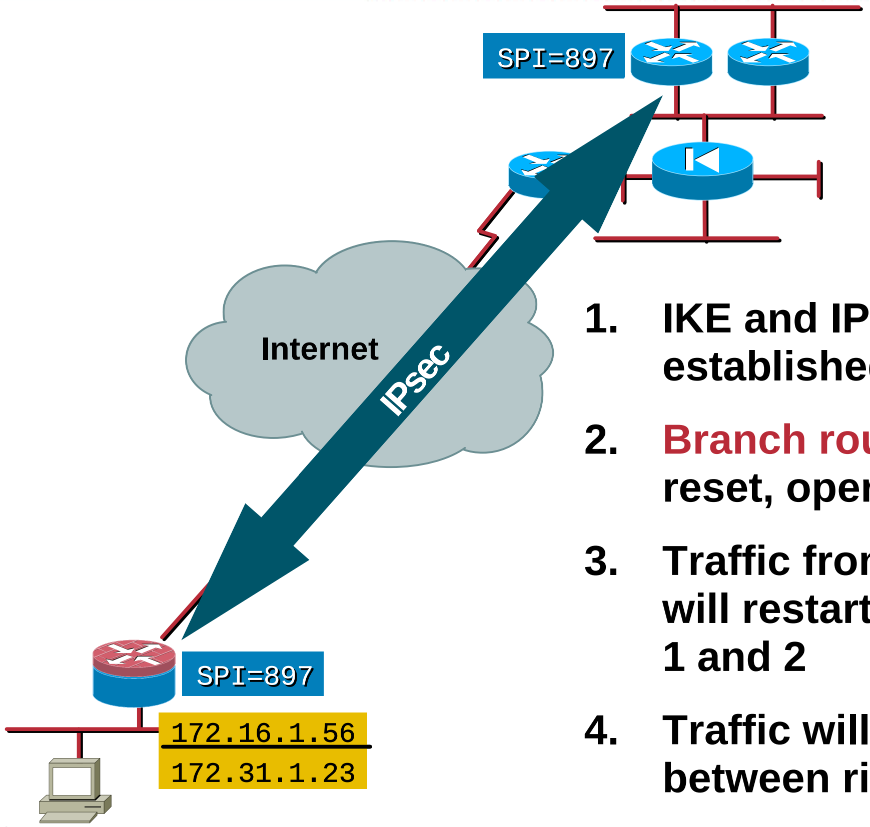
Adding Headquarters IPsec Redundancy



Dual (or Triple) Hub and Spoke

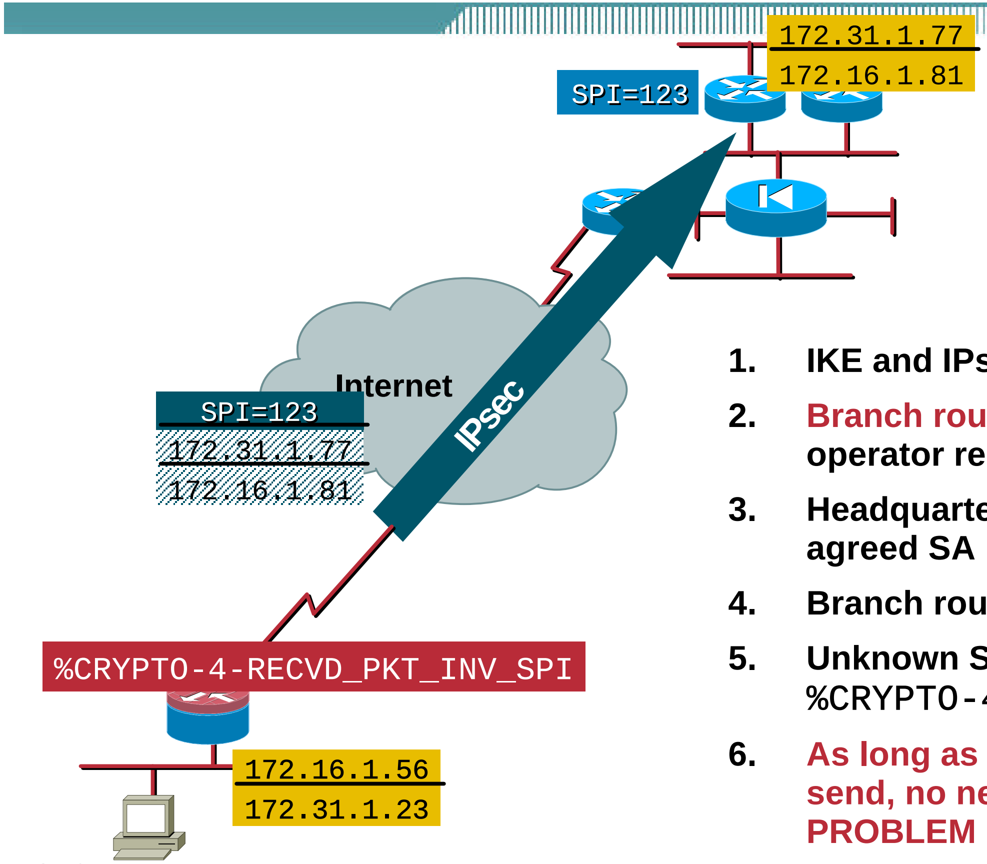
- On normal operation all concentration gateways are on line and share load
- When failure is detected, IPsec is re-established on remaining gateways
- How to detect failure?

IPsec SA Disappears—Case 1



1. IKE and IPsec SA are established
2. Branch router resets (power reset, operator reload,…)
3. Traffic from branch to corporate will restart new IKE phases 1 and 2
4. Traffic will flow back and forth between right and left routers

IPsec SA Disappears—Case 2



%CRYPTO-4-RECVD_PKT_INV_SPI

1. IKE and IPsec SA are established
2. Branch router resets (power reset, operator reload,…)
3. Headquarters router still uses agreed SA
4. Branch router does not have any SA
5. Unknown SPI at branch: `%CRYPTO-4-RECVD_PKT_INV_SPI`
6. As long as branch has nothing to send, no new SA are re-negotiated : PROBLEM !

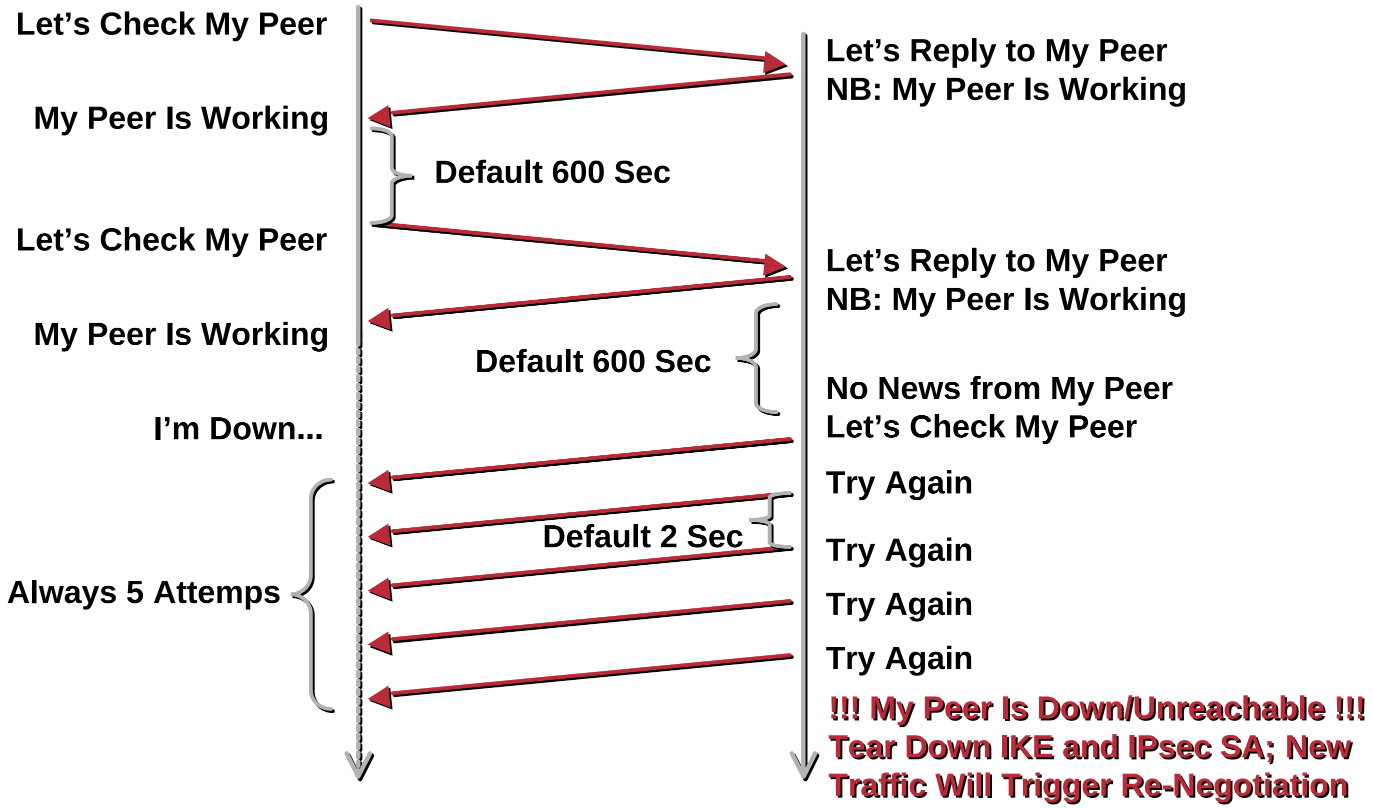
IKE Keep Alive

- Cisco proprietary extension to IKE; keepalive IKE packets will signal headquarters router that branch router has lost the IKE SA
- IOS command

```
crypto isakmp keepalive <sec> <retry interval>
```

- Default: 600 seconds and 2 seconds

IKE Keep Alive Details



IKE Keep Alive Duration

- Defaults are 600 seconds for periodic check and 5 attempts every 2 seconds

  => worst case: 600 + 5*2 = 610 seconds

  => best case: 5*2 = 10 seconds

- Changing default values

  => worst case: 10 + 5*2 = 20 seconds

  => best case: 5*2 = 10 seconds

Tool Kit

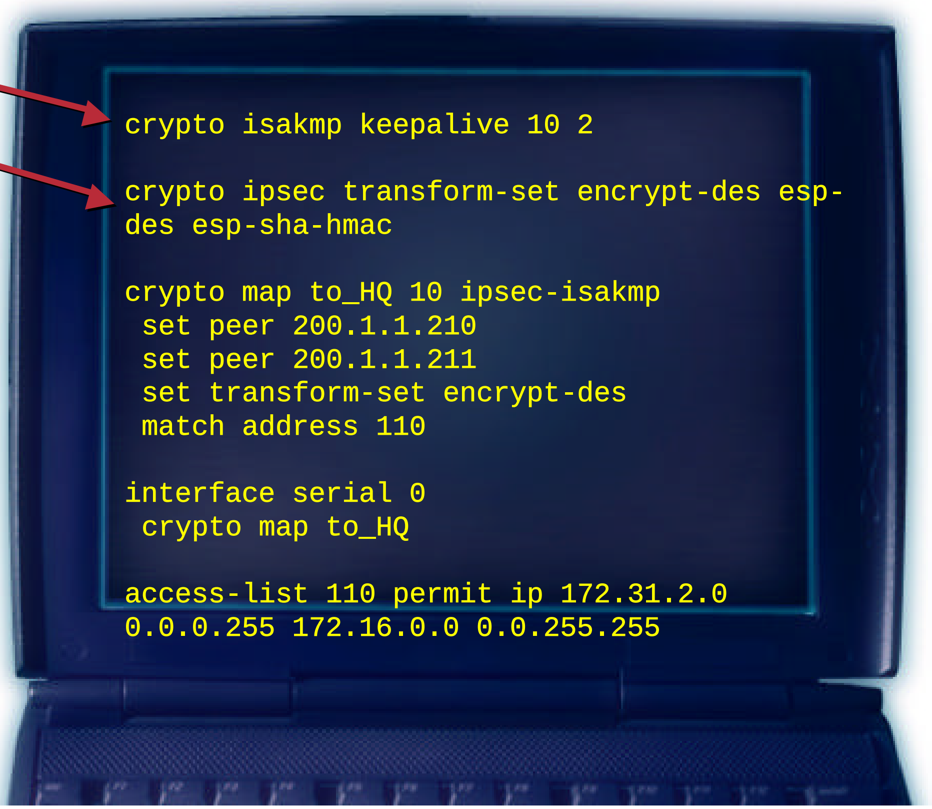
- IKE keepalive
- Multiple peer statements
- ACL for IKE traffic

Branch Office Dual Peer Configuration

Configure Keep Alive

Add a Second Set Peer

If IKE Is Not Established with the First Peer, after 3 Attempts, the Branch Router Will Try the Second

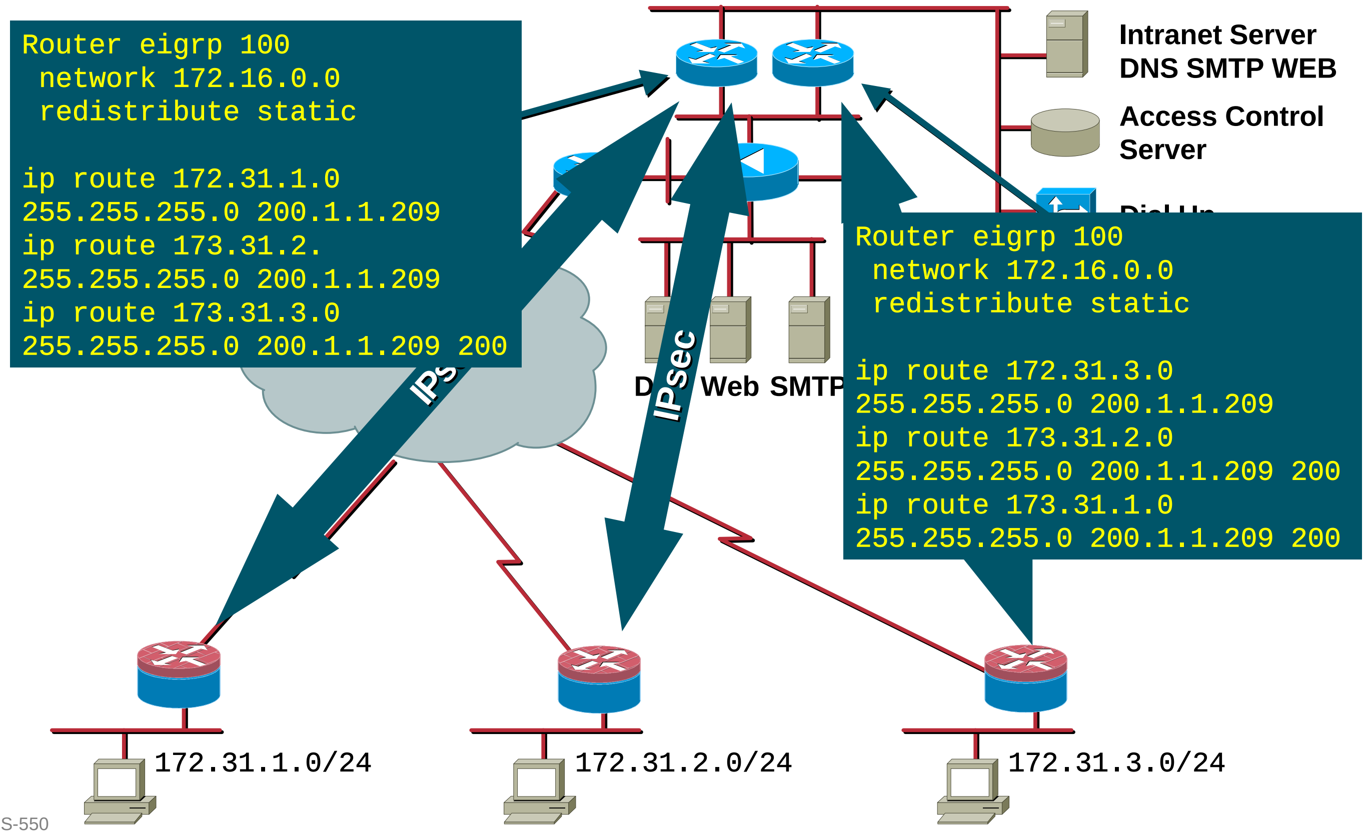


```
crypto isakmp keepalive 10 2

crypto ipsec transform-set encrypt-des esp-
des esp-sha-hmac

crypto map to_HQ 10 ipsec-isakmp
 set peer 200.1.1.210
 set peer 200.1.1.211
 set transform-set encrypt-des
 match address 110

interface serial 0
 crypto map to_HQ

access-list 110 permit ip 172.31.2.0
0.0.0.255 172.16.0.0 0.0.255.255
```

Dual Hub and Spoke Routing Issues

- Branch router has only one default
- Headquarters routers need to announce for which branch they are active
- Branches are on private addresses and not directly connected so no dynamic routing possible
- Work around: Static floating routes

Configuring Routing



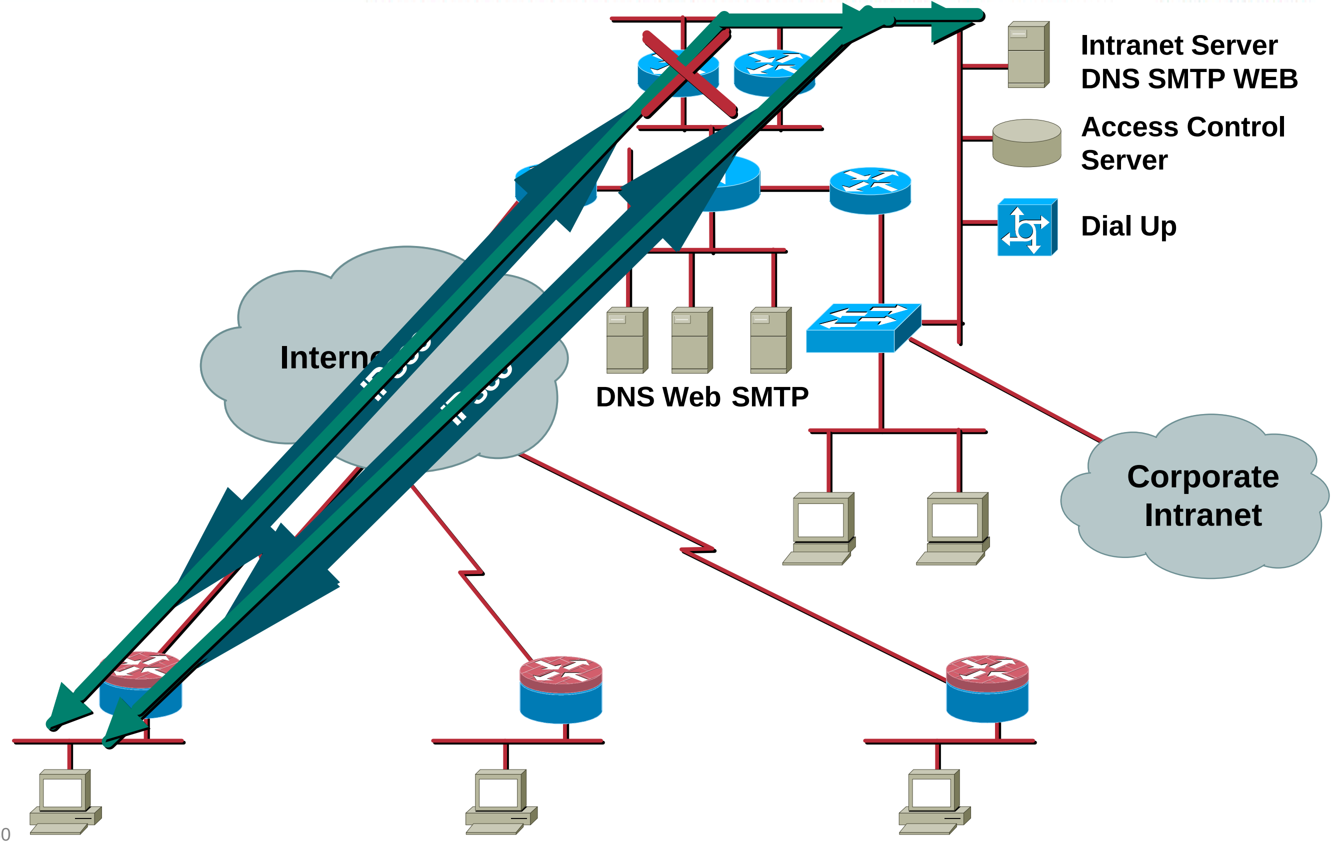
```
Router eigrp 100
 network 172.16.0.0
 redistribute static

ip route 172.31.1.0
255.255.255.0 200.1.1.209
ip route 173.31.2.
255.255.255.0 200.1.1.209
ip route 173.31.3.0
255.255.255.0 200.1.1.209 200
```

```
Router eigrp 100
 network 172.16.0.0
 redistribute static

ip route 172.31.3.0
255.255.255.0 200.1.1.209
ip route 173.31.2.0
255.255.255.0 200.1.1.209 200
ip route 173.31.1.0
255.255.255.0 200.1.1.209 200
```

Dual Hub and Spoke: Issues

- **Primary gateway comes back on line**
- **Dynamic routing protocol announces route again**
- **Static floating routes are removed**
- **Two IPsec tunnels are active until backup tunnel ages**

IPsec Redundancy: Two Active Tunnels



Just Remember…

- Don’t forget to update your ACLs to permit IPsec traffic going to the second (or more) gateway

Performance

- Keepalives add about 5% CPU
- On backup, loads increase suddenly on remaining concentration device(s)

  Concurrent session negotiation

  The increased load is a function of the number of redundant devices

- Be aware of the maximum number of SAs per concentration device

  Active unused SAs consume power

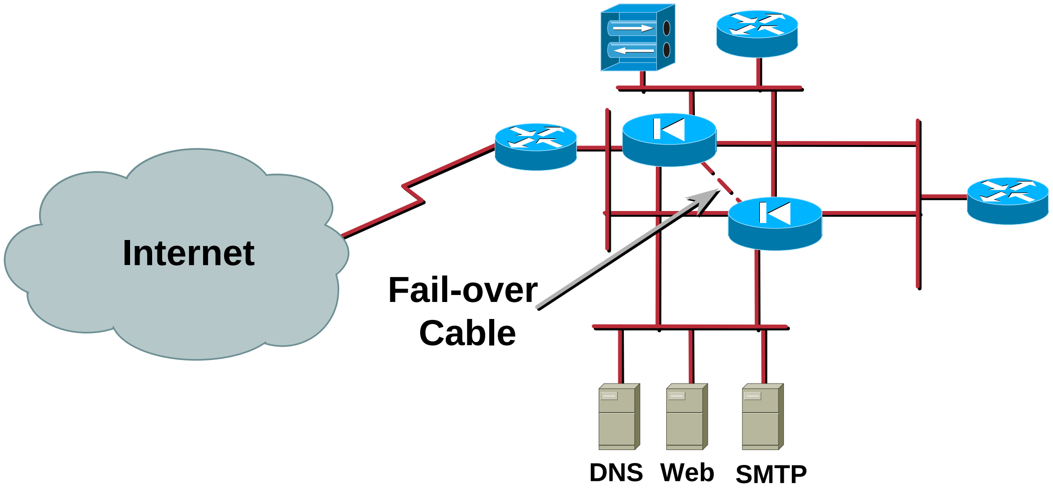
Firewall Redundancy Requirements

- Fail-over
- Stateful fail-over

Local Fail-Over

- **Goal: Being able to detect the failure of one firewall and then back-up to a second one**
- **Limitation: Loss of state, need to be very local due to RS232 distance limited connection**

Local Fail-Over



- Keepalives are exchanged every 15 seconds, backup occurs after having lost 3 of them
- The RS232 interface is used to copy the configuration from master FW to slave FW
- Stateful tables are not exchanged, no load balancing

Stateful Fail-Over

- The more stateful a system is, the more complex it becomes
- If the stateful table is updated for every packet, the slave FW table must be updated as well
- The bandwidth require to exchange the stateful table is almost equal to the firewall throughput

Stateful Fail-Over (Cont.)

- Dedicate a high speed interface on both FW to exchange stateful tables
- The RS232 connection is still used to update configuration and detect power off
- ARP pooling is done on all interfaces every 15 seconds (configurable)
- Convergence time is 1 to 3 lost keepalive, e.g. 15 to 45 seconds

Stateful Fail-Over (Cont.)

- Information replicated to the standby PIX firewall
  - Configuration
  - TCP (except HTTP) connection table including timeout information of each connection
  - Translation (xlate) table
  - System up time (system clock synchronized on both PIX)
- Information not replicated to the standby PIX firewall
  - HTTP connection table
  - User authentication (uauth) table
  - ISAKMP and IPsec SA table
  - ARP table

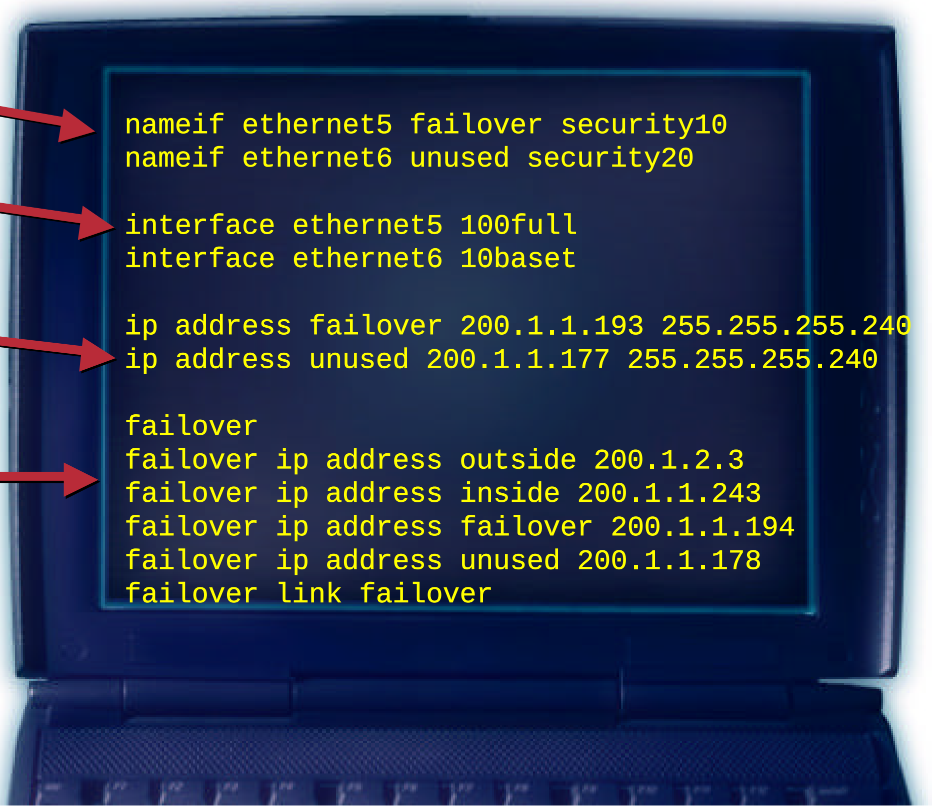
Configurations

Dedicate One Interface to Stateful Fail-over

Configure It to Be Full Duplex

Configure All Unused Interfaces

Configure Fail-over Addresses for ARP Pooling

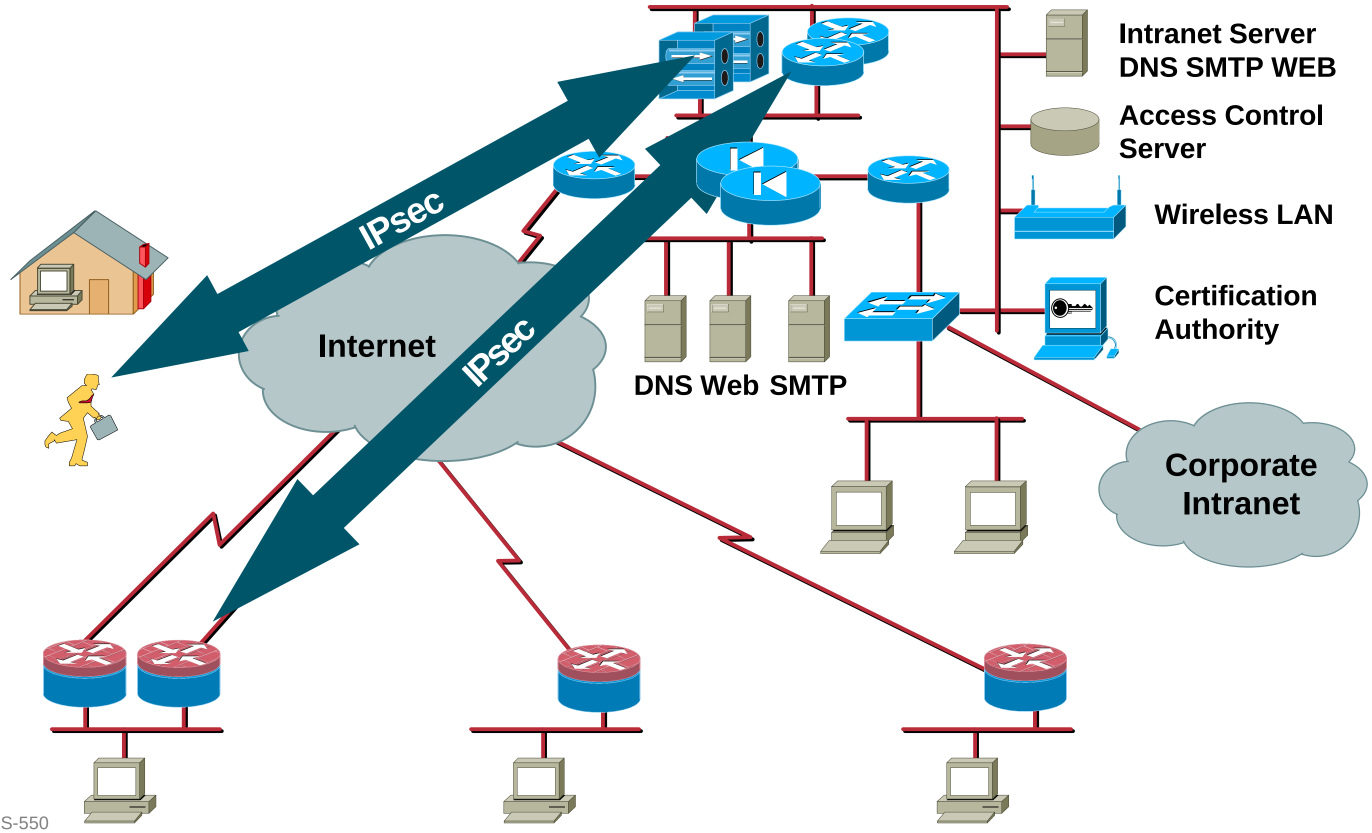


```
nameif ethernet5 failover security10
nameif ethernet6 unused security20

interface ethernet5 100full
interface ethernet6 10baset

ip address failover 200.1.1.193 255.255.255.240
ip address unused 200.1.1.177 255.255.255.240

failover
failover ip address outside 200.1.2.3
failover ip address inside 200.1.1.243
failover ip address failover 200.1.1.194
failover ip address unused 200.1.1.178
failover link failover
```

Just Remember…

- The 2 PIXs must run the same software release
- Interfaces must not be configured in auto speed mode
- Unused interfaces must be configured and cross-connected
- Stateful fail-over interface must be configured as `100full` (full duplex 100Mb/s)
- Xlate have to be cleared once after having configured stateful fail-over

Dual Redundancy



Requirements

- **Zero point of failure**

  WAN, headquarters, branch

- **Use dynamic routing to advertise complex branches address space**

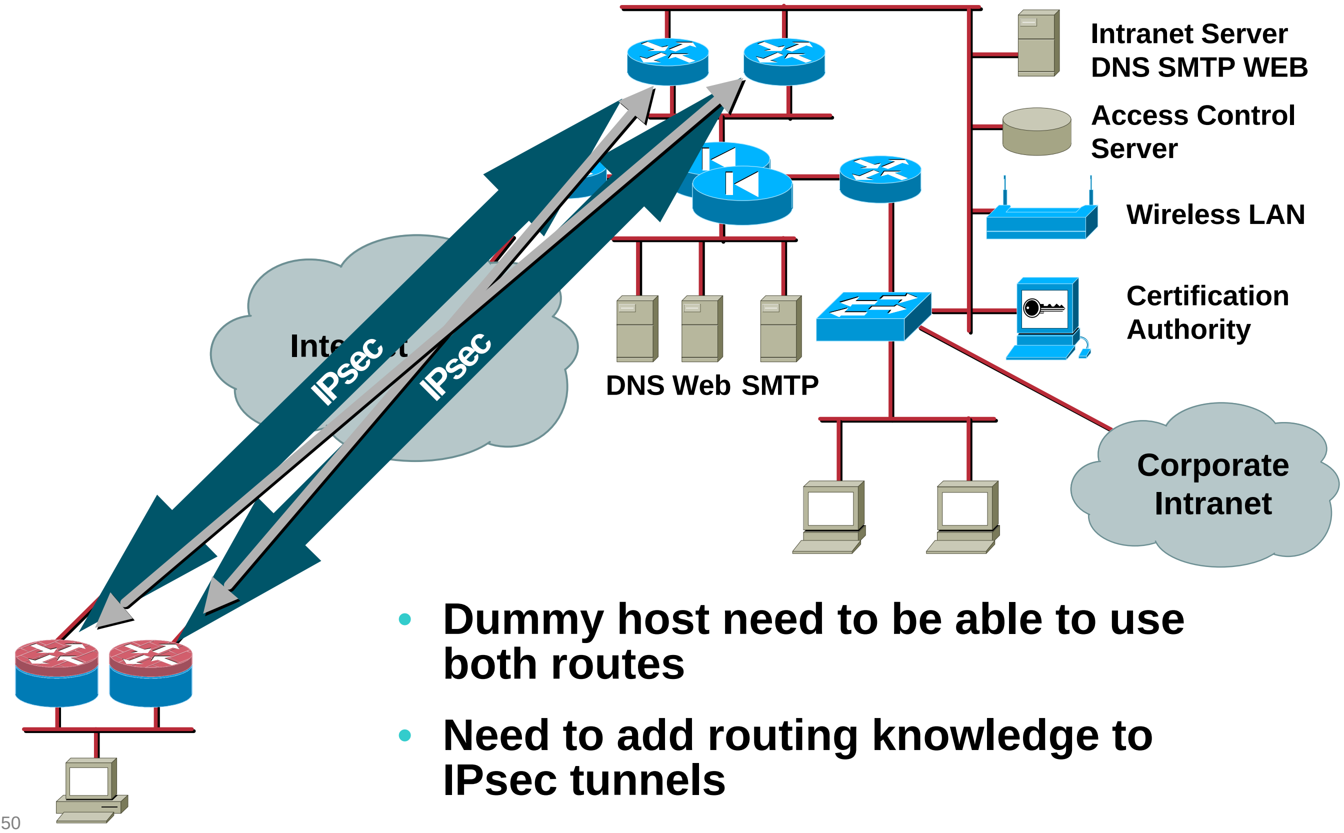
- **Be transparent to local hosts**

Tool Kit

Cisco.com

- IPsec backup peers
- IKE keepalive
- Hot Standby Routing Protocol (HSRP)
- Generic Encapsulation Protocol (GRE)

Dual Redundancy



- Dummy host need to be able to use both routes
- Need to add routing knowledge to IPsec tunnels

HSRP Overview

- Two routers setup to use single “virtual” IP address
- Provides redundancy for the default gateway used by hosts
- Routers do not use the HSRP virtual IP address for routing/forwarding packets
- Return packets can take any path back

HSRP Example Configuration

```
hostname Router_1
!
interface Ethernet0
 ip address 172.31.1.1 255.255.255.0
 standby priority 100
 standby preempt
 standby ip 172.31.1.254
```

```
Hostname Router_2
!
interface Ethernet0
 ip address 172.31.1.2 255.255.255.0
 standby priority 95
 standby preempt
 standby ip 172.31.1.254
```

GRE Tunnel Overview

- RFC 1701—Generic routing encapsulation
  - Tunneling an IP datagram in an IP datagram
    - Multiprotocol, keys, keepalives, sequencing
- Implemented using a virtual interface
  - Can run routing protocols over tunnel
  - Point-to-point
    - Static tunnel destination address
  - Multipoint
    - Dynamic tunnel destination address mapping using NHRP

GRE Tunnels

Cisco.com

- Separate GRE tunnels are built

  Use transport mode IPsec to encrypt GRE tunnel

- Run a routing protocol over the tunnels

  Routing updates control which tunnels are used

- On HSRP router failure or switchover

  Use of the GRE tunnel from remote peer to alternate HSRP router switches when the routing converges

- Can be used to IPsec encrypt other protocols

  Appletalk, DECnet, IPX, Multicast IP

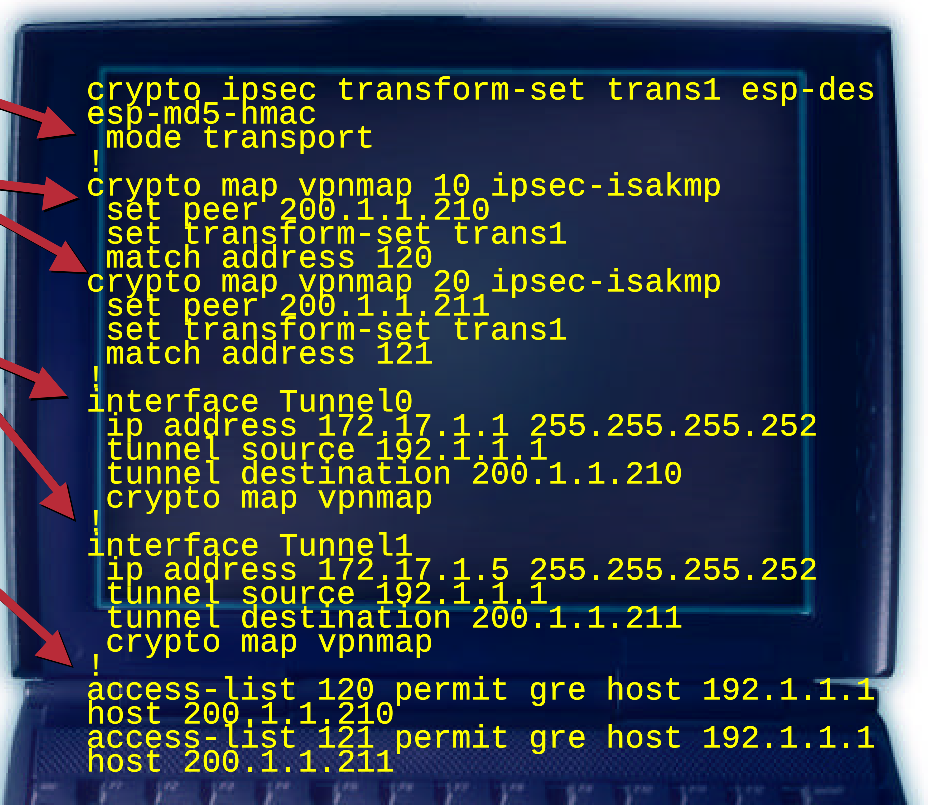
One Branch Router Configuration

Use Transport Mode

One Crypto Map Sequence Per Tunnel

Create One GRE Tunnel with Each Headquarters Router

The ACL Test the Tunnel End Point Addresses



```
crypto ipsec transform-set trans1 esp-des
esp-md5-hmac
 mode transport
!
crypto map vpnmap 10 ipsec-isakmp
 set peer 200.1.1.210
 set transform-set trans1
 match address 120
crypto map vpnmap 20 ipsec-isakmp
 set peer 200.1.1.211
 set transform-set trans1
 match address 121
!
interface Tunnel0
 ip address 172.17.1.1 255.255.255.252
 tunnel source 192.1.1.1
 tunnel destination 200.1.1.210
 crypto map vpnmap
!
interface Tunnel1
 ip address 172.17.1.5 255.255.255.252
 tunnel source 192.1.1.1
 tunnel destination 200.1.1.211
 crypto map vpnmap
!
access-list 120 permit gre host 192.1.1.1
host 200.1.1.210
access-list 121 permit gre host 192.1.1.1
host 200.1.1.211
```

GRE Tunnels

- Both branch routers and both headquarters routers have similar configuration
- Each router has 2 GRE tunnels
- ACL test is done on the GRE endpoints
- Crypto map needs to be applied on both the tunnel and the physical interfaces

GRE Tunnels: Routing Configuration

Headquarters Routers

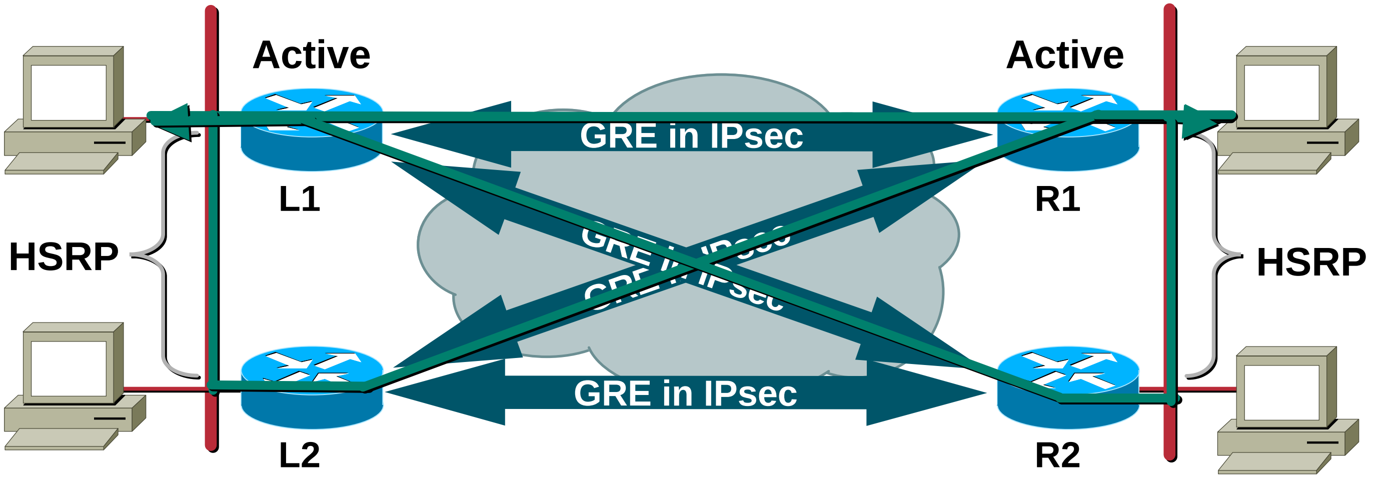
```
router eigrp
 network 172.17.1.0
 network 172.16.1.0
```

Branch Routers

```
router eigrp
 network 172.17.1.0
 network 172.31.1.0
```

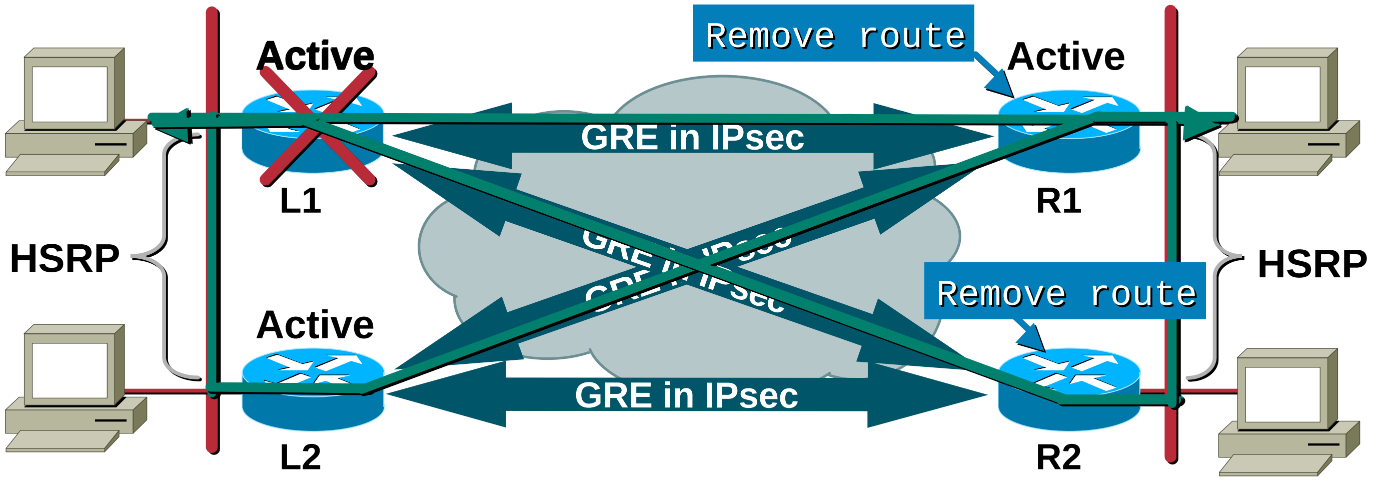
- **Routing is turned on all “private” interfaces**
  - **The tunnel interface**
  - **The intranet interface**
- **Any branch update will be propagated in the GRE tunnels and routing protocol will allow load balancing**

HSRP and IPsec Router Resilience



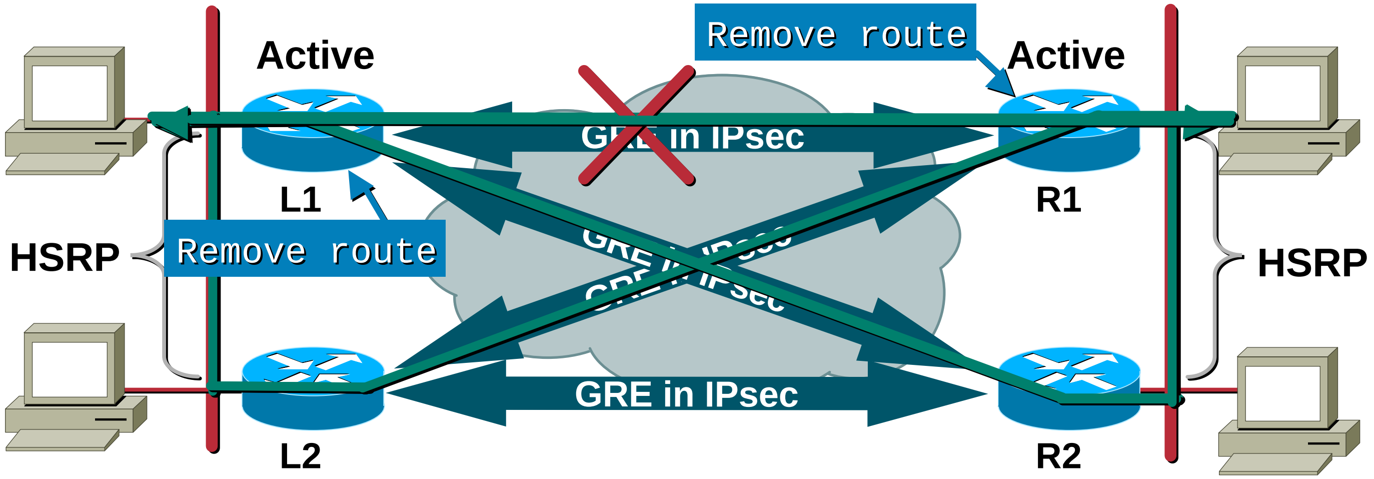
- **At start time, routers L1 and R1 are active**
- **Outbound traffic flows equally in the 2 GRE tunnels attached to primary HSRP routers**
- **Inbound flows arrive from both primary and secondary HSRP routers**

HSRP and IPsec Router Resilience



- **If primary HSRP routers fails, secondary takes over**
- **On other side routing protocols will remove stalled router from next hop list; tunnel interface is not longer used**

HSRP and IPsec Router Resilience



- If WAN connection is lost, appropriate routes will be removed and only 2 tunnels are used
- Outbound traffic only uses active HSRP routers

How Does This Protect Me?

- IPsec provides integrity and confidentiality
- GRE provides WAN redundancy and allows dynamic routing protocols to spread throughout the intranet
- HSRP provides redundancy to routing-less hosts

Just Remember...

- You need to turn on routing on GRE
- Make sure you update your ACL on all firewalls to authorize the new IPsec tunnels
- As long as routing protocols are running into tunnel interface, IPsec SA stays up

Performance

- HSRP and GRE add very little overhead
- Headquarters routers have twice the number of active peers at all time

Summary: Dos and Don’ts

Summary Dos and Don'ts

- Don't:

  Use defaults blindly

  Deploy services that are not needed

  Allow device management from anywhere

  Use clear text passwords in risky places

  Assume filtering is going to destroy performance

  Send important data in the clear across an untrusted network

  Assume incidents aren't going to occur

Summary Dos and Don’ts (Cont.)

- **Do:**
  - Secure network devices
  - Restrict device management
  - Use strong authentication
  - Deploy firewalls and spread filters
  - Encrypt sensitive network traffic

Summary Dos and Don’ts (Cont.)

- **Do (Cont.):**

  Deploy intrusion detection

  Filter source addresses

  Provide redundancy

  Use committed access rate

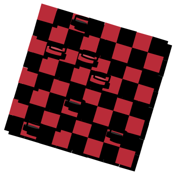
  Use Unicast RPF

  Be prepared for security incidents

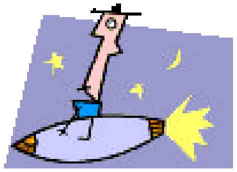
Our Challenge to You

- Building secure networks is a marathon, not a sprint—It will take you a long time to do it right

- Building secure networks is like a game of checkers—You do it step by step



- We hope this course has given you a starting boost—You're ready and able to do the rest!



Are You Ready?

Related Networkers Sessions

Cisco.com

- SEC-101 Introduction to Network Security
- SEC-110 Introduction to IPsec VPN
- SEC-212 (213) Deploying Secure Enterprise part 1 (2)
- SEC-214 Deploying Complex and Large Scale IPsec VPN
- SEC-222 Securing your Telecommuters and Mobile Users
- SEC-230 Deploying and Managing IDS
- SEC-240 Understanding Firewall Technology

More Information

- **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

- **Improving Security on Cisco Routers**

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

Resources

Cisco.com

- **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

- **Distributed Systems Intruder Tools Workshop Report**

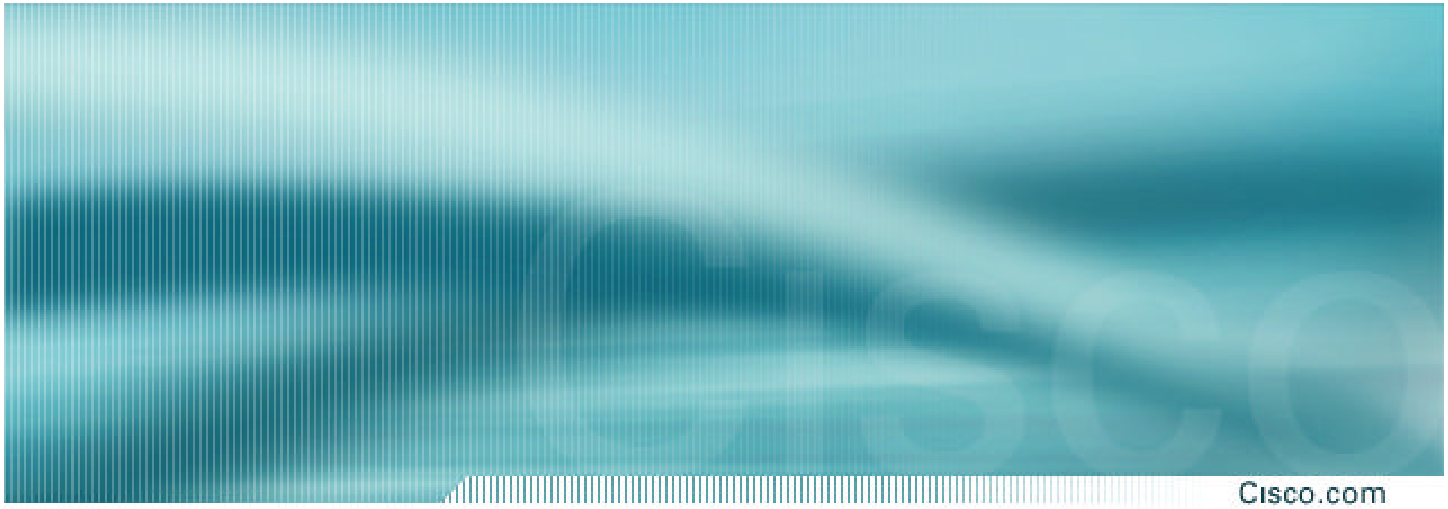
  http://www.cert.org/reports/dsit_workshop.pdf

- **CERT Advisories**

  http://www.cert.org/

- **FIRST**

  http://www.first.org/



Designing Secure Networks: Dos and Don’ts

Session PS-550

Cisco.com

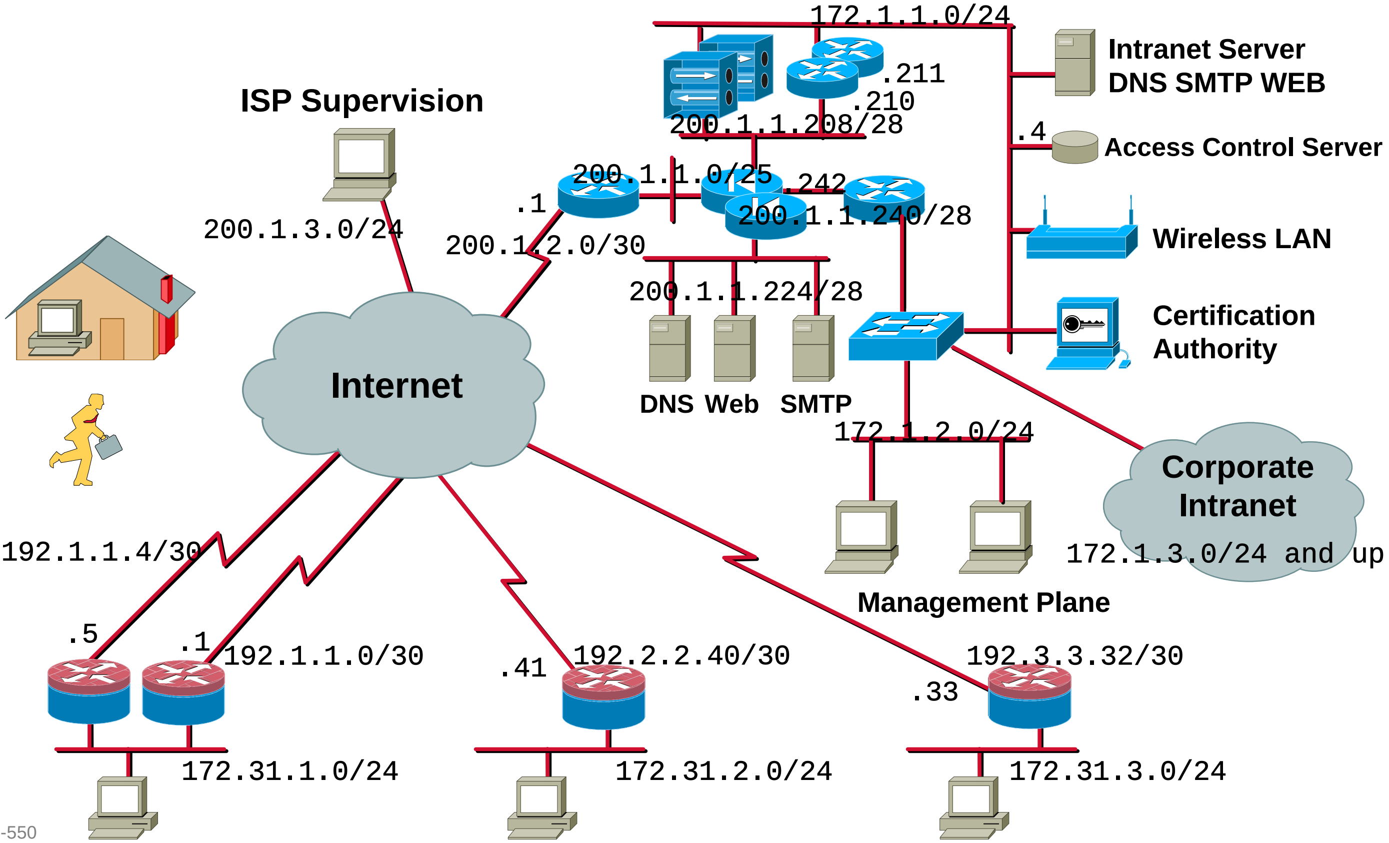
Please Complete Your Evaluation Form

Session PS-550

CISCO SYSTEMS

EMPOWERING THE
INTERNET GENERATION SM

Address Space


172.1.1.0/24
Intranet Server
DNS SMTP WEB
.211
.210
200.1.1.208/28
.4
Access Control Server
ISP Supervision
200.1.1.0/25
.242
.1
200.1.1.240/28
Wireless LAN
200.1.3.0/24
200.1.2.0/30
200.1.1.224/28
Certification
Authority
Internet
DNS
Web
SMTP
172.1.2.0/24
Corporate
Intranet
192.1.1.4/30
172.1.3.0/24 and up
Management Plane
.5
.1
192.1.1.0/30
.41
192.2.2.40/30
192.3.3.32/30
.33
172.31.1.0/24
172.31.2.0/24
172.31.3.0/24