Network Infrastructure Security

APRICOT 2005 Workshop

February 18-20, 2005

Merike Kaeo

merike@doubleshotsecurity.com

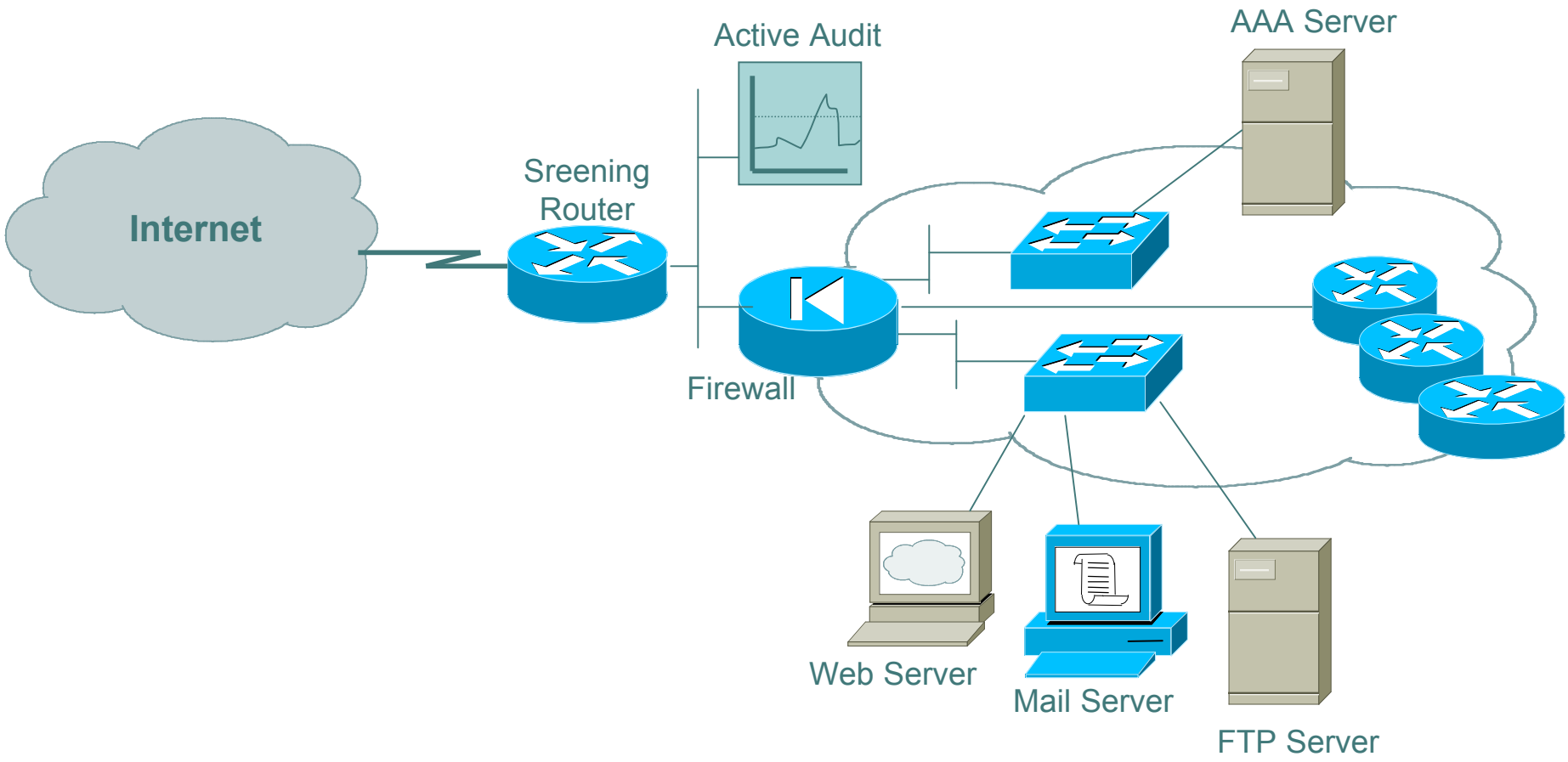
Agenda (Day 3)

- Securing Routing Protocols
  - Route Authentication (MD5)
  - Filtering Policies
  - Flap Damping
  - Prefix Limits
- Auditing Tools
  - Sniffers and Traffic Analyzers
  - Vulnerability Assessment (Nessus, NMAP)
- Mitigating DoS Attacks
  - Blackhole /Sinkhole Routing
  - Rate Limiting
- LAB

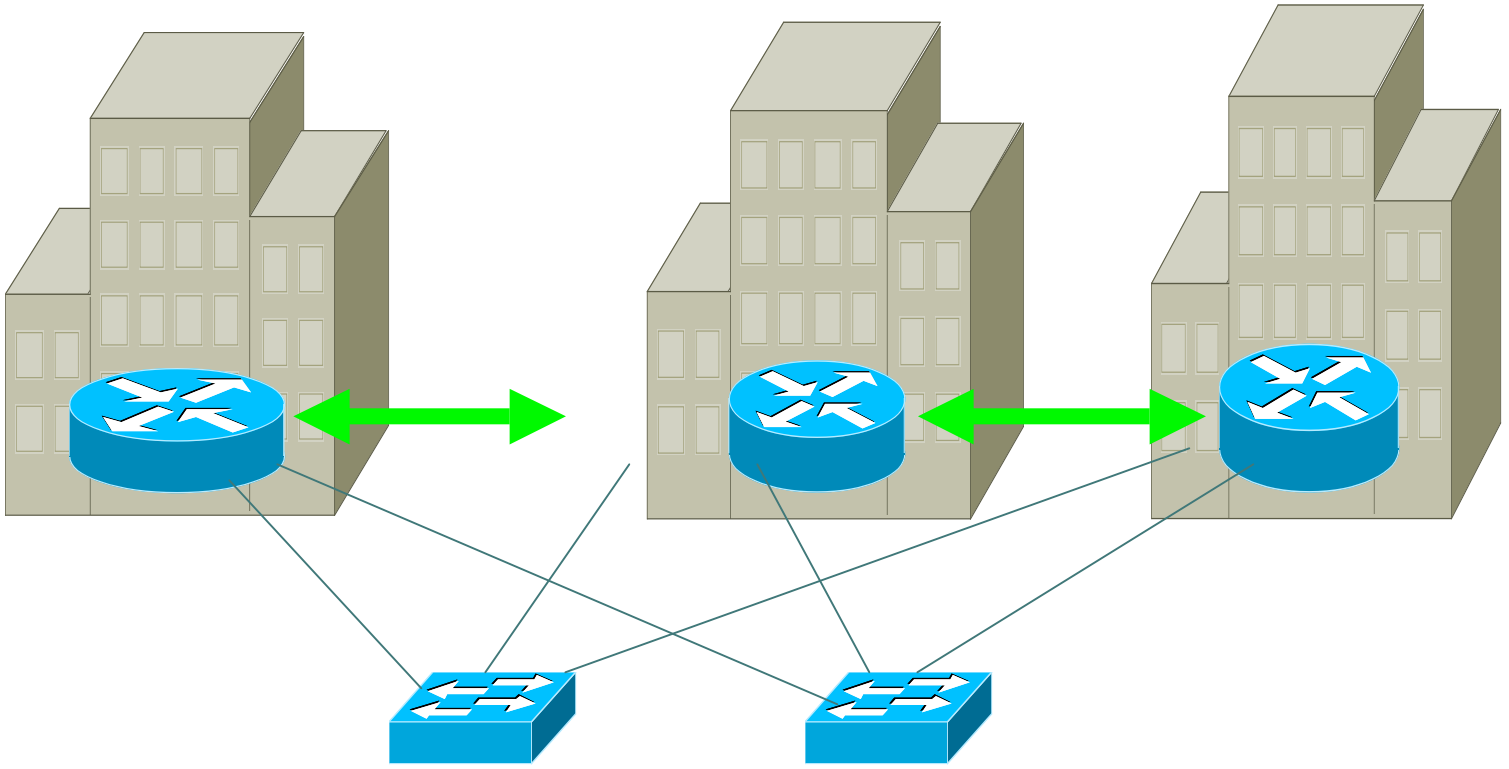
What Are Security Goals?

- Controlling Data / Network Access
- Preventing Intrusions
- Responding to Incidences
- Ensuring Network Availability
- Protecting information in Transit

Typical Secure Infrastructure Architecture



What About Router-to-Router Communication ?



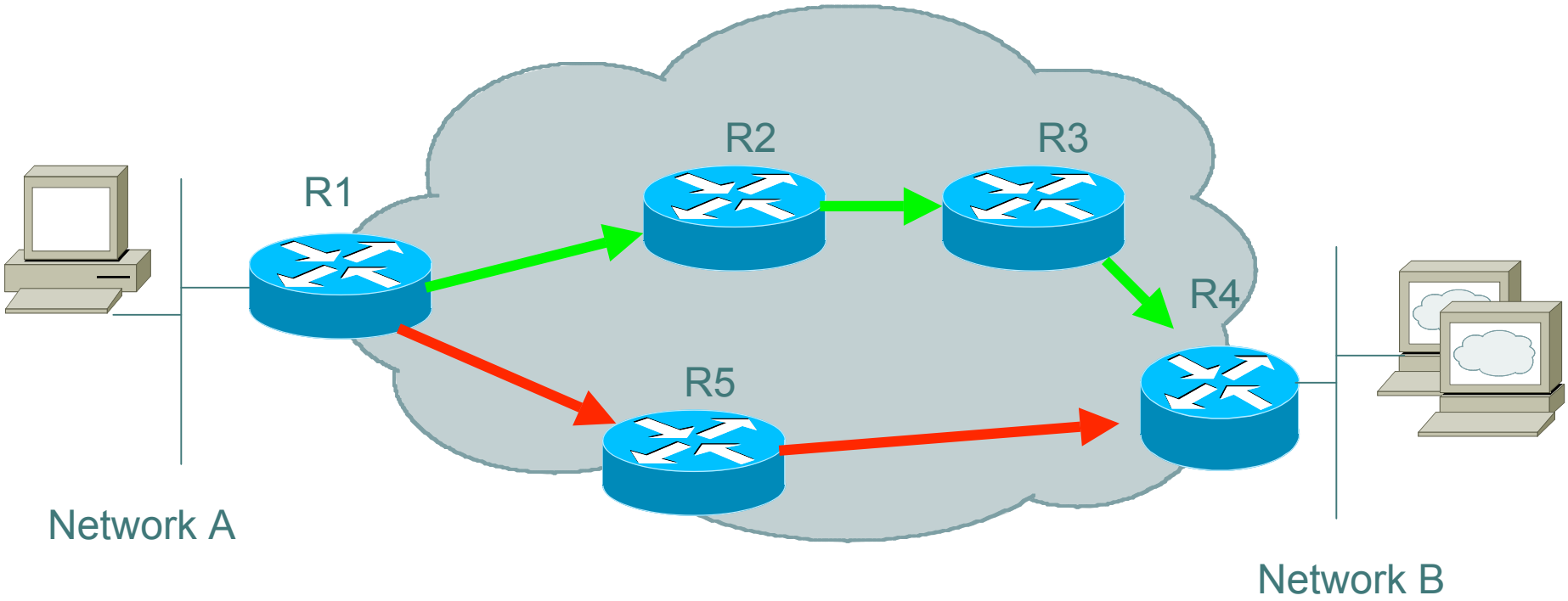
What If Router Becomes Attack Target?

It allows an attacker to:

- Disable the router & network…
- Compromise other routers…
- Bypass firewalls, IDS systems, etc…
- Monitor and record all outgoing an incoming traffic…
- Redirect whatever traffic they desire…

Routing Threats

- Traffic is sent along invalid path
- Traffic is dropped
- Complete network chaos



How Can Routing Threats Be Realized ?

- Protocol error
  - Routing protocol itself
  - TCP issues for BGP
- Software bugs
  - Is it a bug or feature ?
- Active attack
  - More probable than you think !
- Configuration mistakes
  - Most common form of problem

How Bad Is The Problem?

- The Yankee Group's 2003 query of Network operators indicated that 30% - 50% of the network outages were due to configuration error.
- Another IT survey by Infonetics (March 2003) of 8 large Enterprises indicated that network outages cost .1% to 1% of the total revenue ($74.6 million).
  - The most frequent cause of these enterprise outages is server outages.
  - The second most frequent cause is network outages.
    - 50% due to configuration errors.

What Can We Do To Protect The Routing Infrastructure ?

- Understand the Problem
- Establish an Effective Routing Infrastructure Security Policy
  - physical security
  - logical security
  - route authentication
  - route filtering
- Have Procedures In Place For Incident Response
  - procedures for assessing software vulnerability risk
  - auditing configuration modifications

Understand The Problem: What Is A Router?

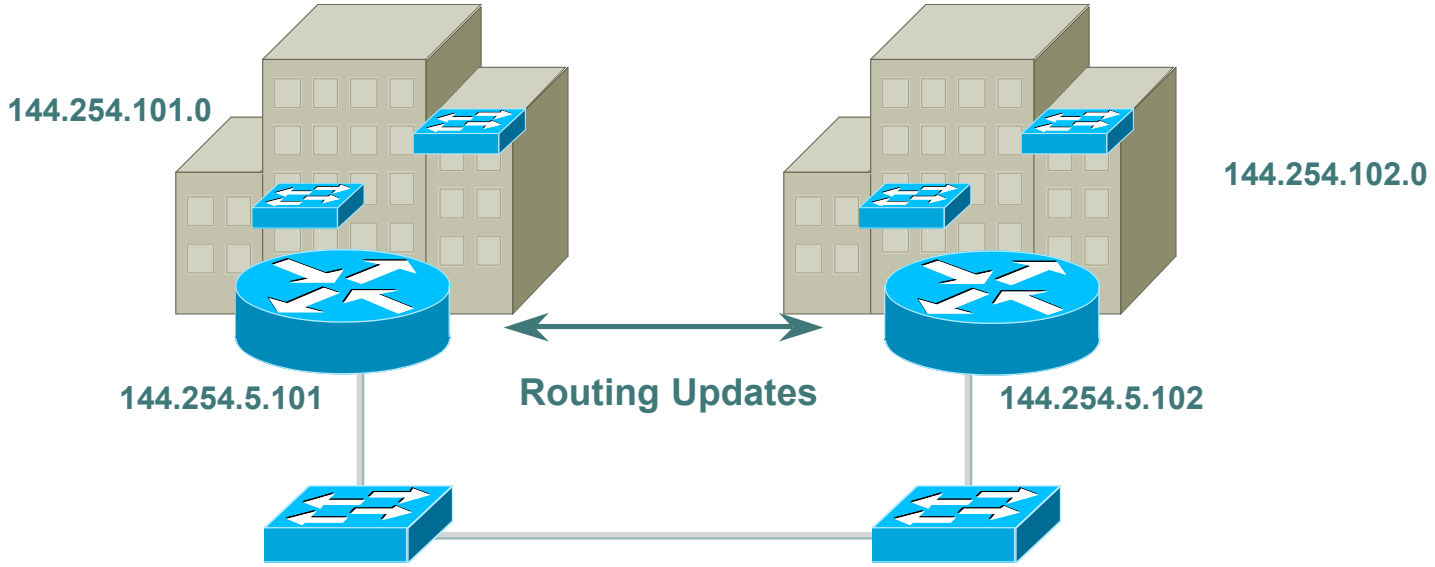
- Routers determine the best path between a given source and destination.
- The decision process is governed by a data structure called the routing table.
- Routing functions and supporting structures are designed to route packets efficiently and reliably, *not securely*.

What Are Routing Security Goals?

- Protect Actual Device
  - Physical concerns
  - Logical concerns
- Protecting Information In Transit
- Ensuring Network Availability

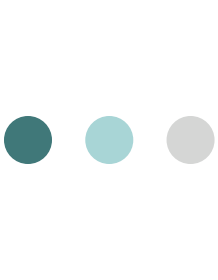
Securing Router-to-Router Communication

- Route authentication
- Routing filters
- Encryption



TCP Reset Attack – Protocol Flaw

- Attacker predicts the target's choice of expected sequence number
- Spoofed packet is sent with the reset bit enabled which resets the TCP connection
- BGP routing protocols runs over TCP



Reality Check

- Software will have bugs
- Network devices will be misconfigured
- Security mitigation techniques reduce the risk of an intrusion

Routing Security Risk Mitigation

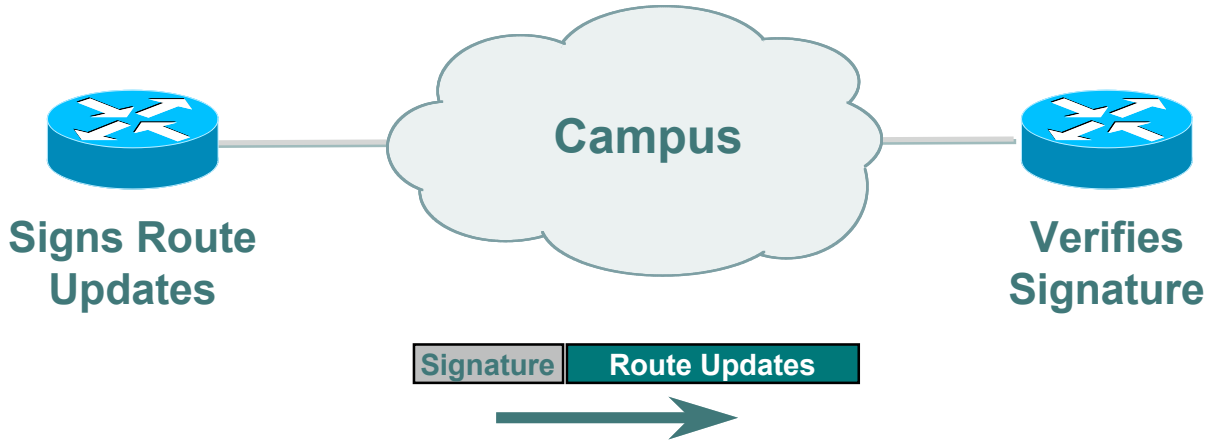
- Route authentication
- Filter routing updates…. especially be careful of redistribution
- Specify which neighbors are allowed to speak to each other

What Is Not Yet Possible

Validating that you have the authorization to send the routes that you are sending

Today's routing protocols only implement techniques for validating source origin and integrity of the contents

Route Authentication

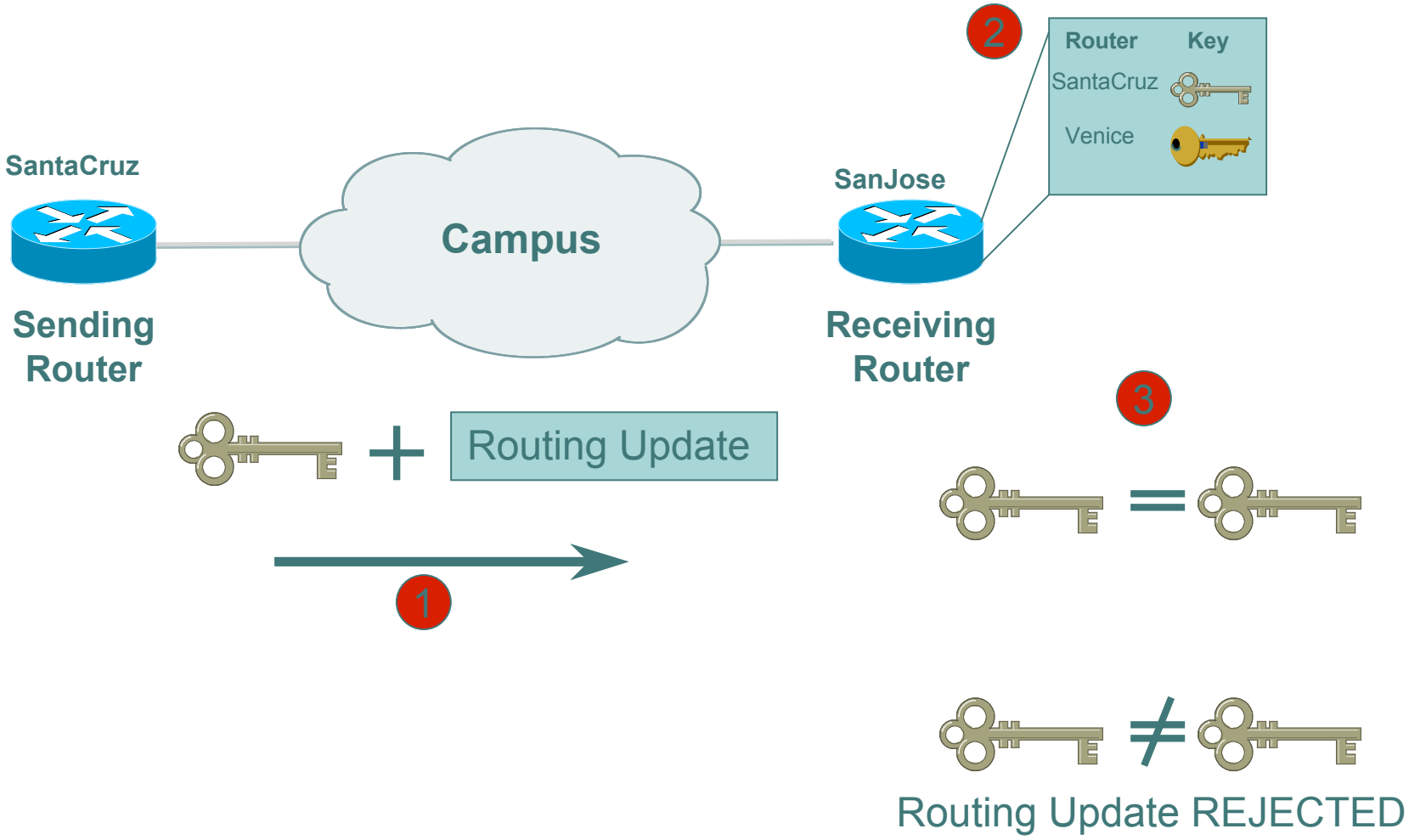


Certifies authenticity of neighbor and integrity of route updates

Why Use Route Authentication

- Route Authentication equates to data origin authentication and data integrity
- In BGP, requires TCP resets to be authenticated so malicious person can't randomly send TCP resets
- In cases where routing information traverses shared networks, someone might be able to alter a packet or send a duplicate packet
- Routing protocols were not initially created with security in mind….this needs to change….

Plaintext Neighbor Authentication

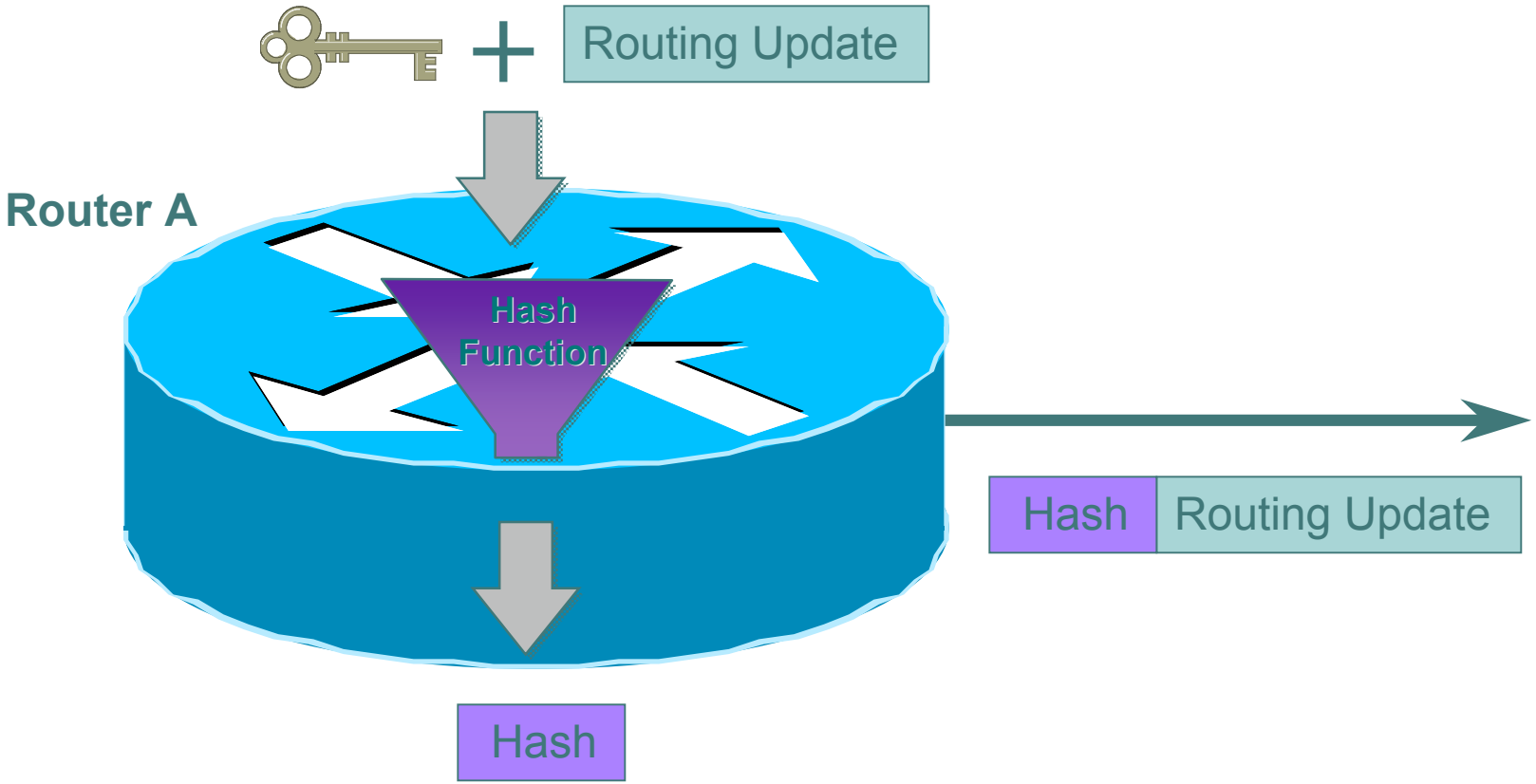


Hash Functions

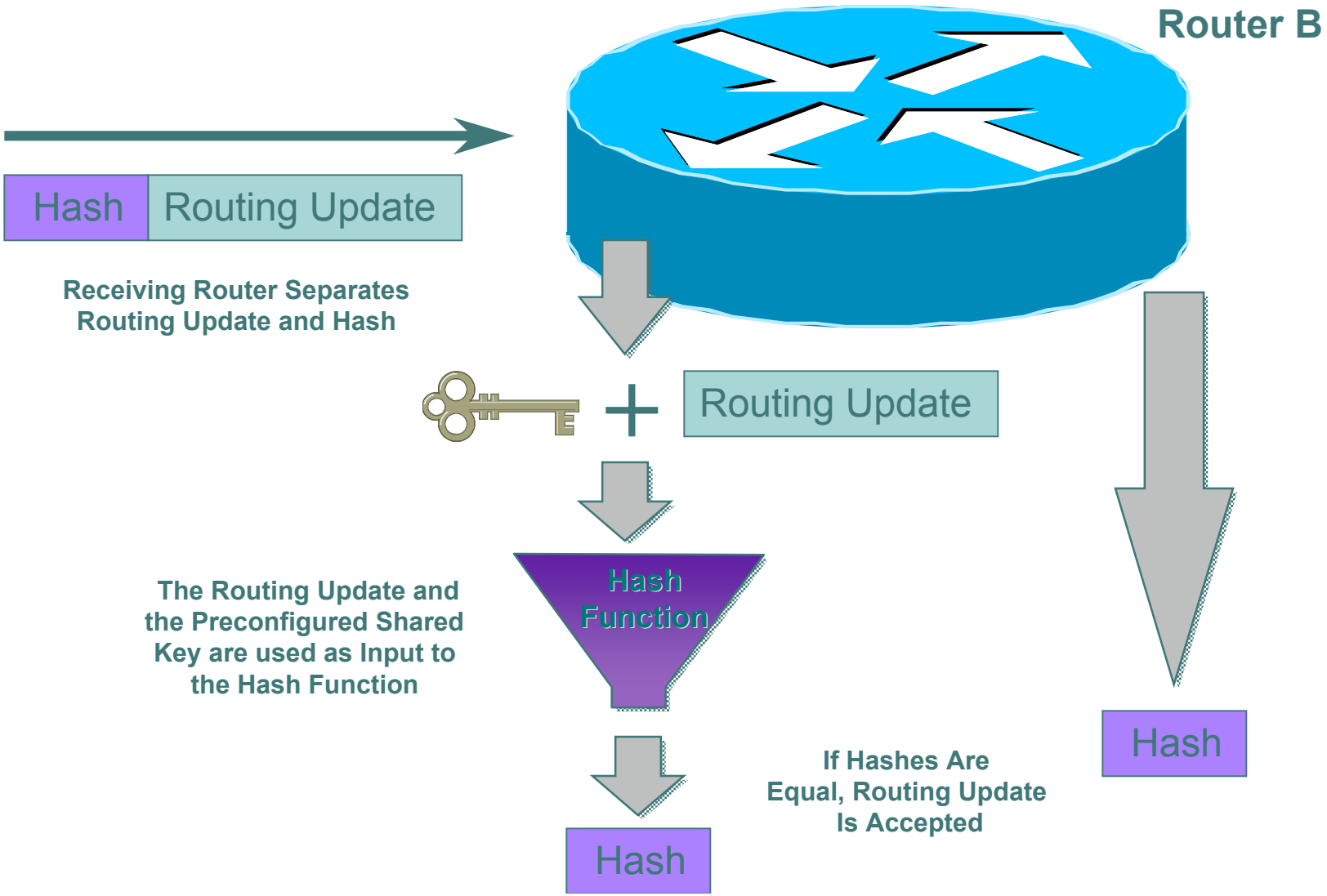
A *hash function* takes an input message of arbitrary length and outputs fixed-length code. The fixed-length output is called the *hash*, or the *message digest*, of the original input message.

Common Algorithms: MD-5 (128), SHA-1 (160)

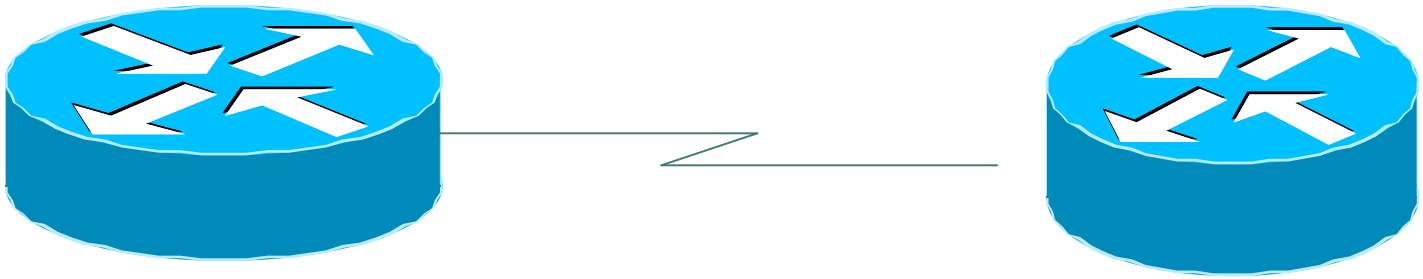
MD-5 Neighbor Authentication: Originating Router



MD-5 Neighbor Authentication: Receiving Router



Sample Configuration (OSPF)



```
interface Loopback0
ip address 70.70.70.70 255.255.255.255

interface Serial2
ip address 192.16.64.2 255.255.255.0

ip ospf message-digest-key 1 md5 mk6
router ospf 10
network 192.16.64.0 0.0.0.255 area 0
network 70.0.0.0 0.255.255.255 area 0
area 0 authentication message-digest
```

```
interface Loopback0
ip address 172.16.10.36 255.255.255.240

interface Serial1/0
ip address 192.16.64.1 255.255.255.0

ip ospf message-digest-key 1 md5 mk6
router ospf 10
network 172.16.0.0 0.0.255.255 area 0
network 192.16.64.0 0.0.0.255 area 0
area 0 authentication message-digest
```

Issues With Current Route Authentication Implementations

- Re-keying is a nightmare
  - session loss
  - route re-computation
- Interoperability issues
- Is SHA-1 a better authentication protocol ?

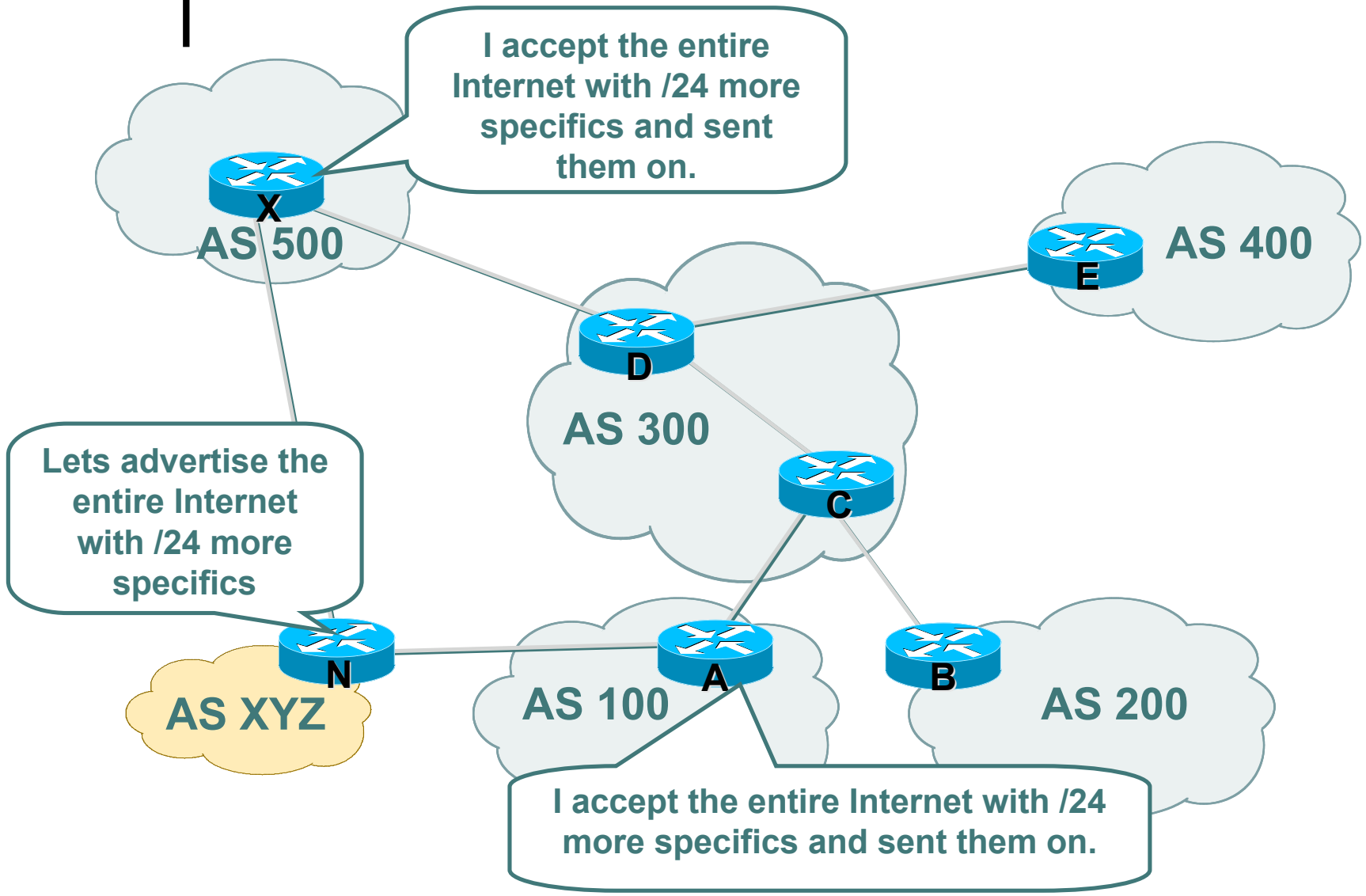
Another option…..

- Use IPsec to secure routing updates
- Advantages
  - automatic re-keying
  - confidentiality of routing updates
- Disadvantages
  - limited interoperability
  - configuration nightmare

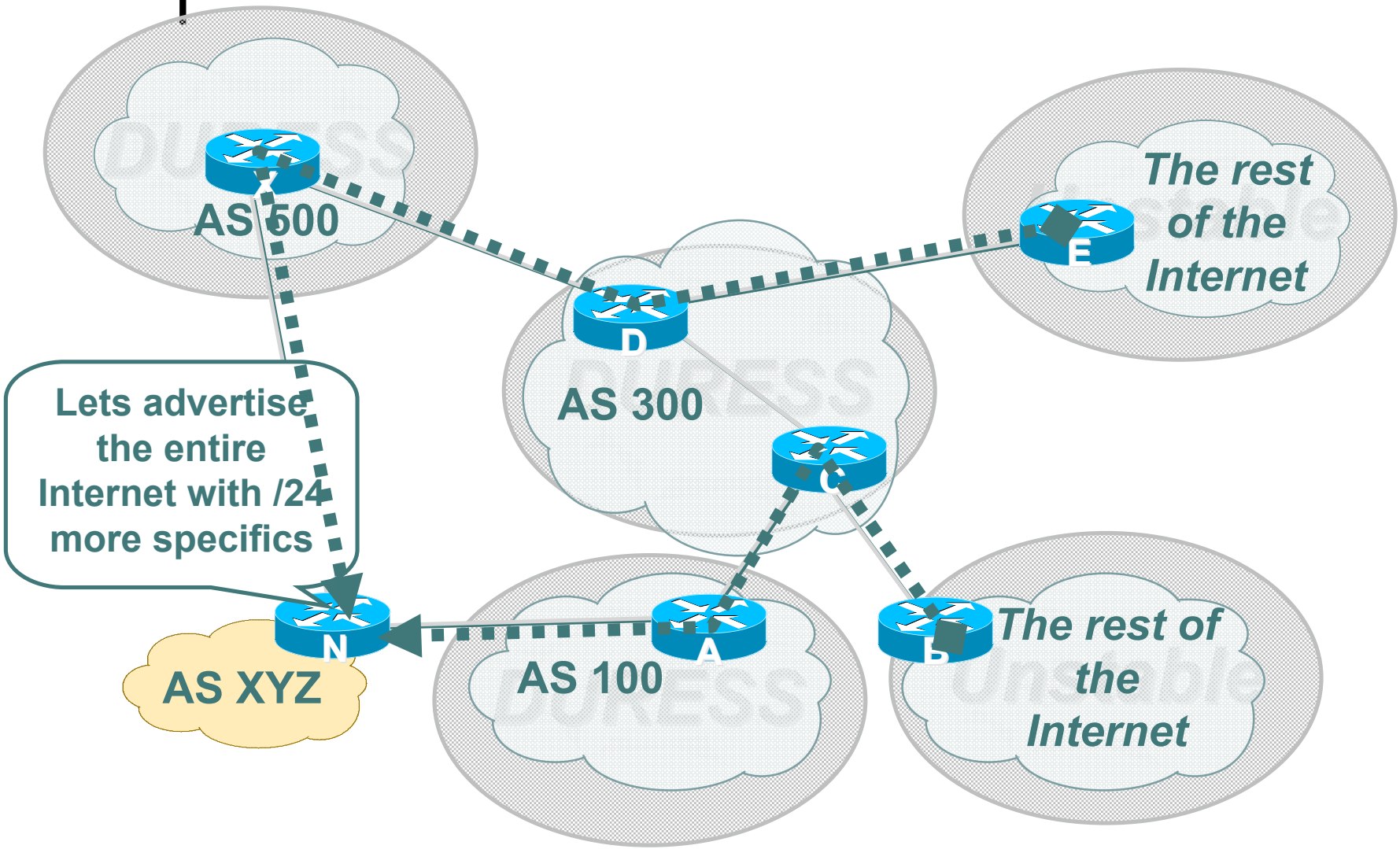
BGP Prefix Filtering

- All BGP Prefixes coming into your network and leaving your network need to be filtered to enforce a policy.
- The problem is most ISPs are not:
  - Filtering Comprehensively
  - Filtering their customer's prefixes
  - Filtering prefixes going out of their network.

Example: No Prefix Filtering

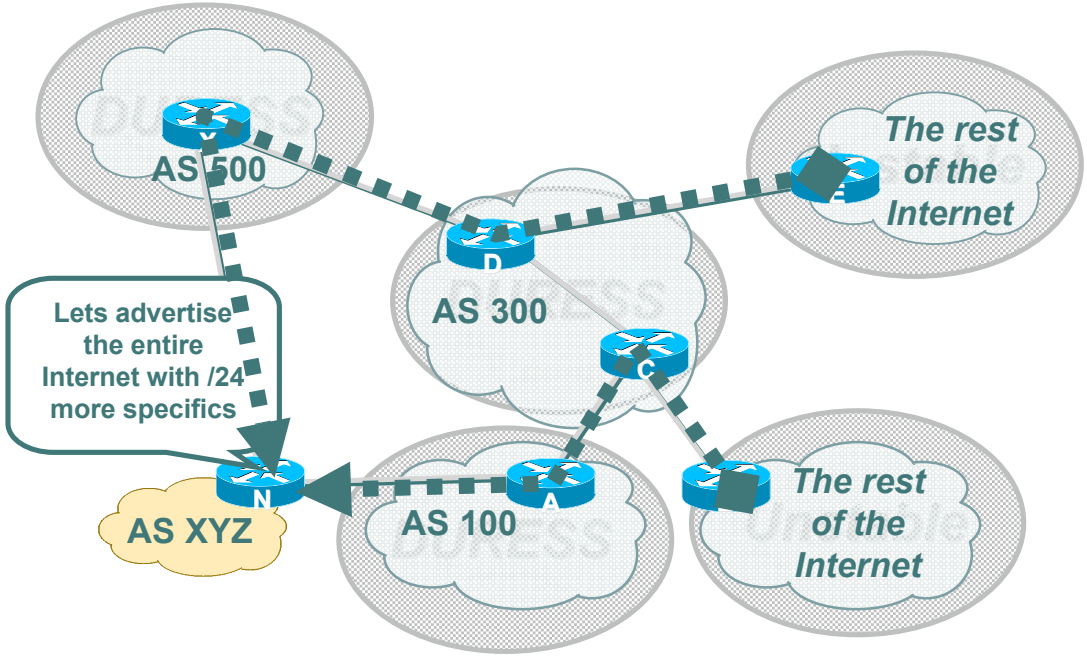


Result of No Prefix Filtering



Impact of No Prefix Filtering

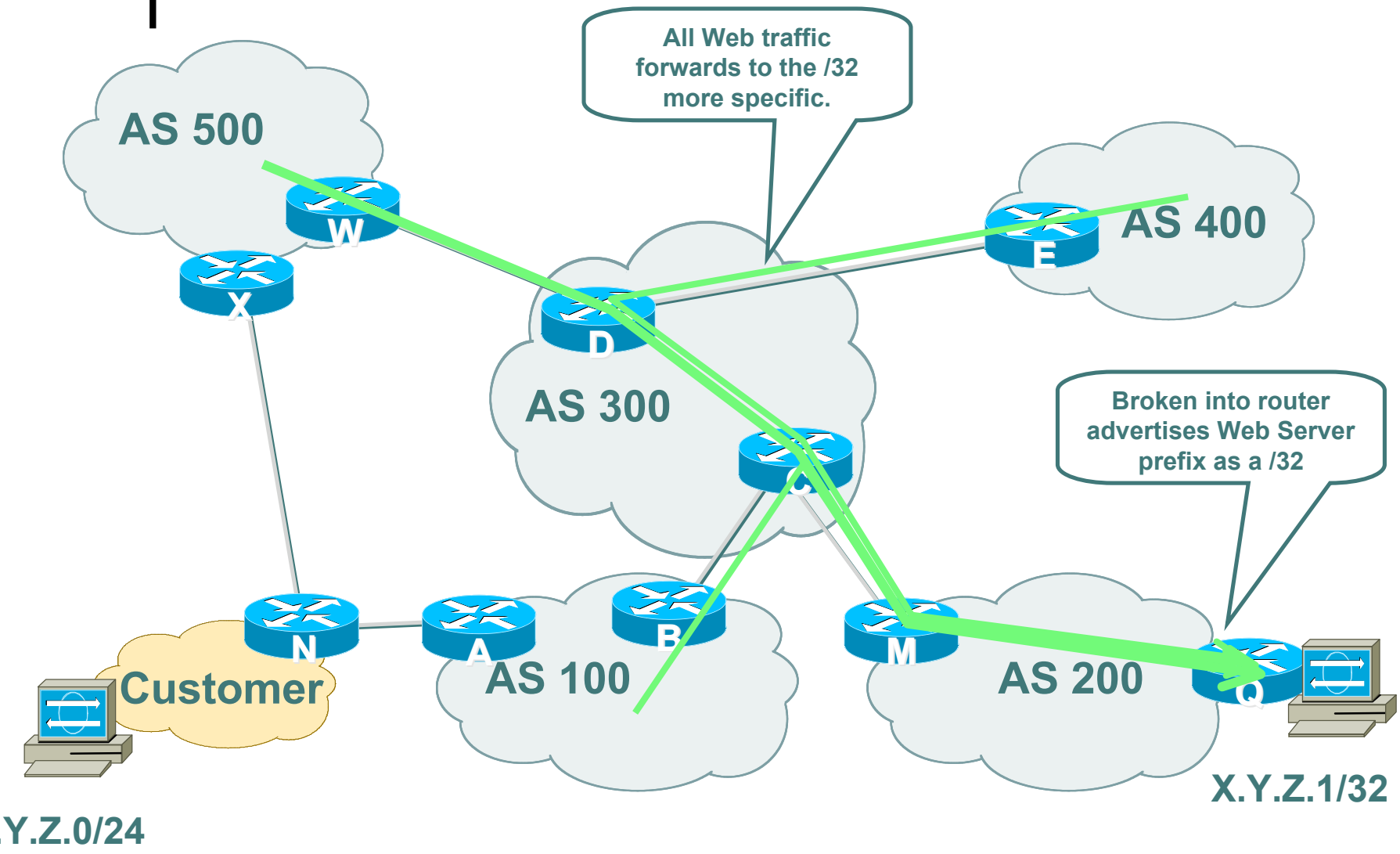
- AS 7007 Incident (1997) was very visible case of problem.
- Key damage are to those ISPs who pass on the garbage.
- Disruption, Duress, and Instability has been an Internet wide effect.



What to Do?

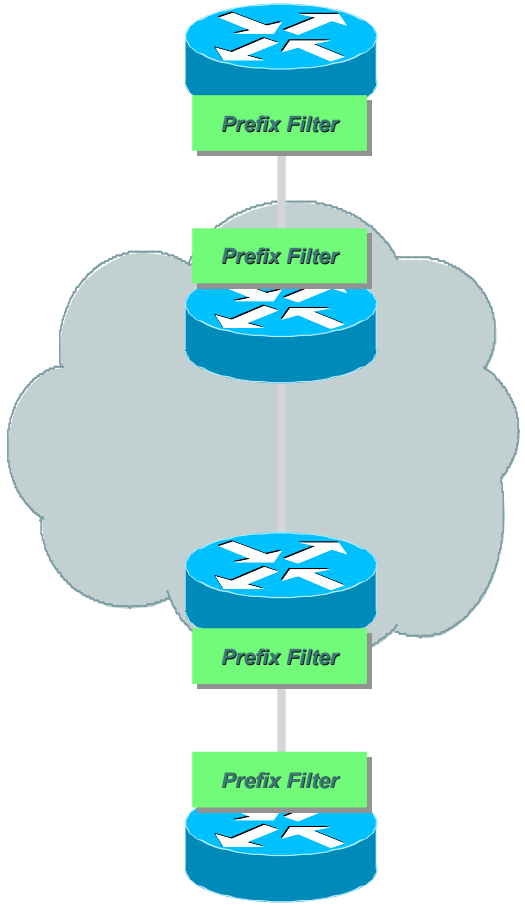
- Take care of your own Network.
  - Filter your customers
  - Filter you advertisements
- Net Police Filtering
  - Mitigate the impact when it happens
- Prefix Filtering and Max Prefix Limits

What Is a Prefix Hijack?



Where to Prefix Filter?

- Customer's Ingress/Egress
- ISP Ingress on Customer (may Egress to Customer)
- ISP Egress to Peer and Ingress from Peer
- Peer Ingress from ISP and Egress to ISP



Receiving Customer Prefixes

- Configuration example on upstream:

```
router bgp 100
  neighbor 222.222.10.1 remote-as 101
  neighbor 222.222.10.1 prefix-list customer in
  !
ip prefix-list customer permit 220.50.0.0/2
ip prefix-list customer deny 0.0.0.0/0 le 32
```

Prefix Filter Bogons and RIR Blocks

- The hard work is done for you via the Bogon Project:
  - http://www.cymru.com/Bogons/index.html
- Cisco Template by Barry Greene
  - ftp://ftp-eng.cisco.com/cons/isp/security/Ingress-Prefix-Filter-Templates/
- Juniper Template by Steven Gill
  - http://www.qorbit.net/documents.html

Other BGP Security/Policy Techniques

- BGP Community Filtering
- MD5 Keys on the eBGP and iBGP Peers
- Max Prefix Limits
- RFC 1998 +++
- BGP Dampening with RIPE-299

What Can You Do to Help?

- Prefix Filter your customers.
- Prefix Filter the Bogons and police other prefixes coming into your network.
- Prefix Filter what you send to the Internet.
- Protect your self
- Protect the Internet
- Stop the BGP Prefix Injection technique

Peering with Other ISPs

- Similar to EBGP customer aggregation except inbound prefix filtering is rarely used (lack of global registry)
- Use maximum-prefix and prefix sanity checking instead
- Still use per-neighbor passwords!

BGP Template: ISP peers peer-group

neighbor nap peer-group

neighbor nap description for peer ISPs

neighbor nap remove-private-AS

neighbor nap version 4

neighbor nap prefix-list sanity-check in

neighbor nap prefix-list cidr-block out

neighbor nap route-map nap-out out

neighbor nap maximum prefix 30000

BGP Template: ISP peers route-map

```
route-map nap-out permit 10
match community 1            ; customers only
set metric-type internal  ; MED = IGP metric
set ip next-hop peer-address ; our own
```

Peer Groups for NAPs: Sanity-Check Prefix-List

```
# FIRST - FILTER OUT YOUR IGP ADDRESS SPACE!!
ip prefix-list sanity-check seq 5 deny 0.0.0.0/32
# deny the default route
ip prefix-list sanity-check seq 10 deny 0.0.0.0/8 le 32
# deny anything beginning with 0
ip prefix-list sanity-check seq 15 deny 0.0.0.0/1 ge 20
# deny masks > 20 for all class A nets (1-127)
ip prefix-list sanity-check seq 20 deny 10.0.0.0/8 le 32
# deny 10/8 per RFC1918
ip prefix-list sanity-check seq 25 deny 127.0.0.0/8 le 32
# reserved by IANA - loopback address
ip prefix-list sanity-check seq 30 deny 128.0.0.0/2 ge 17
deny masks >= 17 for all class B nets (129-191)
ip prefix-list sanity-check seq 35 deny 128.0.0.0/16 le 32
# deny net 128.0 - reserved by IANA
ip prefix-list sanity-check seq 40 deny 172.16.0.0/12 le 32
# deny 172.16 as RFC1918
```

Peer Groups for NAPs: Sanity-Check Prefix-List

```
ip prefix-list sanity-check seq 45 deny 192.0.2.0/24 le 32
# class C 192.0.20.0 reserved by IANA
ip prefix-list sanity-check seq 50 deny 192.0.0.0/24 le 32
# class C 192.0.0.0 reserved by IANA
ip prefix-list sanity-check seq 55 deny 192.168.0.0/16 le 32
# deny 192.168/16 per RFC1918
ip prefix-list sanity-check seq 60 deny 191.255.0.0/16 le 32
# deny 191.255.0.0 - IANA reserved (I think)
ip prefix-list sanity-check seq 65 deny 192.0.0.0/3 ge 25
# deny masks > 25 for class C (192-222)
ip prefix-list sanity-check seq 70 deny 223.255.255.0/24 le 32
# deny anything in net 223 - IANA reserved
ip prefix-list sanity-check seq 75 deny 224.0.0.0/3 le 32
# deny class D/Experimental
```

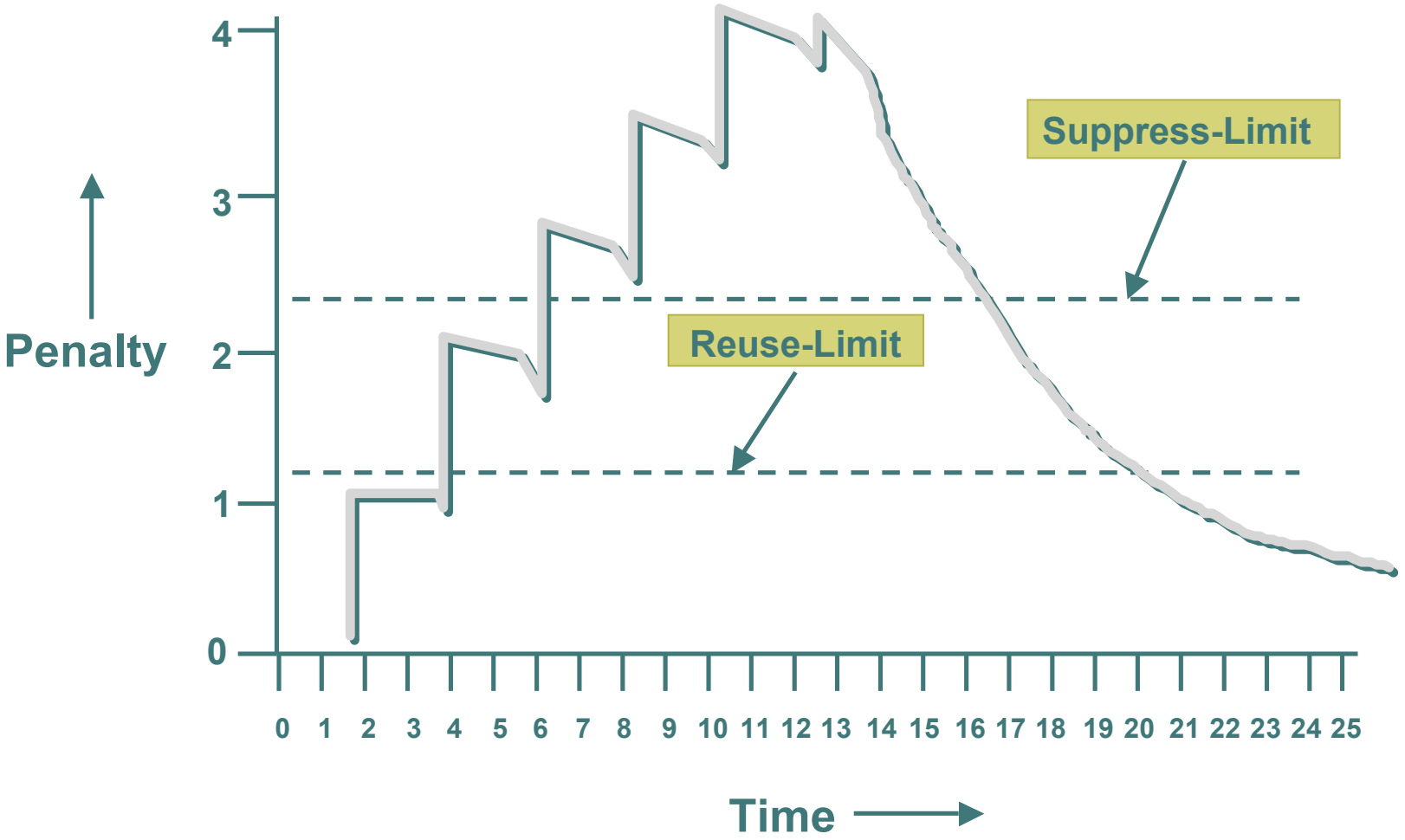
Route Flap Dampening

- Route flaps ripple through the entire Internet
  - Up and down of path
  - Change in attributes
- Wastes CPU
- Objective: Reduce the scope of route flap propagation

Route Flap Dampening (Cont.)

- Fast convergence for normal route changes
- History predicts future behavior
- Advertise stable suppressed routes

Route Flap Dampening



Flap Dampening: Operation

- Add fixed penalty for each flap
  - Flap = withdraw or attribute change
- Exponentially decay penalty
  - Half-life determines rate
- Penalty above suppress-limit = do not advertise up route
- Penalty decayed below reuse-limit = advertise route

Flap Dampening: Operation

- History paths
- Done only for external path
- Alternate paths still usable
- Suppress-limit, reuse-limit and half-life time give control
- Less overhead

Selective Dampening

- Selective dampening based on
  - AS-PATH
  - Community
  - Prefix
- Variable dampening

Dampening Configuration

- bgp damping <halflife-time> <reuse> <suppress> <maximum-suppress-time>
- Example:

```
router bgp 109
bgp dampening route-map SELECTIVE _DAMPENING
!
access-list 110 permit ip any 255.255.255.0 0.0.0.255
access-list 111 permit ip any any
!
route-map SELECTIVE_DAMPENING permit 10
match ip address 110
set dampening 30 125 2000 120
!
route-map SELECTIVE_DAMPENING permit 20
match ip address 111
set dampening 25 750 2000 45
!
```

Audit and Validate Your Routing Infrastructures

- Are appropriate paths used?
  - check routing tables
  - verify configurations
- Is router compromised?
  - check access logs

Routing Security Conclusions

- Current routing protocols do not have adequate security controls
- Mitigate risks by using a combination of techniques to limit access and authenticate data
- Be vigilant in auditing and monitoring your network infrastructure

Router Security Considerations

- Segment areas for route redistribution and ensure limited access to routers in critical backbone areas
- Design networks so outages don't affect entire network but only portions of it
- Control router access….watch against internal attacks on these systems. Use different passwords for router enable and monitoring system root access.
- Latest scanning craze for http access!!!

Routing Security Summary

- Consider MD5 authentication
- Always filter routing updates….especially be careful of redistribution
- How paranoid are you?
  - Specify which neighbors are allowed to speak to each other

Auditing / Logging Tools

- Nmap and ndiff
- Nessus
- The Coroner's Toolkit (TCT)
- Tripwire
- TCPdump

Best Part ……..They are all FREE!!

Nmap

- Identifies services and hosts on a network
- Uses ICMP ECHO sweeps and connections to TCP, UDP and RPC ports
- GUI front-ends available
- Runs on almost every OS
- http://www.nmap.org

Nmap Features

- -sU: UDP port scan
- -sR: RPC protocol scan
- -sI: Ident scan
- -P0: disable pinging hosts before scanning
- -n: don’t do DNS resolution
- Various scan speeds
- Multiple output formats
  - XML
  - machine-parsable
  - greapable

Managing Nmap with Ndiff

- http://www.vinecorp.com/ndiff
- Ndiff includes 3 Perl scripts
  - Ndiff
    - Compares two Nmap files
  - Ngen
    - Creates baseline from user definition
  - Nrun
    - Runs Nmap and ndiff in controllable manner
    - Can run regularly out of cron

The Coroner's Toolkit (TCT)

- 3 tools for UNIX forensics
  - grave-robber: data collection framework
    - Gathers network, host config and user info
    - Saves executables of running programs which have been deleted from disk
    - Make MD5 signatures of collected data
  - unrm and lazarus: recover deleted files
    - unrm pulls unused blocks from a disk drive
    - Lazarus takes ouput of unrm and identifies blocks of intelligible data
  - mactime: checks file access, modify and created times
- http://www.porcupine.org/forensics/tct.html

Tripwire

- www.tripwire.com
- Makes a ‘fingerprint’ of your OS
  - store on read-only media
- Runs from cron every night to verify checksums
  - emails new/changed/missing file information
- Install and run before putting host on net
- Have reports mailed to a different machine

More Useful ‘FREE’ Tools

- Sniffers
  - TCPDump
  - Ethereal
  - Dsniff
- Password Crackers
  - Crack
  - Npasswd and passwd+
- IDS
  - Snort
- Miscellaneous
  - RANCID
    - Monitors a devices configuration
    - Emails differences from previous collection

Logging Pitfalls

- Do you know how to map an IP address to a specific destination?!? (which machine correlates to an IP address)
- Ensure timestamps are valid (NTP sources)
- Log only what's needed….avoid information overload

Data Collection/Correlation

- Collecting data
  - Time correlation, common formatting, etc.
  - These issues are addressed by numerous projects
    - IDEF, IDMEF, CIDF, D-Shield, Incidents.org, etc.
- Correlating data
  - How can we tell what events are related?
  - Attacker's goals determine behavior
  - Multiple hypothesis tracking

Collecting Incident Data

Traditional Forensics

- Immediately shutdown the system (or pull the power cord)
- Make a forensic duplicate
- Perform analysis on the duplicate
- Live system data is rarely recovered.

Infrastructure Forensics

- Live system data is the most valuable.
- Immediate shutdown destroys all of this data.
- Persistent (flash) data will likely be unchanged and useless.
- Investigators must recover live data for analysis

Incident Response

- DO NOT REBOOT THE DEVICE.
- Change nothing, record everything.
- Before you say it is an accident, make sure it isn’t an incident…
- Before you say it is an incident, make sure it isn’t an accident…

Incident Response Evidence

Detailed, Methodical, Unquestionable….

- Where you received the evidence…
- When you received the evidence…
- Who you received the evidence from…
- What your seizure methods were…
- Why you seized the evidence…
- How you maintained your chain of custody…

Assessing Damage

- Check log statistics for unusual activity on corporate perimeter network access points, such as Internet access or dial-in access.
- Verify infrastructure device checksum or operating system checksum on critical servers to see whether operating system software has been compromised.
- Verify configuration changes on infrastructure devices and servers to ensure that no one has tampered with them.

Assessing Damage (cont)

- Check sensitive data to see whether it was accessed or changed.
- Check traffic logs for unusually large traffic streams from a single source or streams going to a single destination.
- Run a check on the network for any new or unknown devices.
- Check passwords on critical systems to ensure that they have not been modified (it would be prudent to change them at this point).

Reporting Guidelines

- Keep the technical level of detail low.
- Work with law enforcement officials to ensure that evidence is protected.
- Delegate all handling of the public to in-house PR people who know how to handle the press.
- Do not break or halt lines of communication with the public.
- Keep the speculation out of public statements.
- Do not allow the public attention to detract from the handling of the event.

RFC 3013 (Recommended ISP Security Services & Procedures)

- ISPs have a duty to make sure that their contact information, in Whois, in routing registries [RFC1786] or in any other repository, is complete, accurate and reachable.
- ISPs should have processes in place to deal with security incidents that traverse the boundaries between them and other ISPs.
- ISPs SHOULD be able to conduct such communication over a secure channel.
- ISPs SHOULD be proactive in notifying customers of security vulnerabilities in the services they provide.

RFC 3013 Notifying Customers

Information that should be included:

- who is coordinating response to the incident
- the vulnerability
- how service was affected
- what is being done to respond to the incident
- whether customer data may have been compromised
- what is being done to eliminate the vulnerability
- the expected schedule for response, assuming it can be predicted

Useful Resources

- http://www.ietf.org
- http://www.sans.org
- http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/default.asp
- http://www.robertgraham.com/pubs/network-intrusion-detection.html

Detecting An Incident

- Accounting discrepancies
- Data modification and deletion
- Users complaining of poor system performance
- Atypical traffic patterns
- Atypical time of system use
- Large numbers of failed login attempts

Intrusion Mitigation

- Regularly Patch OS
- Periodically review system logs
- Keep technical documentation updated
- Sanity check network traffic
- Have incident handling plan
  - Decision-making tool
  - Evidence handling procedures

DoS - Router CPU Vulnerabilities

CPU Overload

- Attacks on applications on the Internet have affected router CPU performance
- 100,000+ hosts infected with most hosts attacking routers with forged-source packets
- Small packet processing is taxing on many routers…even high-end
- Filtering useful but has CPU hit
- MD-5 authentication DoS

Today's DoS Prevention

- Allow only good traffic into your network (ingress filtering)
- Allow only good traffic out of your network (egress filtering)
- Stop directed broadcast traffic (to avoid being an amplifier)

Deny all and permit only what's needed is most effective policy

DoS Filtering

(* these networks may be reallocated)

Description	Network
default	0.0.0.0 /8
loopback	127.0.0.0 /8
RFC 1918	10.0.0.0 /8
RFC 1918	172.16.0.0 /12
RFC 1918	192.168.0.0 /16
Net Test	192.0.2.0 /24
Testing devices *	192.18.0.0 /15
IPv6 to IPv4 relay *	192.88.99.0 /24
RFC 1918 nameservers *	192.175.48.0 /24
End-node auto configuration *	169.254.0.0 /16

Today's DoS Prevention

- Allow only good traffic into your network (ingress filtering)
- Allow only good traffic out of your network (egress filtering)
- Stop directed broadcast traffic (to avoid being an amplifier)

Deny all and permit only what's needed is most effective policy

DoS/DDoS Tools

- Vendor provided
  - Arbor TrafGen
- Open source
  - stream
  - litestorm
  - rc8.o
  - f__kscript
  - slice3

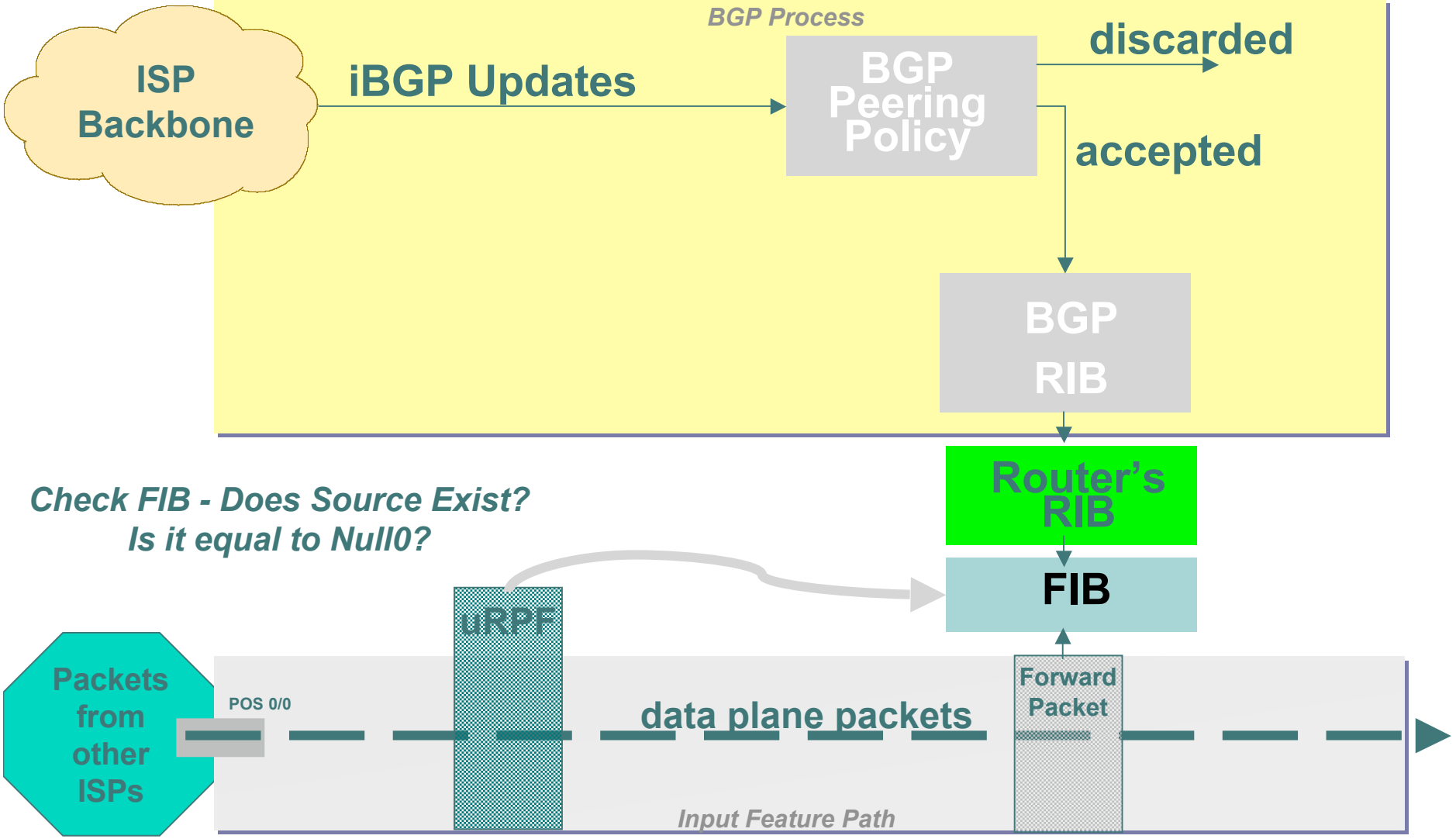
Using IP Routing as a Security Tool

- IP Routing can be used to manipulate traffic on a network to:
  - Null0 (Black Hole)
  - Shunts
  - Sink Hole
  - Analysis Devices
  - Clean up Devices
  - Rate-Limit

Source Based Remote Triggered Black Hole Filtering

- What do we have?
  - *Black Hole Filtering* **– If the** *destination* **address equals Null 0 we drop the packet.**
  - *Remote Triggered* – **Trigger a prefix to equal Null 0 on routers across the Network at iBGP speeds.**
  - uRPF Loose Check – **If the** *source* **address equals Null 0, we drop the packet.**
- Put them together and we have a tool to trigger drop for any packet coming into the network whose source or destination equals Null 0!

uRPF Loose Check



Remote Triggered Drops

- Use one or both techniques to contain a worm
  - Internal deployments limit spread within enterprise
  - Edge deployments limit spread to internet and/or other external destination
- Depending on null0 location, effective quarantine tool
- Rapid reaction, highly scaleable
  - Proven technique used by large service providers

DoS Mitigation Summary

- Consider MD-5 authentication in your routing infrastructures.
- Filter obviously bogus networks at ingress / egress points.
- Use prefix filters.
- Use remote triggered filtering techniques.
- Understand your traffic patterns and help deter attacks to downstream and upstream neighbors.

THANK YOU!

Merike Kaeo - author of:
Designing Network Security, 2nd Edition
ISBN 1587051176