

Three Practical Ways to Improve Your Network

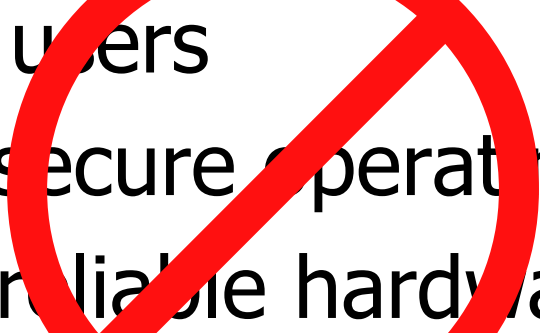
Kevin Miller

Carnegie Mellon University

kcm@cmu.edu

Carnegie Mellon®

Overview

- Eliminate users
 - Perfectly secure operating systems
 - Infinitely reliable hardware
- 

Emphasis on the *practical*

Overview

- IP Anycast
 - Deployment Example
- Source Address Verification
 - Unicast Reverse Path Forwarding
- uRPF for Host Filtering
 - Fast filtering by IP source address

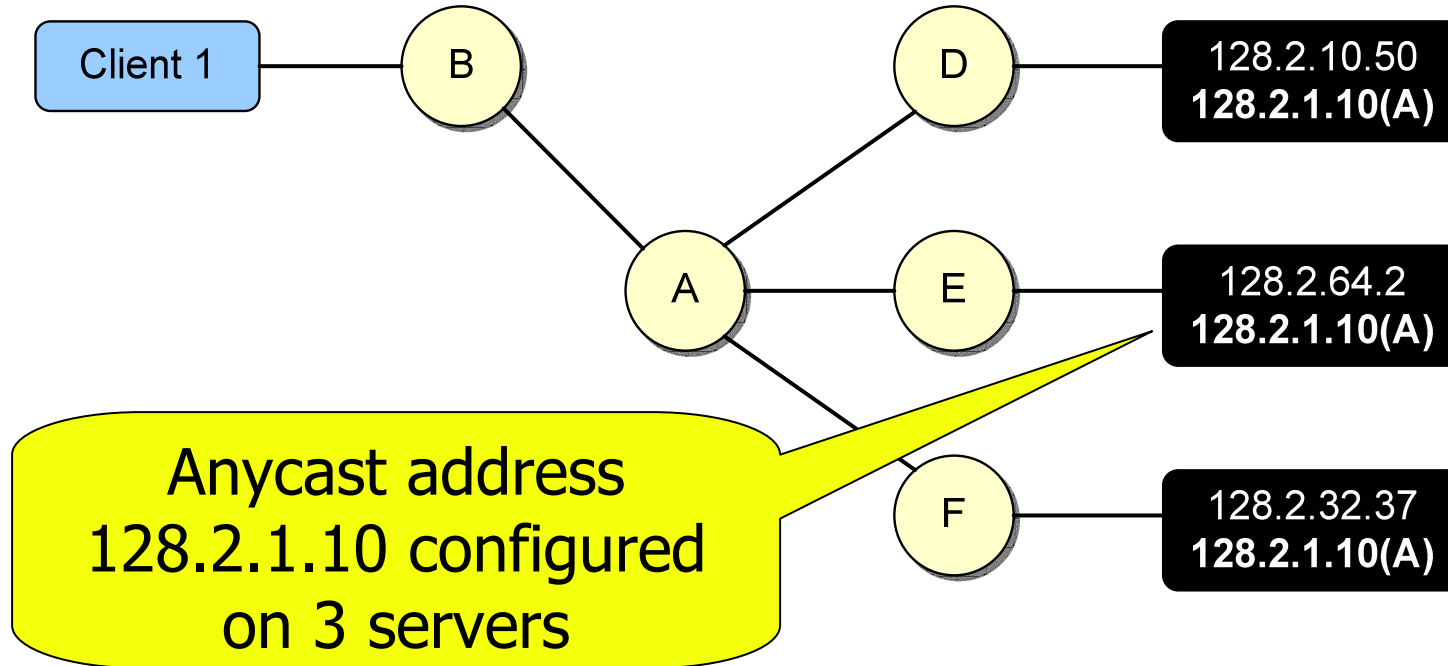
IP Anycast

- Current “Anycast” is “shared unicast”
 - Just a method of configuring routers, hosts in slightly different way
 - Not multicast, don’t be worried
- Assign IP address to multiple hosts
 - Still need a unique management address
- Announce routes to anycast IPs from multiple locations

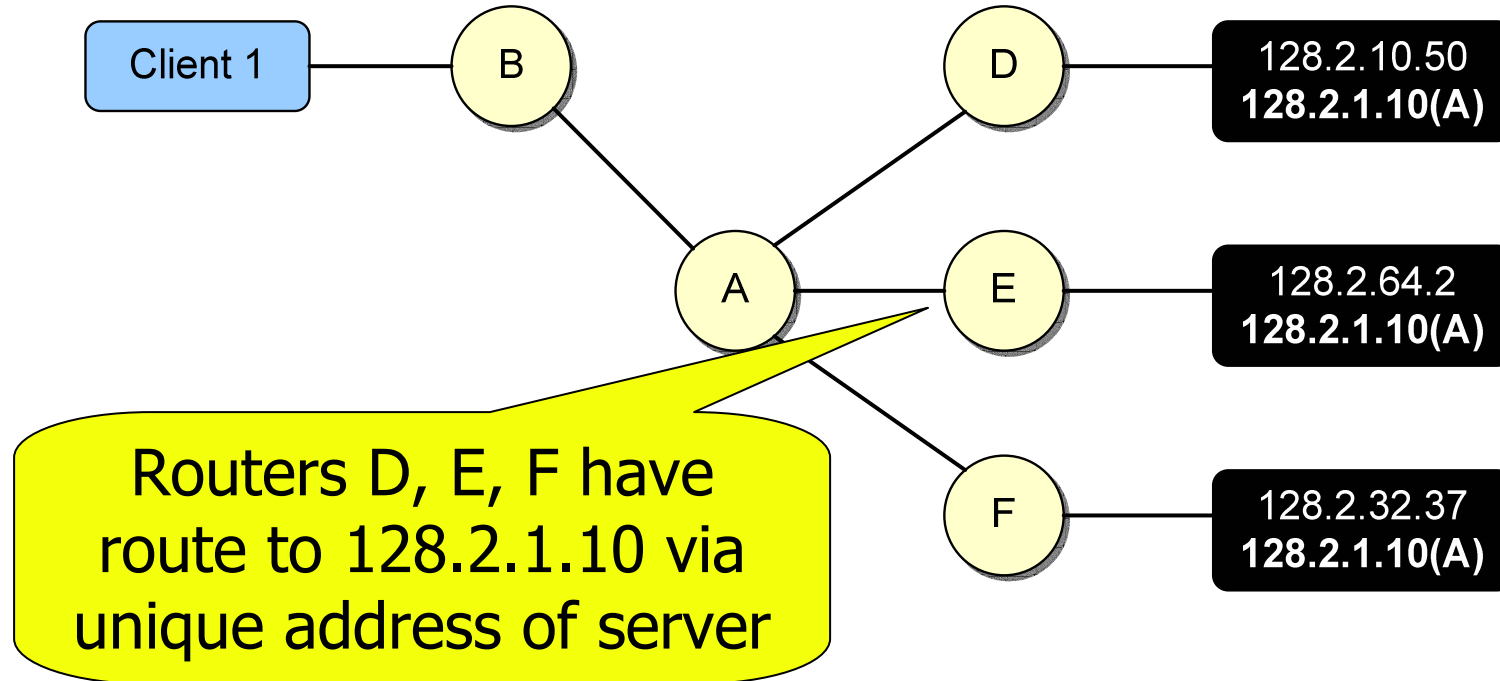
IP Anycast - Configuring

- Configure servers to respond on anycast addresses
 - Often, no additional work required
- Configure clients to use anycast address instead of unique address
 - Recursive DNS: anycast IP configured as resolver
 - Other protocols: update DNS A record

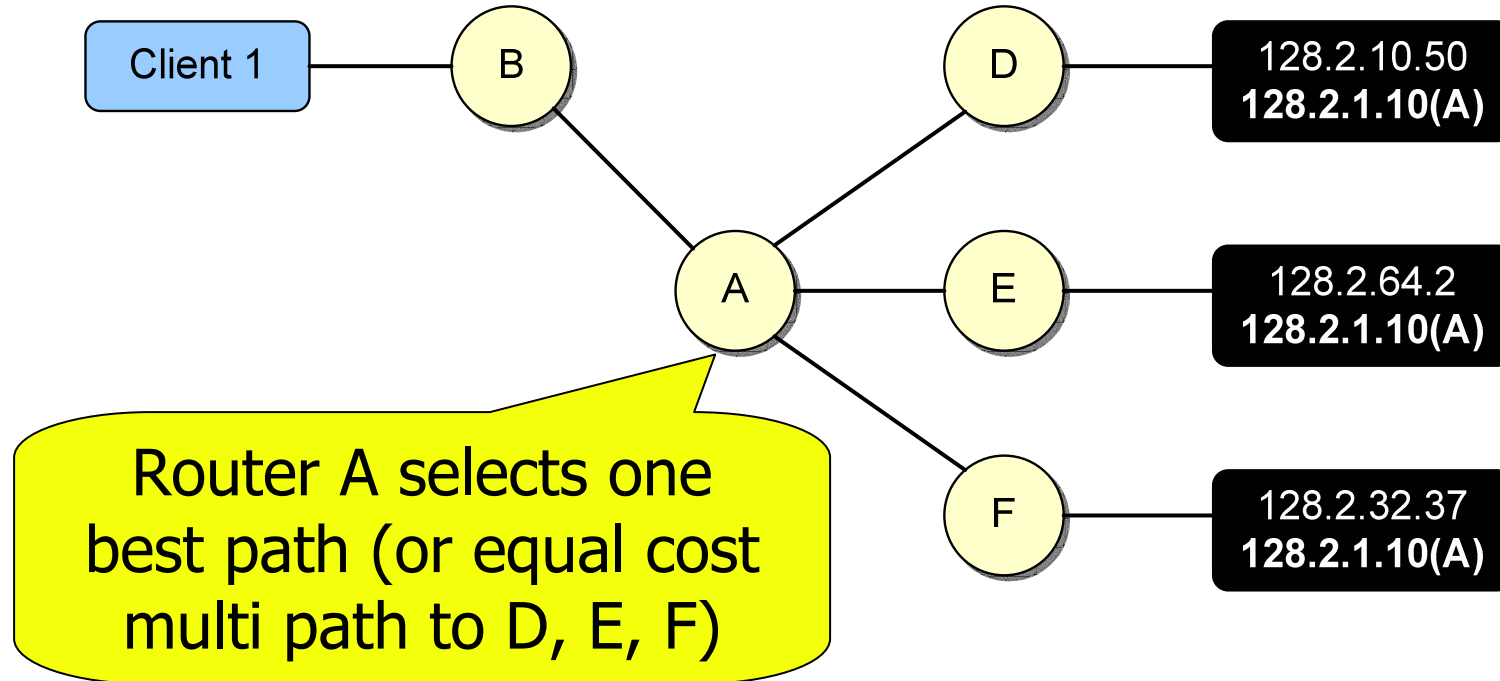
Anycast in Action



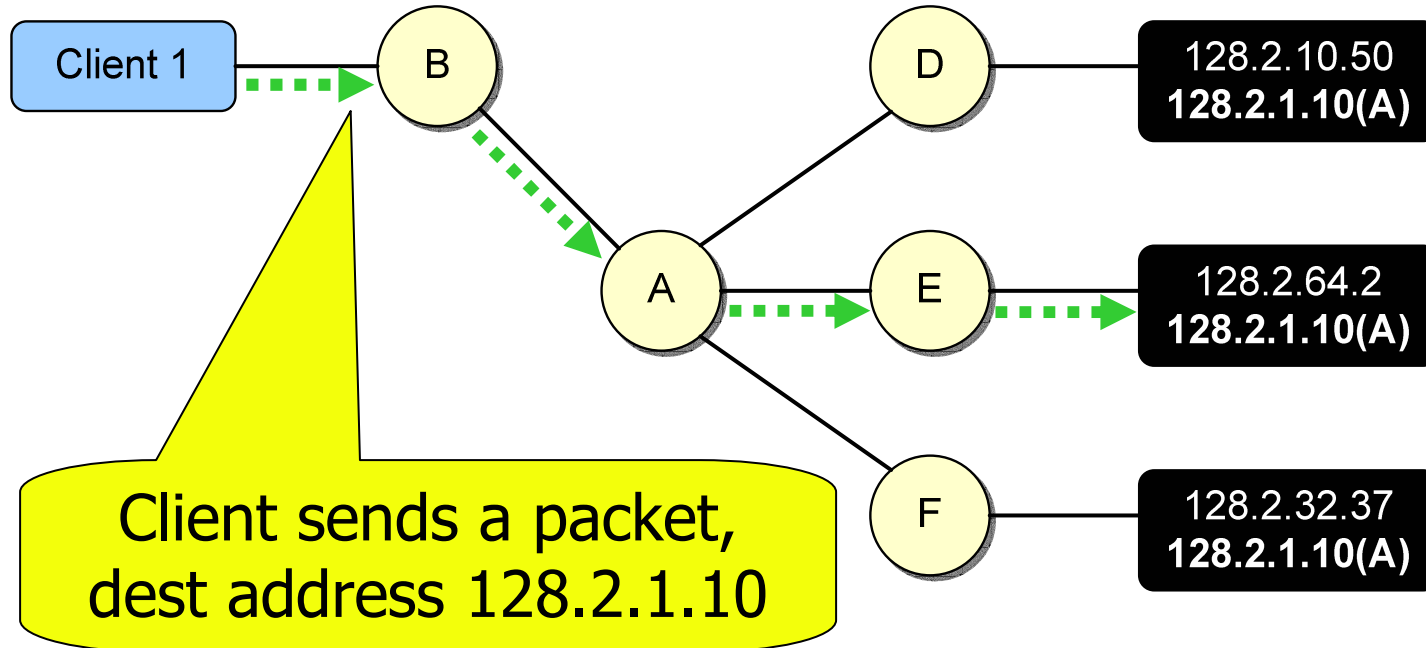
Anycast in Action



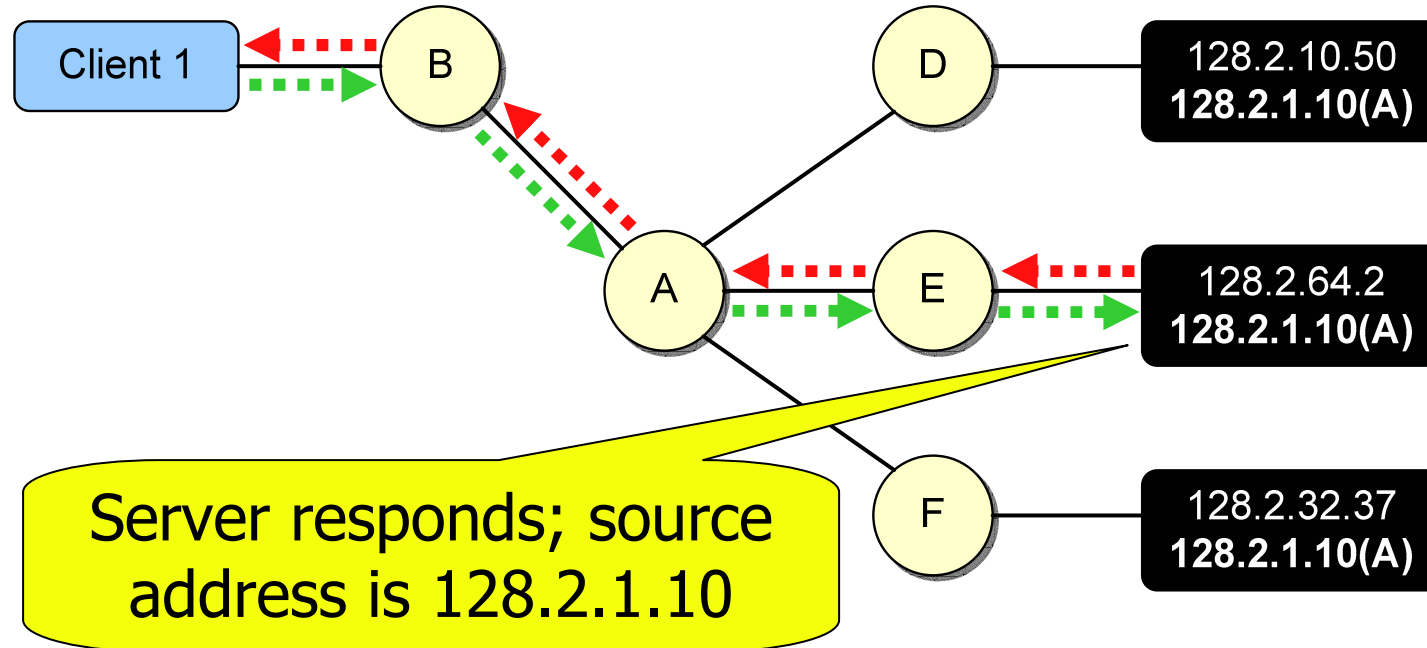
Anycast in Action



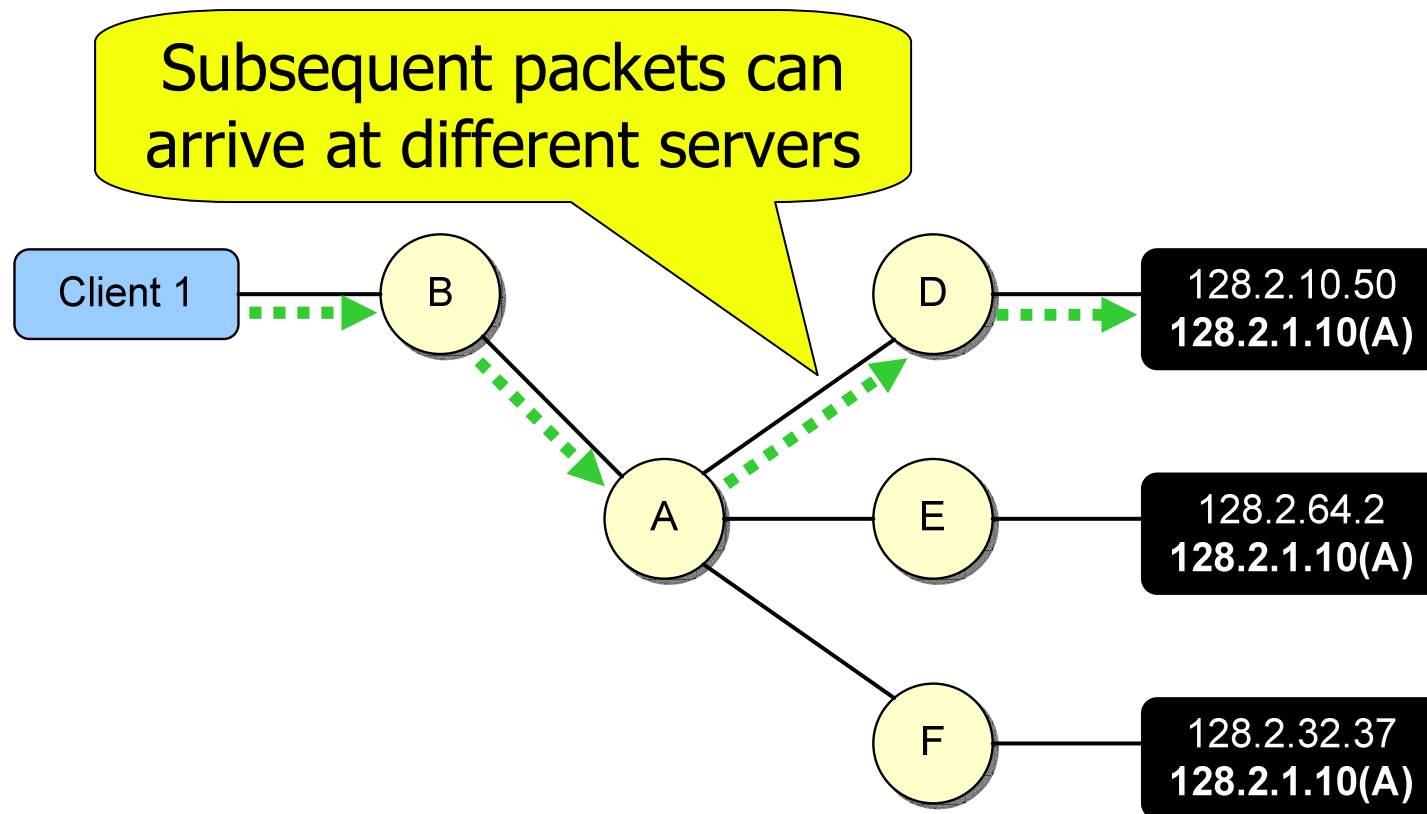
Anycast in Action



Anycast in Action



Anycast in Action



Caching DNS

- Problems
 - Network appears slow on most OSs when primary DNS server is unreachable
 - Difficult to relocate caching DNS servers
- Anycast as the solution
 - Client transparency (easy to move)
 - Service reliability

DNS Clients are Forgetful

OS Resolvers that don't remember a dead DNS server:

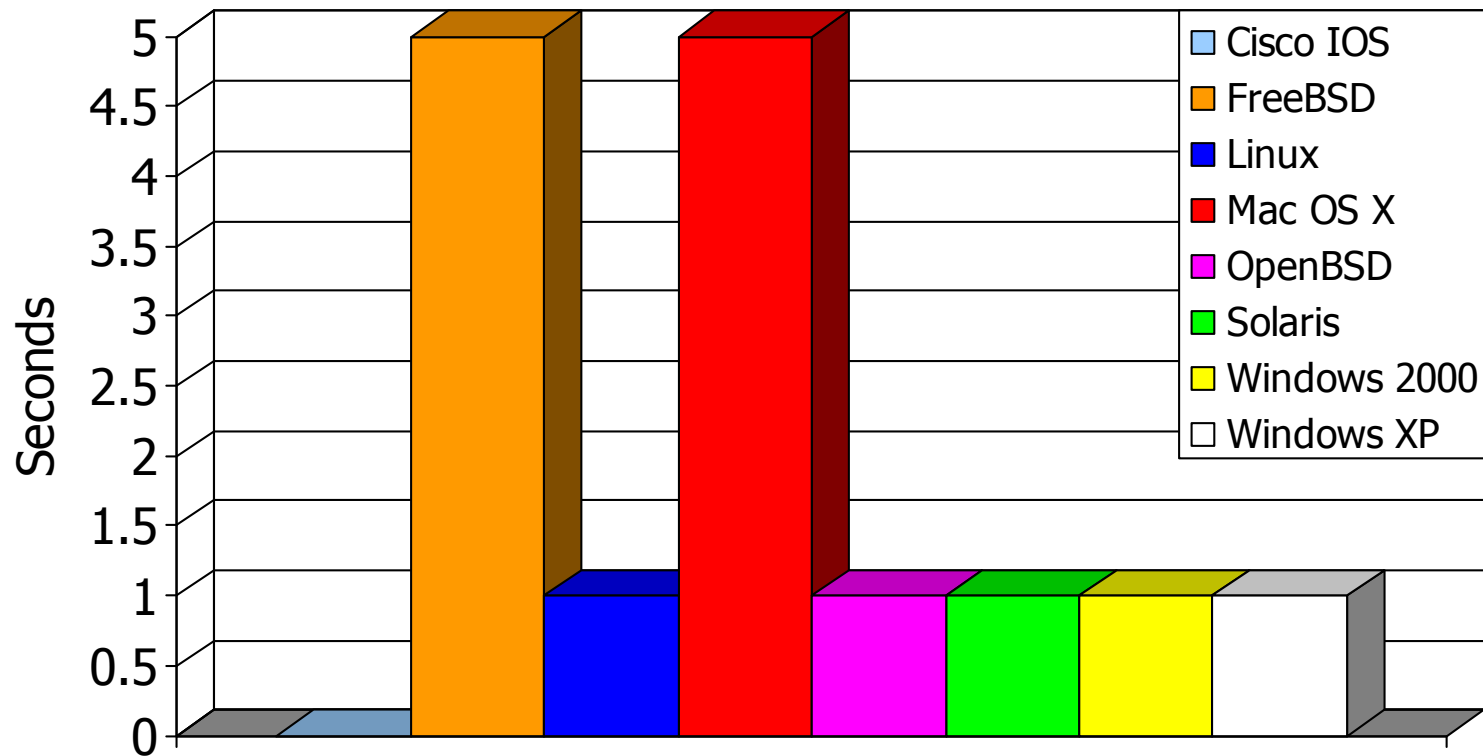
- Cisco IOS 12.1
- FreeBSD 5.1
- Linux 2.4.20
- Mac OS X 10.2.6
- OpenBSD 3.3
- Solaris 8
- Windows 2000 – SP3

Those that do:

- Windows XP

DNS Timeouts Can Be Long

DNS Query Timeout of Several Operating Systems



Compounding the Delay

Start	Query	Type	Server	Result
0s	www.usenix.org.	AAAA	ns1	Timeout
1s	www.usenix.org.	AAAA	ns2	NXDOMAIN
1s	www.usenix.org.a.example.com.	AAAA	ns1	Timeout
2s	www.usenix.org.a.example.com.	AAAA	ns2	NXDOMAIN
2s	www.usenix.org.b.example.com.	AAAA	ns1	Timeout
3s	www.usenix.org.b.example.com.	AAAA	ns2	NXDOMAIN
3s	www.usenix.org.	A	ns1	Timeout
4s	www.usenix.org.	A	ns2	NOERROR

Caching DNS Deployment

- Decided to use anycast for caching DNS
- Select anycast IP addresses
 - 128.2.1.10, 128.2.1.11 (CMU: 128.2/16)
- Assign addresses to clients
 - DHCP, PPP, internal documentation, smoke signals

Caching DNS Deployment

- Configure anycast addresses on servers
- Restrict servers to respond only on anycast addresses
 - Prevent dependencies upon unique addresses
- Ensure queries originate from unique address

BIND 9 Changes

```
options {  
    listen-on { 128.2.1.10; 128.2.1.11; };  
    query-source address 128.2.4.21;  
};
```

Caching DNS Deployment

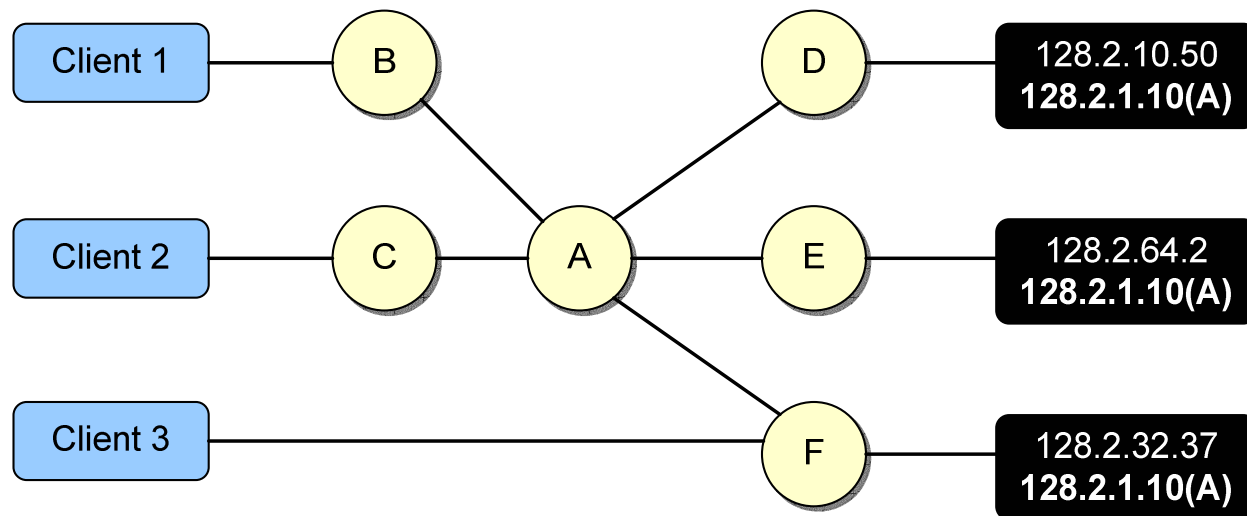
- Configure routing daemon on DNS servers
 - Join our OSPF routing cloud
 - Minimizes outage time when server is down

Typical Routing Table

```
>show ip route 128.2.1.10
Routing entry for 128.2.1.10/32
Routing Descriptor Blocks:
  * 128.2.255.24, from 128.2.4.242, 1d13h ago
    128.2.255.10, from 128.2.4.238, 1d13h ago
    128.2.255.35, from 128.2.4.228, 1d13h ago
```

Caching DNS Deployment

- Some clients directed locally, while others load balanced
- If server fails, reroute in < 10 seconds



Other Potential Uses

- Authoritative DNS (RFC3258)
 - Root servers F, I, K
 - .ORG TLD
- Multicast RP (RFC3446)
- 6to4 Tunneling Routers (RFC3068)
- Syslog, RADIUS, Kerberos
- Single packet request-response UDP protocols are “easy”
- Many services are using anycast; changes network troubleshooting steps

Source Address Verification

- Validate the IP source address of packets entering a router
 - Drop packets with unexpected addresses
- Improve network security
 - Popular DoS vector: spoofing source addresses (Teardrop, Smurf among first)
 - Harder to track back spoofed sources

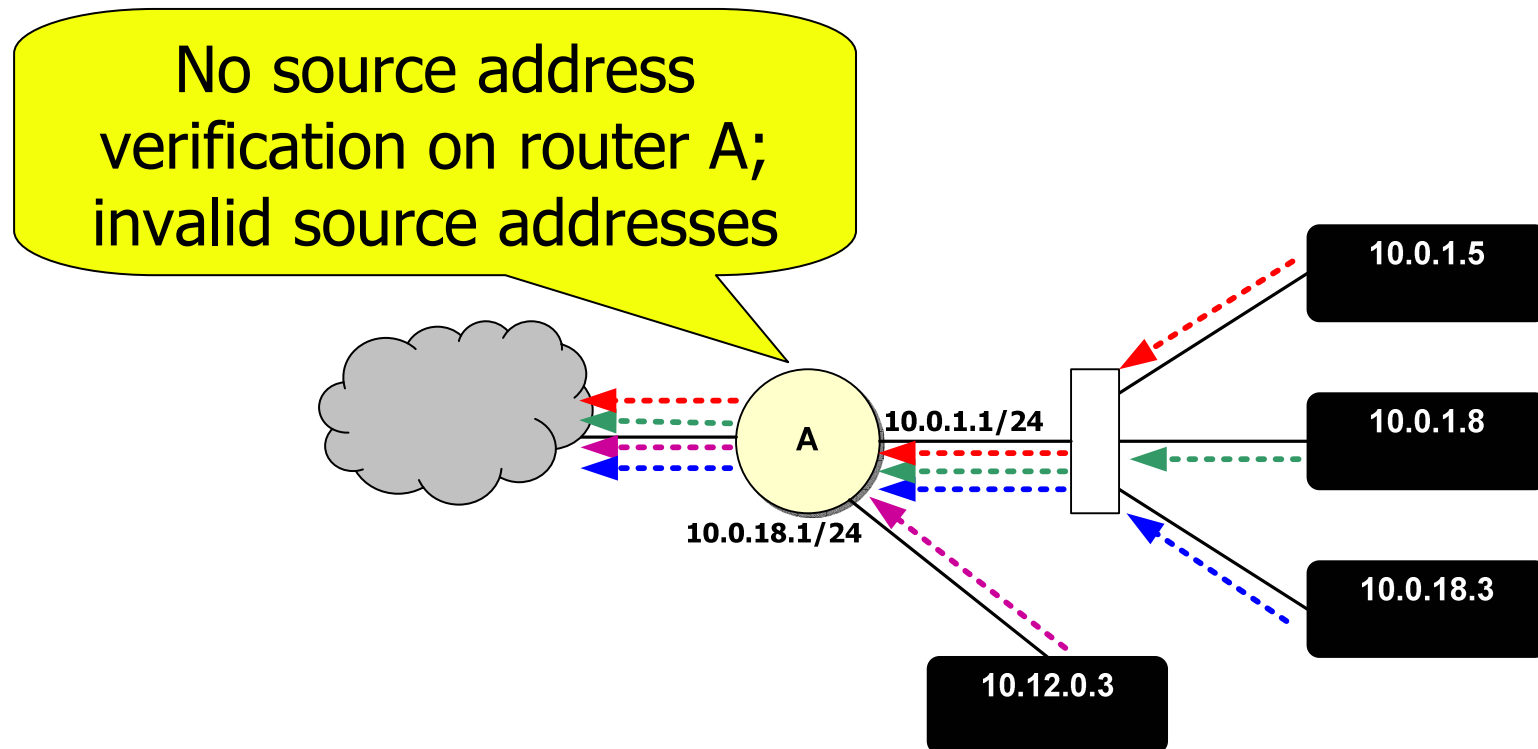
Methods of SAV

- BCP38 recommends network operators deploy ingress filters restricting traffic
 - Acceptable solution, but difficult to implement in the network core
 - Requires operator maintenance and upkeep
 - Stale access lists become a problem
- Research into better ways
 - SAVE Protocol: Additional inter-router communication of allowed ranges

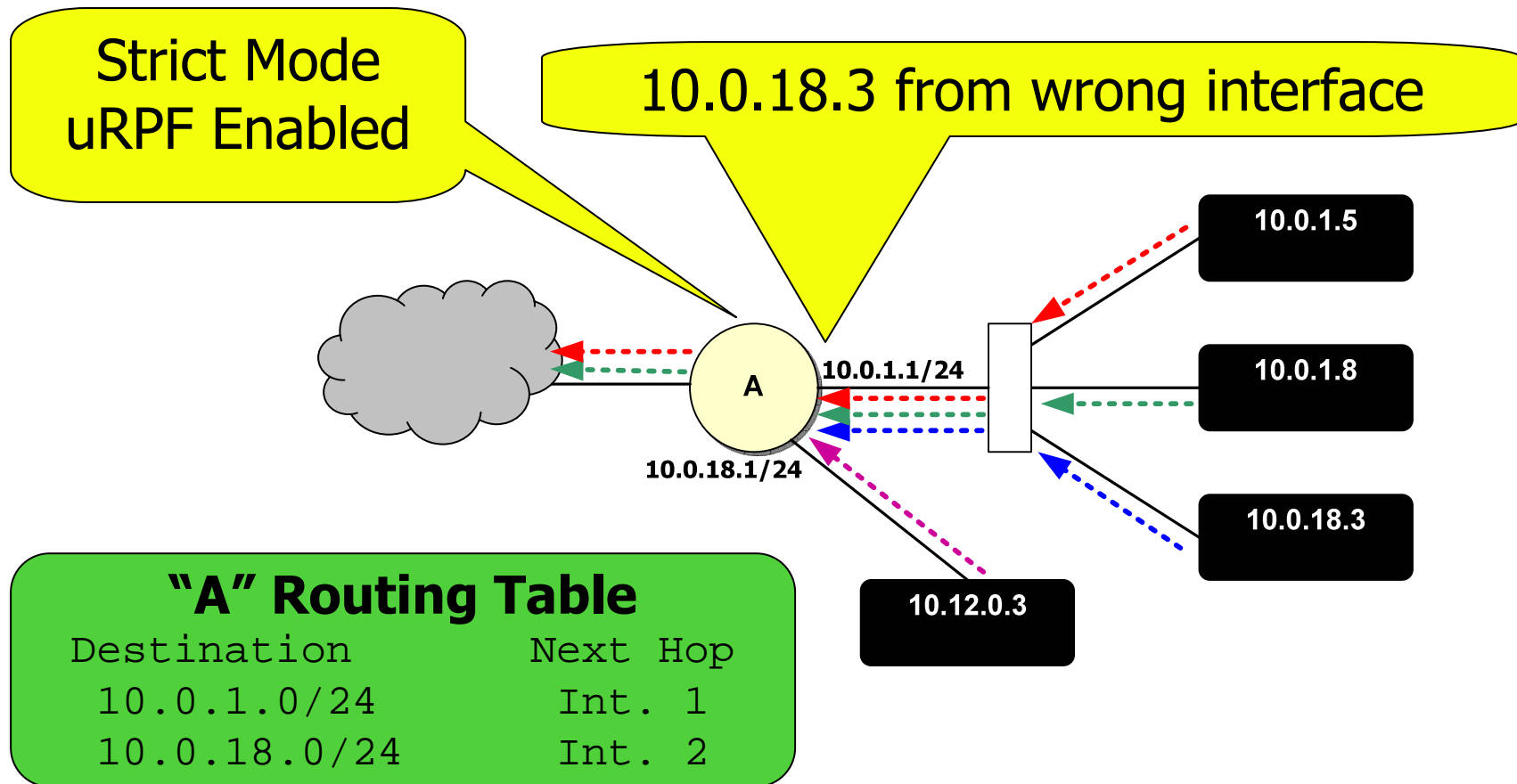
Unicast Reverse Path Forwarding

- Unicast Reverse Path Forwarding
 - Uses unicast forwarding table as policy source; filters adjust dynamically
 - Easy to implement at the edge
 - ‘Loose’ mode acceptable in the core
- Accept packet from interface only if forwarding table entry for source IP address matches ingress interface

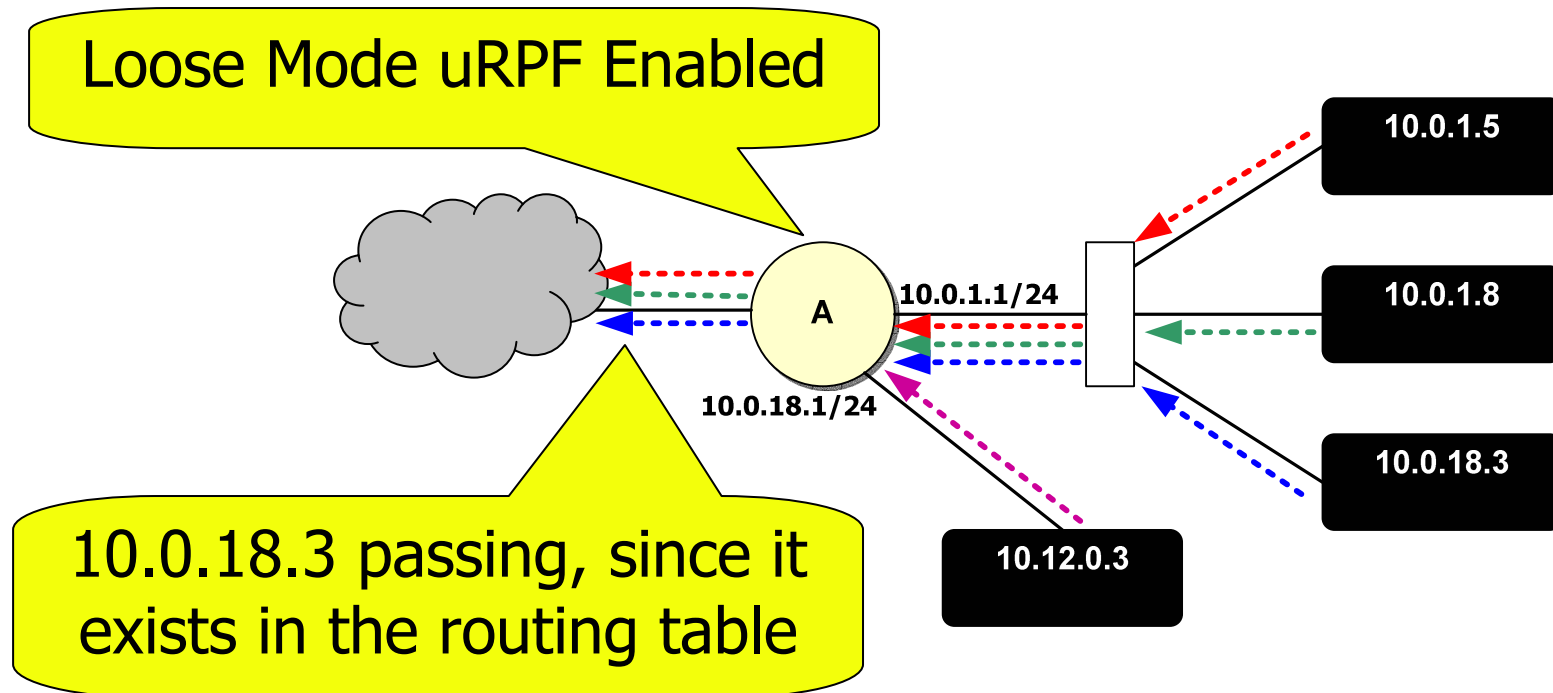
uRPF in Action



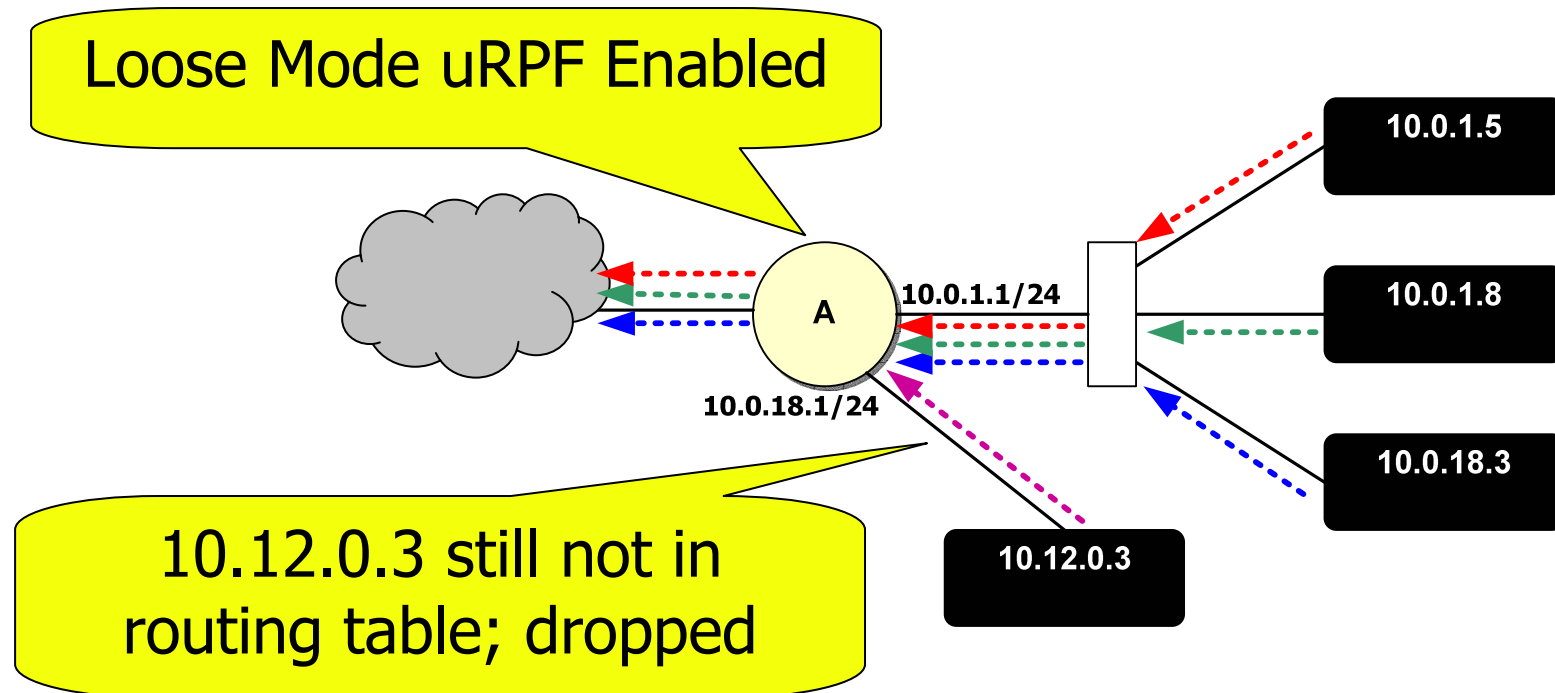
uRPF in Action



uRPF in Action



uRPF in Action



Host Filtering

- Problem:
 - Want to be able to block traffic from certain source addresses quickly
 - Access restrictions (worm-infected hosts)
 - Inbound or outbound traffic flooding
 - Implemented using scripts that talk to routers; hope the router is talking 'correctly'
 - Requires passwords; tedious to maintain
 - Doesn't take too long, but we can do better...

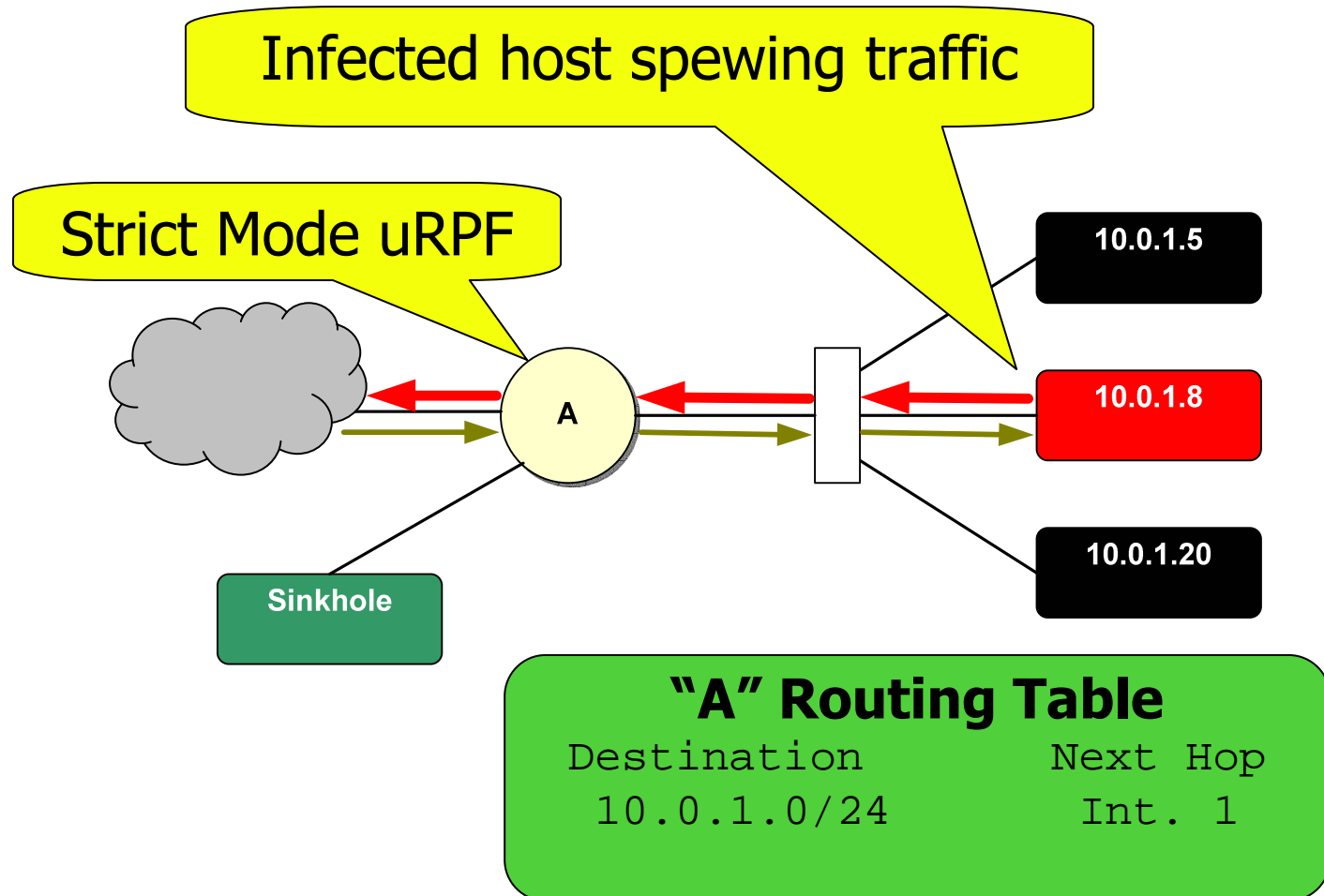
Host Filtering

- Note:
 - uRPF strict mode drops packets with source interface other than next-hop interface of FIB entry for source IP
 - FIB lookups are done using longest prefix matching
 - uRPF strict mode should be in use on every edge interface!

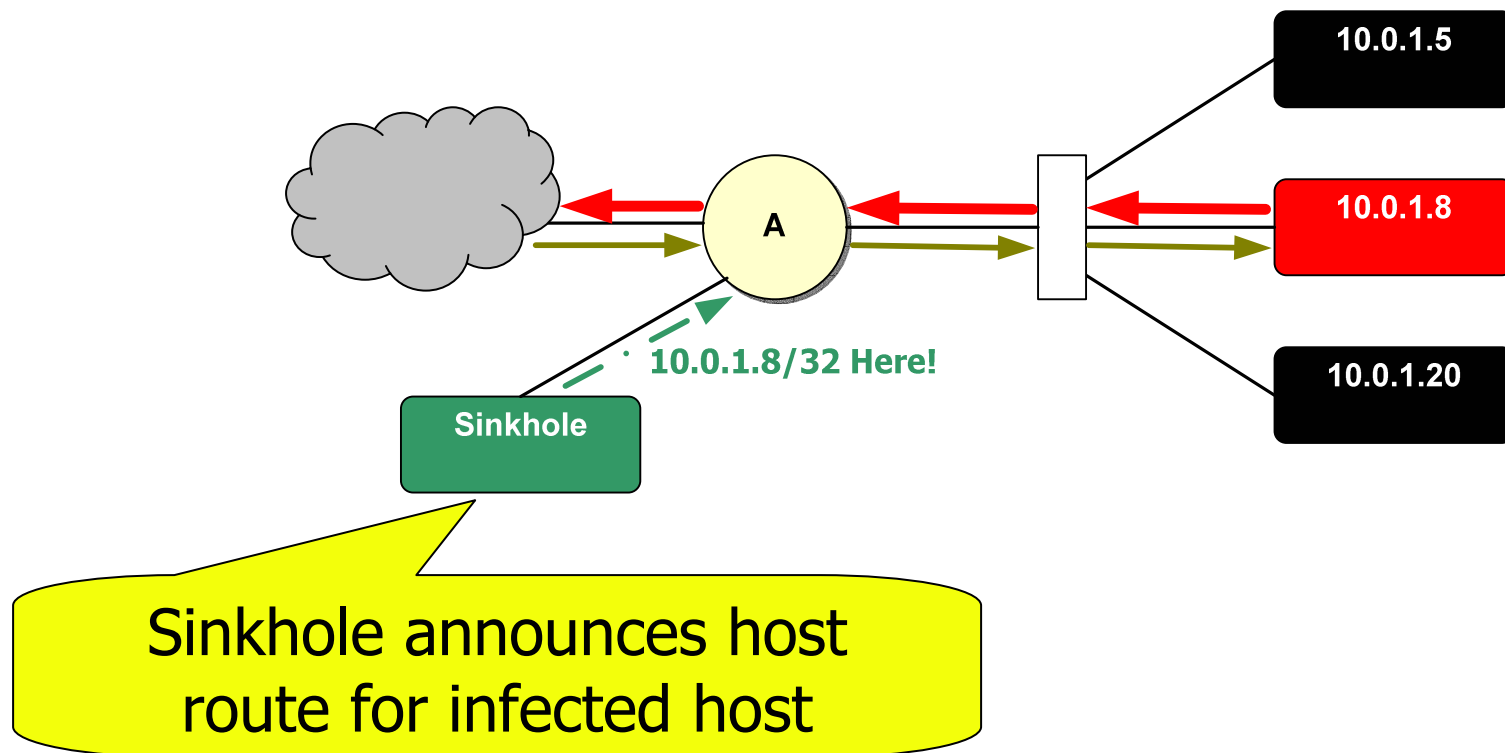
Host Filtering with uRPF

- To filter traffic from an IP, create a FIB entry with /32 prefix for IP ("host route") – with next-hop of anything other than normal ingress interface
- FIB entries can be easily created by propagating host route into IGP

Active Filtering



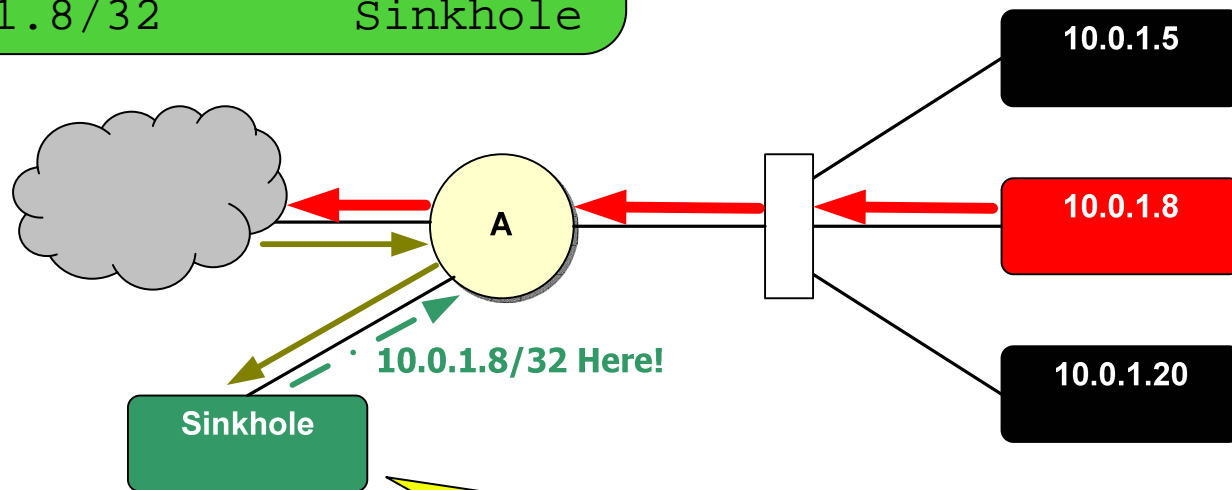
Active Filtering



Active Filtering

"A" Routing Table

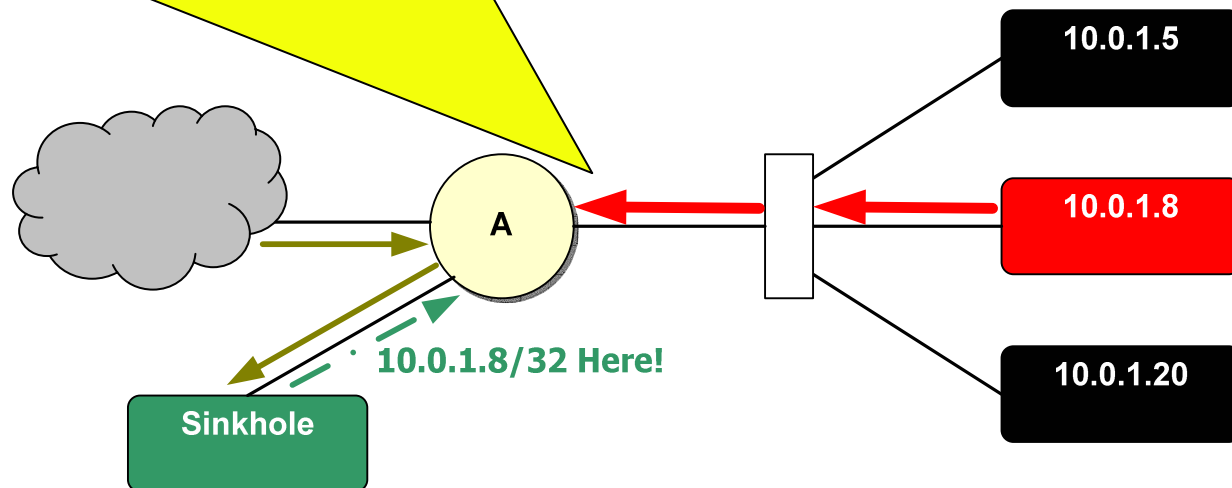
Destination	Next Hop
10.0.1.0/24	Int. 1
10.0.1.8/32	Sinkhole



Traffic to 10.0.1.8 discarded
at sinkhole router

Active Filtering

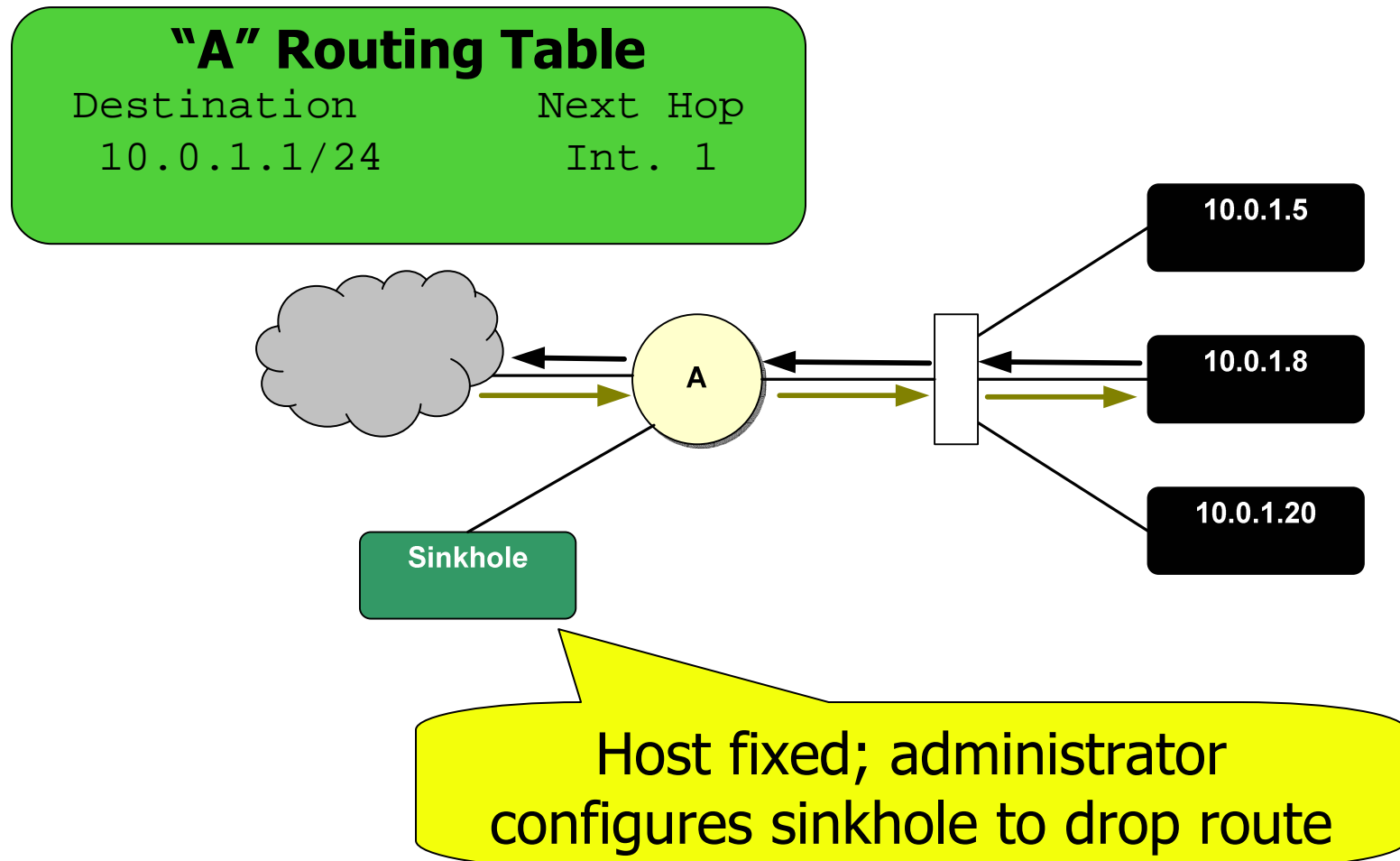
Because of uRPF, traffic from host is discarded
(next hop interface towards sinkhole)



"A" Routing Table

Destination	Next Hop
10.0.1.0/24	Int. 1
10.0.1.8/32	Sinkhole

Active Filtering



Three Practical Ideas

Anycast Caching DNS

Using IP anycast for caching DNS can improve the reliability of recursive DNS service and ease server management tasks.

Source Address Verification

Unicast Reverse Path Forwarding provides an easy, self-maintaining mechanism for source address verification. Enabling uRPF on edge interfaces should become standard operating procedure.

uRPF for Host Filtering

uRPF can be effectively leveraged to quickly apply source address filters. Fast filtering in this manner reduces the response time to network exploits.

Questions?

- Presentation resources:
<http://www.net.cmu.edu/pres/lisa03>
- Kevin Miller: kcm@cmu.edu