

Source Address Validity Enforcement Protocol

Li, Mirkovic, Wang, Reiher and Zhang

S. Venkatesan Department of Computer Science 2008

Source Address Validity Enforcement Protocol

- g Forwarding table
 - For each destination, has the next hop (and cost, ...)
- g For each source address
 - Have a table that tells which interface it must come on (how?)
- g Result: Reduce IP address spoofing.
 - Cannot send packet with an IP address unless IP address is valid for LAN/region sending it.

S. Venkatesan Department of Computer Science 2008

Problems

- g Asymmetric routes
- g Independent of routing protocol
 - Solution is easy if using link state routing protocol
- g Respond to topology changes
- g Incremental deployment
- g Low overhead

S. Venkatesan Department of Computer Science 2008

Assumptions

- g Each router has a set of “source addresses” (or source address space)
- g Source address A for router R:
 - Any IP packet from host with address A must reach R and then to external hosts
 - Example: Hosts in a LAN, Gateway router for an organization, ...

S. Venkatesan Department of Computer Science 2008

SAVE Router's Job

- g For each entry in forwarding table, generate SAVE update (periodically) and send to destination address space
- g Each SAVE router receiving this update
 - sees SAVE update
 - sets up incoming table entries (giving valid incoming interfaces)

S. Venkatesan Department of Computer Science 2008

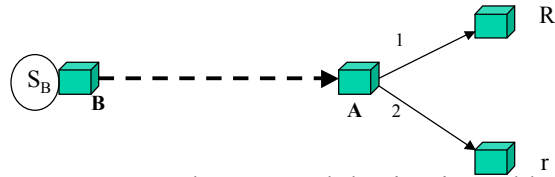
Three Complications

- g SAVE update must follow proper paths
- g Routing Changes
- g Overhead
 - Intermediate router R must piggyback its own update when sending someone else's update
 - Only if R had not sent its own update

S. Venkatesan Department of Computer Science 2008

Complication 1

g SAVE update must follow proper paths



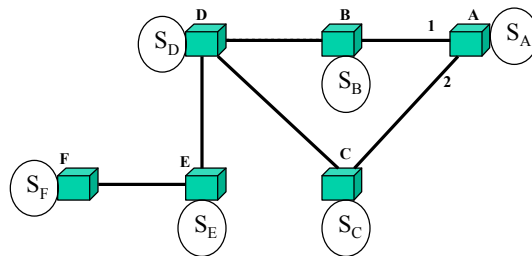
SAVE update toward destination address space

A must send SAVE update to R and r

S. Venkatesan Department of Computer Science 2008

Complication 2

g Routing Changes



Source Space	Valid interface
S_B	1
S_C	2
S_D	1
S_E	1
S_F	1

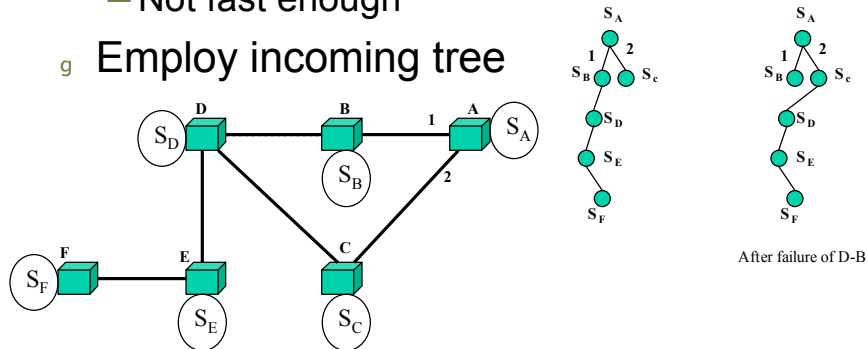
Source Space	Valid interface
S_B	1
S_C	2
S_D	2
S_E	1
S_F	1

S. Venkatesan Department of Computer Science 2008

Routing Change

- g Periodically send SAVE update
 - Not fast enough

- g Employ incoming tree



S. Venkatesan Department of Computer Science 2008

Date Structures

1. Incoming table
 - Each router has valid incoming interface for source address space
2. Incoming Tree
 - Used to derive incoming table
 - If SAVE update crosses A, then router B and reaches R, then: S_A will be child of S_B for incoming tree at R
 - A subtree of R's root node is associated with one incoming interface.
3. SAVE update
 - Three fields: Destination Address Space, Address Space Vector (ASV) (tree) and appendable flag

S. Venkatesan Department of Computer Science 2008

Generation of SAVE updates

- g Router R has source address space S_R
- g Destination address space D
 - $D=\{ip_1, ip_2, \dots, ip_n\}$ that share the same output interface
- g SAVE update:
 - $\{Dest\ Address\ Space=D, ASV=<S_R>, appendable=true\}$
- g Encapsulate and send to one of the IP addresses in D (randomly chosen)

S. Venkatesan Department of Computer Science 2008

Updating Incoming Tree at R

- g R received a SAVE update $<ASV, D, true/false>$
- g $ASV=<S_1, S_2, S_3, \dots, S_n>$ $\{S_i$ is ASV of router $R_i\}$
 - Router R_1 's update (with source address space S_1) was sent to R_2 ;
 R_2 's update was sent to R_3 , etc.
 - What if R_i and R_{i+1} are not adjacent?
- g If S_n is not in R's tree yet, graft entire subtree rooted at S_n under root of R (label the edge with incoming interface)
- g Else if S_n 's existing interface is not same as the one this SAVE update came on, subtree rooted at S_n is remapped to this interface
- g Any other subtree S_i ($i < n$) is now remapped
 - If S_i existed in R's tree before, change tree's position & interface if needed

S. Venkatesan Department of Computer Science 2008

Update Flag

- g R has just initiated an UPDATE towards destination address space D
- g R received a new update towards D
- g R updates S_R but sets appendable to false
 - All downstream routers will stop piggybacking their information to the UPDATE
 - They just did this
 - Propagate only changed part of subtree

S. Venkatesan Department of Computer Science 2008

Forwarding SAVE updates

- g R received an update for destination address space D
- g Forwarding data for D if there are multiple entries in forwarding table for addresses in D?
 - Some of D have one entry; others have another, etc.
 - Create a SAVE update for each subset
- g When to stop forwarding SAVE updates?

S. Venkatesan Department of Computer Science 2008

Optimized Incoming Table

- g Route is symmetric?
 - For an address space A, if the valid incoming interface is same as outgoing interface for A, have a bit in the forwarding table
 - 1=symmetric
 - Incoming=outgoing interface
 - 0=asymmetric;
 - Use incoming table

S. Venkatesan Department of Computer Science 2008

Simulation Experiments

- g See paper

S. Venkatesan Department of Computer Science 2008