

Programming routers to improve network security

**R. Canonico, D. Cotroneo, L. Peluso, S.P. Romano,
G. Ventre
Maurizio D'Arienzo**

*Università di Napoli Federico II
Dipartimento di Informatica e Sistemistica
Napoli - Italy*

Problem statement

- A serious threat for the Internet:
Distributed Denial of Service attacks
- **DDoS goal:** jeopardize the availability of a service by wasting network and system resources through the cooperation of a number of hosts spread on the Internet
- Defence techniques require the identification and isolation of attack sources
- IP address spoofing makes the identification problem hard to solve
- *This is intrinsically an inter-domain problem !*

Marking-based traceback techniques

Source identification through packet marking

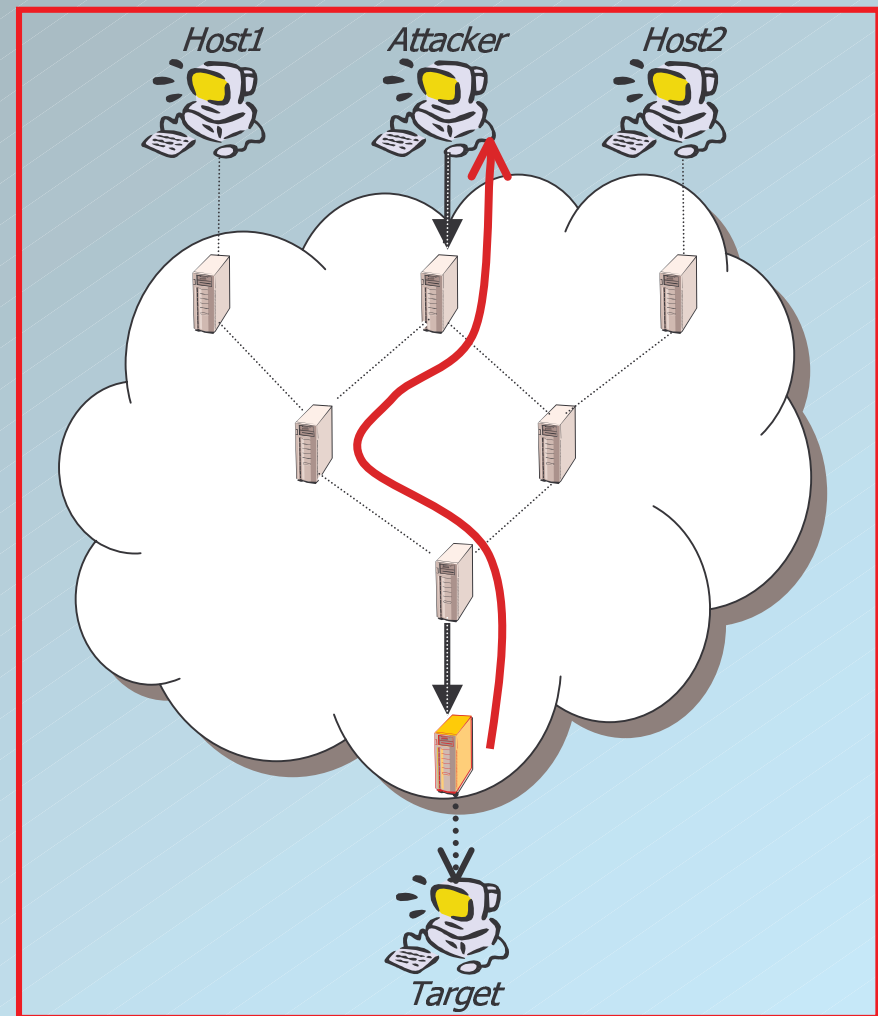
n **Node Append**

- n Fast to converge (1 packet)
- n Reliable source identification
- n Not efficient
- n Requires modification of the IP header at each node

n **Node Sampling**

(e.g. Savage et al. @SIGCOMM 2000)

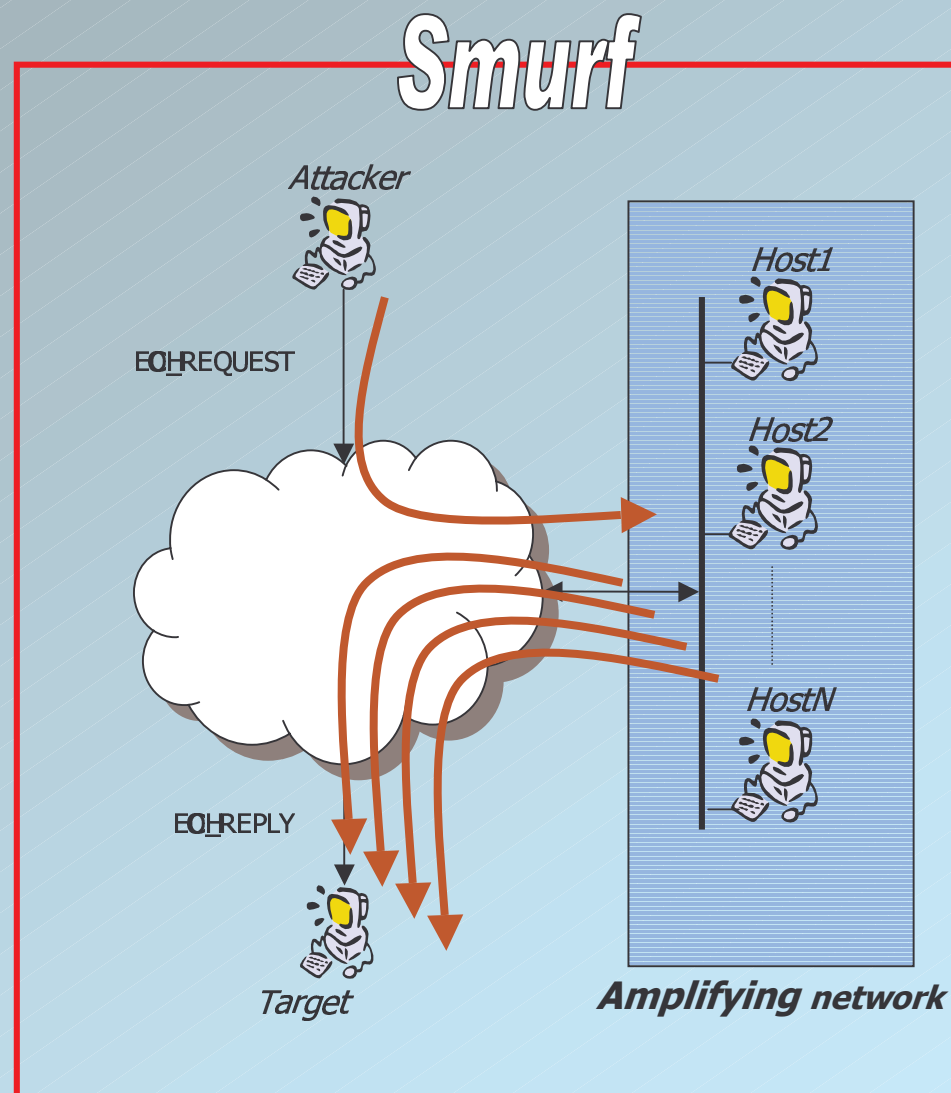
- n Each router puts its address in the packet header with a probability $p < 1$
- n More efficient
- n Slower to converge
- n Source not deterministically identified
- n IP address encoded in packet header (e.g. in the identification field)



A typical DDoS attack: Smurf

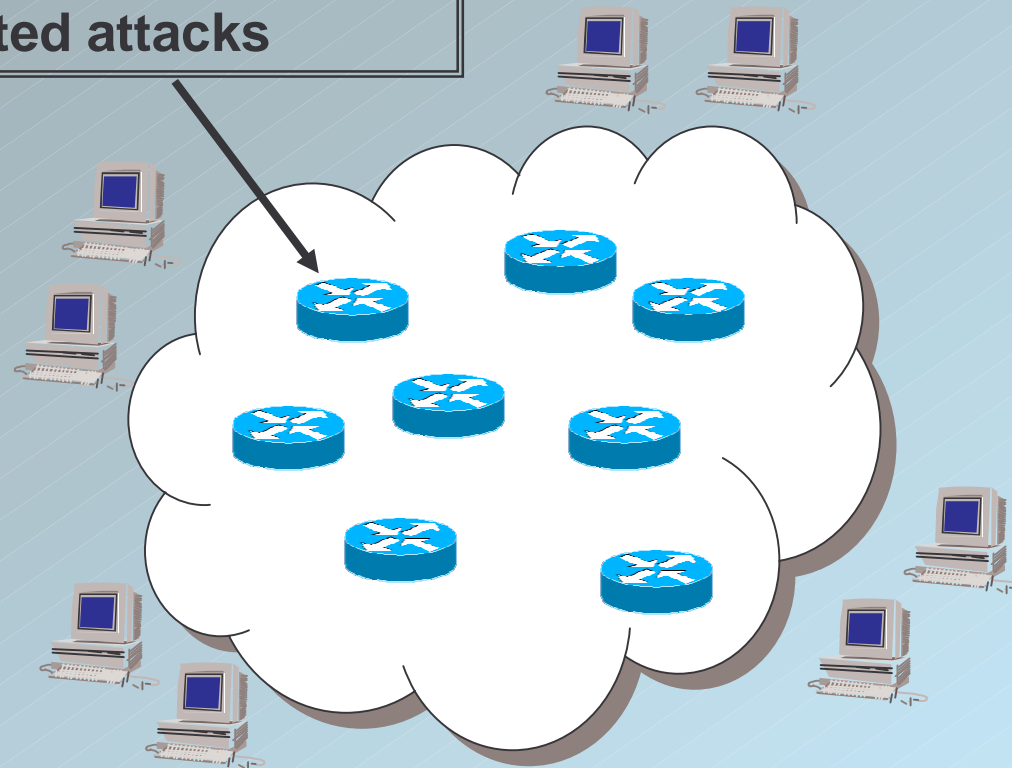
- The attacker sends a number of ICMP **echo_request** messages to the broadcast address of the network, *by using as source addr. the IP address of the target host*
- The hosts of the amplifying network reply by sending an ICMP **echo_reply** message to the target
- The effectiveness of the attack (*gain*) is proportional to the number of hosts located in the amplifying network

Traceback techniques may not be effective for this kind of attack !



A network based strategy

**Network elements must cooperate
to protect the network
from distributed attacks**



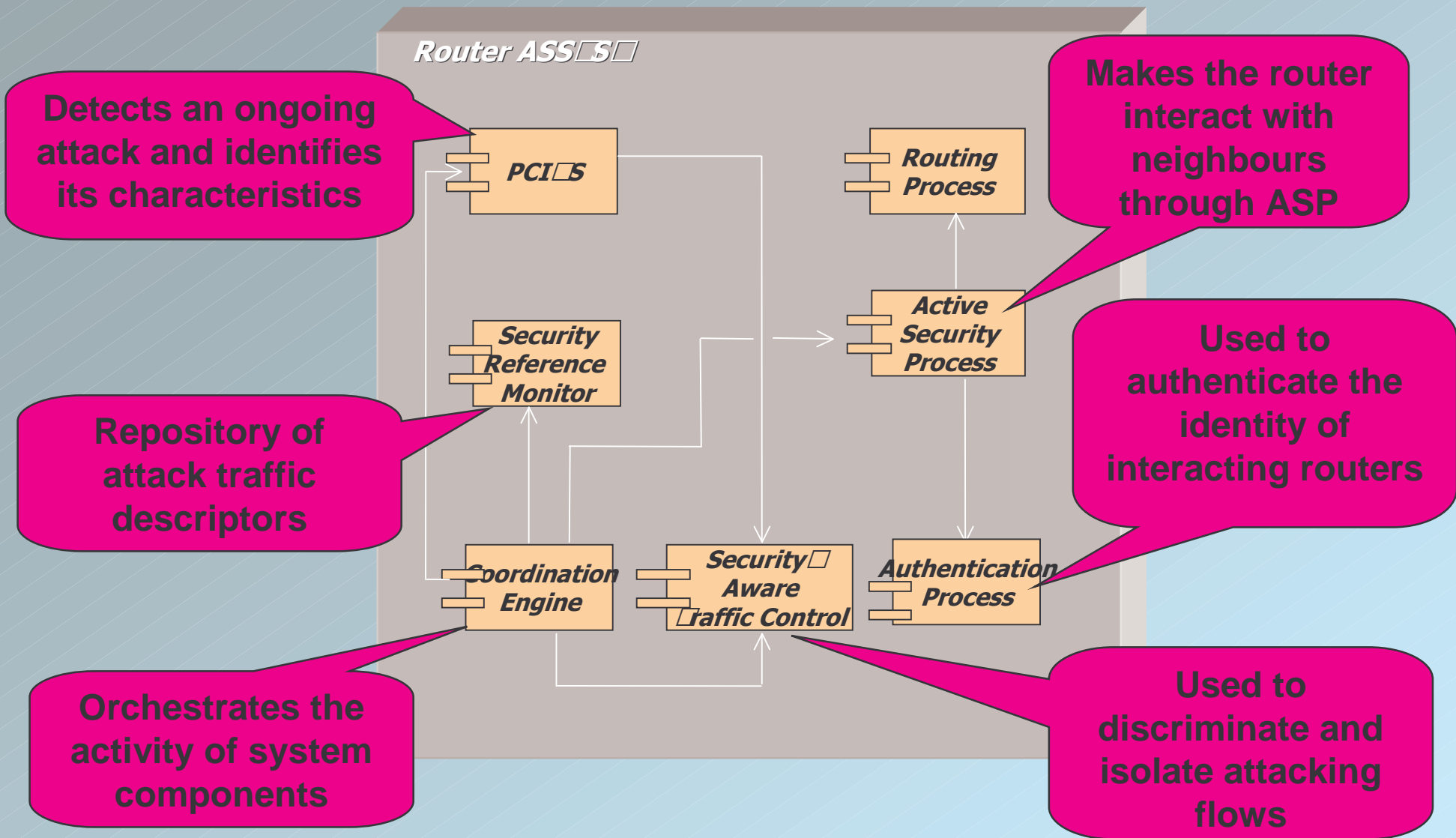
The ASSYST approach

1 Involve network routers in a pro-active defence strategy against *Distributed Denial of Service* attacks

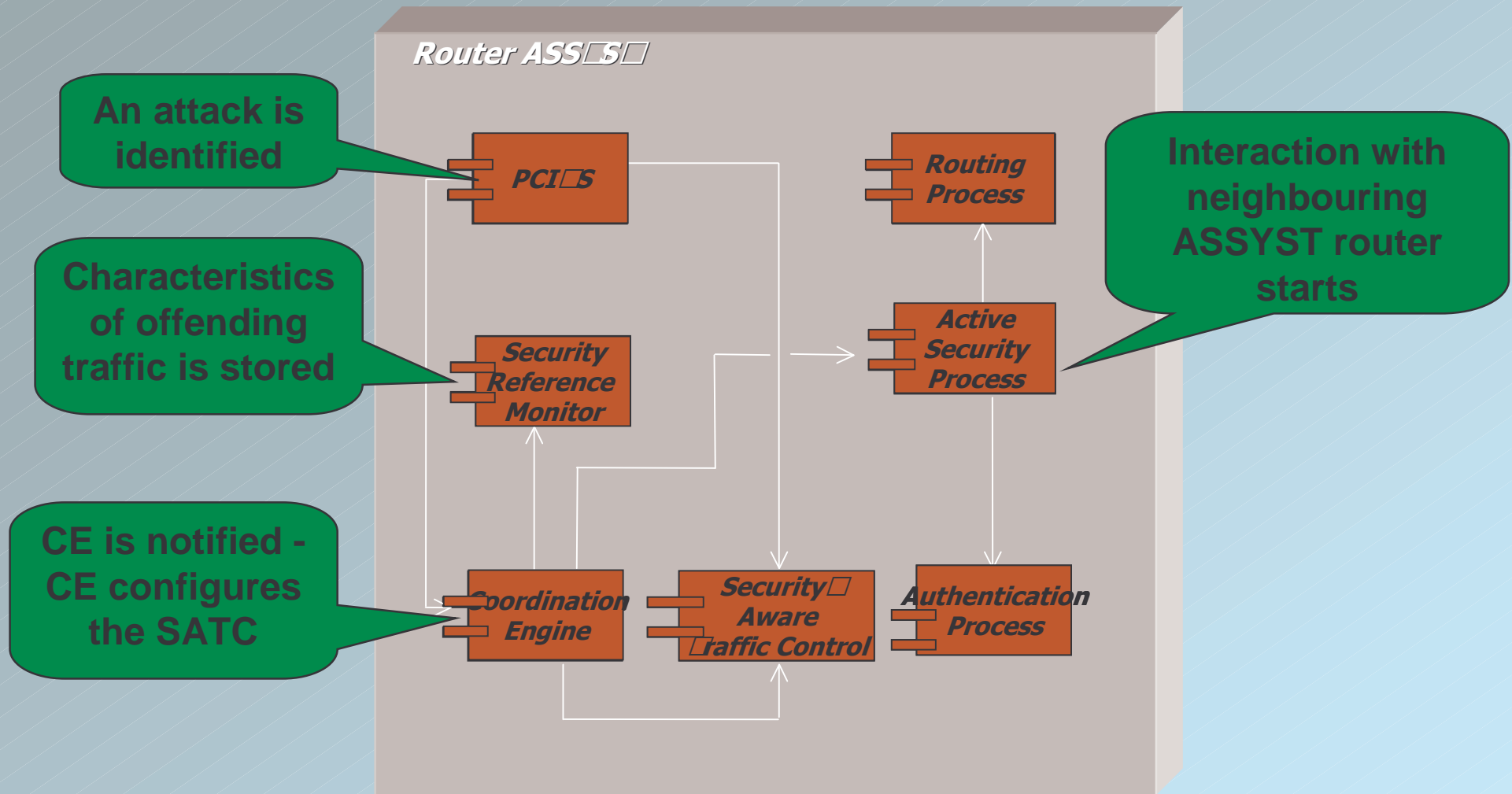
1 ***Characteristics***

- » Detection of attacks within the network
- » Reliable identification of source attacks
- » Limitation of the damage produced by an attack
- » A flexible approach against different kinds of attack

The ASSYST router architecture

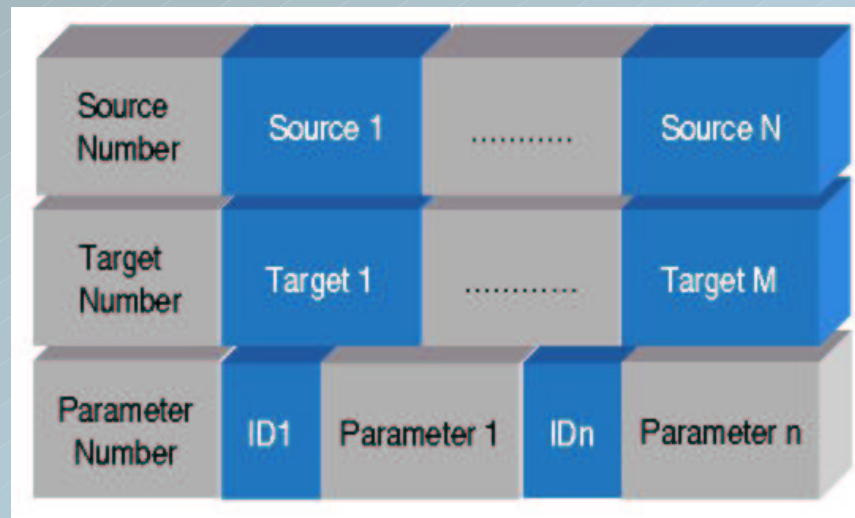


The ASSYST security model



The Active Security Protocol

- ASSYST routers interact through the Active Security Protocol (ASP)
- Once an attack has been detected, its characteristics is described in a Traffic Descriptor object
- ASP uses an extensible format derived from the *Intrusion Detection Message Exchange Format* (IDMEF) defined by the IETF

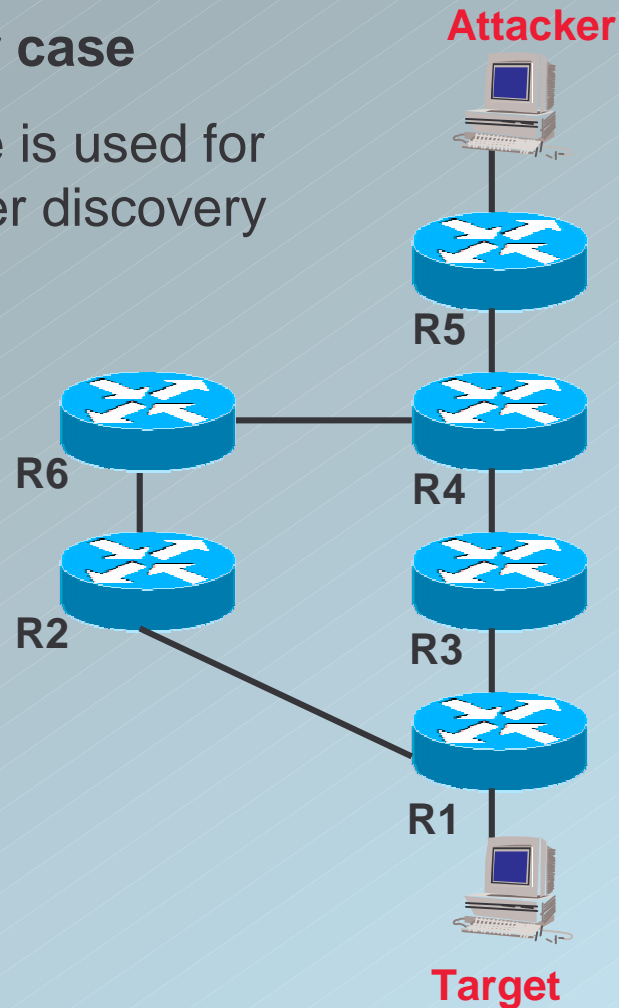


Typical parameters: Throughput, Average TTL, Seq. No., Pending Connections, Packets received – Receive interval

The Active Security Protocol behaviour (1)

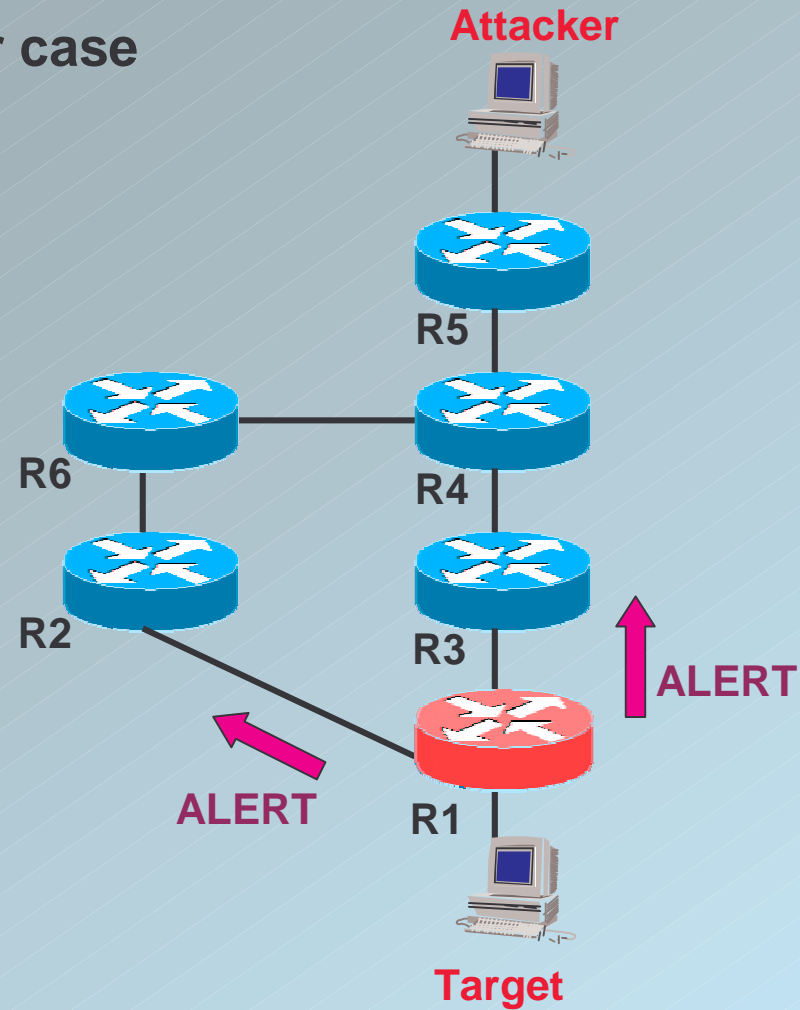
The single attacker case

- A **PROBE** message is used for ASP-enabled router discovery



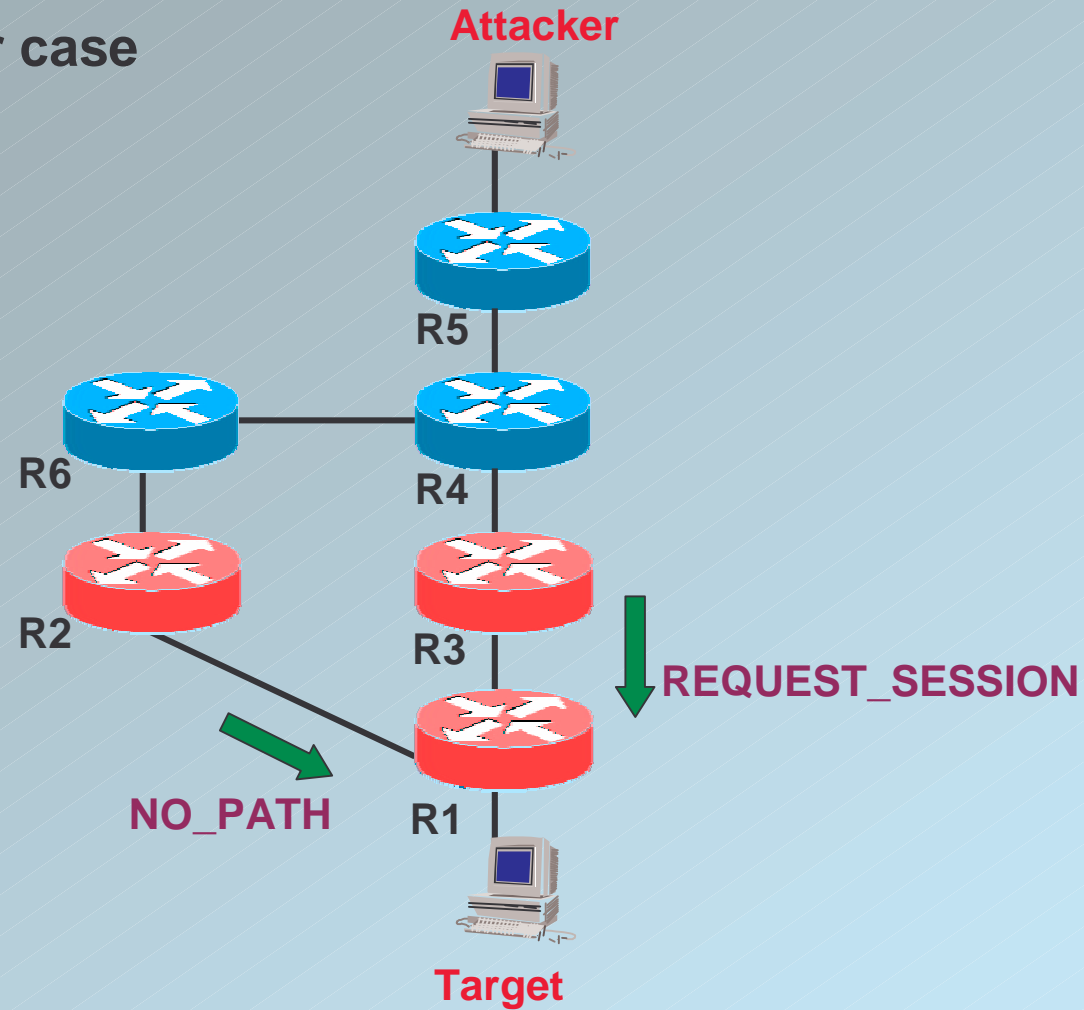
The Active Security Protocol behaviour (2)

The single attacker case



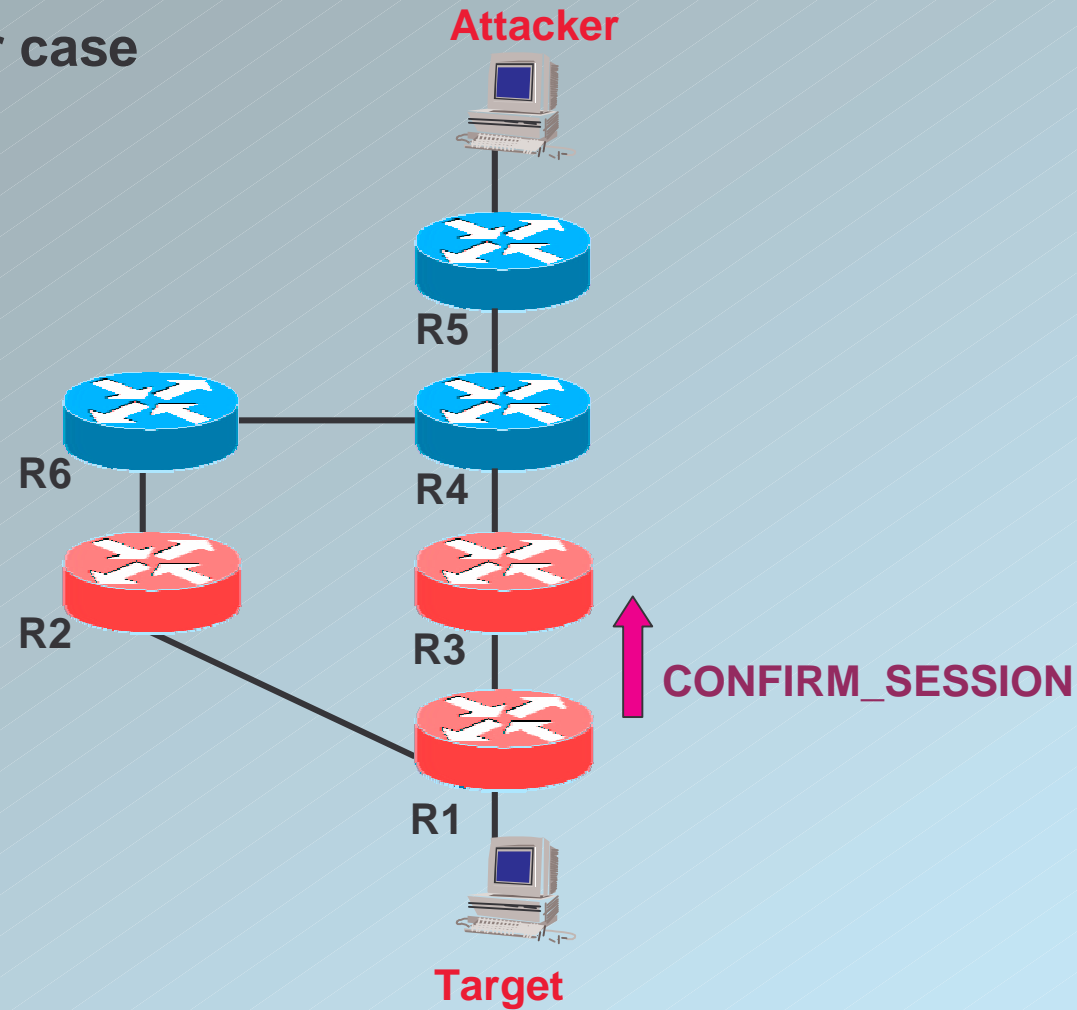
The Active Security Protocol behaviour (3)

The single attacker case



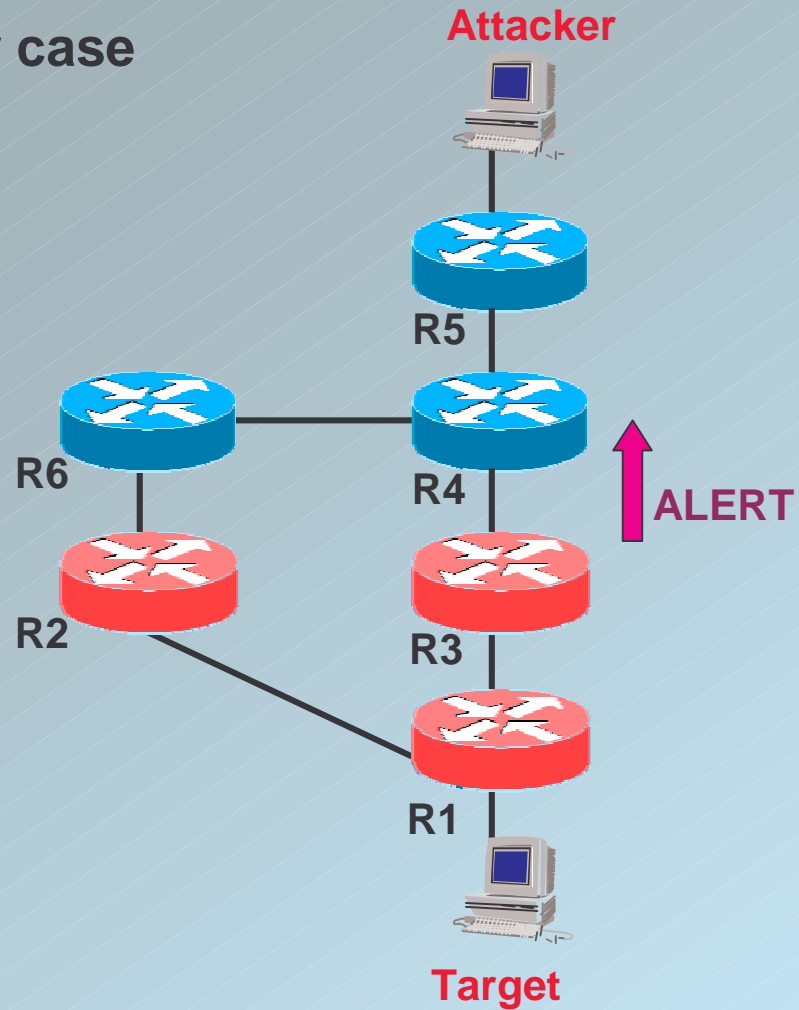
The Active Security Protocol behaviour (4)

The single attacker case



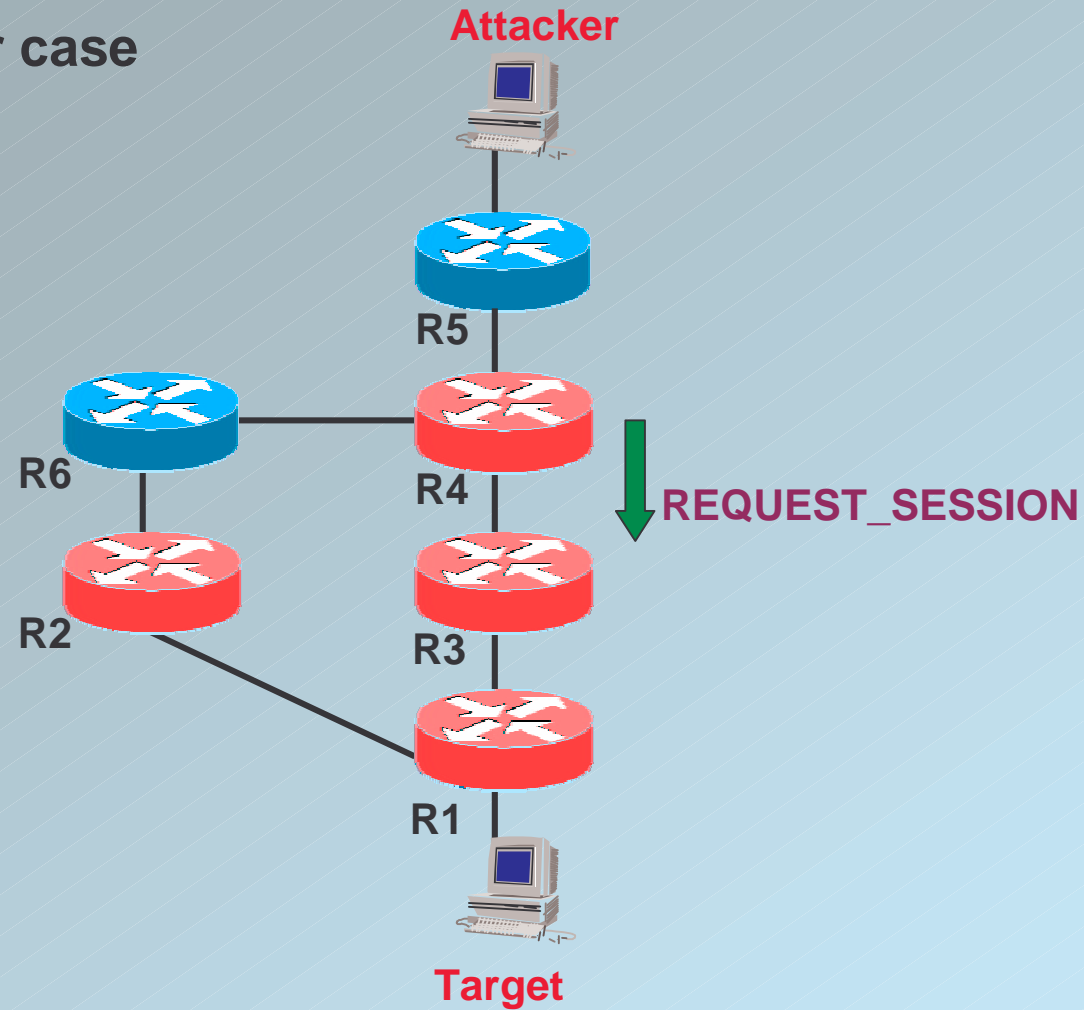
The Active Security Protocol behaviour (5)

The single attacker case



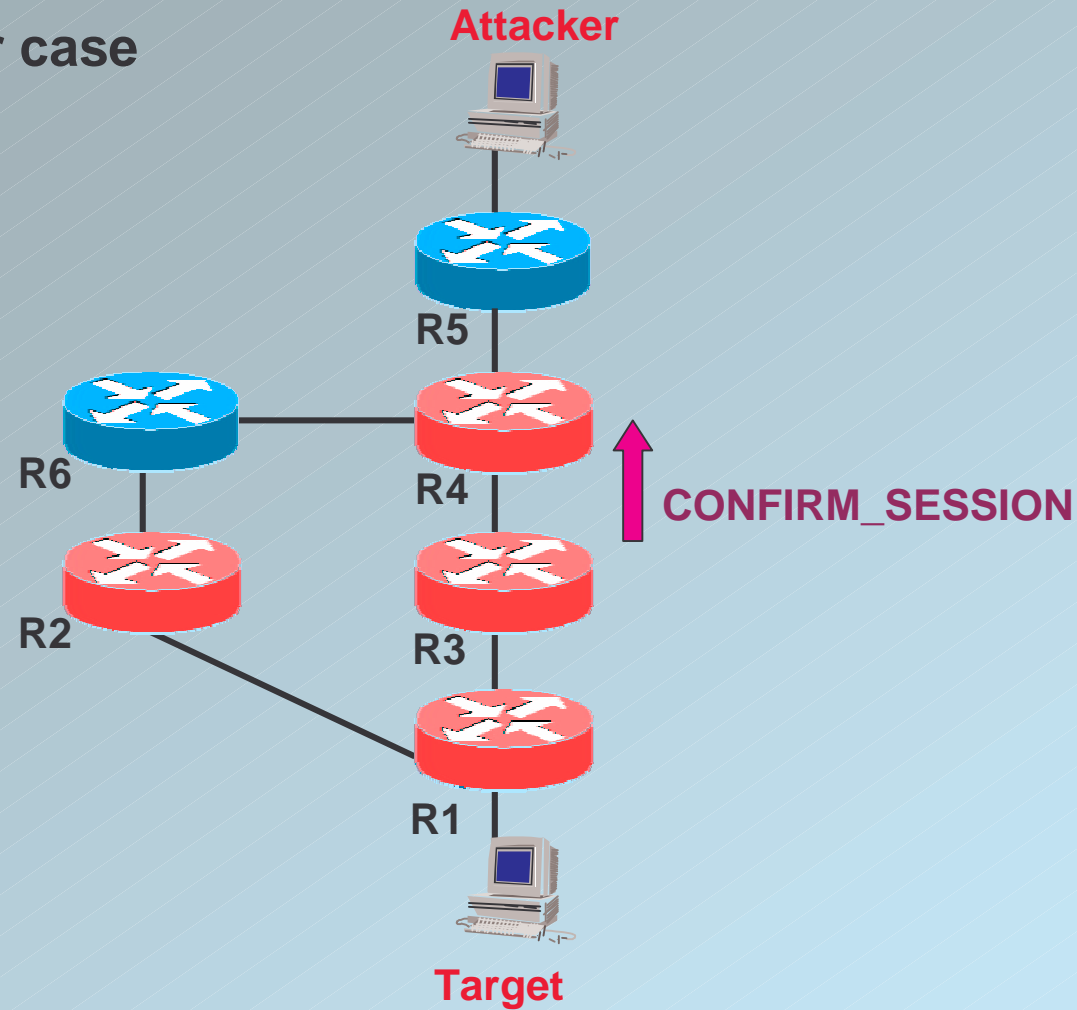
The Active Security Protocol behaviour (6)

The single attacker case



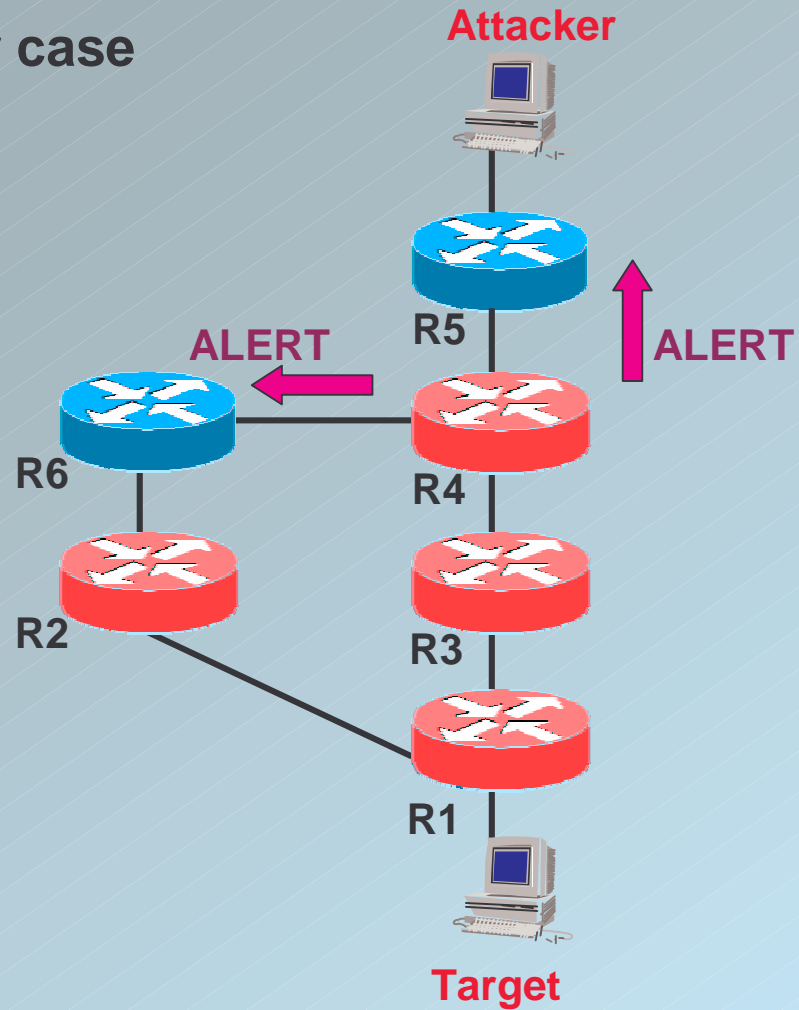
The Active Security Protocol behaviour (7)

The single attacker case



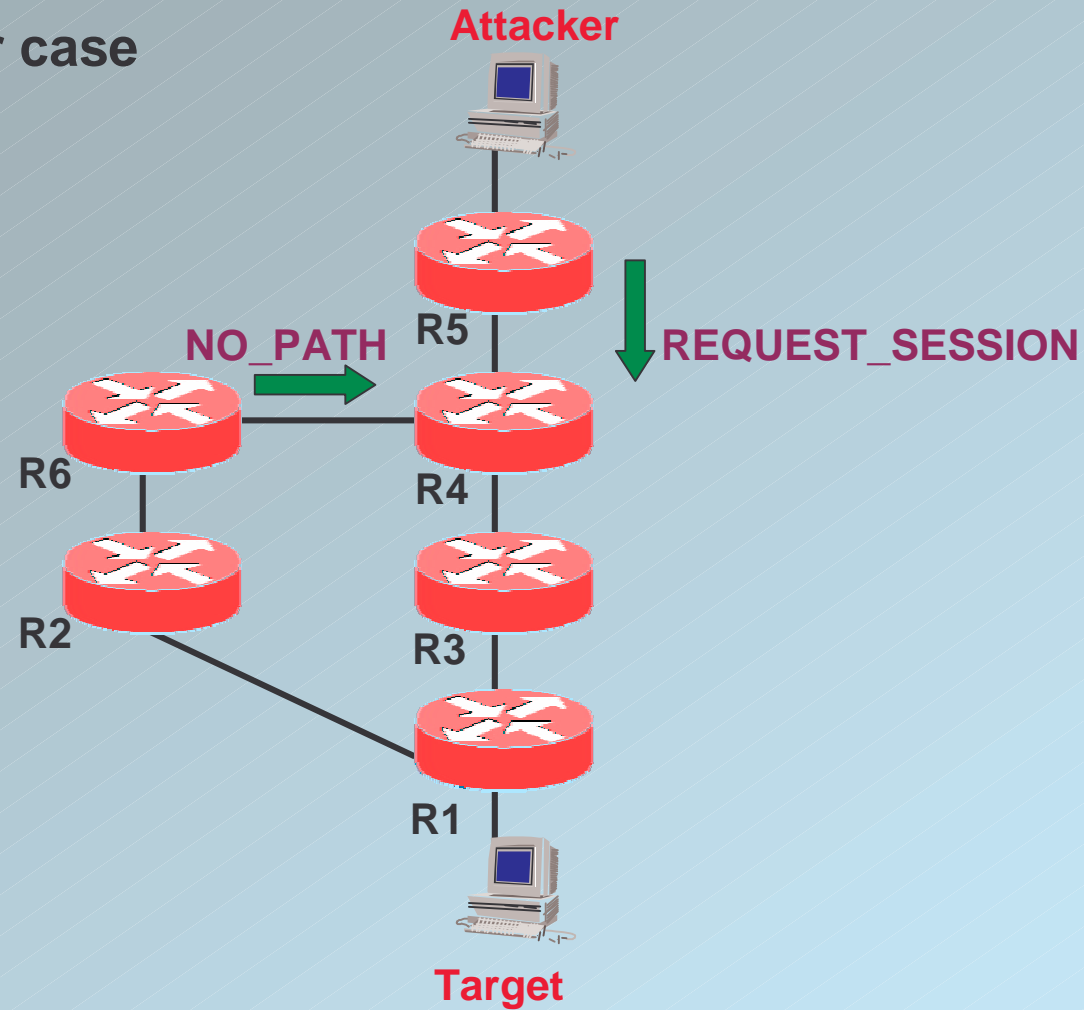
The Active Security Protocol behaviour (8)

The single attacker case



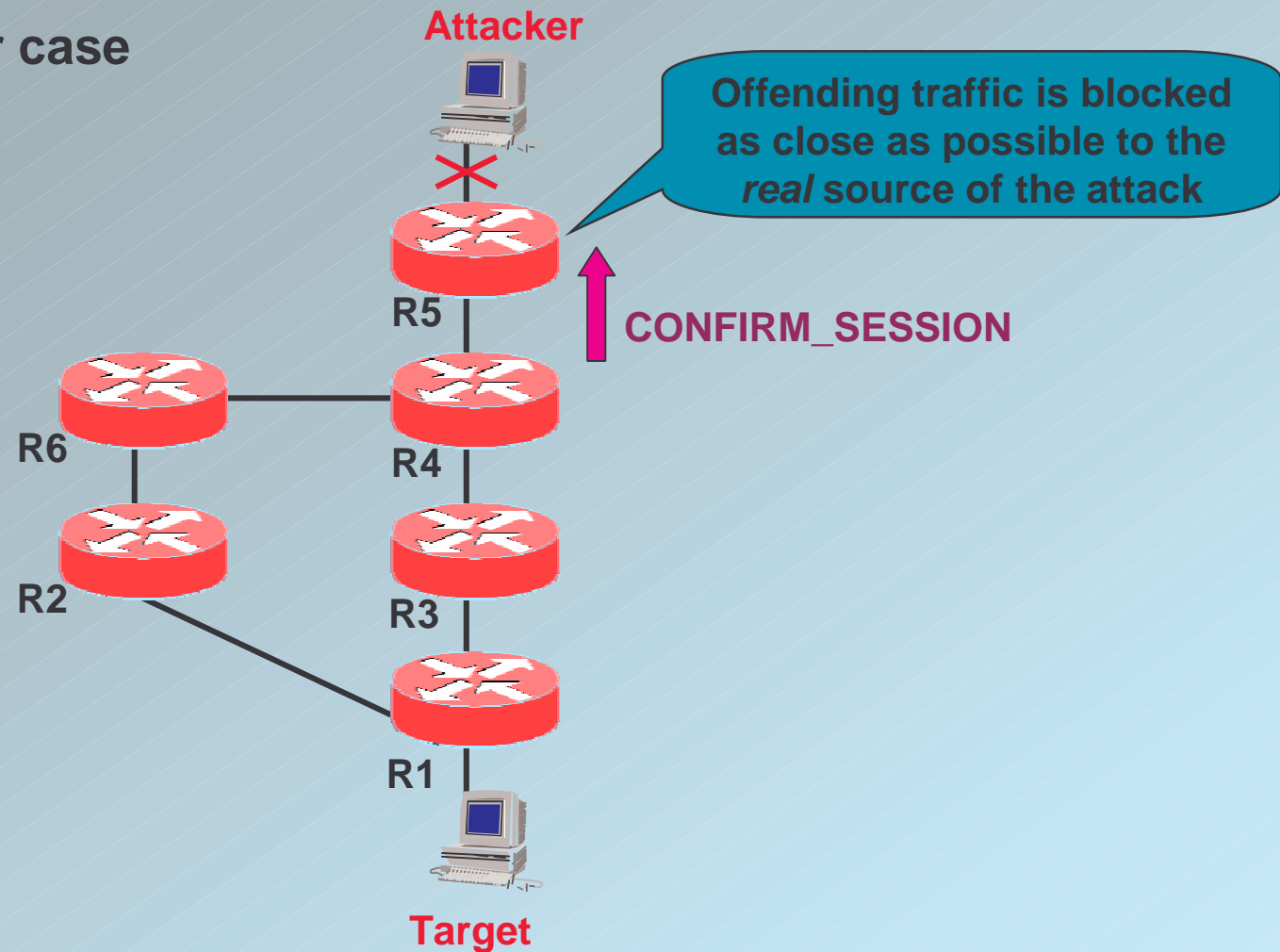
The Active Security Protocol behaviour (9)

The single attacker case



The Active Security Protocol behaviour (10)

The single attacker case



ASP Session states

- 1 Once it has been created in a node, an ASP session can be in one of the following three states:
 - » **Active:** the node is on the path of the attack – the node must send an ALERT message to all the neighbouring ASSYST routers
 - » **Waiting:** the node has been notified of this attack by a neighbouring router but it is not on the path of the attack – the node will remain in this state for a while in order to react to a variation in the path of the attack
 - » **Entrusted:** the node is on the path of the attack but it has received a CONFIRM_SESSION message by a neighbour which is now in charge of monitoring and isolating the offending traffic

On the way of implementing the ASSYST model

- To implement ASSYST a programmable router platform is needed
- Linux seems the ideal platform
- Most of the ASSYST modules can be implemented at user level
- Code uploaded from an entrusted code server on demand
- We are currently investigating the possibility of implementing **ASP** (*Active Security Protocol*)
on ASP (*Active Signalling Protocol* – Steve Berson *et al.* @ ISI.EDU)

Conclusions

- DDOS attacks are a real challenge for the future of the Internet
- Several kinds of attacks are possible
- End-system solutions, tailored for a specific kind of attack, don't solve the problem
- The network must be able to protect itself
- The ASSYST approach detects and isolates attack sources by making the routers cooperate
- The burden of reacting to attacks is moved to the edge
- This approach does not need to be deployed ubiquitously
 - E.g. only at the edge of VPNs