Distributed Systems

Virtual Private Networks

Paul Krzyzanowski
pxk@cs.rutgers.edu

Private networks

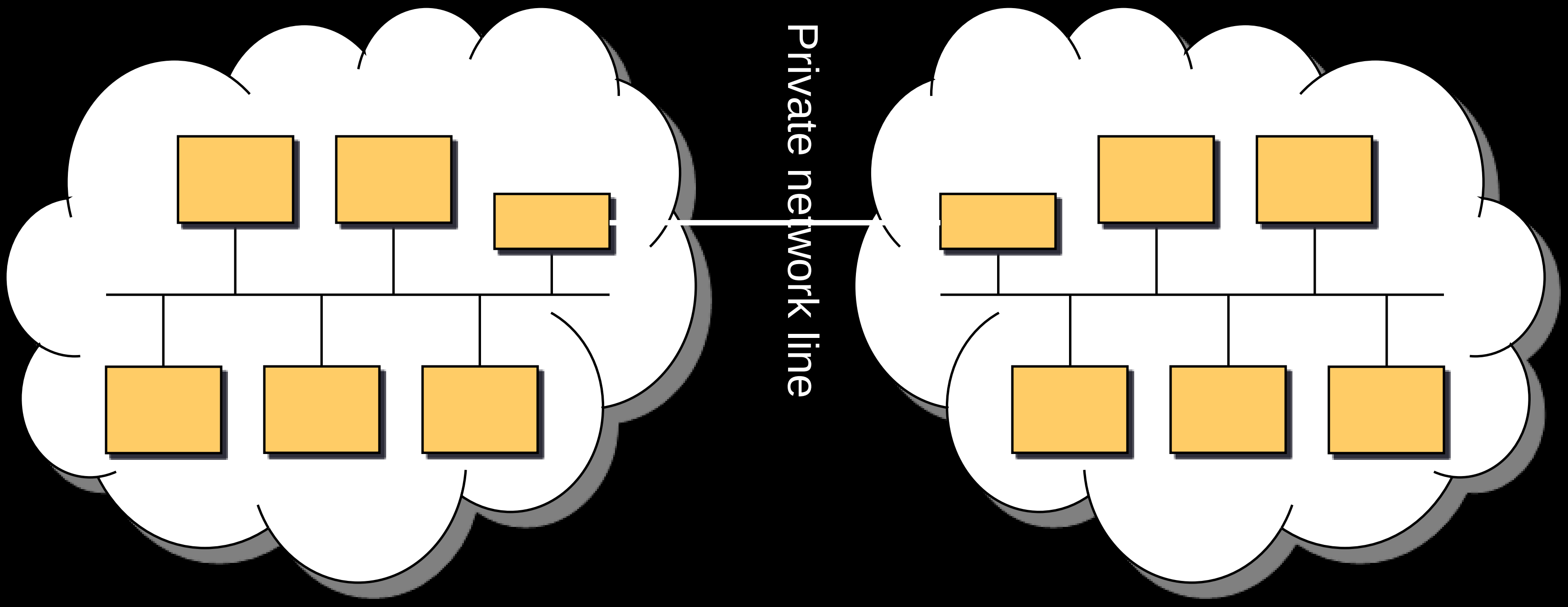
Problem

- You have several geographically separated local area networks that you would like to have connected securely

Solution

- Set up a private network line between the locations
- Routers on either side will be enabled to route packets over this private line

Private networks



LAN A (New York)

LAN B (London)

- Problem: $$$¥¥¥£££€€€ !

Virtual private networks (VPNs)

Alternative to private networks

- Use the public network (internet)

Service appears to users as if they were connected directly over a private network

- Public infrastructure is used in the connection

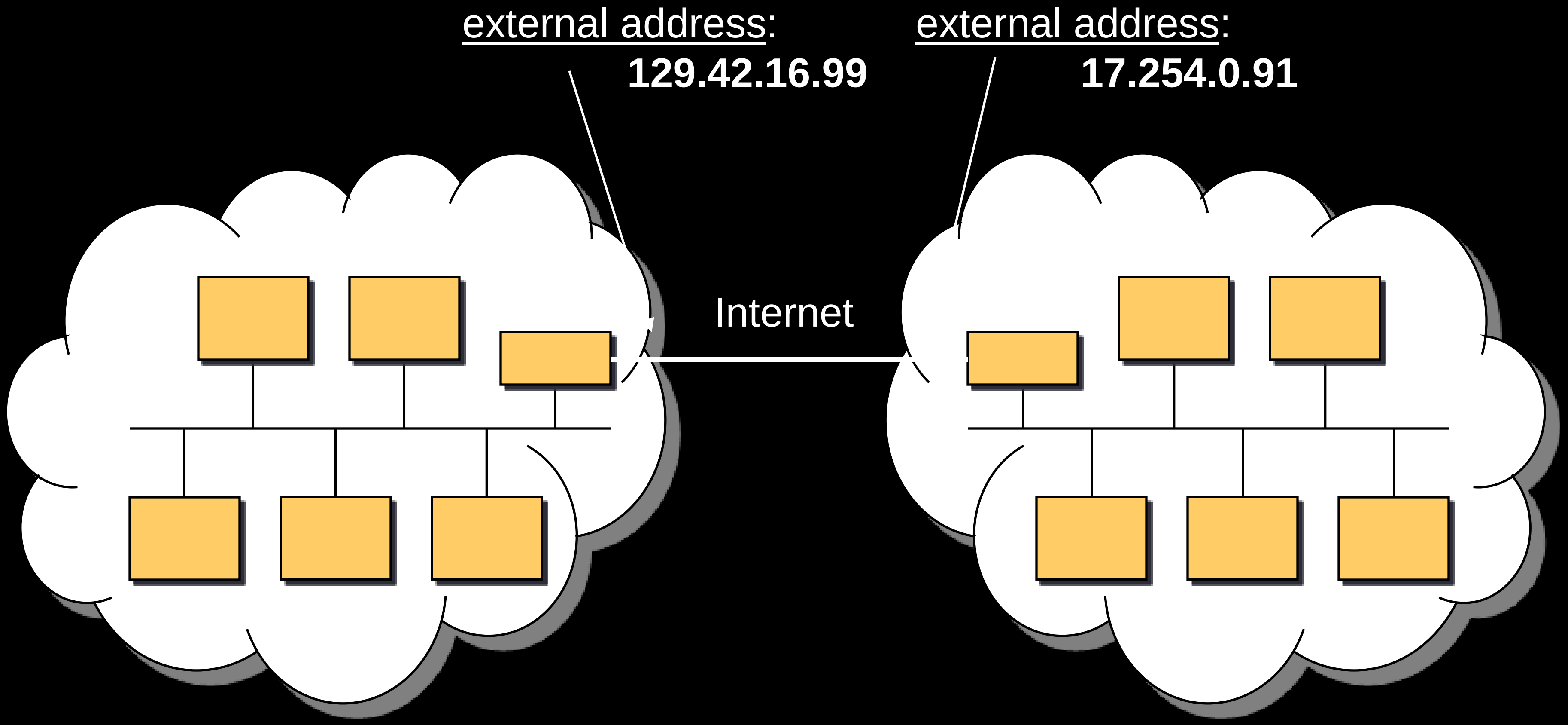
Building a VPN: tunneling

Tunneling

- Links two network devices such that the devices appear to exist on a common, private backbone

- Achieve it with encapsulation of network packets

Tunneling



external address:
129.42.16.99

external address:
17.254.0.91

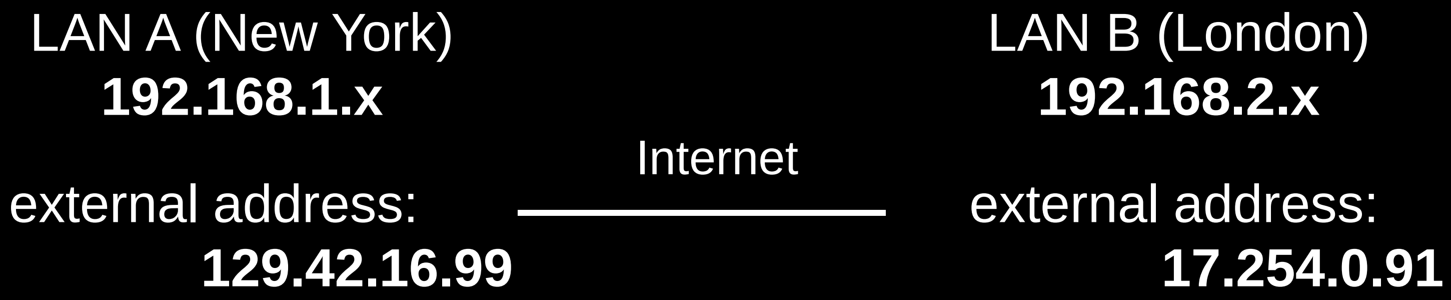
Internet

LAN A (New York)
192.168.1.x

LAN B (London)
192.168.2.x

src:	dest:	data
192.168.1.10	**192.168.2.32**	

Tunneling



LAN A (New York)
192.168.1.x

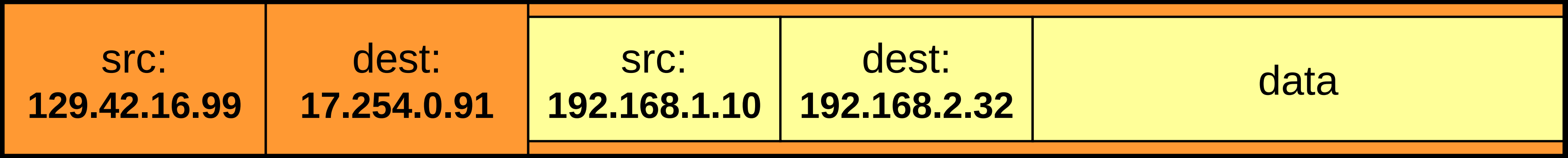
external address:
129.42.16.99

Internet

LAN B (London)
192.168.2.x

external address:
17.254.0.91

- route packets for 192.168.2.x to VPN router
- envelope packet
- send it to remote router



src:
129.42.16.99

dest:
17.254.0.91

src:
192.168.1.10

dest:
192.168.2.32

data

Tunneling

LAN A (New York)
192.168.1.x

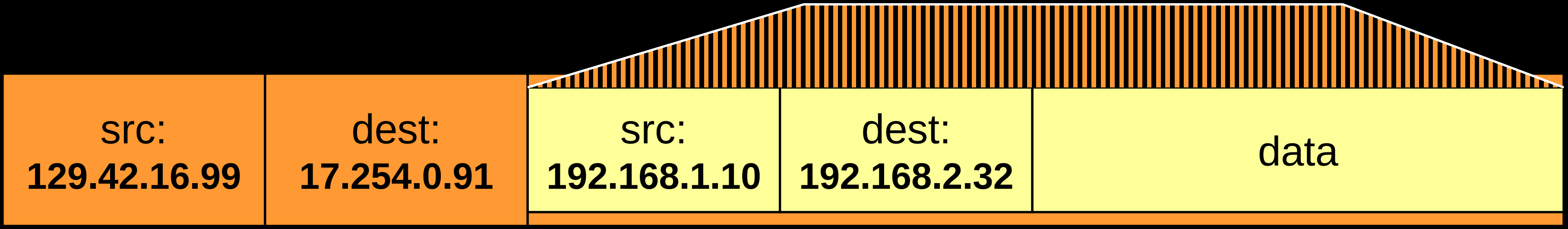
external address:
129.42.16.99

Internet

LAN B (London)
192.168.2.x

external address:
17.254.0.91

-accept packets from 129.42.16.99
-extract data (original IP packet)
-send on local network



src: **129.42.16.99**	dest: **17.254.0.91**	src: **192.168.1.10**	dest: **192.168.2.32**	data

Building a VPN: tunneling

Operation

- LAN-1 and LAN-2 each expose a single outside address and port.
- A machine in the DMZ (typically running firewall software) listens on this address and port
- On LAN-1, any packets addressed to LAN-2 are routed to this system.
  - VPN software takes the entire packet that is destined for LAN-2 and, treating it as data, sends it over an established TCP/IP connection to the listener on LAN-2
- On LAN-2, the software extracts the data (the entire packet) and sends it out on its local area network

Building a VPN: security

No need to make all machines in the local area networks accessible to the public network … just the router

BUT… an intruder can:

- examine the encapsulated packets
- forge new encapsulated packet

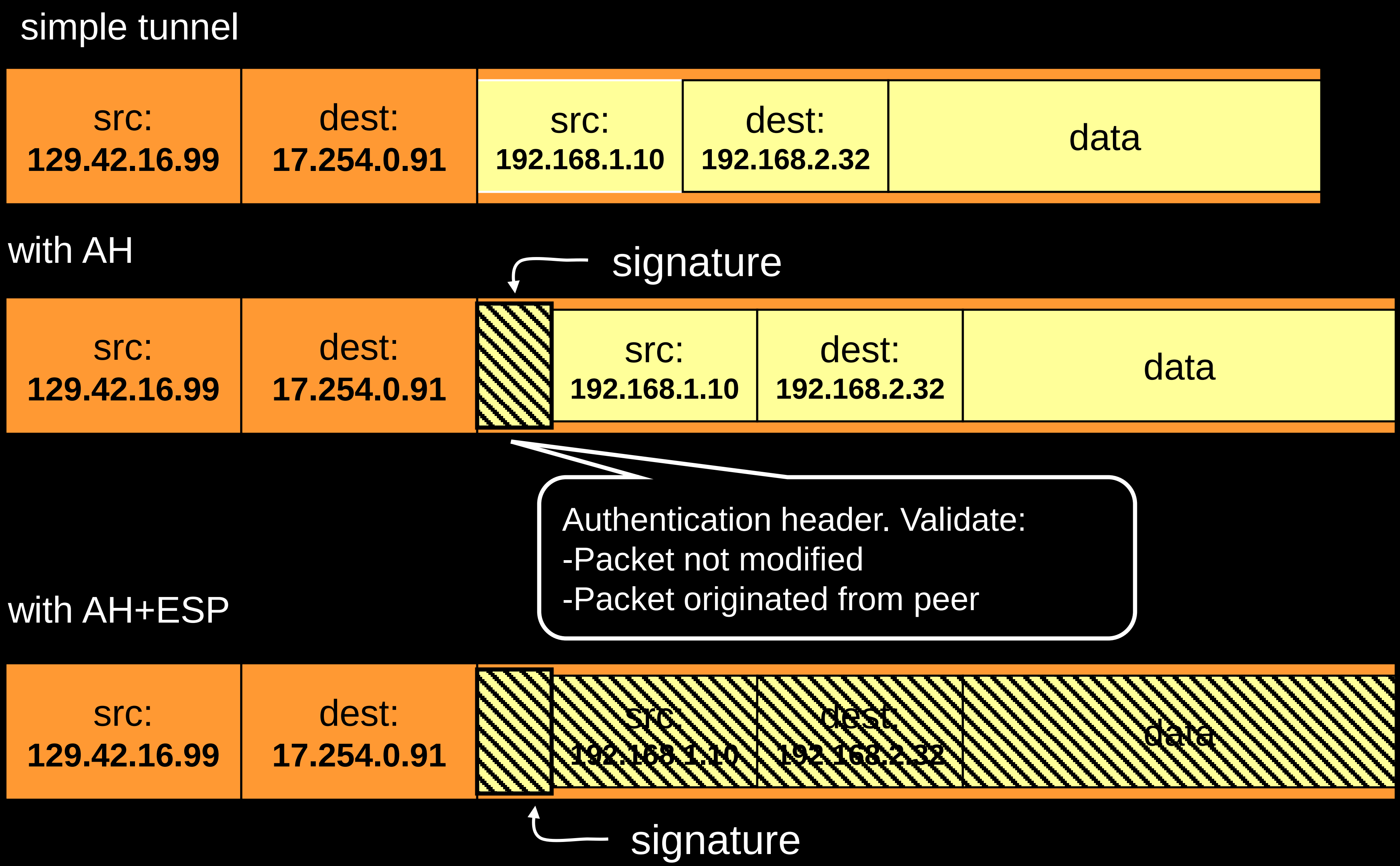
Solution:

- encrypt the encapsulated packets
  - Symmetric algorithm for encryption using session key
- need mechanism for key exchange

IPSEC: RFC 1825, 1827

- IP-layer security mechanism
- Covers authentication and encryption
- Application gets benefits of network encryption without modification
- Additional header added to packet:
  - IP **Authentication header**
    - Identifies proper source and destination – basis of point-to-point authentication
    - **Signature for IP header**
- Encapsulating Security Protocol (**ESP**)
    - Tunnel mode: **encrypt entire IP packet** (data and IP/TCP/UDP headers)
    - or Transport mode: encrypt only IP/TCP/UDP headers (faster)
- Encryption via RC4. DES. DES3, or IDEA
- Key management: manual, Diffie-Hellman, or RSA

IPSEC



simple tunnel

src: 129.42.16.99	dest: 17.254.0.91	src: 192.168.1.10	dest: 192.168.2.32	data

with AH

signature

src: 129.42.16.99	dest: 17.254.0.91	▨	src: 192.168.1.10	dest: 192.168.2.32	data

Authentication header. Validate:
-Packet not modified
-Packet originated from peer

with AH+ESP

src: 129.42.16.99	dest: 17.254.0.91	▨	src: 192.168.1.10	dest: 192.168.2.32	data

signature

PPTP

- PPTP: point-to-point tunneling protocol
- Extension to PPP developed by Microsoft
- Encapsulates IP, IPX, NetBEUI
- Conceptually similar to IPSEC
  - Flawed security

The end