Sicurezza dei Calcolatori sulla rete privata

Prof. Francesco Bergadano

Dipartimento di Informatica

Università di Torino

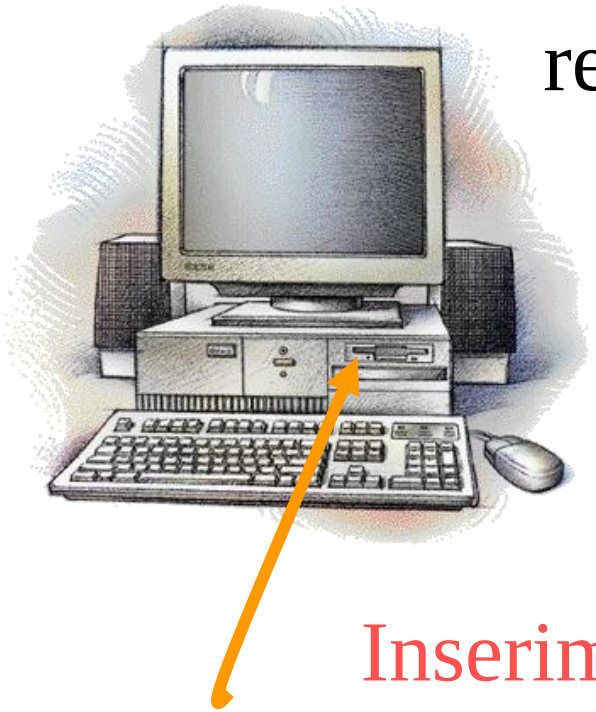
Sicurezza dei Calcolatori

Ambiente relativamente sicuro

Utilizzo diretto non autorizzato

Sicurezza dei Calcolatori

Ambiente relativamente sicuro



Inserimento di attacchi programmati da supporto magnetico

Sicurezza dei Calcolatori

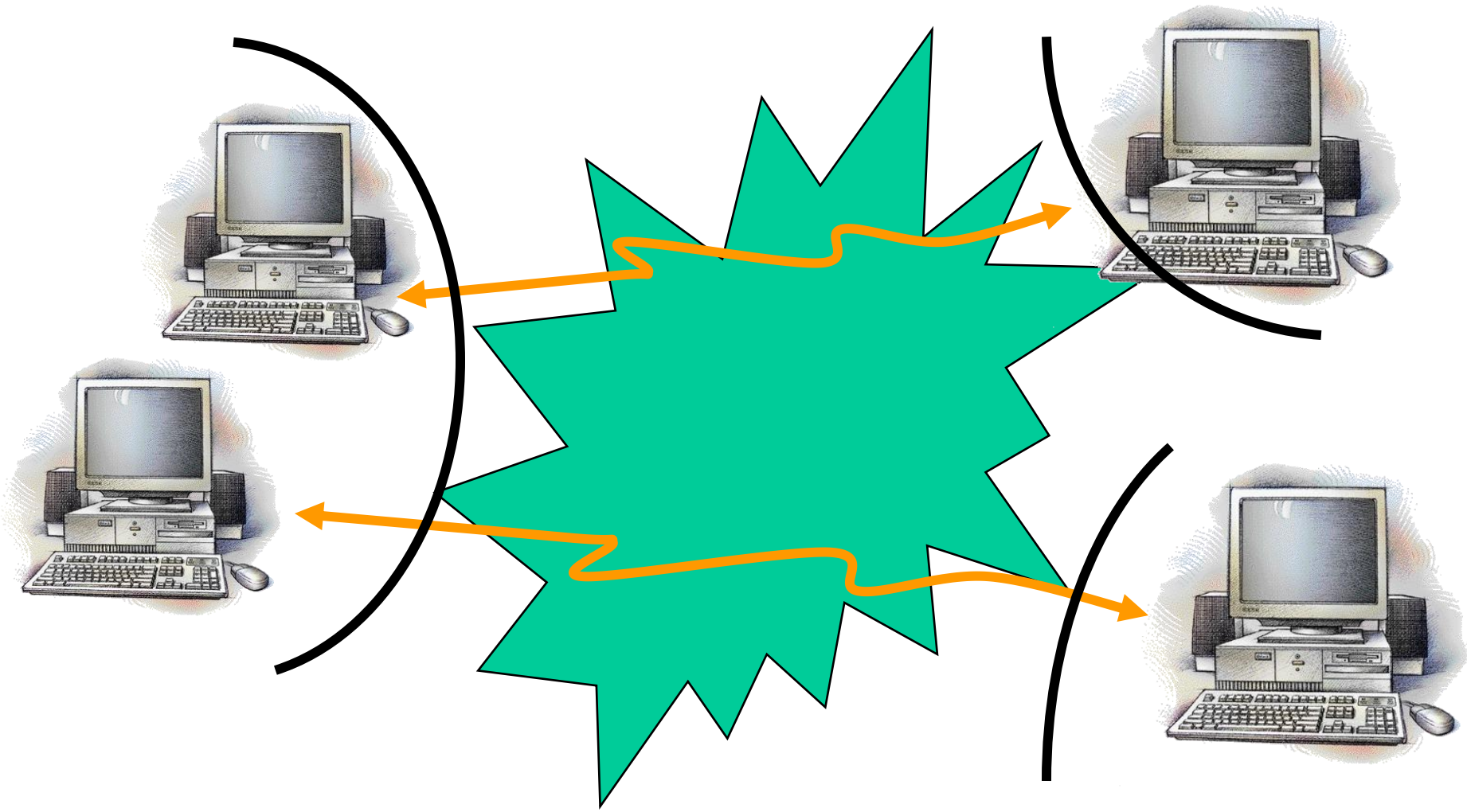
Ambiente relativamente sicuro

Rete insicura

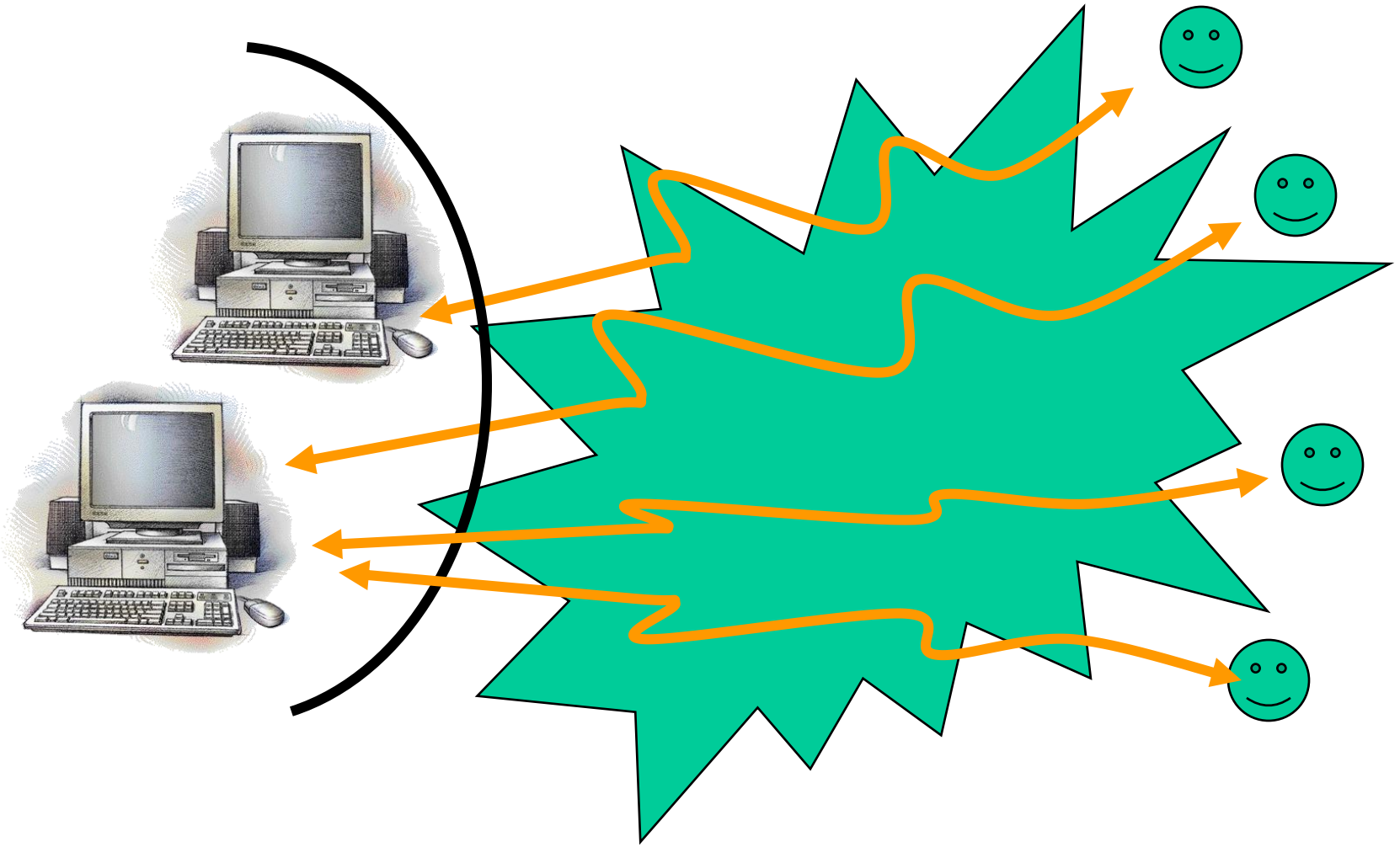
Attacchi da rete locale

Attacchi da rete geografica

Sicurezza delle Reti Private



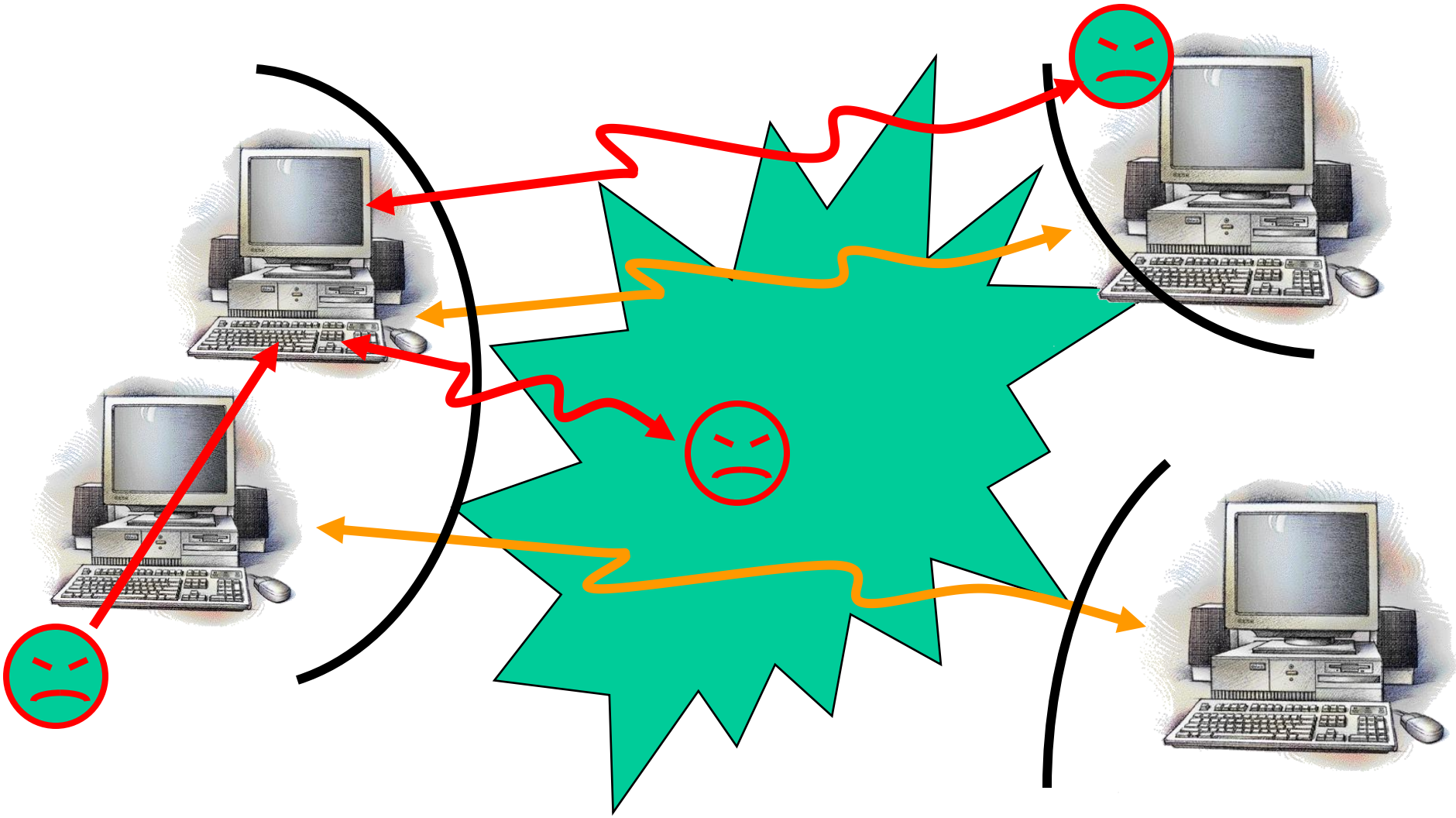
Sicurezza dei Servizi Internet



Problemi su una LAN

- **Intrusioni di utenti non autorizzati**
- **Virus e altri programmi critici per la sicurezza**
- **Sniffing, Spoofing**
- **Spamming, Flooding e denial of service**

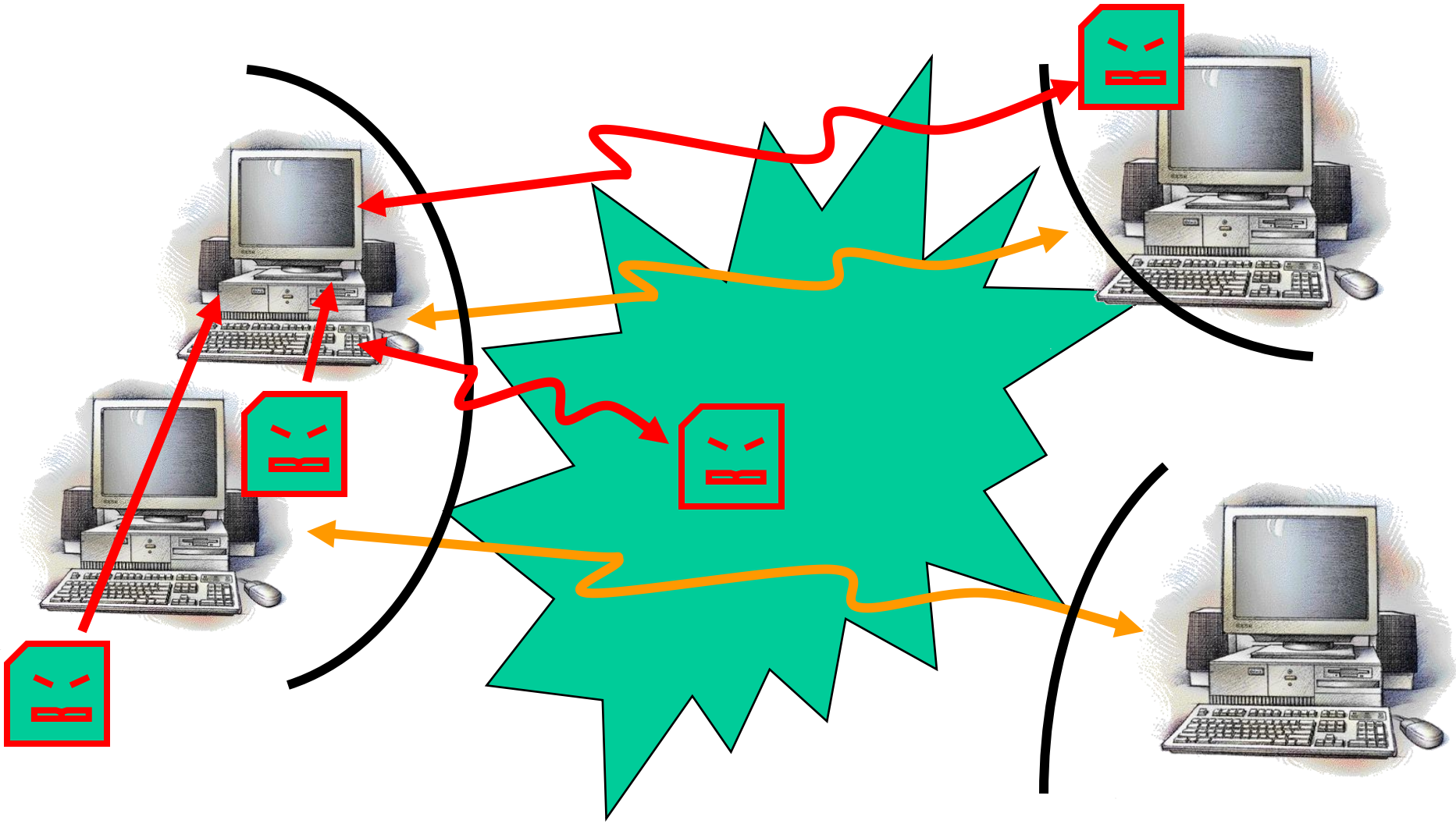
Intrusioni



Come evitare le intrusioni o limitarne i danni

- **Controllo di accesso su ogni calcolatore**
- **Firewall (filtro pacchetti e/o proxy)**
- **Limitare o evitare collegamenti esterni**
- **Logging accurato di sessioni interne e esterne, analisi manuale log**
- **Programmi di rilevamento delle intrusioni (intrusion detection)**

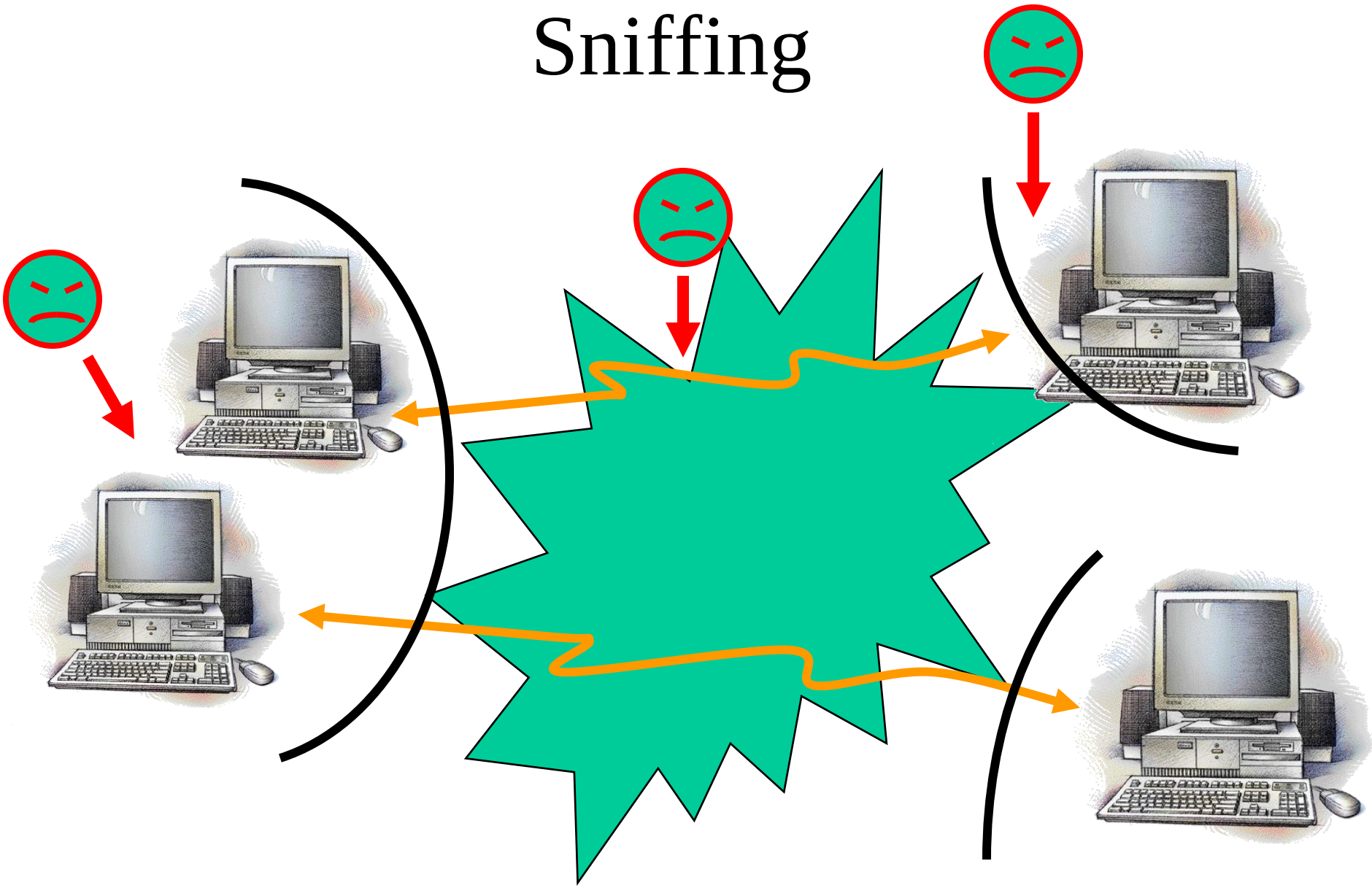
Rischio da programmi esterni



Come evitare il danno introdotto da programmi esterni

- **Probire l'installazione di software eseguita direttamente dall'utente**
- **Installare programmi 'antivirus'**
- **Inserire filtro antivirus sul firewall**
- **Mantenere backup sistematico, eventualmente prevedere disaster recovery**

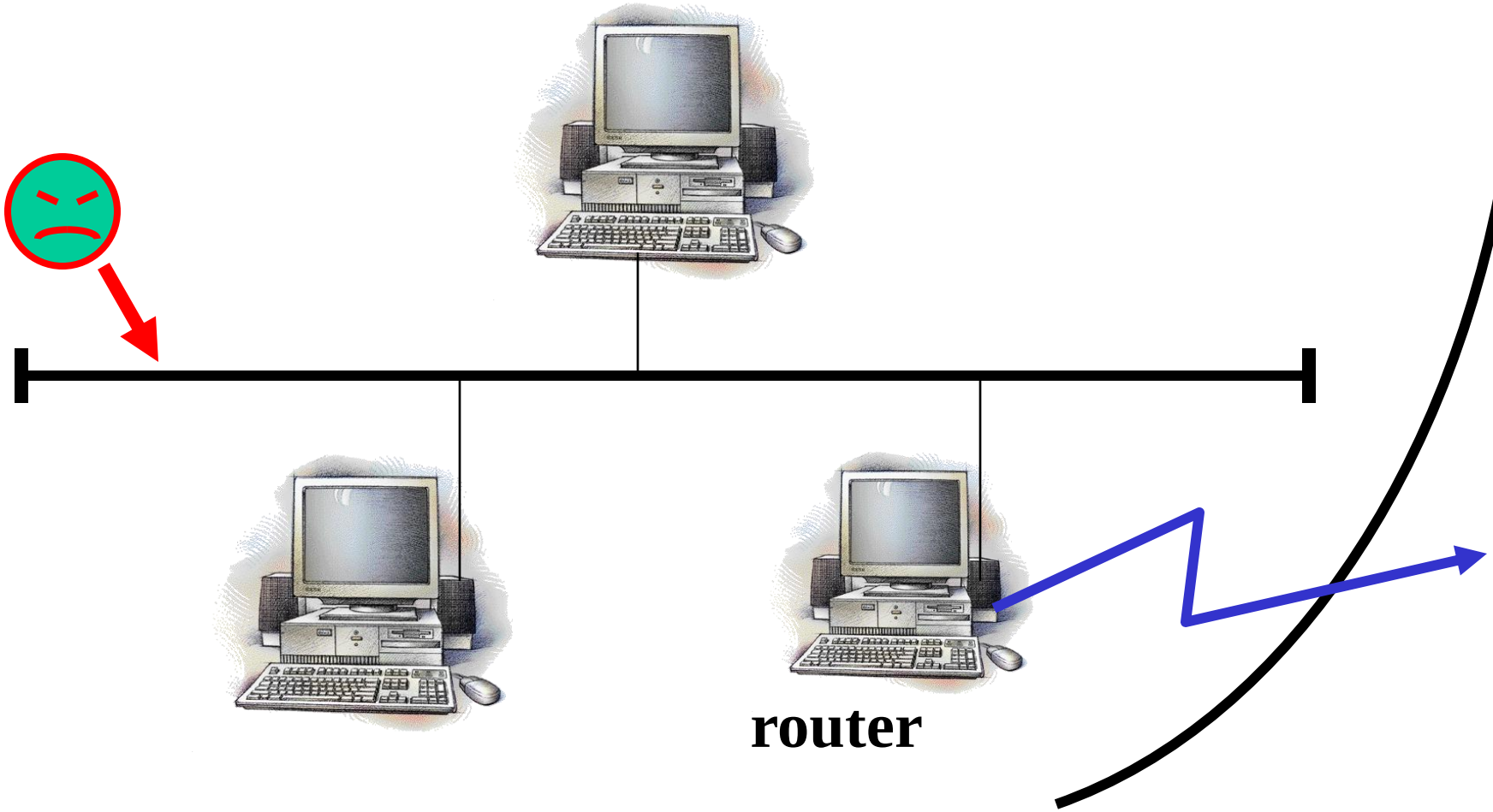
Sniffing



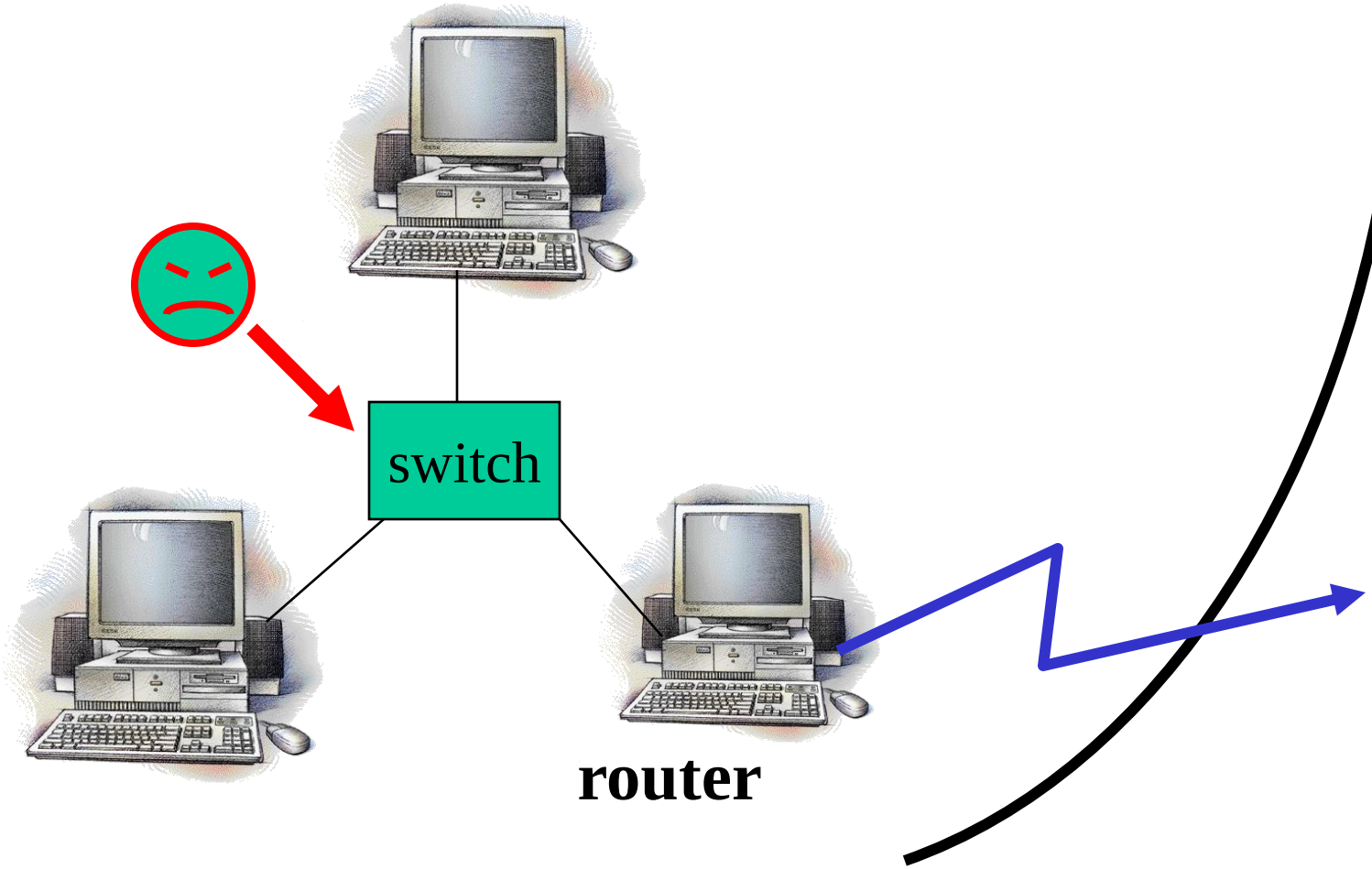
Sniffing (lettura pacchetti su rete)

- **Possibile su LAN aziendale**
- **Possibile su rete locale da dove si collega un utente autorizzato**
- **Più difficile con switch, ma possibile**
- **Possibile ma non comune su rete geografica**

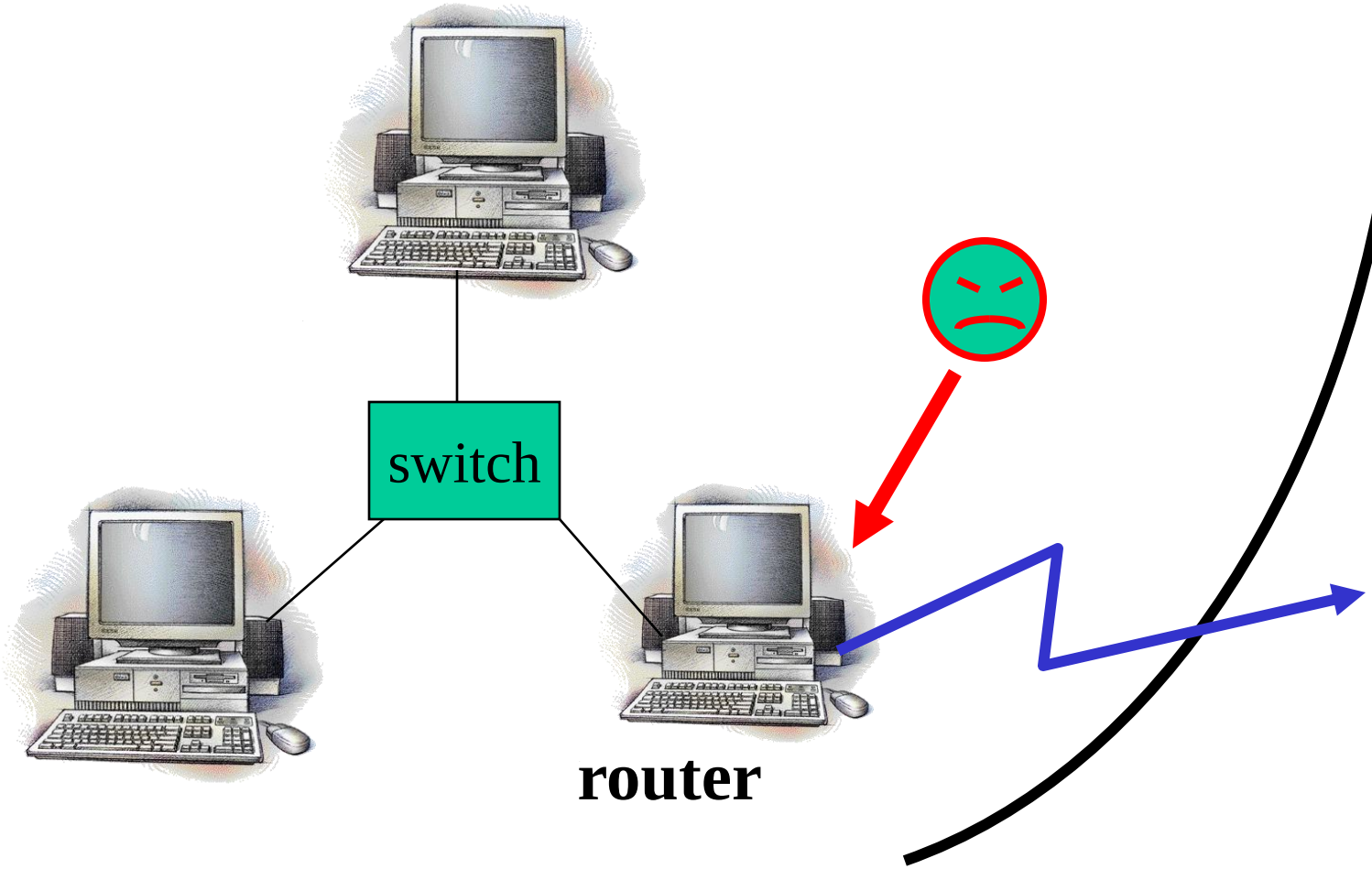
Sniffing su LAN broadcast



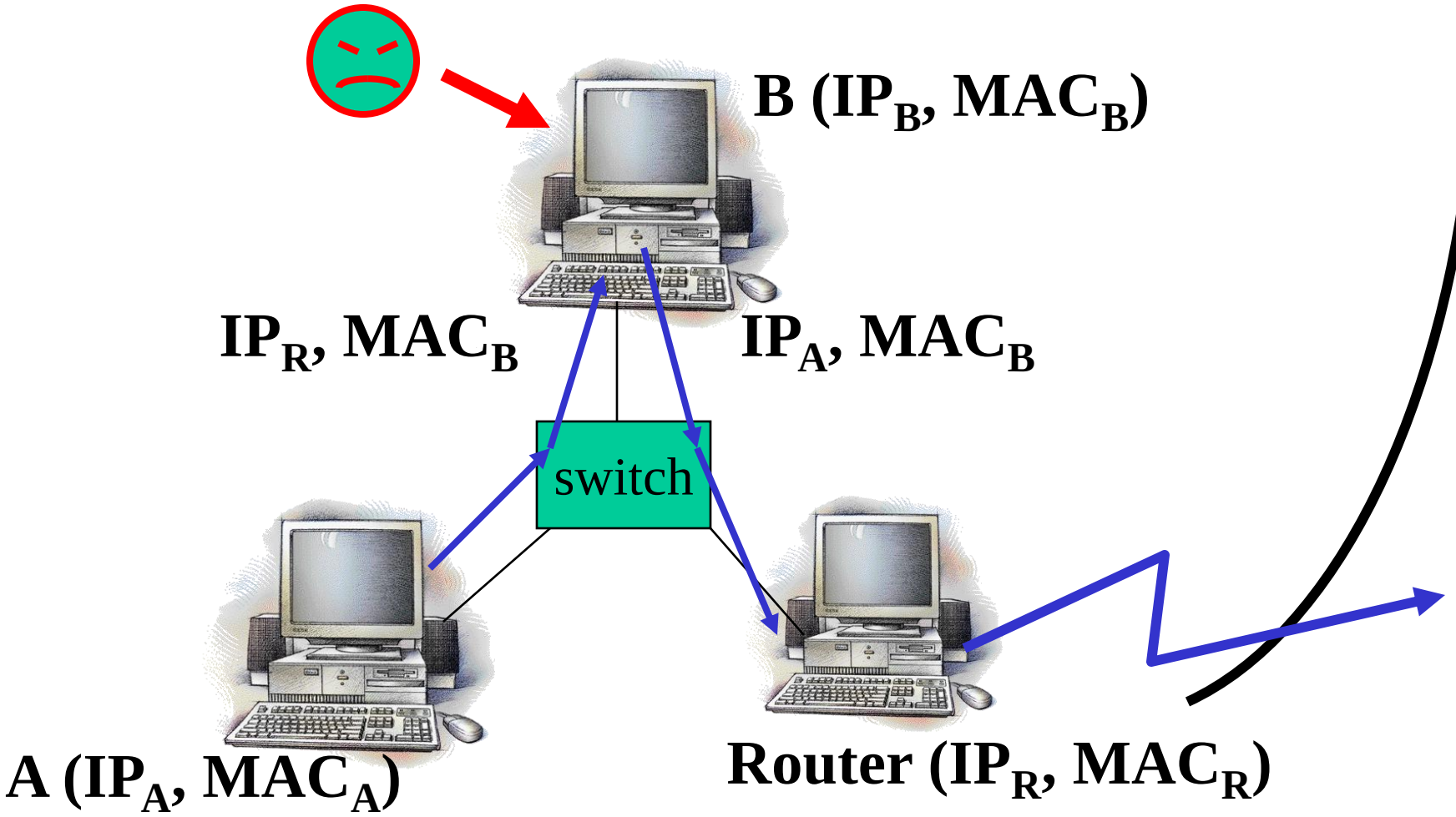
Sniffing su LAN con switch
I manomissione locale switch



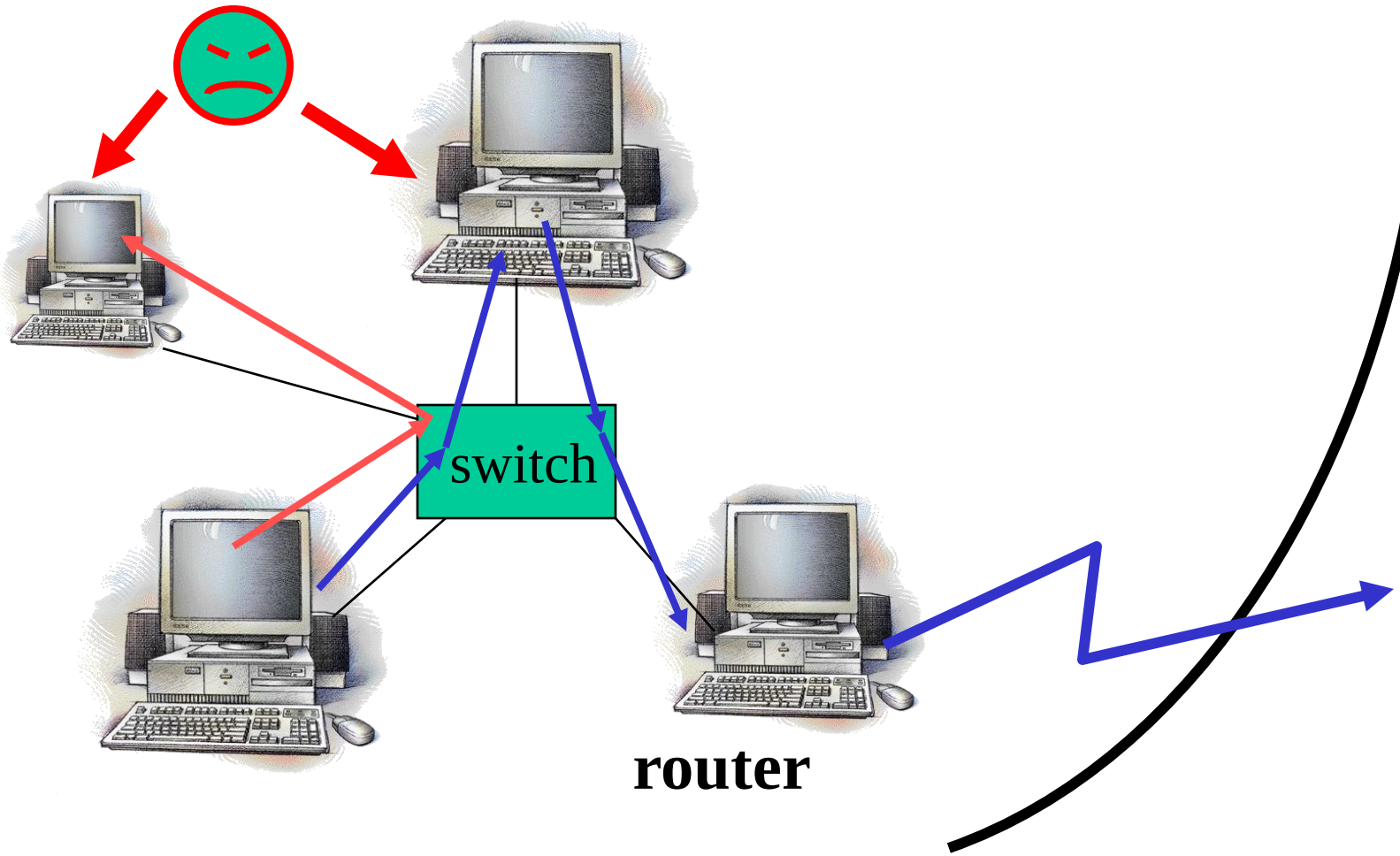
Sniffing su LAN con switch
II manomissione router



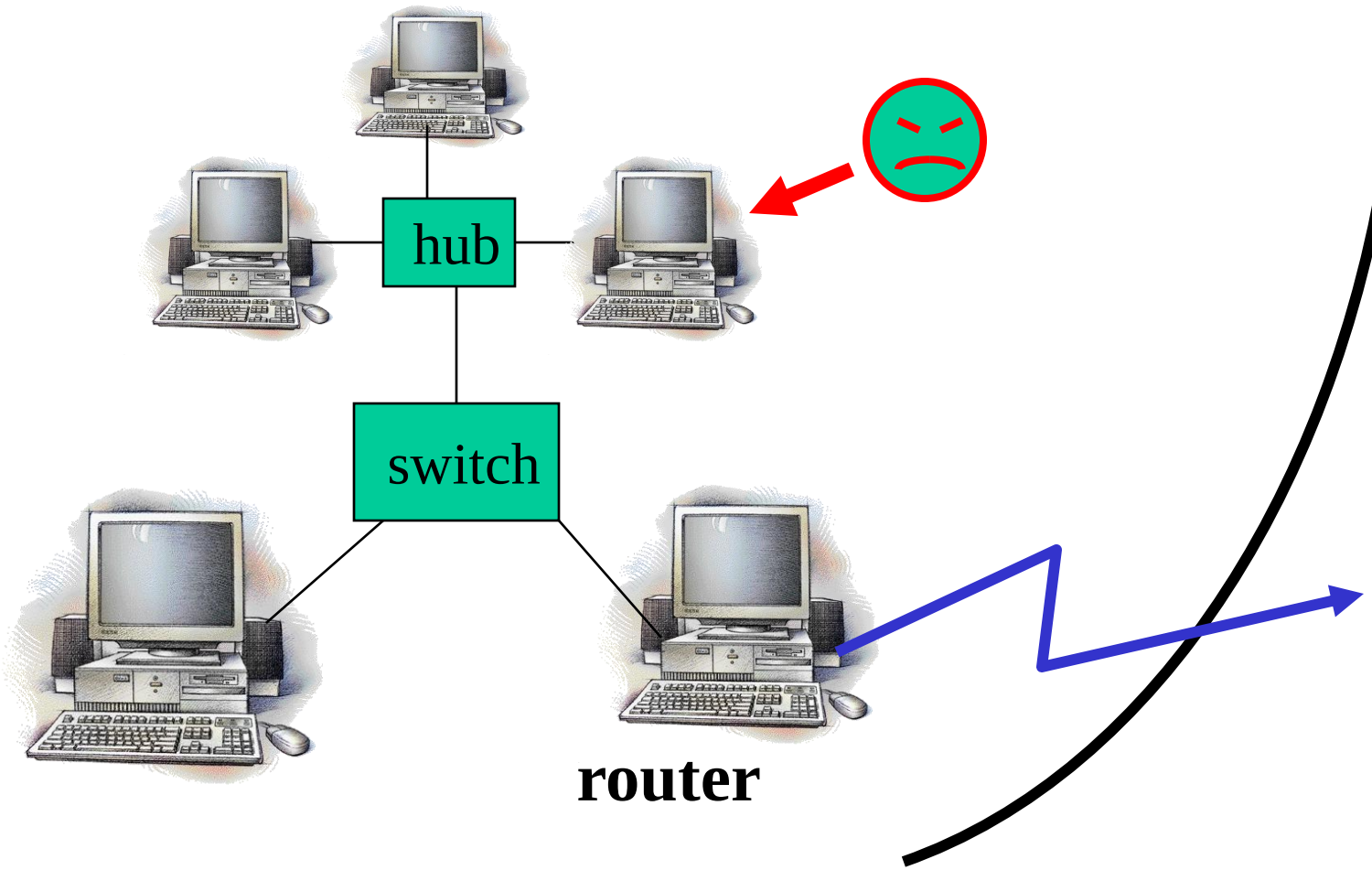
Sniffing su LAN con switch
III indirizzo hardware falso (ARP)



Sniffing su LAN con switch
IV indirizzo IP falso (DNS)



Sniffing su LAN con switch
V diretto su sottorete con hub



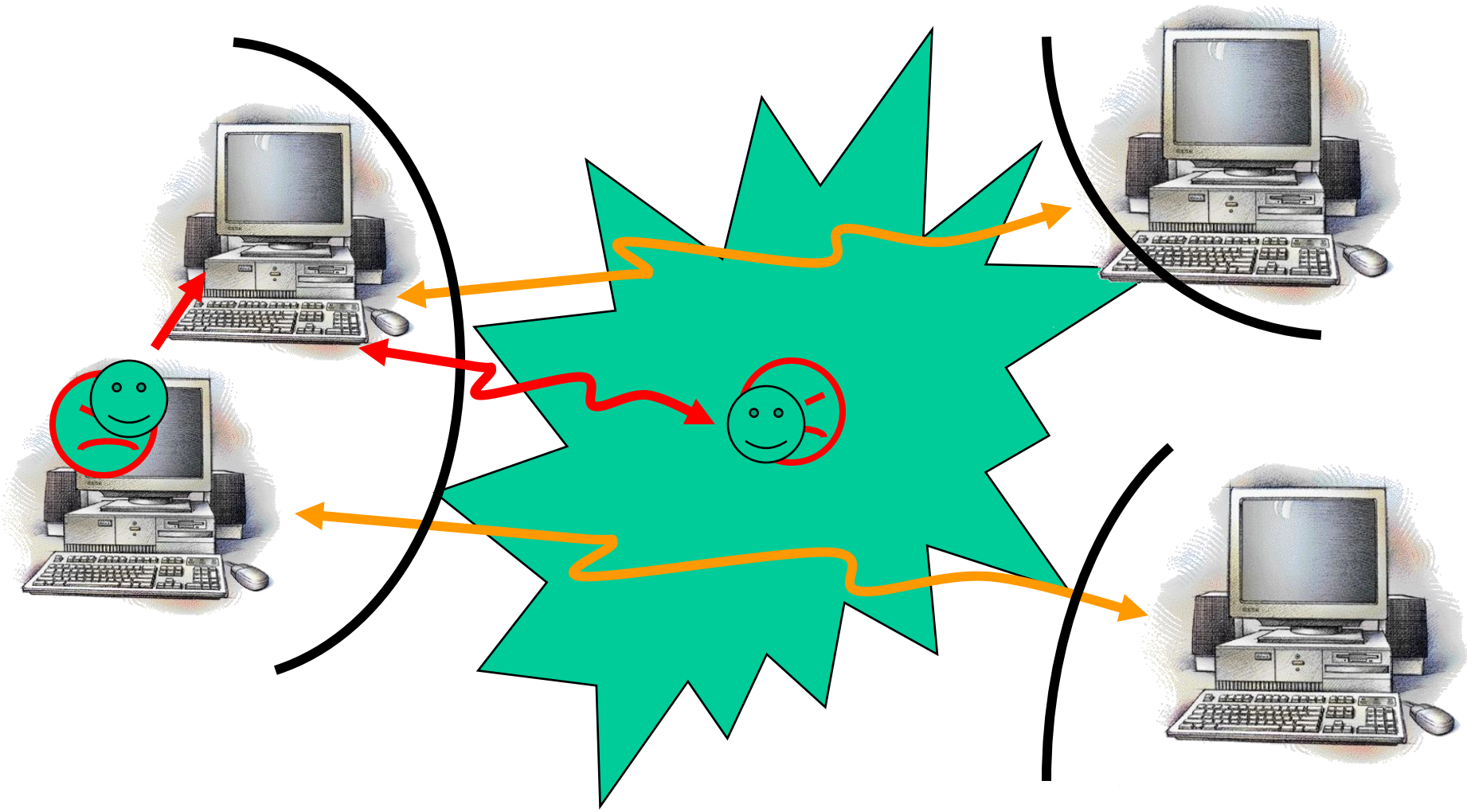
Come evitare sniffing su LAN

- **Usare reti con switch (non hub)**
- **Cifrare a livello applicativo**
- **Cifrare a livello di trasporto**
- **Cifrare a livello IP su ogni calcolatore**
- **Routing livello 2, ARP statico, DHCP statico, rilevamento indirizzi hardware non validi per indirizzo IP**

Come evitare sniffing all'esterno

- **Cifrare a livello applicativo**
- **Cifrare a livello di trasporto**
- **Cifrare a livello IP su router o firewall**
- **Impedire collegamento diretto da rete non controllata**

Spoofing (indirizzi falsi)



Spoofing (falsificazione indirizzi)

- **Indirizzi hardware su LAN**
- **Indirizzi IP**
- **Indirizzi simbolici (DNS)**
- **URL (Web spoofing)**

Spoofing indirizzi hardware

- **Possibile su segmento broadcast della rete locale**
  - **per ricevere agendo su ARP e configurando scheda di rete in modalità ‘promiscua’**
  - **per trasmettere agendo su certi tipi di schede di rete, cambiando l’indirizzo mittente**
- **Inutile su rete geografica**

IP Spoofing

- **Possibile su rete locale anche con TCP**
- **Possibile su rete geografica con UDP**
- **In generale impossibile con TCP su WAN**

DNS Spoofing

- **Configurando i calcolatori con l'indicazione di un DNS server che è possibile controllare**
- **Controllando il DNS server normalmente usato sulla LAN**

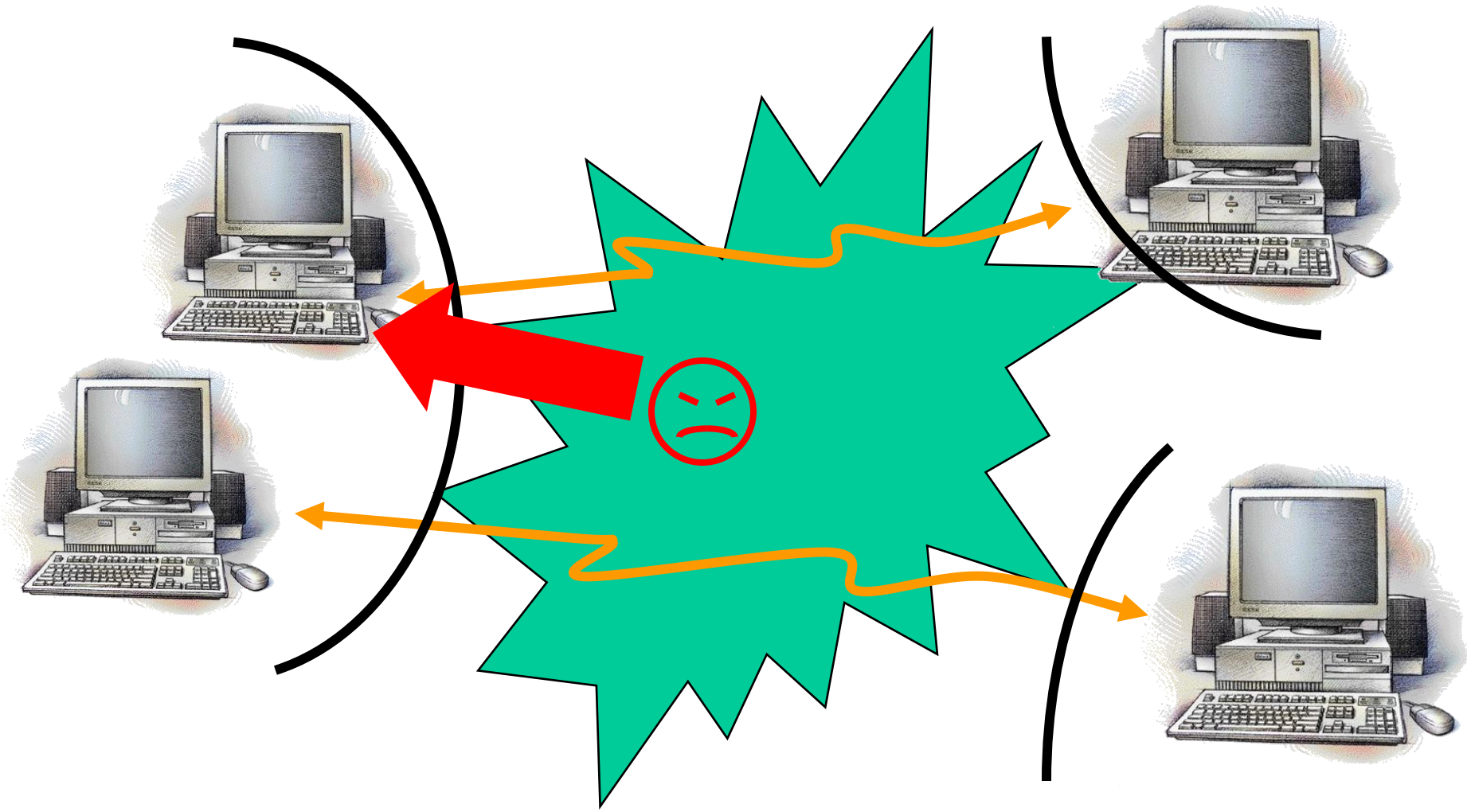
Web Spoofing

Utilizzando una URL credibile per certi contenuti, e controllando il server per quella URL (esempio www.comit.it), oppure

utilizzando una URL qualunque e agendo sui link presenti in pagine Web visitate spesso

Quindi inserendo contenuti arbitrari per la URL che è possibile controllare

Denial of Service (DOS)



Come evitare il denial of service

- **In generale, molto difficile evitarlo**
- **In generale raro (non c'è normalmente un motivo per dedicarvi risorse)**
- **Per applicazioni particolari (allarmi, militari, servizi ad alta affidabilità) occorrono reti dedicate**

Esempio: Syn flooding

- Inizio connessioni TCP a ripetizione verso il calcolatore vittima (possibile con indirizzo IP spoofed, visto che la connessione viene solo iniziata, e l'handshake TCP non deve essere completato)

Esempio 2: ICMP echo request

- Mando un gran numero di echo request verso un calcolatore B (reflector), con un indirizzo IP sorgente falsificato e uguale a quello della vittima

- Caso particolare: “smurf attack”, dove B è un broadcast di rete o sottorete. Il mittente ha indirizzo IP “spoofed” uguale all’indirizzo della vittima A, che si trova sulla stessa rete o sottorete.

Spamming con relay SMTP

Si tratta di una forma particolare di flooding, dove però c'è uno scopo preciso: utilizzare un mail server altrui per inviare posta elettronica in grandi quantità.

Può essere facilmente evitato configurando il mail server in modo adeguato