Strumenti di sicurezza delle reti:

nozioni di base e componenti open-source

ing. Roberto Larcher

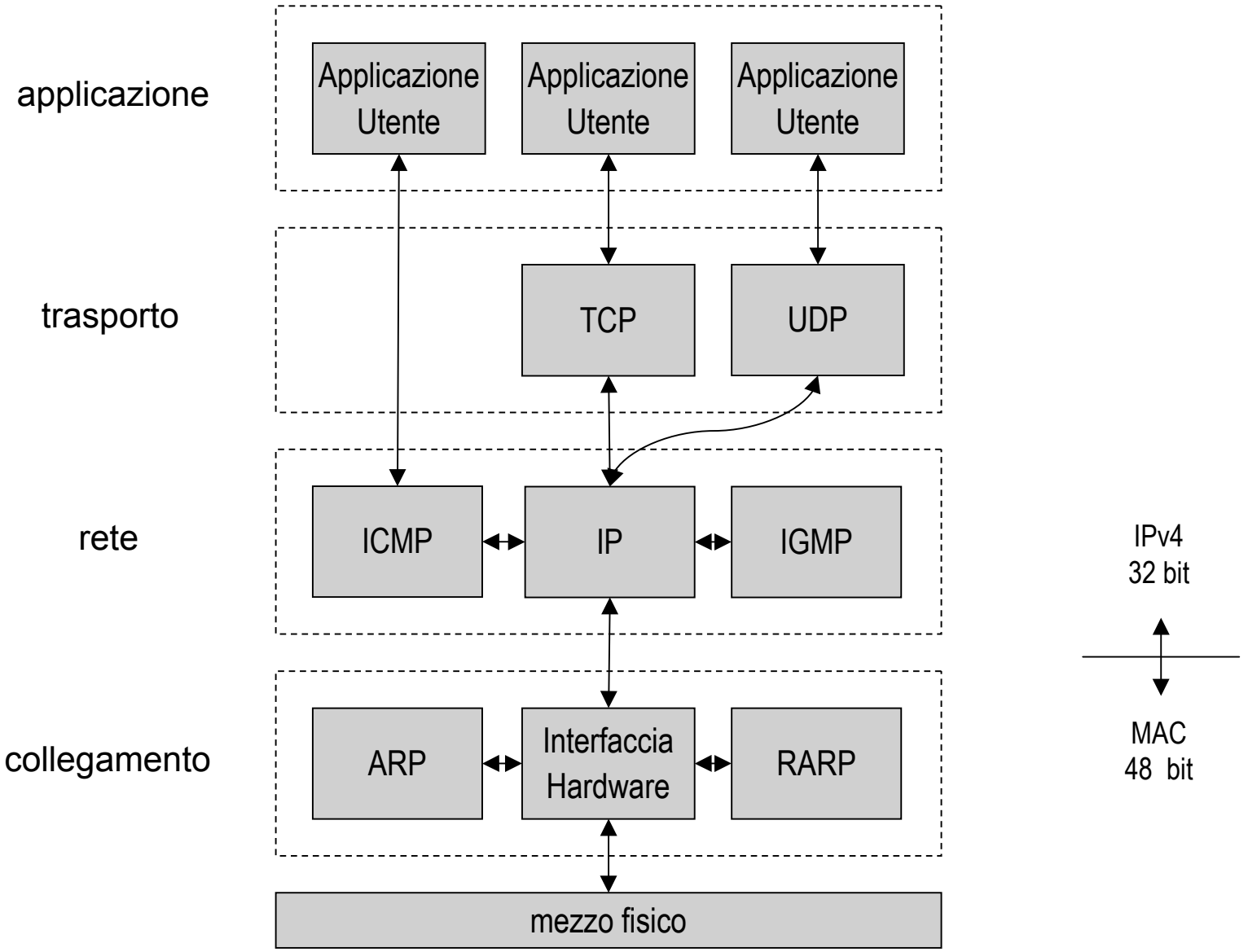
http://utenti.lycos.it/webteca

robertolarcher@hotmail.com

Obiettivi del Seminario

- Prima parte: sapere cosa circola in rete
  - Nozioni di base del protocollo TCP/IP
  - reti a mezzo condiviso (ethernet su hub, token-ring e wi-fi)
  - reti segmentate (switched-ethernet e VLAN).
  - libreria pcap – winpcap
- Seconda parte: agire sui dati
  - la possibilità di forgiare pacchetti di informazione
  - pacchetti “impossibili”
  - libreria Libnet
- Terza parte: alcuni strumenti open-source
  - open-source
  - tool di solo “sniffing”: Snort
  - tool di solo “packet forging”: macof
  - tool di “sniffing & forging”: tcpkill

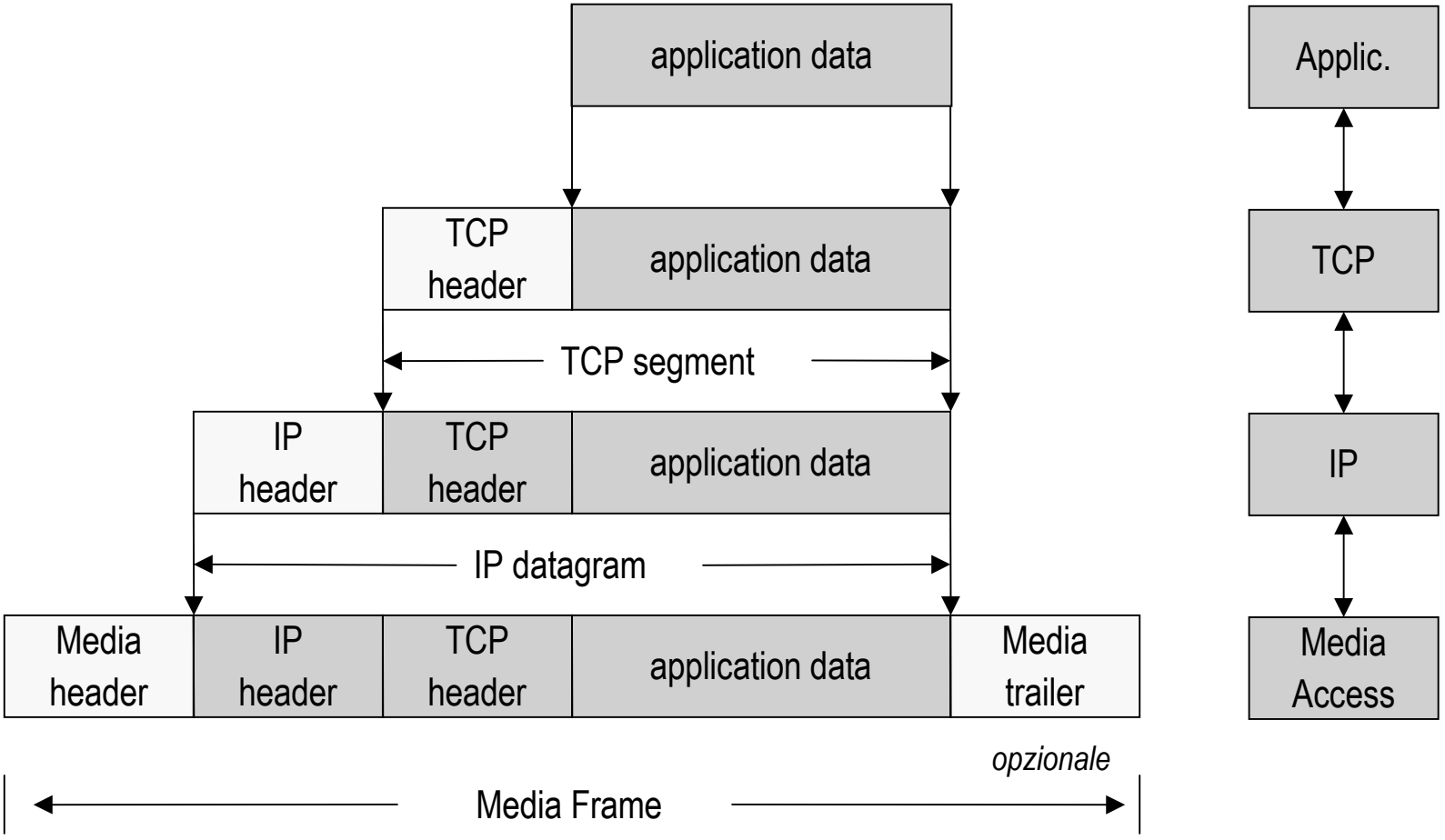
La *suite* TCP/IP: alcuni protocolli



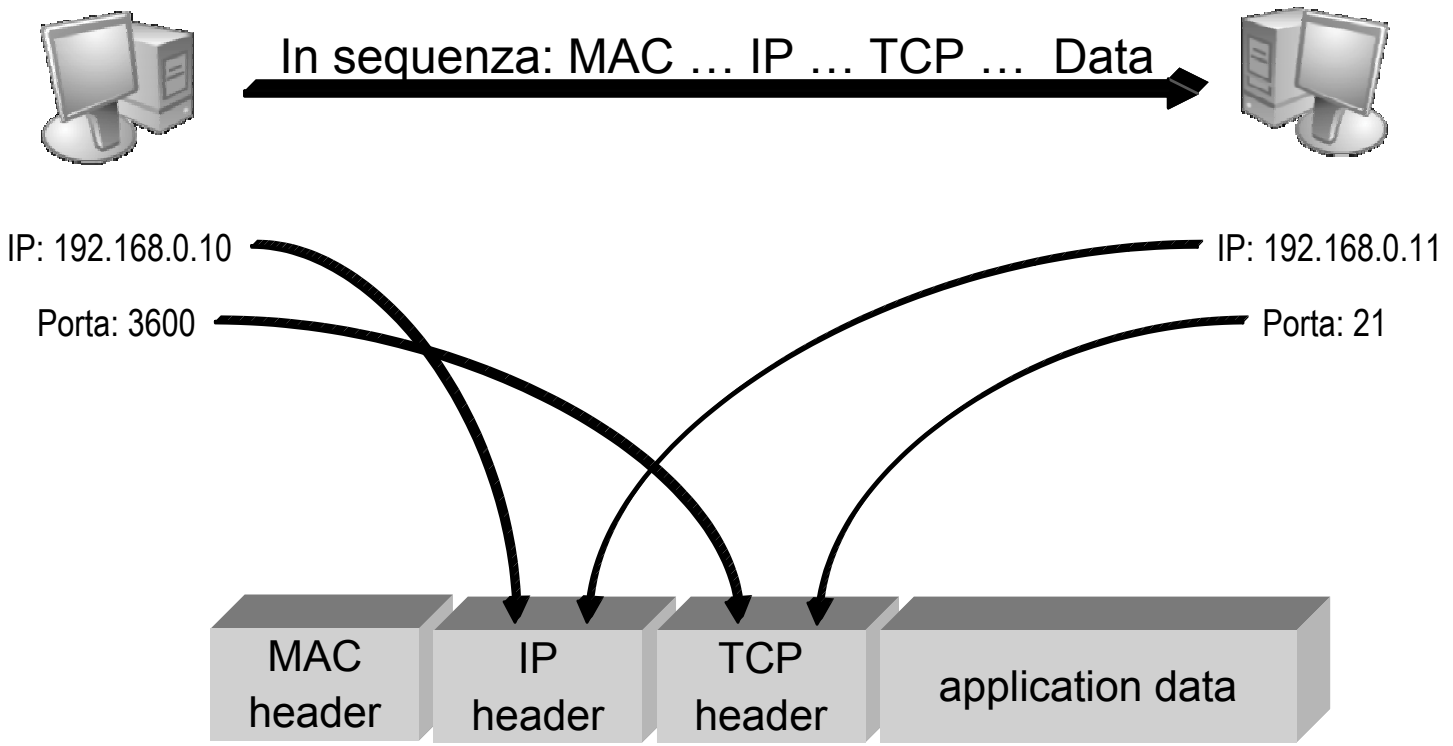
La *suite* TCP/IP: alcuni protocolli (2)

- IP – Internet Protocol
  - Servizio di consegna non affidabile di informazioni
  - Portare a destinazione le informazioni
- TCP – Transmission Control Protocol
  - Trasporto affidabile
  - Protocollo orientato alla connessione
- UDP – User Datagram Protocol
  - Trasporto non affidabile
  - Protocollo *connectionless*
- ICMP – Internet Control Message Protocol
  - Messaggi di controllo ed errore
- ARP – Address Resolution Protocol
  - Gestione di indirizzamenti diversi fra *layers* (2 vs 3)

Incapsulazione dei dati

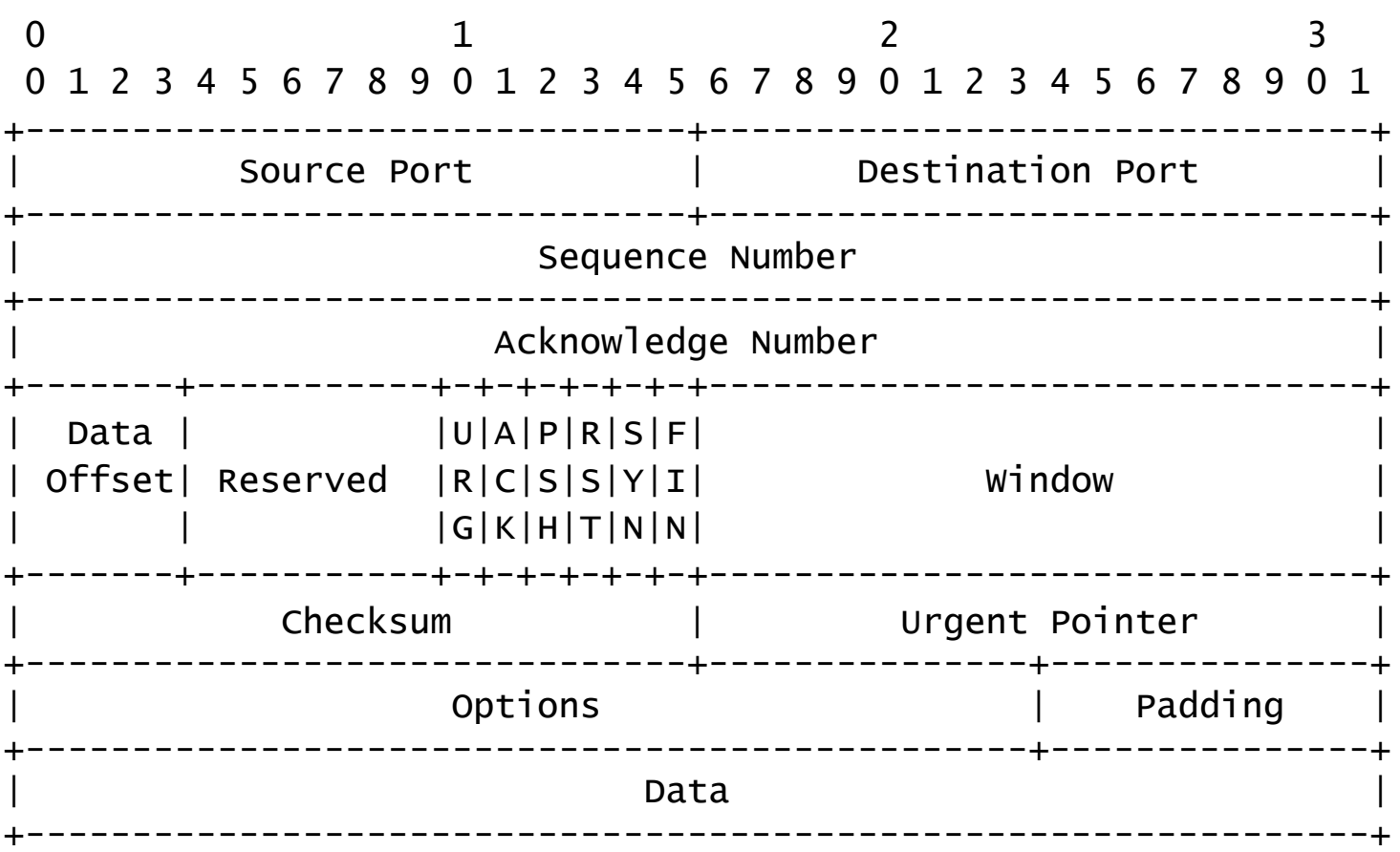


Esempio di comunicazione FTP



I dettagli sono gestiti dal Sistema Operativo

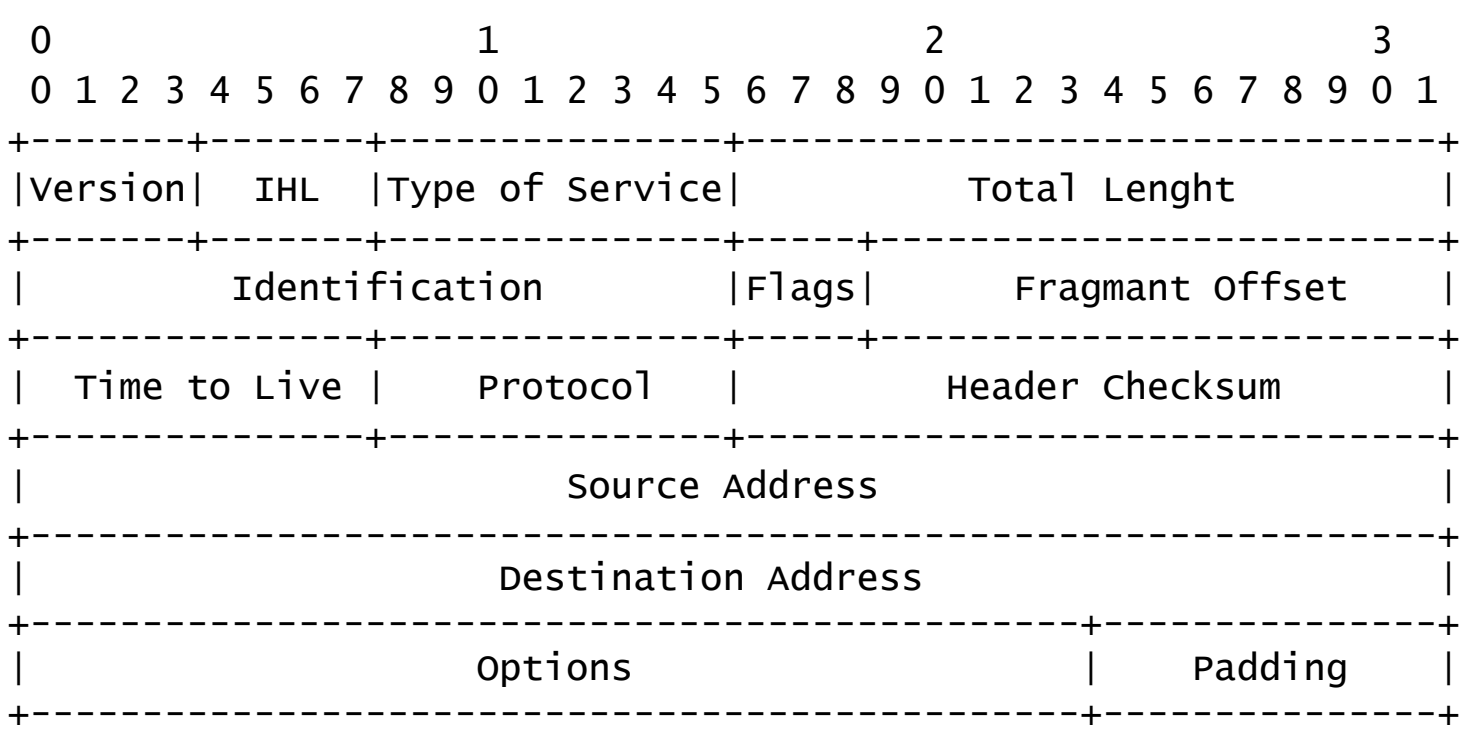
Layer 4: Header TCP



ULTERIORI INFORMAZIONI...

RFC 793 : Transmission Control Protocol DARPA Internet Program Protocol Specification – settembre 1981

Layer 3: Header IPv4



ULTERIORI INFORMAZIONI...

RFC 791 : Internet Protocol DARPA Internet Program Protocol Specification – settembre 1981

Layer 2: Media Access Method

- Metodi di accesso al mezzo fisico
  - Ethernet IEEE 802.3
  - Token Ring IEEE 802.5
  - Wireless IEEE 802.11x
  - FDDI IEEE 802.8
  - …

ULTERIORI INFORMAZIONI...

ANSI/IEEE Std 802.2, 1998 Edition - Logic Link Control
ANSI/IEEE Std 802.5, 1998 Edition - Token Ring Access Method
http://standards.ieee.org/getieee802

Sniffing

Definizione

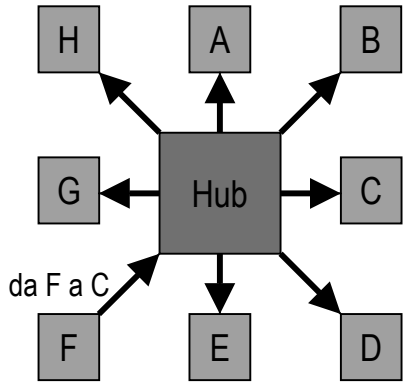
Intercettare ed analizzare il traffico di rete diretto a un nodo diverso dal proprio

Avvertenza

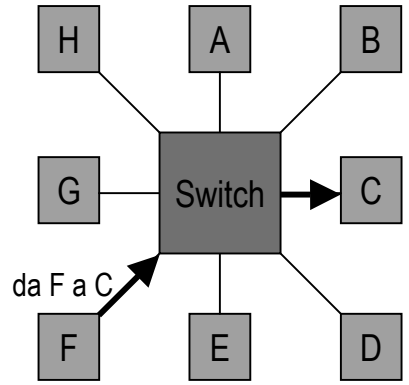
Autorizzazione ad eseguire queste attività

Reti condivise e reti segmentate

- Nelle reti condivise i pacchetti di informazioni vengono inviati a tutti i nodi



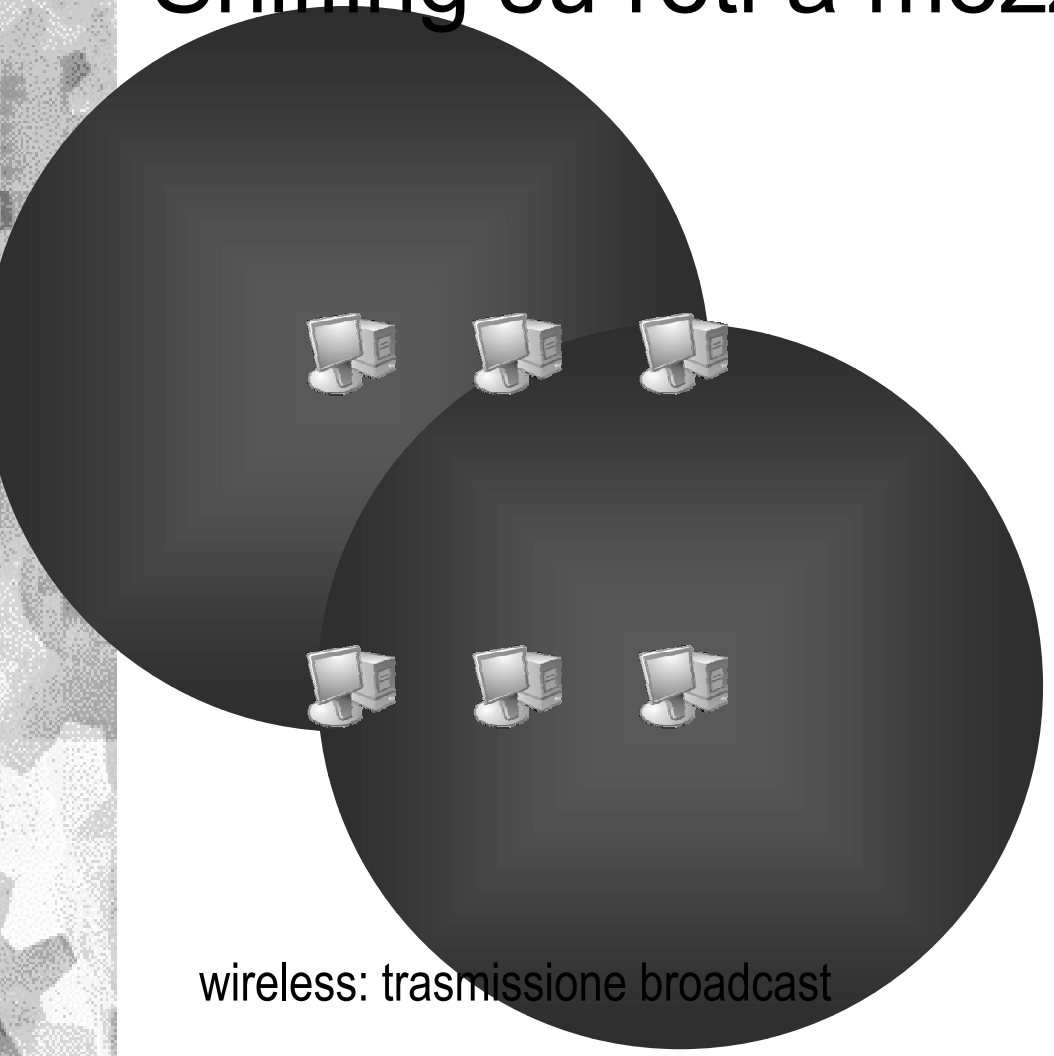
- Nelle reti segmentate i pacchetti vengono inviati solo al nodo destinatario



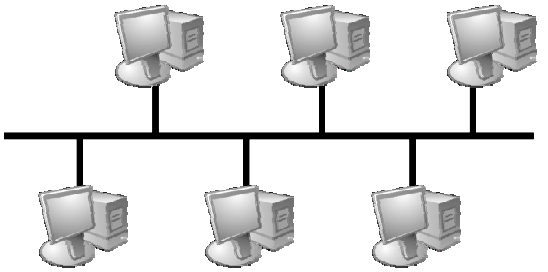
ULTERIORI INFORMAZIONI...

Ethernet Repeaters and Hubs (http://www.erg.abdn.ac.uk/users/gorry/course/lan-pages/hub.html)
Multiple Port Bridges (Switches) (http://www.erg.abdn.ac.uk/users/gorry/course/lan-pages/bridge.htm

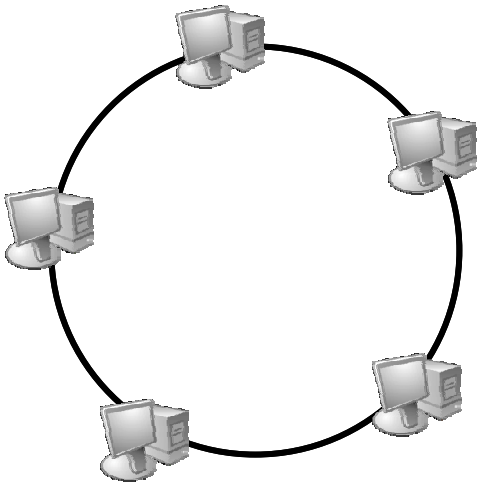
Sniffing su reti a mezzo condiviso



wireless: trasmissione broadcast

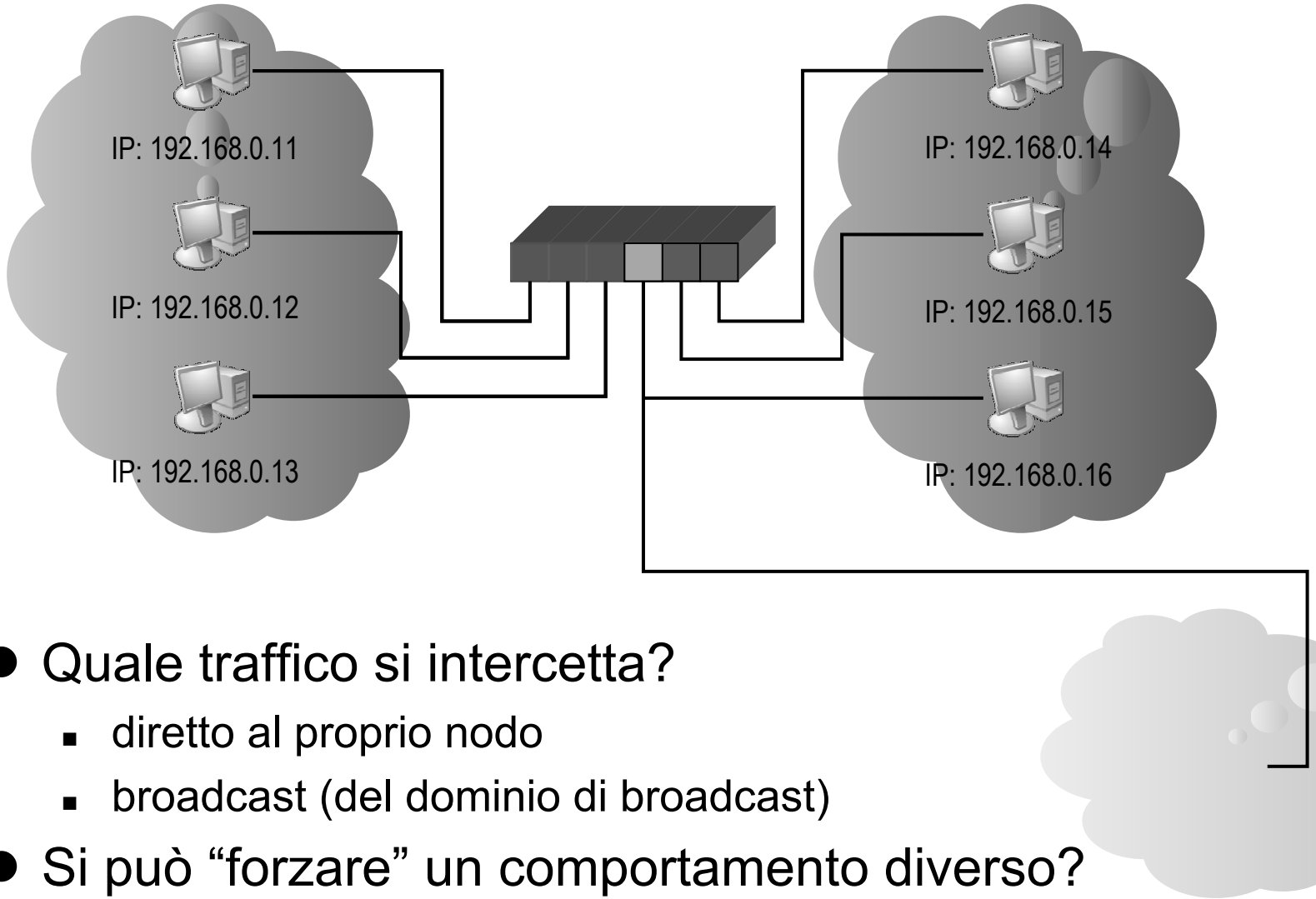


ethernet: trasmissione broadcast



token-ring: ogni stazione riceve ed invia i dati

Sniffing su reti segmentate e VLAN



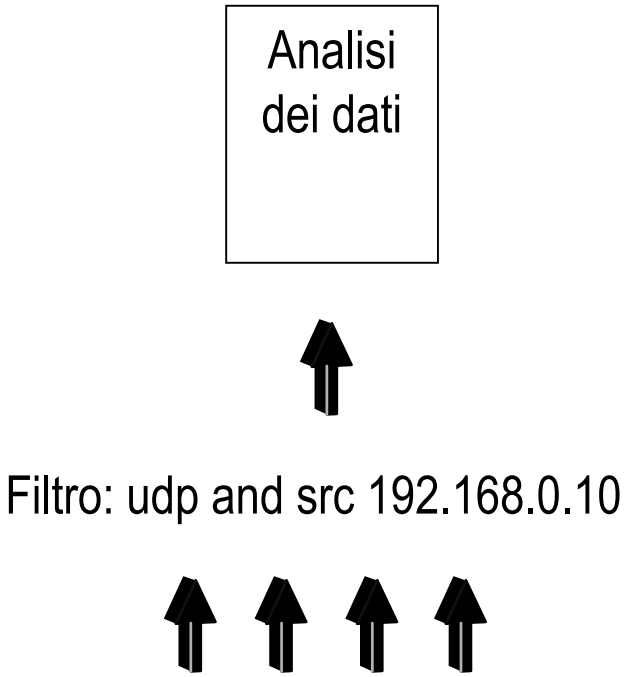
- Quale traffico si intercetta?
  - diretto al proprio nodo
  - broadcast (del dominio di broadcast)
- Si può “forzare” un comportamento diverso?

Sniffing – Componenti Open Source

- Libreria pcap
  - www.tcpdump.org
  - Liberia in C per la cattura di pacchetti
  - Licenza BSD
- Libreria winpcap
  - winpcap.polito.it
  - Versione win32 di libpcap
  - Licenza BSD (old style)

pcap: passi fondamentali di cattura

- Apertura della interfaccia
  - offline
  - online
- Compilazione del filtro
  - filtro di tipo BPF
- Applicazione del filtro
- Analisi dei dati
  - IDS
  - QoS
  - ...



Packet forging

Definizione

Creare a piacimento ed immettere in rete pacchetti di informazioni

Avvertenze

Data la possibilità di immettere in rete pacchetti “impossibili” alcuni sistemi possono reagire in modo indesiderato (DoS)

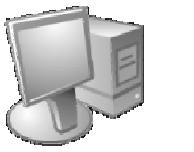
Packet forging

- I dettagli devono essere gestiti da programma
- Prerequisiti
  - Buona conoscenza dei protocolli
  - Buona padronanza delle operazioni su bit e byte
  - Buona conoscenza del linguaggio C
  - Alcuni rudimenti del linguaggio macchina nativo
- Una buona dose di pazienza...

Esempio di forgiatura IP

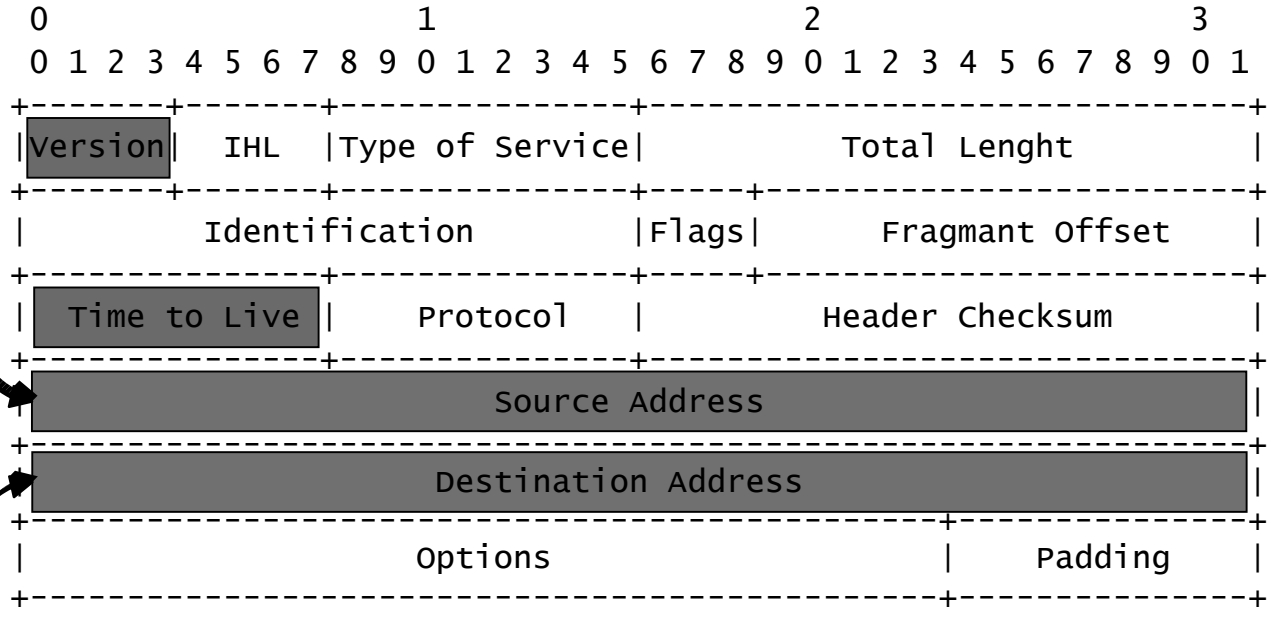
IP: 192.168.0.10

Porta: 3600



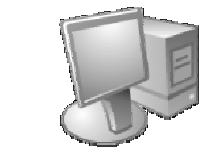
IP: 192.168.0.11

Porta: 21



- Alcuni Dettagli
  - Il protocollo IPv4 viene identificato da Version == 4
  - Il TTL viene decrementato ad ogni salto di rete (hop

Esempio di forgiatura TCP

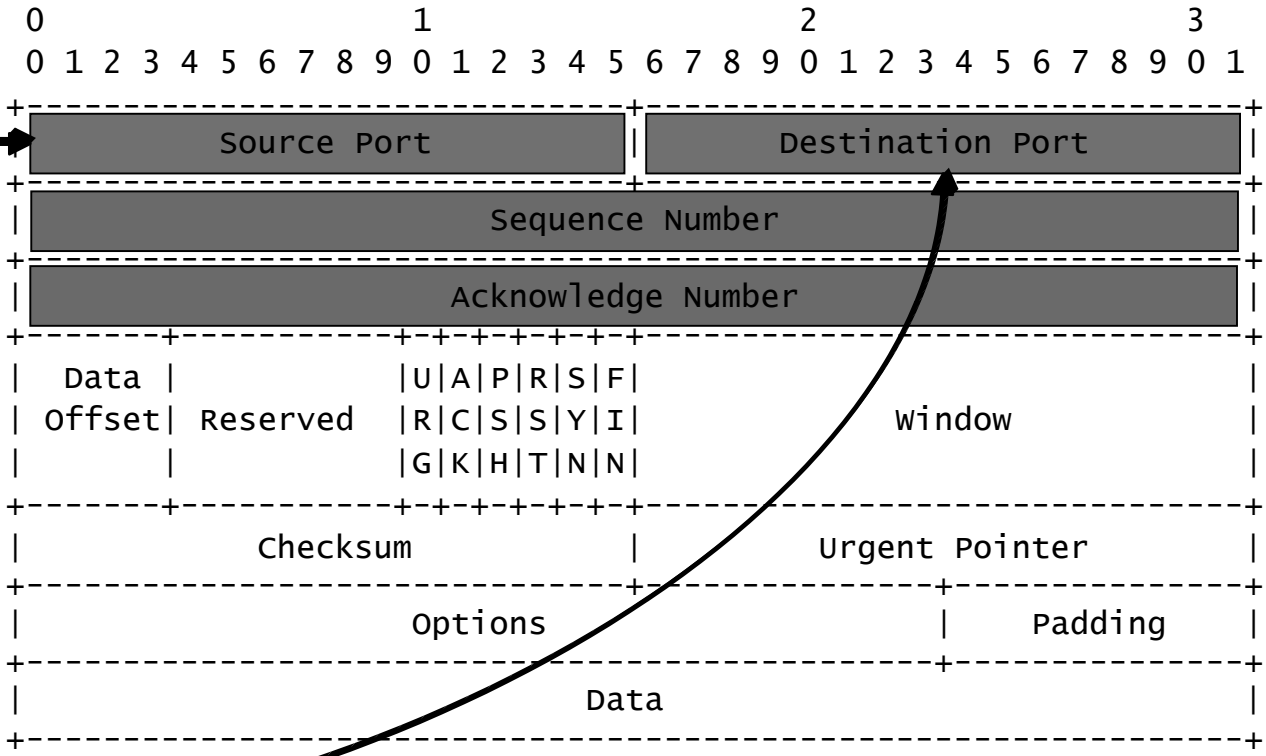


IP: 192.168.0.10

Porta: 3600

IP: 192.168.0.11

Porta: 21



Pacchetti “impossibili”

- Ping of Death
  - Si tratta di inviare un pacchetto ICMP Echo con dimensione superiore a quella stabilita dai protocolli
- Effetto
  - Su alcuni sistemi operativi di “vecchia data” questo causa un crash di sistema

Pacchetti “impossibili” - 2

- Land attack
  - Si tratta di inviare (a un router) un pacchetto TCP/IP con indirizzo di destinazione uguale al mittente e porta di destinazione uguale alla porta mittente
- Effetto
  - Se non opportunamente configurati i router entrano in loop e, come minimo, riducono la loro capacità di servizio

ULTERIORI INFORMAZIONI...

“Router Security Configuration Guide” – National Security Agency, 2002
http://www.nsa.gov

Forging – Componenti Open Source

- Libreria Libnet
  - www.paketfactory.net
  - Liberia in C per la forgiatura di pacchetti
  - Licenza BSD
- Libreria Libnet for win32
  - utenti.lycos.it/webteca
  - Versione win32 di Libnet
  - Licenza BSD – OSI certified
  - Estensioni per altri link layer - Token Ring

Libnet: passi fondamentali

- Inizializzare la libreria
  - Si specifica del metodo di immissione dei pacchetti
  - Si specifica l'interfaccia con cui iniettare i pacchetti
- Costruire il pacchetto
  - Con l'aiuto di apposite funzioni si creano i pacchetti
- Scrivere il pacchetto
  - Il pacchetto viene immesso in rete
- Chiudere la libreria

ULTERIORI INFORMAZIONI...

Building Open Source Security Tools: Components and Techniques – Mike D. Schiffman – Wiley 2003

Libnet: link layer vs raw socks

- metodo di immissione
  - Link Layer: si simula il livello 2
  - Raw Socks: si utilizzano i socket: livello 3 e 4
- raw socks e win32
  - Il supporto del sistema operativo è “parziale”
  - L’indirizzo IP viene impostato dal sistema operativo
- Libnet for win32
  - Per compatibilità con la versione Unix viene simulato il supporto socks

Perché Open Source?

http://www.opensource.org/

Tool di solo (?) sniffing: Snort

- Che cosa è Snort
  - Network Intrusion Detection System
- Come funziona?
  - Intercetta i dati e li confronta con un database di “firme” di intrusione
  - Emette degli alert
- Che componenti Open Source utilizza?
  - pcap - winpcap
  - libnet 1.0.x – LibnetNT

ULTERIORI INFORMAZIONI...

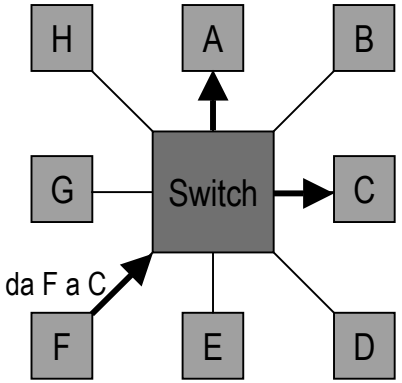
Snort Users Manual – Snort Release 1.9.x – Martin Roesch, 2002
http://www.snort.org

Snort: alcune considerazioni

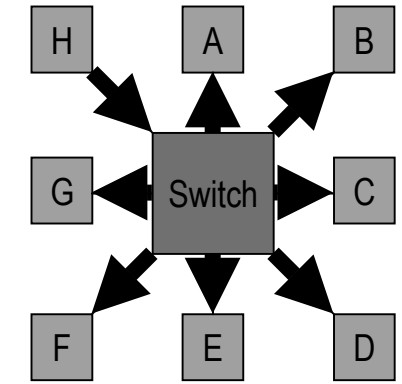
- Tuning
  - Problema dei “falsi” positivi
- Aggiornamento
  - Nuove vulnerabilità / intrusioni
- IDS su reti segmentate
  - Particolari accorgimenti
    - porte di monitoraggio
    - SPAN
  - Posizionamento
    - cosa voglio intercettare?

Reti segmentate?

- Amministratore
  - Imposta una porta di monitoraggio



- Attaccante
  - Cerca di far comportare lo switch come uno hub
  - MAC flood



Tool di solo forging: macof

- Che cosa è macof
  - Generatore di traffico casuale su layer 2
- Che scopo ha?
  - esaurire le tabelle di indirizzamento di uno switch
- Come funziona?
  - brute force
  - invio di pacchetti forgiati con MAC address casuali
- Qual è l'effetto desiderato?
  - fail open (sniff)
  - fail close (DoS)

macof: esempio di codice

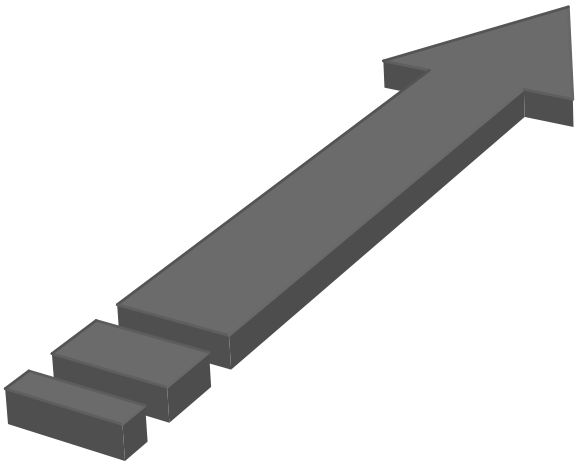
```
for(;;)
{
    src = libnet_get_prand(LIBNET_PRu32);
    dst = libnet_get_prand(LIBNET_PRu32);

    libnet_build_tcp(…);

    libnet_build_ipv4(…);

    libnet_build_link(…);

    libnet_write(…);
}
```



macof: funziona?

- Dipende…
  - Dal tipo di switch
  - Da come è configurato lo switch
- Alcune evidenze sperimentali (cisco)
  - Il fail open è limitato nel tempo
  - Viene limitato alla sola VLAN di “attacco”
  - Viene intercettato solo il rumore generato

ULTERIORI INFORMAZIONI...

Secure Use of VLANs: An @stake Security Assessment http://www.@stake.com
Dsniff http://monkey.org/~dugsong/dsniff/
WebTECA http://utenti.lycos.it/webteca/

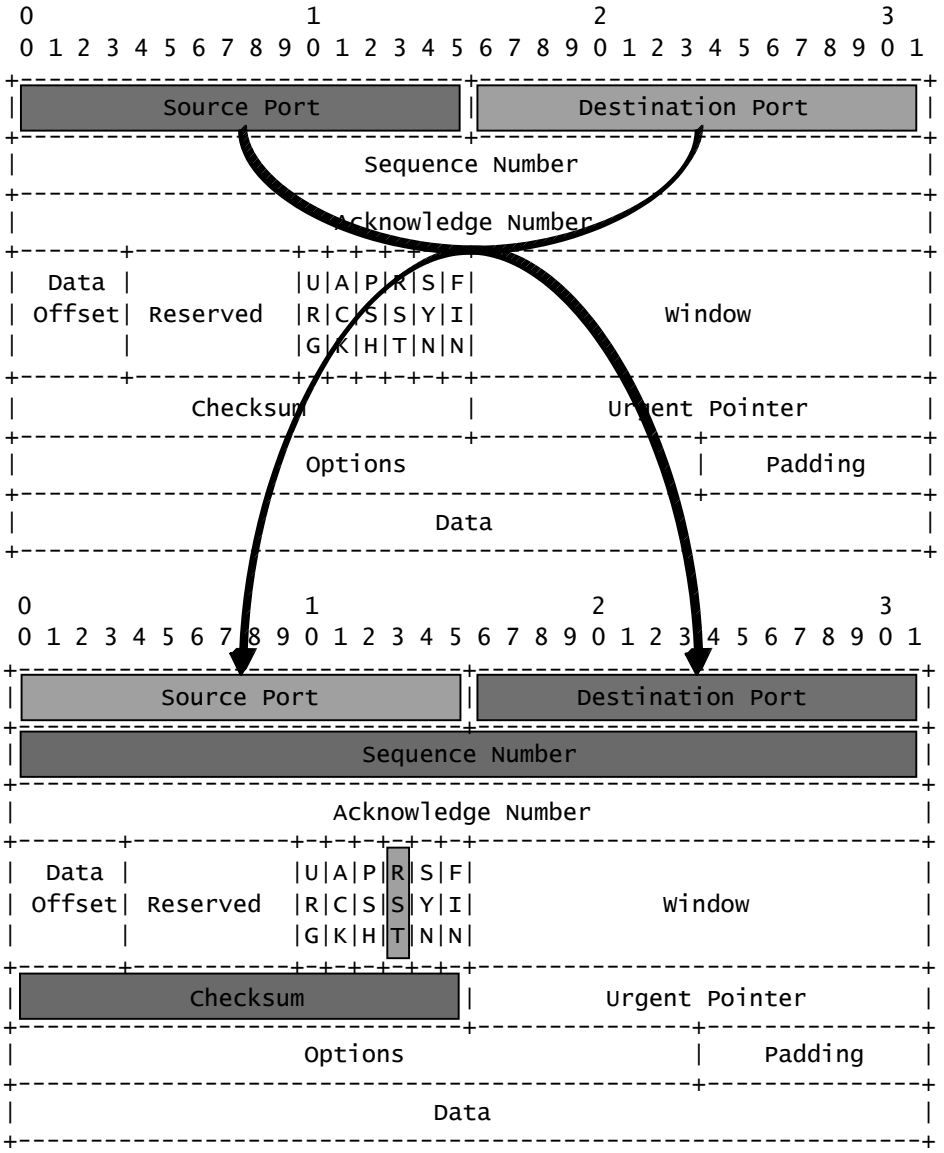
Tool di sniffing & forging: tcpkill

- Che cosa è tcpkill?
  - È un programma che cerca di resettare una connessione TCP già stabilita
- Come funziona?
  - Intercetta il traffico TCP che si desidera interrompere
  - Forgia uno o più pacchetti con flag di reset
- Che componenti Open Source utilizza?
  - pcap - winpcap
  - versione 1: libnet 1.0.x – LibnetNT
  - versione 2: libnet 1.1.x – Libnet for win32

tcpkill: schema di funzionamento

Intercettato (pcap)

forgiato (libnet)



tcpkill: esempio di codice

```
ip->ip_id = libnet_get_prand(LIBNET_PRu16);
seq = ack + (i * win);

t = libnet_build_tcp(
                    ntohs(tcp->th_dport),
                    ntohs(tcp->th_sport),
                    seq,
                    0,
                    TH_RST,
                    0,
                    0,
                    NULL,
                    LIBNET_TCP_H,
                    NULL,
                    0,
                    l,
                    0);
```

tcpkill: funziona?

Sì

ULTERIORI INFORMAZIONI...

Penetration Testing with dsniff – Christopher R. Russel – February 18, 2001
http://rr.sans.org/threats/dsniff.php

Bibliografia

RFCs:
RFC 768: "User Datagram Protocol (UDP)", Postel, J., 1980
RFC 791: "Internet Protocol (IP)", Postel, J. et al., 1981
RFC 793: "Transmission Control Protocol (TCP)", Postel, J. et al., 1981

"Router Security Configuration Guide" – National Security Agency, 2002 - http://www.nsa.gov

Building Open Source Security Tools: Components and Techniques – Mike D. Schiffman, Wiley, 2003

Snort Users Manual – Snort Release 1.9.x – Martin Roesch, 2002
http://www.snort.org

Ethernet Repeaters and Hubs
http://www.erg.abdn.ac.uk/users/gorry/course/lan-pages

TCP/IP Illustrated W. Richard Stevens
http://thermite.stanford.edu/stevens/TCP_Stevens/

Internetworking Technology Handbook – Cisco Systems, Inc – 1992-2002
http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/index.htm

Penetration Testing with dsniff – Christopher R. Russel – February 18, 2001
http://rr.sans.org/threats/dsniff.php

ANSI/IEEE Std 802.2, 1998 Edition - Logic Link Control
ANSI/IEEE Std 802.5, 1998 Edition - Token Ring Access Method
http://standards.ieee.org/getieee802

OSI Open Software Initiative
http://www.opensource.org/