La Sapienza
Università degli Studi di Roma

VULNERABILITA' E PROTEZIONE DELLE RETI

Agenda

Debolezze e vulnerabilità delle reti

- **Attacchi a livello 2 (Data link)**
- **Attacchi a livello 3 (Rete)**
- **Attacchi a livello 4 e superiori**
- **WAN**

La Sapienza
Università degli Studi di Roma

La Sapienza
Università degli Studi di Roma

Concetti di funzionamento delle reti

- La pila ISO/OSI
- I protocolli di livello 2
- I protocolli della suite IP
- I protocolli di livello 4

Composizione della Pila ISO/OSI

- I livelli
- Le attuali implementazioni

I Livelli

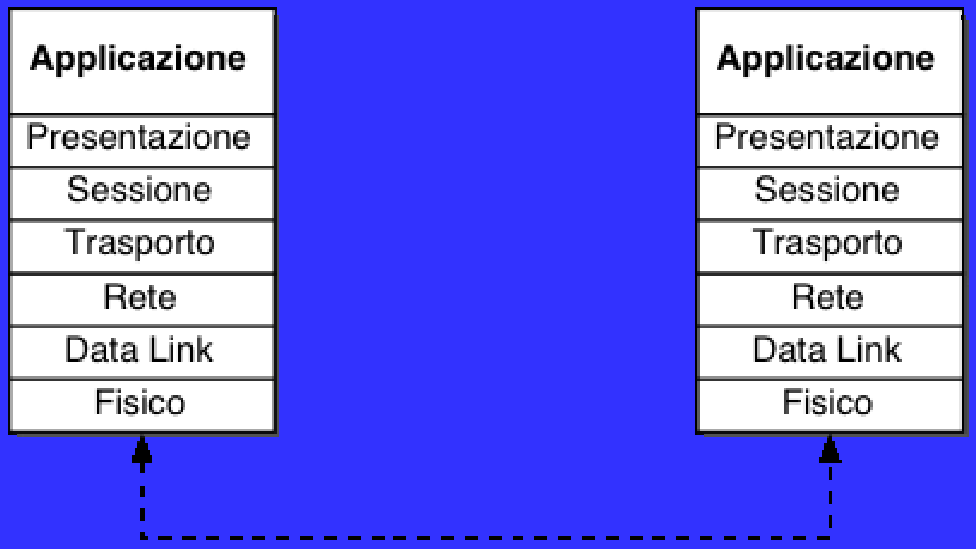
- Applicazione -> vuole inviare DATI
- Presentazione -> trasduce il FORMATO
- Sessione -> mantiene i contatti
- Trasporto -> multiplexing connessione
- Rete -> trasporto oltre la rete locale
- Data Link -> trasporto in rete locale
- Fisico -> trasporto punto punto

La Sapienza
Università degli Studi di Roma

Concetti di funzionamento delle reti

La pila ISO–OSI

Collegamento application to application



Concetti di funzionamento delle reti
La pila ISO–OSI

Livello fisico

E' necessario il livello FISICO ed una codifica dei segnali (es. Term. 3270, 5250)

- Seriale DB9 - 4 bit ricezione, 3 bit invio
- 8 bit di dati, N(essuna) parità, 1bit di stop - velocità 9600 bit/sec (baud)

Livello Data link

Condivisione di un mezzo:

- livello fisico (con gestione della concorrenza, es. CSMA-CD)
- livello data-link (identifica il dispositivo)

Vari standard:

Ethernet, Token Ring, FDDI, Frame Relay

Vari apparati:

Schede di rete, Repeater (Hub), Bridge, Switch

Concetti di funzionamento delle reti
La pila ISO–OSI

Livello Rete

Il pacchetto di livello 2 attraversa molte reti **locali** per andare da una rete di **partenza** ad una rete di **arrivo**

- Sono necessari apparati di Livello 3 (Router, Layer 3 Switch) che sono connessi fra di loro attraverso reti locali
- Utilizzano tabelle di INSTRADAMENTO (routing)
- Operano attraverso un PROCESSO di INOLTRO (forwarding)

Livello Trasporto

Multiplexing del livello rete

- Inserimento di un ulteriore valore di identificazione (porta) (es. 192.168.1.57:80)
- Non è necessario un livello di instramento ulteriore a quello di livello 3
- Modalità di trasporto connessa (TCP) e non connessa (UDP)
- E' possibile avere la conferma della ricezione dei pacchetti inviati

Concetti di funzionamento delle reti
La pila ISO–OSI

Livello Sessione

Evidenzia una **memoria** dello **stato** della sessione - (**NON IMPLEMENTATO**)

- Permette di ricreare l'ambiente nello stato precedente al guasto (es. Blocco trasferimento di un file in ftp)

Livello Presentazione

Gestisce le trasduzioni di formato (es. ASCII – EBCDIC) - (**NON IMPLEMENTATO**)

Livello Applicazione

Utilizza i dati che gli arrivano dal livello di presentazione per eseguire compiti stabiliti

Allo stato attuale l'applicazione si occupa di tutti i compiti dei livelli 5 e 6

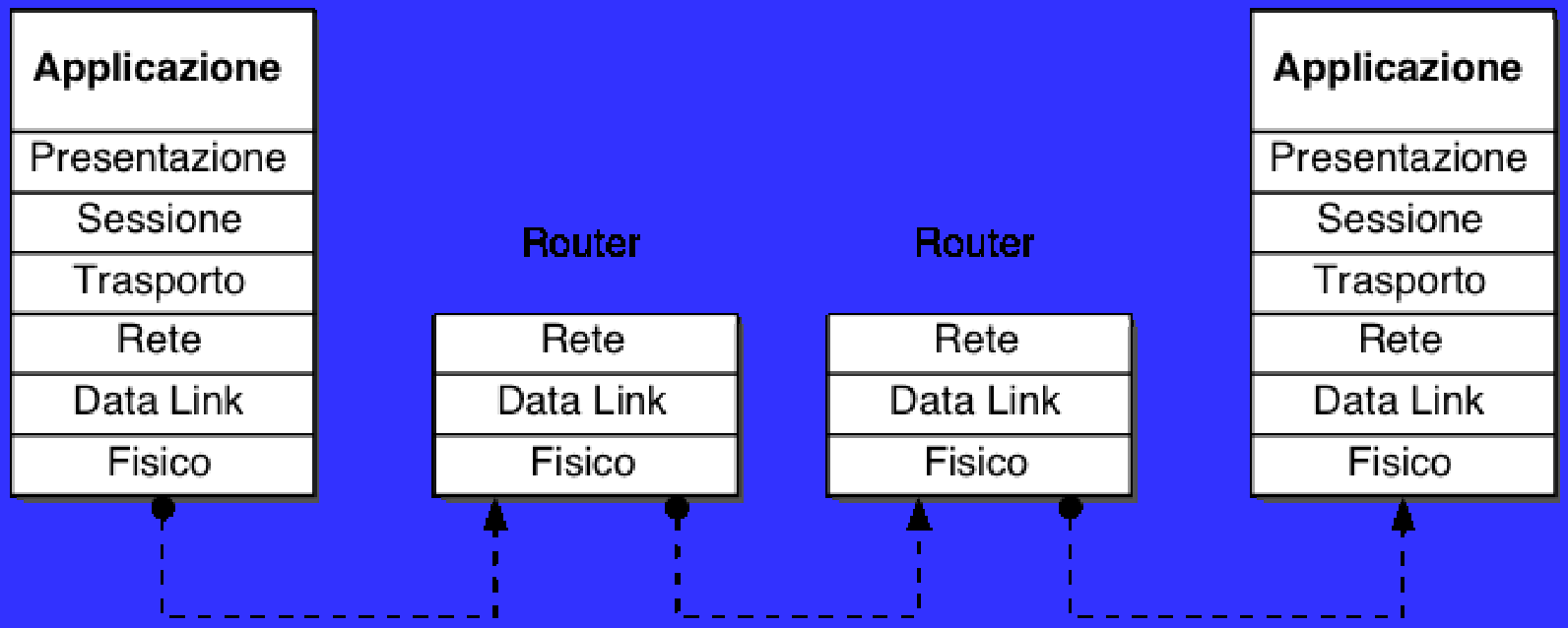
–Gestisce le sessioni (es. transazioni)

–Gestisce la TRASDUZIONE DI FORMATO

Concetti di funzionamento delle reti

La pila ISO–OSI

Esempio di scambio tra applicazioni su rete



Protocolli di livello 2

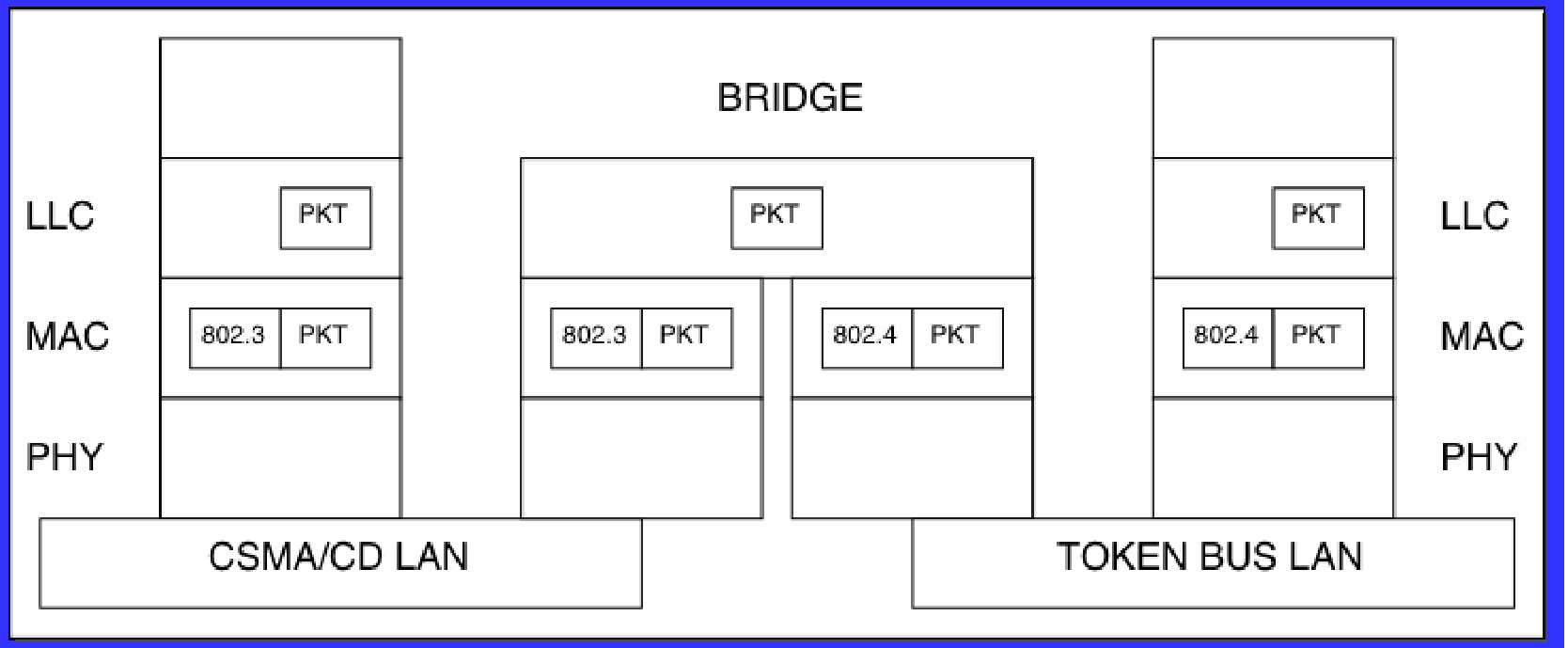
Il livello DATA-LINK (ethernet)

- E' in realtà diviso in due sotto-livelli
  - LLC = Logical Link Control
    - equalizza le differenze fra 802.x
    - è interfaccia verso il livello di rete
  - MAC = Medium Access Control
    - è interfaccia verso lo standard trasmissivo sottostante (CSMA/CD, Token BUS)

Concetti di funzionamento delle reti

Protocolli di livello 2

Esempio: Bridge



Concetti di funzionamento delle reti

Protocolli di livello 2

I campi Data-Link

- **Destination MAC** -> l'indirizzo del NIC di destinazione
  - 6 bytes di 1 hanno il significato di broadcast
- **Source MAC** -> l'indirizzo del NIC di spedizione
  - primi 3 bytes assegnati al costruttore
- **Length** -> lunghezza dei DATI nella frame
  - min 43 bytes, max 1497
- **FRAME** max size 1518 bytes, min size 64 bytes

La Sapienza
Università degli Studi di Roma

Concetti di funzionamento delle reti

Protocolli di livello 2

Il livello 2 gestisce il trasporto di un pacchetto da un capo all'altro di un filo

Protocolli di livello 3

La Internet Protocol SUITE

- IP Suite, da non confondere con l'IP Address
- Non ha particolari specifiche per il Livello 2
- Prevede il protocollo IP per il livello 3
  - Utilizza protocolli di ROUTING (es. BGP4)
  - Utilizza protocolli di DIAGNOSI (es. ICMP)
- Prevede i protocolli TCP e UDP per il livello 4
- Prevede il protocollo XDR per il livello 6

Concetti di funzionamento delle reti

Protocolli di livello 3

ISO/OSI e IPSuite

Application	FTP, Telnet, SMTP, SNMP / NFS
Presentation	XDR
Session	RPC
Transport	TCP - UDP
Network	IP / ICMP
Data-Link	ARP - RARP

Concetti di funzionamento delle reti

Protocolli di livello 3

Template di formato dei pacchetti

- Indirizzo di Destinazione
- Indirizzo Sorgente
- PayLoad
- Campi di controllo
- Campi di Riempimento

Byte	7	1	6	6	2	1500	46	4
	Preambolo	Start OF Frame	Indirizzo DESTINATARIO	Indirizzo MITTENTE	Lungh. DATI	DATI (payload)	PAD	CHK SUM

Concetti di funzionamento delle reti

Protocolli di livello 3

Il livello di RETE (IP Suite)

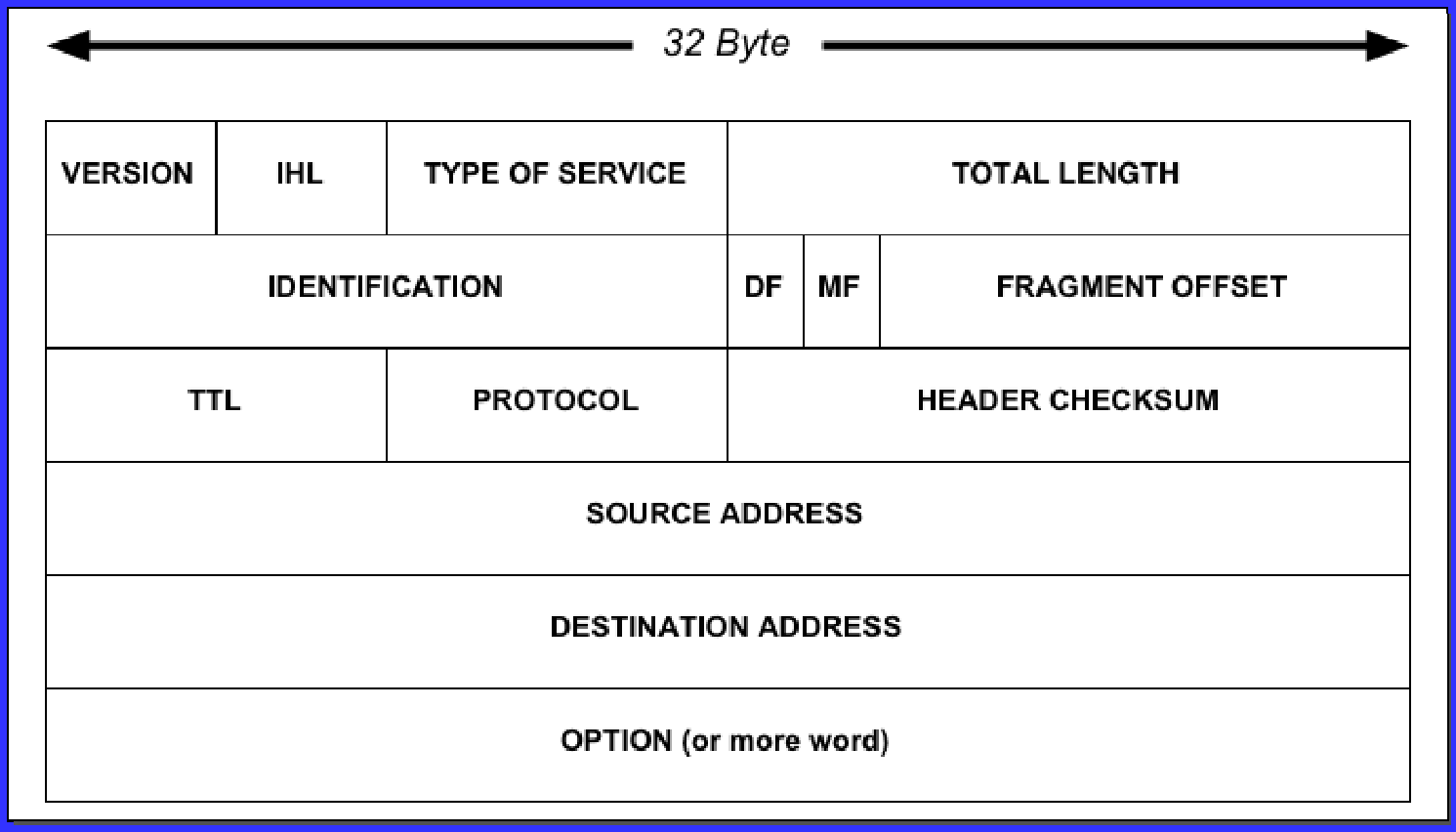
- Nella IP suite è implementato attraverso **IP**
- Trasferisce pacchetti da un **SORGENTE** ad una **DESTINAZIONE** attraversando più reti locali
- Deve conoscere la **TOPOLOGIA di RETE**
- Si deve occupare del **ROUTING**

La Sapienza
Università degli Studi di Roma

Concetti di funzionamento delle reti

Protocolli di livello 3

Com'è fatto un pacchetto IP



Concetti di funzionamento delle reti

Protocolli di livello 3

Uno sguardo ai campi (RFC791)

- Version -> versione del protocollo 4 o 6
- Lenght -> lunghezza dell'intestazione
- ToS -> Precedence, Delay, Throughput, Reliability
- Packet Lenght -> Lunghezza totale
- Campi per la frammentazione
  - Indentification -> id del datagramma originale
  - DF -> flag di non frammentazione
  - MF -> flag di presenza altri frammenti
  - Fragment Offset -> byte dall'inizio del pacchetto
    - tra 0 e 1499
- TTL -> quanti 'hop' prima di essere scartato
- Protocol -> protocollo del payload (ICMP = 1, TCP = 6)
- Header CheckSum -> CheckSum dell'header
- IP Add. Source e IP Dest. Source -> 32 bit
- Option -> 8 bit x 3 campi opzione
- Padding -> riempimento per arrotondamenti

La Sapienza Università degli Studi di Roma

Concetti di funzionamento delle reti

Protocolli di livello 3

L'indirizzamento IP

- Esistono 5 CLASSI DI INDIRIZZAMENTO
  - Classe A = da 1.0.0.0. a 127.255.255.255
  - Classe B = da 128.0.0.0 a 191.255.255.255
  - Classe C = da 192.0.0.0 a 223.255.255.255
  - Classe D = da 224.0.0.0 a 239.255.255.255
  - Classe E = 240.0.0.0 a 247.255.255.255

La Sapienza Università degli Studi di Roma

L'instradamento

- Due diversi algoritmi
  - Distance Vector
    - più vecchio
    - conservativo rispetto alle informazioni
  - Link state packet
    - basato sull'algoritmo di Dijkstra

Concetti di funzionamento delle reti

Protocolli di livello 3

Distance Vector

- Si basa sulla comunicazione della raggiungibilità di una rete fra router adiacenti con metrica di 'salto' (HOP)
- Hanno il problema del COUNT TO INFINITY
- Tendono velocemente alla stabilità, ma lentamente al ri-equilibrio
- es: *RIP*

Link State Packet

- Basati sull'algoritmo di Dijkstra per l'attraversamento di un grafo
- il messaggio di routing contiene tutti i router attraversati
- raggiungono più lentamente la stabilità, ma convergono più rapidamente dopo una variazione
- es: BGP, OSPF

La Sapienza Università degli Studi di Roma

Protocolli di livello 4

Il livello di TRASPORTO (IP Suite)

- La IP suite ha 2 protocolli per il livello di trasporto
  - **TCP** -> Trasmission Control Prot.
    - garantisce la connessione
  - **UDP** -> User Datagram Protocol
    - non garantisce la connessione
    - utilizzato per le trasmissioni MULTICAST

Concetti di funzionamento delle reti

Protocolli di livello 4

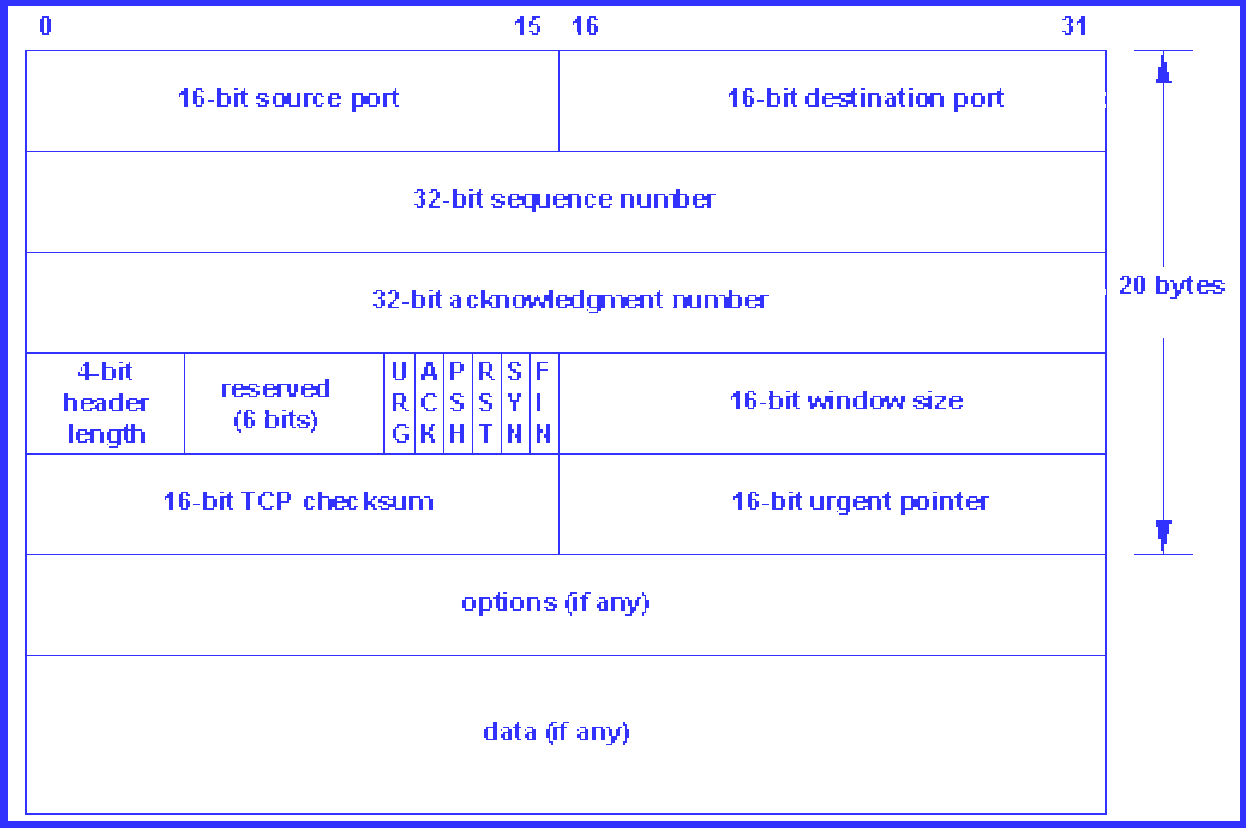
Il concetto di PORTA

- Dopo aver 'deciso' i soggetti della trasmissione (host) si deve decidere a quale 'applicazione' recapitare i dati
- Le porte forniscono il punto terminale delle applicazioni su un host
  - numerate da 0 a 65.535
    - da 0 a 1023 sono porte well-known
    - da 1024 a 65.535 sono porte generiche

Concetti di funzionamento delle reti

Protocolli di livello 4

Un pacchetto TCP



Concetti di funzionamento delle reti

Protocolli di livello 4

I campi del TCP

- Source port & Destination Port
- Sequence Number -> per il riassemblaggio (3WHS)
- Acknowledgment Num -> prossimo numero di sequenza atteso
- Data Offset -> dove iniziano i dati (distanza in dword)
- Flag del QOS
  - URG -> pacchetto con alta priorità
  - ACK -> pacchetto di conferma
  - PSH -> non si attende il Trans. Buffer Full
  - RST -> ristabilire la connessione (reset)
  - SYN -> sincronizzazione dei numeri di seq
  - FIN -> il mittente non ha dati da spedire
- Window -> ottetti di dati accettati (mittente)
- CheckSum -> controllo dell'integrità (verso IP)
- Urgent Pointer -> offset dei dati urgenti
- Options -> NOP e Max Segment Size
- Padding -> tutti 0 a riempimento
- Data

Concetti di funzionamento delle reti

Protocolli di livello 4

Stabilire una connessione TCP

- Attraverso il 3 Way HandShake
  - SYN SEQ=100 (client)
  - ACK 101, SYN SEQ=223 (server)
  - ACK 224 (client)
- Connessione stabilita
- FLUSSO (client server), WIN = 30, ...

Terminare una connessione TCP

- Una sessione di chiusura
  - FIN SEQ = 125 (client non ha più dati da inviare)
  - ACK 126 (il server vuole ricevere il 126)
  - FIN SEQ=300,ACK = 126 (il server vuole chiudere)
  - ACK 301 (il client chiude la connessione)

La Sapienza Università degli Studi di Roma

Concetti di funzionamento delle reti

Protocolli di livello 4

Stati di una connessione TCP

- **LISTEN** -> attesa di connessione
- **SYN-SENT** -> attesa di una richiesta di ritorno
- **SYN-RECV** -> attesa conferma connessione
- **ESTABLISHED** -> stato del trasferimento dati
- **FIN-WAIT1** -> ho inviato un FIN
- **FIN-WAIT2** -> sto aspettando un FIN
- **CLOSE-WAIT** -> aspetto la chiusura dell'APP
- **CLOSING** -> sto aspettando la conferma dopo un FIN
- **LAST-ACK** -> sto aspettando conferma dopo un ACK
- **TIME-WAIT** -> attesa di tempo dopo la conferma della chiusura
- **CLOSED** -> non esiste alcuna connessione

La Sapienza
Università degli Studi di Roma

Concetti di funzionamento delle reti

Protocolli di livello 4

Un pacchetto UDP

Source Port (optional)	Destination Port
Length	CheckSum
DATA	

Alcune applicazioni che utilizzano UDP:

TFTP

SNMP

DNS

La Sapienza
Università degli Studi di Roma

Debolezze e vulnerabilità delle reti

Debolezze e vulnerabilità delle reti

Problematiche

- **Catturare ACCOUNT**
  - spoofing
  - sniffing
  - session hijacking
- **Bloccare il funzionamento di una rete (LAN / WAN)**
  - STP violation
  - arp/icmp storm
  - packet flooding
  - route injection
- **Causare malfunzionamenti nei server**
  - Denial of Service
  - System Hacking
  - Distributed Denial of Service

La Sapienza
Università degli Studi di Roma

Debolezze e vulnerabilità delle reti

Le debolezze del livello DATA-LINK

- Mac address spoofing
- Arp poisoning (Tempesta arp)
- Spanning Tree blocking
- Tempesta broadcast (denial of service)
- Sniffer

Le debolezze del livello RETE

- Icmp flooding
- IP Address Spoof
- Frammentazione IP
- Iniezione di rotte
  - Black Hole
  - Route Flapping

Le debolezze del livello TRASPORTO

- 3-Way Handshake Violation
- Port Scan
- Sequence Number prediction
- Session Hijacking

Debolezze e vulnerabilità delle reti

Le debolezze del livello DATA-LINK

Le azioni da effettuare sulla LAN

- **Spoofing** -> utilizzare indirizzi di altri
- **Poisoning** -> riempire la rete di pacchetti di discovery
- **Sniffing** -> tracciare il traffico altrui
- **Scanning** -> vedere quali sono i punti di attacco
- **Hijacking** -> dirottare le sessioni TCP e il traffico UDP

La Sapienza Università degli Studi di Roma

Debolezze e vulnerabilità delle reti

Le debolezze del livello DATA-LINK

- La LAN è sede di:
  - protocolli per la variazione di topologia
  - protocolli broadcast
    - assegnazione di indirizzi
    - condivisione di risorse
  - traffico unicast che arriva/parte verso altre LAN

- Utenti che utilizzano protocolli di autenticazione in chiaro
- Protocolli di variazione automatica della topologia
- Promisquità fra sistemi client e server
- Assenza di VLAN

La Sapienza Università degli Studi di Roma

Debolezze e vulnerabilità delle reti

Le debolezze del livello DATA-LINK

Funzionamento di uno SWITCH

- Ha una tabella che associa il MAC ADDRESS dei computer connessi alla porta alla quale sono connessi
- Esiste una fase **LEARNING**
  - periodica
- Esiste una fase di **FORWARDING**
- Appena acceso:
  - Stare in ascolto ed inoltrare a tutte le porte meno che a quella di arrivo
  - Associare MAC ADDRESS a porte
  - Inoltrare solo alla porta porta associata
- Cambio di topologia (nuovo MAC connesso)
  - Ripetere il LEARNING

Capacità di memoria

Limitata e quindi se lo bombardiamo con mac address numerosi, per mantenere il servizio attivo diventa un ‘HUB-repeater’

La Sapienza
Università degli Studi di Roma

Debolezze e vulnerabilità delle reti

Le debolezze del livello DATA-LINK

ARP Poisoning

- Protocollo ARP: Address Resolution Protocol
  - permette di associare dinamicamente IP Address con Mac Address
  - Esistono delle ARP-Request
    - who-has 192.168.200.254 tell 192.168.200.35
  - alle quali fanno seguito delle ARP-Reply
    - 192.168.200.254 is-at 0:c0:49:27:7b:50

ARP Poisoning

- Si basa sull'utilizzo della cache ARP
  - aggiornata ogni 4-5 secondi
- Si basa sull'invio gratuito di ARP-Reply
  - ARP non è un protocollo con connessione
- Non basta da solo a superare problemi di isolamento
  - Va utilizzato insieme ad un processo di forwarding che emuli il comportamento di un gateway

Debolezze e vulnerabilità delle reti

Le debolezze del livello DATA-LINK

Sniffer

- Utilizziamo uno sniffer su una macchina senza IP Address
- Non utilizziamo la risoluzione dei nomi
- Collezioniamo gli indirizzi IP
  - ci serve per capire la classe IP
  - le richieste periodiche ci indicheranno il gateway (arp) e la porta 53 il DNS

Debolezze e vulnerabilità delle reti

Le debolezze del livello DATA-LINK

Sniffer (come scovarlo)

- La scheda dello SNIFFER è abilitata al modo PROMISCUO
  - il NIC solleva oltre il livello data-link anche i pacchetti con mac address diverso dal suo
- Costruiamo un pacchetto con Ip-Sospetto e MAC che varia
  - se riceviamo risposta abbiamo scoperto lo sniffer

- Lo sniffer potrebbe aver attivo il filtro per le richieste ICMP (tipo echo request)
- Facciamo delle **richieste TCP** (SYN e RST)
- Utilizziamo delle procedure che creano errori ICMP (errori nell'IP header)

La Sapienza Università degli Studi di Roma

Sniffer (come scovarlo)

- Possiamo utilizzare un ARP request unicast
  - ARP gratuite unicast + ping broadcast
    - ARP e PING con due MAC Addr dfferenti
    - chi risponde senza ARP ha sniffato

Sniffer (come scovarlo)

- Uso del Reverse DNS LookUP da parte dello sniffer
  - si chiede al DNS che nome corrisponde all'IP proposto (record PTR)
  - gli sniffer fanno spesso uso di questa query
  - per scovarli basta fare dei ping circolari (tutte le macchine della LAN) verso IP che non esistono (il pacchetto avrà come mittent eun indirizzo inesistente e destinatario quello dello sniffer da scovare)

Debolezze e vulnerabilità delle reti

Le debolezze del livello DATA-LINK

Sniffer (come scovarlo)

- Metodo del SOURCE-ROUTE (IP)
- configurazione di informazioni source-route all'interno del header dell' IP
- rotta loose-source all'interno del PING
  - gli host non hanno il routing attivo
  - se arriva una risposta con TTL = TTL partenza abbiamo beccato lo sniffer

La Sapienza Università degli Studi di Roma

Debolezze e vulnerabilità delle reti

Le debolezze del livello Rete

Attacchi dal livello Rete per LAN

- Basati sui protocolli Broadcast IP e ICMP
  - ICMP smurf (DOS)
  - IP spoofing

La Sapienza Università degli Studi di Roma

Debolezze e vulnerabilità delle reti

Le debolezze del livello Rete

Il protocollo ICMP

- ICMP -> protocollo incapsulato nel livello 3 per la verifica di malfunzionamenti
  - ping -> echo request--echo reply
  - traceroute -> TTL exceeded
- Messaggi ICMP non possono generare altri messaggi di errore ICMP
  - errori -> port unreachable, service unreachable, host redirection

La Sapienza Università degli Studi di Roma

Debolezze e vulnerabilità delle reti

Le debolezze del livello Rete

Il pacchetto ICMP

Type	Code	CheckSum
Identifier		Seq.Number
DATA (ICMP payload)		

- Type -> Tipo di messaggio
- Code-> Sub-Tipo di messaggio
- Id. + Seq.-> Usati nell'Echo reply (Type 0)

Debolezze e vulnerabilità delle reti

Le debolezze del livello Trasporto

Attacchi dal livello Trasporto per LAN

- Port Scanning
- Session Hijacking

La Sapienza
Università degli Studi di Roma

Debolezze e vulnerabilità delle reti

Le debolezze del livello Trasporto

Il port scanning

- E' possibile sfruttare il 3W-HS per avere informazioni sui servizi offerti dalla vittima
- E' possibile utilizzare i messaggi ICMP
- E' possibile utilizzare la frammentazione IP
- E' possibile sfruttare l'IP spoofing per proteggere la nostra identità

La Sapienza
Università degli Studi di Roma

Debolezze e vulnerabilità delle reti

Le debolezze del livello Trasporto

Come funziona un Port Scanner (1)

- TCP connect() -> provo ad aprire una connessione
  - Questa modalità viene loggata
- TCP SYN -> mando un SYN ed aspetto di ricevere
  - SYN / ACK -> il server dietro la porta è in ascolto
  - RST -> la porta è chiusa
  - Questa modalità non viene loggata da tanti server
- TCP FIN -> mando un FIN ed aspetto un RST
  - se c'è un demone non risponde
  - i firewall di solito non bloccano i FIN
  - le macchine di solito non loggano i FIN
- XMAS -> FIN URG PSH attivi
- Problema: qualche macchina WIN non risponde con il RST -> discriminazione fra Win e *NIX

La Sapienza Università degli Studi di Roma

Debolezze e vulnerabilità delle reti

Le debolezze del livello Trasporto

Come funziona un Port Scanner (2)

- IP Fragmentation -> si frammenta il pacchetto TCP in tanti piccoli pacchetti IP
  - Anche l'header TCP viene frammentato in modo da evitare i Packet Filter
  - Attenzione che alcuni sniffer vanno in core dump con pacchetti + piccoli di 36 bytes
- TCP Reverse ident -> il demone ident manda risposte ad un a connessione anche se non è stato lui ad intraprenderla
- UDP -> si manda un pacchetto UDP di 0 bytes e si aspetta:
  - ICMP port unreachable se la porta è chiusa
- IP Protocol -> si mandano dei pacchetti IP raw senza indicazione del protocollo che si vuole utilizzare
  - se arriva un ICMP protocol unreachable il protocollo non è disponibile

La Sapienza Università degli Studi di Roma

Debolezze e vulnerabilità delle reti

Le debolezze del livello Trasporto

Contromisure al Port Scanning

- Limitare il numero di messaggi ICMP
- Ritardare il RST e l'ACK per le connessioni
- Non accettare pacchetti XMAS
- Monitorare la rete (Network Intrusion Detection System)

Debolezze e vulnerabilità delle reti

Le debolezze del livello Trasporto

Session Hijacking

- Quando un utente stabilisce una connessione TCP si sincronizza con la sua controparte grazie ai numeri di sequenza
- Un pacchetto con un numero di sequenza valido e un IP valido è un pacchetto della sessione TCP a tutti gli effetti (SPOOF)
- L'utilizzo dell'ARP poisoning è un aiuto
- L'utilizzo del blocco del server e del client sono necessari

Le debolezze delle WAN

- Concentrazione del traffico in uscita/ingresso
- Accessibilità dei servizi dall'esterno
- Tunneling dei servizi dall'interno
- Protocolli di Routing non autenticati

Debolezze e vulnerabilità delle reti

Le debolezze delle WAN

Le ‘azioni’ sulle WAN

- **Footprinting** -> collezionare info generiche
- **Enumeration/Scanning** -> collezionare info specifiche
- **Exploit** -> ottenere accessi su macchine interne
- **DOS e DDOS di servizi remoti** -> impedire l’accesso ai servizi offerti
- **Route Injection** -> creare zone irragiungibili dall’esterno

La Sapienza
Università degli Studi di Roma

Footprinting

- L'arte di collezionare informazioni sulla rete in cui si trova la 'vittima'
  - Open Source FP
    - WHOis DB
    - DNS
    - Sito web
  - Passo successivo è l'enumerazione

Debolezze e vulnerabilità delle reti

Le debolezze delle WAN

Trovare l'intervallo di indirizzi

- Si fanno delle prove di discovery iniziando dalle informazioni che si sono dedotte
  - nameserver
  - webserver
  - altri

Utilizzo dei traceroute server

- Servono per capire da quante parti la WAN è acccessibile al mondo esterno
- Ci danno una visione a 360 gradi di servizi replicati (content management)
- www.traceroute.org

La Sapienza Università degli Studi di Roma

Debolezze e vulnerabilità delle reti

Le debolezze delle WAN

Enumerazione

- Dobbiamo capire quali servizi ci offre la rete vista dall'esterno per poter, nella successiva fase, tentare exploit che ci diano accesso alle macchine interne
- Utilizziamo le informazioni generiche raccolte per acquisirne di maggiormente specifiche

Debolezze e vulnerabilità delle reti

Le debolezze delle WAN

Primo passo: ICMP

- Enumeriamo facendo scanning delle macchine trovate attraverso UDP
  - il messaggio ICMP PORT Unreachable ci aiuta
- Uso nmap con -sU (UDP protocol)
  - se mi dice filtered c'è un firewall
  - con traceroute posso sapere qual è l'indirizzo del firewall (l'ultimo prima della vittima)

La Sapienza
Università degli Studi di Roma

Debolezze e vulnerabilità delle reti

Le debolezze delle WAN

Passo 2: SO fingerprint

- Devo capire il tipo di sistema operativo per catalogarlo
  - ogni versione avrà degli exploit
- Ho a disposizione il comando nmap
  - nmap -O -v identifica il tipo di SO
    - attenzione genera SYN Stealth
  - nmap -p80,2333 -O -v (una chiusa e una aperta)

Debolezze e vulnerabilità delle reti

Le debolezze delle WAN

Passo 3: tentare l'accesso

- Tento l'accesso attraverso il protocollo telnet ai vari servizi offerti
  - telnet IP-vittima porta
- Esistono protocolli 'chiacchieroni' che mi dicono la loro versione
  - metto le informazioni da parte per l'hacking

La Sapienza Università degli Studi di Roma

La Sapienza
Università degli Studi di Roma

FINE