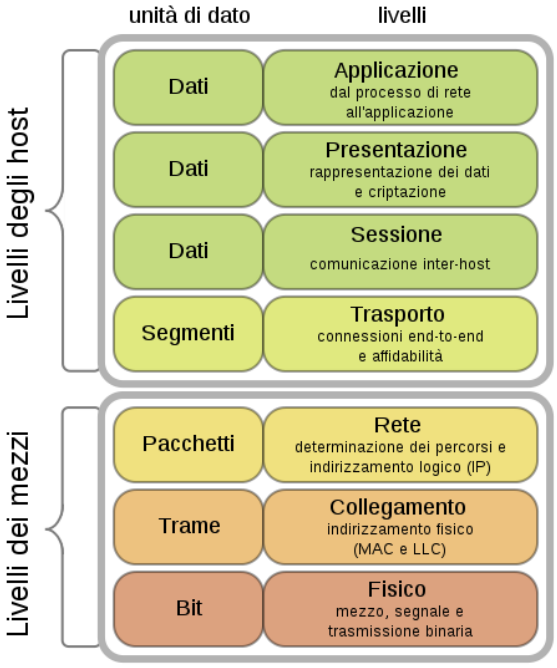
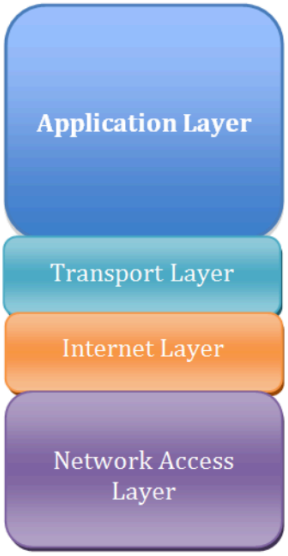
Domande teoriche e spunti di riflessione

1.1.1 Livelli della pila protocollare ISO/OSI



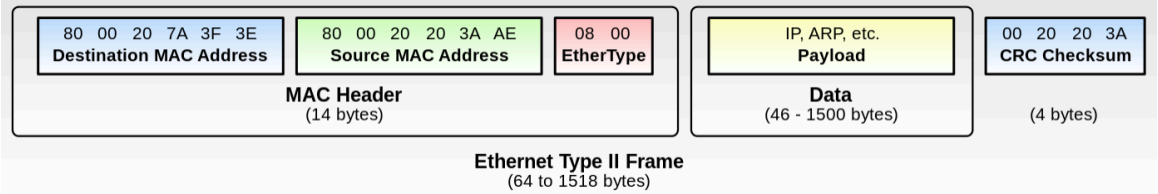
TCP/IP

1.1.2 Livelli della pila protocollare TCP/IP



1.1.3 Informazioni contenute nell'intestazione del frame Ethernet

Un frame Ethernet è l'unità dati trasportata al livello 2 del modello di riferimento ISO/OSI. Il formato più comune è il seguente:



1.1.4 Indirizzamento in internet

Quando un pc vuole comunicare al di fuori della sua rete locale, serve creare una corrispondenza tra indirizzo IP e MAC address. Viene gestita tramite il protocollo ARP, che permette di conoscere il MAC address di un computer dato il suo indirizzo IP tramite un'interrogazione distribuita.

1.2.1 Dispositivi di rete

- Hub: dispositivo di livello fisico che replica il segnale entrante in una porta su ogni altra porta.
- Switch: dispositivo di livello 2 che inoltra una trama Ethernet entrante esclusivamente sulle porte dove è possibile che il destinatario sia in ascolto
- Router: si occupa a livello 3 di istradare e inoltrare i pacchetti
- Firewall: componente a livello 3,4,5 che permette il filtraggio dei pacchetti entranti in una rete.

1.2.2 Dominio di collisione e dominio di broadcast

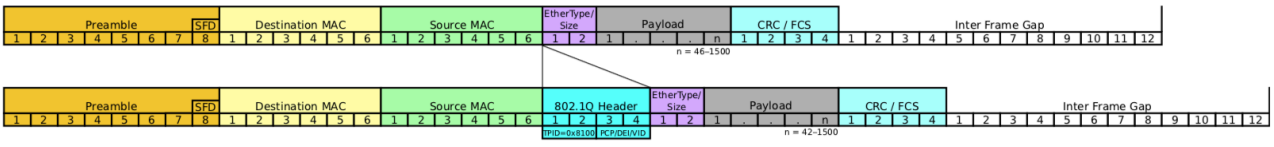
Più host collegati da un hub appartengono allo stesso dominio di collisione. Se infatti tentassero di trasmettere contemporaneamente si creerebbero collisioni e il decadimento delle prestazioni di una rete.
Un dominio di broadcast è l'insieme delle macchine appartenenti ad una sottorete. Ogni router "spezza" i domini di broadcast.

1.3.1 Vantaggi delle VLAN

– risparmio economico di acquisto e gestione
– riduzione del traffico di broadcasting
– possibilità di gestire con maggior granularità gli aspetti legati alla sicurezza

1.3.2 Utilizzo dei dispositivi di rete liv. 1,2 all'interno di una LAN suddivisa in VLAN

Per identificare i pacchetti che transitano tra più VLAN è necessario introdurre un campo *tag* che identifichi la VLAN di appartenenza.



1.3.3 Distinzione tra modalità "access" e modalità "trunk"

Access link — le due porte appartenenti alla connessione sono associate a una VLAN specifica (si dice che sono configurate in modalità access). Tutti i pacchetti che transitano per quella linea sono implicitamente appartenenti alla stessa VLAN.
Trunk link — E` il caso più interessante: lo stesso link porta trame appartenenti a varie VLAN.

1.3.4 Incapsulamento 802.1Q

IEEE 802.1Q è uno standard che permette a più reti virtuali VLAN di condividere lo stesso collegamento fisico senza perdita di informazioni tra un apparato e un altro.

802.1Q aggiunge 4 byte all'header:
- I primi 2 servono per identificare il nuovo formato del frame
- Gli ultimi 2 riguardano il tag control information TCI (detto anche VLAN Tag). Possono esserci fino a 4096 VLAN diverse

2.1.1 Protocollo IP e ICMP

Il protocollo IP è nato per interconnettere reti eterogenee per tecnologia, prestazioni, gestione, è implementato sopra altri protocolli di livello collegamento, come Ethernet. Non garantisce cioè alcuna forma di affidabilità della comunicazione in termini di controllo di errore, controllo di flusso e controllo di congestione.

l'Internet Control Message Protocol (ICMP) è un protocollo di servizio che si occupa di trasmettere informazioni riguardanti malfunzionamenti e informazioni di controllo tra reti di calcolatori.

2.1.2 Protocollo ARP

L'Address Resolution Protocol (ARP) è un protocollo di rete appartenente al protocollo internet (IP) versione 4 operante a livello di accesso alla rete, il cui compito è fornire la "mappatura" tra l'indirizzo IP (32 bit - 4 byte) e l'indirizzo MAC (48 bit - 6 byte) corrispondente di un terminale in una rete locale ethernet.

2.1.3 Rete di classe A, B, C. Maschere di rete. Notazione CIDR

Classe A
- Il primo byte rappresenta la rete; gli altri tre gli host per ogni rete.
- In notazione decimale gli IP variano nel modo seguente: 0-127.H.H.H;
- La maschera di rete è 255.0.0.0 (o anche detta /8 in quanto i bit di rete sono 8);
- Questi indirizzi in binario iniziano con il bit 0.

Classe B
- I primi due byte rappresentano la rete; gli altri due gli host per ogni rete.
- In notazione decimale gli IP variano nel modo seguente: 128-191.N.H.H;
- N varia da 0 a 255.
- La maschera di rete è 255.255.0.0 (anche detta /16 in quanto i bit di rete sono 16);
- Questi indirizzi in binario iniziano con i bit 10.

Classe C
- I primi tre byte rappresentano la rete; l'ultimo gli host per ogni rete.
- In notazione decimale gli IP variano nel modo seguente: 192-223.N.N.H;
- La maschera di rete è 255.255.255.0 (anche detta /24 perché i bit di rete sono 24);
- Questi indirizzi in binario iniziano con i bit 110.

La maschera di rete (subnet mask) metodologia utilizzata per definire il range di appartenenza di un host all'interno di una sottorete IP.

La notazione CIDR serve per esprimere indirizzi ed è la seguente: *a.b.c.d./x*, dove *x* è la subnet mask, il numero di bit (contati partendo dal più significativo a sinistra) che compongono la parte di indirizzo della rete.

Esempio: la subnet mask di una rete /24 è la seguente

```
24            ->  11111111.11111111.11111111.00000000
255.255.255.0 ->  11111111.11111111.11111111.00000000
```

2.1.4 Indirizzo di broadcast

L'indirizzo di broadcast è un indirizzo IP che consente l'invio delle informazioni a tutti gli host sulla stessa sottorete invece che ad un singolo destinatario.
Si ricava calcolando l'OR logico bit a bit tra l'indirizzo e la maschera di rete invertita.

Esempio:	Indirizzo:	192.168.1.1
	Maschera:	255.255.255.0 (dunque /24)
Si ha:	192.168.1.1	= 11000000 . 10101000 . 00000001 . 00000001
	255.255.255.0	= 11111111 . 11111111 . 11111111 . 00000000
	Dunque l'indirizzo di broadcast è 192.168.1.255	

2.1.5 IP privati

Sono una classe di indirizzi IP riservati alle reti locali, al fino di ridurre gli indirizzi pubblici.

Indirizzo iniziale	Indirizzo finale	Classi	Blocco CIDR più grande	Numero di indirizzi disponibili
10.0.0.0	10.255.255.255	Singola classe A	10.0.0.0/8 (255.0.0.0)	16.777.216
172.16.0.0	172.31.255.255	16 classi B contigue	172.16.0.0/12 (255.240.0.0)	1.048.576
192.168.0.0	192.168.255.255	256 classi C contigue	192.168.0.0/16 (255.255.0.0)	65.536

2.2.1 Più piccola sottorete che contiene un intervallo di indirizzi

Si procede dividendo a metà il range di indirizzi dalla rete a disposizione finché è sufficiente per non sprecare indirizzi.

2.2.2 In quali casi posso aggregare più sottoreti in un unica riga di una tabella di routing

Quando il nodo successivo per raggiungere le varie sottoreti è lo stesso router per tutte le sottoreti

2.2.3 Stesso IP nella rete, in quali casi funziona e in quali no

Se si trova nella stessa sottorete non funziona, se c'è un traduttore di IP tra una settorete e l'altra può funzionare

2.3.1 Interfaccia virtuale di un router

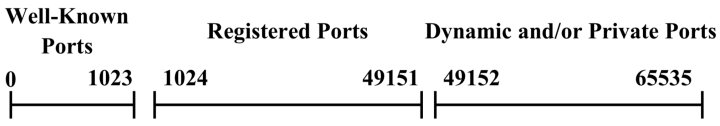
E' un'interfaccia fisica del router assegnata alla quale è assegnato un range IP e collegata ad uno o più switch per le sottoreti

2.3.2 Informazioni necessarie ad uno switch livello 3

A quali porte è collegata ogni VLAN. "in quali porte sono le vlan"

3.1.1 Perché gli indirizzi di livello 4 si chiamano "porte"? A cosa sono normalmente associati?

Una porta è assegnata ad un processo su una macchina. Le porte son divise in 3 range



3.1.2 Numeri di sequenza TCP

I numeri di sequenza servono a identificare e posizionare in maniera ordinata il carico utile del segmento TCP all'interno del flusso di dati, affinché i pacchetti possano essere riordinati una volta giunti a destinazione

3.1.3 Quando è conveniente usare UPD al posto di TCP?

Quando non c'è la necessità di una connessione veloce e non c'è la necessità che ogni pacchetto arrivi. (Es: chiamata vocale)

3.2.1 Perché gli indirizzi IP privati sono così diffusi?

Perché permettono di formare un sacco di reti private con un sacco di host.

3.2.2 Informazioni aggiuntive richieste per operare in Port Forwarding

Le porte già in uso dal router (interne ed esterne)

3.2.3 Quale informazioni deve conservare un router per gestire una connessione TCP in modalità NAT?

La connessione TCP è caratterizzata da una coppia di porte

3.2.4 Su quali campi delle intestazioni TCP/IP agisce un router NAT?

Sugli indirizzi sorgente/destinazione di sicuro

4.1.1 Protocolli DNS, RIP, DHCP, HTTP

DNS: sistema utilizzato per la risoluzione di nomi dei nodi (host) della rete in indirizzi IP.
RIP: protocollo di routing a distance vector. Tiene il conto del numero di nodi (max 15) da sorgente a destinazione evitando loop
DHCP: protocollo di configurazione IP dinamica che permette ai dispositivi di una certa rete locale di ricevere automaticamente ad ogni richiesta di accesso a una rete IP (quale una LAN) la configurazione IP necessaria per stabilire una connessione e operare su una rete.
HTTP: protocollo per il trasferimento di informazioni client-server sulla porta 80.

4.1.2 SQL, HTML

Lo so già

4.1.3 Stack e Heap di un'applicazione

In un programma le variabili stanno in una zona di memoria detta stack, mentre le zone di memoria allocate con malloc stanno in una diversa zona, detta heap.

4.2.1 Perchè lo scambio dei file di zona è sempre più raro nel protocollo DNS?

Perché un attaccante potrebbe richiederlo per capire la struttura (dominio e ip) delle macchine presenti in una rete.

4.2.2 Caratteristiche di una macchina zombie per un idle port scan

Sono macchine con poco traffico, usate per distribuire la fase di scanning ossia far scansionare qualche porta da ognuna di esse al fine di rendere meno sospetto lo scanning delle porte di una macchina vittima

4.2.3 Prevenzione attacco di buffer overflow

Standard di codifica rigidi, uso di linguaggi che negano la disabilitazione del controllo di limiti di un vettore oppure inserimento nello stack di valori di controllo che se compromessi indicano un possibile buffer overflow in corso.

4.2.4 Fattori che rendono ancora attuali gli attacchi di denial of service

L'utilizzo di molte macchine attraverso le quali inviare molte richieste SYN ad un server rendono efficace il DDoS e permettono di saturare le risorse disponibili di un server

4.3.1 Struttura di massima di un ACL

Protocollo	Sorgente	Destinazione	Flag	Azione	
TCP	0.0.0.0/0:*	12.34.56.71/32:80	*	PASS	Mondo → web server
TCP	12.34.56.71/32:80	0.0.0.0/0:*	ESTABLISHED	PASS	Web server → mondo
TCP	12.34.56.70/32:*	0.0.0.0/0:80	*	PASS	Proxy → mondo
TCP	0.0.0.0/0:80	12.34.56.70/32:*	ESTABLISHED	PASS	Mondo → proxy
*	*	*	*	DROP	Proibire tutto il resto

4.3.2 Perché usare un packet filtering firewall?

E' comodo e visibile per tenere d'occhio la lista (ACL) dei pacchetti che possono filtrare

4.3.3 Vantaggi e svantaggi Proxy applicativo

Vantaggi: può fare da intermediario tra mondo e web server al fine di proteggerlo, velocizza le risposte grazie al caching, identifica gli utenti
Svantaggi: può soccombere in condizioni di traffico elevato

4.4.2 Cos'è una DMZ?

Una demilitarized zone è una sottorete isolata che contiene dei servizi informatici accessibili sia da reti esterne (WAN) che da intranet e il cui scopo è quello di far usufruire questi servizi nella maniera più sicura possibile (tramite ACL)

4.4.3 In cosa consiste l'hardening?

Consiste nell'irrobustire i servizi offerti dai server, attraverso l'aggiunta di un personal firewall che lasci cadere tutti i pacchetti non direttamente correlabili a no dei servizi offerti. Sostanzialmente si chiudono tutte le porte non utilizzate e si limitano i servizi all'essenziale