

Scaletta classwork

Seminario reti veicolari

GUARDARE PDF

PROTOCOLLO IEEE 802.11 (WLAN)

Le WLAN operano sulle bande libere ISM (Industrial, Scientific and Medical), ovvero quelle attorno ai 2.4GHz e ai 5GHz. L'ERP, che e' un parametro che identifica la potenza emessa nella direzione massima, e' di 100mW, offrendo copertura tra gli 80 e i 100 metri.

Il protocollo 802.11 ha visto varie generazioni, alcune delle quali sono:

- 802.11: La prima versione dello standard IEEE 802.11 venne presentata nel 1997 e viene chiamata "802.11y", specifica la velocita' di trasmissione tra 1 e 2Mbps e utilizzava raggi infrarossi o le onde radio nella frequenza di 2.4GHz per la trasmissione del segnale
- 802.11b: ha visto la sua comparsa ufficiale nel 1999 e ha la capacita' di trasmettere al massimo 11Mbps e utilizza il CSMA con il Collision Advance (CMSA/CA) come metodo di trasmissione delle informazioni
- 802.11n (WiFi 4): e' stato annunciato nel gennaio 2007, la velocita' di rete di questo standard e' attorno ai 300Mbps. Questo standard, oltre ad essere estremamente piu' veloce rispetto agli standard precedenti, include anche la possibilita' di utilizzare la tecnologia MIMO (multiple-in multiple-out).
- 802.11ac (WiFi 5): approvato nel 2014, questo standard opera nell'intorno delle frequenze dei 5GHz. La velocita' massima teorica di questo standard all'interno di una WLAN multi-stazione e' di 1Gbit/s con una velocita' massima di un singolo collegamento di 500MBps.
- 802.11ax (WiFi 6): presentato nel maggio 2018, e' stato progettato per lavorare nella banda di frequenza tra 1 e 7 GHz. Durante il CES 2018 di Las Vegas sono stati mostrati dei test che hanno raggiunto velocita' massime di 11Gbps. Con una velocita' massima di un singolo collegamento di 1Gbps.
- 802.11be (WiFi 7): per il 2024 e' stato presentato il nuovo standard che dovrebbe avere una capacita' di 30bps con una frequenza tra i 2.4 e 5 GHz e forse anche 6GHz.

Le ultime versioni dello standard utilizzano antenne multiple per migliorare le prestazioni in presenza dei fenomeni aleatori nel mezzo radio.

Lo standard IEEE 802.11 prevede diverse modalita' di funzionamento.

- **Independent Basic Service Set (IBSS):** i terminali in copertura radio reciproca si indirizzano direttamente fra loro (peer-to-peer)
- **Basic Service Set (BSS):** un dispositivo hardware copre una certa area e serve da punto di accesso (Access Point) per l'intera rete. Ci sono due possibili modalità di funzionamento:
 - Distributed Coordination Function (DCF): tutte le comunicazioni passano per l'Access Point
 - Point Coordination Function (PCF): l'Access Point interrompe periodicamente la modalità DCF per interrogare i terminali a polling
- **Extended Service Set (ESS):** più BSS con Access Point collegati fra loro mediante cavo o radio

Il protocollo di accesso usato nel DCF é casuale CSMA. Siccome con mezzi radio il Collision Detect non é utilizzabile per via dell'aleatorietá nella potenza ricevuta, si usa la tecnica di Collision Avoidable (CSMA/CA): essa prevede una 4-way handshaking che risolve i problemi del terminale nascosto ed esposto:

- un trasmettitore fa carrier sensing per un tempo DIFS (Distributed Inter-Frame Service) prima di trasmettere
- poi informa i vicini e il destinatario che é in procinto di trasmettere con un pacchetto RTS (Request To Send)
- i trasmettitori che ricevono il RTS non trasmettono
- il ricevitore dopo un tempo SIFS (Short Inter-Frame Space) informa di essere pronto a ricevere con un pacchetto CTS (Clear To Send) e i suoi vicini che lo ricevono non trasmettono

Internetworking

L'internetworking si occupa dell'interconnessione di reti allo scopo di rendere disponibili a tutti gli utenti e le macchine interconnesse i servizi offerti dalla rete. Vengono utilizzati protocolli e strategie dell'Internet Engineering Task Force (IETF) descritti in documenti chiamati Request For Comment (RFC). I dispositivi hardware per far transitare i pacchetti tra le reti si differenziano tra di loro sulla base del livello sul quale operano e quindi sulla loro complessita' realizzativa.

- **repeater:** ripetitore a livello fisico
- **bridge:** ripetitore a livello di Data Link
- **router:** ripetitore a livello di Network
- **gateway:** ripetitori per livelli superiori a quello di Network

IP (Internet Protocol)

L'Internet Protocol é il protocollo di livello 3 alla base di Internet, la rete a pacchetto attualmente piú diffusa al mondo. IP é un protocollo di tipo datagram sviluppato inizialmente per creare una rete per

interconnettere postazioni della difesa americana e mantenere la connessione anche se una parte venisse distrutta, dando vita alla commutazione a pacchetto. Inoltre, IP é un protocollo a pacchetti senza connessione e di tipo best effort, cioè che non garantisce alcuna forma di affidabilità della comunicazione. In questo protocollo non c'è nessun tipo di controllo di errore, controllo di flusso e controllo di congestione: l'affidabilità può essere realizzata dai protocolli di trasporto del livello 4. Esistono due versioni del protocollo IP: l'originaria v4 e la più recente v6, quest'ultima nata dall'esigenza di gestire meglio il crescente numero di dispositivi connessi ad Internet. IP nasce prima del modello OSI e si occupa anche della frammentazione: riceve dal livello 4 dei pacchetti di 64KB e li frammenta in segmenti, che riassume in ricezione per formare i 64KB da restituire al livello 4. I pacchetti sono composti da un header e dai dati.

Indirizzi IPv4

Gli indirizzi IPv4 sono composti da 32 bit. Vengono tipicamente espressi utilizzando una notazione a punti (dot notation) che separano quattro campi di 8 bit ciascuno (e.g.: 192.168.1.6). Esistono 4 diversi schemi di indirizzamento (rete e stazione):

	Bit iniziali	Bit reti	Bit host	range indirizzi
Classe A	0	7	24	da 0.0.0.0 a 127.255.255.255
Classe B	10	14	16	da 128.0.0.0 a 191.255.255.255
Classe C	110	21	8	da 192.0.0.0 a 223.255.255.255
Classe D	1110	0	28	da 224.0.0.0 a 239.255.255.255
Usi futuri	11110			

Gli indirizzi pubblici sono rilasciati e regolamentati dall'ICANN (Internet Corporation for Assigned Names and Numbers) e da altri enti internazionali. Gli enti detentori di una classe possono suddividere ulteriormente la classe. Per ogni rete due indirizzi sono dedicati: uno per identificare la rete stessa e uno per il broadcast:

- XXX.YYY.ZZZ.0: rete
- XXX.YYY.ZZZ.255: broadcast

tutti gli altri sono indirizzi unicast. Nelle diverse classi alcuni indirizzi sono riservati per applicazioni intranet (e.g.: nella classe C sono 192.168.0.0 - 192.168.255.255) o per scopi intrahost (e.g.: nella classe A sono 127.0.0.0 - 127.255.255.255, con 127.0.0.1 detto localhost per ogni host anche privo di scheda di rete per scrivere applicazioni di rete utilizzando l'host stesso).

NETMASK

Se il destinatario é nella stessa rete (intranet) allora il pacchetto può essere messo sulla rete e il destinatario lo vedrà; altrimenti (internet) occorre inviare il pacchetto fuori affidandolo alla macchina che identifica l'accesso al mondo esterno, detta gateway. Gli indirizzi IP di sorgente e destinatario, però, non sono sufficienti per capire se il payload é destinato sulla stessa rete o all'esterno. Per fare ciò, si utilizza il NETMASK: esso permette di risolvere il problema di cosa é locale e cosa é remoto verificando se IP_DEST é dentro l'intervallo di indirizzi della rete locale. La rete di un indirizzo IP é l'AND logico fra l'indirizzo IP e la NETMASK.

Esempio

IP_DEST	195.32.62.2
NETMASK	255.255.255.0

IP_DEST AND NETMASK = 195.32.62.0: nella rete ci sono tutti gli indirizzi 195.32.62.X

DHCP

Ogni nodo deve essere configurato per poter operare in una qualsiasi rete. A questo scopo esiste il Dynamic Host Configuration Protocol (DHCP), un protocollo applicativo che permette a un nodo di apprendere autonomamente la configurazione della rete a cui si connette. Opera in questo modo:

1. l'host interessato invia una richiesta di configurazione in broadcast
2. se é presente un server DHCP nella rete, questo risponde all'host sorgente con la configurazione da adottare e il tempo di validita' della configurazione stessa

Scaduto il tempo di validita' della configurazione (lease time), in assenza di comunicazioni da parte dell'host, il server DHCP considera la macchina spenta.