ESAME DI STATO DI ISTRUZIONE SECONDARIA SUPERIORE

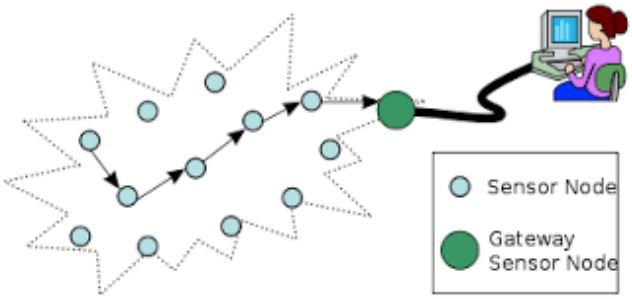
Indirizzo: ITTL - INFORMATICA E TELECOMUNICAZIONI
ARTICOLAZIONE TELECOMUNICAZIONI

Tema di: TELECOMUNICAZIONI e SISTEMI E RETI

Il candidato svolga la prima parte della prova e risponda a due dei quesiti tra quelli proposti.

PRIMA PARTE

Per monitorare la situazione in cui si trova un ghiacciaio in alta montagna, deve essere realizzata una rete di 16 sensori che monitorino la temperatura dell'aria, la temperatura del ghiaccio in superficie e la temperatura del ghiaccio ad una profondità di 10 cm. Ogni sensore, in tecnologia IoT, viene posto a coprire una determinata area e ciascuno di essi è montato su di una struttura che, tramite un apposito picchetto, lo rende facilmente impiantabile nel ghiaccio. I sensori sono elettricamente autonomi, in quanto dotati di batterie al litio, caricate attraverso un piccolo pannello solare.



La loro struttura è basata su microcontrollore e sono connessi in LOS (Line of Sight) con un vicino rifugio di montagna, dove è posizionato un Access Point (per IoT).
Ogni sensore, costituito da tre trasduttori di temperatura montati sullo stesso picchetto, ha un indirizzo IP statico ed un dispositivo WiFi di collegamento che opera in banda 2.4 GHz con relativa antenna integrata.

La sezione RF dei sensori è caratterizzata dai seguenti dati:

Protocols 802.11 b/g/n (HT20) *802.11n support (2.4 GHz), up to 72.2 Mbps* *Frequency Range 2.4G ~ 2.5G (2400M ~ 2483.5M)*	
TX Power *802.11 b: +20 dBm* *802.11 g: +17 dBm* *802.11 n: +14 dBm*	*Rx Sensitivity* *802.11 b: –91 dbm (11 Mbps)* *802.11 g: –75 dbm (54 Mbps)* *802.11 n: –72 dbm*

L'Access Point (per IoT) dedicato a ricevere i dati dai sensori presenta le seguenti caratteristiche:

Frequency Range 2.400 to 2.4835GHz	
TX Power *802.11 b: +18 dBm* *802.11 g: +16 dBm* *802.11 n: +18 dBm*	*Rx Sensitivity* *802.11 b: –87 dbm (11 Mbps)* *802.11 g: –73 dbm (54 Mbps)* *802.11 n: –71 dbm*

Il rifugio dispone di una piccola rete locale, costituita di 5 PC fissi, un centro stampa ed una piccola area wireless per gli ospiti, gestita da un secondo Access Point; oltre a servire il personale e gli ospiti per le normali attività su Internet, la rete deve avere un collegamento protetto per l'invio dei dati rilevati sul ghiacciaio verso un centro di ricerche del CNR.

La connessione con il territorio è realizzata tramite connessione wireless long-range, con antenna dedicata.

Il candidato, sulla base delle specifiche fornite e fatte le eventuali ipotesi aggiuntive ritenute necessarie:

a) progetti e disegni la struttura completa della rete, tenendo conto delle diverse attività, fornendo un piano di indirizzamento ed una programmazione dei dispositivi necessari;

b) progetti la struttura del pacchetto utile ad inviare i dati dal sensore all'Access Point (per IoT), formulando un'ipotesi relativa al flusso dei dati verso l'Access Point;

c) calcoli la distanza massima di ciascun sensore dall'Access Point (per IoT), per avere un margine di fading di almeno 20dB;

d) valuti e documenti le caratteristiche salienti di una connessione WiMax per il collegamento alla rete Internet;

e) progetti la connessione protetta verso il centro ricerche indicando le modalità software con cui sia possibile l'invio dei dati a distanza.

SECONDA PARTE

Il candidato scelga due dei quesiti e formuli una risposta della **lunghezza massima di 20 righe** esclusi eventuali grafici, schemi e tabelle.

1. Descrivere cosa si intende per cablaggio strutturato di una LAN.
2. Indicare le informazioni che ci fornisce il parametro BER, riferito ad una tratta di connessione, e quali sono le modalità di misura.
3. Indicare quali sono le caratteristiche del protocollo HDLC.
4. Descrivere le caratteristiche dei principali protocolli di Routing.

Durata massima della prova: 7 ore.

È consentito l'uso di manuali tecnici e di calcolatrice non programmabile.

È consentito l'uso del dizionario bilingue (italiano-lingua del paese di provenienza) per i candidati di madrelingua non italiana.

SOLUZIONE (BOZZA)

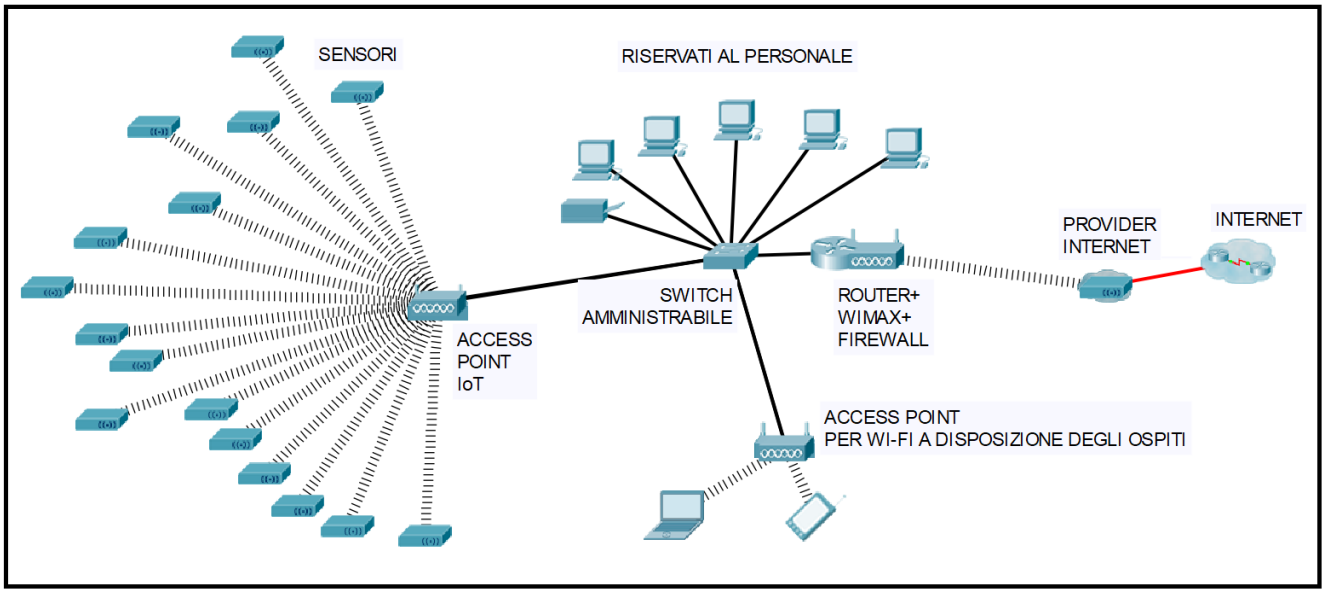
a) Progetti e disegni la struttura completa della rete, tenendo conto delle diverse attività, fornendo un piano di indirizzamento ed una programmazione dei dispositivi necessari

Oltre a quelli indicati nelle specifiche di progetto, una possibile infrastruttura di rete che soddisfa i requisiti richiesti comprende i seguenti apparati:

- un router dotato di interfaccia radio Wi-Max (o collegato/integrato con un modem radio Wi-Max) e almeno un'interfaccia cablata Ethernet 1000BASE-T, un firewall software o hardware;
- uno switch amministrabile con porte Ethernet 100/1000BASE-T, a cui vengono collegati in modo cablato i 5 PC fissi, la stampante di rete posta nel centro stampa e i due access point

I PC fissi e il centro stampa, costituito da una stampante collegata in rete sono riservati al personale e sono interconnessi in modo cablato allo switch.

L'infrastruttura di rete che si viene a realizzare può quindi essere schematizzata nel seguente modo:



Per quanto concerne il piano di indirizzamento si possono definire 3 subnet (sottoreti) con indirizzi IPv4 privati, che saranno mappate su 3 VLAN distinte:

- **subnet sensor node**, che deve mettere a disposizione un numero di indirizzi IPv4 non inferiore a 18 (16 per i sensori + indirizzo di subnet + indirizzo di broadcast);
- **subnet della rete del personale**, comprendente i PC fissi, la stampante di rete, gli apparati di rete (access point, switch amministrabile) che metta a disposizione non meno di 12 indirizzi IPv4;
- **subnet ospiti**, che metta a disposizione un numero di indirizzi IPv4 sufficiente a servire la clientela del rifugio; essendo un rifugio di alta montagna si ipotizza che il numero massimo di dispositivi degli ospiti che possono richiedere contemporaneamente un indirizzo IPv4 sia 100. Si ipotizza anche che normalmente solo circa il 20% dei dispositivi acceda a Internet contemporaneamente per cui essi possono venire serviti da un solo access point.

Il piano di indirizzamento può essere ritagliato da uno dei blocchi di indirizzi IPv4 privati:

10.0.0.0/8; 172.16.0.0/12; 192.168.0.0/16

Si applica la metodologia VLSM (*Variable Lenght Subnet Mask*) per ottenere blocchi di indirizzi IPv4 contigui da assegnare alle tre subnet IP.

Soluzione a cura del prof. Onelio Bertazioli

Essendo indicativamente il numero complessivo di indirizzi IPv4 necessari all'incirca 130 è possibile utilizzare un blocco iniziale con subnet mask /24 che mette a disposizione in totale $N = 2^8 = 256$ indirizzi IPv4.

Per comodità di calcolo si sceglie quindi come blocco di partenza il **blocco 10.0.0.0/24**

Possiamo quindi procedere alla suddivisione del blocco in sottoblocchi da assegnare alle diverse subnet IPv4.

Allungando di 1 bit la subnet mask, che diventa /25, si ottengono i seguenti due blocchi:

a) **10.0.0.0/25 (subnet mask 255.255.255.128)**, che mette a disposizione degli host un totale di

$N = 2^7 - 2 = 126$ indirizzi IPv4; il blocco a) può quindi essere utilizzato per la **subnet IP degli ospiti**;

b) 10.0.0.128/25; questo blocco può essere ulteriormente suddiviso in due parti allungando la subnet mask di 1 bit, che diventa così una /26 (255.25.255.192), ottenendo i seguenti due blocchi:

primo blocco: 10.0.0.128/26 ; secondo blocco: 10.0.0.192/26

Il secondo blocco (10.0.0.192/26), che mette a disposizione un totale di $N = 2^6 = 64$ non viene utilizzato ed è a disposizione per futuri ampliamenti dell'infrastruttura di rete.

Il primo blocco (**10.0.0.128/26**) può essere ulteriormente suddiviso, allungando la subnet mask di 1 bit che diventa una /27, ottenendo così i seguenti blocchi:

c) **10.0.0.128/27 (subnet mask 255.255.255.224)**, che mette a disposizione degli host un totale di $N = 2^5 - 2 = 30$ indirizzi IPv4; il blocco c) può quindi essere utilizzato per la **subnet IP dei sensori**;

d) 10.0.0.160/27, che mette a disposizione degli host un totale di $N = 2^5 - 2 = 30$ indirizzi IPv4; il blocco d) può essere utilizzato per la **subnet IP del personale** (anche se non è ottimizzato) oppure può essere ulteriormente suddiviso, allungando la subnet mask di 1 bit (/28) in due blocchi:

e) **10.0.0.160/28 (subnet mask 255.255.255.240),** che mette a disposizione degli host un totale di

$N = 2^4 - 2 = 14$ indirizzi IPv4; il blocco e) può quindi essere utilizzato per la subnet IP del personale; l'altro blocco non viene utilizzato.

Si procede quindi alla stesura del piano di indirizzamento di ciascuna subnet IPv4

SUBNET IP OSPITI

Indirizzo IPv4	Subnet mask	Assegnazione degli indirizzi IPv4
10.0.0.0	255.255.255.128	Indirizzo della subnet Ospiti
10.0.0.1	255.255.255.128	Default Gateway (router)
10.0.0.2	255.255.255.128	Access Point
10.0.0.3	255.255.255.128	LIBERO
……	……..	
10.0.0.9	255.255.255.128	LIBERO
10.0.0.10	255.255.255.128	range DHCP da 10.0.0.10 a 10.0.0.110
10.0.0.11	255.255.255.128	
……	……..	
10.0.0.109	255.255.255.128	
10.0.0.110	255.255.255.128	range DHCP da 10.0.0.10 a 10.0.0.100
10.0.0.111	255.255.255.128	LIBERO
…….	……..	LIBERI
10.0.0.126	255.255.255.128	PC LINUX di servizio con server DHCP
10.0.0.127	255.255.255.128	Indirizzo di broadcast

SUBNET IP DEI **SENSOR NODE**

Indirizzo IPv4	Subnet mask	Assegnazione statica degli indirizzi IPv4
10.0.0.128	255.255.255.224	Indirizzo subnet sensor node
10.0.0.129	255.255.255.224	SENSOR NODE EUI1
10.0.0.130	255.255.255.224	SENSOR NODE EUI2
10.0.0.131	255.255.255.224	SENSOR NODE EUI3
10.0.0.132	255.255.255.224	SENSOR NODE EUI4
10.0.0.133	255.255.255.224	SENSOR NODE EUI5
10.0.0.134	255.255.255.224	SENSOR NODE EUI6
10.0.0.135	255.255.255.224	SENSOR NODE EUI7
10.0.0.136	255.255.255.224	SENSOR NODE EUI8
10.0.0.137	255.255.255.224	SENSOR NODE EUI9
10.0.0.138	255.255.255.224	SENSOR NODE EUI10
10.0.0.139	255.255.255.224	SENSOR NODE EUI11
10.0.0.140	255.255.255.224	SENSOR NODE EUI12
10.0.0.141	255.255.255.224	SENSOR NODE EUI13
10.0.0.142	255.255.255.224	SENSOR NODE EUI14
10.0.0.143	255.255.255.224	SENSOR NODE EUI15
10.0.0.144	255.255.255.224	SENSOR NODE EUI16
10.0.0.145	255.255.255.224	PC di servizio per test e prove di connettività
10.0.0.146	255.255.255.224	LIBERO
…….	……..	LIBERI
10.0.0.158	255.255.255.224	Default gateway (router)
10.0.0.159	255.255.255.224	Indirizzo di Broadcast

SUBNET IP DEL PERSONALE

Indirizzo IPv4	Subnet mask	Assegnazione statica degli indirizzi IPv4
10.0.0.160	255.255.255.240	Indirizzo Subnet personale
10.0.0.161	255.255.255.240	Default gateway (router)
10.0.0.162	255.255.255.240	Switch
10.0.0.163	255.255.255.240	Access point sensor node
10.0.0.164	255.255.255.240	Access point ospiti
10.0.0.165	255.255.255.240	Stampante rete
10.0.0.166	255.255.255.240	PC 1
10.0.0.167	255.255.255.240	PC 2
10.0.0.168	255.255.255.240	PC 3
10.0.0.169	255.255.255.240	PC 4
10.0.0.170	255.255.255.240	PC 5
10.0.0.171	255.255.255.240	liberi
…….	……..	
10.0.0.174	255.255.255.240	
10.0.0.175	255.255.255.240	Indirizzo di Broadcast

La rete configurata può quindi essere schematizzata nel seguente modo:

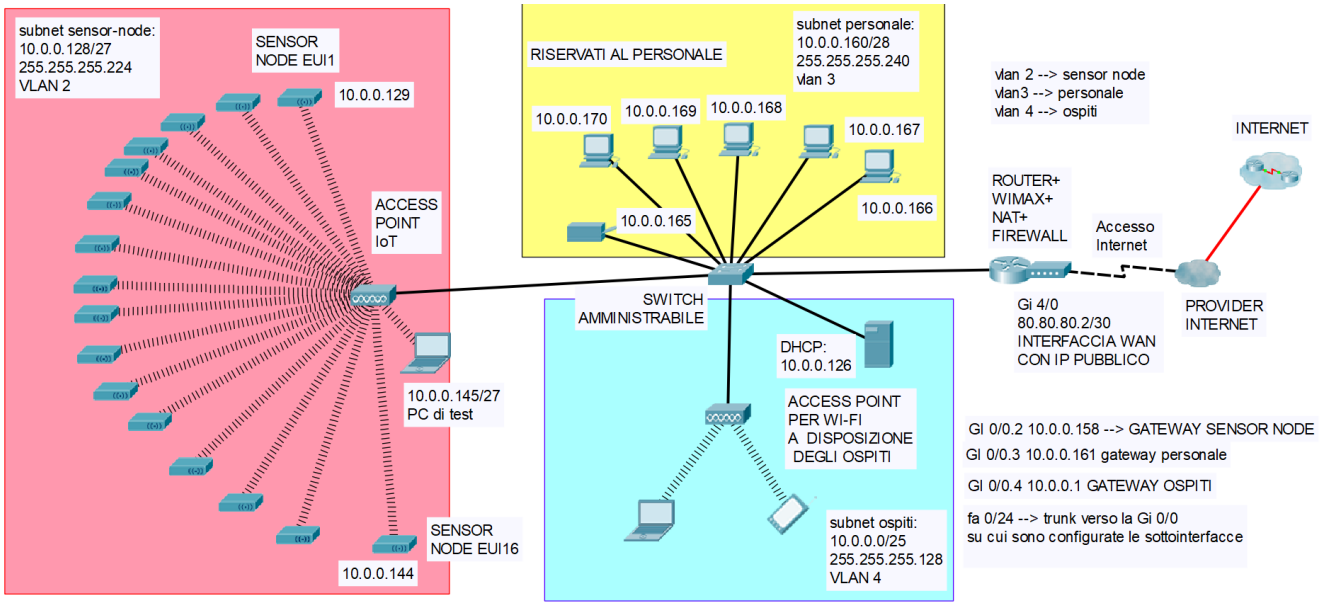


FIGURA 2 Schema finale della rete con apparati configurati

- **Configurazione degli apparati.**

Gli access point (AP) sono configurati con un SSID che non è quello di default.

Configurazione access point IoT

- **Modalità operativa a standard 802.11b**, in quanto garantisce le migliori prestazioni in termini di livelli di potenza di trasmissione e sensibilità di ricezione e quindi massimizza la distanza a cui possono essere posti i sensori;
- **livello di potenza in trasmissione massimo** (18 dBm), si impiega un'**antenna con guadagno pari a 2 dBi** in modo da operare con valore massimo di EIRP consentito dalle normative, che è pari a EIRPmax = +20 dBm;
- **Canale n. 1, con frequenza 2412 MHz, in quanto è il meno attenuato**
- SSID nascosto (non viene irradiato in broadcast);
- autenticazione e crittografia con WPA2-PSK (Personal) e AES
- filtraggio sugli indirizzi MAC che consente l'accesso in rete solo ai sensor node e al PC di servizio
- per semplificare l'assegnazione degli indirizzi IPv4 ai sensor node è possibile impiegare un AP che integri un DHCP e fare in modo che l'assegnazione degli indirizzi IPv4 sia statica ma avvenga tramite il server DHCP, legando l'indirizzo IPv4 assegnato a un sensor node all'indirizzo MAC della scheda Wi-Fi integrata.

Configurazione access point ospiti

- Canale Wi-Fi N. 11, in modo da non creare interferenze con il canale impiegato dall'AP per IoT
- Modalità operativa 802.11n
- SSID irradiato in broadcast
- autenticazione e crittografia con WPA2-PSK (Personal) e AES
- per semplificare l'assegnazione degli indirizzi IPv4 agli ospiti è possibile impiegare un AP che integri un server DHCP; in caso contrario si prevede l'impiego di un server DHCP su PC Linux.

Configurazione dello Switch amministrabile

Si effettua la configurazione con i seguenti passaggi[1].

1) Creazione delle tre VLAN

```
Switch(config)#vlan 2
Switch(config-vlan)#name sensor-node
Switch(config-vlan)#vlan 3
Switch(config-vlan)#name personale
Switch(config-vlan)#vlan 4
Switch(config-vlan)#name ospiti
Switch(config-vlan)#exit
Switch(config)# exit
```

2) Assegnazione delle porte dello switch alle VLAN

```
Switch(config)#interface range fa0/10-15
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 3 (personale)
Switch(config-if-range)#exit

Switch(config)#interface fa0/1
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 2 (sensori)
Switch(config-if-range)#exit

Switch(config)#interface fa0/2
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 4 (ospiti)
Switch(config-if-range)#exit
```

Prima opzione (da preferire): lo switch è collegato al router con una sola interfaccia, sulla quale si configurano 3 sottointerfacce

- l'interfaccia dello switch collegata al router viene configurata come trunk

```
Switch(config)#interface Fa0/24
Swirch(config-if)#switchport mode trunk
Switch(config-if)#end
```

[1] A titolo esemplificativo sono riportati i comandi da utilizzare per configurare apparati Cisco System.

Configurazione del router tramite cui si accede a Internet (esclusa la VPN)

- sul router si creano tre sottointerfacce della interfaccia Gi 0/0 e le si associa alle rispettive VLAN

```
router-rifugio (config)#interface Gi0/0.2          (sensori)
router-rifugio (config-subif)#encapsulation dot1q  2
router-rifugio (config-subif)#ip address 10.0.0.158 255.255.255.224

router-rifugio (config-subif)#interface Gi0/0.3   (personale)
router-rifugio (config-subif)#encapsulation dot1q  3
router-rifugio (config-subif)#ip address 10.0.0.161 255.255.255.240

router-rifugio (config-subif)#interface Gi0/0.4   (ospiti)
router-rifugio (config-subif)#encapsulation dot1q  4
router-rifugio (config-subif)#ip address 10.0.0.1 255.255.255.128
```

NOTA
Sono riportati degli esempi di impostazioni configurate, con le seguenti corrispondenze:
10.0.0.128 255.255.255.224 0.0.0.31 subnet sensori; gateway 10.0.0.158 Gi 1/0 (subIF Gi 0/0.2) vlan 2
10.0.0.160 255.255.255.240 0.0.0.15 subnet personale gateway 10.0.0.161 Gi 2/0 (subIF Gi 0/0.3) VLAN 3
10.0.0.0 255.255.255.128 0.0.0.127 subnet ospiti gateway 10.0.0.1 Gi 0/0 ((subIF Gi 0/0.4) vlan 4

Le corrispondenze tra router con 3 interfacce e router con 1 sola interfaccia possono essere le seguenti:
Gi 0/0 → Gi 0/0.4
Gi 1/0 → Gi 0/0.2
Gi 2/0 → Gi 0/0.3
Nel seguito mettere l'interfaccia o la sottointerfaccia a second ache si opti per la soluzione di router con 3 interfacce oppure con router con 1 interfaccia (la Gi 0/0 e 3 sottointerfacce Gi 0/0.2, Gi 0/0.3, Gi 0/0.4)

Seconda opzione (deprecata): lo switch è collegato al router con tre interfacce, ognuna delle quali fa da default gateway per una subnet IP.

```
Switch(config)#interface fa0/22  (porta che collega l'I/F del router che fa da gateway verso Internet)
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 4 (ospiti)
Switch(config-if-range)#exit

Switch(config)#interface fa0/23  (porta che collega l'I/F del router che fa da gateway verso Internet)
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 2 (sensori)
Switch(config-if-range)#exit

Switch(config)#interface fa0/24  (porta che collega l'I/F del router che fa da gateway verso Internet)
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 3 (personale)
Switch(config-if-range)#exit
```

- Per separare le 3 subnet si usano tre Access Control List (ACL) standard, la 2, la 3 e la 4

ACL 2 (da applicare alla IF Gi 1/0, o alla subIF Gi 0/0.2, quella dei sensori) che nega l'accesso a IPv4 sorgenti appartenenti alle altre due subnet:

- nega (deny) l'uscita di pacchetti aventi indirizzo sorgente appartenente alla rete 10.0.0.160/28 e 10.0.0.1/127
- permette (permit) il resto (any):

```
router-rifugio(config)#access-list 2 deny 10.0.0.160 0.0.0.15
router-rifugio(config)#access-list 2 deny 10.0.0.1 0.0.0.127
router-rifugio(config)#access-list 2 permit any
```

ACL 3 (da applicare alla IF Gi 2/0, o alla subIF Gi 0/0.3, quella del personale) che nega l'accesso a IP sorgenti appartenenti alle altre due subnet

- nega (deny) l'uscita di pacchetti aventi indirizzo sorgente appartenente alle subnet 10.0.0.1/25 e 10.0.0.128/27
- permette (permit) il resto (any):

```
router-rifugio(config)#access-list 3 deny 10.0.0.128 0.0.0.31
router-rifugio(config)#access-list 3 deny 10.0.0.1 0.0.0.127
router-rifugio(config)#access-list 3 permit any
```

ACL 4 (da applicare alla IF Gi 0/0, o alla subIF Gi 0/0.4, quella degli ospiti) che nega l'accesso a IP sorgenti appartenenti alle altre due subnet:

- nega (deny) l'uscita di pacchetti aventi indirizzo sorgente appartenente alle subnet 10.0.0.128/27 e 10.0.0.160/28
- permette (permit) il resto (any):

```
router-rifugio(config)#access-list 4 deny 10.0.0.128 0.0.0.31
router-rifugio(config)#access-list 4 deny 10.0.0.160 0.0.0.15
router-rifugio(config)#access-list 4 permit any
```

- Si applica l'ACL 2 alla interfaccia Gi 1/0, o alla Gi 0/0.2, (10.0.0.158)
- Si applica l'ACL 3 alla interfaccia Gi 2/0, o alla Gi 0/0.3, (10.0.0.161)
- Si applica l'ACL 4 alla interfaccia Gi 0/0, o alla Gi 0/0.4, (10.0.0.1)

```
router-rifugio(config)#int Gi 1/0   (o Gi 0/0.2)
router-rifugio(config-if)# ip access-group 2 out
router-rifugio(config-if)#exit

router-rifugio(config)#int Gi 2/0   (o Gi 0/0.3)
router-rifugio(config-if)#ip access-group 3 out
router-rifugio(config-if)#end

router-rifugio(config)#int Gi 0/0   (o Gi 0/0.4)
router-rifugio(config-if)#ip access-group 4 out
router-rifugio(config-if)#end
```

L'indirizzo IPv4 dell'**interfaccia WAN del router** (lato Internet) è un indirizzo IPv4 pubblico assegnato dall'ISP

Soluzione a cura del prof. Onelio Bertazioli

Per quanto concerne il **routing** è sufficiente configurare una *default* route che abbia come *next hop* l'interfaccia del router dell'ISP tramite cui si accede a Internet:

```
router-rifugio(config)#ip route 0.0.0.0 0.0.0.0  <Ind_IP_router_provider>
```

- Configurazione del NAT overload o PAT

Poiché nelle subnet interne si utilizzano indirizzi IPv4 privati, va poi configurata la funzione NAT/PAT sul router, che sostituisce nei pacchetti IP in uscita gli indirizzi IPv4 privati con un indirizzo IP pubblico (qui si utilizza quello dell'interfaccia WAN del router) ed effettua la sostituzione inversa per i pacchetti ricevuti da Internet.

```
router-rifugio#conf  term
router-rifugio(config)#access-list 10 permit 10.0.0.0  0.0.0.255
router-rifugio(config)#ip nat inside source list 10 interface Gi 4/0 overload
router-rifugio(config)#interface Gi 4/0  (interfaccia WAN)
router-rifugio(config-if)#ip nat outside
router-rifugio(config-if)#exit
router-rifugio(config)#int Gi 0/0  (o Gi 0/0.4)
router-rifugio(config-subif)#ip nat inside
router-rifugio(config-subif)#exit
router-rifugio(config)#int Gi 1/0   (o Gi 0/0.2)
router-rifugio(config-subif)#ip nat inside
router-rifugio(config-subif)#exit
router-rifugio(config)#int Gi 2/0 (o Gi 0/0.3)
router-rifugio(config-subif)#ip nat inside
router-rifugio(config-subif)#exit
router-rifugio(config)#end
router-rifugio#copy run start
```

La verifica del NAT dopo avere fatto un ping da un PC verso Internet può essere fatta con il comando:

```
router-rifugio#show ip nat translations
```

Esempio di configurazione del **server DHCP** per la subnet ospiti in ambiente LINUX

```
# Sample configuration file for ISC dhcpd for Debian

subnet 10.0.0.0 netmask 255.255.255.128 {
 range 10.0.0.10  10.0.0.110;
 option domain-name-servers 208.67.220.220, 208.67.222.222;
 option domain-name "LAB-TELECOMUNICAZIONI";
 option routers 10.0.0.1;
  option broadcast-address  10.0.0.127;
  default-lease-time 6000;
  max-lease-time 72000;
 }

# Fixed IP addresses can also be specified for hosts.
# decommentare per assegnare un indirizzo IP statico
# host PC-IP-FISSO {
#   hardware ethernet xx:xx:xx:xx:xx:xx;
#   fixed-address 10.0.0.111;
}
```

b) In ambito IoT un sensor node (detto anche *end node* o *mote* o *device*) può essere costituito da:

- un sistema integrato a microcontrollore (System on a Chip, per esempio analogo ad Arduino MKR WiFi 1010, già dotato di modulo radio WiFi) dotato di software di comunicazione (protocolli TCP/IP e protocollo dello strato 2 MAC IEEE 802.11 – Wi-Fi - nel caso in esame), in grado di eseguire dei programmi memorizzati (i più evoluti possono essere dotati di sistema operativo, di solito di tipo LINUX)
- interfacce verso i sensori, con possibilità di acquisire direttamente valori analogici (convertitore A/D integrato);
- un modulo radio integrato, nel caso in esame di tipo Wi-Fi, dotato di antenna esterna o interna.

In ambito IoT ciascun *sensor node* viene identificato univocamente tramite un identificativo a 64 bit di tipo IEEE EUI64, noto anche come devEUI (*Device Extended Unique Identifier*). In termini generali la PDU (Protocol Data Unit) di applicazione (è preferibile utilizzare il termine pacchetto solo per le PDU dello strato 3 – rete) con cui vengono trasferiti i dati dei sensori (incapsulati nel payload di un pacchetto IPv4) potrebbe essere composta dai seguenti campi:
"tipo di messaggio inviato (dati o eventuali messaggi di servizio/diagnostica)";
"identificativo (es. devEui) del *sensor node*";
"dati", costituiti per esempio da: ID sensore 1 + dato rilevato dal sensore 1; ID sensore 2 + dato rilevato dal sensore 2; ID sensore 3 + dato rilevato dal sensore 3.

Opzionalmente potrebbero anche essere inseriti I seguenti campi: "timestamp (istante di tempo di invio)"; "contatore del numero di frame inviati"; "checksum" (rivelazione errori).
L'invio degli identificativi e dei dati (che costituiscono il *payload* della PDU MQTT) potrebbe anche essere effettuato impiegando il protocollo di applicazione MQTT (*Message Queuing Telemetry Transport*), ampiamente utilizzato in ambito IoT per via della sua semplicità. In questo caso si viene ad avere il seguente protocol stack (o pila protocollare):

MQTT (Strato di applicazione) – TCP (Strato 4) – IPv4 (Strato 3)– MAC IEEE802.11 (Strato 2) – Strato fisico IEEE802.11.

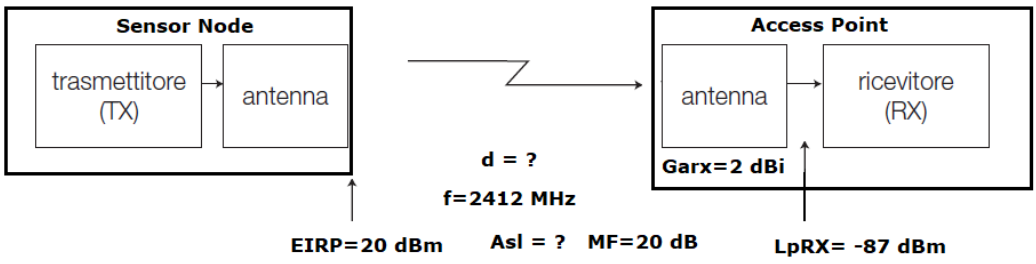
- **Flusso di dati verso l'AP**

I dati forniti dai sensori possono essere inviati a intervalli di tempo regolari per esempio ogni 5-10 minuti.
Il flusso di dati generato da ciascun sensor node verso l'AP è quindi a bassissima velocità.

Opzionalmente si potrebbe calcolare il numero di byte (B) che compongono gli header dei protocolli utilizzati per la trasmissione: 2 B se si utilizza MQTT a livello applicazione; 20 B a livello trasporto se si utilizza TCP (8B se si utilizza UDP); 20 B per IPv4, 34 B per MAC IEEE802.11. In totale quindi 76 B di header a cui vanno aggiunti i pochi Byte del payload della PDU di applicazione e quelli di sincronizzazione (preambolo) a livello fisico.
Indicativamente si trasmettono all'incirca 100 B, quindi 800 bit, alla volta (per esempio ogni 5 minuti), il che conferma un flusso di dati a bassissima velocità.

c) La distanza massima a cui può essere messo un sensore viene calcolata determinando la massima attenuazione consentita, che a sua volta può essere determinata con un bilancio di potenza (o link budget). Per la tratta di uplink (sensor node trasmette, AP riceve) con le scelte effettuate in fase di configurazione si ha:
EIRP = +20 dBm;
Margine di fading MF=20 dB;
guadagno dell'antenna ricevente GantRX= 2 dBi;
minimo livello richiesto in ricezione, pari alla sensibilità del ricevitore (sensitivity), LpRX = -87 dBm

Soluzione a cura del prof. Onelio Bertazioli



LpRX=EIRP - (Asl + MF) +GaRX

Poiché si opera in visibilità ottica (LOS), si può così calcolare la massima attenuazione dello spazio libero consentita dal collegamento:

$$Asl = EIRP - LpRX - MF + GaRX = 20 - (-87) - 20 + 2 = 89\ dB$$

Dalla formula di calcolo dell'attenuazione dello spazio libero si determina la distanza massima consentita:

$$Asl = 32{,}5 + 20log_{10}(f_{MHz}) + 20log_{10}(d_{km}) \rightarrow\ 20log_{10}(d_{km}) = 89 - 32{,}5 - 67{,}6 = -11{,}1$$

$$d_{km} = 10^{11{,}1/20} \cong 0{,}27\ \rightarrow distanza\ massima\ \cong 270\ m$$

d) Il Wi-Max è una tecnologia radio impiegabile per offrire connessioni Internet wireless, che consente di offrire connessioni fino a un massimo di 30 Mbit/s in down link e fino a 3 Mbit/s in uplink. Opera attorno alle frequenze di 3,5 GHz o di 5 GHz, impiega la tecnica di trasmissione a larga banda OFDM (Orthogonal Frequency Division Multiplexing) e sistemi d'antenna MIMO (Multiple Input Multiple Output) con canali radio di banda pari a 3,5 MHz o 7 MHz; nei sottocanali OFDM può trasmettere con modulazioni adattative che possono andare dalla QPSK alla 64 QAM; il full duplex può essere ottenuto con la tecnica TDD (Time Division Duplex) Non si ritiene necessario approfondire ulteriormente la tematica in quanto Wi-Max è attualmente una tecnologia poco diffusa.

e) Per realizzare una connessione protetta verso il centro di ricerca è possibile configurare una VPN (Virtual Private Network) *site to site* che interconnetta, tramite il router (+ firewall) del rifugio e attraverso Internet, la subnet IPv4 dei sensor node con un router (+ firewall) a cui fa capo una subnet IPv4 del centro di ricerca.

In alternativa, se i sensor node sono di tipo evoluto, è possibile impiegare un protocollo come TLS (Transport Layer Security) in grado di crittografare (per esempio con cifratura AES) i dati inviati, in modo che siano protetti durante il transito su Internet.

Si può anche far notare che attualmente esistono tecnologie wireless, genericamente indicate come LPWAN (*Low Power Wide Area Network*), più adatte del Wi-Fi a operare in ambito IoT, come per esempio la tecnologia LoRaWAN (*Log Range Wide Area Network*) che ha le seguenti caratteristiche salienti:

- può operare nella banda libera (ISM) a 868 MHz (o anche a 433 MHz)
- i *sensor node* (detti anche *mote* o *end device*) sono caratterizzati da bassi consumi e durata molto lunga delle batterie
- il gateway può essere realizzato anche con dispositivi a basso costo, come Raspberry Pi, dotati di modulo radio LoRa e collegati in rete in qualsiasi modo (Ethernet, WiFi, ecc.); il gateway riceve i dati inviati dai sensor node via radio (con la tecnologia wireless *LoRa*, di tipo *spread spectrum*) e li inoltra via Internet a un network server LoRaWAN, il quale può poi inoltrarli a un server applicativo del centro ricerche;
- il collegamento radio (wireless) tra sensor node e gateway LoRaWAN può estendersi su distanze rilevanti (anche di circa 10 km in ambiente aperto)
- i dati vengono inviati dai sensor node già crittografati (con algoritmo AES) e quindi protetti.

Soluzione a cura del prof. Onelio Bertazioli

Per quanto concerne la seconda parte si rimanda ai libri di testo.

Libri consigliati:

Onelio Bertazioli
Corso di Telecomunicazioni vol. 2 e vol. 3
ed. Zanichelli

Manuale Cremonese di Informatica e Telecomunicazioni