

Modulo 10 – Fondamenti del routing e delle subnet

Upon completion of this module, the student will be able to perform tasks related to the following:	
10.1	Internet Protocol - Routed
10.2	IP Routing Protocols
10.3	Mechanics of Subnetting

10.1 Protocolli Routed

10.1.1 Protocolli Routable e routed

Un protocollo è un insieme di regole che determina come i computer possano comunicare tra di loro attraverso una rete. Un protocollo descrive:

- Il formato a cui il messaggio deve essere conforme
- Il modo in cui i computer devono scambiarsi un messaggio nel contesto di una attività particolare.

Un protocollo routed (instradabile) permette ad un router di inviare dati tra nodi di reti diverse. Affinché un protocollo sia routable deve avere la possibilità di assegnare un numero di rete ed un numero di host ad ogni dispositivo. Alcuni protocolli, come IPX, richiedono solo un numero di rete perché usano l'indirizzo MAC come indirizzo host. Altri protocolli, come IP, richiedono l'assegnazione completa sia della parte network sia della parte host. Questi protocolli richiedono anche una network mask per differenziare i 2 numeri. L'indirizzo di rete è ottenuto facendo l'AND tra l'indirizzo e la network mask. La network mask permette di raggruppare indirizzi IP sequenziali e trattarli come un solo indirizzo snellendo ad esempio così le tabelle dei router di Internet.

10.1.2 IP come protocollo router

IP (Internet Protocol) è lo schema di indirizzamento gerarchico più usato. IP è un protocollo: connectionless, non affidabile, best-effort delivery.

Il termine connectionless significa che nessuna connessione dedicata viene stabilita prima della trasmissione. IP determina la strada più efficiente per i dati basandosi sui protocolli di routing.

I termini non affidabile e best-effort indicano che IP non verifica che i dati raggiungano effettivamente la destinazione, questa funzione è trattata dai livelli superiori.

10.1.3 Propagazione dei pacchetti e switching all'interno di un router

Quando un pacchetto viaggia attraverso le reti verso la destinazione finale, le intestazioni di livello 2 vengono modificate da ogni dispositivo di livello 3. I frame Ethernet usano gli indirizzi MAC, altri protocolli di livello 2, ad esempio PPP per i link seriali o le connessioni Frame Relay, usano differenti schemi di indirizzamento.

Non appena un frame è ricevuto da un'interfaccia di un router viene estratto l'indirizzo MAC di destinazione, se l'indirizzo coincide con quello dell'interfaccia o se è broadcast il frame è accettato altrimenti viene buttato. Nel frame accettato viene estratto il CRC (Cyclic Redundancy Check) e viene calcolato per verificare se il frame è senza errori. Se il test fallisce il frame è buttato. Se il test viene passato vengono tolte le informazioni di livello 2 ed il frame è passato al livello 3.

Se il pacchetto è destinato al router viene poi passato al livello 4, mentre se è diretto ad una rete differente viene cercato il percorso da seguire nella routing table del router ed inviato sulla apposita interfaccia. Vengono raggiunte le informazioni di livello 2 ed è calcolato un nuovo CRC.

10.1.4 IP (Internet Protocol)

Ci sono 2 tipi di servizi di spedizione: connectionless e connection-oriented.

Molti servizi di rete usano il sistema connectionless, in cui i vari pacchetti possono seguire percorsi diversi e sono riassemblati dopo che arrivano a destinazione. In un sistema connectionless la destinazione non viene contattata prima che il pacchetto sia inviato (simile al sistema postale).

Nei sistemi connection-oriented viene stabilita una connessione tra sorgente e destinazione prima che i dati vengano trasferiti (simile al sistema telefonico).

I processi di rete connectionless sono spesso chiamati processi packet switched, nel senso che i pacchetti possono essere smistati su percorsi differenti. La determinazione del percorso può seguire vari criteri.

I processi connection-oriented sono spesso chiamati processi circuit switched. Tutti i pacchetti viaggiano sequenzialmente sullo stesso circuito fisico.

Internet è una gigantesca rete connectionless in cui i pacchetti sono trattati da IP. TCP aggiunge i servizi di affidabilità a livello 4 a IP.

10.1.5 Anatomia di un pacchetto IP

I pacchetti IP consistono dei dati dei livelli superiori più un'intestazione IP. L'IP header consiste di:

0	4	8	16	19	24	31
VERS		HLEN		Service Type		Total Length
Identification				Flags		Fragment Offset
Time to Live			Protocol		Header Checksum	
Source IP Address						
Destination IP Address						
IP Options (if any)					Padding	
Data						
...						

- **Version** – Indicates the version of IP currently used; four bits. If the version field is different than the IP version of the receiving device, that device will reject the packets.
- **IP header length (HLEN)** – Indicates the datagram header length in 32-bit words. This is the total length of all header information, accounting for the two variable-length header fields.
- **Type-of-service (TOS)** – Specifies the level of importance that has been assigned by a particular upper-layer protocol, eight bits.
- **Total length** – Specifies the length of the entire packet in bytes, including data and header, 16 bits. To get the length of the data payload subtract the HLEN from the total length.
- **Identification** – Contains an integer that identifies the current datagram, 16 bits. This is the sequence number.
- **Flags** – A three-bit field in which the two low-order bits control fragmentation. One bit specifies whether the packet can be fragmented, and the other specifies whether the packet is the last fragment in a series of fragmented packets.
- **Fragment offset** – Used to help piece together datagram fragments, 13 bits. This field allows the previous field to end on a 16-bit boundary.
- **Time-to-live (TTL)** – A field that specifies the number of hops a packet may travel. This number is decreased by one as the packet travels through a router. When the counter reaches zero the packet is discarded. This prevents packets from looping endlessly.
- **Protocol** – indicates which upper-layer protocol, such as TCP or UDP, receives incoming packets after IP processing has been completed, eight bits.
- **Header checksum** – helps ensure IP header integrity, 16 bits.
- **Source address** – specifies the sending node IP address, 32 bits.
- **Destination address** – specifies the receiving node IP address, 32 bits.
- **Options** – allows IP to support various options, such as security, variable length.
- **Padding** – extra zeros are added to this field to ensure that the IP header is always a multiple of 32 bits.
- **Data** – contains upper-layer information, variable length up to 64 Kb.

Gli indirizzi IP sorgente e destinazione sono importanti, gli altri campi sono molto flessibili.

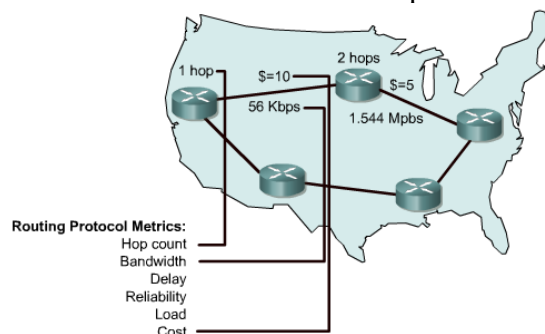
10.2 Protocolli di routing IP

10.2.1 Panoramica sul routing

Il routing è una funzione del livello 3 del modello OSI, è uno schema di organizzazione gerarchico che permette di raggruppare assieme singoli indirizzi e trattarli come fossero un unico indirizzo fino alla destinazione. Il routing è il processo di trovare il percorso più efficiente tra 2 dispositivi. Il principale dispositivo che attua il routing è il router, il quale ha 2 funzioni chiave:

1. mantenere le routing table ed assicurare che gli altri router conoscano i cambiamenti nella topologia della rete. Per far questo si usa un routing protocol.
2. quando arriva un pacchetto il router deve usare la routing table per determinare dove inviarlo. Il router lo pone sulla apposita interfaccia e aggiunge le necessarie informazioni al frame.

Il router è un dispositivo di livello 3 che usa 1 o più metriche per determinare il percorso ottimale. Le metriche di routing sono valori usati per determinare i vantaggi di un percorso su un altro. I protocolli di routing usano varie combinazioni di metriche per determinare il miglior percorso.



The network layer is responsible for routing packets through a network.

Il più comune protocollo routabile è l'IP, esistono anche IPX/SPX e AppleTalk. Un esempio di protocollo non routabile è NetBEUI, che è piccolo, veloce ed efficiente, ma è limitato ad un solo segmento.

10.2.2 Routing e switching

Lo switching avviene a livello 2 ed il routing a livello 3. Per effettuare lo switching vengono usate le ARP table, che contengono la coppia di indirizzi IP – MAC. Per il routing si usano le routing table che dicono come una via è stata conosciuta (ad esempio C = rete direttamente connessa e R = via appresa tramite il protocollo RIP), l'indirizzo di rete IP delle reti note, la distanza delle reti e l'interfaccia da usare per arrivare alla rete di destinazione.

Uno switch interconnette segmenti appartenenti alla stessa rete, se un host deve raggiungere un host di una rete diversa manda il frame al router (default gateway), il quale esamina l'indirizzo IP di destinazione ed in base alla routing table lo invia sull'interfaccia opportuna.

La differenza tra gli indirizzi MAC e IP è che i MAC non sono organizzati logicamente mentre gli IP sono organizzati in modo gerarchico. I router devono trattare un grosso volume di indirizzi per cui hanno bisogno di raggruppare assieme tutti quelli appartenenti alla stessa rete e trattarli come un singolo indirizzo fino a che non si arriva al segmento di destinazione.

Gli switch non bloccano i messaggi broadcast mentre i router sì, per questo forniscono un livello di sicurezza più alto ed un controllo della banda.

Features	Router	Switch
Speed	Slower	Faster
OSI Layer	Layer 3	Layer 2
Addressing used	IP	MAC
Broadcasts	Blocks	Forwards
Security	Higher	Lower

10.2.3 Routed e routing

I protocolli usati a livello 3 in grado di trasferire dati tra host di reti differenti sono detti protocolli routed o routable. Esempi di protocolli routed sono IP, IPX, DECnet, AppleTalk, Banyan, VINES, XNS.

I protocolli di routing permettono ai router di scambiarsi le informazioni e di instradare i protocolli routed. Esempi di protocolli di routing sono RIP, IGRP, OSPF, BGP, EIGRP.

10.2.4 Determinazione del percorso

La determinazione del percorso avviene a livello 3 e abilita un router a confrontare l'indirizzo di destinazione con le strade disponibili nelle routing table e selezionare il percorso migliore.

Il router apprende le strade o col routing statico o con il routing dinamico. Le vie configurate manualmente dall'amministratore sono quelle statiche, mentre quelle apprese da altri router mediante i protocolli di routing sono quelle dinamiche.

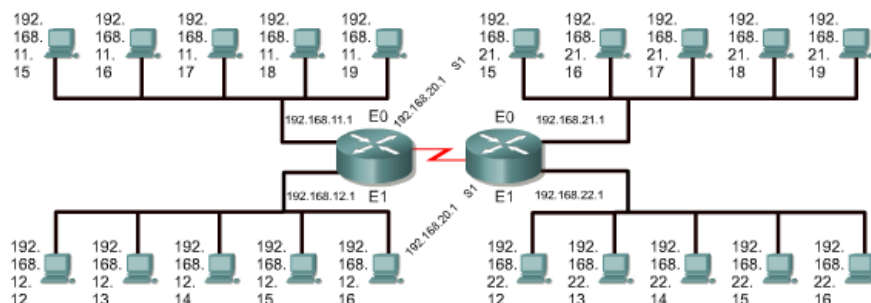
Il router usa la determinazione del percorso per decidere su quale porta deve inoltrare il pacchetto che arriva, questa funzione è detta routing del pacchetto. Ogni router che un pacchetto incontra sul suo cammino è detto hop, l'hop count è la distanza percorsa. I router possono usare per la determinazione del percorso load, bandwidth, cost, reliability.

Quando un router riceve un pacchetto estrae l'indirizzo della rete di destinazione e cerca nelle routing table se vi è un percorso disponibile. Se non vi fosse alcun riferimento verso quella rete guarda se vi è una default route configurata. La default route deve essere configurata dall'amministratore e viene usata come ultima risorsa per inviare un pacchetto. Se non vi è neanche la default route il pacchetto viene buttato ed in genere viene restituito un messaggio di errore che indica che la destinazione è irraggiungibile.

10.2.5 Routing table

I router usano i routing protocols per costruire e mantenere le routing tables che contengono le informazioni sulle strade. Questo aiuta nel processo di determinazione del percorso. I routing protocols riempiono le routing tables con una varietà di informazioni che dipendono dal protocollo usato. I dispositivi di livello 3 interconnettono domini broadcast o LAN, è richiesto uno schema di indirizzamento gerarchico affinché possa avvenire il trasferimento dei dati. I router tengono importanti informazioni nelle loro routing table:

- tipo di protocollo di routing
- associazione destinazione – next hop
- metrica di routing, che esprime la desiderabilità di un percorso
- interfaccia di uscita, cioè l'interfaccia su cui devono essere mandati fuori i dati per raggiungere la destinazione finale.



Routing Table			
Learned	Network Address	Hop	Interface
C	- 192.168.11.0	0	E0
C	- 192.168.12.0	0	E1
C	- 192.168.20.0	0	S0
R	- 192.168.21.0	1	S0
R	- 192.168.22.0	1	S0

Routing Table			
Learned	Network Address	Hop	Interface
C	- 192.168.21.0	0	E0
C	- 192.168.22.0	0	E1
C	- 192.168.20.0	0	S1
R	- 192.168.11.0	1	S1
R	- 192.168.12.0	1	S1

I router comunicano con gli altri router per mantenere le routing table attraverso messaggi, alcuni protocolli di routing mandano i messaggi periodicamente ad intervalli regolari, mentre altri li mandano solo quando vi sono variazioni nella topologia. Alcuni protocolli trasmettono l'intera routing table, mentre altri trasmettono solo le vie che sono cambiate. Analizzando i messaggi di routing dei vicini, un router costruisce e mantiene le routing table.

10.2.6 Algoritmi di routing e metriche

Ogni routing protocol usa un differente algoritmo per decidere su quale porta inviare un pacchetto. Per prendere queste decisioni si usano le metriche. I routing protocol hanno spesso uno o più di questi scopi:

- **Ottimizzazione:** descrive la capacità di un algoritmo di selezionare il percorso migliore. La strada dipenderà dalle metriche usate.
- **Semplicità e basso sovraccarico:** più semplice è l'algoritmo e più efficientemente sarà processato dalla CPU e dalla memoria. Questo è importante su reti molto grandi come Internet.
- **Robustezza e stabilità:** un algoritmo deve comportarsi correttamente anche con circostanze inusuali come rottura dell'hardware o alte condizioni di traffico.
- **Flessibilità:** un algoritmo deve adattarsi velocemente ad una varietà di cambiamenti della rete: disponibilità dei router, memoria dei router, cambiamenti di banda, ritardi.
- **Rapida convergenza:** la convergenza è il processo di condivisione da parte di tutti i router sulle strade disponibili.

Ogni algoritmo di routing genera un numero, chiamato valore della metrica, per ogni percorso della rete. Gli algoritmi sofisticati usano più metriche combinandole in un unico valore. Tipicamente i valori più bassi indicano i percorsi preferibili. Le metriche più comuni sono:

- **Bandwidth**
- **Delay:** è il tempo necessario per muovere un pacchetto dalla sorgente alla destinazione, dipende dalla banda dei collegamenti intermedi e dalla congestione della rete.
- **Load:** la quantità di attività di una risorsa di rete come ad esempio un router
- **Reliability:** si riferisce in genere al tasso di errore di un collegamento
- **Hop count:** è il numero di router che un pacchetto deve attraversare per arrivare a destinazione. Ogni router che si passa è 1 hop.
- **Ticks:** è il ritardo di una linea espresso in IBM PC clock ticks, 1 tick è circa 1/18 di secondo.
- **Cost:** è un valore arbitrario assegnato dall'amministratore di rete.

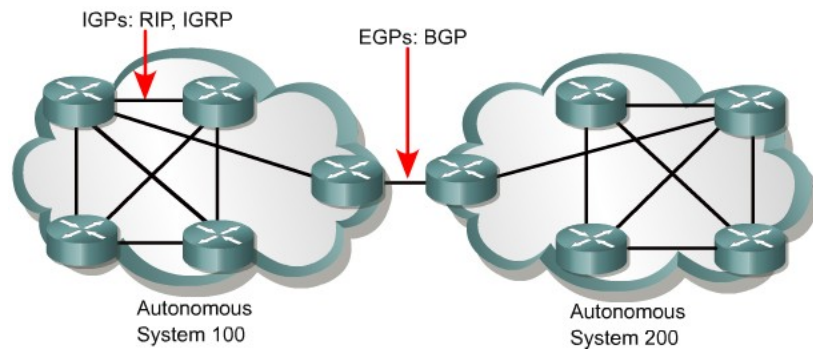
Protocol	Metric	Maximum number of routers	Origins
RIP	Hop count	15	Xerox
IGRP	<ul style="list-style-type: none"> • Bandwidth • Load • Delay • Reliability 	255	Cisco

10.2.7 IGP e EGP

Un sistema autonomo è una rete o un insieme di reti sotto il controllo di un amministratore comune. Due famiglie di routing protocols sono IGP (Interior Gateway Protocol) e EGP (Exterior Gateway Protocol). IGP instrada i dati all'interno di un sistema autonomo mentre EGP li instrada tra differenti sistemi autonomi.

Esempi di IGP: RIP, IGRP, EIGRP, OSPF, IS-IS

Esempio di EGP: BGP.



10.2.8 Link state e distance vector

I protocolli di routing possono essere classificati o come IGP o come EGP. Gli IGP a loro volta possono essere divisi in 2 gruppi: distance vector o link state.

Il routing distance vector determina la distanza e la direzione di ogni segmento della rete. La distanza può essere il numero di hop count. I router che usano gli algoritmi distance vector inviano tutta o parte della routing table ai router vicini ad intervalli regolari, questo avviene anche se non ci sono variazioni nella rete. Quando un router riceve un routing update, verifica tutte le strade note e può fare variazioni alla routing table. Questo processo è noto come routing by rumor.

Esempi di protocolli distance vector sono:

- RIP (Routing Information Protocol): è il protocollo IGP più comune in Internet, come unica metrica usa l'hop count
- IGRP (Interior Gateway Routing Protocol): sviluppato da Cisco per reti grandi ed eterogenee.
- EIGRP (Enhanced IGRP): sviluppato da Cisco, comprende molte caratteristiche di un protocollo link state, per questo è anche stato chiamato protocollo ibrido bilanciato.

I protocolli link state sono stati sviluppati per ovviare alle limitazioni dei protocolli distance vector. Essi rispondono velocemente ai cambiamenti della rete ed inviano gli aggiornamenti solo quando si hanno variazioni nella rete. Gli aggiornamenti periodici, detti link state refreshes, avvengono ad intervalli molto lunghi, ad esempio 30 minuti.

Quando una via cambia, il dispositivo che rileva il cambiamento crea un LSA (Link State Advertisement) su quel link, che viene trasmesso a tutti i dispositivi vicini. Ogni dispositivo tiene una copia del LSA, aggiorna il suo database e invia l'LSA a tutti i dispositivi vicini. Questa inondazione di LSA è richiesta per assicurare che tutti i dispositivi abbiano i database aggiornati.

Gli algoritmi link state usano i loro database per creare delle strade che preferiscono la via più breve. Esempi di protocolli link state sono: OSPF (Open Shortest Path First) e IS-IS (Intermediate System to Intermediate System).

10.2.9 Routing Protocols

RIP è un protocollo distance vector che usa come unica metrica l'hop count. Se ci sono più strade verso la destinazione RIP seleziona la via con minor hop count, che non è detto che sia la via più veloce. RIP non può instradare un pacchetto con più di 15 hop.

RIP versione 1 (RIPv1) richiede che tutti i dispositivi usino la stessa subnet mask perché non includono la subnet mask nelle informazioni di routing, questo è noto come routing classful.

RIP versione 2 (RIPv2) fornisce il prefisso di routing e non invia subnet mask, questo è noto come routing classless. Con questo protocollo è possibile usare differenti subnet mask, questo è detto VLSM (Variable Length Subnet Masking).

IGRP è un protocollo distance vector sviluppato a Cisco per reti grandi che andavano oltre le possibilità ad esempio del RIP. IGRP può selezionare la via basandosi su delay, bandwidth, load, reliability. IGRP supporta un numero molto maggiore di RIP di hop count. E' un routing di tipo classful, quindi non permette le subnet mask variabili.

OSPF è un protocollo link state sviluppato da IETF nel 1988 per reti grandi.

IS-IS è un protocollo link state usato per instradare protocolli diversi da IP. Integrated IS-IS è una versione espansa di IS-IS che supporta più protocolli tra cui IP.

EIGRP è un protocollo proprietario Cisco, è una versione avanzata di IGRP, fornisce una migliore efficienza come: convergenza rapida e basso uso della banda. E' un protocollo distance vector avanzato che usa anche funzioni link state, per questo a volte è classificato come protocollo ibrido.

BGP è un esempio di protocollo EGP. BGP scambia informazioni tra sistemi autonomi. E' il protocollo principale usato dalle maggiori compagnie in Internet. BGP4 è la prima versione di BGP che supporta CIDR (Classless Interdomain Routing) e l'aggregazione delle strade. BGP prende le decisioni in base alle network policies che sono regole attribuite ai vari percorsi.

10.3 I meccanismi del subnetting

10.3.1 Classi di indirizzi IP

Le classi di indirizzi IP offrono un range da 256 a 16,8 milioni di host per rete. Per gestire efficacemente un limitato numero di indirizzi IP, tutte le classi possono essere divise in sottoreti più piccole.

Class A	Network			Host
Octet	1	2	3	4

Class B	Network		Host	
Octet	1	2	3	4

Class C	Network			Host
Octet	1	2	3	4

Class D	Host			
Octet	1	2	3	4

Class D addresses are used for multicast groups. There is no need to allocate octets or bits to separate network and host addresses. Class E addresses are reserved for research use only.

10.3.2 Introduzione al subnetting

Per creare le sottoreti (subnet) i bit della parte host di un indirizzo IP devono essere rassegnati come bit della parte network, partendo sempre dai bit più a sinistra. Gli indirizzi con subnet includono il campo network, il campo subnet ed il campo host. I campi subnet e host sono creati dai bit originali della parte host.

Class C network address 192.168.10.0
11000000.10101000.00001010.00000000 N . N . N . H
11000000.10101000.00001010.00000000 N . N . N . sN H
In this example three bits have been assigned to designate the subnet.

Class B network address 147.10.0.0
10010011.00001010.00000000.00000000 N . N . H . H
10010011.00001010.00000000.00000000 N . N . sN H . H
In this example five bits have been assigned to designate the subnet.

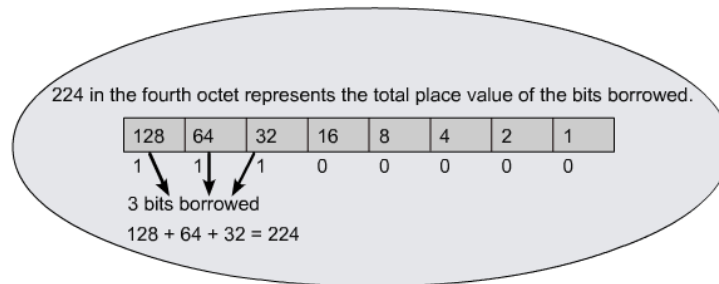
Class A network address 28.0.0.0
00011100.00000000.00000000.00000000 N . H . H . H
00011100.00000000.00000000.00000000 N . sN . sN H . H
In this example twelve bits have been assigned to designate the subnet.

Oltre alla maneggevolezza, le subnet permettono di contenere i domini broadcast e dare sicurezza alle LAN, in quanto l'accesso ad altre subnet può avvenire solo attraverso un router, il quale

garantisce la sicurezza ad esempio attraverso le access list, le quali permettono o vietano l'accesso a determinati host.

10.3.3 Stabilire la subnet mask

Il numero di bit da usare nella parte subnet dipende dal massimo numero di host richiesto. I 2 bit meno significativi di un indirizzo IP devono sempre appartenere alla parte host. Supponendo di avere un indirizzo IP di classe C e di prestare 3 bit per creare le subnet, la subnet mask risulta: 255.255.255.224 che può anche essere rappresentata nel formato slash come /27, dove 27 è il numero di bit usati per le parti network e subnet.



Per determinare il numero di bit da usare nella parte subnet si considera il numero di host richiesto in una subnet, ad esempio supponiamo che sia 30. Dalla seguente tabella, andando in Usable hosts si vede che i bit da usare (Bits borrowed) sono 3.

Slash format	/25	/26	/27	/28	/29	/30	N/A	N/A
Mask	128	192	224	240	248	252	254	255
Bits borrowed	1	2	3	4	5	6	7	8
Value	128	64	32	16	8	4	2	1
Total Subnets		4	8	16	32	64		
Usable Subnets		2	6	14	30	62		
Total Hosts		64	32	16	8	4		
Usable Hosts		62	30	14	6	2		

Con 3 bit di subnet si hanno $2^3 = 8$ sottoreti.

Gli host utilizzabili sono sempre 2 meno di quelli totali perché 2 indirizzi sono usati come indirizzo di rete e indirizzo broadcast.

Il numero di host utilizzabili è dato da $2^{\text{bit host}} - 2$.

10.3.4 Applicare la subnet mask

Una volta creata la subnet mask, la si può utilizzare per creare lo schema delle subnet. Ad esempio con un indirizzo in classe C con 3 bit di subnet si ha:

Subnetwork #	Subnetwork ID	Host Range	Broadcast ID
0	192.168.10.0	.1--.30	192.168.10.31
1	192.168.10.32	.33--.62	192.168.10.63
2	192.168.10.64	.65--.94	192.168.10.95
3	192.168.10.96	.97--.126	192.168.10.127
4	192.168.10.128	.129--.158	192.168.10.159
5	192.168.10.160	.161--.190	192.168.10.191
6	192.168.10.192	.193--.222	192.168.10.223
7	192.168.10.224	.225--.254	192.168.10.255

Con 5 bit della parte host si hanno 32 host possibili. Per trovare il range di indirizzi di una subnet bisogna ragionare in binario nelle parti subnet e host. Ad esempio per la subnet 0 bisogna scrivere 0 con 3 bit in binario, facendo variare poi tutti gli altri bit:

000 00000 = 0

.....

000 11111 = 31

Per cui la 1° subnet va da 192.168.10.0 a 192.168.10.31.

Per la subnet 1 si ha:

001 00000 = 32

.....

001 11111 = 63 per cui da 192.168.10.32 a 192.168.10.63.

Da notare che quando tutti i bit della parte host valgono 0 si ha l'indirizzo della sottorete, mentre se valgono 1 si ha l'indirizzo broadcast. Per cui nella subnet 0 si ha:

192.168.10.0 = indirizzo sottorete

192.168.10.1 = indirizzo 1° host

192.168.10.30 = indirizzo 30° host

192.168.10.31 = indirizzo broadcast

10.3.5 Subnettare le reti in Classe A e B

La procedura per creare subnet nelle classi A e B è identica a quella della classe C solo che ci sono molti più bit coinvolti, si può arrivare a 22 bit di subnet in classe A e a 14 in classe B.

Class B network address 147.10.0.0 (14 bits available)	
11001011.00001010.00000000.00000000	
N . N . H . H	
10010011.00001010.00000000.00000000	
N . N . sN . sN H	
In this example 12 bits have been assigned to designate the subnet.	

Assegnando 12 bit di un indirizzo in classe B la subnet mask è 255.255.255.240 o /28.

Class A network address 28.0.0.0 (22 bits available)	
00011100.00000000.00000000.00000000	
N . H . H . H	
00011100.00000000.00000000.00000000	
N . sN . sN . sN H	
In this example 20 bits have been assigned to designate the subnet.	

Assegnando 20 bit di un indirizzo in classe A la subnet mask è 255.255.255.240 o /28.

10.3.6 Calcolare l'indirizzo delle subnet facendo l'AND

I router usano le subnet mask per determinare l'indirizzo delle sottoreti, da un indirizzo IP basta fare l'operazione di AND binario con la subnet mask. L'AND equivale ad una moltiplicazione, fornisce 1 solo se entrambi i bit sono 1.

Packet address	201.10.11.65	11001001.00001010.00001011.01000001
AND		
Mask	255.255.255.224	11111111.11111111.11111111.11100000
Subnetwork ID	201.10.11.64	11001001.00001010.00001011.01000000