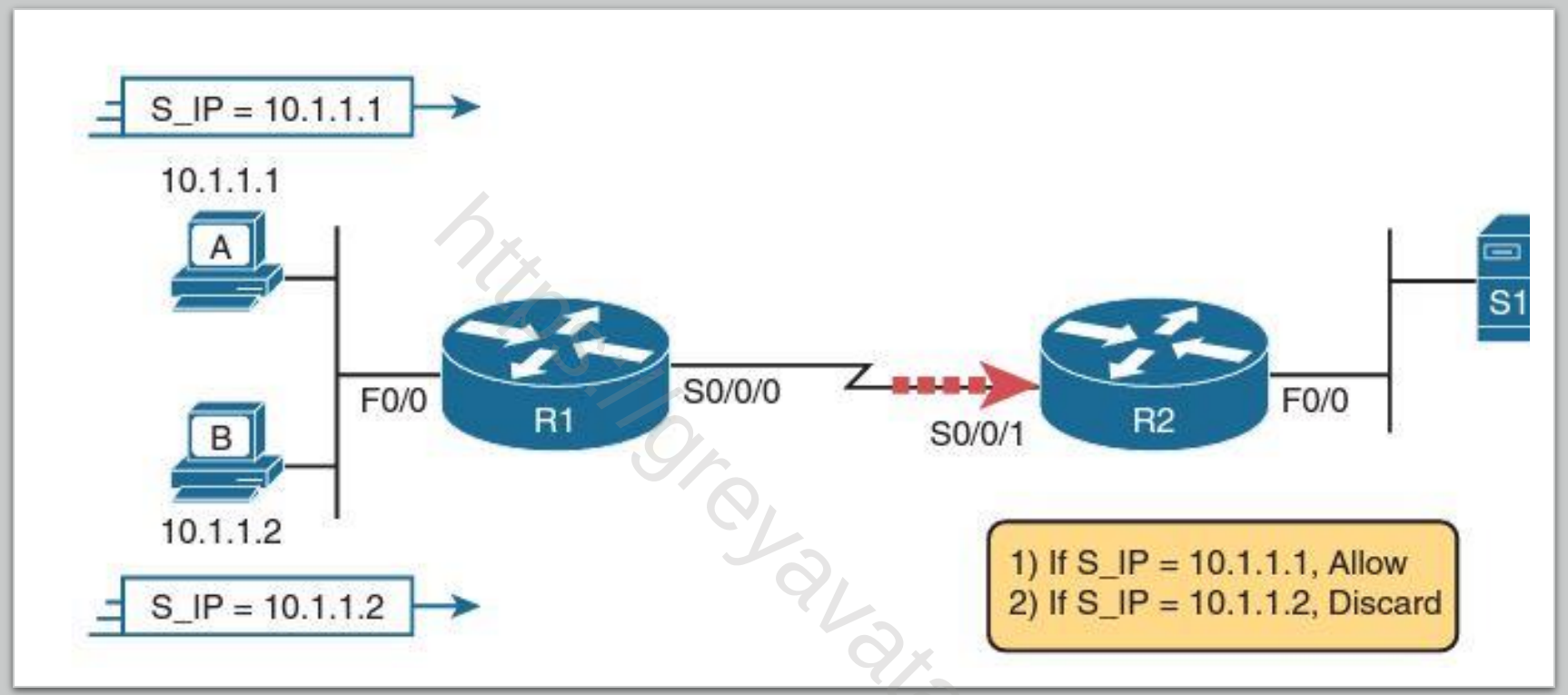
CCNA 200-301
ACL

INTRODUZIONE

Le access control lists (IP ACL) servono per identificare i pacchetti. Per fare questo, le ACL contengono una lista di valori che i router possono ricercare negli header IP,TCP,UDP.

Le ACL vengono utilizzate in diversi modi, ma il principale è quello di filtrare i pacchetti.

I router CISCO possono applicare le ACL ai pacchetti in ingresso o ai pacchetti in uscita da un'interfaccia. In altri termini le ACL sono associate ad un'interfaccia ed ad una direzione IN/OUT



In questo esempio l'ACL viene applicata all'interfaccia S0/0/0 di R2 in INGRESSO.

Le due regole indicano:

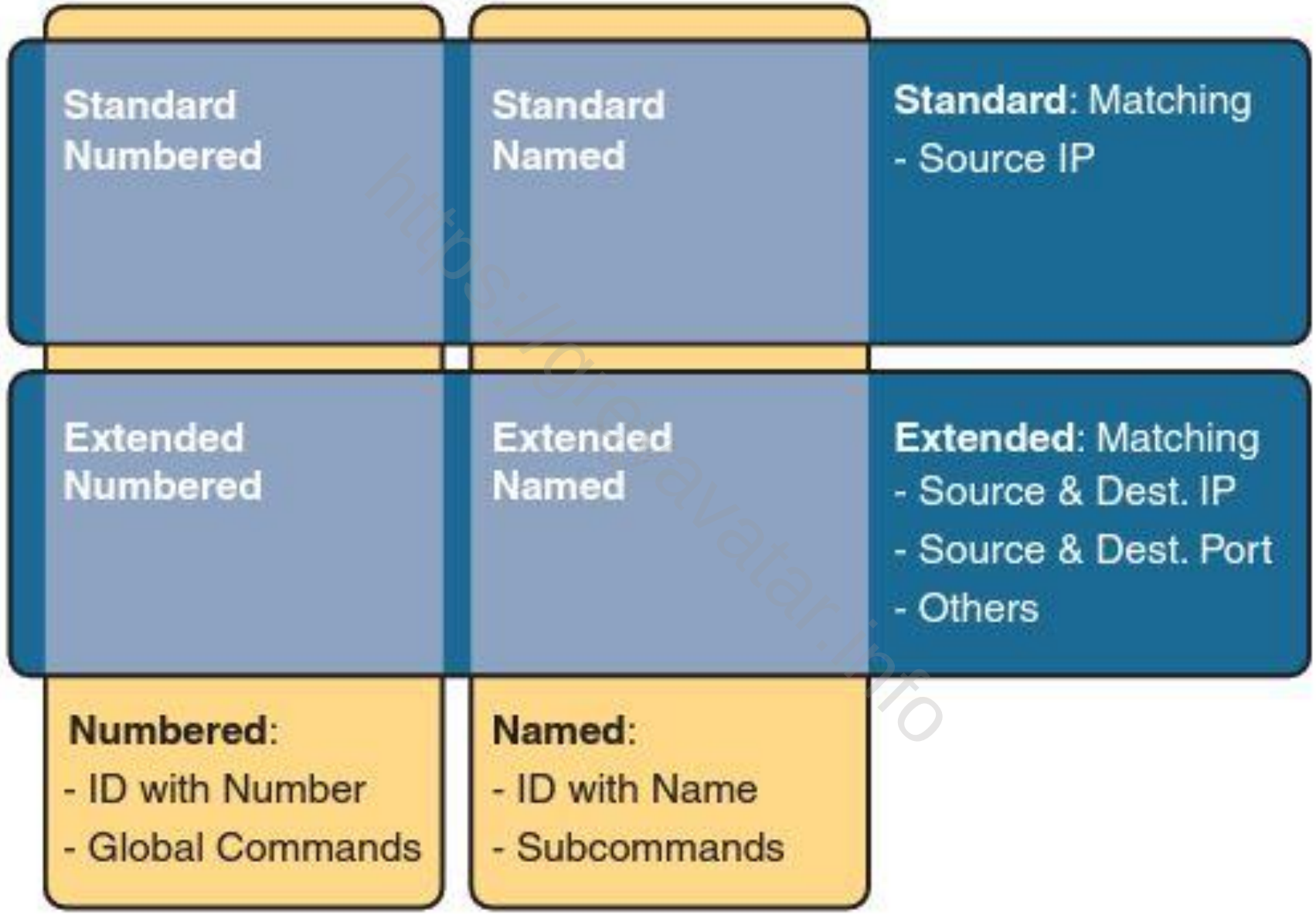
1. Se l'IP sorgente è 10.1.1.1 il traffico è consentito
2. Se l'ip sorgente è 10.1.1.2 il traffico è bloccato

Il risultato è che solo il traffico dell'host A attraverserà il router R2

CCNA 200-301
ACL

TIPI

- STANDARD NUMERATE (1-99)
- EXTENDED numerate (100-199)
- ACL addizionali (1300-1999 Standard, 2000-2699 Extended)
- ACL con nome


Standard
Numbered
Standard
Named
Standard: Matching
- Source IP
Extended
Numbered
Extended
Named
Extended: Matching
- Source & Dest. IP
- Source & Dest. Port
- Others
Numbered:
- ID with Number
- Global Commands
Named:
- ID with Name
- Subcommands

Match con un **range** di IP

access-list 1 permit 10.1.1.0 0.0.0.255

0.0.0.225 è una Wildcard Mask ovvero l'opposto di una Mask

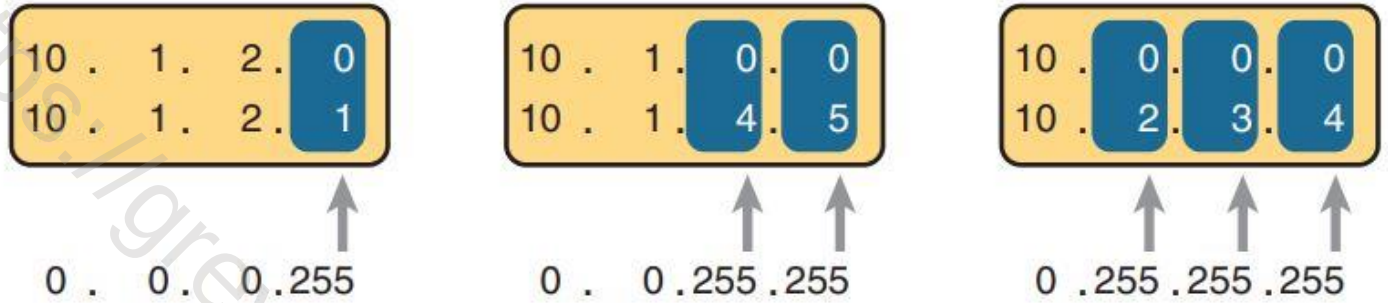
Match con un **sigolo** host

access-list {1-99 | 1300-1999} {permit | deny} matching-parameters

access-list 1 permit 10.1.1.1

access-list 1 permit host 10.1.1.1 (vecchia versione del comando)

WILDCARDS



- Decimale 0: il router deve confrontare l'otteto
- Decimale 255: Il router ignora l'otteto.

WILDCARD MASK CORRETTA PER UNA SUBNET

- Usa la subnet come valore sorgente nel comando access-list
- Per trovare la wildcard sottrarre a 255.255.255.255 il valore della mask di rete

255.255.255.255 –

255.255.252.000 =

000.000.003.255

IMPLEMENTARE UNA ACL STANDARD

1. Pianificare la posizione di applicazione (router ed interfaccia) e la direzione (IN o OUT)
    1. Una ACL andrebbe aggiunta vicino alla destinazione del pacchetto. (Per evitare di scartare pacchetti non voluti)
    2. Ricorda le standard ACL identificano i pacchetti solo in base all'IP sorgente.
2. Le ACL vanno create dalla configurazione globale
    1. Le regole vengono valutate dall'alto al basso
    2. Alla fine della ACL c'è un deny implicito
3. La ACL va applicata all'interfaccia corretta con il comando **ip access-group number {in | out}**

INPLEMENTARE UNA EXTENDED ACL

1. Pianificare la posizione di applicazione (router ed interfaccia) e la direzione (IN o OUT).
    1. Una ACL estesa va posizionata il più possibile vicino alla sorgente. (In questo modo salvo banda)
    2. Ricorda che tutti i campi devono essere corretti per identificare il pacchetto
2. I comandi per creare l'ACL si possono sintetizzare così:
    1. **access-list** access-list-number {**deny | permit**} protocol source source-wildcard destination destination-wildcard [**log | log-input**]
    2. **access-list** access-list-number {**deny | permit**} {**tcp | udp**} source source-wildcard [operator [port]] destination destination-wildcard [operator [port]] [**established**] [**log**]

ACL IDENTIFICATE DAL NOME