Access Control Lists

HUAWEI TECHNOLOGIES CO., LTD.

Foreword

Many technologies and protocols depend on Access Control Lists (ACL) for greater management and filtering of traffic as part of security measures or application requirements. The implementation of ACL in support of other technologies, and as a form of security are required to be understood, and as such common forms of ACL solutions are introduced.

Objectives

Upon completion of this section, trainees will be able to:

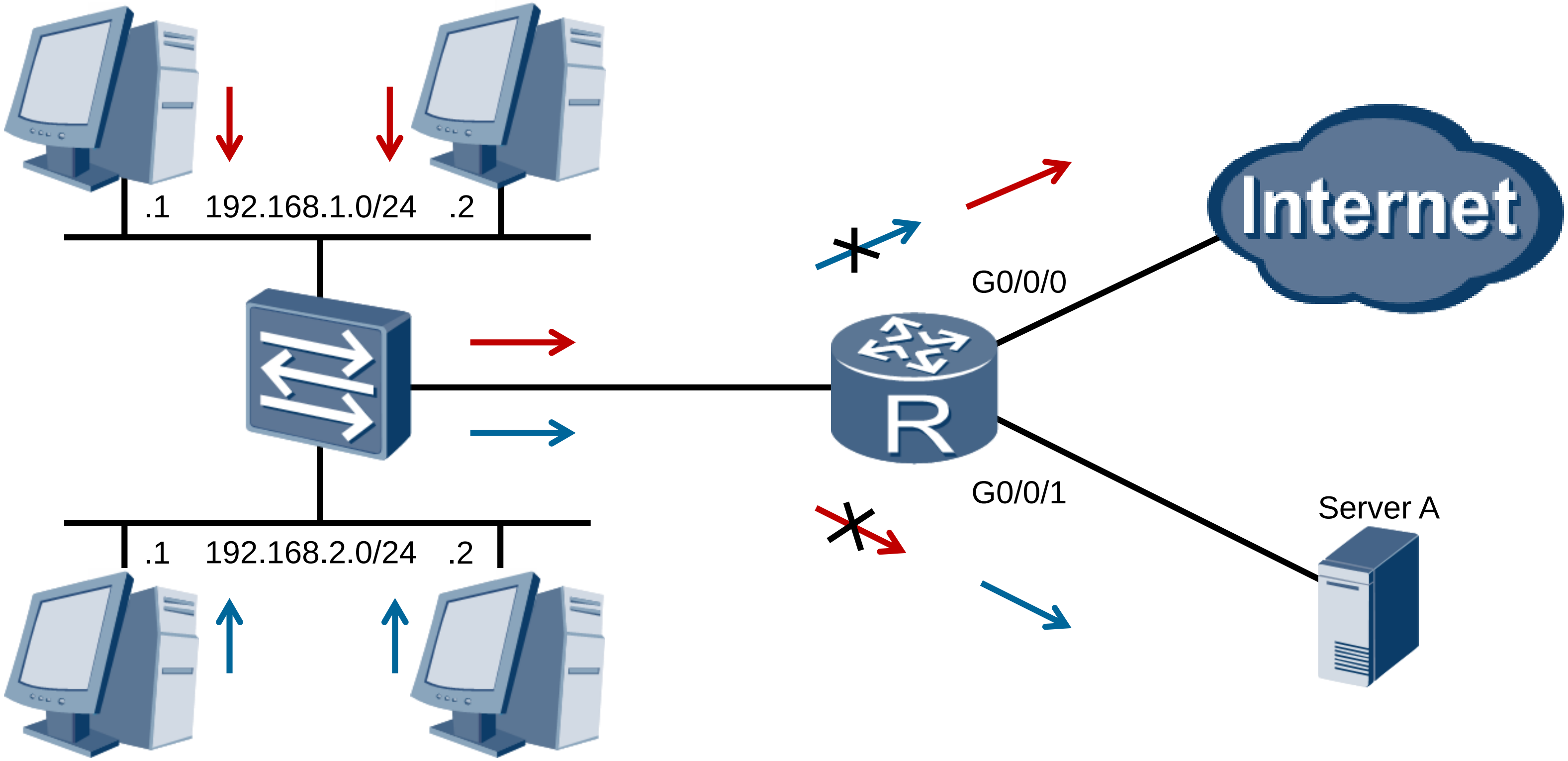
- Describe the applications for ACL in the enterprise network.
- Explain the decision making behavior of Access Control Lists.
- Successfully implement Basic and Advanced Access Control Lists.

ACL

Utilizzate per:

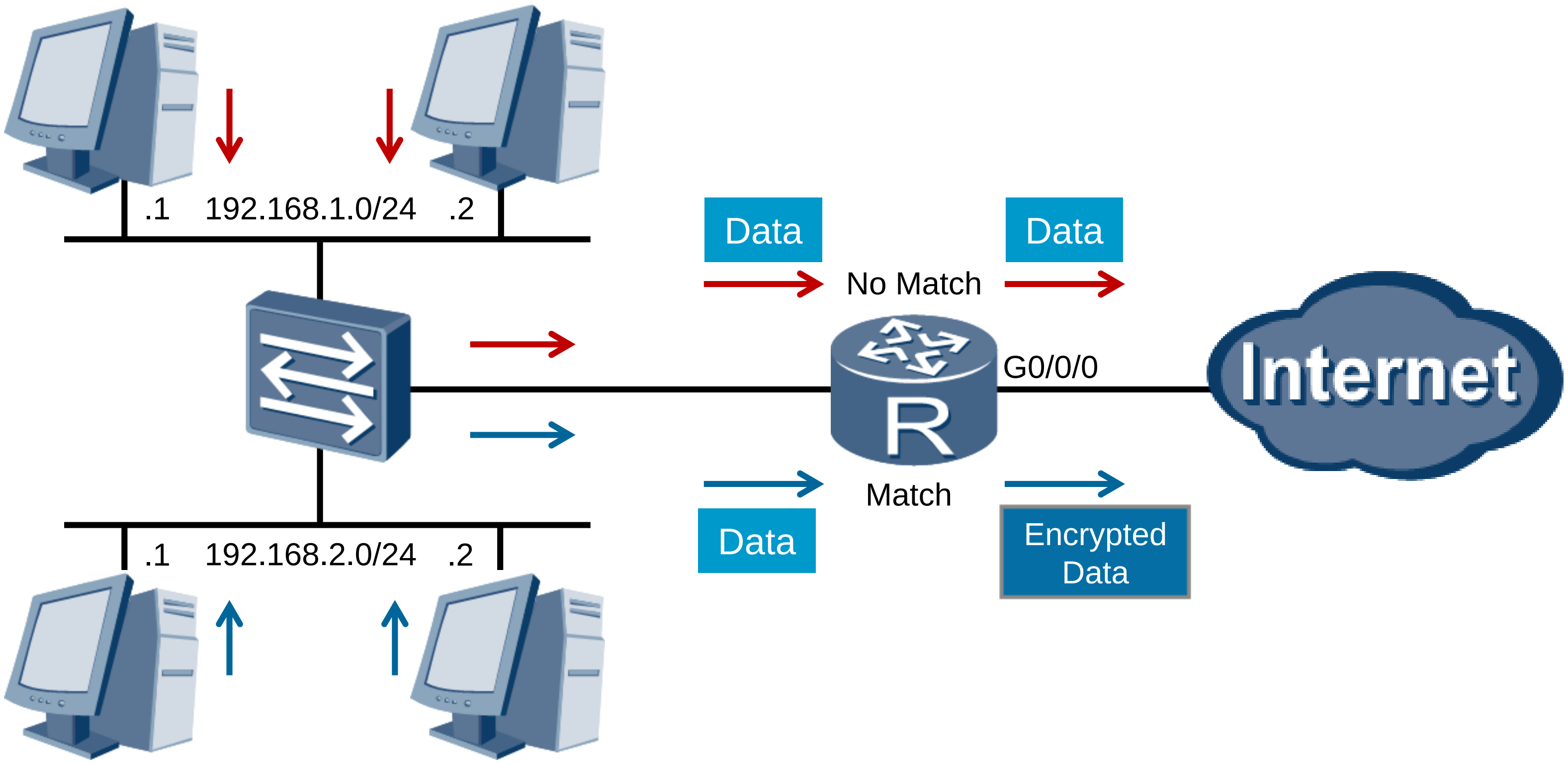
- **Filtrare** – **Classificare** – **Selezionare** dei pacchetti in INGRESSO o in USCITA da una interfaccia di rete.
- Due step :
  - Matching del pacchetto sulla ACL;
  - Esecuzione dell’operazione sul pacchetto che ha effettuato il match.

Filtering **Restricted** Traffic



- Packets are filtered based on addresses and parameters.
- Rules allow packets to be either permitted or denied.

Filtering **Interesting** Traffic



- Packets can be filtered to manipulate behavior and actions.
- Parameters and forwarding behavior can be altered as a result.

ACL Types

Types	Value Ranges	Parameters
Basic	2000-2999	Source IP
Advanced	3000-3999	Source & Destination IP, Protocol, Source & Destination Port
Layer 2 ACL	4000-4999	MAC Address

- Three forms of ACL can be applied to AR2200 series routers.
- Parameters for packet filtering vary for each ACL type.

ACL Rule Management

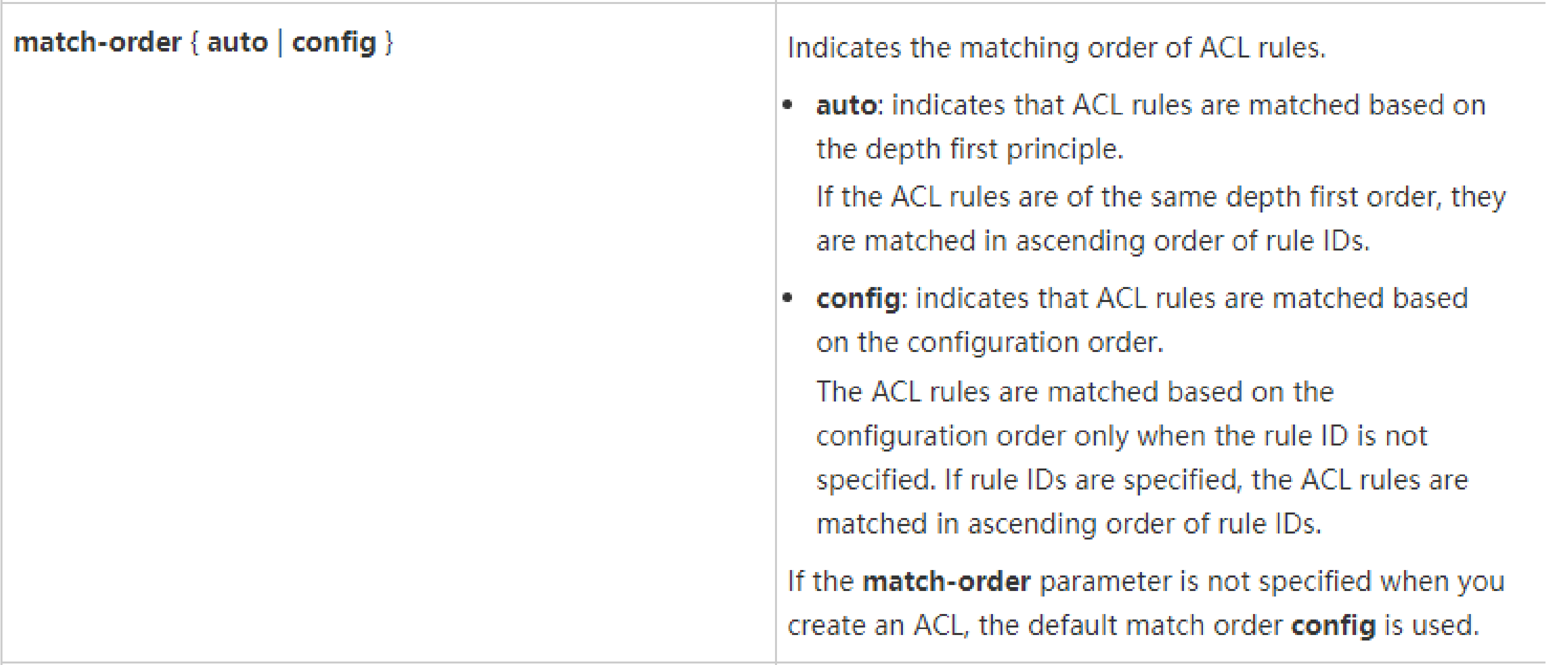
Configuration order:

- Le ACL vengono controllate per ID crescente;
- Modalità predefinita.

Automatic order:

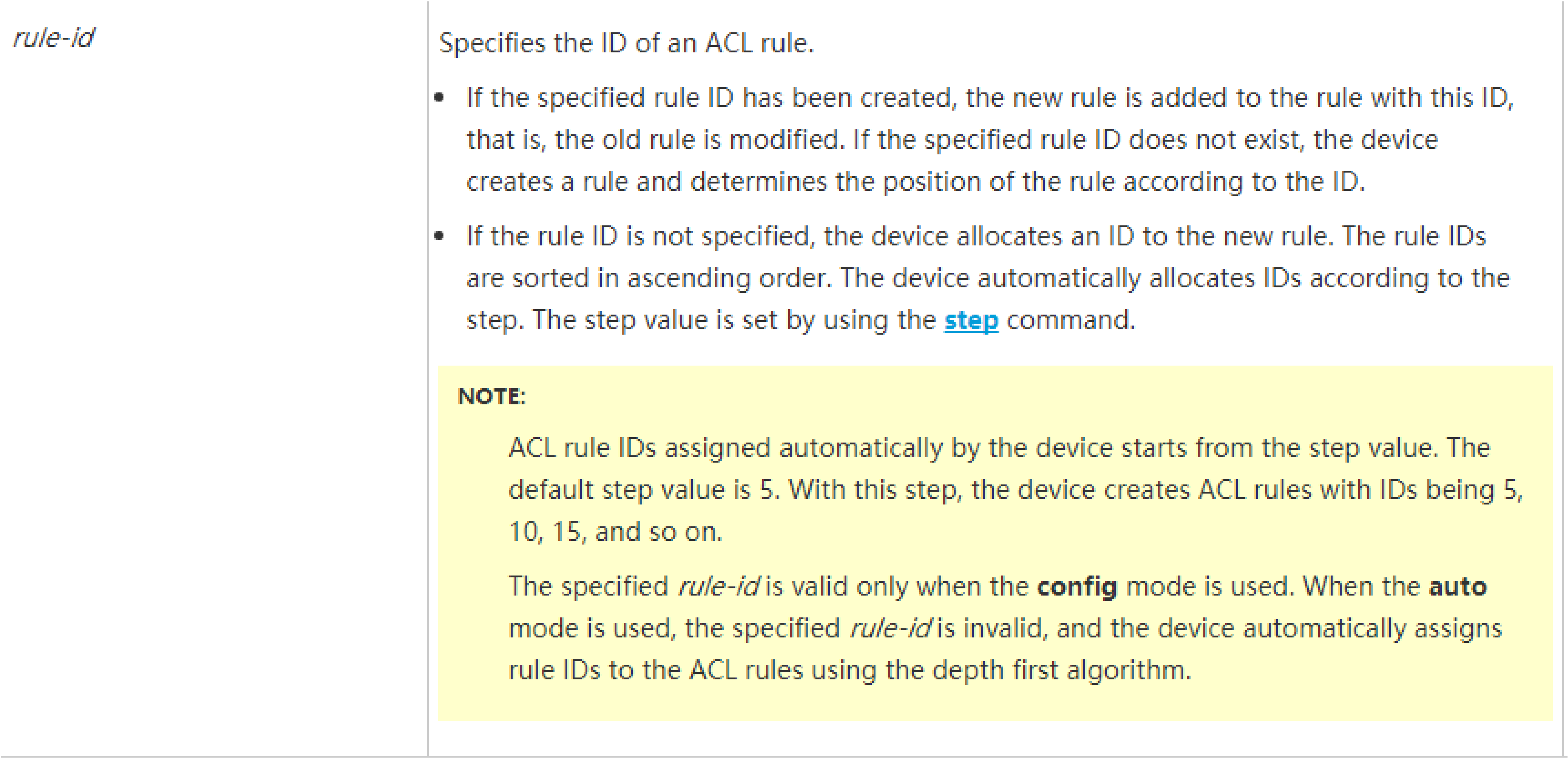
- Depth first principle;
- Le regole più accurate sono controllate per prime;

ACL Rule Management



match-order { **auto** | **config** }	Indicates the matching order of ACL rules. - **auto**: indicates that ACL rules are matched based on the depth first principle. If the ACL rules are of the same depth first order, they are matched in ascending order of rule IDs. - **config**: indicates that ACL rules are matched based on the configuration order. The ACL rules are matched based on the configuration order only when the rule ID is not specified. If rule IDs are specified, the ACL rules are matched in ascending order of rule IDs. If the **match-order** parameter is not specified when you create an ACL, the default match order **config** is used.

ACL Rule Management



rule-id	Specifies the ID of an ACL rule. • If the specified rule ID has been created, the new rule is added to the rule with this ID, that is, the old rule is modified. If the specified rule ID does not exist, the device creates a rule and determines the position of the rule according to the ID. • If the rule ID is not specified, the device allocates an ID to the new rule. The rule IDs are sorted in ascending order. The device automatically allocates IDs according to the step. The step value is set by using the **step** command. **NOTE:** ACL rule IDs assigned automatically by the device starts from the step value. The default step value is 5. With this step, the device creates ACL rules with IDs being 5, 10, 15, and so on. The specified *rule-id* is valid only when the **config** mode is used. When the **auto** mode is used, the specified *rule-id* is invalid, and the device automatically assigns rule IDs to the ACL rules using the depth first algorithm.

ACL Rule Management

Wildcard Mask

- Metodo per comunicare al SO quali parti di un indirizzo debbono essere ignorate quando si esegue un confronto.
  - 0: viene effettuato il confronto;
  - 1: viene ignorato.
- Analoga al caso di OSPF;

ACL Rule Management

Wildcard Mask – Calcolo rapido

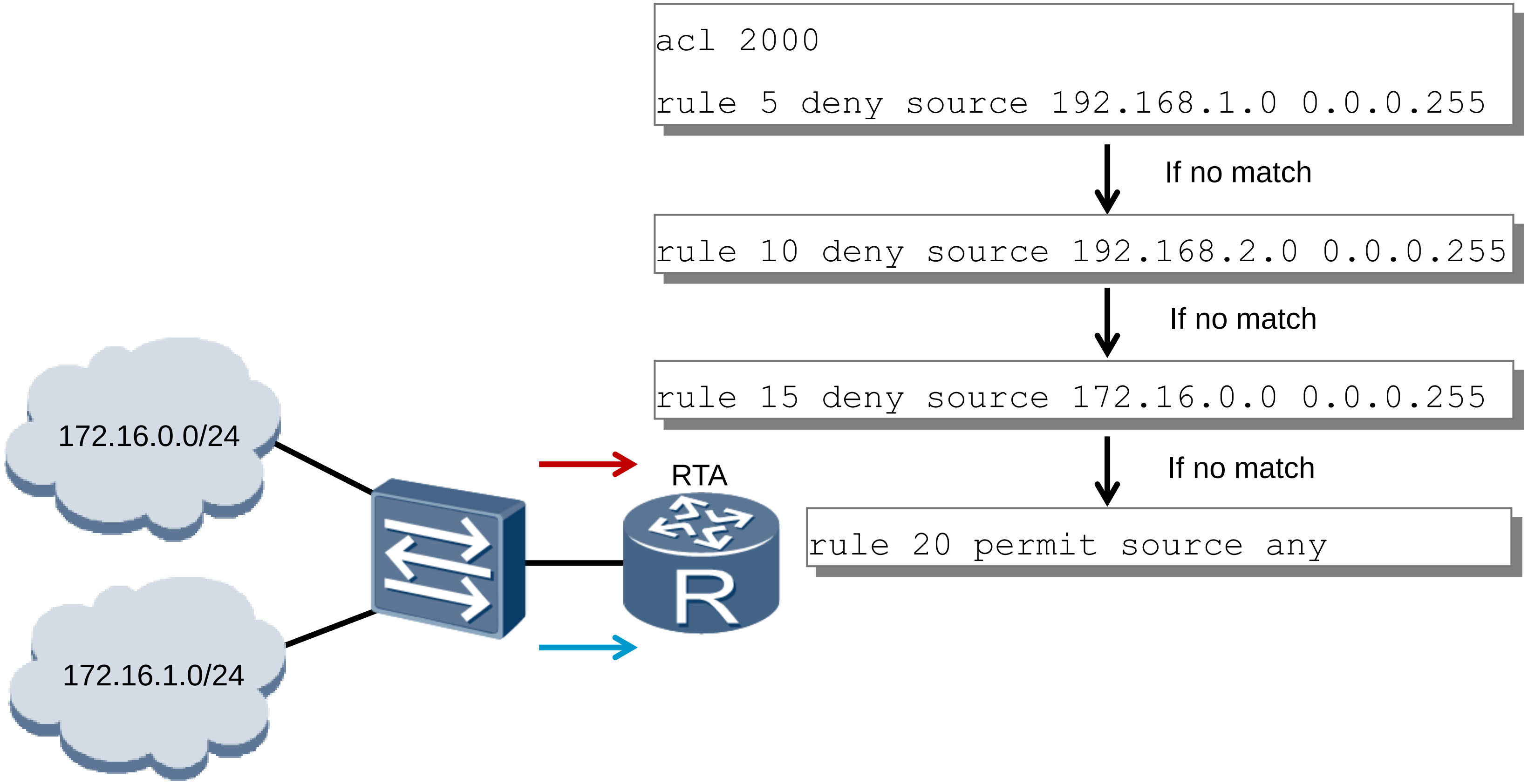
- Data una sottorete es: 172.16.8.0 255.255.252.0 determinare la wildcard mask che ne consente il match.
- La sottorete viene riscritta nello stesso modo: 172.16.8.0
- La wildcard mask viene calcolata:

  255.255.255.255 –

  255.255.252.0 =

  0 . 0 . 3 . 255

ACL Rule Management



```
acl 2000
rule 5 deny source 192.168.1.0 0.0.0.255
rule 10 deny source 192.168.2.0 0.0.0.255
rule 15 deny source 172.16.0.0 0.0.0.255
rule 20 permit source any
```

- Rules are used to manage the decision process for each ACL.

ACL Rule Management – Importante!!!

Le ACL in questo corso sono utilizzate prevalentemente per:

- traffic-filter;
- traffic-classifier;

Il comportamento di VRP riguardo al caso in cui un pacchetto non riesca ad effettuare il match con alcuna regola è il seguente:

- traffic-filter -> implicit permit;
- traffic-classifier -> implicit deny (esempio: NAT);

Basic ACL

Sintassi Basic ACL

rule [rule-id] { deny | permit } [source { source-address source-wildcard | any } | logging] *

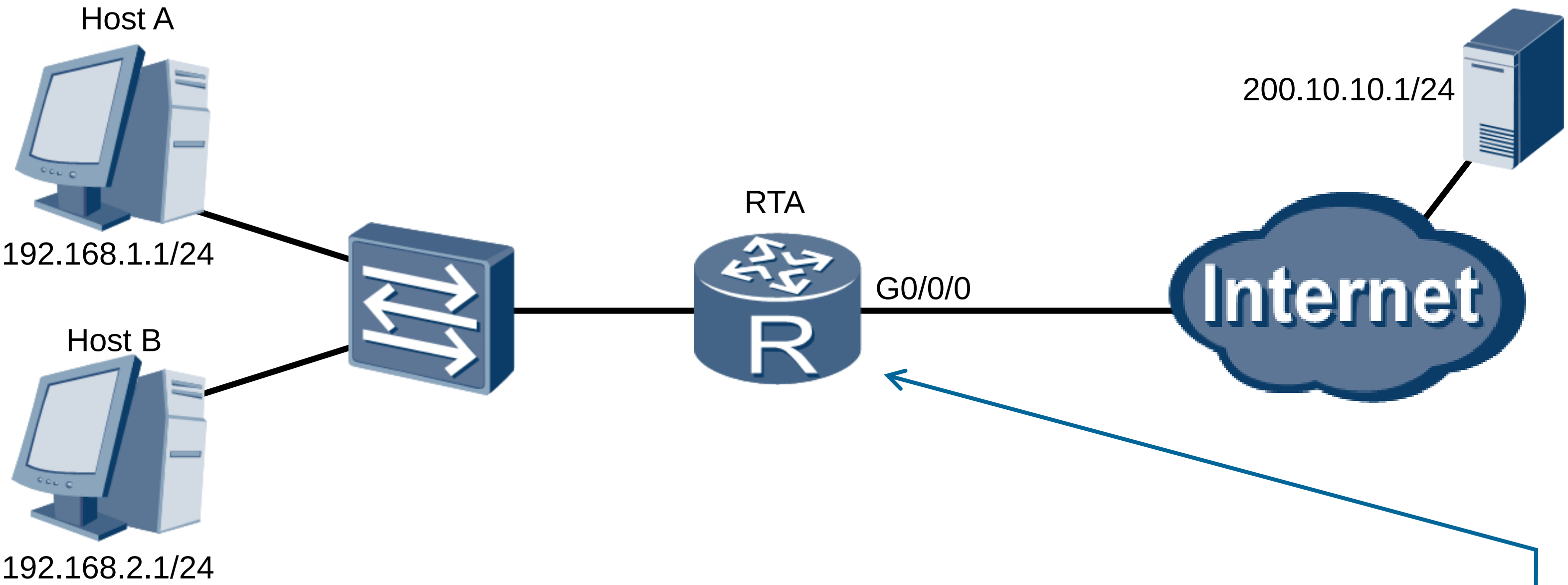
Source: ANY -> indicates any source IP address of packets

il source IP è 0.0.0.0 o la source wildcard è 255.255.255.255

Esempio:

rule 5 permit source 192.168.32.1 0

Basic ACL



```
[RTA]acl 2000
[RTA-acl-basic-2000]rule deny source 192.168.1.0 0.0.0.255
[RTA-acl-basic-2000]rule permit source 192.168.2.0 0.0.0.255
[RTA]interface GigabitEthernet 0/0/0
[RTA-GigabitEthernet0/0/0]traffic-filter outbound acl 2000
```

Configuration Validation

```
Host A> ping 200.10.10.1
Ping 200.10.10.1: 32 data bytes, Press Ctrl_C to break
Request timeout!
Request timeout!
Request timeout!
...
```

```
[RTA]display acl 2000
Basic ACL 2000, 2 rules
Acl's step is 5
 rule 5 deny source 192.168.1.0 0.0.0.255 (5 matches)
 rule 10 permit source 192.168.2.0 0.0.0.255
```

- The rules and matching order can be verified for each ACL.
- Basic ACL rules are matched based on each source IP address.

Advanced ACL

Sintassi advanced ACL

Varia a seconda del protocollo che viene indicato:

ICMP – TCP – UDP – GRE – OSPF – etc.

Caso TCP

```
rule [ rule-id ] { deny | permit } { protocol-number | tcp }
[ destination { destination-address destination-wildcard | any } |
destination-port { eq port | gt port | lt port | range port-start port-
end } | source { source-address source-wildcard | any } | source-
port { eq port | gt port | lt port | range port-start port-end } | tcp-flag
{ ack | fin | psh | rst | syn | urg | established }  | logging ]
```

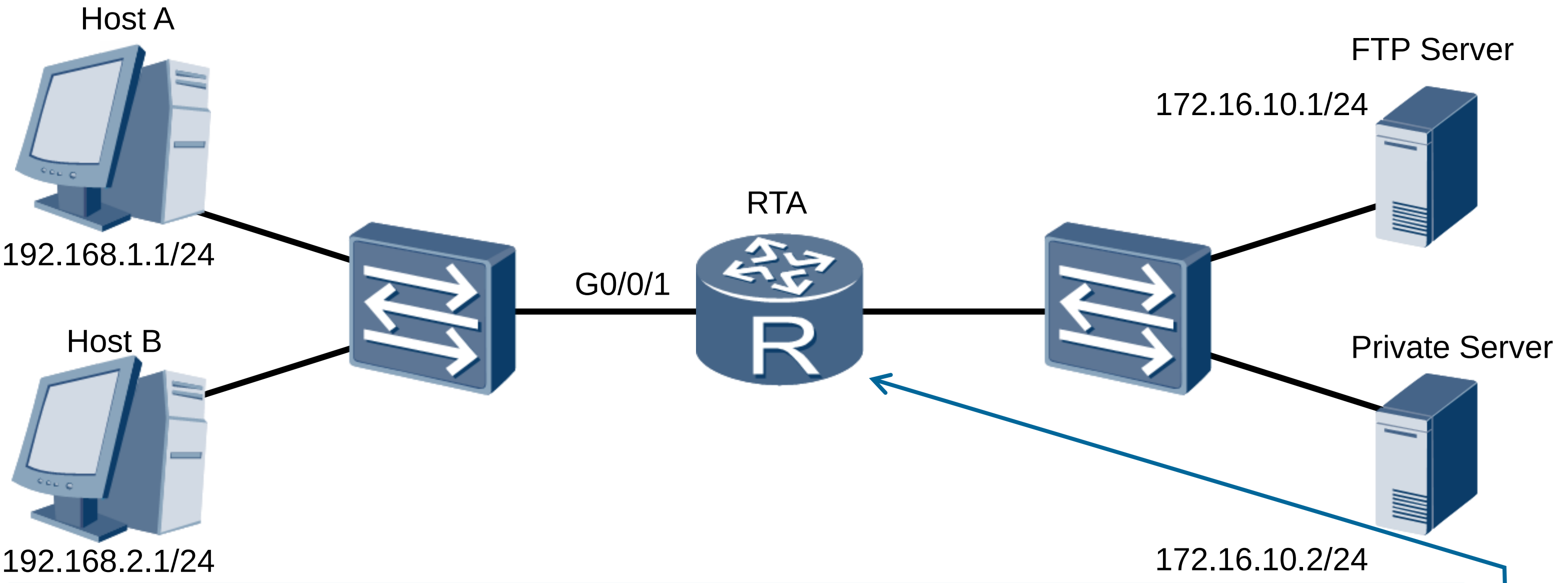
Advanced ACL

Sintassi advanced ACL

Caso UDP

rule [rule-id] { deny | permit } { protocol-number | udp } [destination { destination-address destination-wildcard | any } | destination-port { eq port | gt port | lt port | range port-start port-end } | source { source-address source-wildcard | any } | source-port { eq port | gt port | lt port | range port-start port-end } | logging]

Advanced ACL



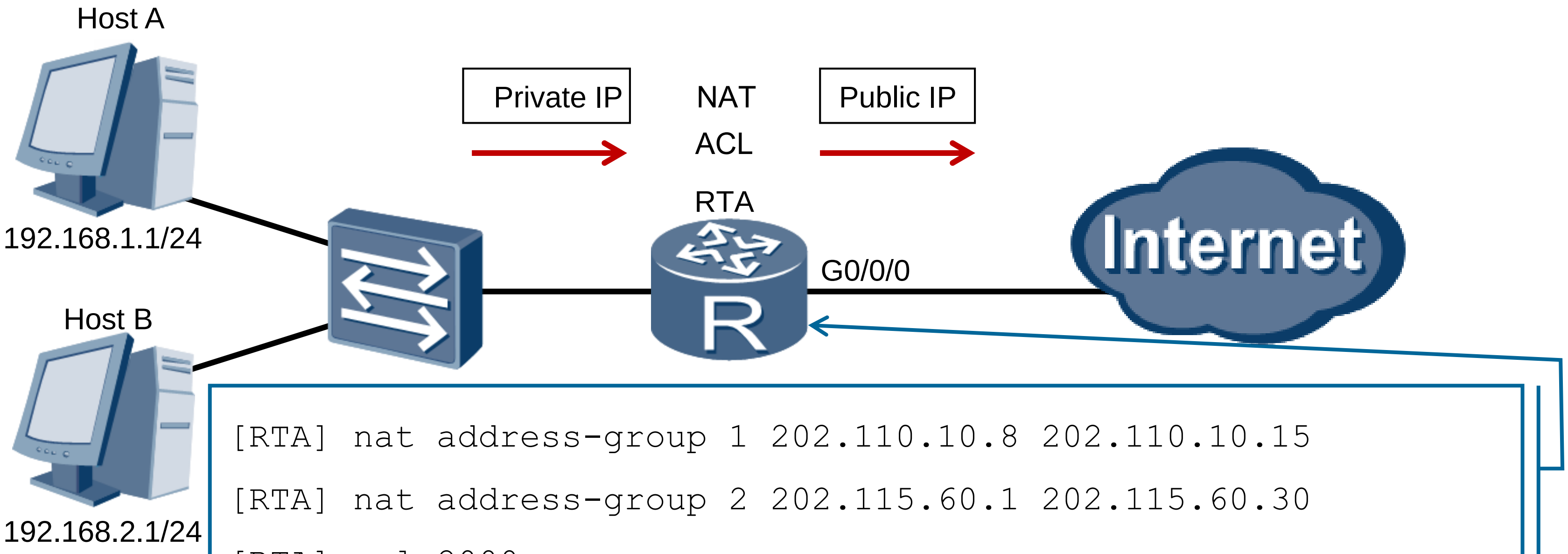
```
[RTA]acl 3000 match-order auto
[RTA-acl-adv-3000]rule deny tcp source 192.168.1.0 0.0.0.255
destination 172.16.10.1 0.0.0.0 destination-port eq 21
[RTA-acl-adv-3000] rule deny ip source 192.168.2.0 0.0.0.255
destination 172.16.10.2 0.0.0.0
[RTA-GigabitEthernet0/0/1]traffic-filter inbound acl 3000
```

Configuration Validation

```
[RTA]display acl 3000
Advanced ACL 3000, 2 rules
Acl's step is 5
rule 5 deny tcp source 192.168.1.0 0.0.0.255 destination 172.16.10.1 0
destination-port eq ftp
rule 10 deny ip source 192.168.2.0 0.0.0.255 destination 172.16.10.2 0
```

- Advanced ACL rules defined in the range of 3000-3999 add complexity due to the number of parameters used for filtering.

ACL Application - NAT



```
[RTA] nat address-group 1 202.110.10.8 202.110.10.15
[RTA] nat address-group 2 202.115.60.1 202.115.60.30
[RTA] acl 2000
[RTA-acl-basic-2000] rule permit source 192.168.1.0 0.0.0.255
[RTA] acl 2001
[RTA-acl-basic-2001] rule permit source 192.168.2.0 0.0.0.255
[RTA] interface GigabitEthernet 0/0/0
[RTA-GigabitEthernet0/0/0] nat outbound 2000 address-group 1
[RTA-GigabitEthernet0/0/0] nat outbound 2001 address-group 2
```

Nota bene!

Le regole di traffic filter vengono applicate subito prima che il pacchetto lasci l’interfaccia.

Pertanto se sulla stessa interfaccia insiste un NAT &&

un TRAFFIC-FILTER, viene eseguito prima il nat e poi il filter.

Attenzione quindi agli IP considerati! Il filter non conosce il mapping degli IP privato-pubblico e viceversa,

ma si applica solamente agli IP risultanti dal mapping!!!!!

Buone Pratiche

Regole generali di configurazione delle ACL:

- Le **ACL estese** debbono essere configurate **il più vicino possibile alla sorgente** dei pacchetti che vogliamo filtrare. In questo modo viene generato meno traffico;
- Le **ACL standard** debbono essere configurate **il più vicino possibile alla destinazione** dei pacchetti. Sono delle ACL molto generiche e in questo modo si evitano errori nel filtraggio del traffico;
- Le regole più specifiche debbono essere configurated per prime nella ACL;
- Le ACL possono rendere il troubleshooting MOLTO COMPLESSO!

Troubleshooting

Cosa controllare in caso di problemi?

- Determinare su quale interfaccia è impostata la ACL e la direzione;
- Controlllare attentamente:
  - Il corretto ordinamento delle regole;
  - Che non siano stati scambiati gli indirizzi di sorgente/destinazione;
  - Che non siano stati fatti errori di sintassi (soprattutto nella defizione dei protocolli);
- Le ACL in ingresso non debbono bloccare i protocolli di routing;

Thank you

www.huawei.com