Clase X

Interconexión de redes de datos (IRD101)

Agenda

- Configuración, verificación y detección de fallos DHCP en un router.
- Listas de control de acceso.

Introducción Protocolo DHCP

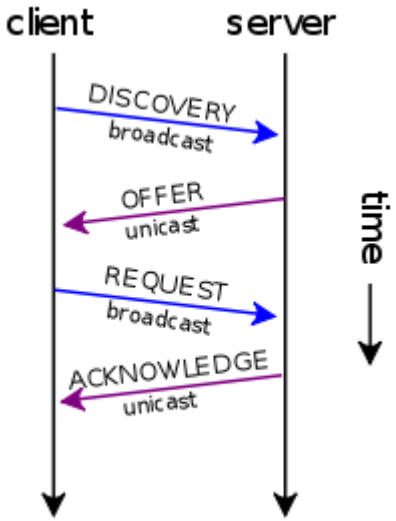
El protocolo de configuración dinámica de host (DHCP) es utilizado por workstations (hosts) para obtener su información de configuración inicial: dirección IP, máscara de subred, default gateway y servidor DNS, etc. Se encuentra definido en el RFC2131.

DHCP utiliza un modelo cliente servidor donde uno o más servidores DHCP brindan la información solicitada a los hosts.

Utiliza los puertos 67 (UDP) y 68 (UDP).

Introducción Protocolo DHCP

Sesión típica DHCP



DHCPDISCOVER

- El cliente busca a los servidores DHCP disponibles.

DHCPOFFER

- Un servidor DHCP disponible le responde al cliente.

DHCPREQUEST

- El cliente solicita al servidor los parámetros de red necesarios.

DHCPACK

- El servidor le responde al cliente con los parámetros de red necesarios.

Introducción Protocolo DHCP

Los parámetros de configuración son arrendados (leased) por el cliente al servidor por un periodo de tiempo específico.

Si se requiere que el servicio DHCP sea proporcionado por un equipo remoto se utiliza el siguiente comando aplicado a una interfaz:

```
ip helper-address remote_DCHP_server_IP
```

Configuración DHCP en router.

Los comandos básicos para configuración de DHCP son los siguientes:

```
Router(config)# dhcp pool ciudadela
Router(dhcp-config)#network 192.168.1.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.1.1
Router(dhcp-config)#dns-server 8.8.8.8
Router(dhcp-config)#domain-name udb.local
Router(dhcp-config)exit
Router(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.4
```

Configuración DHCP en router.

La configuración anterior permite configurar un pool DHCP denominado “ciudadela” que entregará direcciones IP correspondientes a la red 192.168.1.0/24, con una puerta de enlace predeterminada 192.168.1.1, un servidor DNS 8.8.8.8, pertenecientes al dominio “udb.local” y excluyendo el siguiente rango de direcciones IP del leasing: 192.168.1.1 a 192.168.1.4

Verificación y detección de fallos

Se tienen los siguientes comandos que son útiles para resolución de problemas:

```
HQ-RT#show ip dhcp binding
IP address       Client-ID/              Lease expiration        Type
                 Hardware address
10.0.1.11        000B.BE95.6256           --                     Automatic
10.0.1.12        0010.1185.D481           --                     Automatic
10.0.1.13        0006.2A5D.B172           --                     Automatic
10.0.1.14        000C.CFE7.B019           --                     Automatic
10.0.2.11        0090.0CED.A63D           --                     Automatic
10.0.2.12        000A.F336.A582           --                     Automatic
10.0.3.11        0006.2AC2.E463           --                     Automatic
10.0.3.12        0009.7C62.0136           --                     Automatic
```

Muestra la asignación de IP proporcionada por un servidor DHCP.

Verificación y detección de fallos

Muestra información relacionada con los pools de direcciones por DHCP.

```
HQ-RT#show ip dhcp pool

Pool HQ :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 4
 Excluded addresses             : 3
 Pending event                  : none

 1 subnet is currently in the pool
 Current index        IP address range                    Leased/Excluded/Total
 10.0.1.1             10.0.1.1         - 10.0.1.254        4    / 3     / 254
```

```
C:\>ipconfig /all

Windows 2000 IP Configuration

  Host Name . . . . . . . . . . . . : PC
  Primary DNS Suffix . . . . . . . : cisco.com
  Node Type . . . . . . . . . . . . : Hybrid
  IP Routing Enabled. . . . . . . . : No
  WINS Proxy Enabled. . . . . . . . : No
  DNS Suffix Search List. . . . . . : cisco.com

Ethernet adapter Local Area Connection :

  Connection-specific DNS Suffix . : Central
  Description . . . . . . . . . . . : 3Com EtherLink XL 10/100 PCI TX NIC(3C905B-TX)
  Physical Address. . . . . . . . . : 00-10-5A-86-5A-CA
  DHCP Enabled. . . . . . . . . . . : Yes
  Autoconfiguration Enabled . . . . : Yes
  IP Address. . . . . . . . . . . . : 192.168.1.2
  Subnet Mask . . . . . . . . . . . : 255.255.255.248
  Default Gateway . . . . . . . . . : 192.168.1.1
  DHCP Server . . . . . . . . . . . : 10.0.0.6
  DNS Servers . . . . . . . . . . . : 10.0.0.2
  Primary WINS Server . . . . . . . : 10.0.0.2
  Lease Obtained. . . . . . . . . . : Tuesday, April 26, 2005 6:04:29 PM
  Lease Expires . . . . . . . . . . : Wednesday, April 27, 2005 6:04:29 PM
```

Listas de control de acceso

Las listas de control de acceso (ACLs) permiten a los especialistas de red filtrar el tráfico manejado por un router. Cada ACL le define al router que paquetes debe descartar y cuales debe procesar.

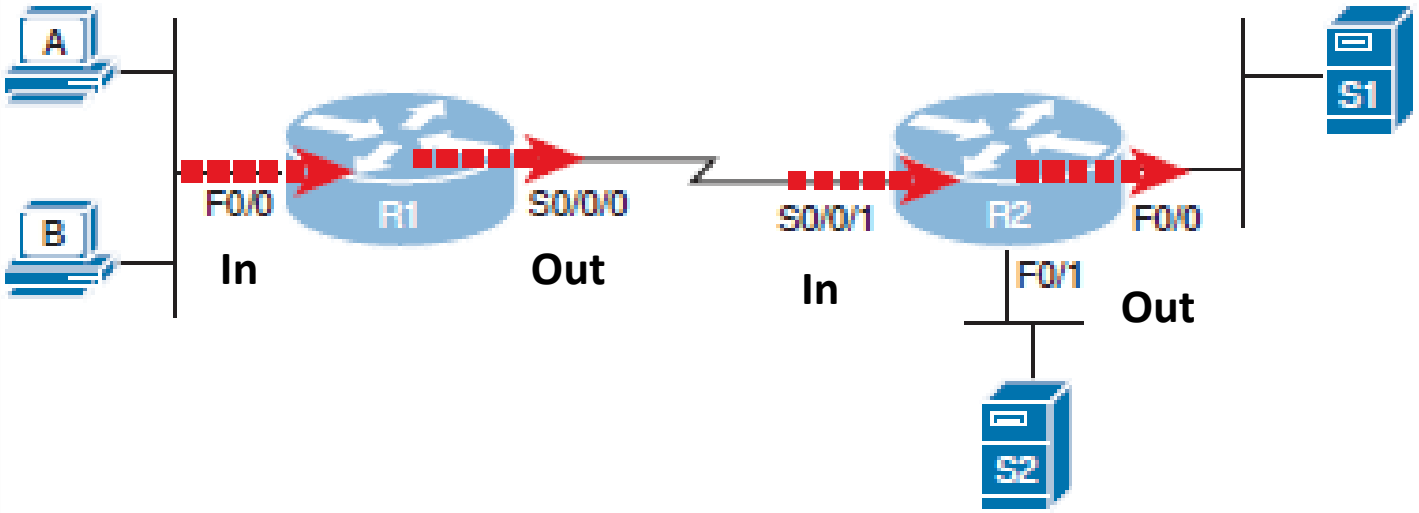
Existen dos tipos:

- Listas de acceso estándar.
- Listas de acceso extendidas.

ACLs: Ubicación y dirección.

Las ACLs son aplicadas en el punto de ingreso de los paquetes a una interfaz o en el punto de salida. En otras palabras, la ACL se asocia con una interfaz y un flujo de paquetes (ya sea de entrada o de salida).

ACLs: Ubicación y dirección.

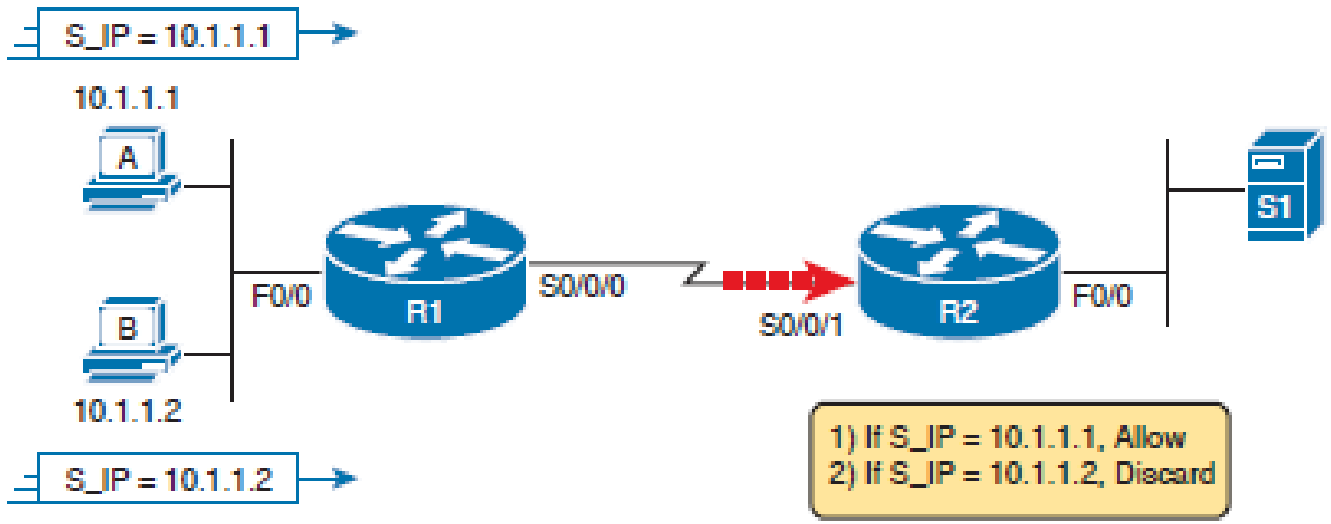


Interface	Device	Direction
F0/0	R1	Inbound
S0/0/0	R1	Outbound
S0/0/1	R2	Inbound
F0/0	R2	Outbound

Las flechas indican las posiciones y el sentido de las ACLs que pudiesen ser utilizadas para filtrar el tráfico originado desde host A hacia S1.

ACLs: Selección de paquetes.

Después de conocer la ubicación y el sentido de las ACLs se debe indicar al router que tipo de paquetes se requieren sean filtrados y las acciones a aplicar.



Acciones.

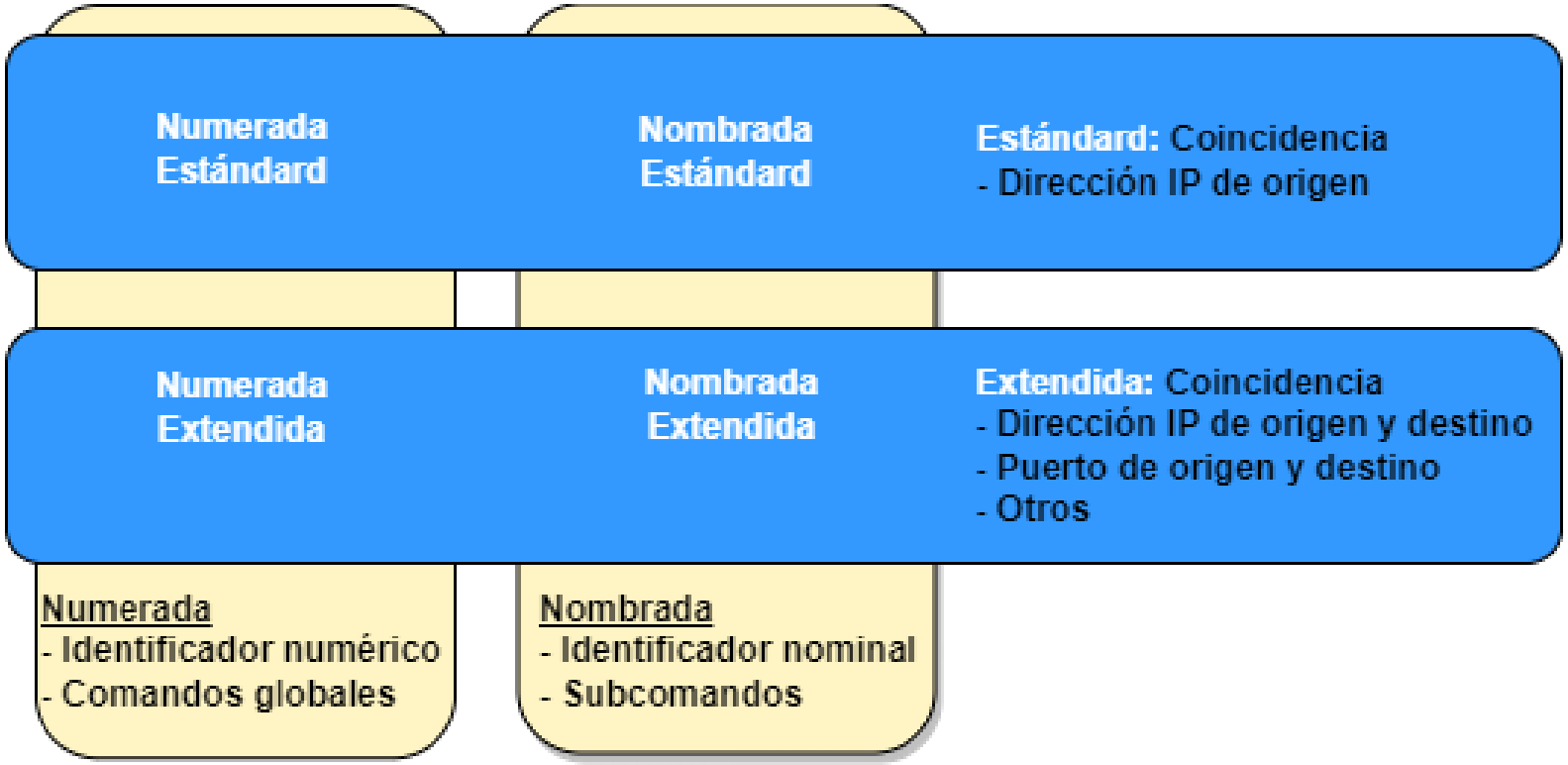
Allow -> **Permit**
Discard -> **Deny**

ACLs: Tipos

Se tienen principalmente los siguientes tipos de ACLs:

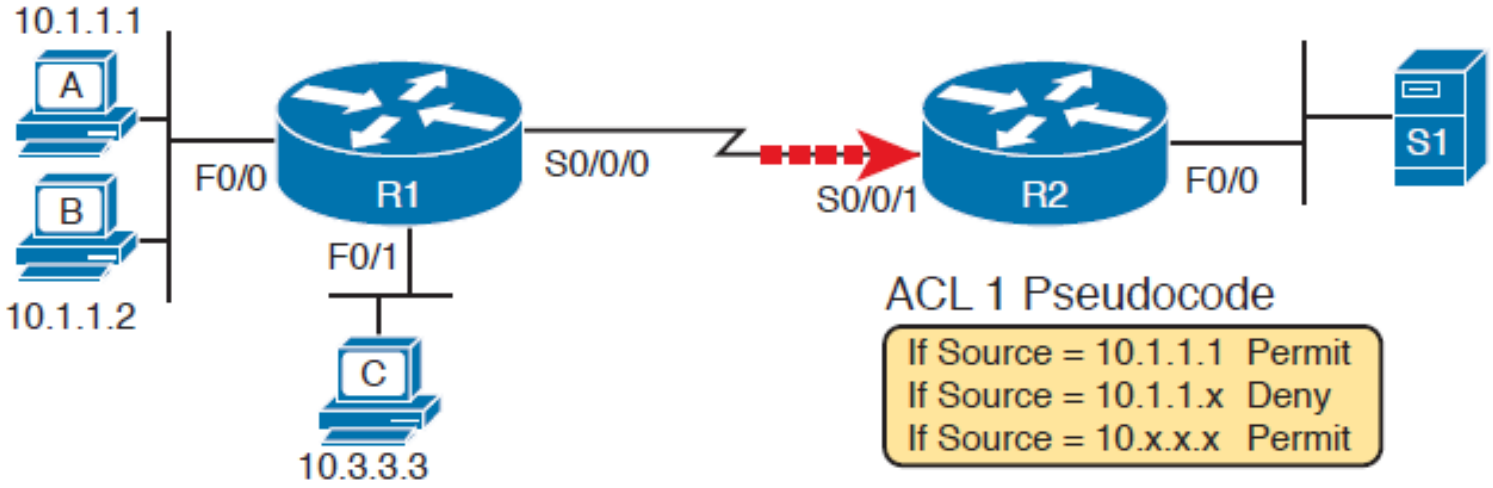
- ACLs estándar numeradas (1-99)
- ACLs extendidas numeradas (100-199)
- ACLs nombradas

ACLs: Comparación de tipos



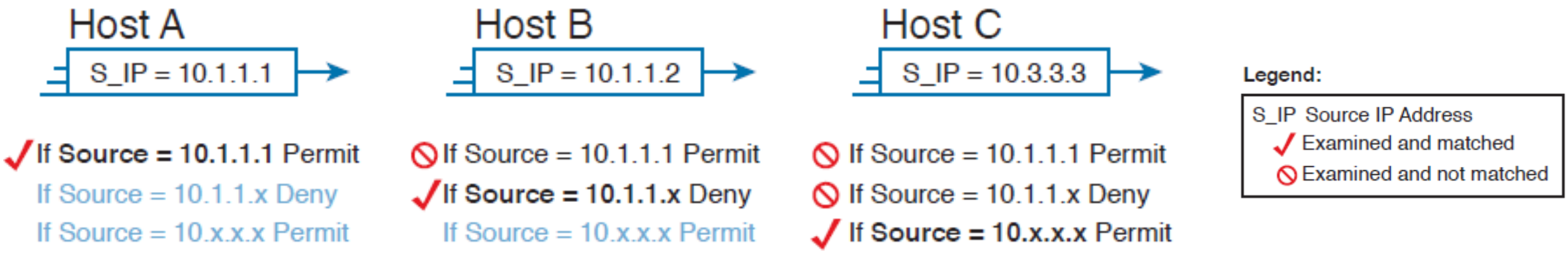
ACLs estándar numeradas.

Ejemplo 1: Consideremos el siguiente escenario donde se ha aplicado un filtro de tráfico en la interface S0/0/1 en dirección inbound.



ACLs estándar numeradas.

Primero se realizará match (coincidencia) con la condición más específica del filtro, sino se continuarán evaluando las demás condiciones. Para la comunicación entre A,B,C y S1 se tendrán los siguientes resultados:



ACLs estándar numeradas.

Si no aplica ninguna de las condiciones, el paquete será descartado debido a que se aplicará una condición de ***deny all*** implícito.

La sintaxis de la ACL es la siguiente:

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

ACLs estándar numeradas.

Cada lista de acceso estándar numerada puede tener uno o más comandos de *access-list* con el mismo número (un número no es mejor que otro).

Luego se evalúan las acciones (permit o deny) y finalmente se examinan las condiciones relacionados con el encabezado del paquete de origen.

Una ACL estándar sólo hace match con la dirección IP de origen o porciones de la red de origen delimitadas por la máscara wildcard.

Máscara Wildcard.

Para obtener una máscara wildcard simplemente se invierten los bits correspondientes a la máscara de subred de la siguiente forma:

Subnet Mask Bits	11111111.11110000.00000000.00000000
Wildcard Mask Bits	00000000.00001111.11111111.11111111

Máscara Wildcard.

Luego convertir el resultado a formato decimal punteado, a continuación unos ejemplos:

Máscara de subred	Máscara Wildcard
255.255.255.0	0.0.0.255
255.255.0.0	0.0.255.255
255.255.252.0	0.0.3.255
255.240.0.0	0.15.255.255

Máscara Wildcard.

También se tiene la siguiente alternativa de restarle a 255.255.255.255 el valor de la máscara de subred para obtener el valor de la máscara wildcard, de la siguiente forma:

```
  255.255.255.255
- 255.255.252.0
-----------------
    0.   0.   3. 255
```

ACLs estándar numeradas.

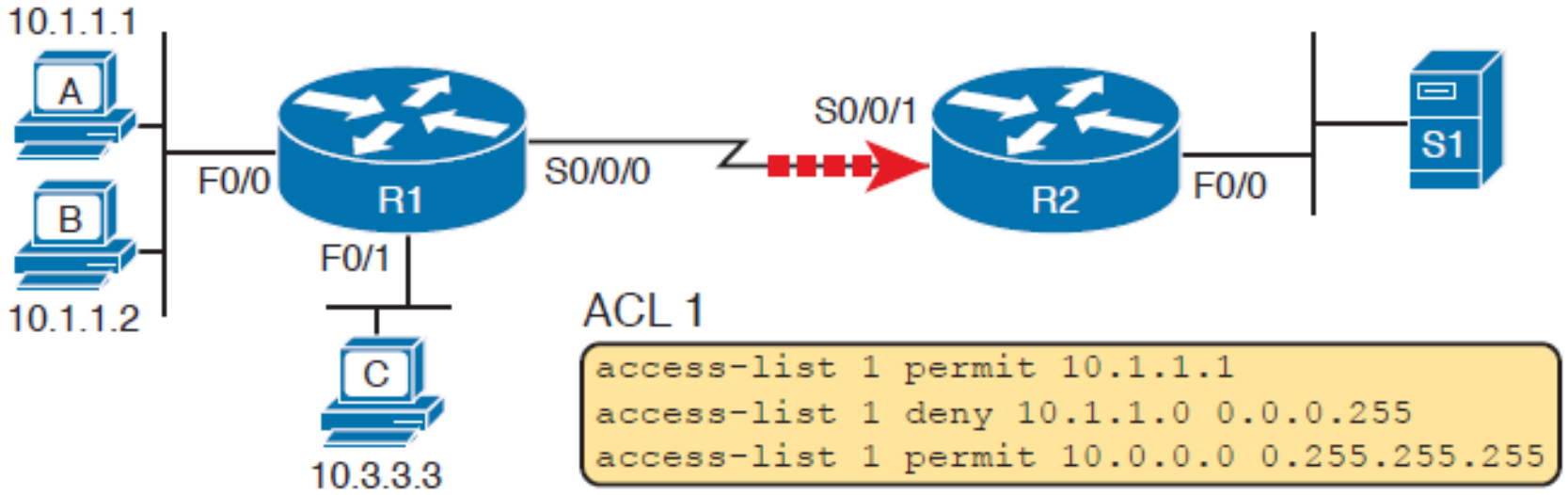
Para el ejemplo 1 la definición de una de las sentencias de la ACL es:

```
access-list 1 permit 10.1.1.1
```

Cuando se requiere que el match de la ACL no se aplique solamente a una dirección IP sino red completa o a una porción de una red se utiliza una herramienta denominada: ***máscara wildcard***.

ACLs estándar numeradas.

Retomando el ejemplo 1, la definición de las ACLs quedará definida de la siguiente forma:



ACLs estándar numeradas.

Donde la interpretación de la ACL1 es la siguiente:

- **Línea 1:** Match y permitir para todos los paquetes que coincidan exactamente con la dirección IP de origen 10.1.1.1
- **Línea 2:** Match y denegar todos los paquetes cuya dirección de origen coincida en sus primeros tres octetos con 10.1.1
- **Línea 3:** Match y permitir todas las direcciones de origen cuyo primer octeto tenga el valor de 10.

Implementación de ACLs estándar.

La sintaxis genérica es la siguiente:

```
access-list access-list-number {deny | permit} source [source-wildcard]
```

Paso 1: Planificar la ubicación (router e interfaz) y la dirección (entrada o salida):

a) Las ACLs estándar deben ser colocadas lo más cercano posible del destino para que evitar que otros paquetes sean descartados de forma no intencional.

b) Debido a que las ACLs solo pueden hacer match con las direcciones IP de origen, identificar la dirección IP de origen de los paquetes que vayan hacia la dirección que la ACL examinará.

Implementación de ACLs estándar.

Paso 2: Configurar uno o más comandos para conformar la ACL, teniendo en cuenta lo siguiente:

a) La lista se evaluará de forma secuencial, utilizando la lógica del primer match.

b) La acción por defecto, si el paquete no hace match con ninguna de las condiciones de la ACL es **deny** (descartar) el paquete.

Paso 3: Habilitar la ACL en la interfaz seleccionada, en la dirección correcta, utilizando el subcomando de interfaz **ip access-group *number* {in | out}**

Implementación de ACLs estándar.

Finalmente para el ejemplo 1, los comandos para la aplicación de la ACL quedarían definidos de la siguiente forma:

```
R2# configure terminal
R2(config)# access-list 1 permit 1.1.1.1
R2(config)# access-list 1 deny 10.1.1.0 0.0.0.255
R2(config)# access-list 1 permit 10.0.0.0 0.255.255.255
R2(config)# interface S0/0/1
R2(config-if)# ip access-group 1 in
```

Implementación de ACLs estándar.

Para la verificación de la ACL se utilizan los siguientes comandos:

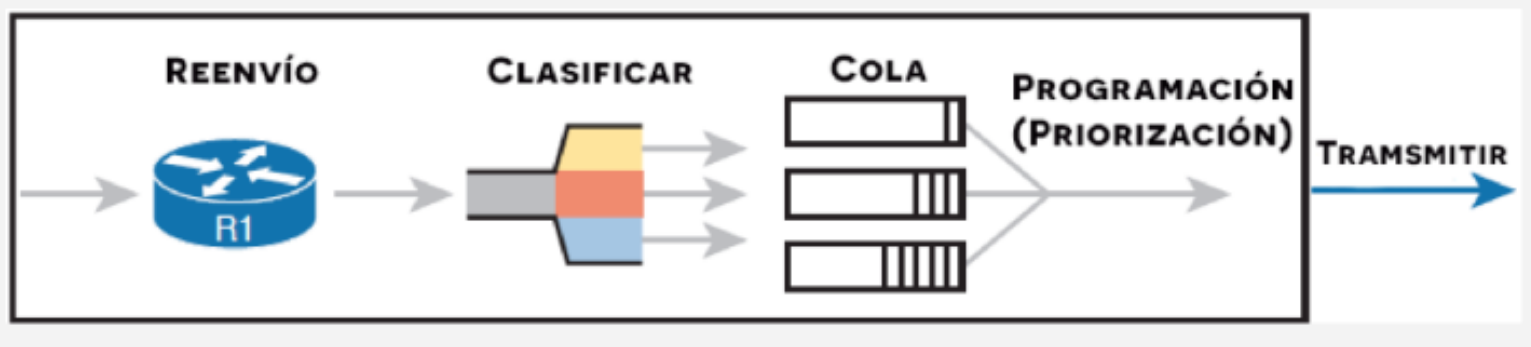
```
R2# show ip access-lists
Standard IP access list 1
    10 permit 10.1.1.1 (107 matches)
    20 deny   10.1.1.0, wildcard bits 0.0.0.255 (4 matches)
    30 permit 10.0.0.0, wildcard bits 0.255.255.255 (10 matches)
R2# show access-lists
Standard IP access list 1
    10 permit 10.1.1.1 (107 matches)
    20 deny   10.1.1.0, wildcard bits 0.0.0.255 (4 matches)
    30 permit 10.0.0.0, wildcard bits 0.255.255.255 (10 matches)
```

Implementación de ACLs estándar.

```
R2# show ip interface s0/0/1
Serial0/0/1 is up, line protocol is up
  Internet address is 10.1.2.2/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.9
  Outgoing access list is not set
  Inbound  access list is 1
! Lines omitted for brevity
```

Listas de control de acceso

Las ACLs además de filtrar el tráfico de red pueden ser utilizadas para la clasificación de tráfico al cual se le aplicará QoS.



UNIVERSIDAD DON BOSCO

VITAM IMPENDERE VERO

EDUCACIÓN SUPERIOR CON ESTILO SALESIANO

AUTORIDAD DE AVIACIÓN CIVIL A.A.C. EL SALVADOR
Certificación del Técnico en Mantenimiento Aeronáutico
2016-2021

ACAAI
Agencia Centroamericana de Acreditación de Programas de Arquitectura y de Ingeniería

ISPO
INTERNATIONAL SOCIETY FOR PROSTHETICS AND ORTHOTICS
Acreditación Internacional en la carrera de Técnico en Ortesis y Prótesis
Presencial 2016-2021
A distancia 2018-2020

CdA
Comisión de Acreditación Calidad de la Educación Superior
UNIVERSIDAD DON BOSCO
ACREDITADA
2017 - 2022

Instituciones Salesianas de Educación Superior