ACL y Listas de acceso extendidas
REDES CISCO

Eduardo V. Abad

ACL y Listas de acceso extendidas
REDES CISCO

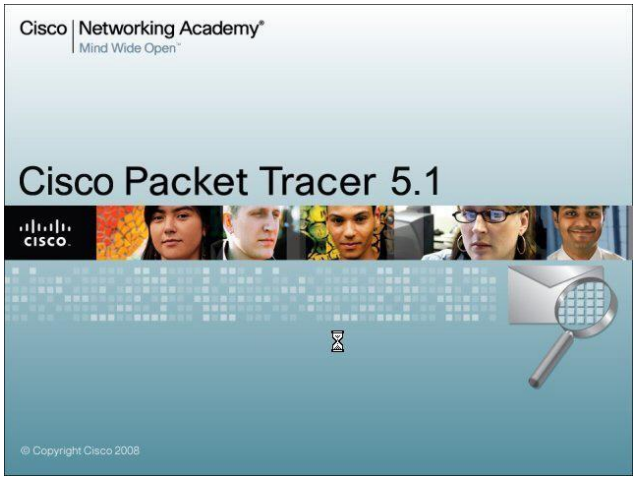
Eduardo V. Abad

INTRODUCCIÓN

Ahora es el turno de trabajar con hardware y tecnologías CISCO que permiten implementar todos los protocolos de red en sus distintitas capas de modelo OSI.

Seguiremos interactuando con el uso de hardware físico CISCO, pero antes de pasar a la configuración física, tenemos que recurrir al software conocido como Packet Tracer que es precisamente un simulador de la empresa CISCO que permite conocer y manipular el hardware que ellos comercializan.

Es una serie de entrenador para todos aquellos que desean conocer las tecnologías CISCO o aquellos que quieren una certificación.



ACL y Listas de acceso extendidas
REDES CISCO
Eduardo V. Abad

- Listas de acceso:

  Son un mecanismo, que permite regular el comportamiento general o individual en una red, para su acceso o salida a un determinado recurso, que se encuentre en la red.

Cabe mencionar, que las listas de acceso tienen dos categorías:

- Estándares.
- Extendidas.

Algunas notas del tema:

LISTAS DE ACCESO (ACL'S)

Estandar{1-99}{1300-1999}
Extendidas{100-199}

Las listas de acceso se aplican a un interfaz en comun.

Se den poner la lista de acceso ala interfaz mas cerca de la red q se desea denegar.

SIEMPRE POR DEFAULT ESTA EN :deny any.

Hay que poner :

Para aplicar unicamente donde se debe
access-list 10 permit any

access-list ? rangos

access-list 10

APLICAR LA LISTA AL FAST

Router(config)#interface fa0/0
Router(config-if)#ip access-group 10 out

estandar no deniega protocolos. solo host.

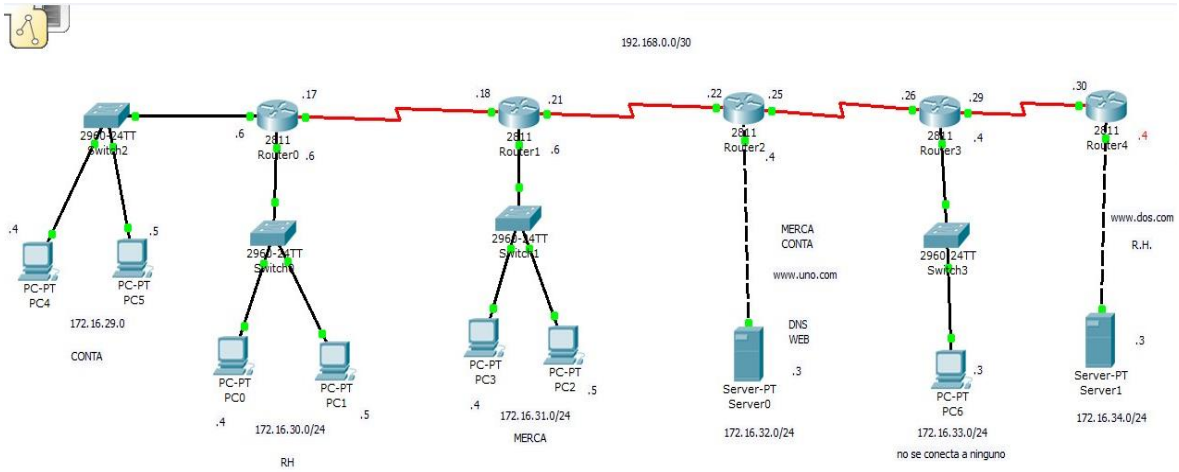
extendidas : si bloquean protocolos y host.

ACL y Listas de acceso extendidas
REDES CISCO

Eduardo V. Abad

PRÁCTICA 1

Se tiene la siguiente topología:



Se debe construir la siguiente topología, que contenga los elementos que se describen abajo:

a) Pc's.
b) Switch's 2960
c) Router's 2811
d) Servidores.

Por medio del protocolo de enrutamiento que se desee se deben comunicar todos los elementos de la red. Obedeciendo a la siguiente distribución de red:

172.16.29.0
172.16.30.0
172.16.31.0
172.16.32.0
172.16.33.0
172.16.34.0

Con las máscaras /24.

Y para los seriales:
Red: 192.168.0.0
Mascara: /30

Configuración de la práctica:

El objetivo con esto es delimitar el acceso únicamente, alos clientes correspondientes para que estos puedan ingresar a su respectivo servidor.

Mercadotécnica y Contabilidad; Servidor 1 Pero no a Servidor 2.

RH : Servidor 2 Pero no a Servidor 1

RH

access-list 20 deny 172.16.33.0 0.0.0.255
interface fa0/0
ip access-group 20 out

Router>enable
Router#config t

Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
Router(config)#access-list 20 deny 172.16.29.0 0.0.0.255
Router(config)#interface fa0/0
Router(config-if)#ip access-group 20 out
Router(config-if)#

Router(config)#access-list 20 deny 172.16.31.0 0.0.0.255

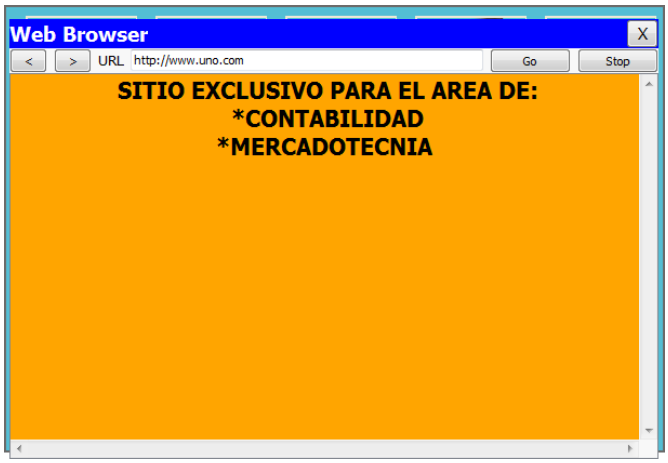
Router(config)#interface fa0/0
Router(config-if)#ip access-group 20 out
Router(config-if)#

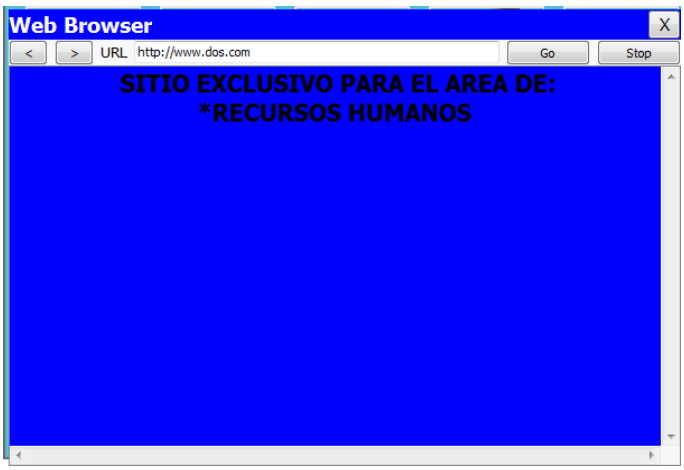
Router>enable
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
Router(config)#
Router(config)#access-list 20 deny 172.16.33.0 0.0.0.255
Router(config)#interface fa0/0
Router(config-if)#ip access-group 20 out
Router(config-if)#
/****************
Router>enable
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
Router(config)#
Router(config)#access-list 20 deny 172.16.32.0 0.0.0.255
Router(config)#interface fa0/0

Router(config-if)#ip access-group 20 out
Router(config-if)#
/***************

Finalmente con el elemento Cloud, solo procedemos a unir las redes de los PC'S que deseamos que pertenezcan a nuestra lista de acceso y realizar las pruebas.

Salidas en pantalla:



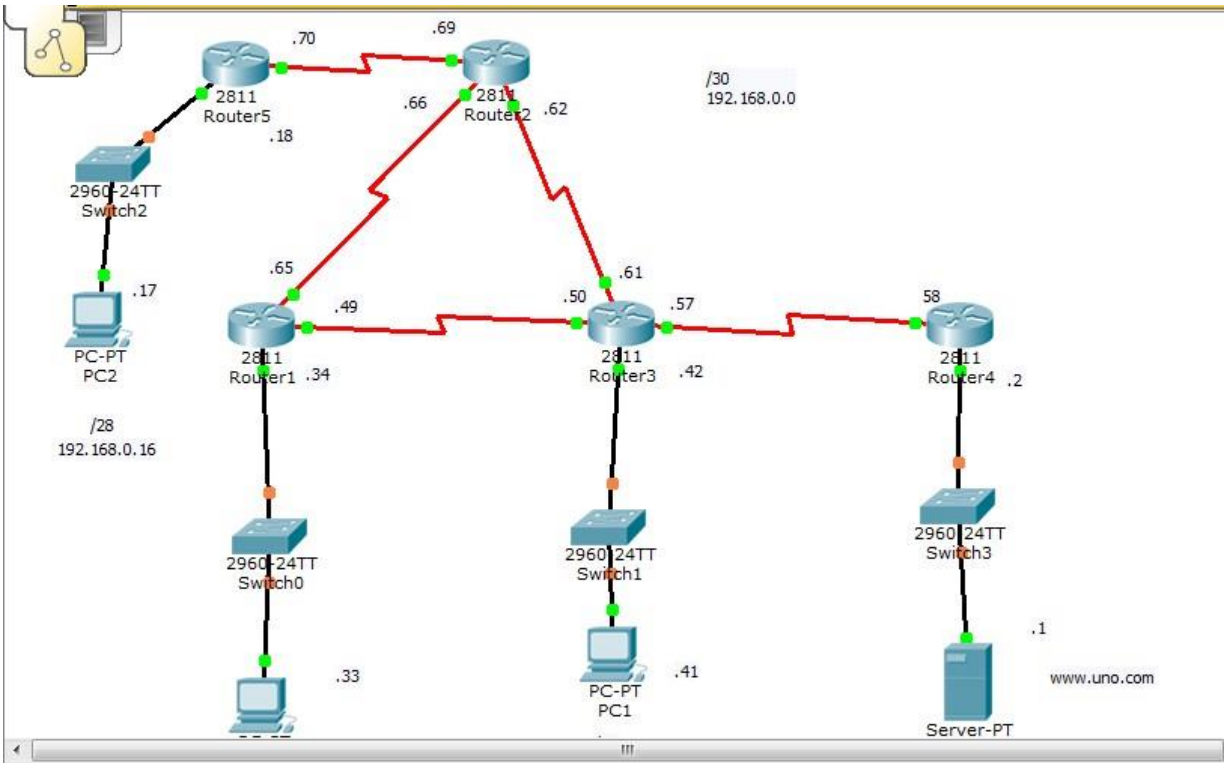


ACL y Listas de acceso extendidas
REDES CISCO
Eduardo V. Abad

PRÁCTICA 2
SERVIDOR WEB FILTRADO ACL

Creación de listas de acceso personalizadas, para filtrar conexiones por mascara de red tipo comodín.

Se tiene la siguiente topología.



Se configurar la red, con la distribución de IP antes mencionadas la red contara:

- Servidor Web centralizado bajo un router que contenga la página: *www.uno.com*

NOTA Si solo quiero permitir el acceso a la red: 192.168.0.16

Lo más recomendado es usar listas de acceso tipo *permit* y no *deny* ya que solo queremos permitir una red y denegar dos, esto se hace con la necesidad de no hacer más grande la configuración.

Access-list 20 permit 192.168.0.16 255.255.255.15

Y Sobre la interfaz donde se conecta directamente el servicio a aplicar la lista se configura lo siguiente.

#Interface fa0/0

 # Ip access-group 20 out.

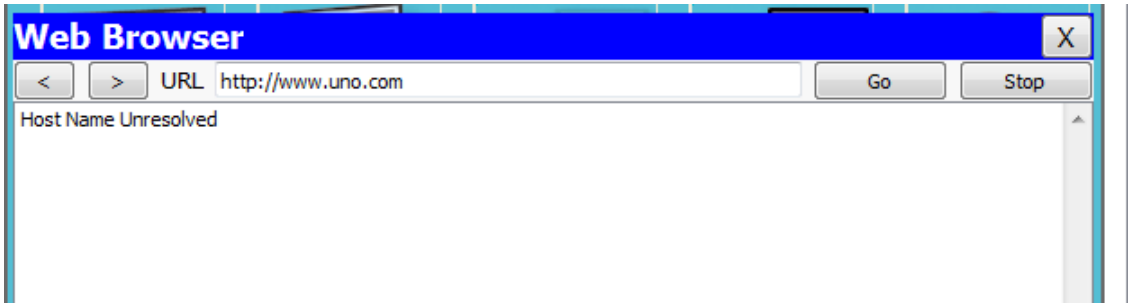
El porqué se denota que la máscara comodín es la 255.255.255.15 por y no la que corresponde a /28 que es 255.255.255.240

Es por que se realiza una configuración binaria.

192.168.000.1111 = 1111 =15

Es por eso que se coloca de esa manera y así es como se regula el acceso a esta página:

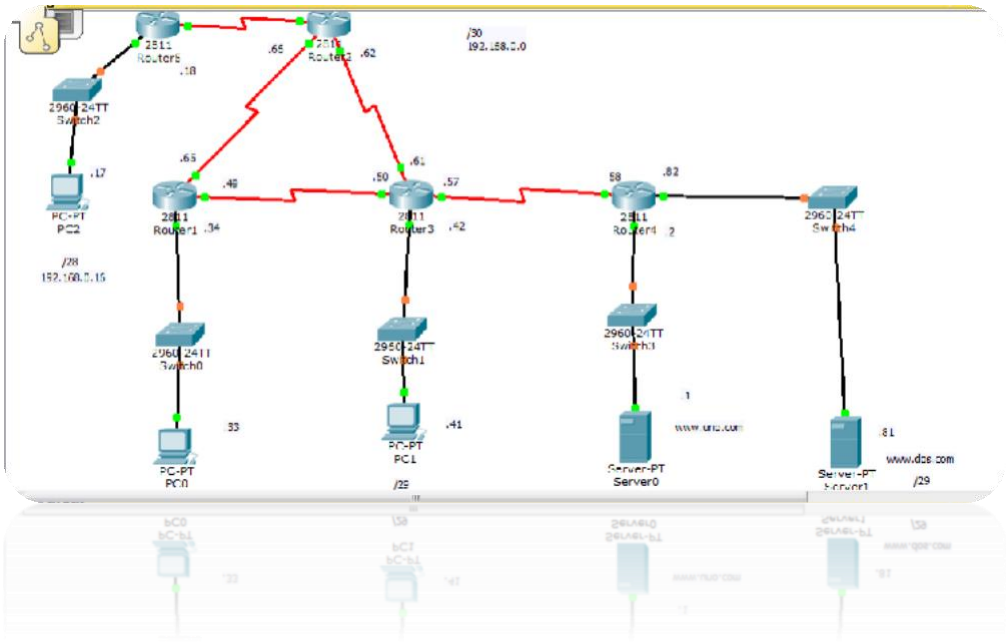
Desde host loqueado debe suceder lo siguiente:



ACL y Listas de acceso extendidas
REDES CISCO
Eduardo V. Abad

PRÁCTICA 3
DOS SERVIDORES WEB FILTRADO ACL

Teniendo en cuenta la construcción de la siguiente topología:



La red cuenta con dos servidores DNS:

1) www.uno.com

2) www.dos.com

Respectivamente ambos servidores solo deberán proveer de servicio a determinadas redes es decir.

www.uno.com Solo deberá proveer de servicio a la red 192.168.0.16

www.dos.com A las redes 192.168.0.32 y 192.168.0.40

Entonces para esto la configuración para el primer servidor se queda tal cual la teníamos en el al configuración de la práctica anterior.

Y para el acceso del segundo servidor se deberá realizar una lista de acceso que regule el acceso a las redes asignadas, es decir que solo permita esas dos redes y excluya ala 192.168.0.16.

La regla de acceso resultaría de la siguiente manera:

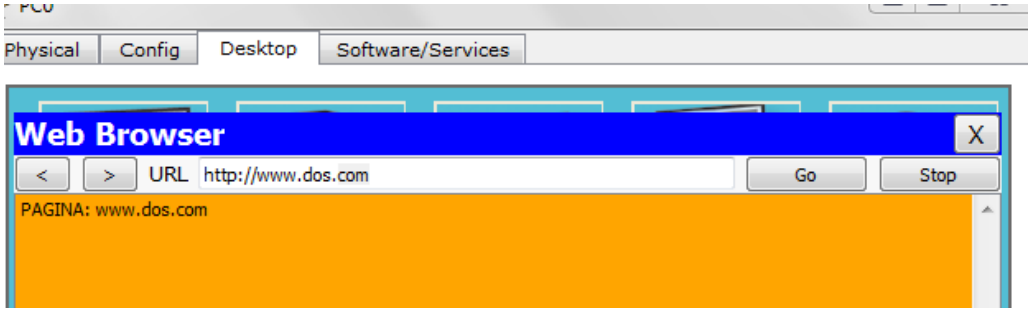
```
 network 192.168.0.0
!
ip classless
!
!
access-list 20 permit 0.0.0.16 255.255.255.15
access-list 21 permit 0.0.0.32 255.255.255.7
access-list 21 permit 0.0.0.40 255.255.255.7
!
!
```

Y las configuraciones de access-group así:

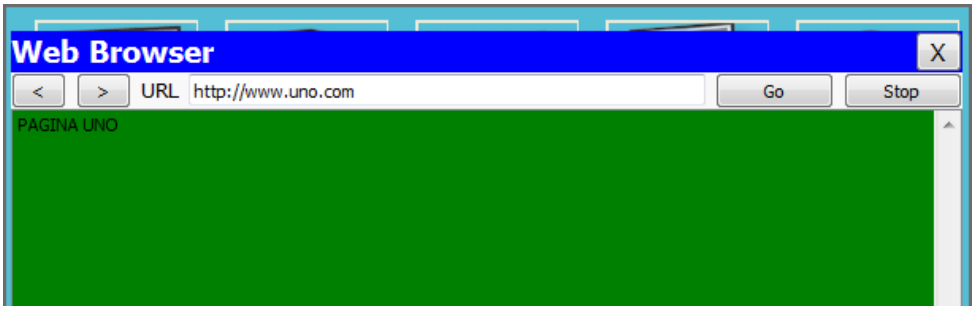
Interface fa0/1

Ip access-group 21 out.

Desde la red que puede llegar a**: www.dos.com**



Desde la red que puede llegar a: **www.uno.com**



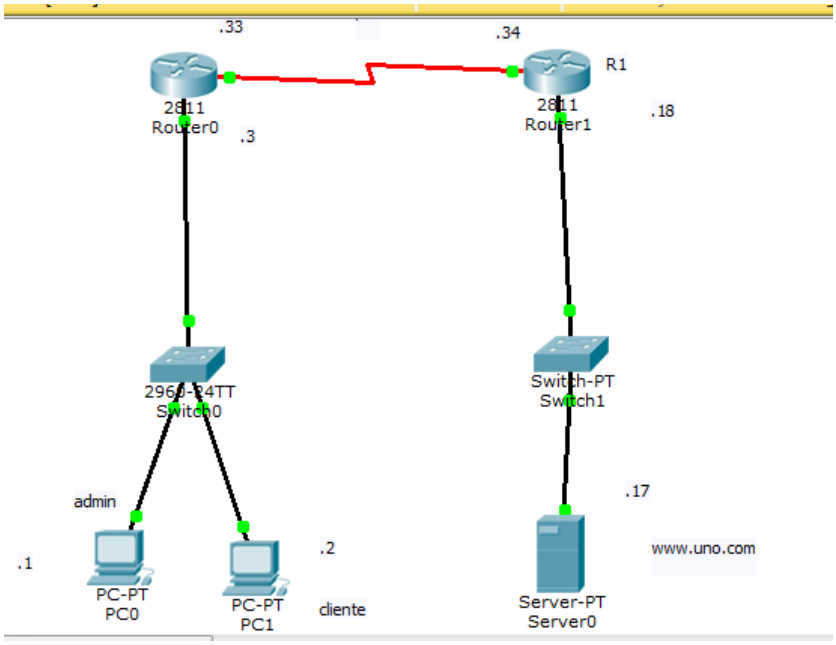
Nota: Si se elimina las listas de acceso todas la PC'S tienen acceso a cualquier página.

ACL y Listas de acceso extendidas
REDES CISCO
Eduardo V. Abad

PRÁCTICA 4
LISTAS DE ACCESO EXTENDIDAS

Se pretende utilizar listas de acceso extendidas para bloquear acceso a diferentes puertos en específico.

Teniendo la siguiente topología de red:



Que contiene lo siguiente:

- Servidor Web : **www.uno.com**
- Cuenta con 2 clientes.
- Una configuración de router con telnet. Port # 23

Se crearan las siguientes rutas de acceso que definan lo descrito a continuación:

- La PC administrador llegar por servicio de TELNET al Router que tiene la configuración TELNET.
- Pero no llegara al servidor web.

- La pc con nombre cliente no podrá llegar a la administración por telnet. Pero si podrá visualiza la Página web.

```
ip classless
!
!
access-list 100 permit tcp host 192.168.0.1 host 192.168.0.34 eq telnet
access-list 100 deny tcp host 192.168.0.1 host 192.168.0.17 eq www
access-list 100 deny tcp host 192.168.0.2 host 192.168.0.34 eq telnet
access-list 100 permit tcp host 192.168.0.2 host 192.168.0.17 eq www
access-list 100 permit tcp any any
!
 --More--
```

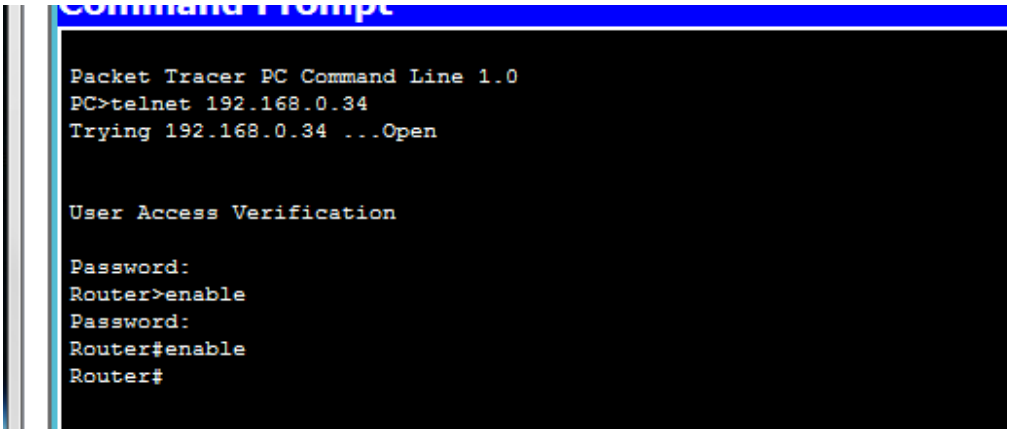
```
nterface FastEthernet0/0
ip address 192.168.0.3 255.255.255.240
ip access-group 100 in
duplex auto
speed auto

nterface FastEthernet0/1
```

Llega telnet. 192.168.0.34

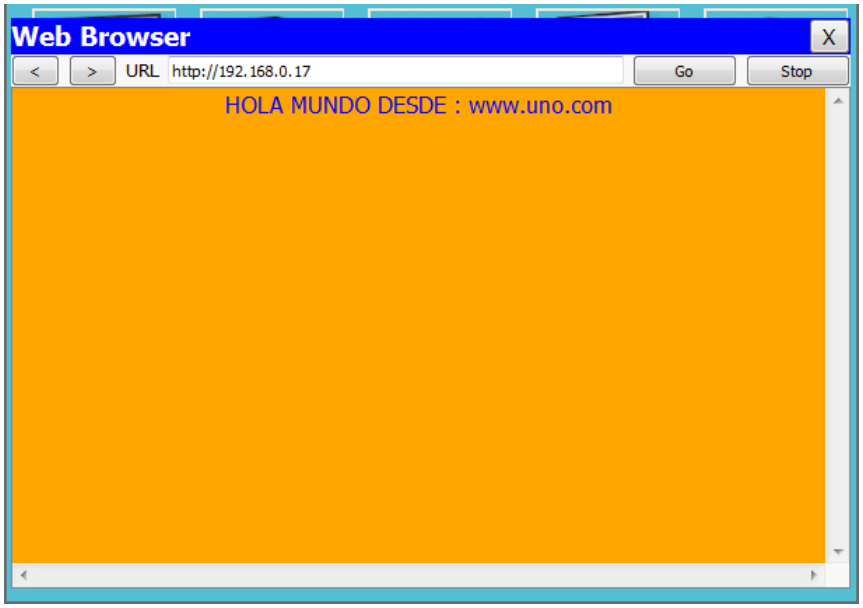
Pass: cisco

User: Admin.



Cliente.

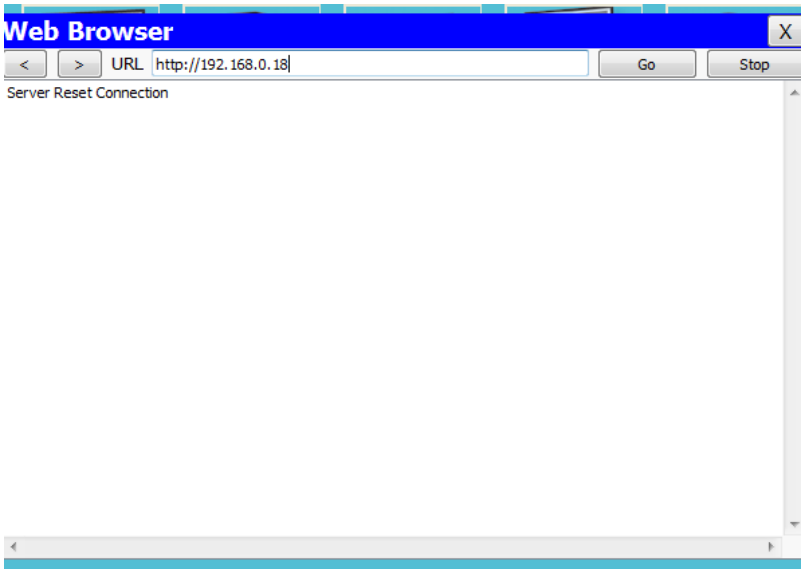
Pagina: www.uno.com



ACL y Listas de acceso extendidas
REDES CISCO

Eduardo V. Abad

Administrador



Cliente