


# Listas de Control de Acceso

Parte II


Profesor Juan Carlos Cuéllar Q.

## OBJETIVOS

- Entender el funcionamiento de las listas de control de acceso extendidas.
- Configurar listas de control de acceso extendidas.
- Verificar la correcta configuración de las listas de control de acceso.
- Ejercicio propuestos.




## GUÍA DE CONFIGURACIÓN




1. Mediante el número de la lista de acceso defino si es estándar o extendida.
2. Se debe configurar una lista por interfaz, protocolo y dirección.
3. El orden de las sentencias es crucial para el análisis de lo que se desea.
4. Las sentencias más restrictivas deben ubicarse al inicio de la lista.
5. Siempre al final de cada lista hay un “deny all” implícito, por lo tanto debe configurarse un “permit” de tal manera que no se filtre todo el tráfico.
6. Cree las listas de acceso antes de aplicarlas a las interfaces.
7. Las listas de acceso filtran el tráfico que pasa a través del enrutador, y no se aplican al tráfico originado desde el enrutador (caso especial).

Ing. Juan Carlos Cuéllar Q. 3



## COMO IDENTIFICAR EL TIPO DE LISTA DE CONTROL DE ACCESO




Listas de control de acceso estándar rango:

**1-99 , 1300-1999**

Listas de control de acceso extendidas rango:

**100-199, 2000-2699**

Ing. Juan Carlos Cuéllar Q. 4



UNIVERSIDAD  
**ICESI**

## CONTROLANDO EL ACCESO AL ENRUTADOR

```
Router(config)#username name privilege level number  
password text
```

```
Router(config)#privilege exec level number command
```

**Privilege level 0: disable, enable, exit, help and logout**

```
Router# configure terminal  
Router(config)#line vty 0 4  
Router(config-line)#login local
```

**El comando login local activa el uso de una base de Datos para la autenticación.**

Ing. Juan Carlos Cuéllar Q. 5

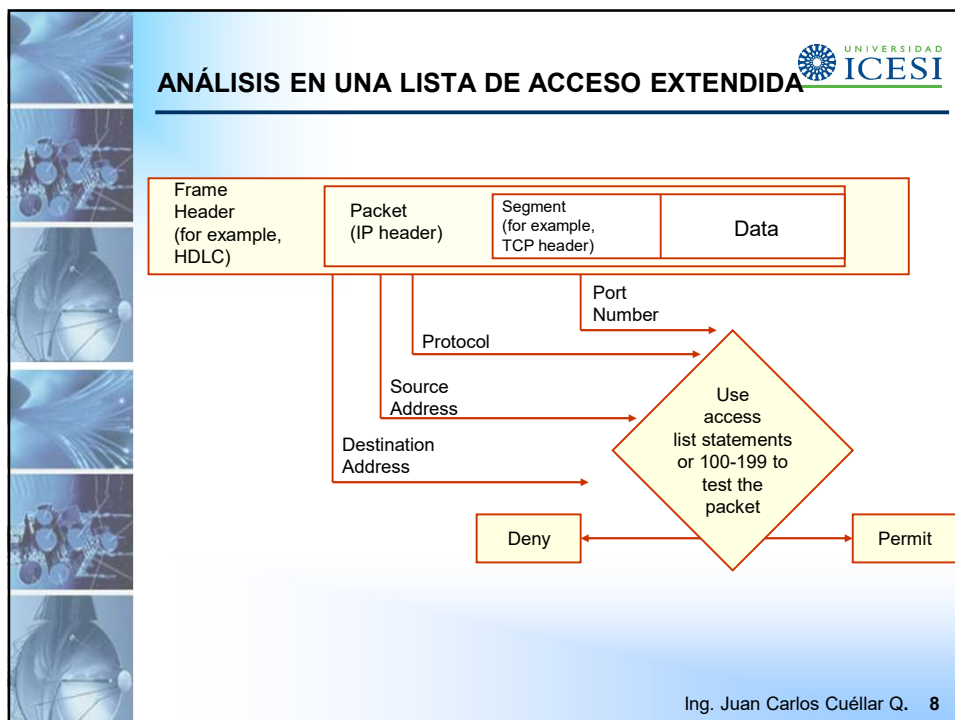
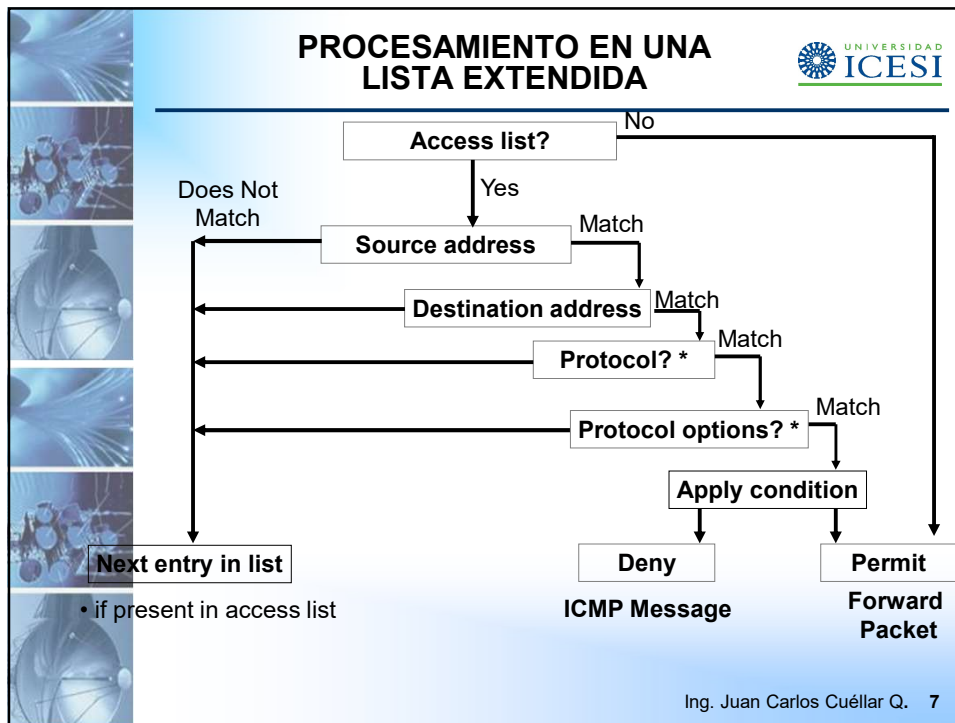
UNIVERSIDAD  
**ICESI**

## CONTROLANDO EL ACCESO AL ENRUTADOR...

Recomendaciones para su configuración:

1. Defina nombre de usuario y password.
2. Defina que comandos puede ejecutar dicho usuario.
3. Ejecute el comando login local a las terminales virtuales.
4. No ejecutar el comando login local a la consola.
5. No ejecutar el comando login local sin haber creado el usuario con su password.

Ing. Juan Carlos Cuéllar Q. 6



## CONFIGURACIÓN PARA LISTAS DE ACCESO EXTENDIDAS



```
Router (config) # access-list access-list-number  
{ permit | deny } protocol source source-wildcard  
[operator port] destination destination-wildcard  
[ operator port ] [ established ] [log]
```

- Configura los parámetros de análisis en la lista de acceso.

```
Router(config-if)# ip access-group access-list-  
number {in | out }
```

- Activa la lista de acceso en la interfaz requerida con la dirección en que se debe realizar el análisis.

Ing. Juan Carlos Cuéllar Q. 9

## COMPARACIÓN ENTRE LAS LISTAS DE ACCESO



Standard	Extended
Filters Based on Source.	Filters Based on Source and destination.
Permit or deny entire TCP/IP protocol suite	Specifies a specific IP Protocol and port number.
Range is 1 through 99	Range is 100 through 199.

Ing. Juan Carlos Cuéllar Q. 10

## LISTA DE ACCESO EXTENDIDA BASADA EN TCP



```
access-list access-list-number { permit | deny } tcp
{ source source-wildcard | any }
[ operator source-port | source-port]
{ destination destination-wildcard | any }
[ operator destination-port | destination-port ]
[ established ]
```

- Se filtra el protocolo TCP y el puerto o nombre de la aplicación.

Ing. Juan Carlos Cuéllar Q. 11

## NOMBRES DE PUERTOS TCP



bgp	gopher	sunrpc
chargen	hostname	syslog
daytime	irc	tacacsds
discard	klogin	talk
domain	kshell	telnet
echo	lpd	time
finger	nnntp	uucp
ftp control	pop2	whois
ftp-data	pop3	www

En la lista de acceso puede colocar el nombre de la aplicación el número de puerto.

Ing. Juan Carlos Cuéllar Q. 12

## LISTA DE ACCESO EXTENDIDA BASADA EN UDP



```
access-list access-list-number { permit | deny } udp  
{ source source-wildcard | any }  
[ operator source-port | source-port ]  
{ destination destination-wildcard | any }  
[ operator destination-port | destination-port ]  
[ established ]
```

Se filtra el protocolo UDP y el puerto o nombre de la aplicación.

Ing. Juan Carlos Cuéllar Q. 13

## NOMBRES DE PUERTOS UDP



biff	nameserver	syslog
bootpc	netbios-dgm	tacacsds-ds
bootps	netbios-ns	talk
discard	ntp	tftp
dns	rip	time
dnsix	snmp	whois
echo	snmptrap	xmcp
mobile-ip	sunrpc	

En la lista de acceso puede colocar el nombre de la aplicación el número de puerto.

Ing. Juan Carlos Cuéllar Q. 14

## LISTA DE ACCESO EXTENDIDA BASADA EN ICMP



Router (config) #

```
access-list access-list number { permit | deny } icmp  
  
{ source source-wildcard | any }  
  
{ destination destination-wildcard | any }  
  
[ icmp-type [ icmp-code ] | icmp message ]
```

La lista de acceso filtra el tipo de mensaje ICMP

Ing. Juan Carlos Cuéllar Q. 15

## MENSAJES ICMP Y SUS NOMBRES

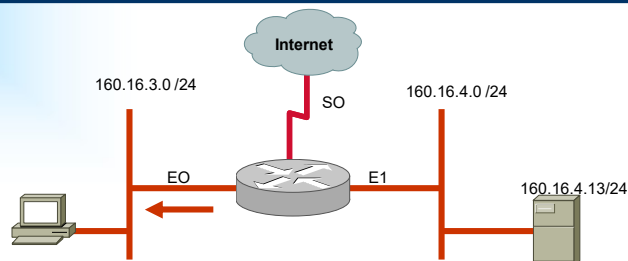


Administratively-prohibited	information replay	port unreachable
Alternate-address	mask-replay	reassembly-timeout
Conversion-error	mask-request	redirect
Dod-host-prohibited	mobile-redirect	router-advertisement
Dod-net-prohibited	net-direct	router-solicitation
Echo	net tos-redirect	source-quench
Echo replay	net-tos-unreachable	source-route-failed
General-parameters-problem	net-unreachable	time-exceeded
Host-isolated	network-unknown	traceroute
Host-tos-redirect	no-room-for-option	ttl-exceeded
Host-tos-unreachable	option-missing	unreacheable
Host-unknown	packet-too-big	
Host-unreachable	parameter-problem	

Ing. Juan Carlos Cuéllar Q. 16



## EJEMPLO No.1

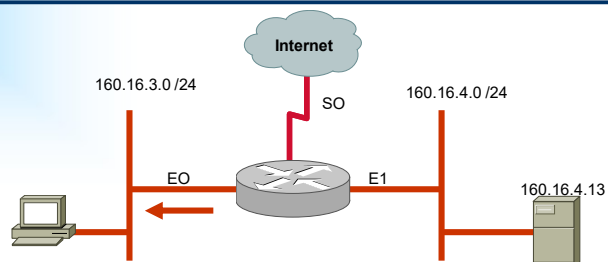


```
access-list 101 deny tcp 160.16.4.0 0.0.0.0.255 160.16.3.0 0.0.0.255 eq 21
access-list 101 deny tcp 160.16.4.0 0.0.0.0.255 160.16.3.0 0.0.0.255 eq 20
access-list 101 permit ip any any

interface ethernet 0
ip access-group 101 out
```

Ing. Juan Carlos Cuéllar Q. 17

## EJEMPLO No.2

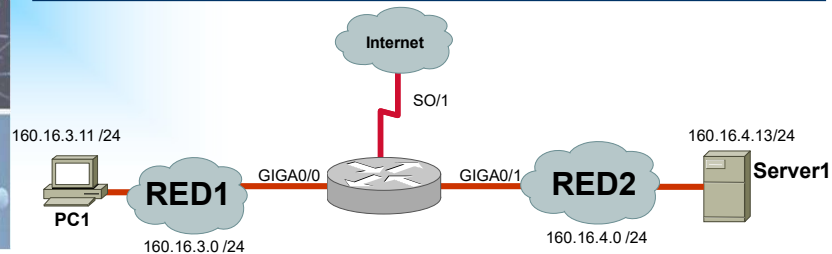


```
access-list 101 deny tcp 160.16.4.0 0.0.0.255 any eq 23
access-list 101 permit ip any any

interface ethernet 0
ip access-grup 101 out
```

Ing. Juan Carlos Cuéllar Q. 18

## EJEMPLO No.3



Configure las listas de control de acceso necesarias para garantizar lo siguiente:

- 1- Que la RED1 puede hacer http solo al Server1.
- 2- Que solo el PC1 de la RED1 pueda hacer telnet al Server1.
- 3- Que la RED1 pueda navegar en Internet.
- 3- Que la RED2 no tenga acceso a Internet, esto para proteger al Server1 de posibles ataques.

Ing. Juan Carlos Cuéllar Q. 19

## LISTAS DE ACCESO NOMBRADAS (NAMED)

- Característica que poseen los IOS Release 11.2 o posterior.

```
Router(config)# ip access-list { standard | extended } name
```

- El nombre elegido debe ser único.

```
Router(config {std- | ext-}nacl)# { permit | deny }  
{ ip access list test conditions }  
{ permit | deny } { ip access list test conditions }  
no { permit | deny } { ip access list test conditions }
```

```
Router(config-if)# ip access-group name { in | out }
```

- Activa la lista de acceso en la interfaz física.

Ing. Juan Carlos Cuéllar Q. 20

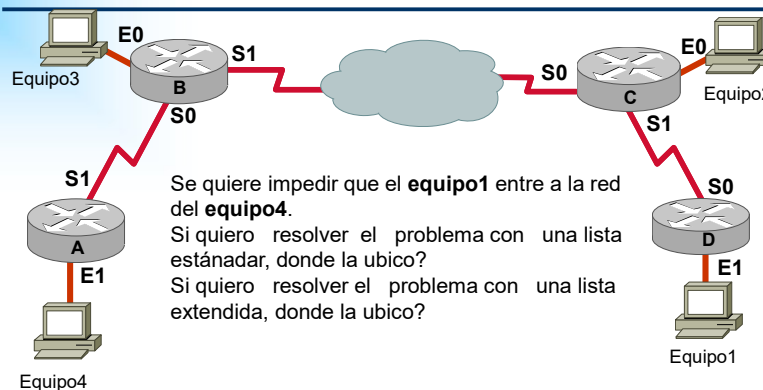
## RECOMENDACIONES PARA LA CONFIGURACIÓN DE LISTAS DE ACCESO



- El orden de las sentencias es crucial. Se recomienda utilizar un editor de texto para reconfigurar la lista.
- Recuerde colocar las sentencias más específicas al inicio de la lista.
- No reordene o retire sentencias. Use el comando `no access-list number` para eliminar toda la lista de acceso.
- Recuerde el deny all implícito. Coloque al menos una sentencia que permita todo o lo que usted considere.

Ing. Juan Carlos Cuéllar Q. 21

## DONDE UBICAR LISTAS ESTÁNDAR Y EXTENDIDAS?



### Recomendación:

Configurar las listas de acceso estándar cerca del destino.

Configurar las listas de acceso extendidas cerca de la fuente.

Ing. Juan Carlos Cuéllar Q. 22

## VERIFICANDO LA CONFIGURACIÓN DE LAS LISTAS DE ACCESO



```
Router1#show ip int e0
Ethernet0 is up, line protocol is up
Internet address is 10.1.1.11/24
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
Outgoing access list is not set
Inbound access list is 1
Proxy ARP is enabled
Security level is default
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachable are always sent
ICMP mask replies are never sent
IP fast switching is enabled
IP fast switching on the same interface is disabled
IP Feature Fast switching turbo vector
IP multicast fast switching is enabled
IP multicast distributed fast switching is disabled
<text omitted>
```

Ing. Juan Carlos Cuéllar Q. 23

## VERIFICANDO LA CONFIGURACIÓN DE LAS LISTAS DE ACCESO




```
Router1#show {protocol} access-list { access-list number }
```

```
Router1#show access-lists {access-list number}
```

```
Router1#show access-lists
Standard IP access list 1
  permit 10.2.2.1
  permit 10.3.3.1
  permit 10.4.4.1
  permit 10.5.5.1
Extended IP access list 101
  Permit tcp host 10.22.22.1 any eq telnet
  permit tcp host 10.33.33.1 any eq ftp
  permit tcp host 10.44.44.1 any eq ftp-data
```

Ing. Juan Carlos Cuéllar Q. 24




## IP Accounting en listas de acceso

IP accounting es una facilidad para verificar si las listas de acceso extendidas están bien configuradas.

IP accounting permite verificar que paquetes están transitando por el enrutador, que hacen match con la lista de acceso o no.

```
interface ethernet 0/0
ip accounting output-packets
ip accounting access-violations
!
interface ethernet 0/1
ip accounting output-packets
ip accounting access-violations
```

Ing. Juan Carlos Cuéllar Q. 25



## IP Accounting en listas de acceso...


**Router# show ip accounting**

Muestra el tráfico que pasa por el enrutador mostrando dirección IP fuente, destino, cantidad de paquetes y Bytes.


**Router# show ip accounting access-violations**

Muestra la dirección IP fuente y destino de los paquetes descartados, al igual que el número de la lista de acceso.

Ing. Juan Carlos Cuéllar Q. 26



## IP Accounting database



Una base de datos es utilizada para los paquetes que pasan por el enrutador y para los paquetes que son denegados.


Cuando la base de datos se llena aparece un mensaje como este:

```
Accounting threshold exceeded for 13475 packets violations access list(s)
```


Con el comando **ip accounting-threshold** se puede cambiar el tamaño de esta base de datos, por defecto es de 512 entradas.

Con el comando **clear ip accounting** puede limpiar esta base de datos.

Ing. Juan Carlos Cuéllar Q. 27



## Access list entry logging



Con el comando **log** que se coloca al final de las listas de acceso extendidas se puede verificar que paquete hizo match con la lista y este reporte va un log del enrutador.

```
access-list 101 deny tcp any host 192.168.1.10 eq 20 log
access-list 101 deny tcp any host 192.168.1.10 eq 21 log
access-list 101 permit tcp any host 192.168.1.10 eq 23 log
logging buffered
!
interface ethernet 0/1
ip access-group 101 out
```


Si se desea enviar los logs a un servidor de logs se puede utilizar el siguiente comando:


**logging 192.168.1.20**

Donde el enrutador envia los logs al servidor 192.168.1.20 vía syslog.

Ing. Juan Carlos Cuéllar Q. 28







Kiwi Syslog Service Manager (Registered - Version 8.2.17)


File Edit View Manage Help


Display 00 (Default)

!	Date	Time	Priority	Hostname	Message
	06-05-2007	15:52:08	System4.Debug	192.168.10.165	Test user connected to website http://205.204.17.55/index.html
	06-05-2007	15:52:06	System0.Warning	192.168.10.89	Test user connected to website http://205.162.200.113/index.html
	06-05-2007	15:52:03	Cron.Notice	192.168.10.203	Test user connected to website http://209.252.233.155/index.html
	06-05-2007	15:52:01	Daemon.Info	192.168.10.201	Test user connected to website http://216.50.131.83/index.html
	06-05-2007	15:51:47	System0.Notice	192.168.10.77	Test user connected to website http://200.12.148.104/index.html
	06-05-2007	15:51:44	Local3.Info	192.168.10.188	Test user connected to website http://218.210.113.80/index.html
	06-05-2007	15:51:44	Kernel.Info	192.168.10.68	Test user connected to website http://214.237.112.128/index.html
	06-05-2007	15:51:43	Local7.Info	192.168.10.179	Test user connected to website http://203.74.32.87/index.html
	06-05-2007	15:51:43	Local7.Info	192.168.10.153	Test user connected to website http://222.33.104.53/index.html
	06-05-2007	15:51:40	System4.Info	192.168.10.102	Test user connected to website http://200.243.58.241/index.html
	06-05-2007	15:51:40	Mail.Info	192.168.10.225	Test user connected to website http://207.167.179.233/index.html
	06-05-2007	15:51:40	System1.Info	192.168.10.65	Test user connected to website http://218.11.242.24/index.html
	06-05-2007	15:51:37	Local2.Debug	192.168.10.135	Test user connected to website http://197.113.220.28/index.html
	06-05-2007	15:51:36	Local3.Debug	192.168.10.48	Test user connected to website http://199.6.170.60/index.html
	06-05-2007	15:51:36	System5.Debug	192.168.10.40	Test user connected to website http://206.227.1.130/index.html
	06-05-2007	15:51:30	Local4.Debug	192.168.10.59	Test user connected to website http://210.179.80.146/index.html
	06-05-2007	15:51:27	Kernel.Notice	192.168.10.184	Test user connected to website http://215.115.243.34/index.html
	06-05-2007	15:51:26	Cron.Notice	192.168.10.246	Test user connected to website http://203.245.220.41/index.html
	06-05-2007	15:51:23	User.Warning	192.168.10.249	Test user connected to website http://220.213.89.137/index.html
	06-05-2007	15:51:22	System1.Warning	192.168.10.120	Test user connected to website http://194.118.154.130/index.html

100% 588 MPH 15:52 06-05-2007

Ing. Juan Carlos Cuéllar Q. 29





Kiwi Syslog Service Manager (Registered - Version 8.2.17)

File Edit View Manage Help

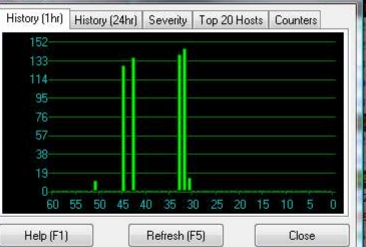
Display 00 (Default)

!	Date	Time	Priority	Hostname	Message
	06-05-2007	14:45:24	Syslog.Info	192.168.10.49	Test user connected to website http://195.252.78.129/index.html
	06-05-2007	14:45:24	Daemon.Info	192.168.10.80	Test user connected to website http://194.92.215.30/index.html
	06-05-2007	14:45:21	Local5		0.1.235/index.html
	06-05-2007	14:45:16	System		0.1.234.138/index.html
	06-05-2007	14:45:14	Local5		2.174.211/index.html
	06-05-2007	14:45:11	Local0		2.233.144/index.html
	06-05-2007	14:45:08	System		1.103.32/index.html
	06-05-2007	14:45:07	Syslog		0.204.209/index.html
	06-05-2007	14:45:05	Daemon		2.230.162/index.html
	06-05-2007	14:45:02	System		0.8.25.86/index.html
	06-05-2007	14:44:59	Local7		2.225.89/index.html
	06-05-2007	14:44:58	System		1.187.212/index.html
	06-05-2007	14:44:55	User.C		0.5.130.207/index.html
	06-05-2007	14:44:51	Kernel		2.63.83/index.html
	06-05-2007	14:44:43	Lpr.Error		0.8.46.229/index.html
	06-05-2007	14:44:38	System		2.27.240/index.html
	06-05-2007	14:44:34	Local0		4.139.181/index.html
	06-05-2007	14:44:33	Syslog.Info	192.168.10.33	Test user connected to website http://220.145.97.3/index.html
	06-05-2007	14:44:33	System0.Info	192.168.10.107	Test user connected to website http://224.59.198.203/index.html
	06-05-2007	14:44:29	System2.Warning	192.168.10.193	Test user connected to website http://220.179.168.91/index.html
	06-05-2007	14:44:24	Local2.Notice	192.168.10.1	Test user connected to website http://222.133.21.159/index.html

100% 588 MPH 15:15 06-05-2007


Syslog Statistics

History (1hr) History (24hr) Severity Top 20 Hosts Counters




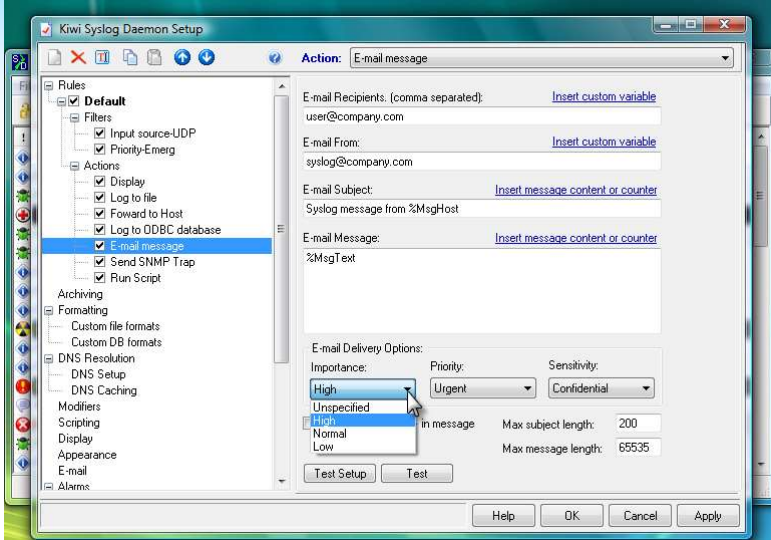
Help (F1) Refresh (F5) Close

Ing. Juan Carlos Cuéllar Q. 30




new brand of  
solarwinds

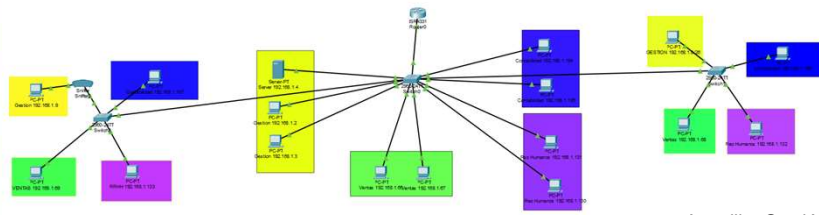




Ing. Juan Carlos Cuéllar Q. 31

## Ejercicio



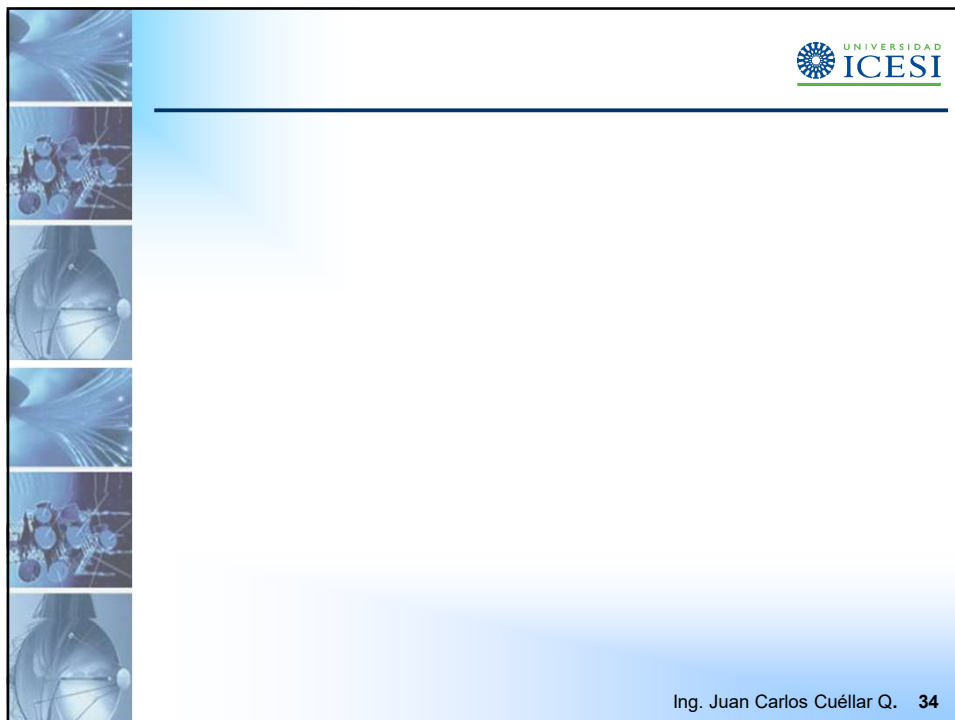
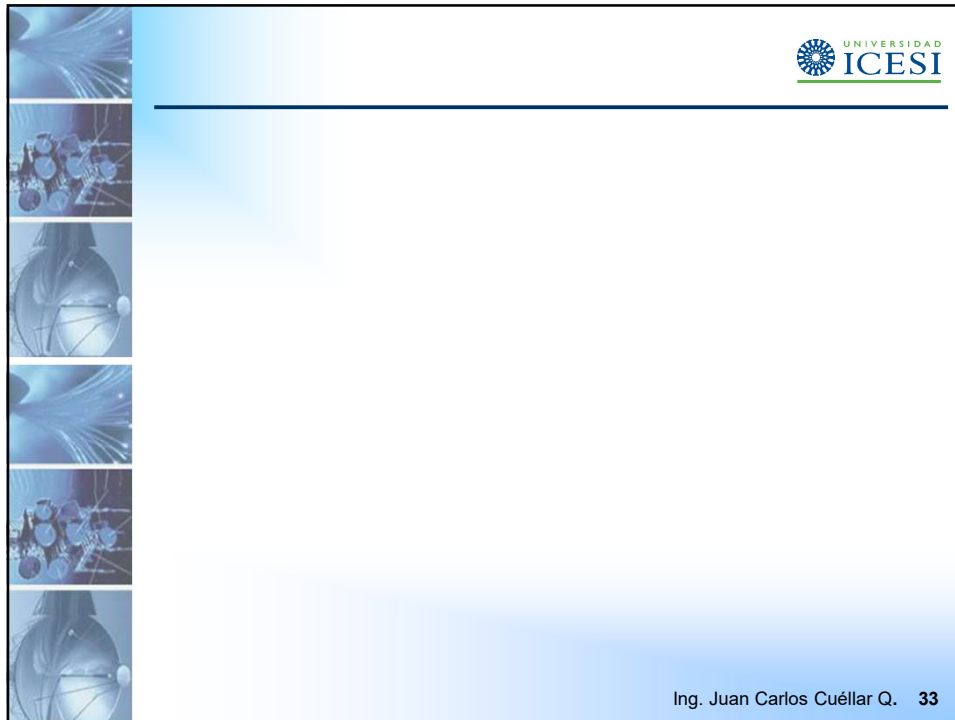


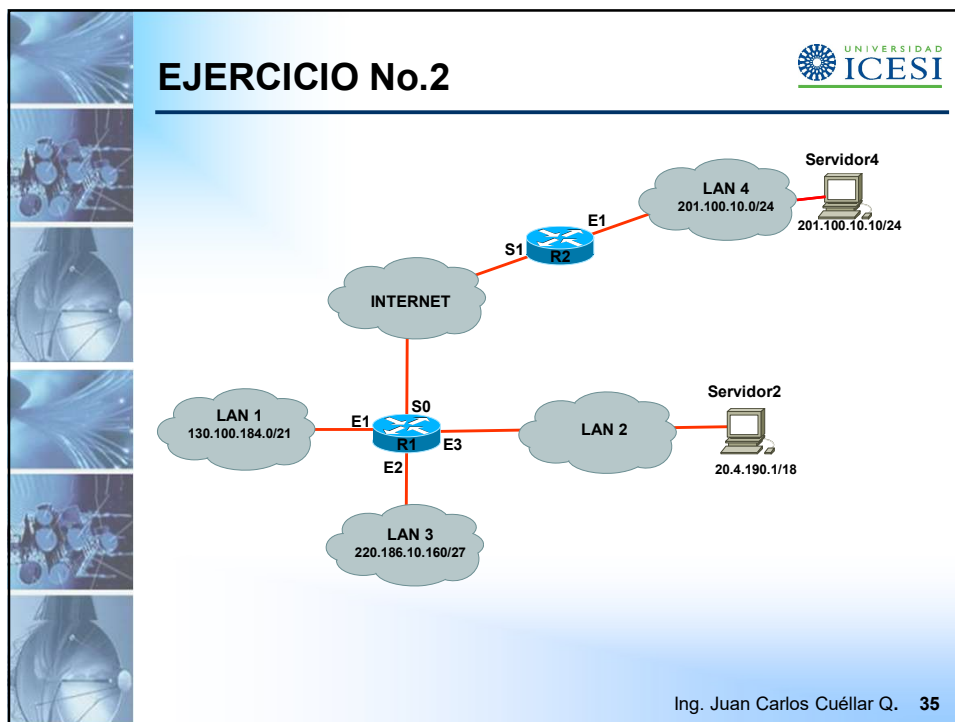
Amarillo: Gestión  
Azul: Contabilidad  
Verde: Ventas  
Violeta: RRHH

1. **Verificar que todos los equipos pueden hacer ping entre sí y pueden acceder al FTP y HTTP del servidor de Gestión.**
2. Que solo puedan hacer FTP al servidor los equipos de ventas y contabilidad.
3. Que todas las VLANs puedan hacer HTTP al servidor de gestión. Modificar página web inicial.
3. Que solo un PC de Ventas pueda hacer ping al servidor de gestión.
4. Cualquier otro tipo de tráfico no especificado **no** está permitido.

32







## Ejercicio No.2

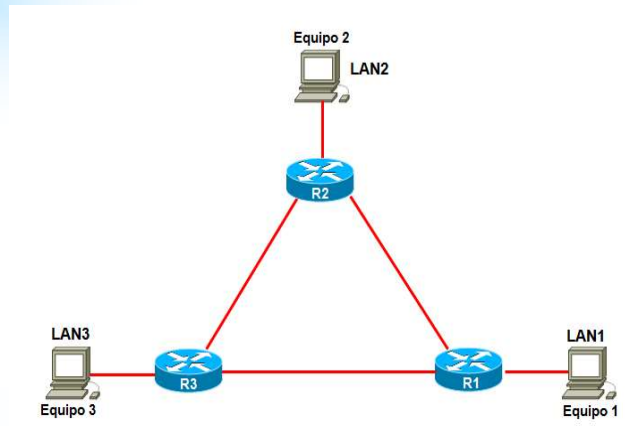
- Que solo los equipos de la LAN1, LAN3 y LAN4 puedan hacer telnet al Servidor2.
- Que todos los equipos conectados a R1 puedan hacer http al Servidor4.
- Que solo los equipos de LAN3 y LAN4 puedan navegar en Internet.

Que solo desde el servidor2 se les pueda hacer telnet a los enrutadores R1 y R2.

Cualquier otro tipo de conexión no especificada NO está permitida.

Ing. Juan Carlos Cuéllar Q. 36

## Práctica de Laboratorio



Ing. Juan Carlos Cuéllar Q. 37