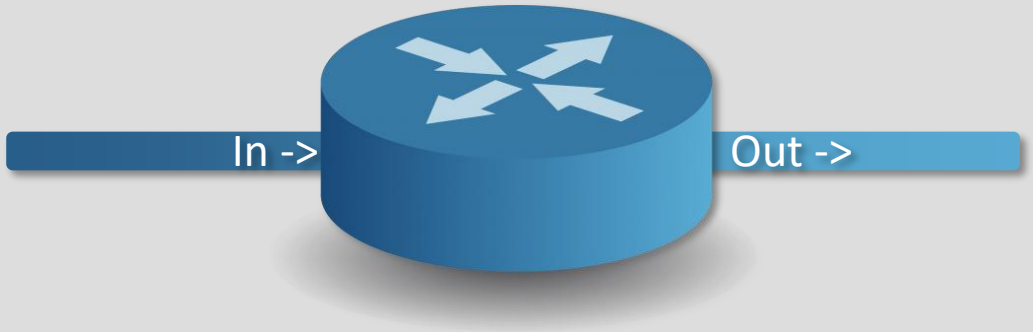
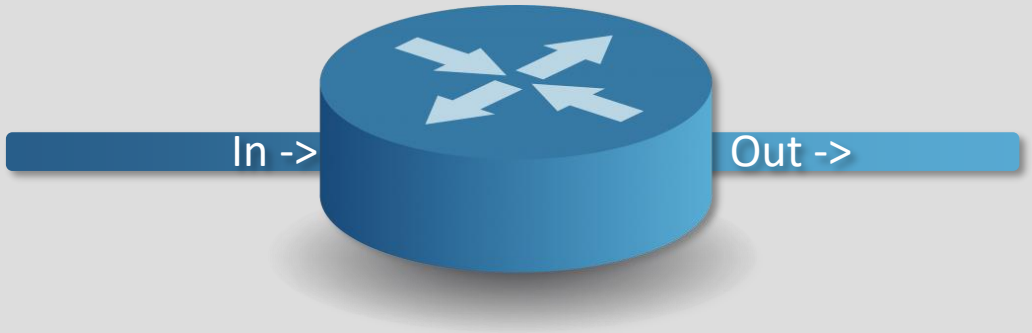
IPv4 Access Control Lists (IP ACLs)



- Source IP Address.
- Destination IP Address.
- Protocol Type.
- Source Port Number.
- Destination Port Number.

- Packet Filtering.
- QoS.
- Routing Updates Filtering.

Types of IP ACLs



Numbered ACL	Named ACL	Filtered Information
Standard (1–99) (1300–1999)	**Standard**	- Source IP
Extended (100–199) (2000–2699)	**Extended**	- Source & Dest. IP - Source & Dest. Port - IP Protocol - Protocol information

```
Router# configure terminal
Router(config)# access-list 1 permit -------
Router(config)# access-list 1 permit -------
Router(config)# access-list 1 deny   -------
Router(config)# access-list 1 deny   -------
```

```
Router(config)# interface gigabitEthernet 0/0
Router(config-if)# ip access-group 1 ---------
Router(config-if)# end
```

```
Router# configure terminal
Router(config)# ip access-list standard My_List
Router(config-std-nacl)# permit ---------
Router(config-std-nacl)# permit ---------
Router(config-std-nacl)# deny   ---------
Router(config-std-nacl)# deny   ---------
Router(config-std-nacl)# exit
```

```
Router(config)# interface gigabitEthernet 0/0
Router(config-if)# ip access-group My_List -----
Router(config-if)# end
```

Wildcard mask

192 . 168 . 250 . 230 0 . 0 . 0 . 0

IPv4	192	168	250	230
Wildcard Mask	0	0	0	0

IPv4	1100 0000	1010 1000	1111 1010	1110 0110
Wildcard Mask	0000 0000	0000 0000	0000 0000	0000 0000

Wildcard mask

192 . 168 . 250 . 230 0 . 0 . 0 . 255

IPv4	192	168	250	230
Wildcard Mask	0	0	0	255

IPv4	1100 0000	1010 1000	1111 1010	1110 0110
Wildcard Mask	0000 0000	0000 0000	0000 0000	1111 1111

IPv4	192	168	250	0
Wildcard Mask	0	0	0	255

Wildcard mask

192 . 168 . 250 . 230 0 . 0 . 255 . 255

IPv4	192	168	250	230
Wildcard Mask	0	0	255	255

IPv4	1100 0000	1010 1000	1111 1010	1110 0110
Wildcard Mask	0000 0000	0000 0000	1111 1111	1111 1111

IPv4	192	168	0	0
Wildcard Mask	0	0	255	255

Wildcard mask

192 . 168 . 250 . 230 0 . 255 . 255 . 255

IPv4	192	168	250	230
Wildcard Mask	0	255	255	255

IPv4	1100 0000	1010 1000	1111 1010	1110 0110
Wildcard Mask	0000 0000	1111 1111	1111 1111	1111 1111

IPv4	192	0	0	0
Wildcard Mask	0	255	255	255

Wildcard Mask Calculation

200 . 150 . 10 . 128 /26

26 = 8 + 8 + 8 + 2

255 255 255 192

128	64	32	16	8	4	2	1

IPv4	200	150	10	128
Subnet Mask	255	255	255	192

255 255 255 255

\- 255 255 255 192

0 0 0 63

IPv4	200	150	10	128
Wildcard Mask	0	0	0	63

Wildcard Mask Calculation

10 . 32 . 0 . 0 /12

10 = 8 + 4 + 0 + 0

255 240 0 0

128	64	32	16	8	4	2	1

IPv4	10	32	0	0
Subnet Mask	255	240	0	0

255 255 255 255

− 255 240 0 0

0 15 255 255

IPv4	10	32	0	0
Wildcard Mask	0	15	255	255

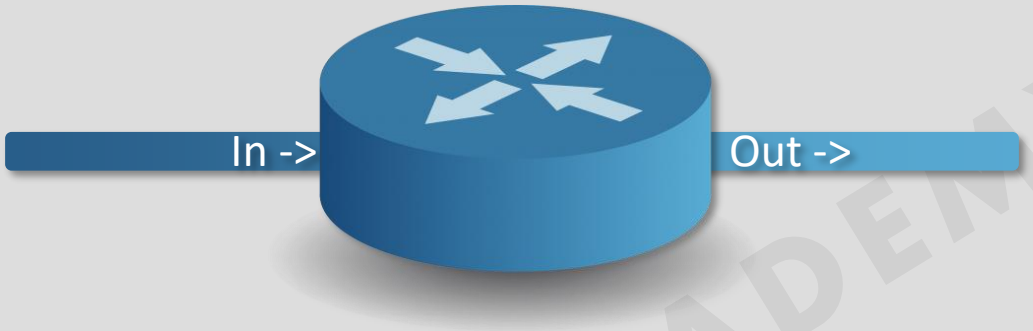
Wildcard Mask Keywords

- Cisco IOS provides two keywords to identify the most common uses of wildcard masking.

host: This keyword substitutes for the **0.0.0.0 mask** and indicates that all IPv4 address bits must match to filter just one host address.

any: This keyword substitutes for the **255.255.255.255 mask** and indicates to ignore the entire IPv4 address or to accept any addresses.

Activating an ACL



Router(config)# **interface** ----------
Router(config-if)# **ip access-group** ------ ***in***

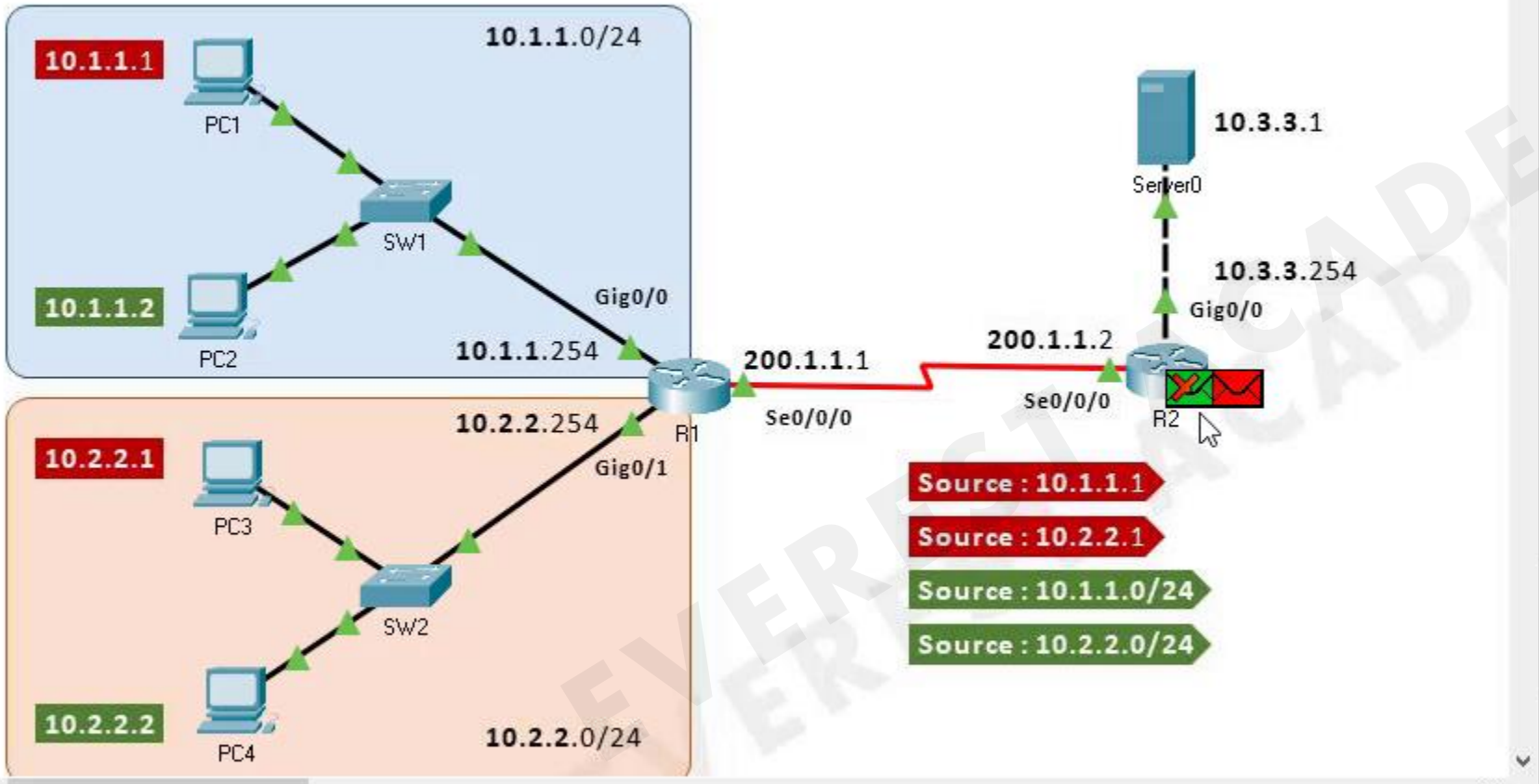
Router(config)# **interface** ----------
Router(config-if)# **ip access-group** ------ ***out***

Important Configuration Guidelines

- Order of statements is important: Put the **most restrictive** statements at the top of the list and the **least restrictive** at the bottom.
- ACL statements are processed **top-down** until a match is found, and then no more statements in the list are processed.
- If **no match** is found in the ACL, the packet is dropped (**implicit deny**).
- Each grouping of ACL statements needs either a **unique number** or **a unique name**.
- The router **cannot filter** traffic that it, itself, originates.
- Only **one IP ACL** can be applied to an interface in each direction (inbound and outbound).
- Applying an **empty ACL** to an interface permits all traffic by default.
- In order for an ACL to have an **implicit deny** statement, you need at least one actual permit or deny statement in the ACL.
- Place **extended** ACLs as close as possible to the **source** of the packet. This strategy allows ACLs to discard the packets early.
- Place **standard** ACLs as close as possible to the **destination** of the packet. This strategy avoids the mistake with standard ACLs

Standard ACL

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



Simulation Panel

Event List

Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	PC1	ICMP
	0.001	PC1	SW1	ICMP
	0.002	SW1	R1	ICMP
	0.003	R1	R2	ICMP
	0.003	--	R2	ICMP

Reset Simulation | Constant Delay | Captured to: 0.003 s

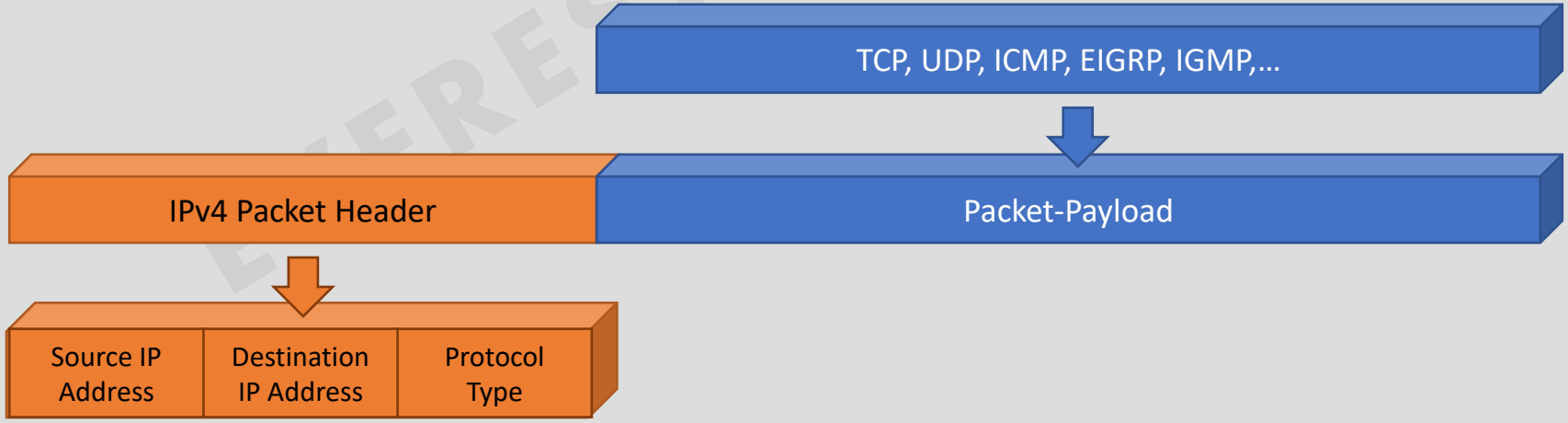
Play Controls

Event List Filters - Visible Events
ICMP
Edit Filters | Show All/None

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic
	In Progress	PC1	Server0	ICMP		0.000	N

Extended ACL

Numbered ACL	Named ACL	Filtered Information
Standard (1–99) (1300–1999)	**Standard**	- Source IP
Extended (100–199) (2000–2699)	**Extended**	- Source & Dest. IP - Source & Dest. Port - IP Protocol (**IP**, TCP, UDP, ICMP, EIGRP, IGMP,…) - Protocol information



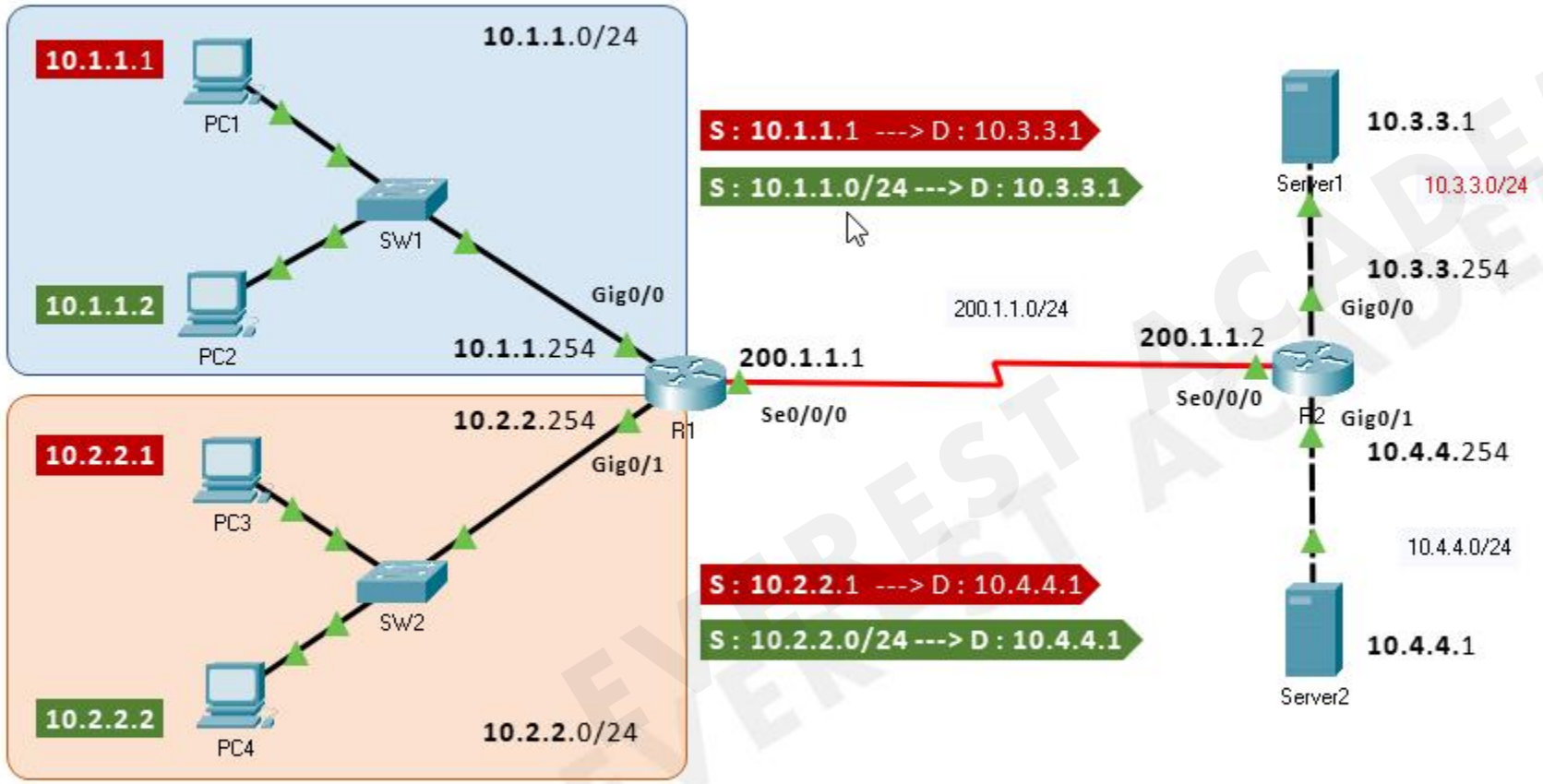
IP Extended ACL

Numbered ACL	Named ACL	Filtered Information
Standard (1–99) (1300–1999)	**Standard**	- Source IP
Extended (100–199) (2000–2699)	**Extended**	- Source & Dest. IP - Source & Dest. Port - IP Protocol (**IP**, TCP, UDP, ICMP, EIGRP, IGMP,…) - Protocol information

```
access-list 100-199/2000-2699 {permit | deny} IP source [source-wildcard] destination [destination-wildcard]
```

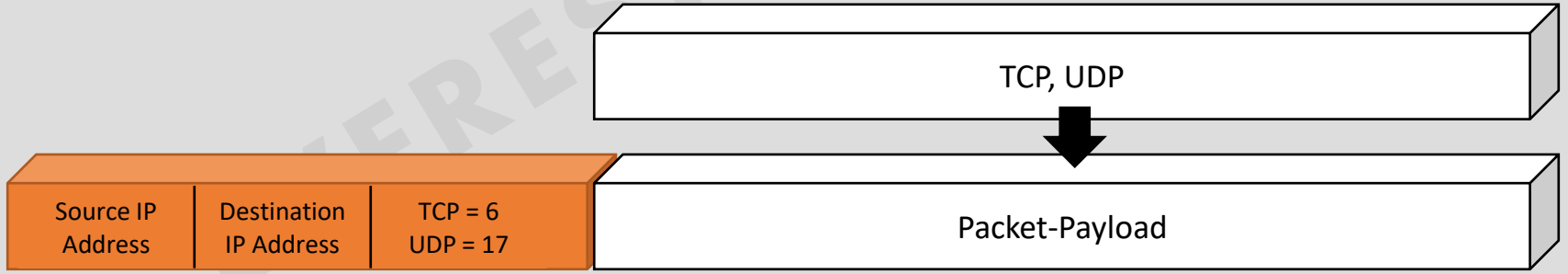
IP Extended ACL

access-list 100-199/2000-2699 **{permit | deny} IP** source **[source-wildcard]** destination **[destination-wildcard]**

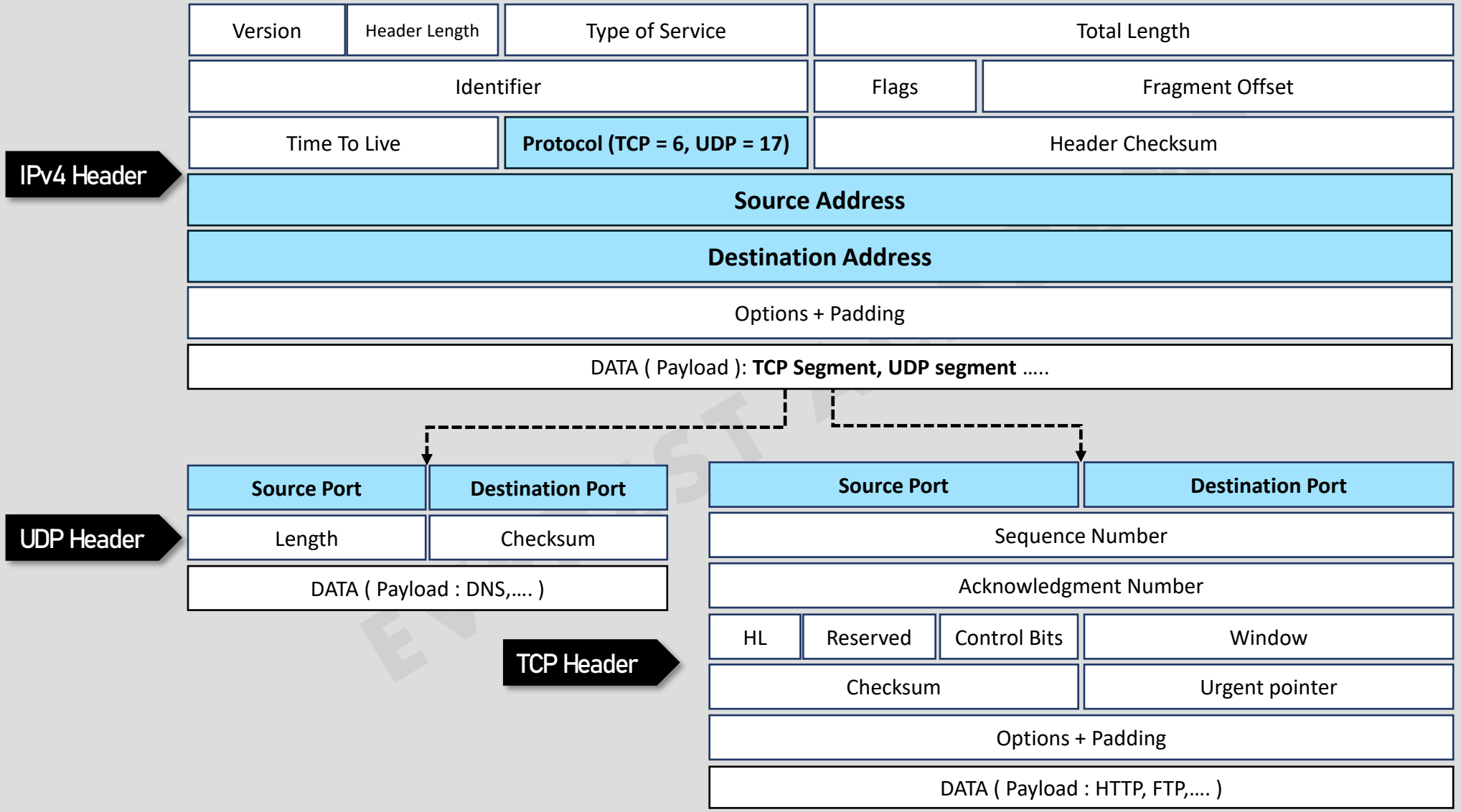


Extended ACL (TCP, UDP)

Numbered ACL	Named ACL	Filtered Information
Standard (1–99) (1300–1999)	**Standard**	- Source IP
Extended (100–199) (2000–2699)	**Extended**	- Source & Dest. IP - Source & Dest. Port - IP Protocol (**IP**, TCP, UDP, ICMP, EIGRP, IGMP,…) - Protocol information



Extended ACL (TCP, UDP)



Extended ACL (TCP, UDP)

Extended ACL Syntax with TCP and UDP Port Numbers Enabled

#access-list 100-199 {permit | deny} {TCP | UDP} {Source_IP} {Source-wildcard} **{Source_Port}** {Destination_IP} {Destination-wildcard} **{Destination_Port}**

[eq --- , ne --- , lt --- , gt --- , range ---]

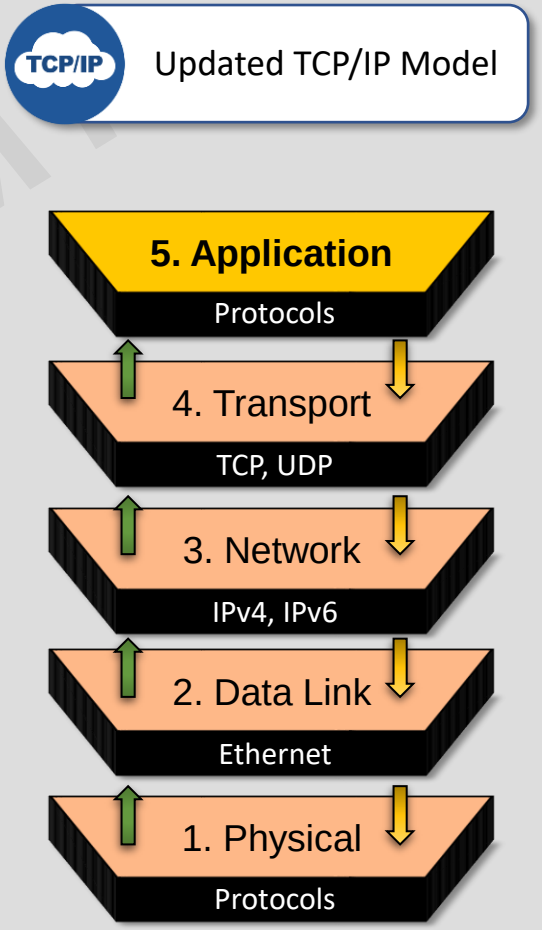
Equal (eq), not equal (ne), less than (lt), greater than (gt).

Port Group	Port Number Range
Well Known Ports	0 - 1023
Registered Ports	1024 - 49151
Dynamic or Private Ports	49152 - 65535

Extended ACL (TCP, UDP)

Popular Applications and Their Well-Known Port Numbers

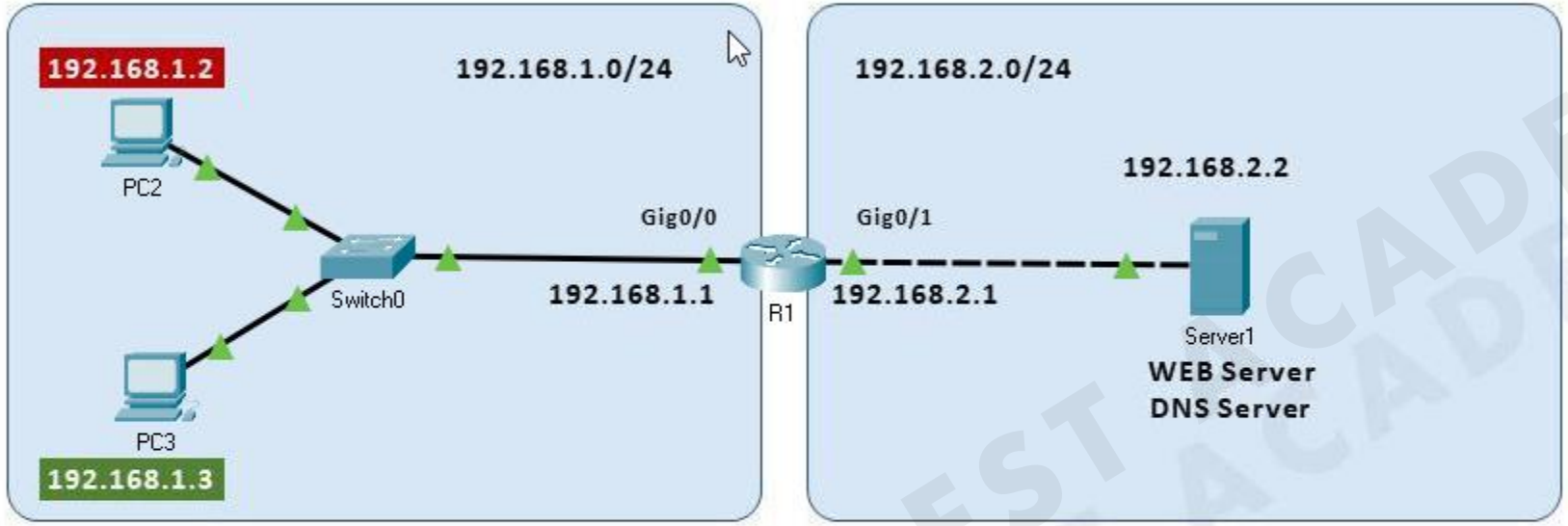
Protocol		Port Number	Keyword
FTP data	File Transfer Protocol .	**TCP (20)**	**ftp-data**
FTP control	File Transfer Protocol .	**TCP (21)**	**ftp**
Telnet	Teletype Network.	**TCP (23)**	**telnet**
SMTP	Simple Mail Transfer Protocol.	**TCP (25)**	**smtp**
DNS	Domain Name System.	**TCP, UDP (53)**	**domain**
DHCP server	Dynamic Host Configuration Protocol.	**UDP (67)**	**bootps**
DHCP client	Dynamic Host Configuration Protocol.	**UDP (68)**	**bootpc**
TFTP	Trivial File Transfer Protocol .	**UDP (69)**	**tftp**
HTTP	Hypertext Transfer Protocol .	**TCP (80)**	**www**
POP3	Post Office Protocol.	**TCP (110)**	**pop3**



Logical | Physical | x: 399, y: 92 | [Root] | 00:33:30

Extended ACL (TCP, UDP)

#access-list 100-199 {permit | deny} {TCP | UDP} {Source_IP} {Source-wildcard} **{Source_Port}** {Destination_IP} {Destination-wildcard} **{Destination_Port}**




```
configure  terminal
access-list 100  deny    udp  192.168.1.2  0.0.0.0    192.168.2.2  0.0.0.0  eq  53
access-list 100  permit  udp  192.168.1.0  0.0.0.255  192.168.2.2  0.0.0.0  eq  53
access-list 100  permit  tcp  192.168.1.0  0.0.0.255  192.168.2.2  0.0.0.0  eq  80
access-list 100  deny    ip       any                 any
interface gig0/0
ip access-group 100 in
```

Time: 00:01:06 | Realtime | Simulation

4331 | 4321 | 1941 | 2901 | 2911 | 819IOX | 819HGW | 829 | 1240 | PT-Router | PT-Empty | 184

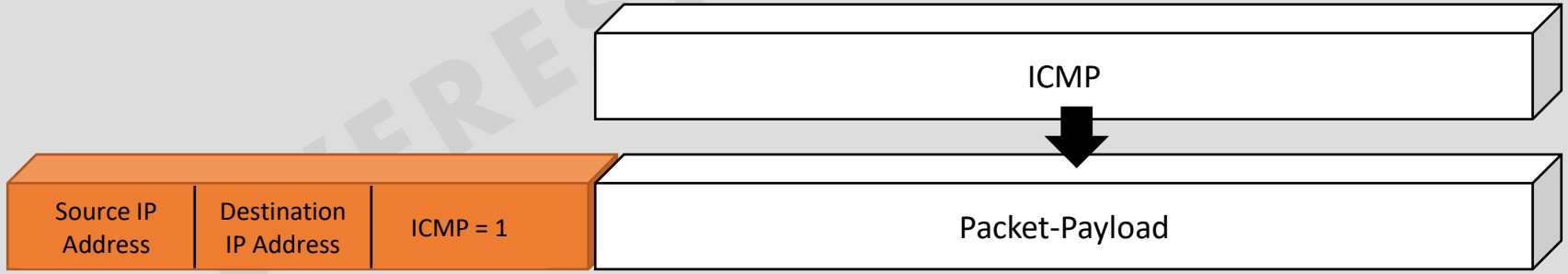
CGR1240

Scenario 0 | New | Delete | Toggle PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	N

Extended ACL (ICMP)

Numbered ACL	Named ACL	Filtered Information
Standard (1–99) (1300–1999)	**Standard**	- Source IP
Extended (100–199) (2000–2699)	**Extended**	- Source & Dest. IP - Source & Dest. Port - IP Protocol (**IP**, TCP, UDP, **ICMP**, EIGRP, IGMP,…) - Protocol information



Extended ACL (ICMP)

IPv4 Header

Version	Header Length	Type of Service	Total Length
Identifier		Flags	Fragment Offset
Time To Live	**Protocol (ICMP = 1)**	Header Checksum	
Source Address			
Destination Address			
Options + Padding			
DATA (Payload): **ICMP Packet**			

Type	Codes	Description
0/8	0	Echo Reply/Echo Request
3	0-15	Destination Unreachable
4	0	Source Quench
5	0-3	Redirect
9/10	0	Router Advertisement
11	0-1	Time Exceeded
12	0	Parameter Problem
13/14	0	Timestamp Request/Timestamp Reply
17/18	0	Address Mask Request/Address Mask Reply

ICMP Header

Type	**Code**	**Checksum**
Identifier		Sequence number
Data (default is 32 Bytes)		

رابط دورة المدخل الى شبكات سيسكو CCNA 200-301 على موقع يودمي , هذه الدورة من إعداد المدرب عبد الرحمن العلوش

icmp

	Time	Source	Destination	Protocol	Length	Info
86	29.096536	192.168.1.10	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=71/18176, ttl=128 (reply in 87)
87	29.097093	192.168.1.1	192.168.1.10	ICMP	74	Echo (ping) reply id=0x0001, seq=71/18176, ttl=30 (request in 86)

Wireshark · Packet 86 · Ethernet

```
> Frame 86: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on
> Ethernet II, Src: Pegatron_bd:2d:31 (38:60:77:bd:2d:31), Dst: D-LinkIn_
v Internet Protocol Version 4, Src: 192.168.1.10, Dst: 192.168.1.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x7533 (30003)
  > Flags: 0x0000
    Fragment offset: 0
    Time to live: 128
    Protocol: ICMP (1)
    Header checksum: 0x4232 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.10
    Destination: 192.168.1.1
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4d14 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 71 (0x0047)
    Sequence number (LE): 18176 (0x4700)
    [Response frame: 87]
  v Data (32 bytes)
      Data: 6162636465666768696a6b6c6d6e6f707172737475767761…
      [Length: 32]
```

Request

Wireshark · Packet 87 · Ethernet

```
> Frame 87: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on
> Ethernet II, Src: D-LinkIn_12:6d:b6 (74:da:da:12:6d:b6), Dst: Pegatron
v Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.10
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x7533 (30003)
  > Flags: 0x0000
    Fragment offset: 0
    Time to live: 30
    Protocol: ICMP (1)
    Header checksum: 0xa432 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.1
    Destination: 192.168.1.10
v Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x5514 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 71 (0x0047)
    Sequence number (LE): 18176 (0x4700)
    [Request frame: 86]
    [Response time: 0.557 ms]
  v Data (32 bytes)
      Data: 6162636465666768696a6b6c6d6e6f707172737475767761…
      [Length: 32]
```

Reply

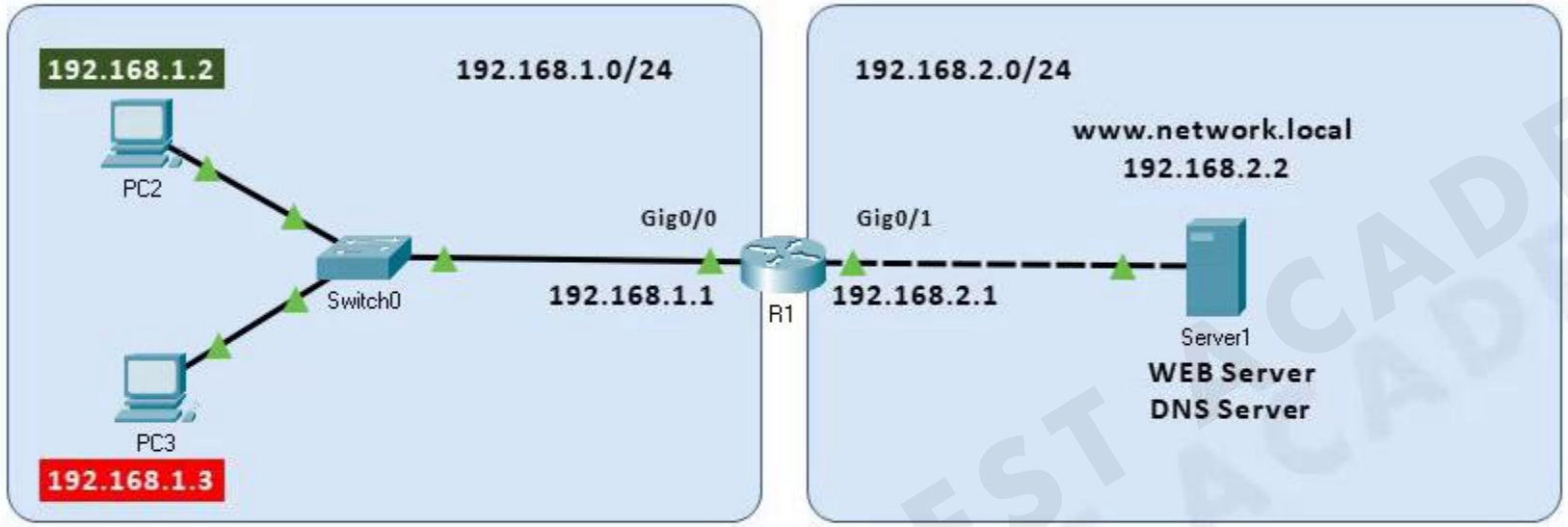
Extended ACL (ICMP)

Extended ACL Syntax with ICMP Messages Enabled

```
#access-list 100-199 {permit | deny} {ICMP} {Source_IP} {Source-wildcard}  {Destination_IP} {Destination-wildcard} {icmp_message}
```

Extended ACL (ICMP)

#access-list 100-199 {permit | deny} **ICMP** {Source_IP} {Source-wildcard} {Destination_IP} {Destination-wildcard} {icmp_message}




```
access-list  100  permit  icmp  host  192.168.1.2  host  192.168.2.2  echo
access-list  100  permit  udp   host  192.168.1.2  host  192.168.2.2  eq 53
access-list  100  permit  tcp   host  192.168.1.2  host  192.168.2.2  eq 80
access-list  100  deny    ip    any   host  192.168.2.2
interface gig0/0
ip access-group  100  in
```

Named ACL

Numbered ACL	Named ACL	Filtered Information
Standard (1–99) (1300–1999)	**Standard**	- Source IP
Extended (100–199) (2000–2699)	**Extended**	- Source & Dest. IP - Source & Dest. Port - IP Protocol (**IP**, TCP, UDP, **ICMP**, EIGRP, IGMP,…) - Protocol information

- Named ACLs had three big differences compared to numbered ACLs:
  - Using names instead of numbers to identify the ACL, making it easier to remember the reason for the ACL.
  - Using ACL subcommands, not global commands, to define the action and matching parameters.
  - Using ACL editing features that allow the CLI user to delete individual lines from the ACL and insert new lines.

COM4 - Tera Term VT

File Edit Setup Control Window Help

```
Router#
```

acl.txt - Notepad

File Edit Format View Help

```
conf t
access-list 100 permit tcp host 10.0.0.1 host 200.1.1.1 eq 22
access-list 100 permit tcp host 10.0.0.1 host 200.1.1.1 eq 23
access-list 100 permit tcp host 10.0.0.1 host 200.1.1.1 eq 80
access-list 100 deny ip any any
end

------------------------------------------------------------
conf t
ip access-list extended ALC1
 permit tcp host 10.0.0.1 host 200.1.1.1 eq 22
 permit tcp host 10.0.0.1 host 200.1.1.1 eq 23
 permit tcp host 10.0.0.1 host 200.1.1.1 eq 80
 deny   ip any any
end

------------------------------
conf t
no ip access-list extended ALC1
end
```

Ln 17, Col 1 | 100% | Windows (CRLF) | UTF-8