

ACCESS - CONTROL LIST

- ✓ Access List is a basic firewall software integrated in Cisco IOS.
- ✓ Act as a protocol *"firewall"*
- ✓ Provides layer 3 and layer 4 security
- ✓ Control the flow of traffic from one network to another
- ✓ Filters the IP packets
- ✓ There should be at least one permit statement
- ✓ An implicit deny blocks all traffic by default
- ✓ Can have one access list per interface per direction
- ✓ Deny, Permit, Source Address, Destination Address, Inbound, Outbound
- ✓ Operators (eq, neq, lt, gt)

ACCESS LIST TYPES:

- ✓ STANDARD ACCESS LIST.
- ✓ EXTENDED ACCESS LIST.
- ✓ NAMED ACCESS LIST.

STANDARD ACCESS LISTS:

Standard access lists for IP checks only the '*source address*'.

RANGE: 1 to 99. Expanded Range: 1000 – 1999

EXTENDED ACCESS LISTS:

Extended access lists checks both '*source*' and '*destination*' IP addresses. They also can check for '*specific protocols*', '*port numbers*', and other parameters.

RANGE: 100 to 199. Expanded Range: 2000 to 2699.

NAMED ACCESS LIST

A feature for Cisco IOS Release 11.2 or newer, Named IP access lists can be used to delete individual entries from a specific access list. This enables you to modify your access lists without deleting and then reconfiguring them.

Removing of specific statement in a numbered access-lists is not possible

Wildcard Mask

✓ It is a value to inform access list to check the IP address.

✓ A wildcard mask bit **0** means **check** the corresponding bit value.

✓ A wildcard mask bit **1** means **will not check** that corresponding bit value.

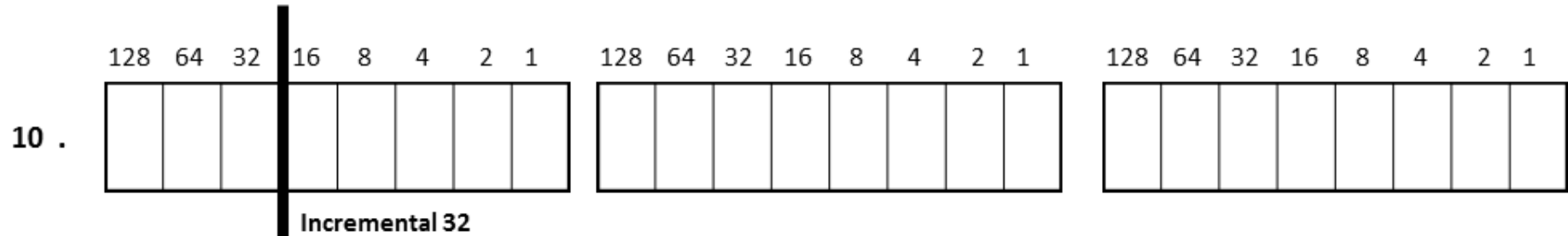
✓ The use of wildcard masks is most prevalent when building Access Control Lists (ACLs) on Cisco routers. ACLs are filters and make use of wildcard masks to define the scope of the address filter.

✓ Address filtering uses wildcard masking to indicate to the software whether to check or ignore corresponding IP address bits when comparing the address bits in an access list entry to a packet being submitted to the access list.

✓ By carefully setting wildcard masks, an administrator can select single or several IP addresses for permit or deny tests.

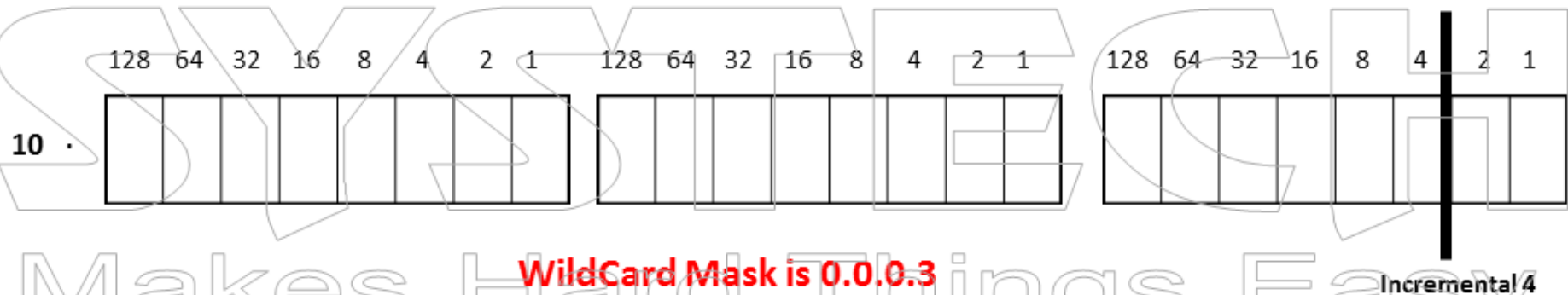
✓ If you do not supply a wildcard mask with a source or destination address in an access list statement, the software assumes a default wildcard mask of 0.0.0.0.

FIND WILDCARD MASK FOR 10.0.0.0 / 11 ?



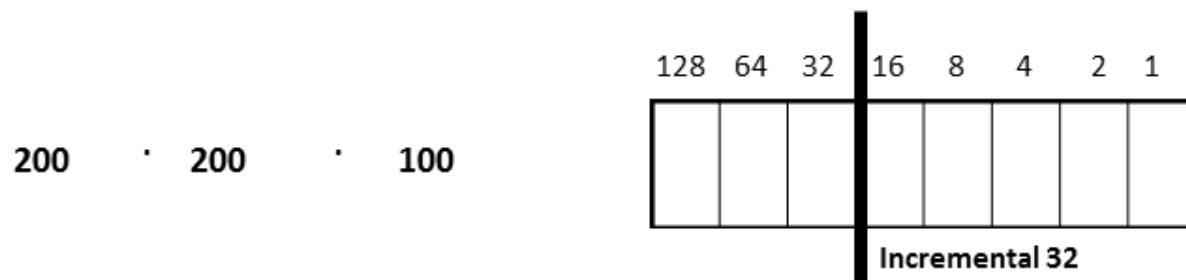
Wildcard Mask is 0.31.255.255

FIND WILDCARD MASK FOR 10.0.0.0 / 30 ?



Wildcard Mask is 0.0.0.3

FIND WILDCARD MASK FOR 200.200.100.0 / 27 ?



Wildcard Mask is 0.0.0.31

Activate Windows
Go to Settings to activate Windows.

Transmission Control Protocol (TCP)

The Transmission Control Protocol (TCP) is a virtual circuit protocol that is one of the core protocols of the Internet protocol suite. Using TCP, applications on networked hosts can create *connections* to one another, over which they can exchange data in packets. The protocol guarantees reliable and in-order delivery of data from sender to receiver

User Datagram Protocol (UDP)

The User Datagram Protocol (UDP) is one of the core protocols of the Internet protocol suite. Using UDP, programs on networked computers can send short messages sometimes known as datagram to one another. UDP does not provide the reliability and ordering guarantees that TCP does. Compared to TCP, UDP is required for broadcast (send to all on local network) and multicast (send to all subscribers).

Reserved TCP and UDP Port Numbers

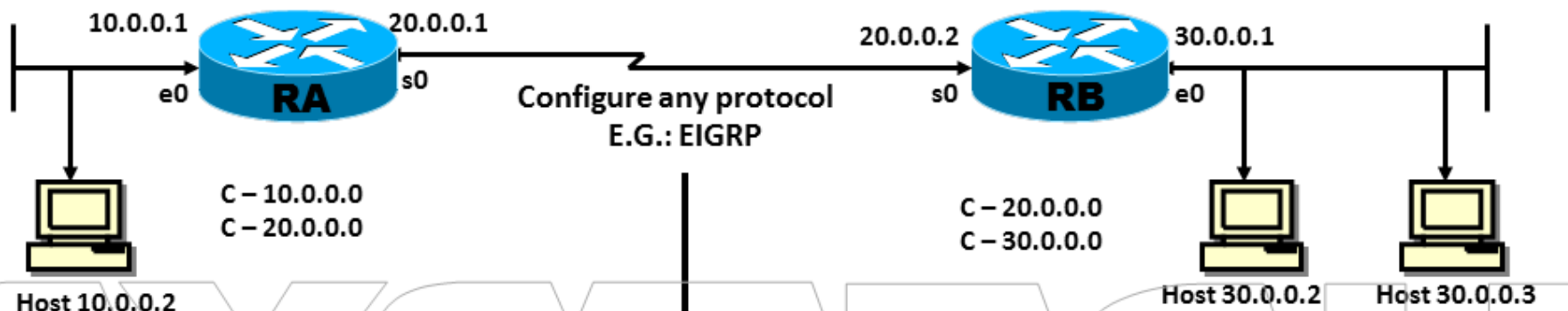
DECIMAL	KEYWORD	DESCRIPTION
0		Reserved
1 – 4		Unassigned
5	RJE	Remote Job Entry
7	ECHO	Echo
9	DISCARD	Discard
11	USERS	Active Users
13	DAYTIME	Daytime
15	NETSTAT	Who is Up or NETSTAT
17	QUOTE	Quote of the Day
19	CHARGEN	Character Generator
20	FTP-DATA	File Transfer Protocol (data)
21	FTP	File Transfer Protocol
23	TELNET	Terminal Connection
25	SMTP	Simple Mail Transfer Protocol
37	TIME	Time of Day
39	RLP	Resource Location Protocol
42	NAMESERVER	Host Name Server
43	NICNAME	Who Is

Activate Windows
Go to Settings to activate Windows.

Reserved TCP and UDP Port Numbers

DECIMAL	KEYWORD	DESCRIPTION
53	DOMAIN	Domain Name Server
67	BOOTPS	Bootstrap Protocol Server
68	BOOTPC	Bootstrap Protocol Client
69	TFTP	Trivial File Transfer Protocol
75		Any Private Dial-out Service
77		Any Private RJE Service
79	FINGER	Finger
80	HTTP	Hypertext Transfer Protocol
95	SUPDUP	SUPDUP Protocol
101	HOSTNAME	NIC Host Name Server
102	ISO-TSAP	ISO-TSAP
113	AUTH	Authentication Service
117	UUCP-PATH	UUCP Path Service
119	NNTP	N/W News Transfer Protocol
123	NTP	Network Time Protocol
133-159		Unassigned 1
60-223		Reserved
224-241		Unassigned
242-255		Unassigned

STANDARD ACCESS - LIST



Set Password for TELNET in RA.

Now the Host 30.0.0.2 and 30.0.0.3 can access Router A through TELNET.

To deny 30 Network (30.0.0.2 and 30.0.0.3 must not access RA)

```
RA # access-list 1 deny 30.0.0.0 0.255.255.255
```

Range

Wild card mask

30.0.0.3 must alone access RA.

```
RA # access-list 1 permit 30.0.0.3 0.0.0.0
```

(or)

```
RA # access-list 1 permit host 30.0.0.3 (without wildcard mask)
```

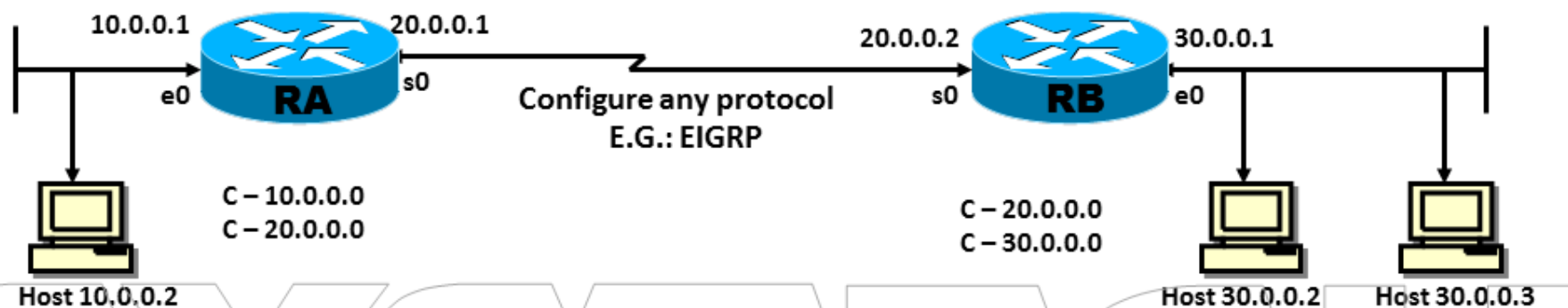
```
RA # line VTY 0 4
```

```
RA # access-class 1 in
```

Range

```
RA # sh ip access-list.
```


EXTENDED ACCESS - LIST



FTP (file transfer protocol) is a commonly used protocol for exchanging files over any network that supports the TCP/IP protocol (such as the Internet or an intranet).

PORT NO: 21

HTTP (Hypertext Transfer Protocol) is a method used to transfer or convey information on the World Wide Web. Its original purpose was to provide a way to publish and retrieve HTML pages

PORT NO: 80

ICMP (Internet Control Message Protocol) is one of the core protocols of the Internet protocol suite. It is chiefly used by networked computers' operating systems to send error messages—indicating, for instance, that a requested service is not available or that a host or router could not be reached.

To installing IIS and FTP features

Open **control panel** → Click **Programs and Features**

The screenshot shows the 'Programs and Features' window in Windows. The title bar is blue and says 'Programs and Features'. The address bar shows the path: 'Control Panel > All Control Panel Items > Programs and Features'. On the left sidebar, there are links: 'Control Panel Home', 'View installed updates', and 'Turn Windows features on or off' (with a blue arrow pointing to it). The main area has the heading 'Uninstall or change a program' and a sub-heading 'To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.' Below this is a table with columns: 'Name', 'Publisher', 'Installed On', 'Size', and 'Version'. The table is currently empty. At the bottom, there is a summary bar that says 'Currently installed programs Total size: 339 MB' and '3 programs installed'. The Windows taskbar is visible at the bottom with icons for Internet Explorer, File Explorer, and the Start button. The system tray shows the time as 12:04 AM on 6/21/2017.

Programs and Features

Control Panel > All Control Panel Items > Programs and Features

Search Programs and Features

Control Panel Home

View installed updates

[Turn Windows features on or off](#)

Uninstall or change a program

To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.

Name	Publisher	Installed On	Size	Version
------	-----------	--------------	------	---------

Currently installed programs Total size: 339 MB
3 programs installed

Activate Windows
Go to Settings to activate Windows.

12:04 AM
6/21/2017

Select IIS and FTP services and click ok

Programs and Features

Control Panel Home

Uninstall or change a program

To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.

View installed updates

Turn Windows features on or off

Organize

Name

Windows Features

Turn Windows features on or off

To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.

- ☐ .NET Framework 3.5 (includes .NET 2.0 and 3.0)
- ☒ .NET Framework 4.5 Advanced Services
- ☐ Active Directory Lightweight Directory Services
- ☐ Hyper-V
- ☒ Internet Explorer 10
- ☒ Internet Information Services
 - ☒ FTP Server
 - ☒ Web Management Tools
 - ☒ World Wide Web Services
- ☐ Internet Information Services Hostable Web Core
- ☒ Media Features
- ☐ Microsoft Message Queue (MSMQ) Server

OK Cancel

Currently installed programs Total size: 339 MB
3 programs installed

Activate Windows
Go to Settings to activate Windows

12:04 AM
6/21/2017

HTTP

Save systech.html files in c:\inetpub\wwwroot

Now the Host 30.0.0.2 and 30.0.0.3 can access http.
(Type in Internet Explorer - http:\\10.0.0.2\systech.html in 30.0.0.2 & 30.0.0.3)

Deny 30.0.0.2 accessing HTTP:

```
RA # access-list 150 deny tcp host 30.0.0.2 host 10.0.0.2 eq 80
```

```
RA # access-list 150 permit ip any any  
(or)
```

```
RA # access-list 150 permit tcp 30.0.0.0 0.255.255.255 10.0.0.0 0.255.255.255.
```

```
RA # int s0
```

```
RA # ip access-group 150 in
```

Now HTTP will not work in 30.0.0.2 but Host 30.0.0.3 can access HTTP.

Activate Windows
Go to Settings to activate Windows.

Named & Time based Access List

RA # time-range WEBSERVER

RA #periodic daily 10:00 to 18:00

RA # ip access-list extended WEBSERVER

RA # permit tcp any host 10.0.0.2 eq 80 time-range WEBSERVER

RA # int s0

RA # ip access-group WEBSERVER in

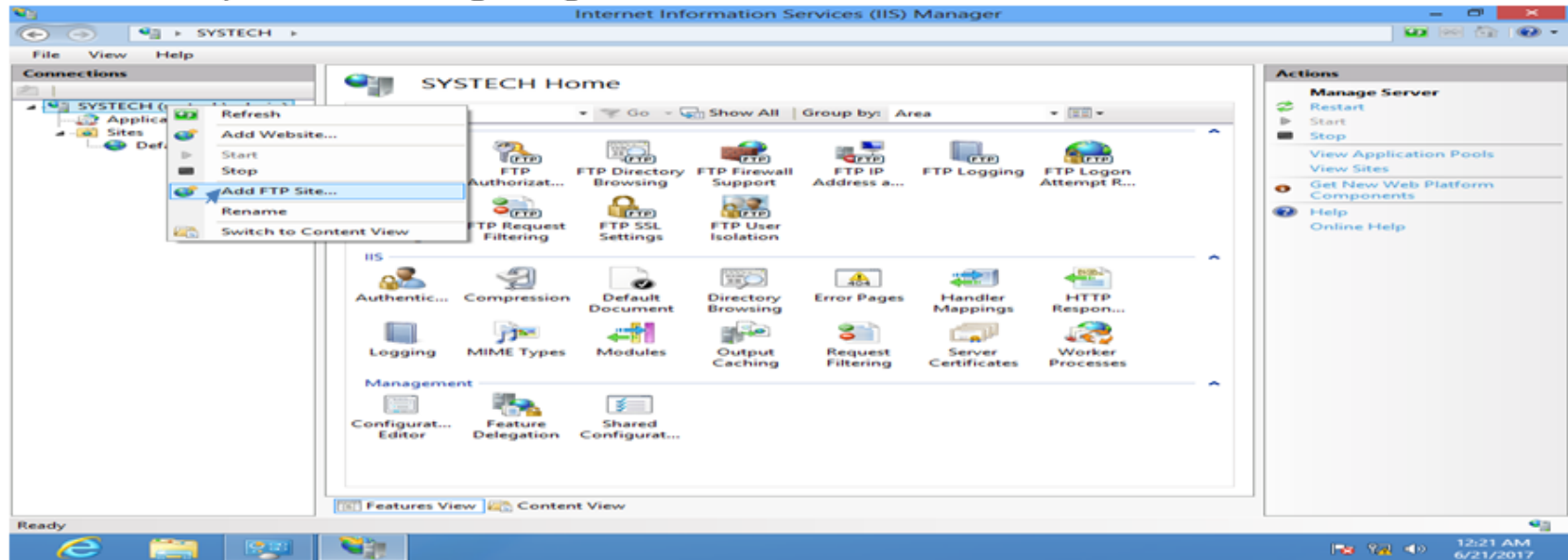
Now WEBSERVER will not work in 30.0.0.2 and Host 30.0.0.3 can access HTTP.

RA # sh clock

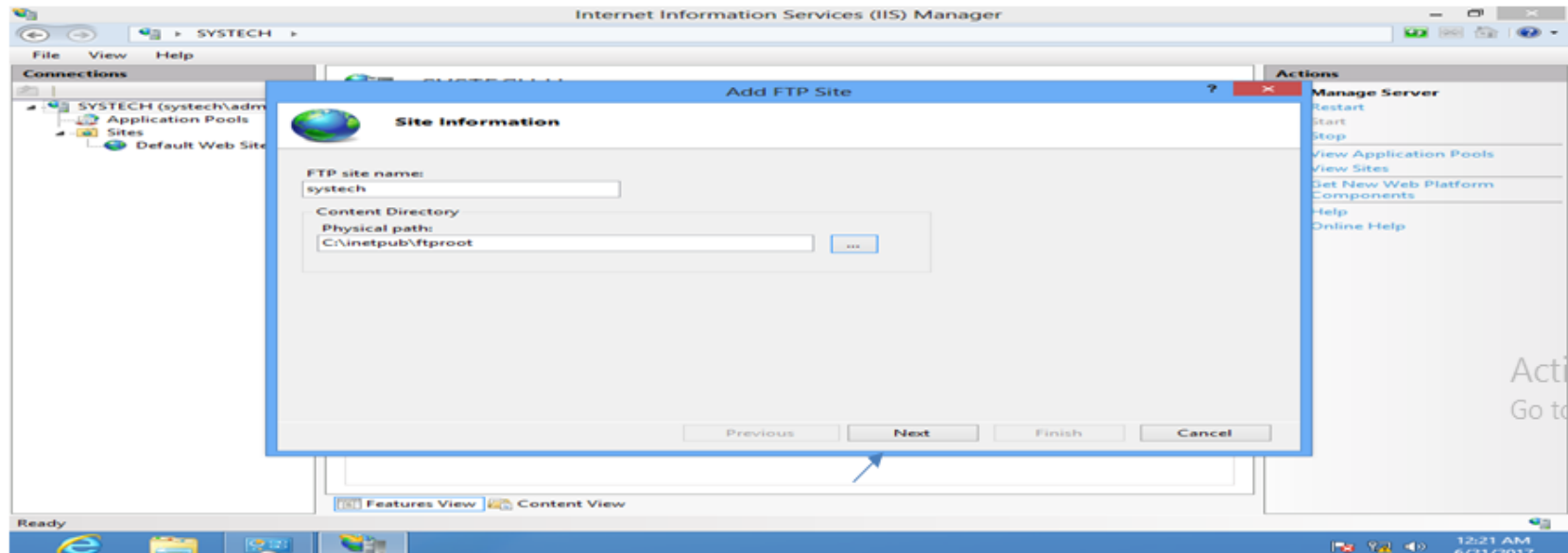
RA # clock set 15:03:00 20 december 2012.

Configuring FTP

Step 1: Open IIS Manager right click **Site** click **Add FTP Site**

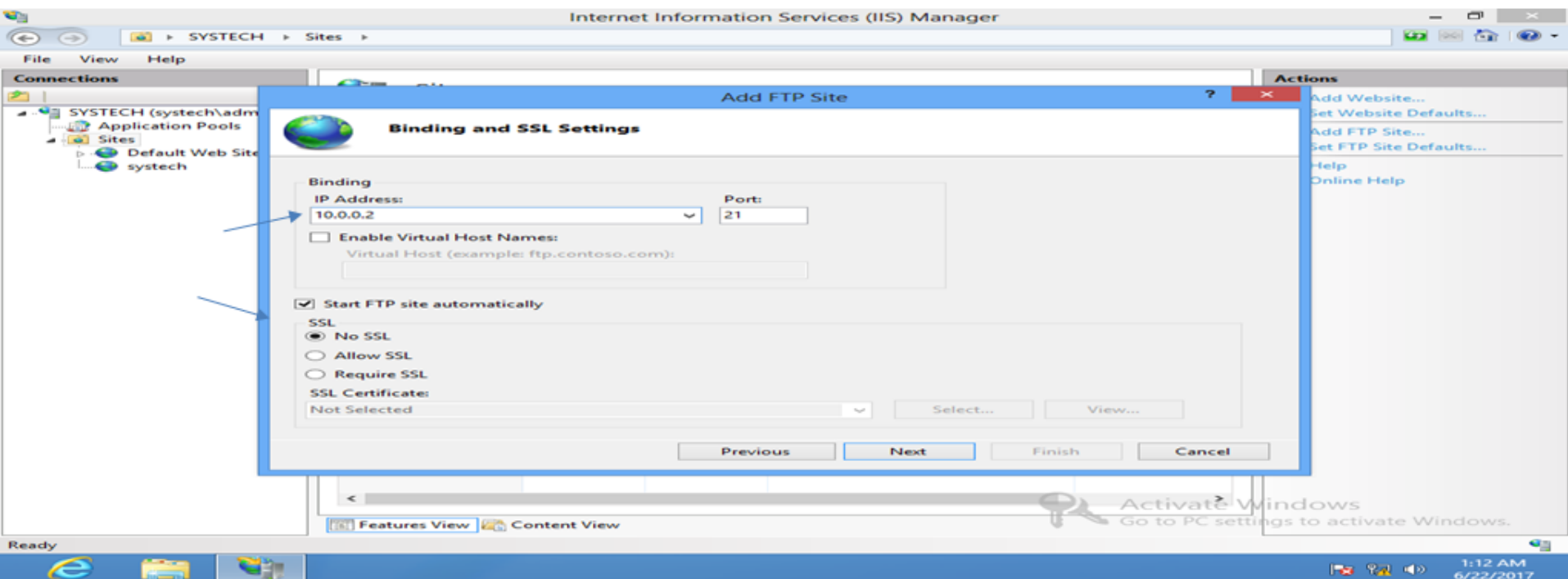


Step 2: Enter **FTP file name** and choose the **FTP Folder** location

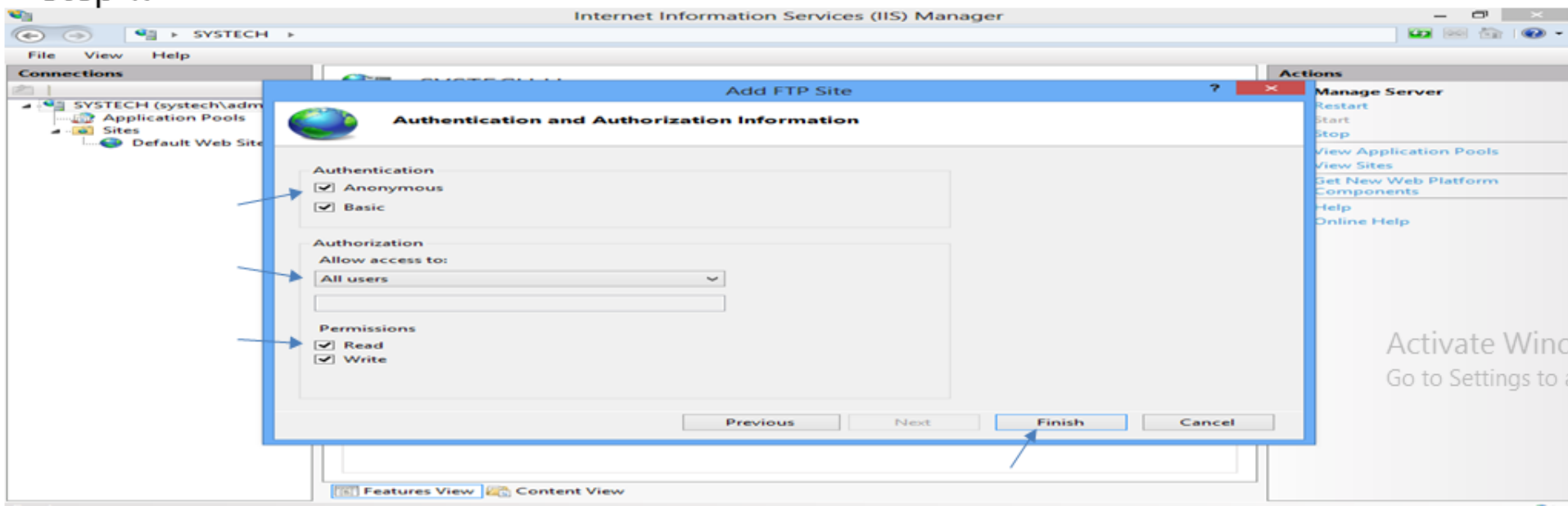


Activate Window
Go to Settings to a

Step 3: Enter the IP Address and click Next.



Step 4:



FTP

Save setup files in c:\inetpub\ftproot

Now the Host 30.0.0.2 and 30.0.0.3 can access FTP.
(Type in Internet Explorer ftp://10.0.0.2 in 30.0.0.2 & 30.0.0.3)

Deny 30.0.0.2 accessing FTP:

```
RA # access-list 100 deny tcp host 30.0.0.2 host 10.0.0.2 eq 21 (or) ftp
```

```
RA # access-list 100 permit ip any any  
(or)
```

```
RA # access-list 100 permit tcp 30.0.0.0 0.255.255.255 10.0.0.0 0.255.255.255.
```

```
RA # int s0
```

```
RA # ip access-group 100 in
```

Now FTP will not work in 30.0.0.2 but Host 30.0.0.3 can access FTP.

Activate Windows
Go to Settings to activate Windows.

ICMP

Now our Network 10 can ping Host 30.0.0.2 and 30.0.0.3.
(in host 10.0.0.2 ping 30.0.0.1 & 30.0.0.2, it will ping)

Deny 10.0.0.2 accessing 30.0.0.0 N/W:

RA # access-list 170 deny icmp host 10.0.0.2 30.0.0.0 0.255.255.255 echo.
Range

RA # access-list 170 permit ip any any

RA # int e0

RA # ip access-group 170 in

Now host 10.0.0.2 will not ping with 30.0.0.2 and 30.0.0.3