Cybersecurity

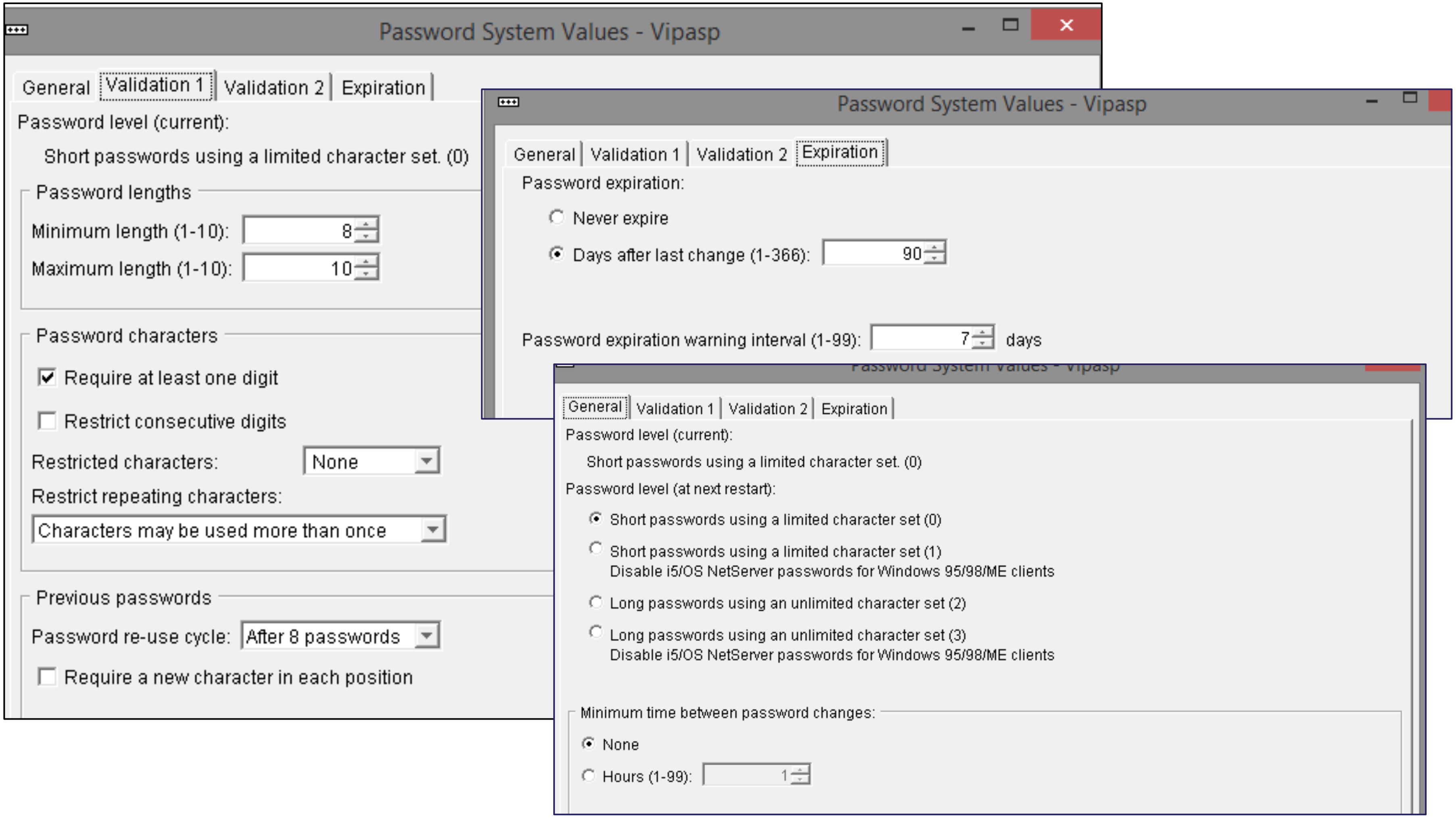
Network Security

- Network security comprises authentication and encryption
- Authentication is typically accomplished through a username and password
- Other forms of authentication are digital certificates, smart cards, and biometrics

Administrator Account

- User provides password for default administrator account
- Default administrator account name should be changed to better secure network
- Ability to delete or rename the administrator account varies according to operating system

Setting Password Criteria (admin)



Password System Values - Vipasp

General | Validation 1 | Validation 2 | Expiration

Password level (current):

Short passwords using a limited character set. (0)

Password lengths

Minimum length (1-10): 8

Maximum length (1-10): 10

Password characters

☑ Require at least one digit

□ Restrict consecutive digits

Restricted characters: None

Restrict repeating characters:

Characters may be used more than once

Previous passwords

Password re-use cycle: After 8 passwords

□ Require a new character in each position

Password System Values - Vipasp

General | Validation 1 | Validation 2 | Expiration

Password expiration:

○ Never expire

● Days after last change (1-366): 90

Password expiration warning interval (1-99): 7 days

Password System Values - Vipasp

General | Validation 1 | Validation 2 | Expiration

Password level (current):

Short passwords using a limited character set. (0)

Password level (at next restart):

● Short passwords using a limited character set (0)

○ Short passwords using a limited character set (1)
Disable i5/OS NetServer passwords for Windows 95/98/ME clients

○ Long passwords using an unlimited character set (2)

○ Long passwords using an unlimited character set (3)
Disable i5/OS NetServer passwords for Windows 95/98/ME clients

Minimum time between password changes:

● None

○ Hours (1-99): 1

User Account Passwords

- To make passwords more secure administrators should:
  - Set defaults for password histories, age, and length
  - Educate users about poor and secure passwords

Poor Passwords

- Poor passwords contain:
  - Words that are found in a dictionary
  - Names familiar to the password owner
  - Keyboard patterns
  - Social security numbers
- Secure passwords are less vulnerable to hashing techniques

Wired Equivalent Privacy (WEP)

- First attempt use encryption to secure the data transferred across a wireless network
- Algorithm not complex and can be easily cracked
- A VPN can add to the security set in place by WEP

Wi-Fi Protected Access (WPA)

- Developed by the Wi-Fi organization to overcome the vulnerabilities of WEP
- Compatible with 802.11 devices
- Wi-Fi Protected Access 2 (WPA2) is an enhanced version of WPA
- WPA2 is compatible with the 802.11i standard

Denial of Service (DoS)

- One of the most common attacks on a server
- Can overload a server to the point that it crashes or is not able to complete a legitimate user request

Trojan Horse

- Example: Free download that contains malicious code
- That code could contain virus, worm, or backdoor
- Example: Can imitate legitimate logon screen
- When user logs on, name and password are sent to unauthorized user

E-mail Attachments

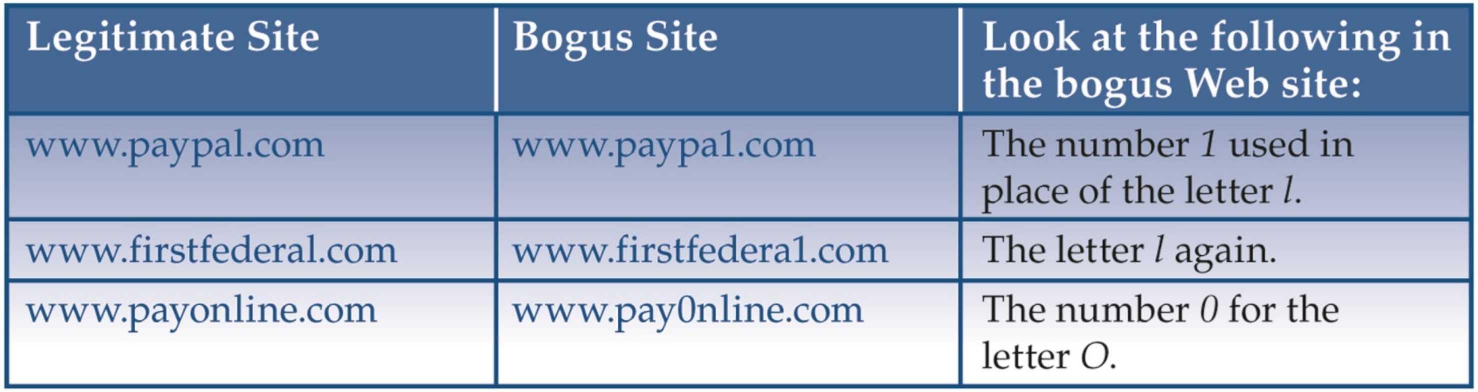
- Source of most commonly encountered viruses
- Malicious code can be programmed into attachment
- When recipient opens attachment, malicious program is activated

Social Engineering

- Relies on the gullibility of a network user and his or her respect for authority

Phishing

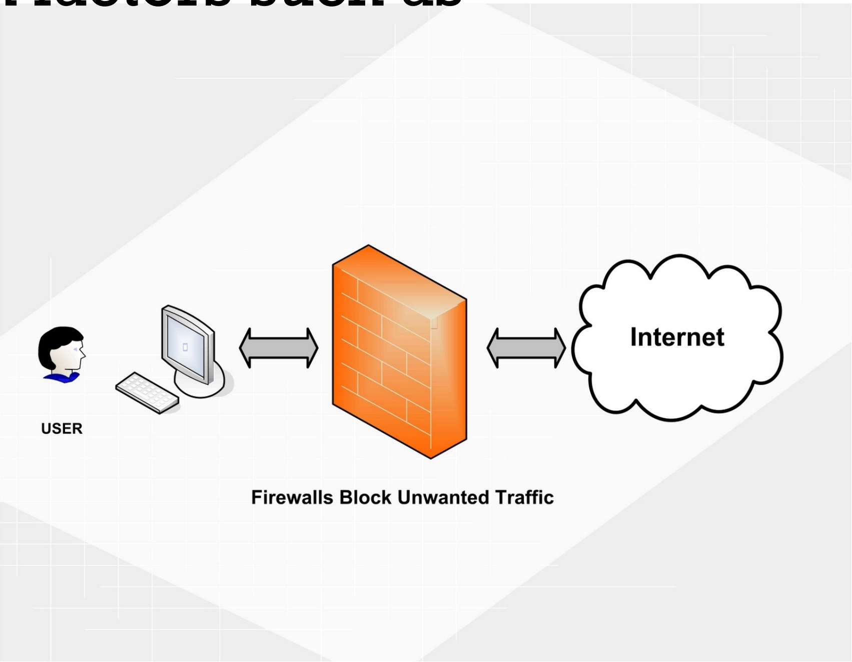
- E-mail can appear as if it’s from a legitimate company, such as a credit card company
- E-mail requests user’s personal information, such as social security number or bank account PIN
- Phony web sites that look authentic, but have slightly different domain names



Legitimate Site	Bogus Site	Look at the following in the bogus Web site:
www.paypal.com	www.paypa1.com	The number *1* used in place of the letter *l*.
www.firstfederal.com	www.firstfedera1.com	The letter *l* again.
www.payonline.com	www.pay0nline.com	The number *0* for the letter *O*.

Firewall

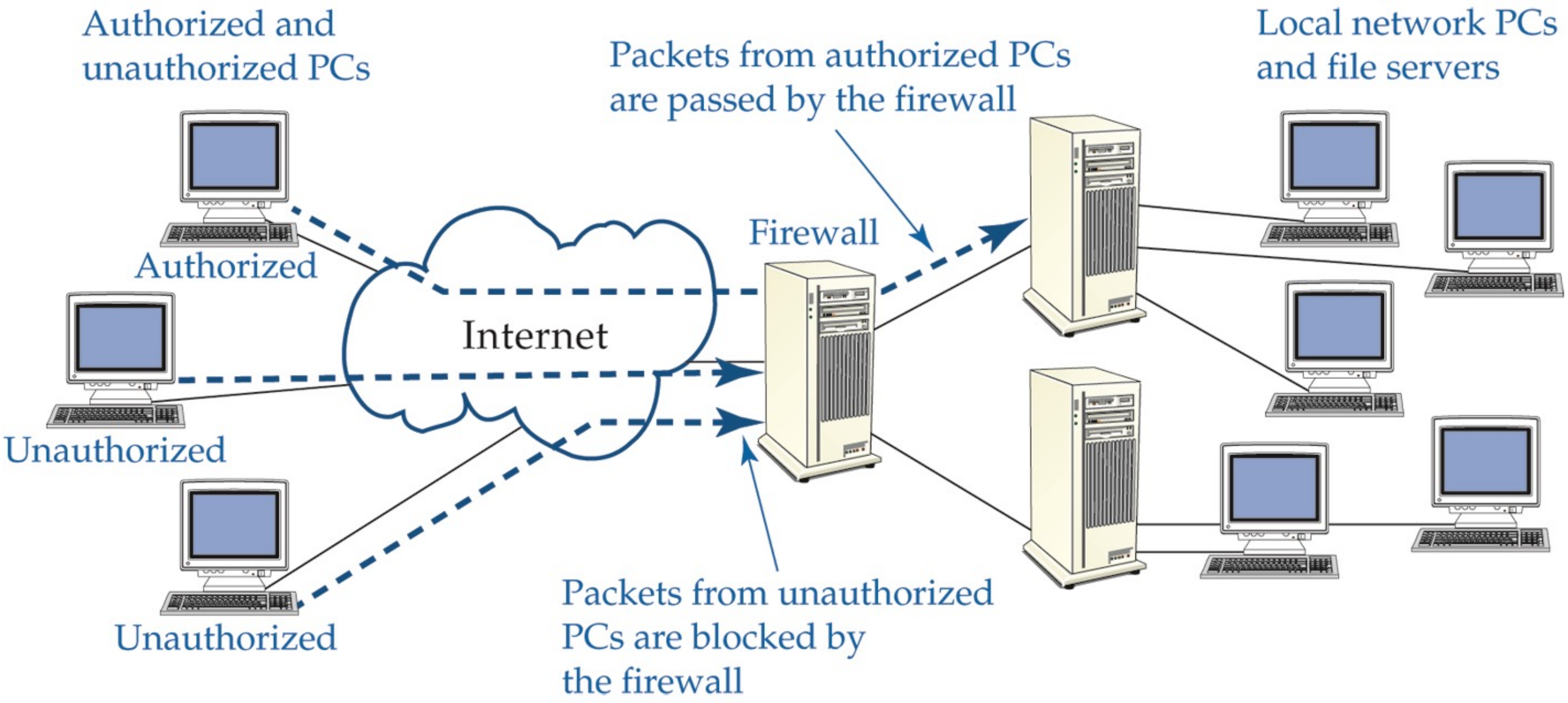
- Can consist of hardware, software, or a combination
- Servers, routers, and PCs may be used
- Designed to filter inbound and outbound flow of network packets based on factors such as
  - IP address
  - Port number
  - Software application
  - Packet contents
  - Protocol



What is a Firewall?

- A layer of security between your home network and the Internet. Since a router or modem is the main connection from a home network to the Internet, a firewall is often packaged with those devices.
- Firewalls are a combination of hardware and software. The hardware part gives firewalls excellent performance, while the software part allows firewalls to be tailored to your specific needs.

Firewall Example


Authorized and unauthorized PCs
Packets from authorized PCs are passed by the firewall
Local network PCs and file servers
Authorized
Firewall
Internet
Unauthorized
Unauthorized
Packets from unauthorized PCs are blocked by the firewall

What is a Firewall?

- Some applications outside a network require manually changing your firewall to allow them access. Examples of these applications include online games, VPN, and Voice-Over-IP.
- A firewall does not secure against every kind of data and attack. (still need to run a virus-checker on all your computers.)
- Other products such as Windows and macOS create software firewalls. These can cause network problems, because they are trying to apply different security to your network, which other firewalls will not accept. May need to disable conflicting firewalls.
- Firewall features vary by model - newer and more expensive products have more advanced features. Firewall features are described in a product's datasheet, and their configuration information is found in the manuals.
- The term firewall is often used to describe the part of a network that is protected by a firewall, as in the phrase behind the firewall. Parts of a network that are outside the firewall are more vulnerable to attack.

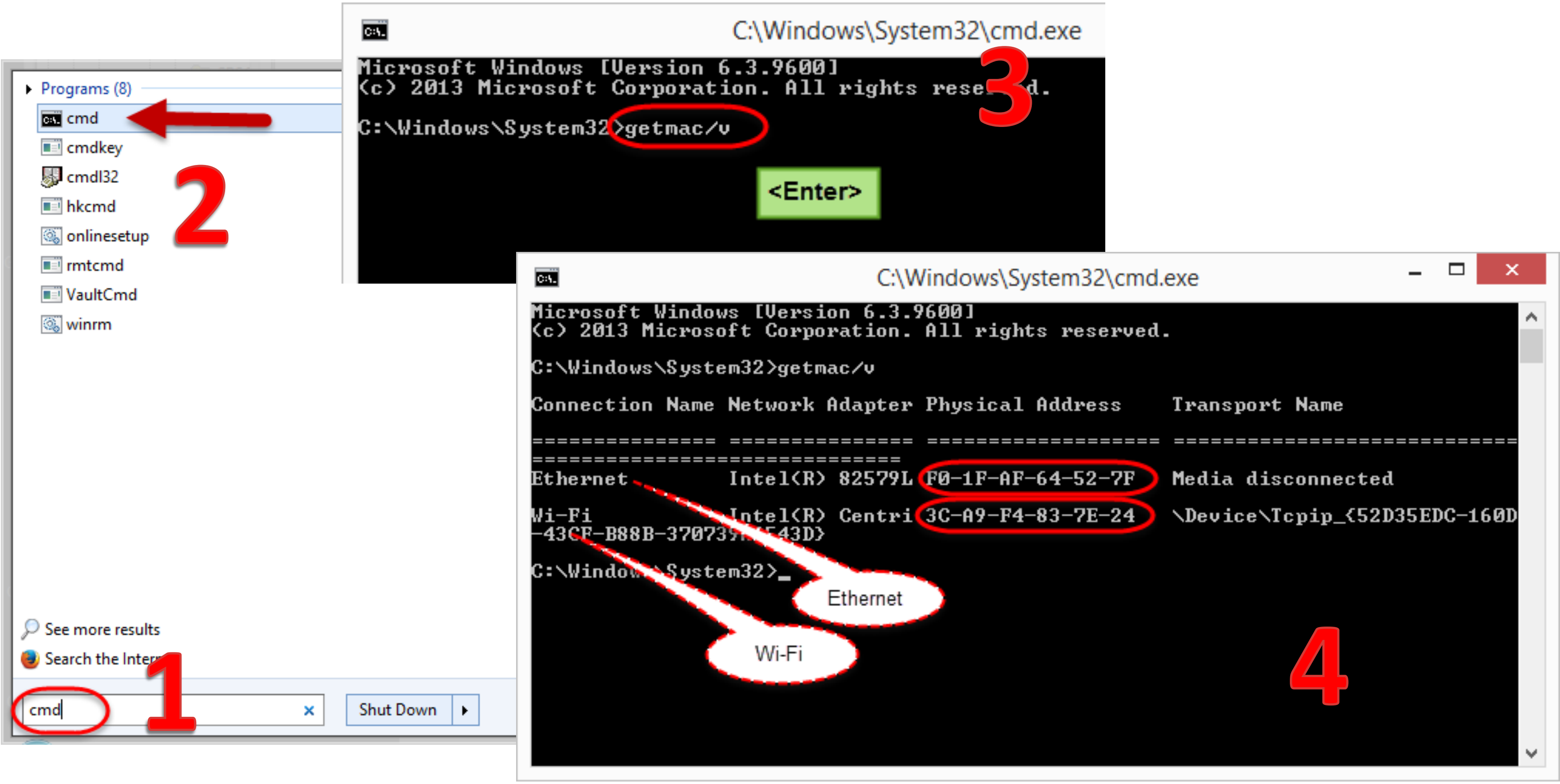
Network Address Translation (NAT)

- Allows unregistered private network addresses to communicate with legally registered IP addresses
- Advantages
  - Hides internal IP addresses, thus providing security
  - Eliminates need for multiple registered IP addresses
  - Allows multiple ISDN (Integrated Services for Digital Network) connections to be combined into one Internet connection

Media Access Control (MAC) Filtering

- To configure MAC filtering, administrator creates an Access Control List (ACL)
- ACL is located on Wireless Access Point (WAP)
- ACL contains list of MAC addresses belonging to authorized wireless network devices

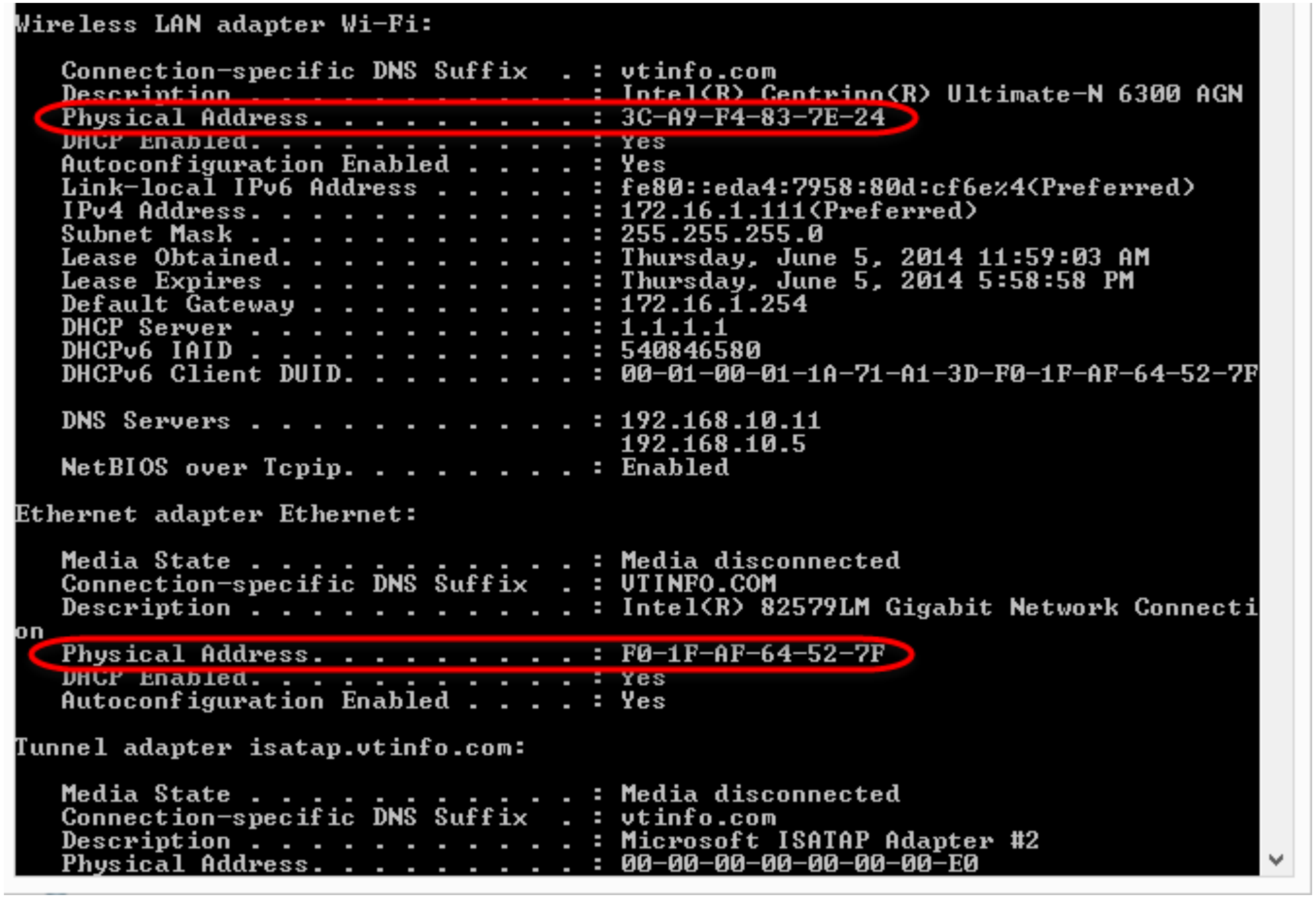
Find your MAC Address



```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights rese  d.

C:\Windows\System32>getmac/v
```

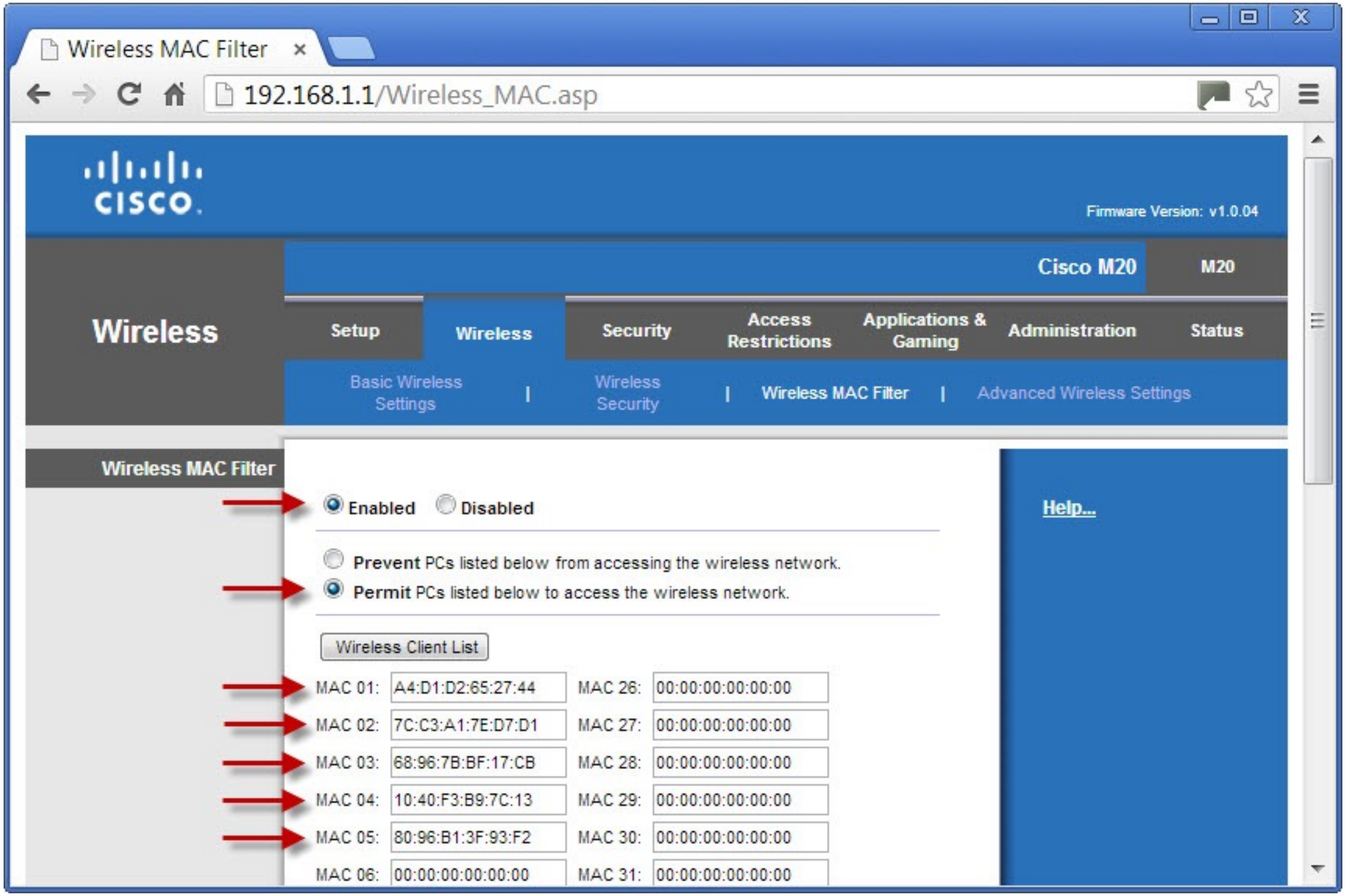
```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\System32>getmac/v

Connection Name Network Adapter Physical Address    Transport Name

=============== =============== =================== ===========================
==============================
Ethernet        Intel(R) 82579L F0-1F-AF-64-52-7F   Media disconnected

Wi-Fi           Intel(R) Centri 3C-A9-F4-83-7E-24   \Device\Tcpip_{52D35EDC-160D
-43CF-B88B-370739[illegible]43D}

C:\Windows\System32>_
```

Also: ipconfig /all



```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : vtinfo.com
   Description . . . . . . . . . . . : Intel(R) Centrino(R) Ultimate-N 6300 AGN
   Physical Address. . . . . . . . . : 3C-A9-F4-83-7E-24
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::eda4:7958:80d:cf6e%4(Preferred)
   IPv4 Address. . . . . . . . . . . : 172.16.1.111(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Thursday, June 5, 2014 11:59:03 AM
   Lease Expires . . . . . . . . . . : Thursday, June 5, 2014 5:58:58 PM
   Default Gateway . . . . . . . . . : 172.16.1.254
   DHCP Server . . . . . . . . . . . : 1.1.1.1
   DHCPv6 IAID . . . . . . . . . . . : 540846580
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-1A-71-A1-3D-F0-1F-AF-64-52-7F

   DNS Servers . . . . . . . . . . . : 192.168.10.11
                                       192.168.10.5
   NetBIOS over Tcpip. . . . . . . . : Enabled

Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : VTINFO.COM
   Description . . . . . . . . . . . : Intel(R) 82579LM Gigabit Network Connecti
on
   Physical Address. . . . . . . . . : F0-1F-AF-64-52-7F
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Tunnel adapter isatap.vtinfo.com:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : vtinfo.com
   Description . . . . . . . . . . . : Microsoft ISATAP Adapter #2
   Physical Address. . . . . . . . . : 00-00-00-00-00-00-00-E0
```

CISCO Router MAC Filter Setup



192.168.1.1/Wireless_MAC.asp

● Enabled ○ Disabled

○ **Prevent** PCs listed below from accessing the wireless network.

● **Permit** PCs listed below to access the wireless network.

MAC 01:	A4:D1:D2:65:27:44	MAC 26:	00:00:00:00:00:00
MAC 02:	7C:C3:A1:7E:D7:D1	MAC 27:	00:00:00:00:00:00
MAC 03:	68:96:7B:BF:17:CB	MAC 28:	00:00:00:00:00:00
MAC 04:	10:40:F3:B9:7C:13	MAC 29:	00:00:00:00:00:00
MAC 05:	80:96:B1:3F:93:F2	MAC 30:	00:00:00:00:00:00
MAC 06:	00:00:00:00:00:00	MAC 31:	00:00:00:00:00:00