

Module 2: Network Devices and Theory

Analog Modems



Baud: Number of tone changes per second.

Bits per Second (bps): The number of 1s and 0s that can be transmitted over the line.

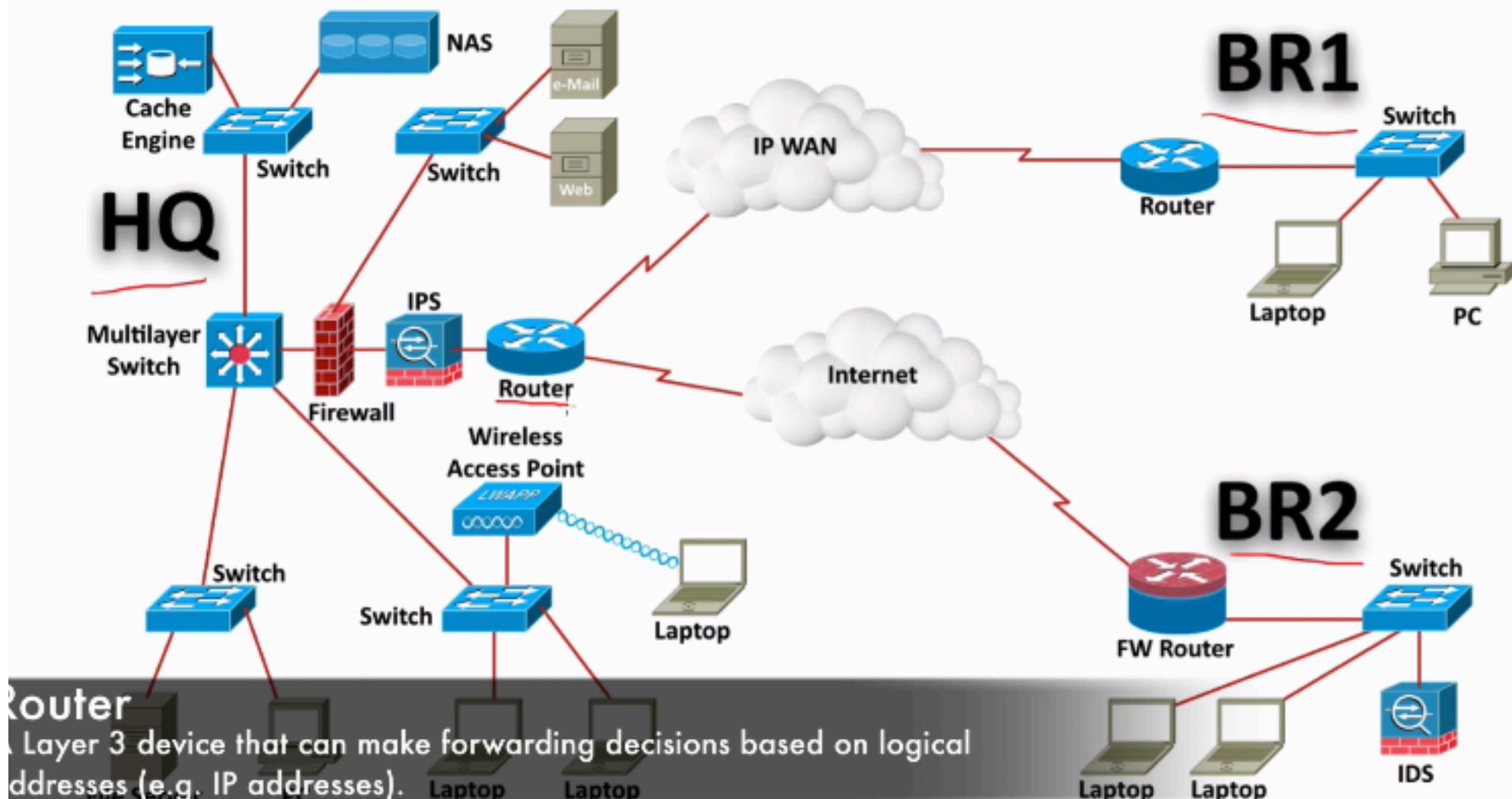
300 bps: 300 baud using one channel.

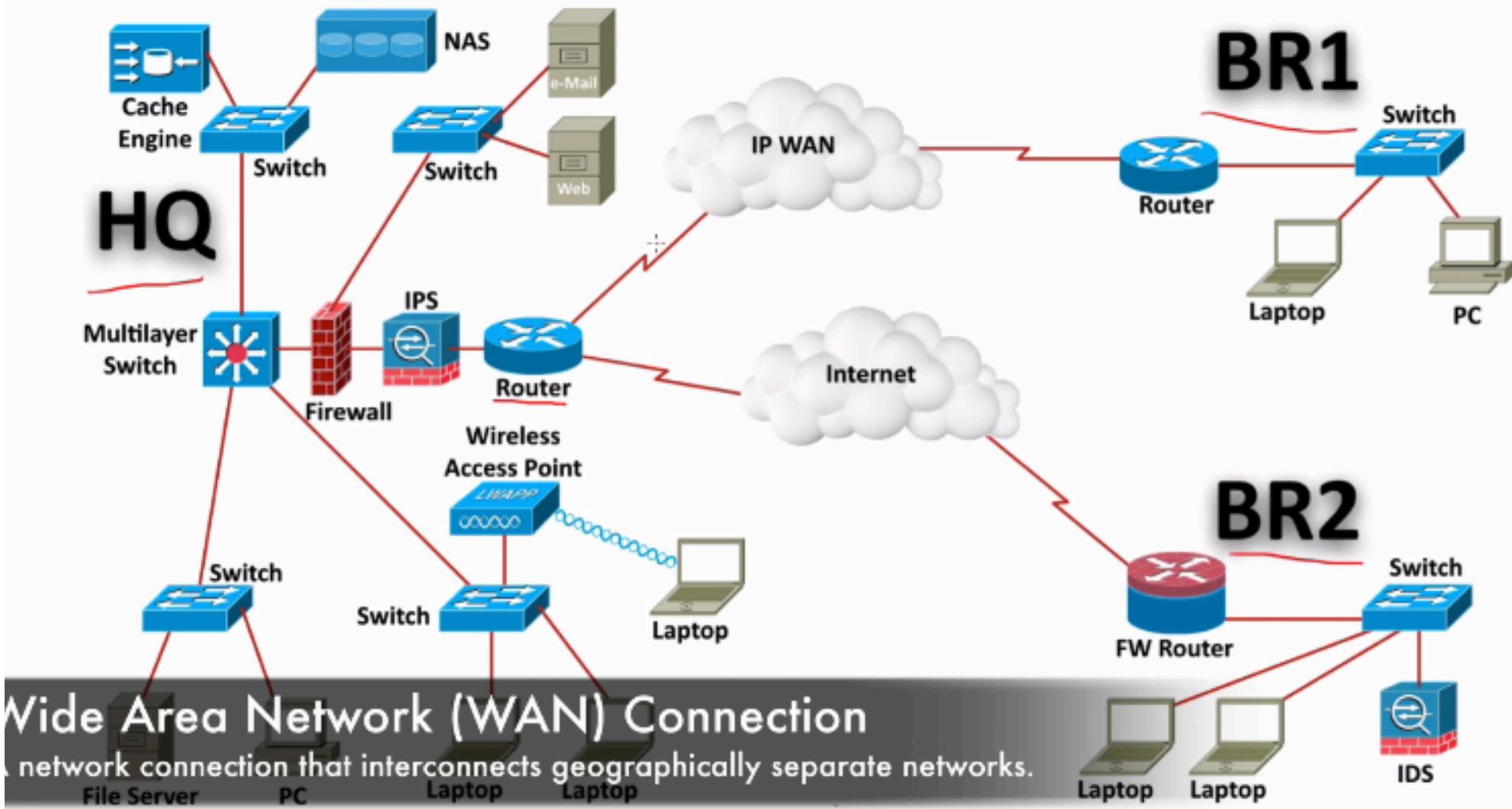
2400 bps: 2400 baud using one channel.

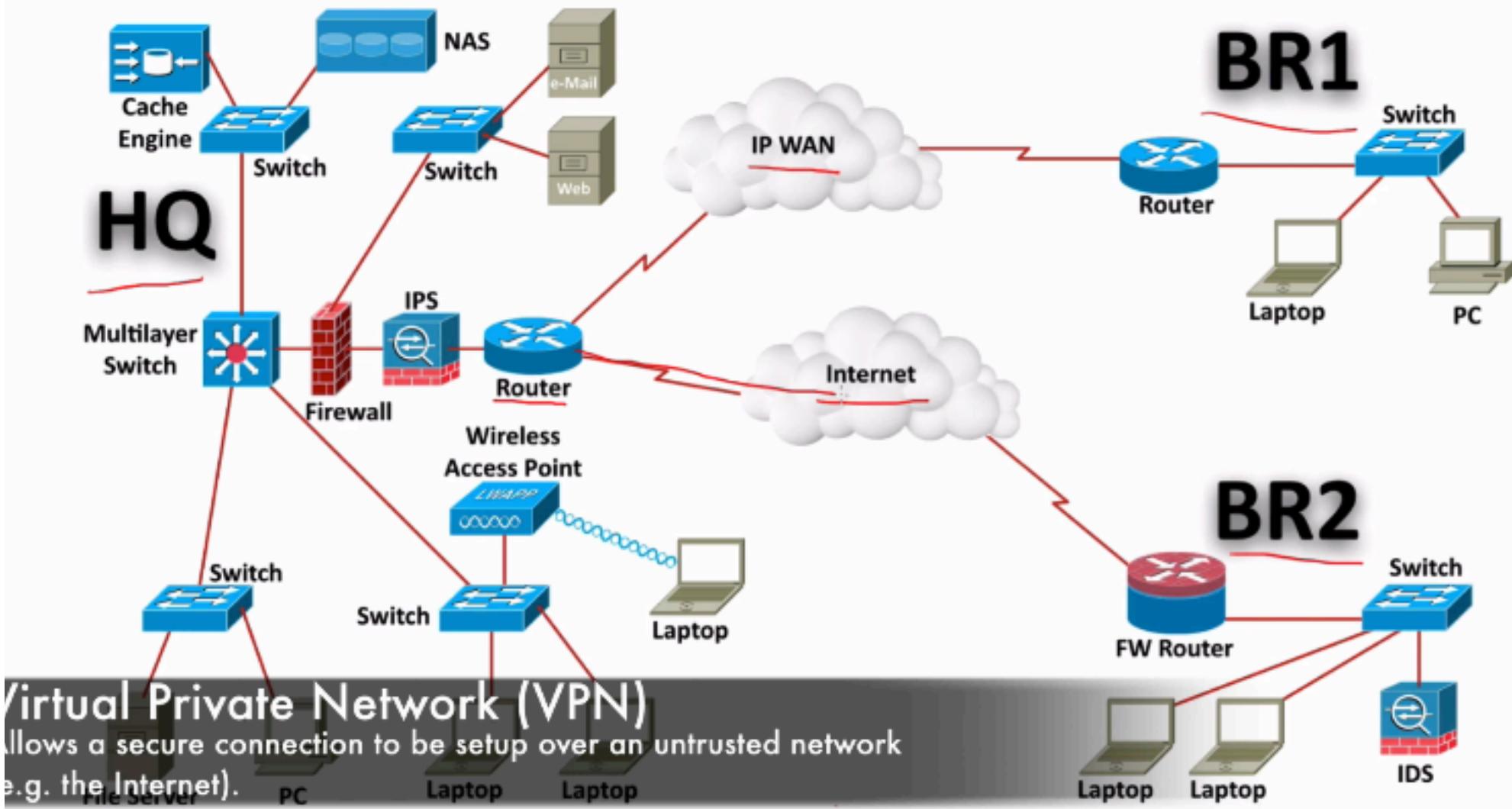
9600 bps: 2400 baud using four channels.

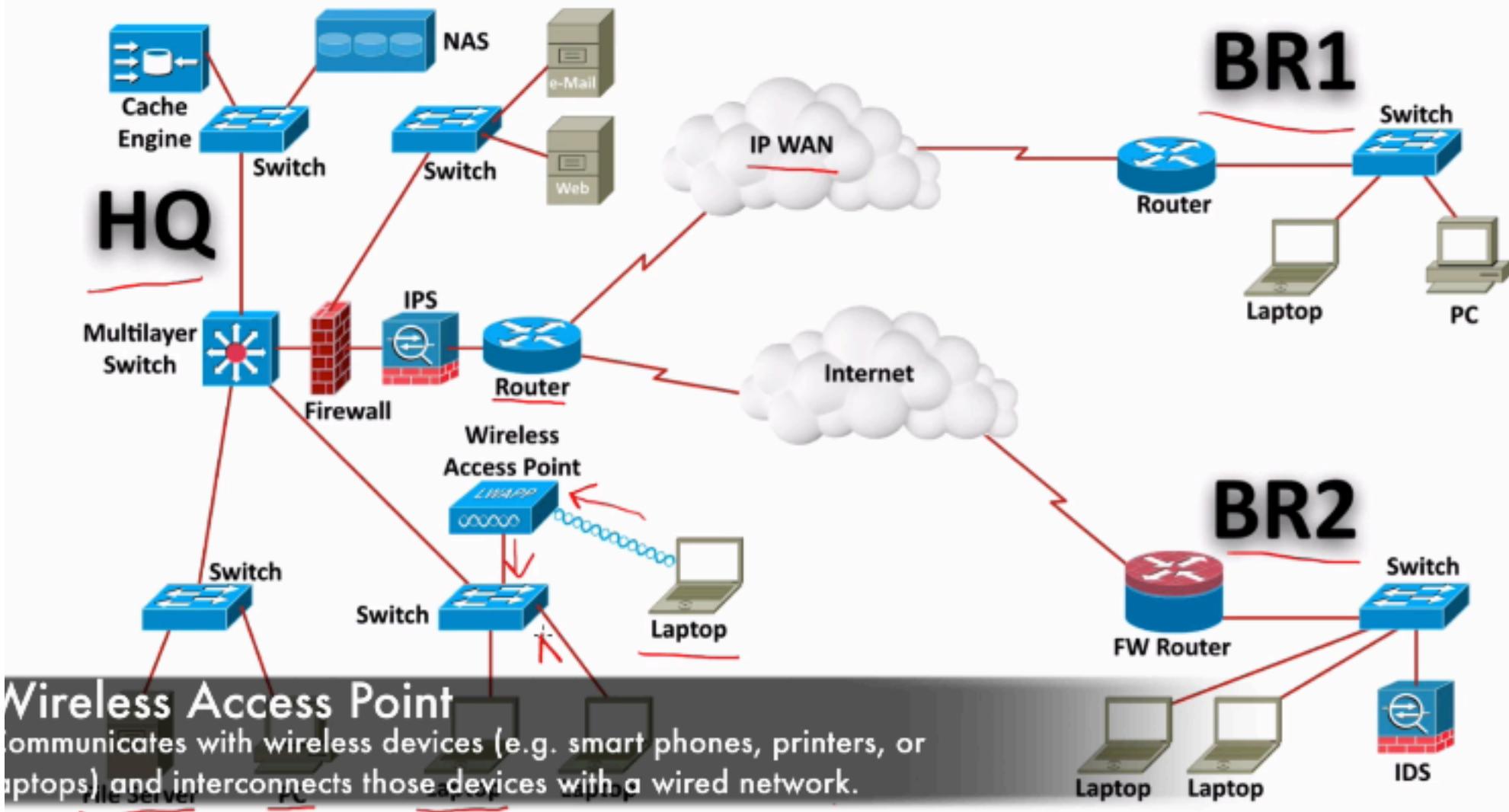
28.8 kbps: 2400 baud using twelve channels.

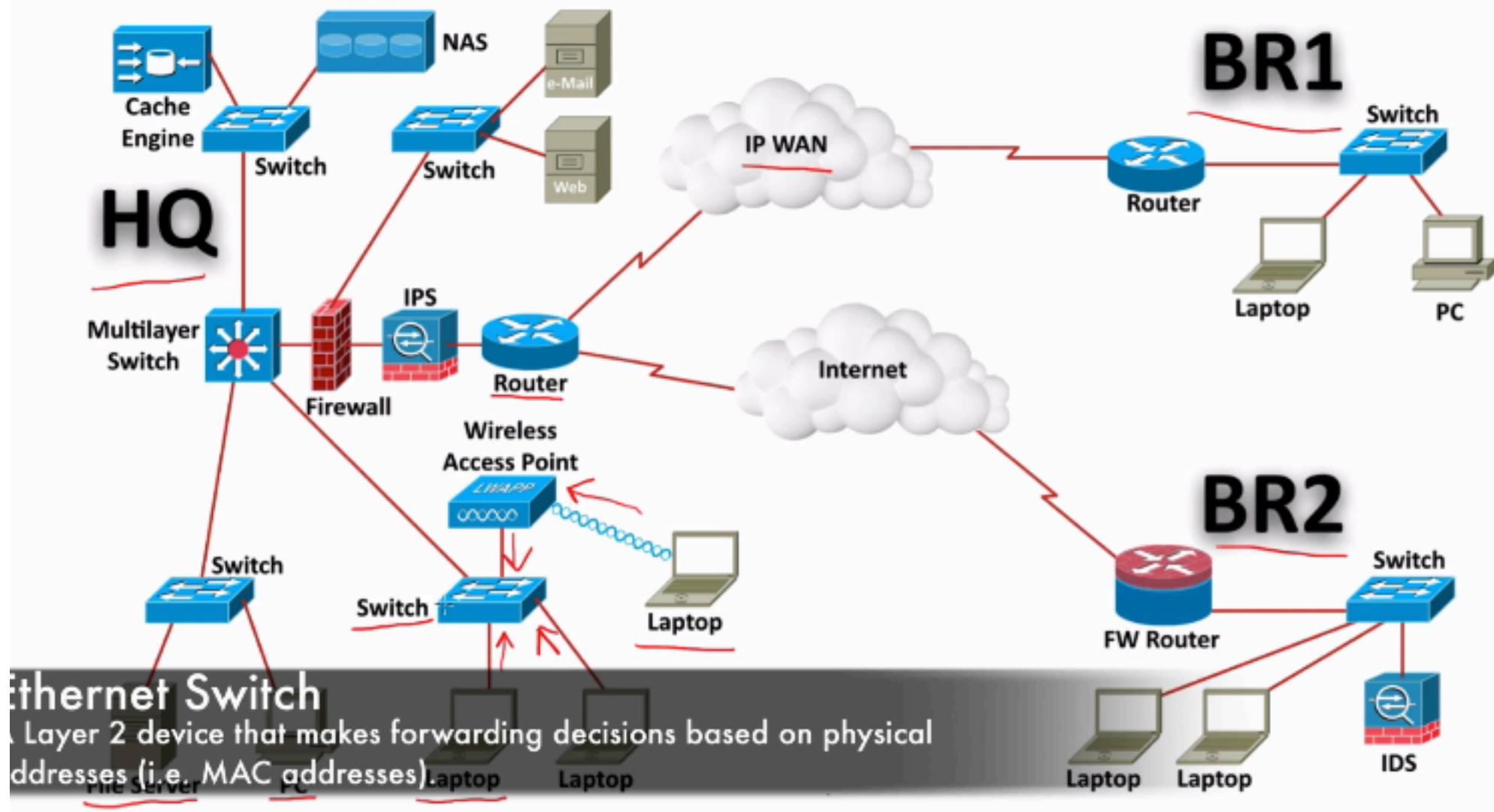
Common Infrastructure Devices

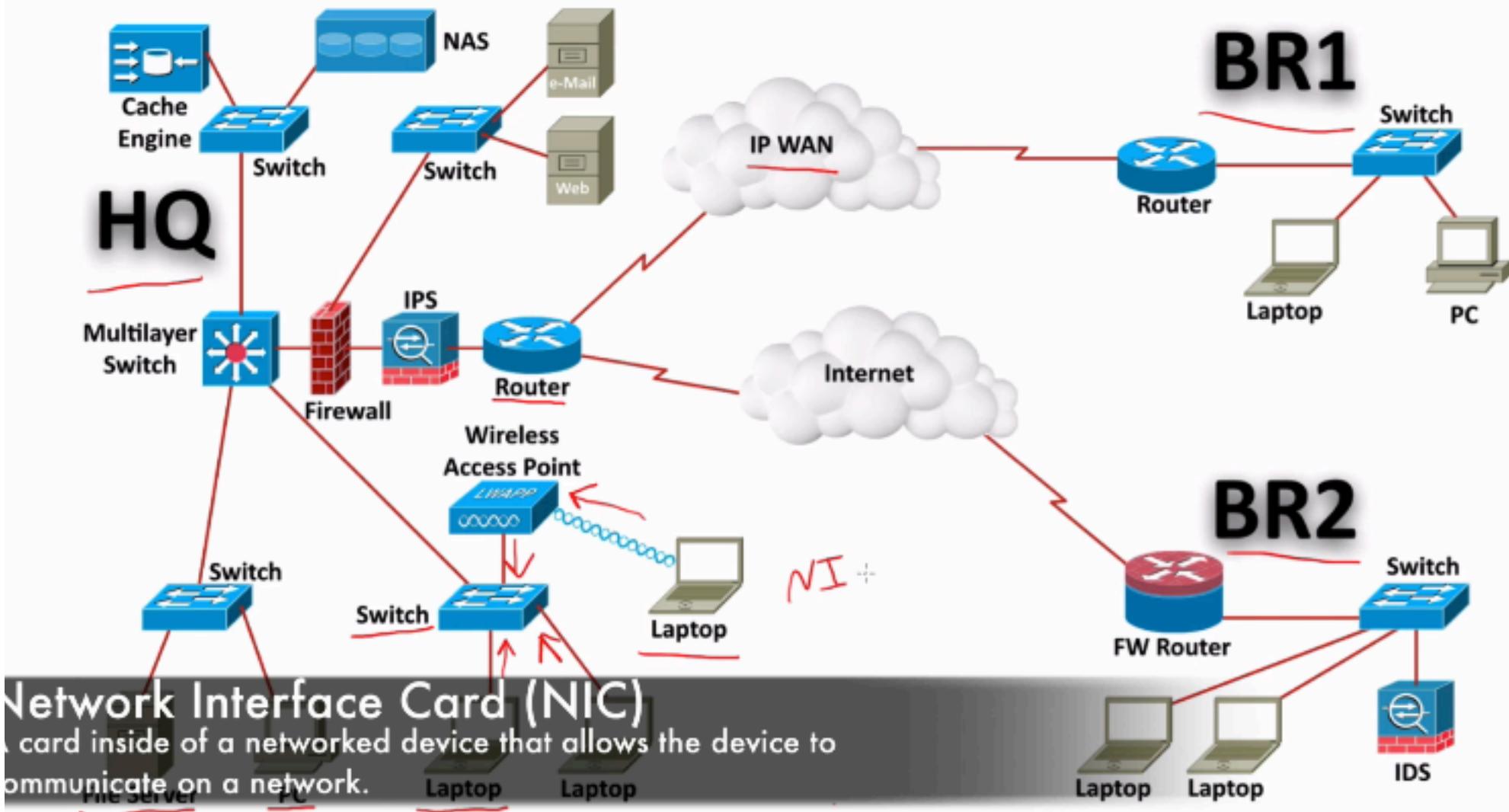


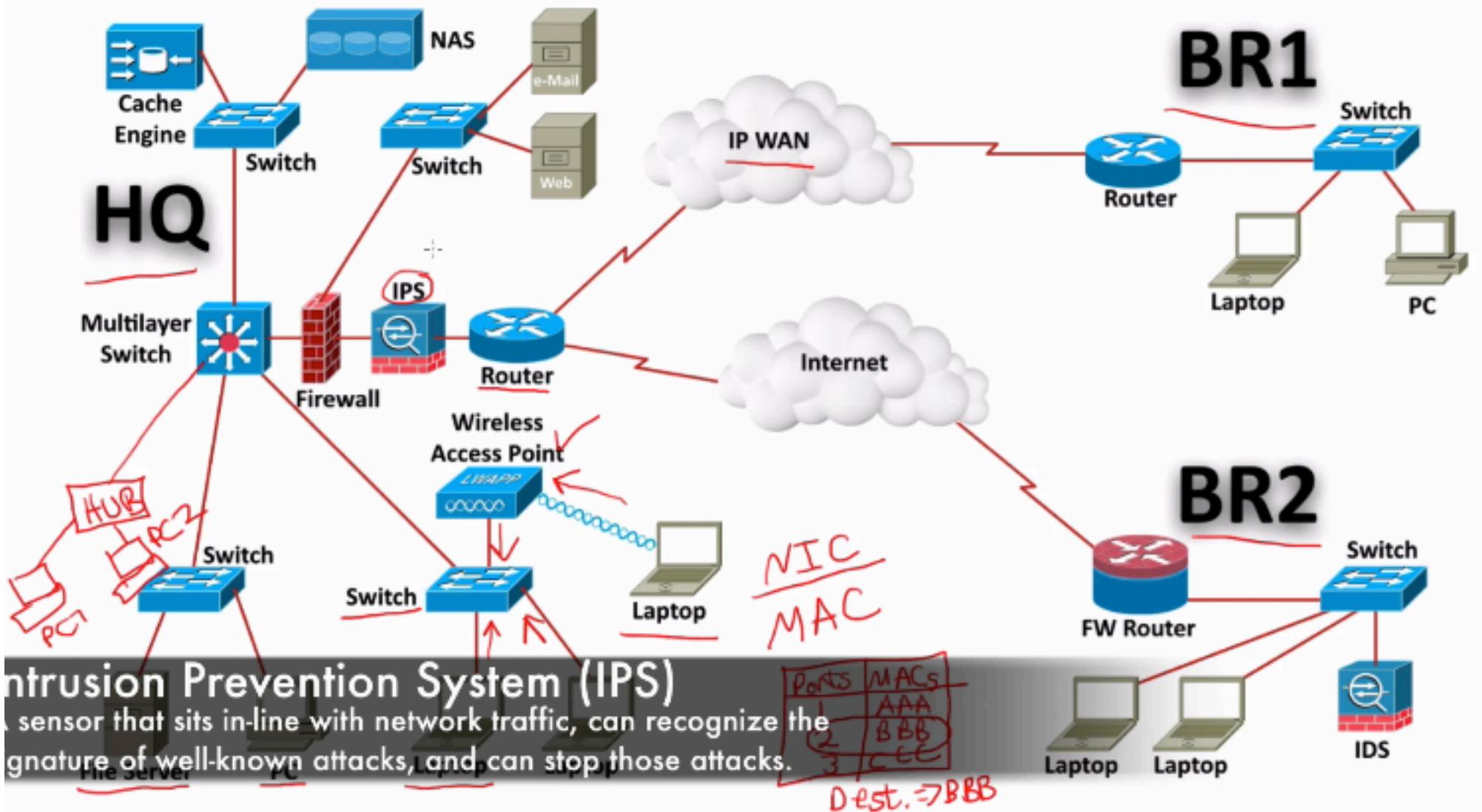


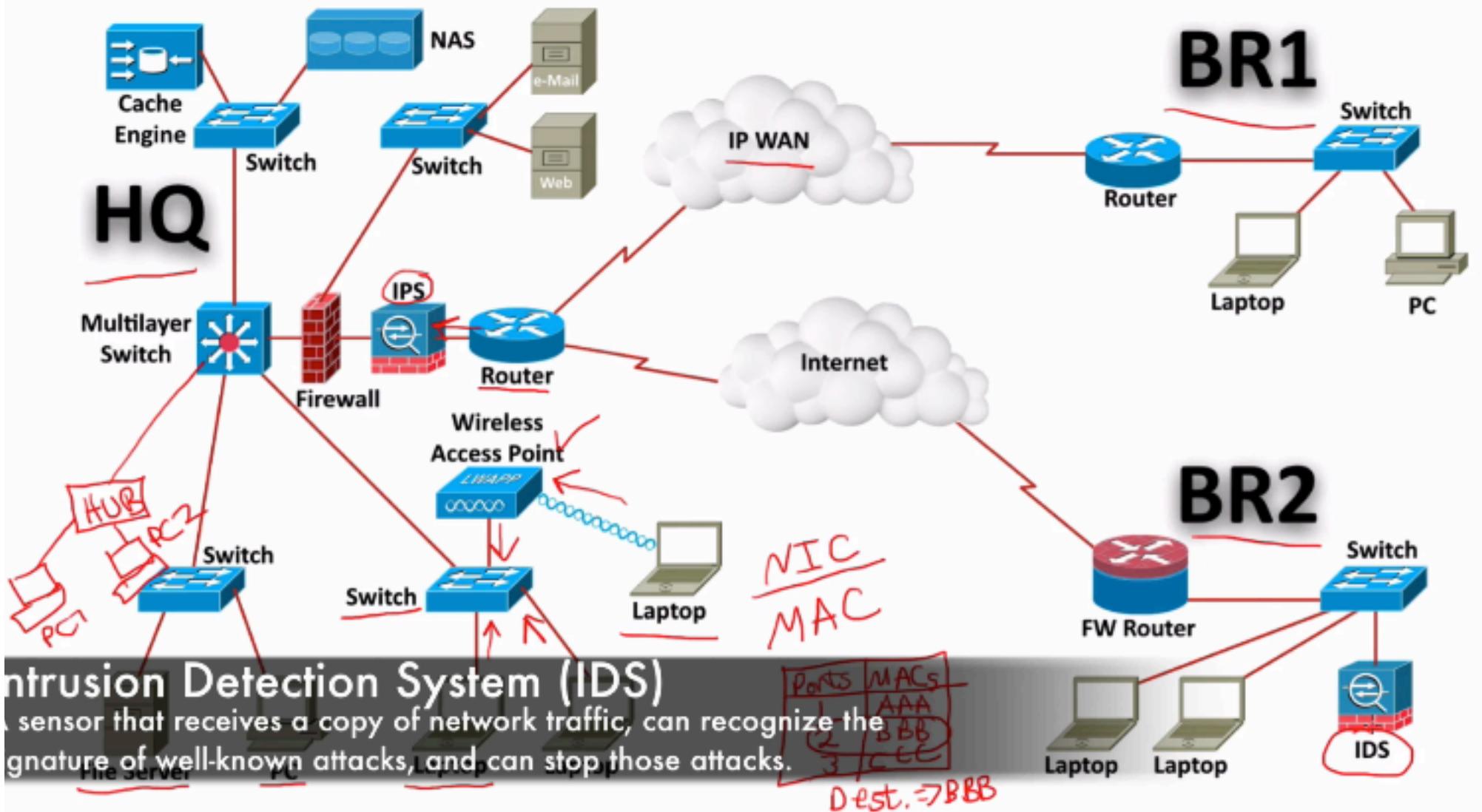


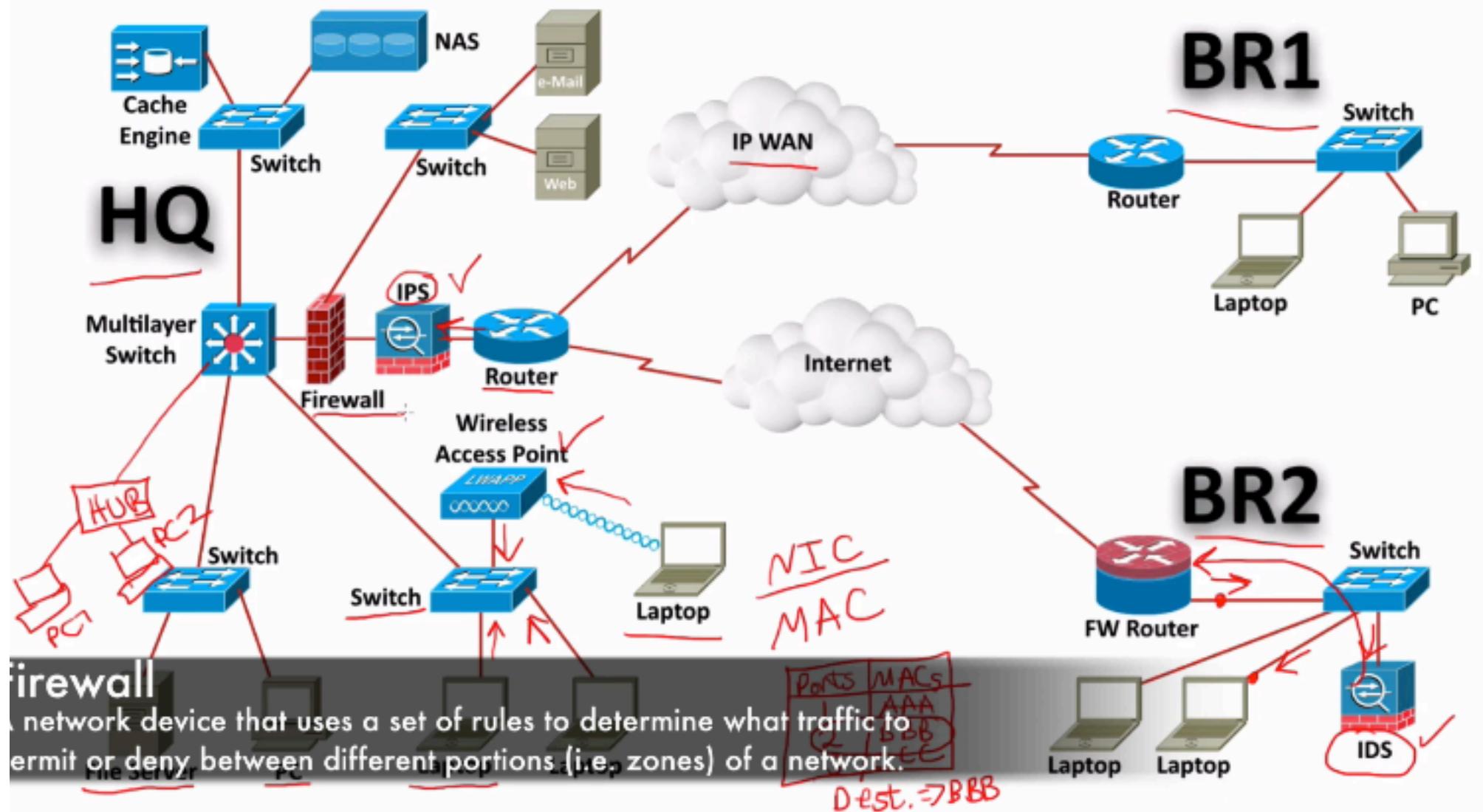


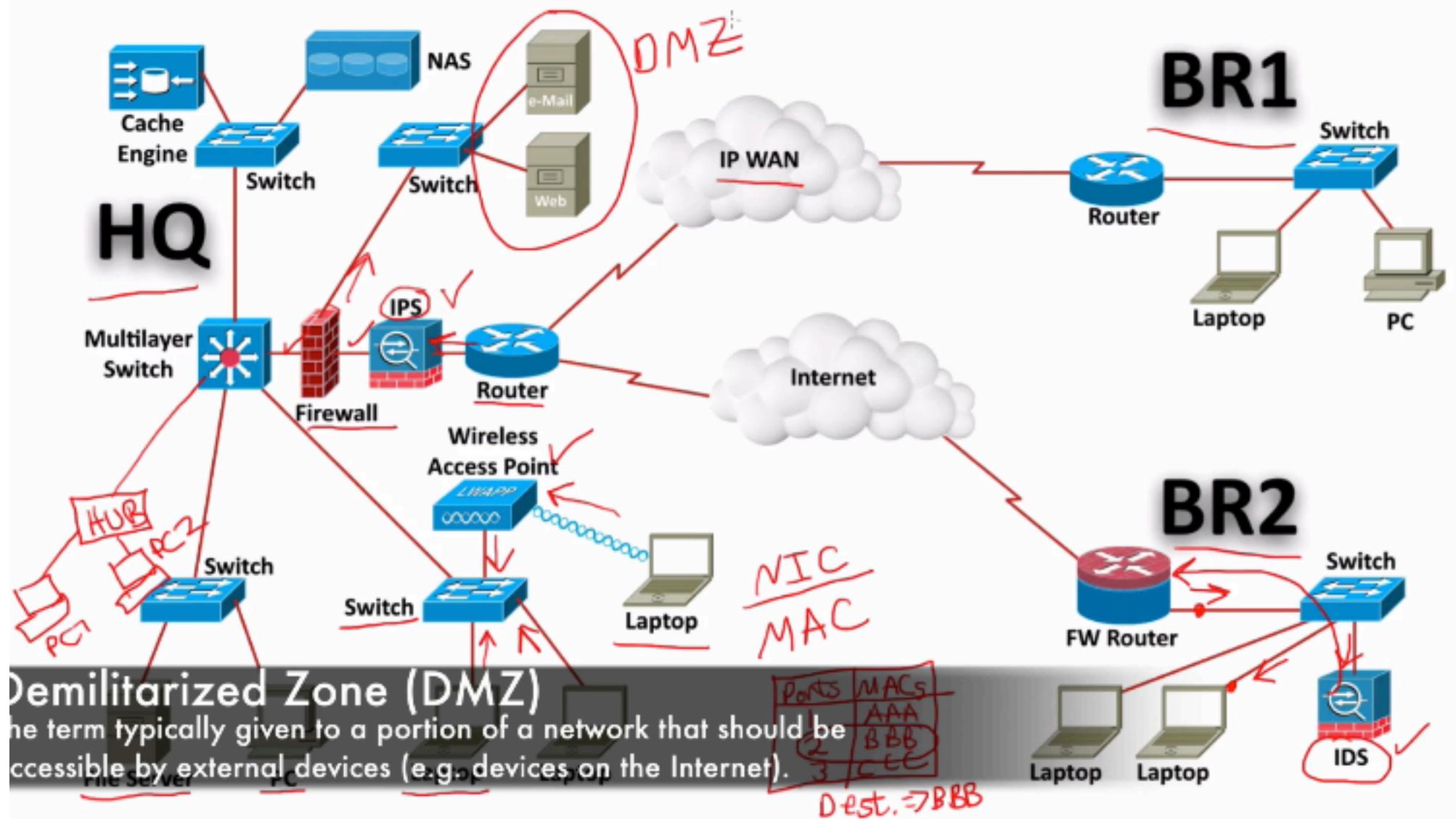


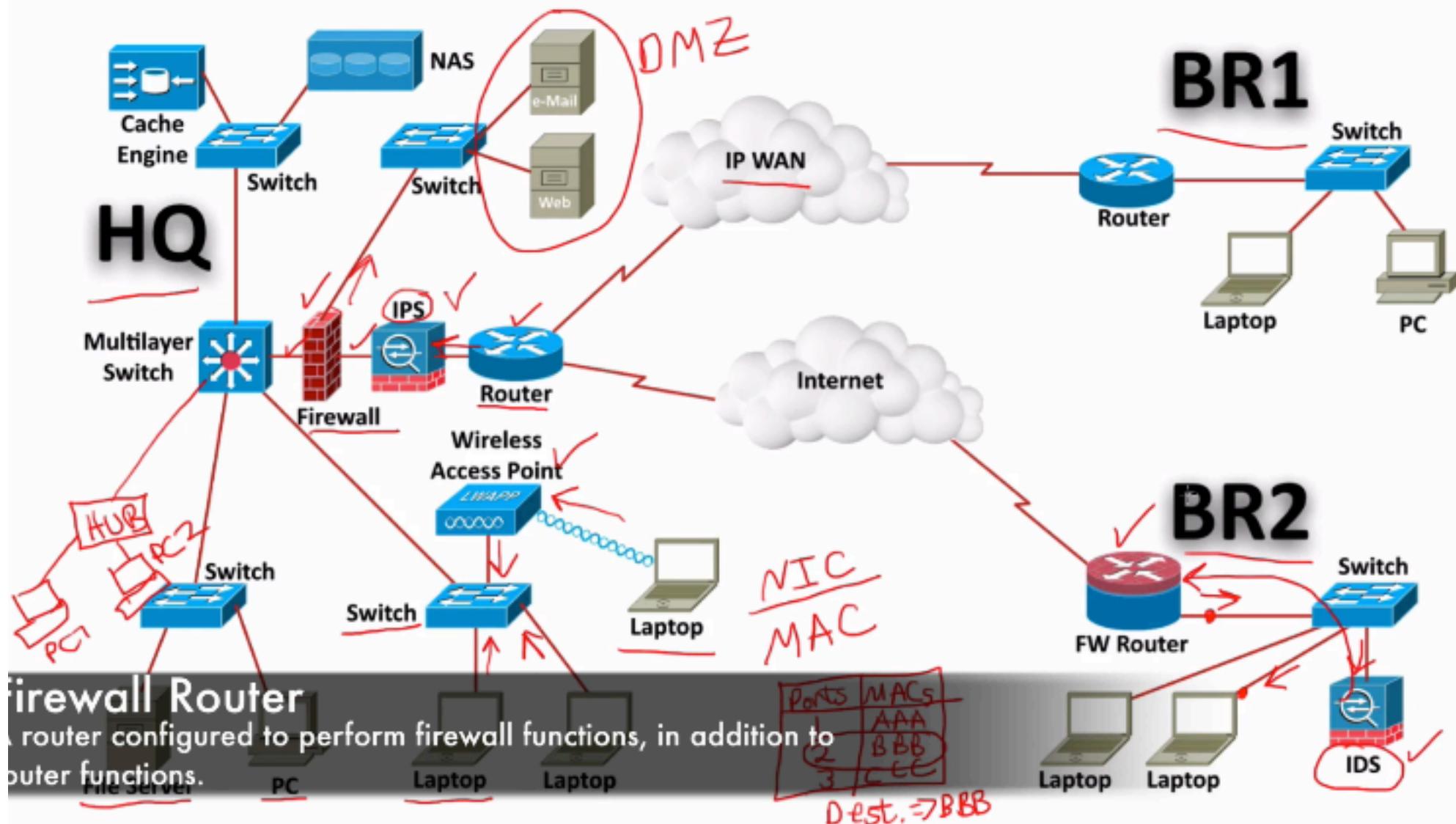


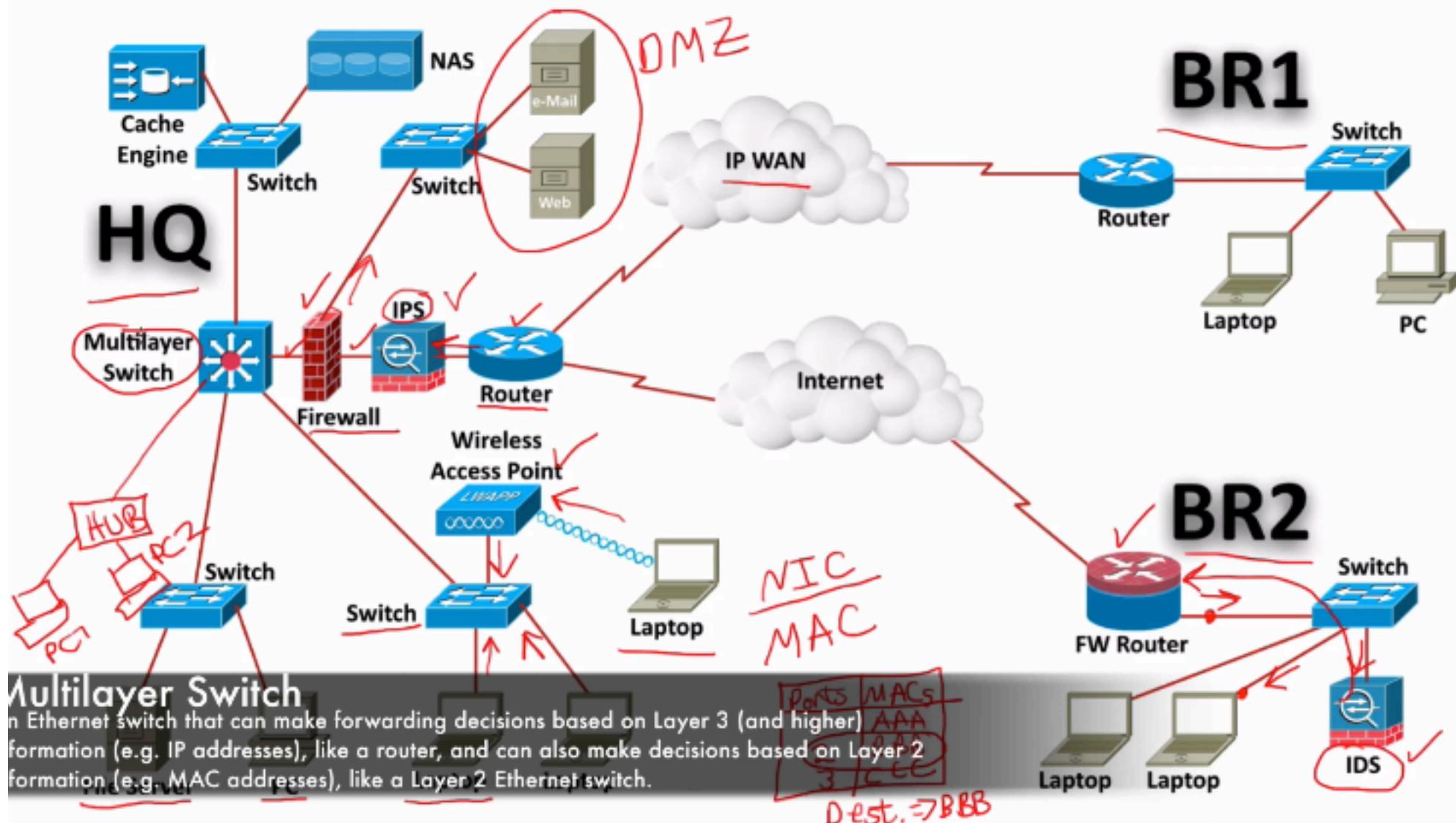


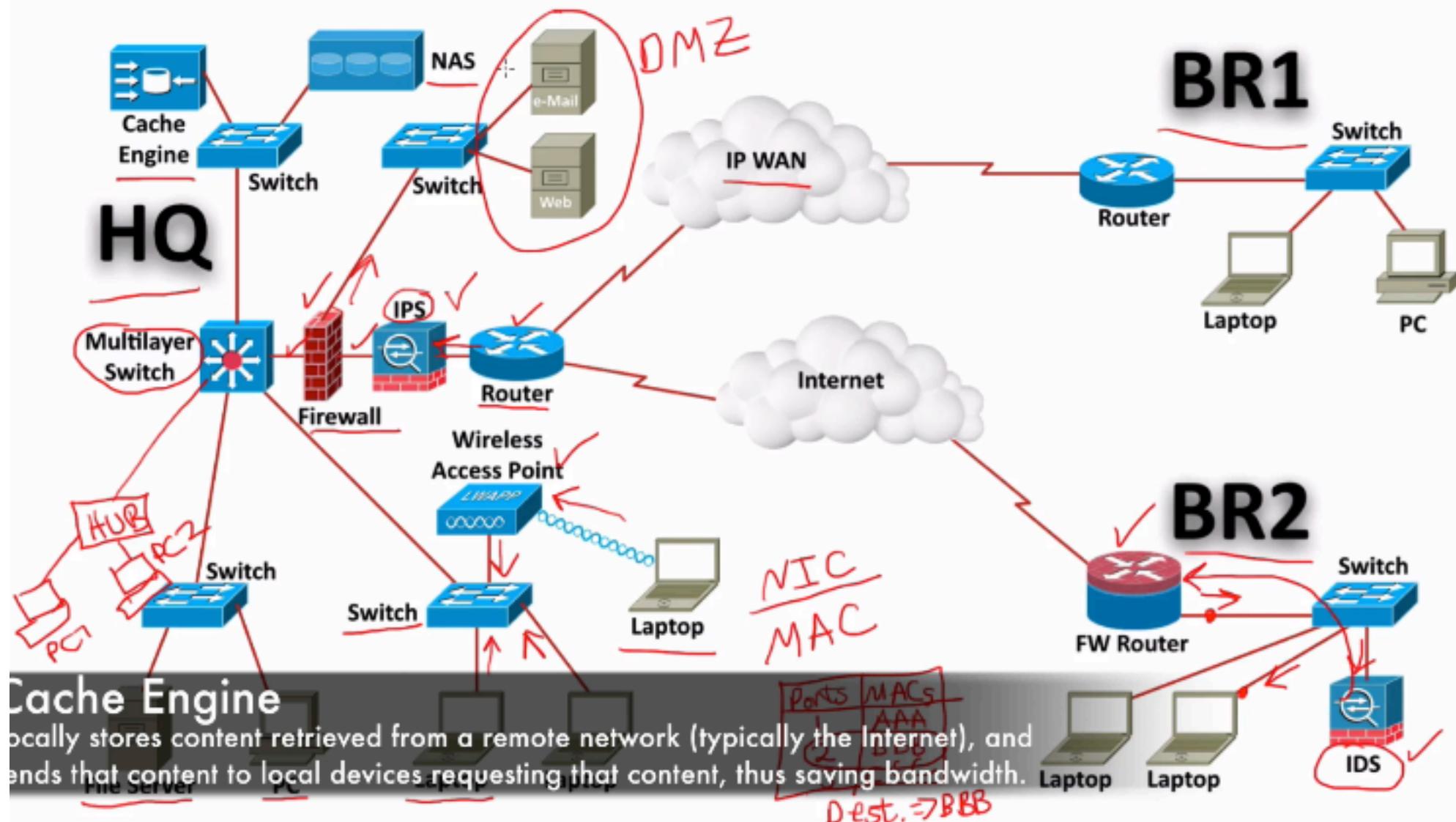


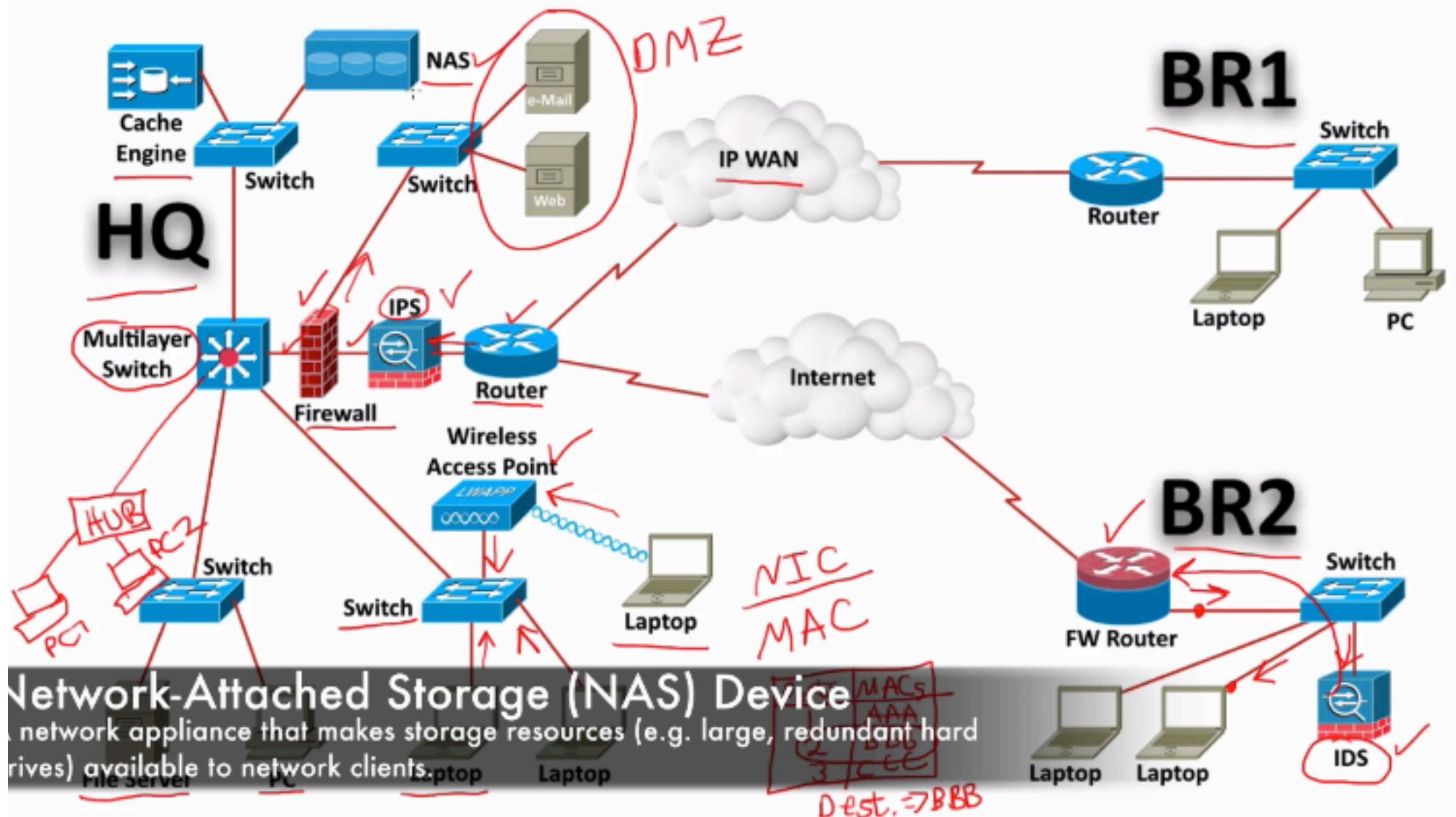




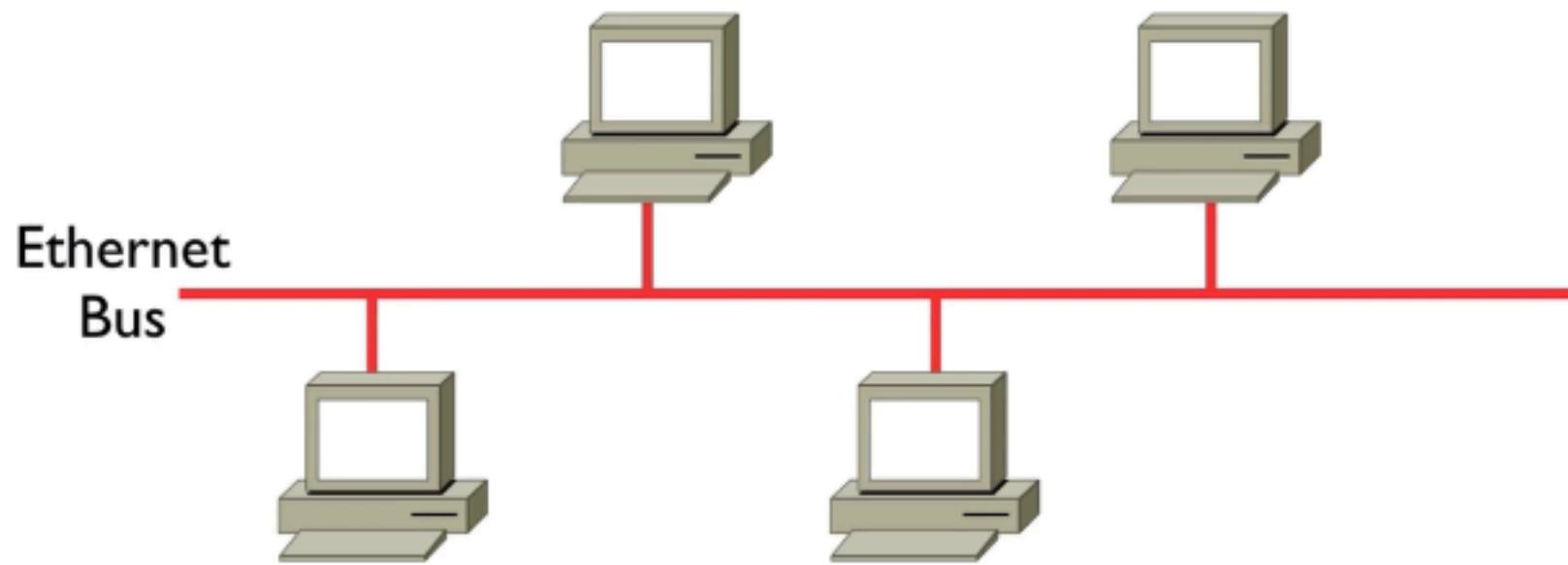




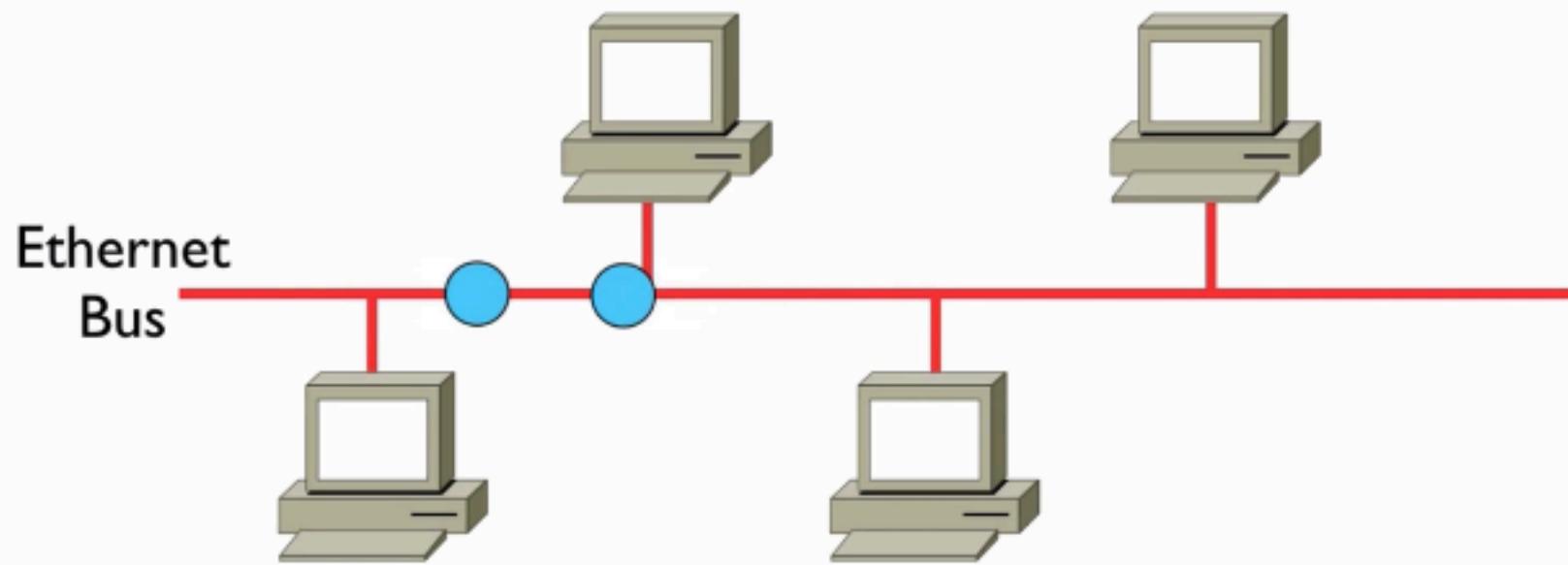


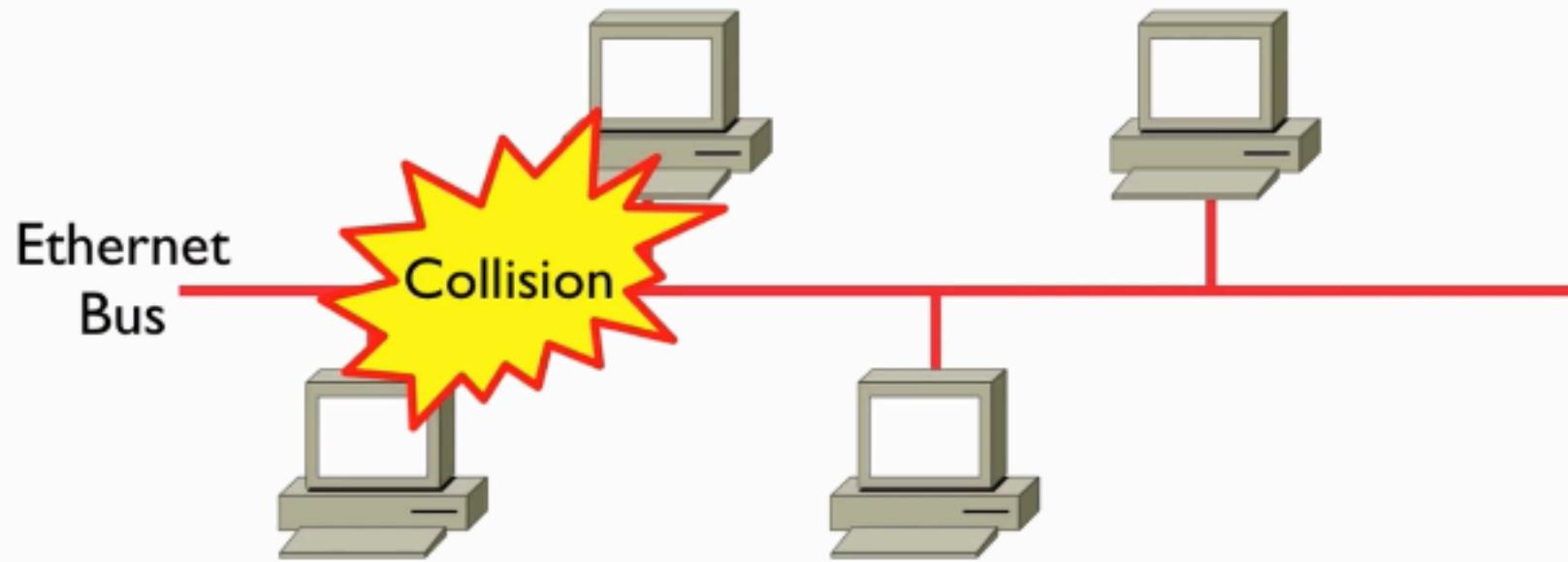


Collision Domains



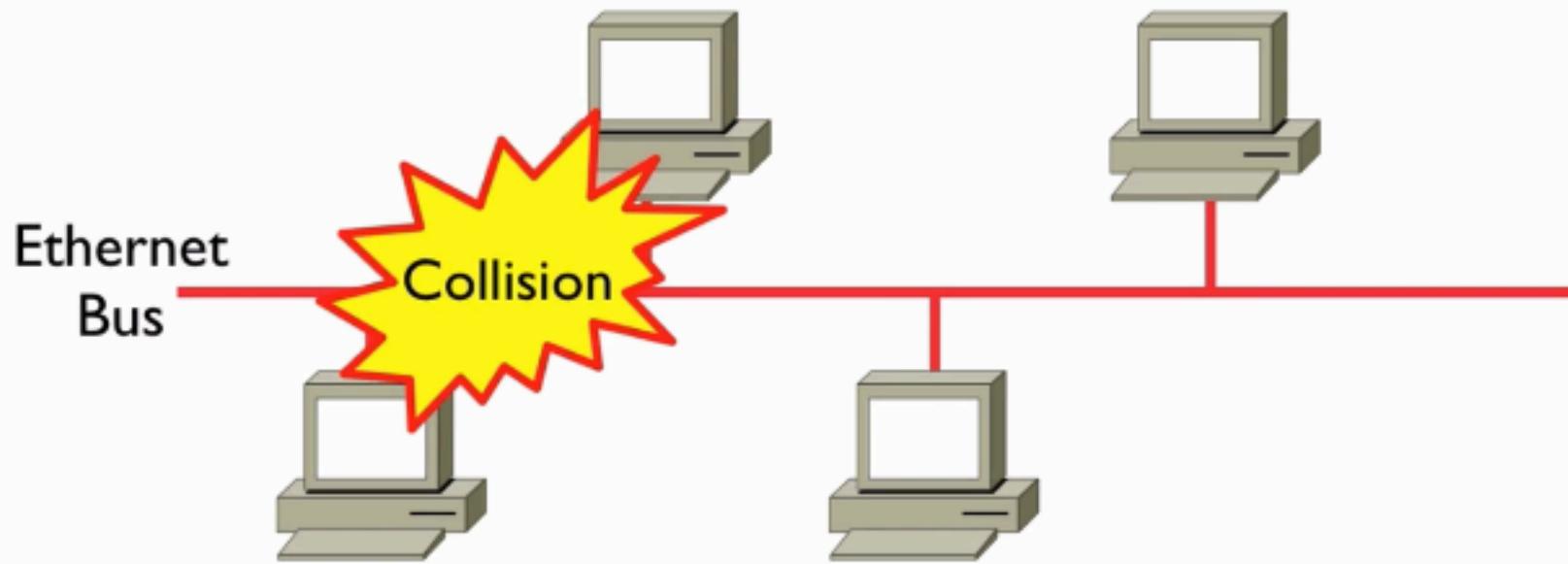
CSMA/CD
Carrier Sense Multiple Access with Collision Detection





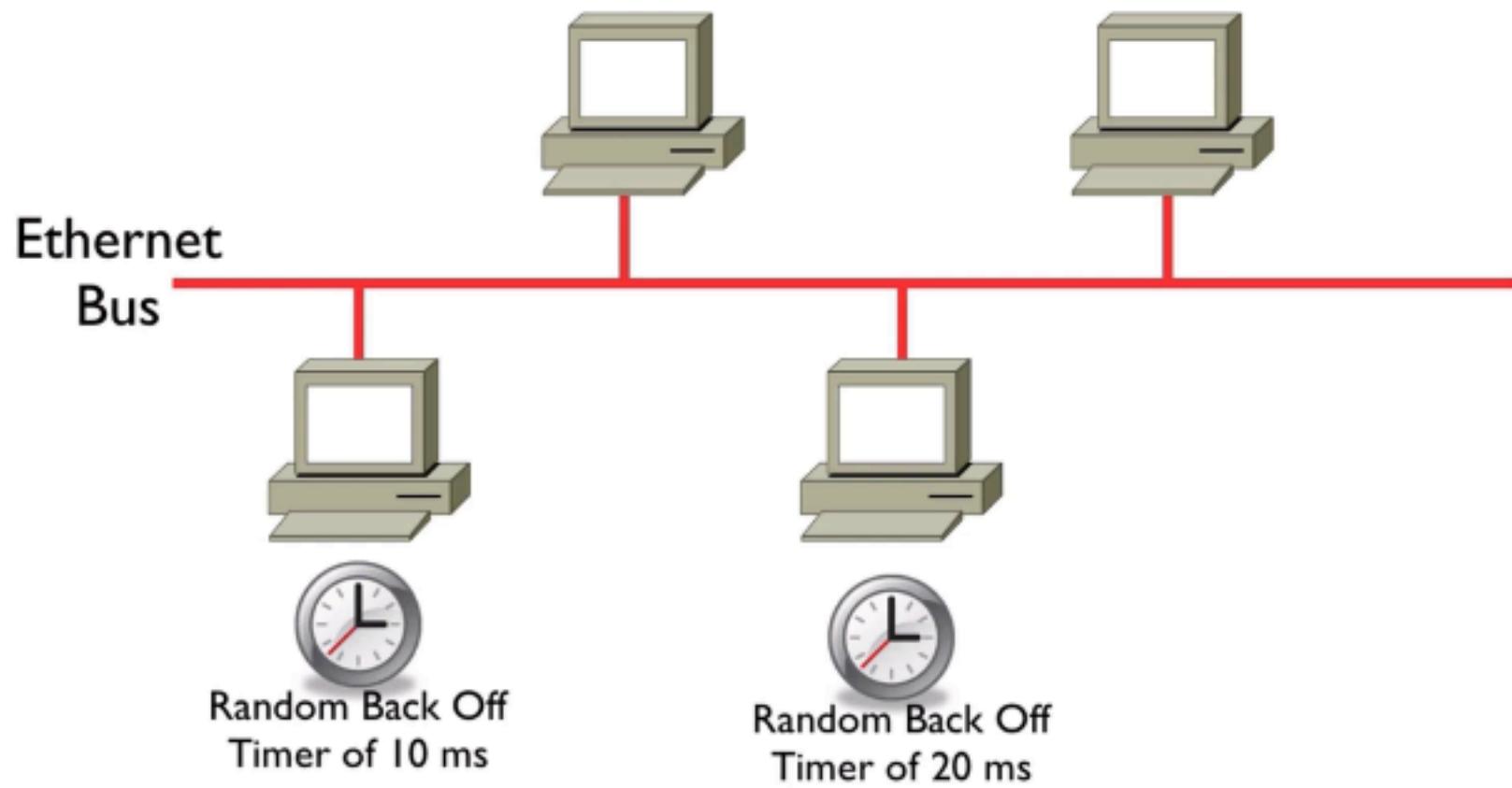
Collision

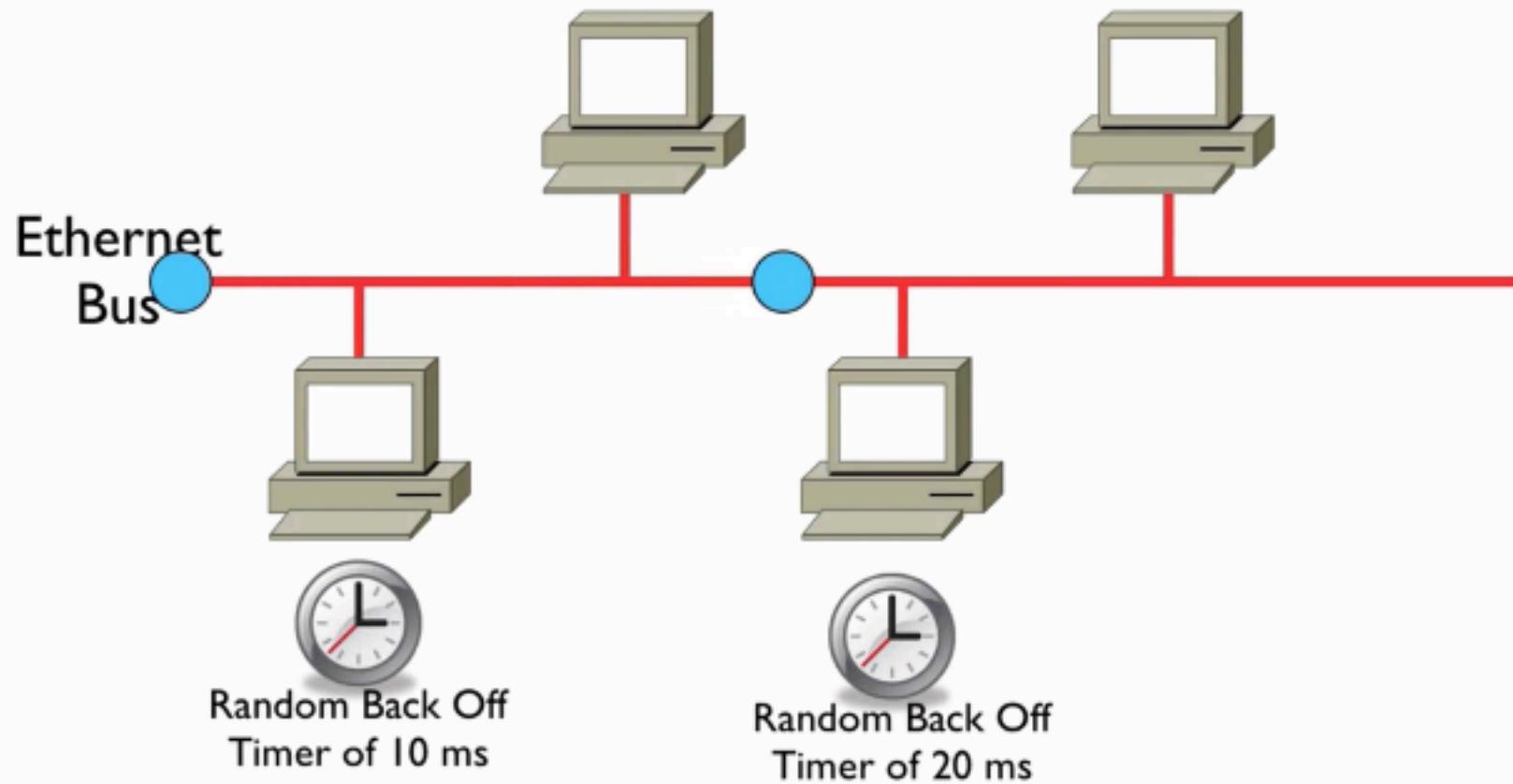
Interference occurring as a result of two stations transmitting at the same time.

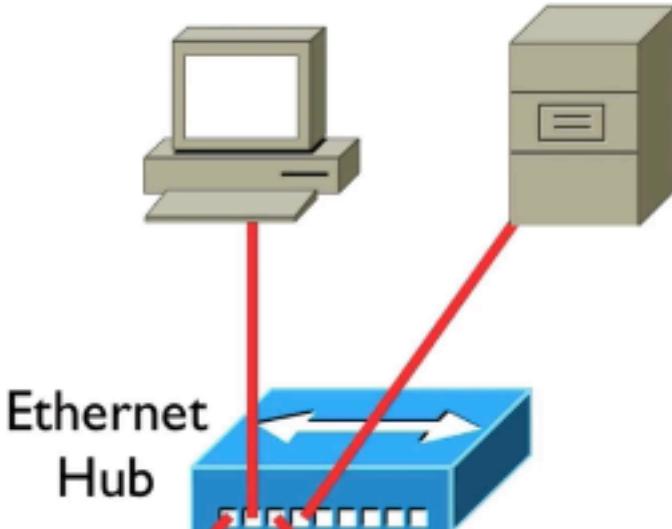


Jamming

The continued transmission of a frame that has collided, in an effort to allow all devices on the shared segment to detect the collision.



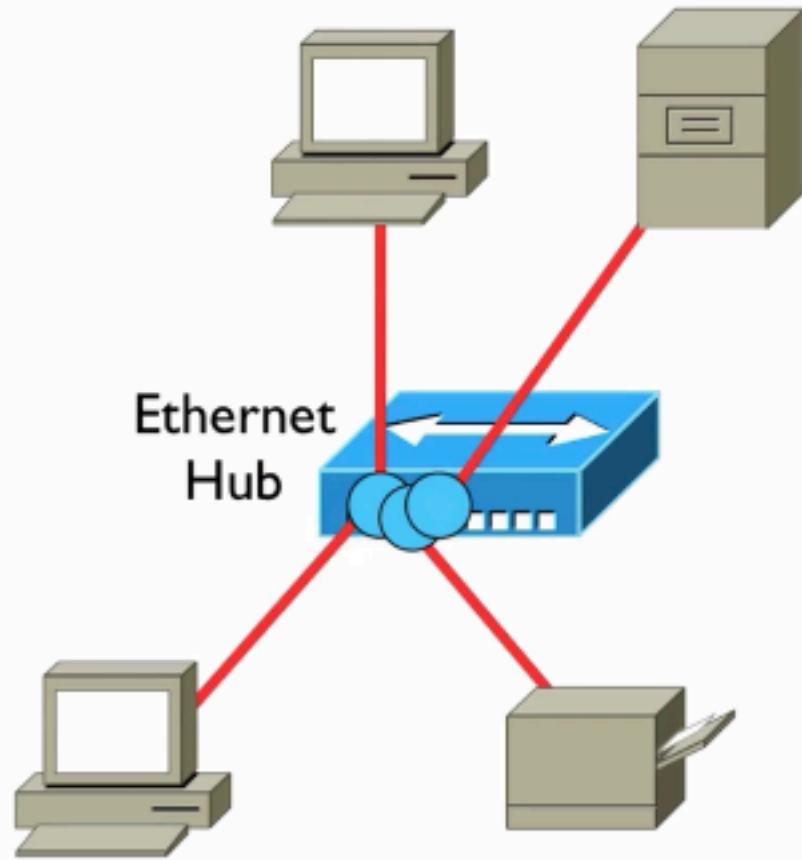




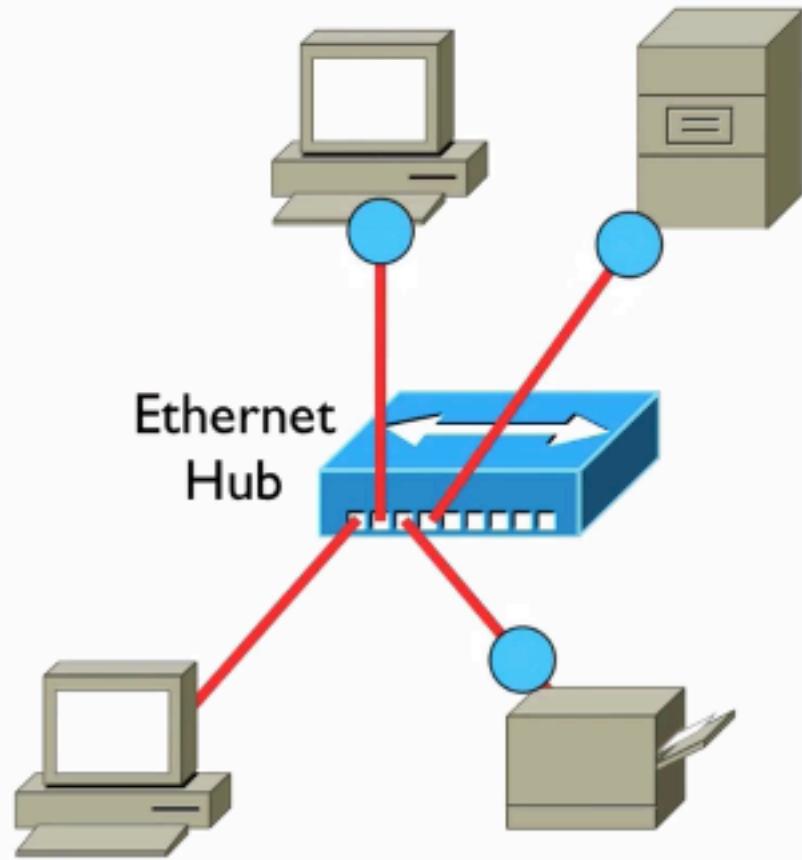
One Collision Domain

Ethernet Hub

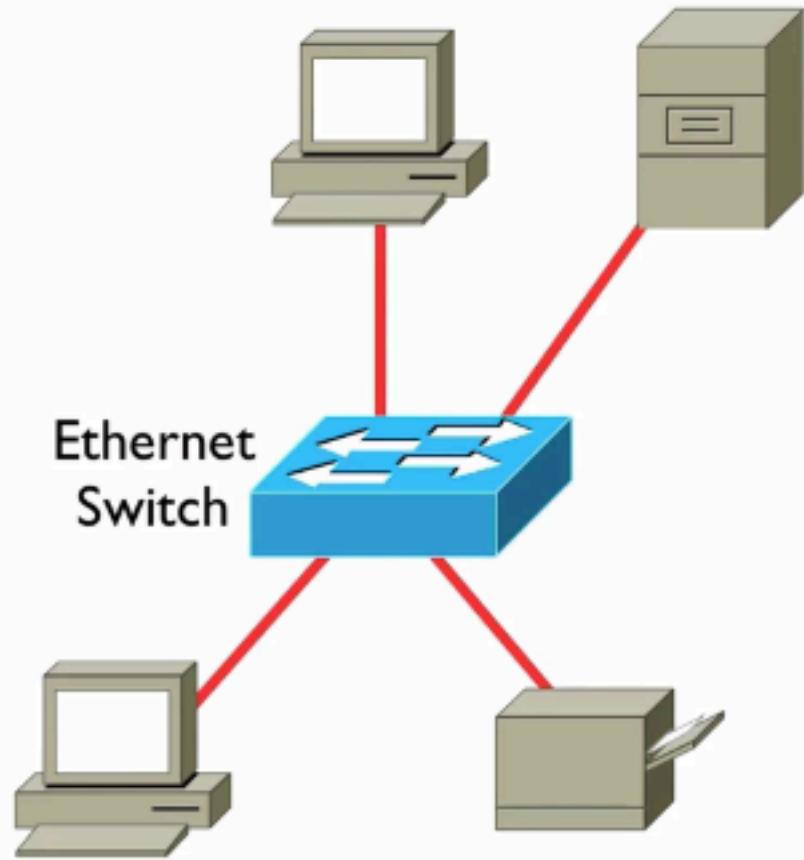
All ports on an Ethernet hub belong to the same collision domain.



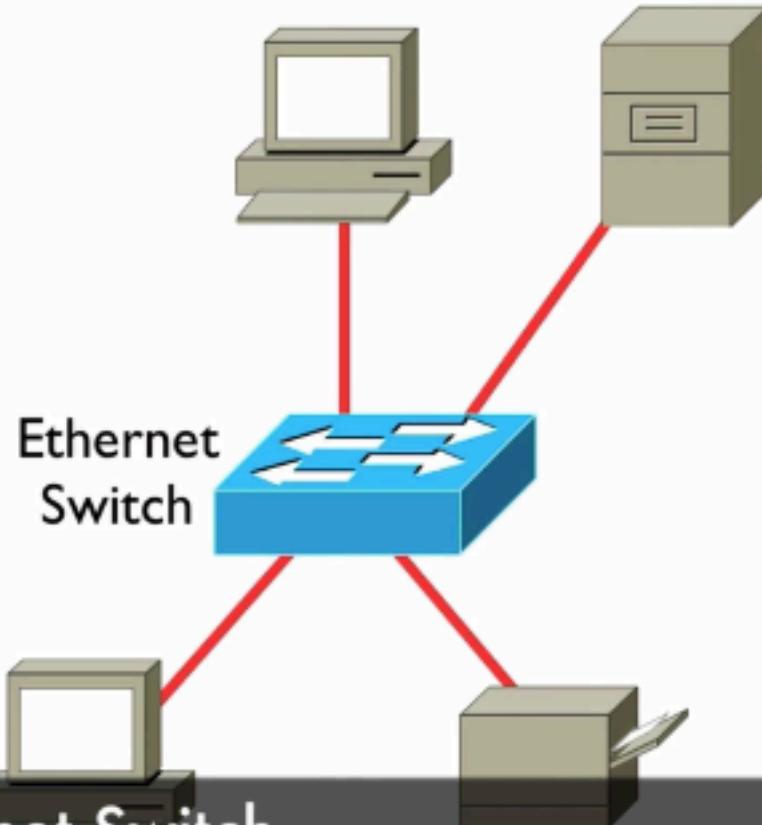
One Collision Domain



One Collision Domain



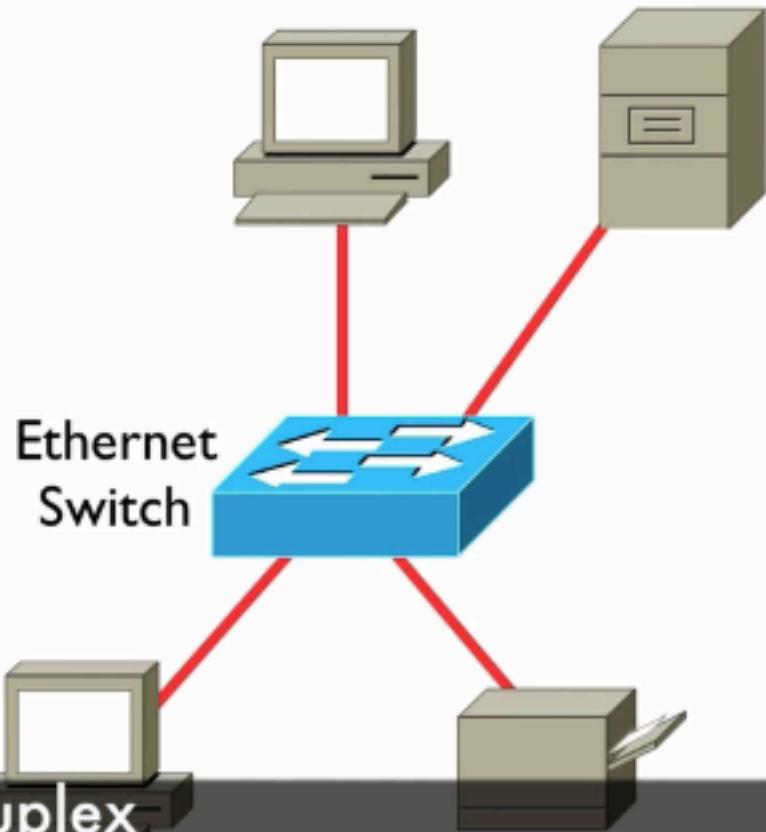
Four Collision Domains



Four Collision Domains

Ethernet Switch

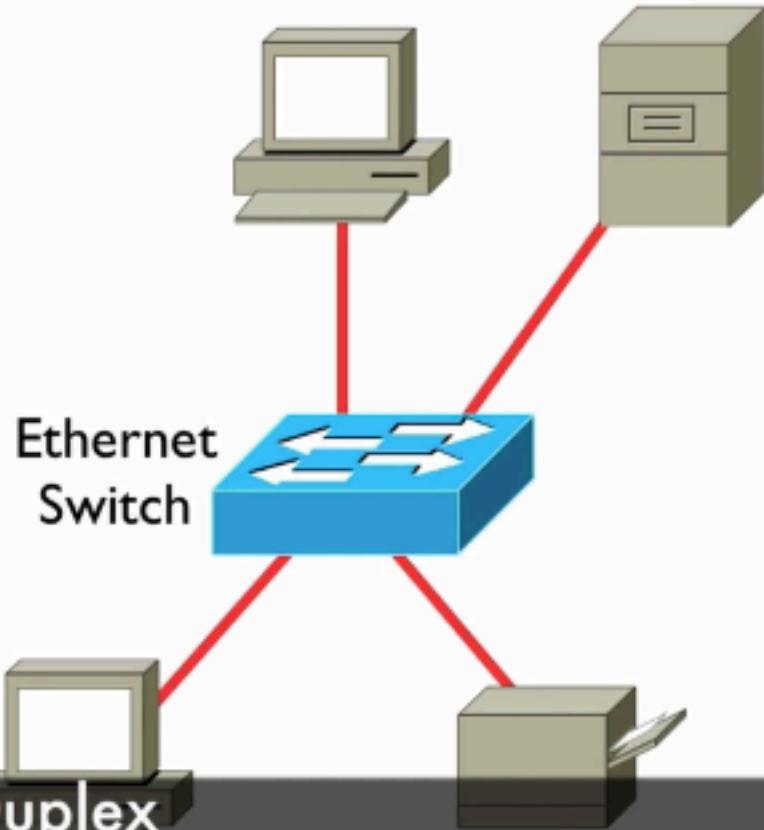
Each port on an Ethernet switch is in its own collision domain.



Four Collision Domains

Full-Duplex

Ethernet switch ports can be configured to simultaneously transmit and receive. This "full-duplex" mode disables CSMA/CD on a port.

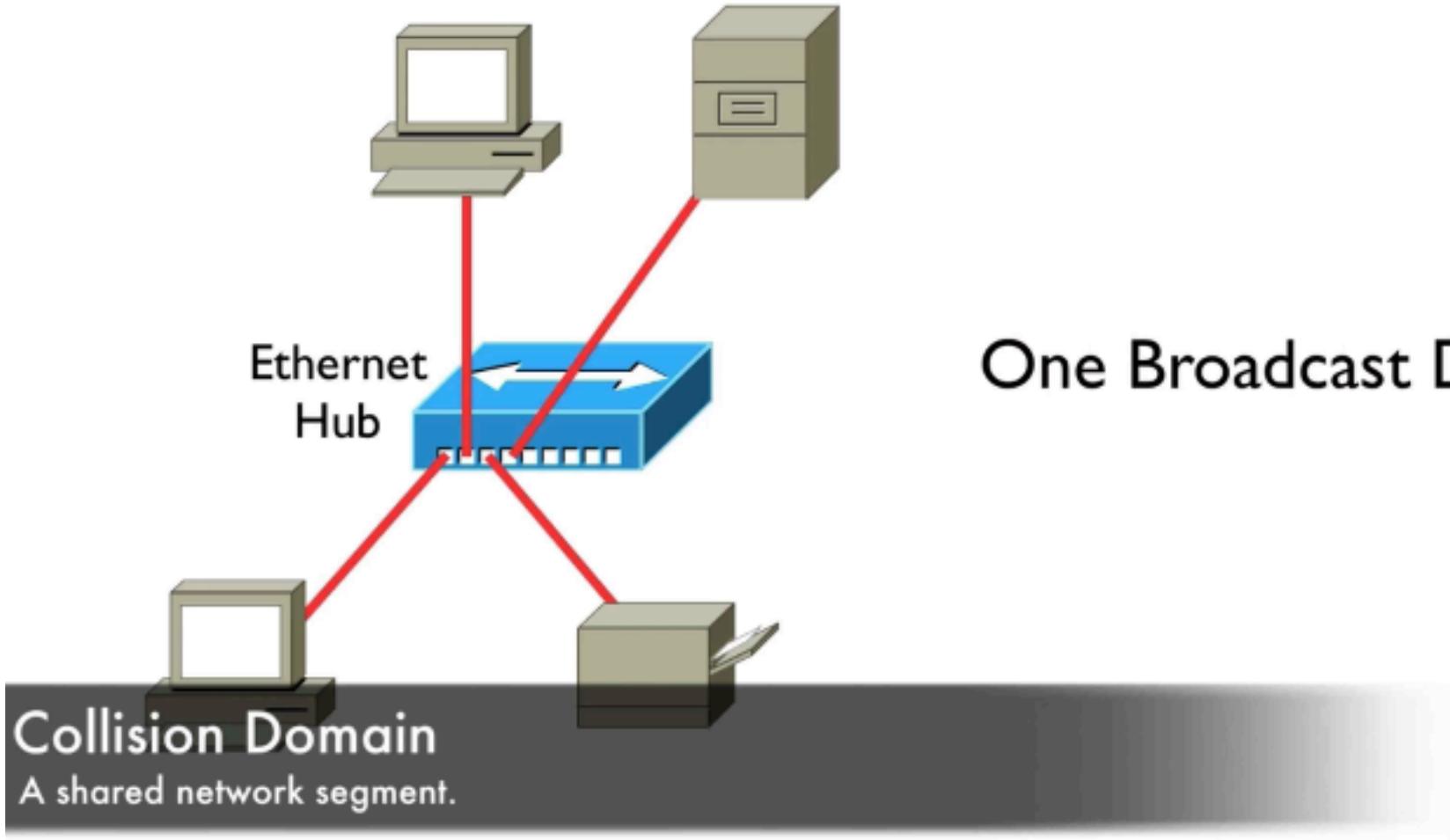


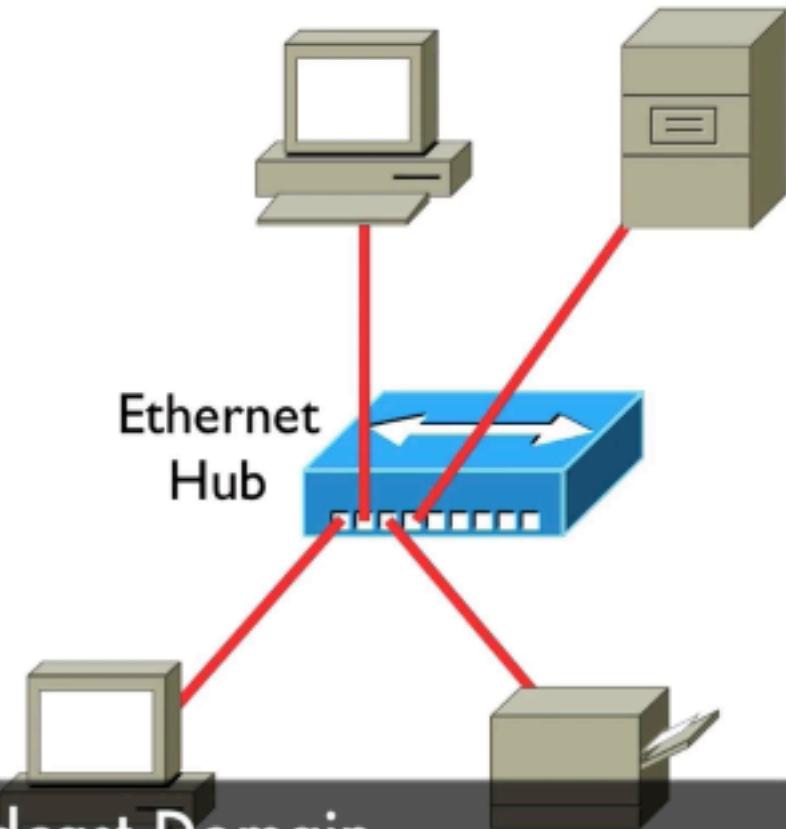
Four Collision Domains

Half-Duplex

Ethernet hub ports can only receive or transmit at any one time. This "half-duplex" mode uses CSMA/CD.

Broadcast Domains

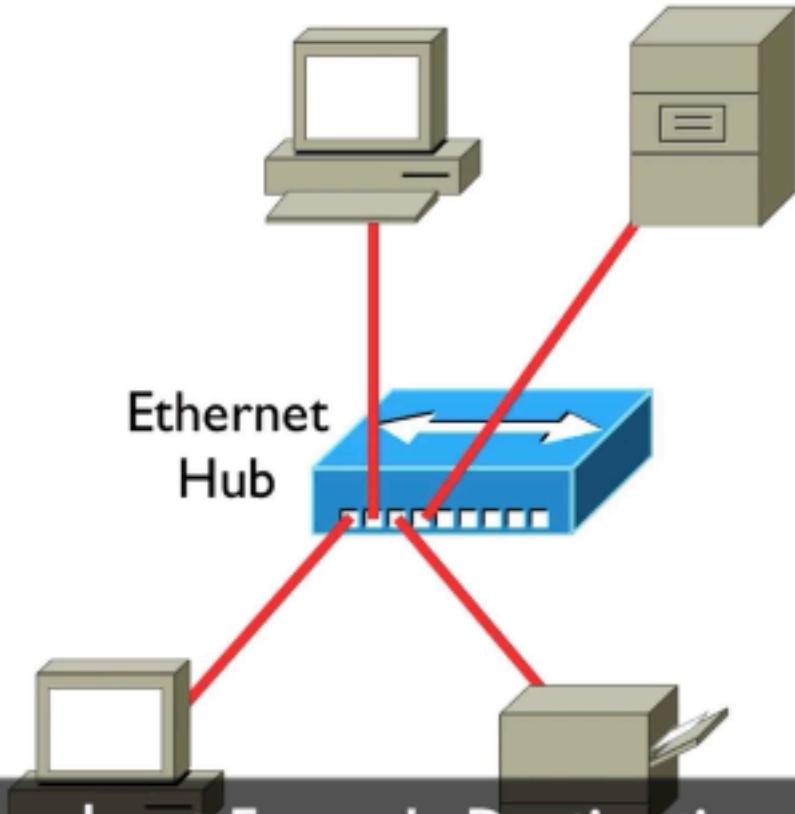




One Broadcast Domain

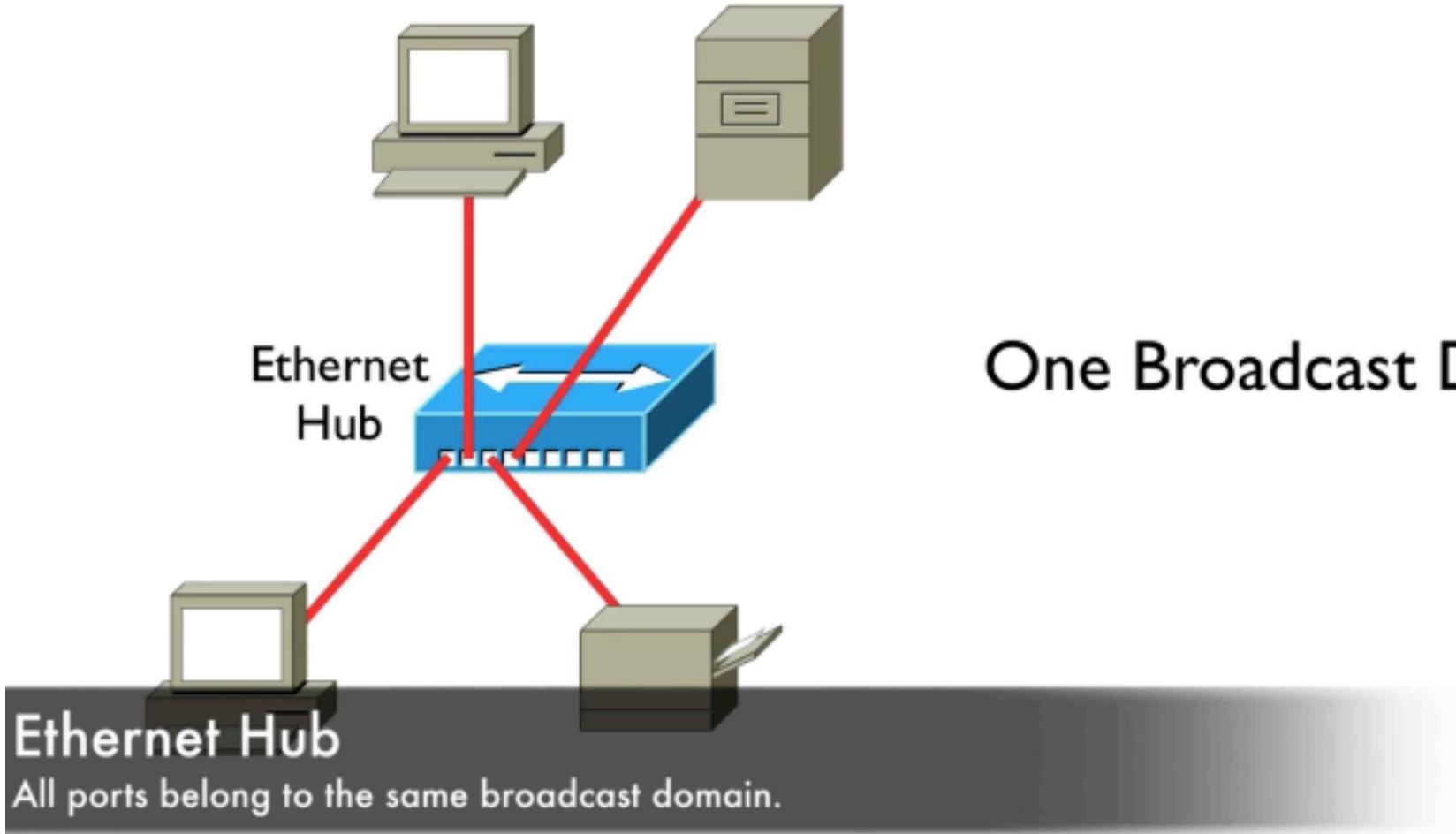
Broadcast Domain

Defines how far a broadcast travels in a network.



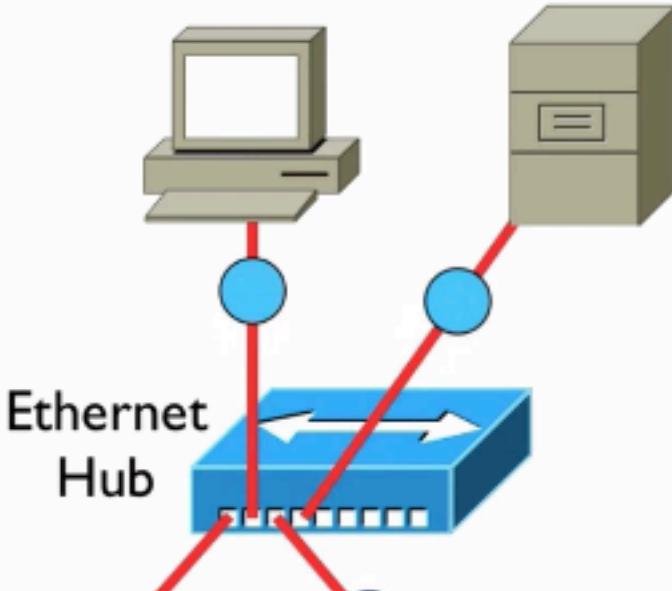
One Broadcast Domain

A Broadcast Frame's Destination MAC Address
FFFF.FFFF.FFFF



One Broadcast Domain

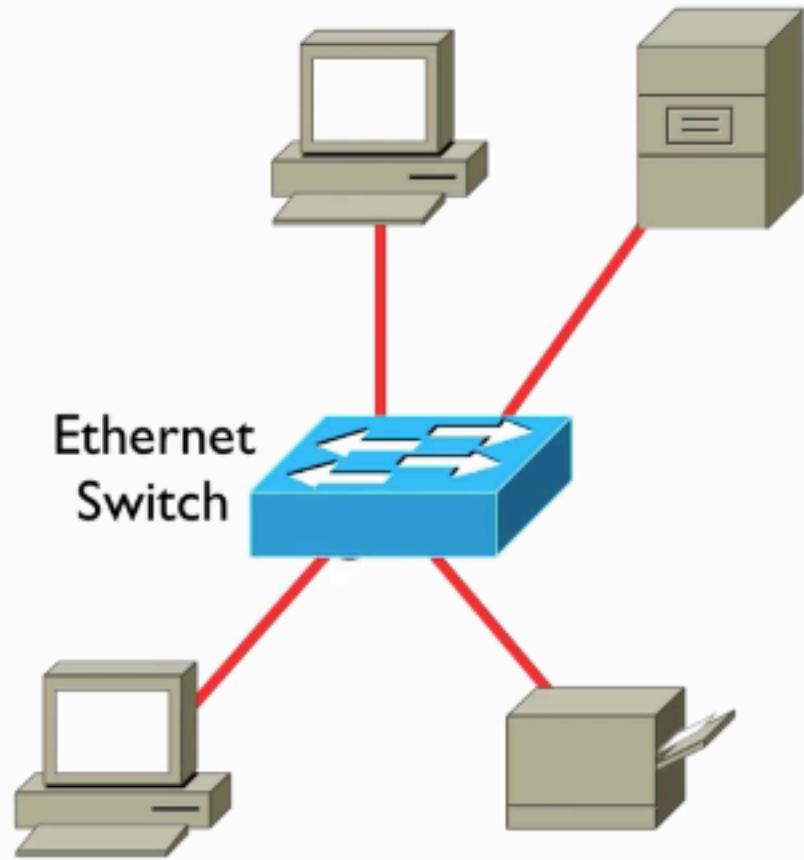
Ethernet Hub
All ports belong to the same broadcast domain.



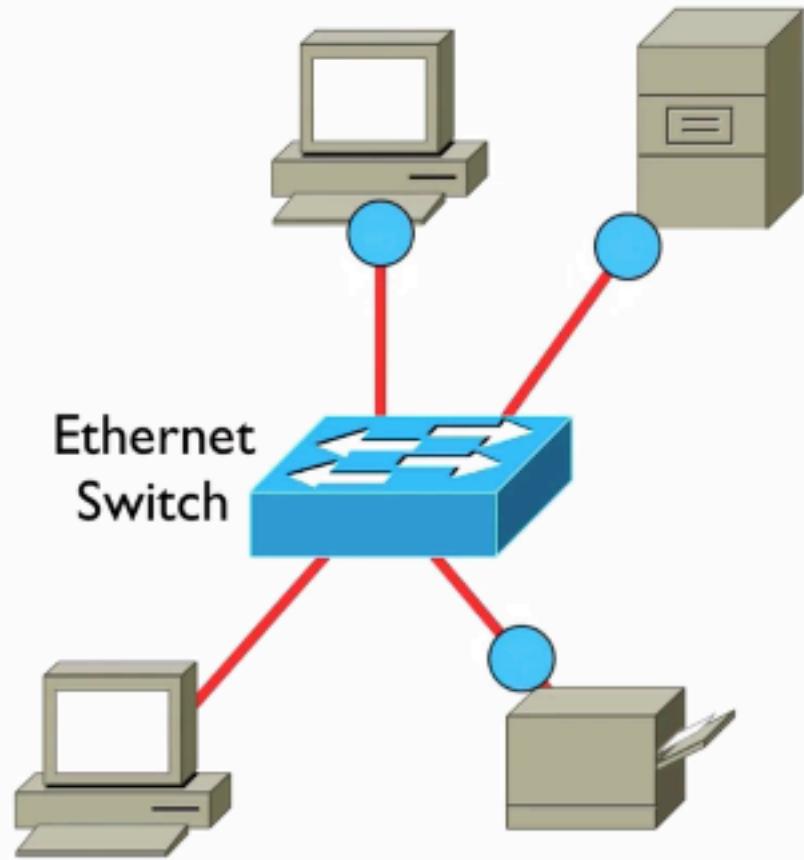
One Broadcast Domain

Ethernet Hub

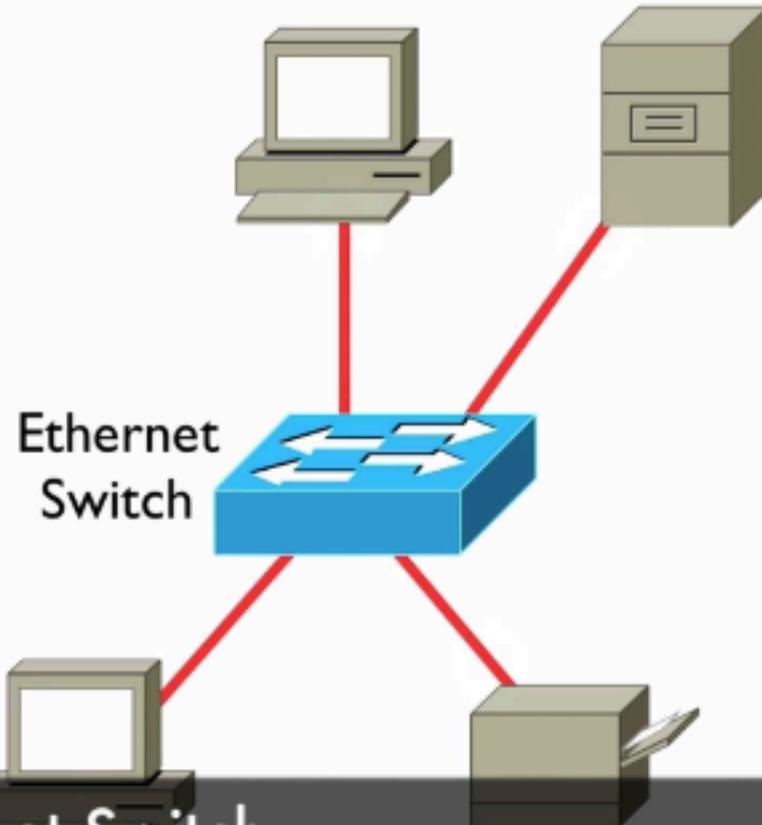
All ports belong to the same broadcast domain.



One Broadcast Domain

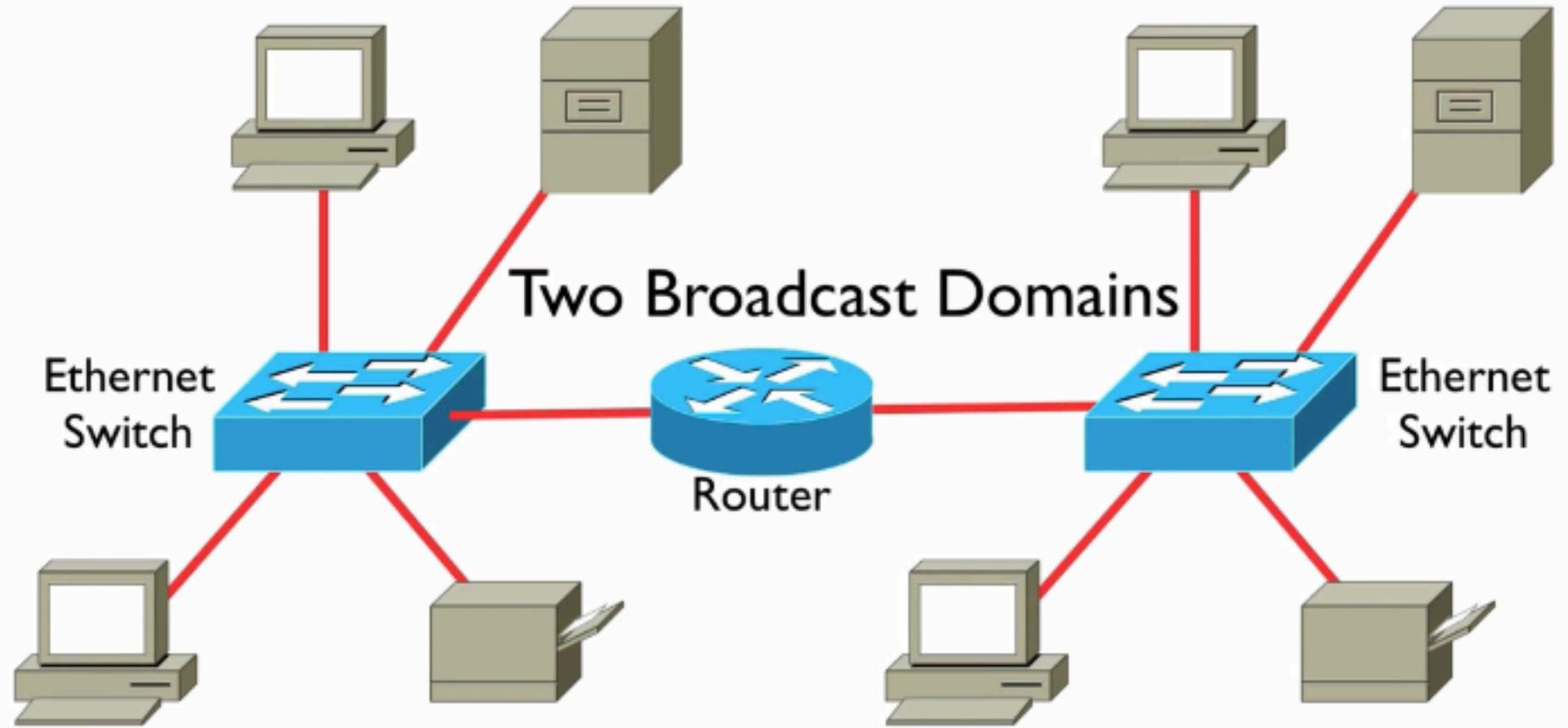


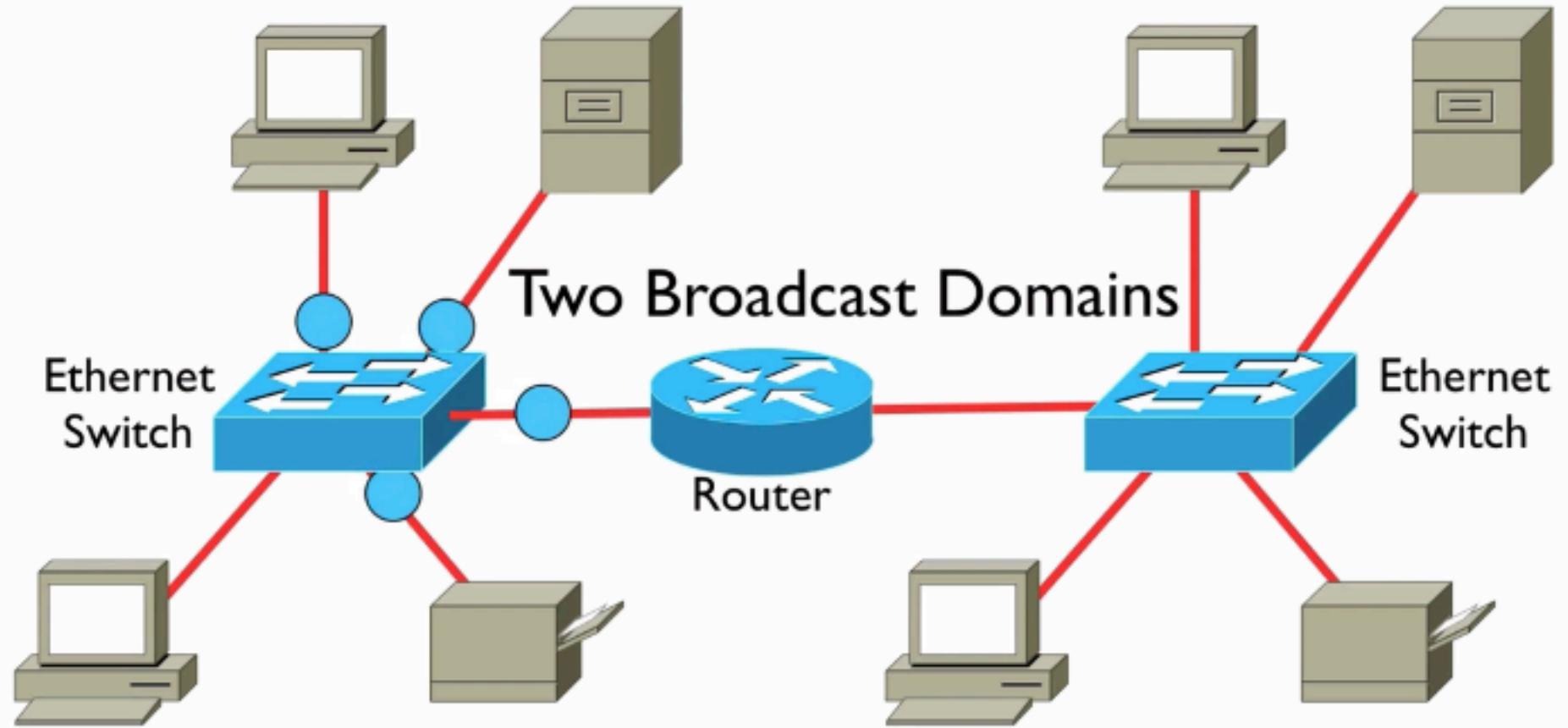
One Broadcast Domain

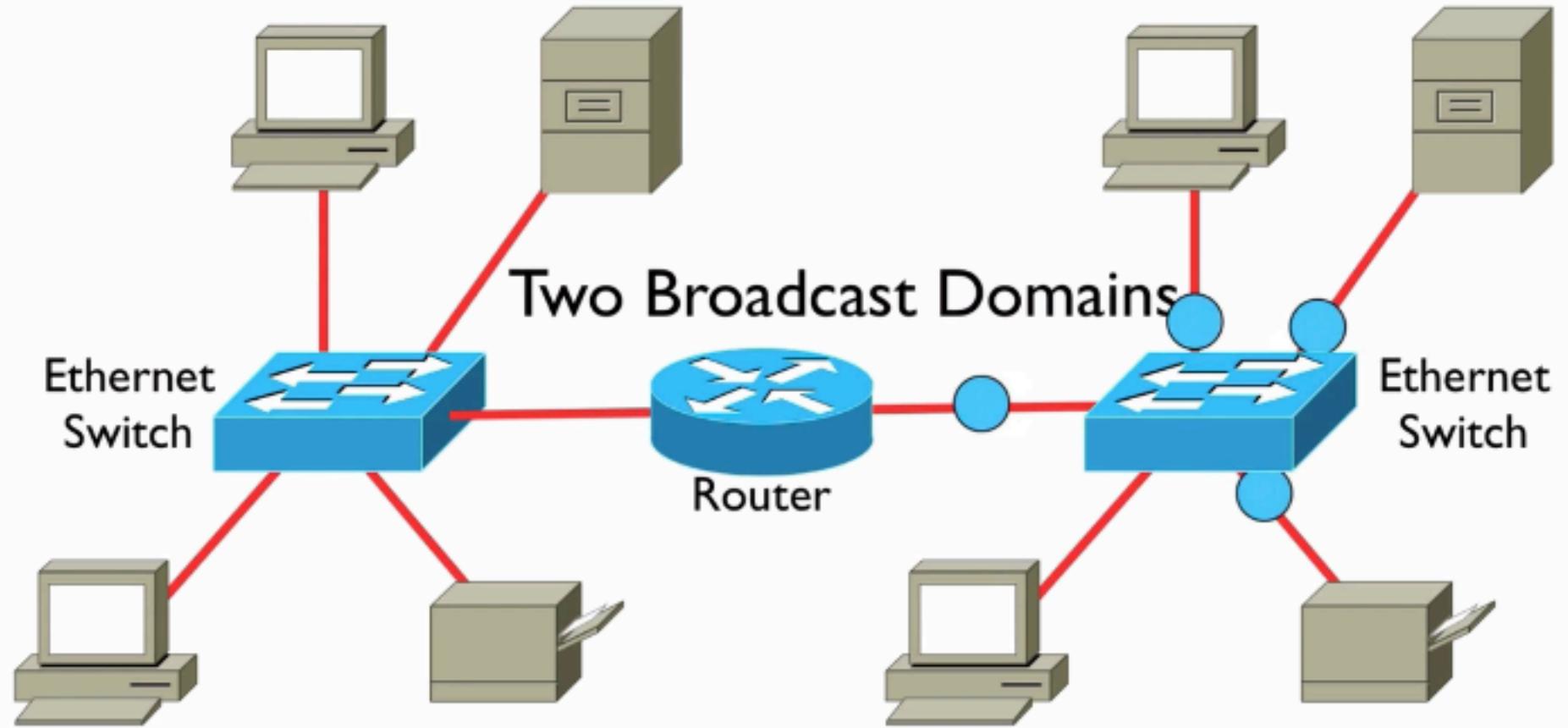


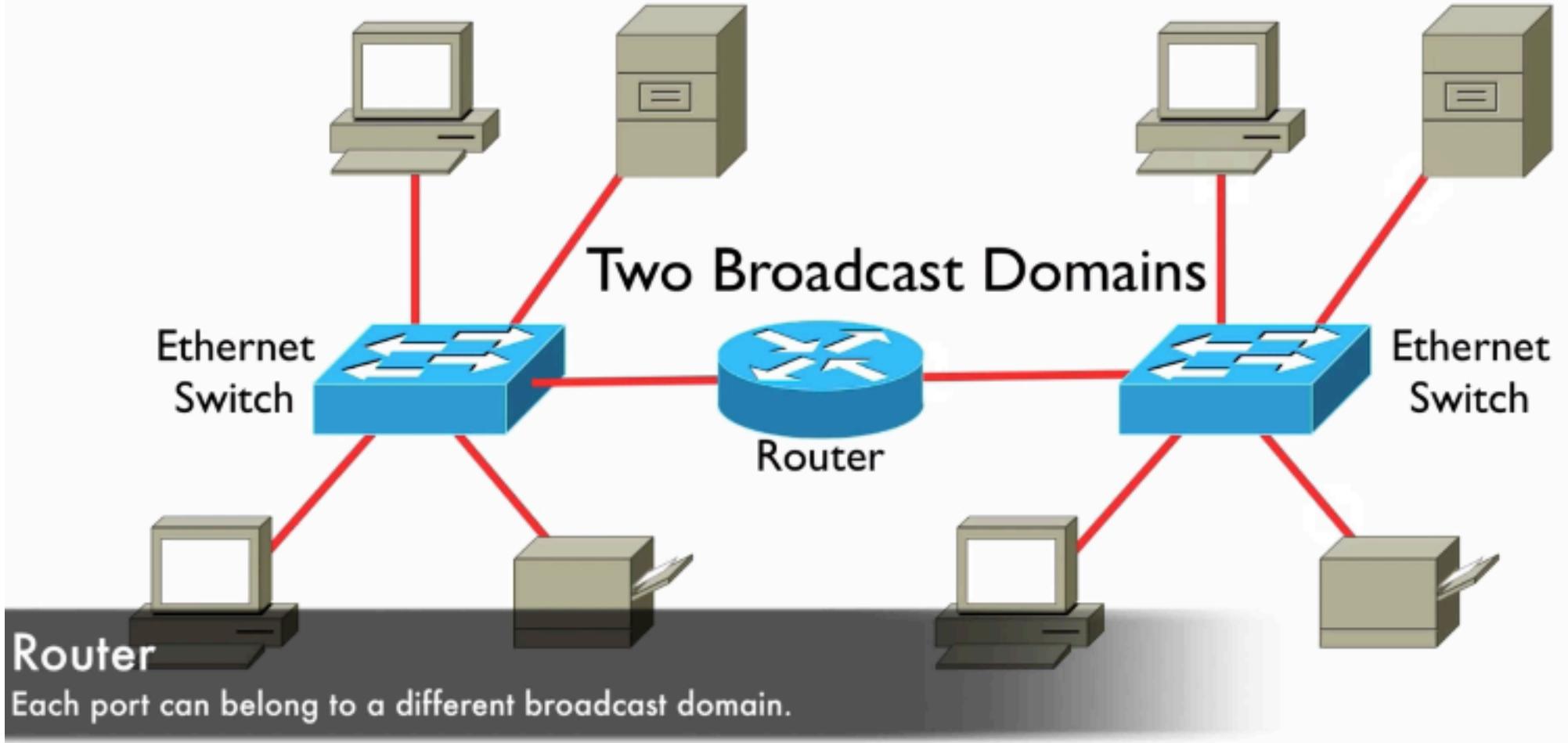
One Broadcast Domain

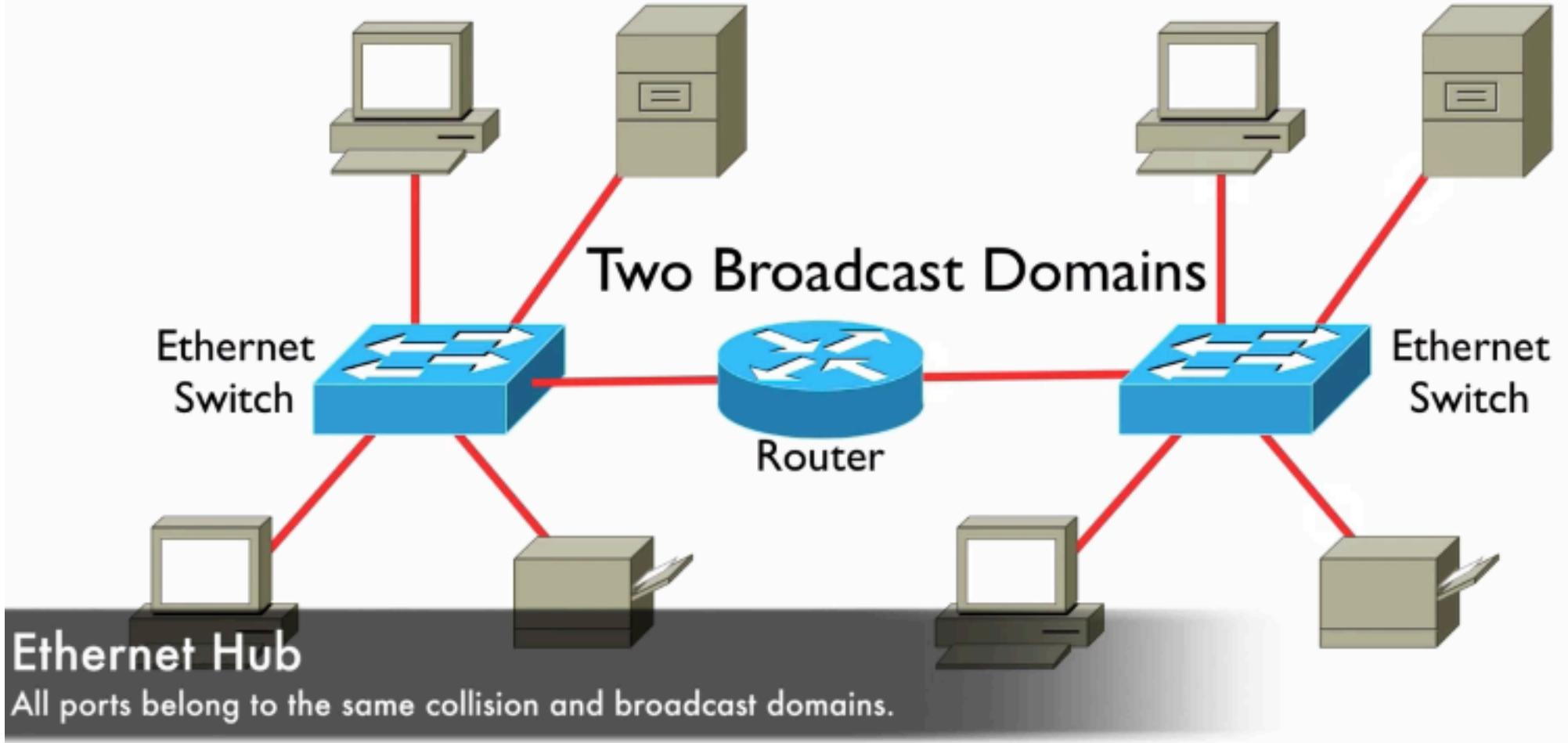
Ethernet Switch
All ports belong to the same broadcast domain.

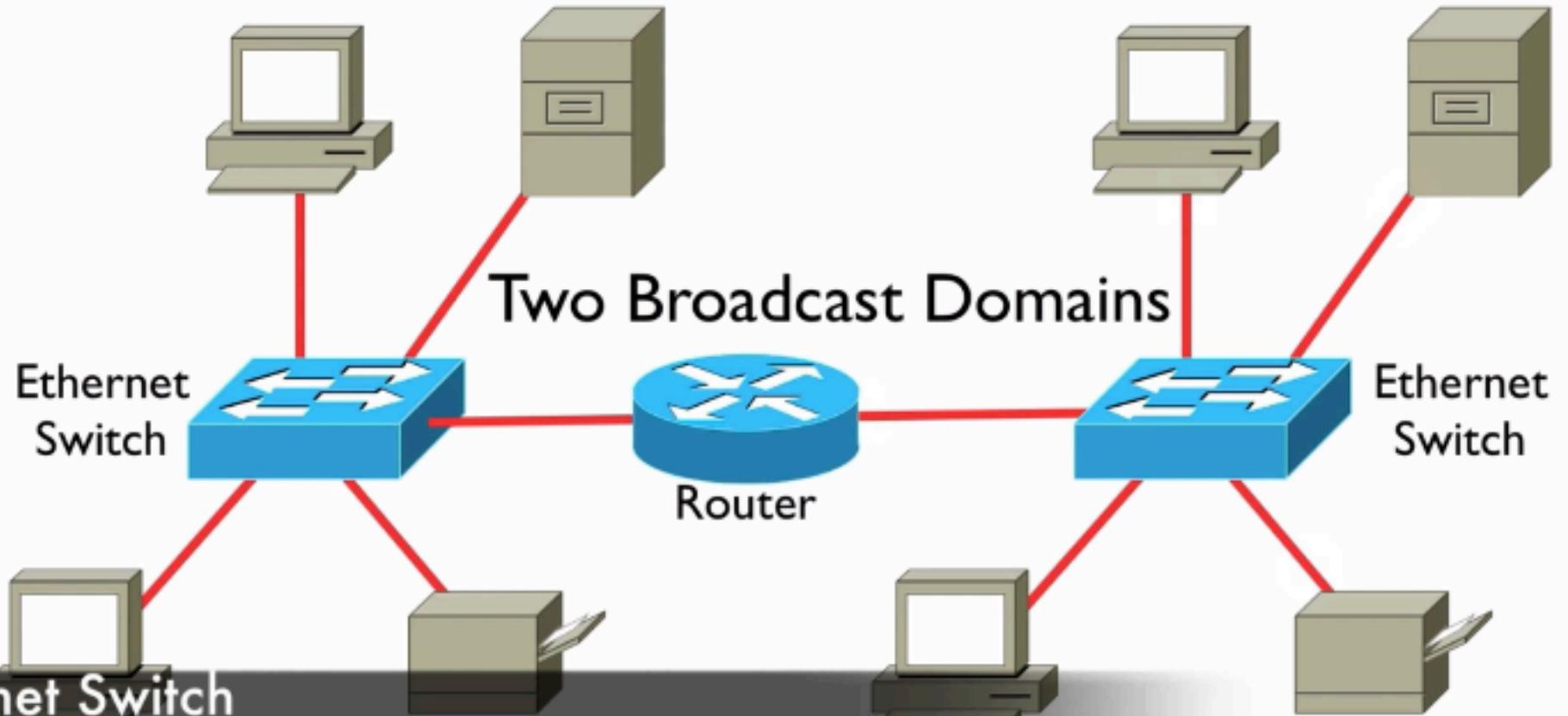






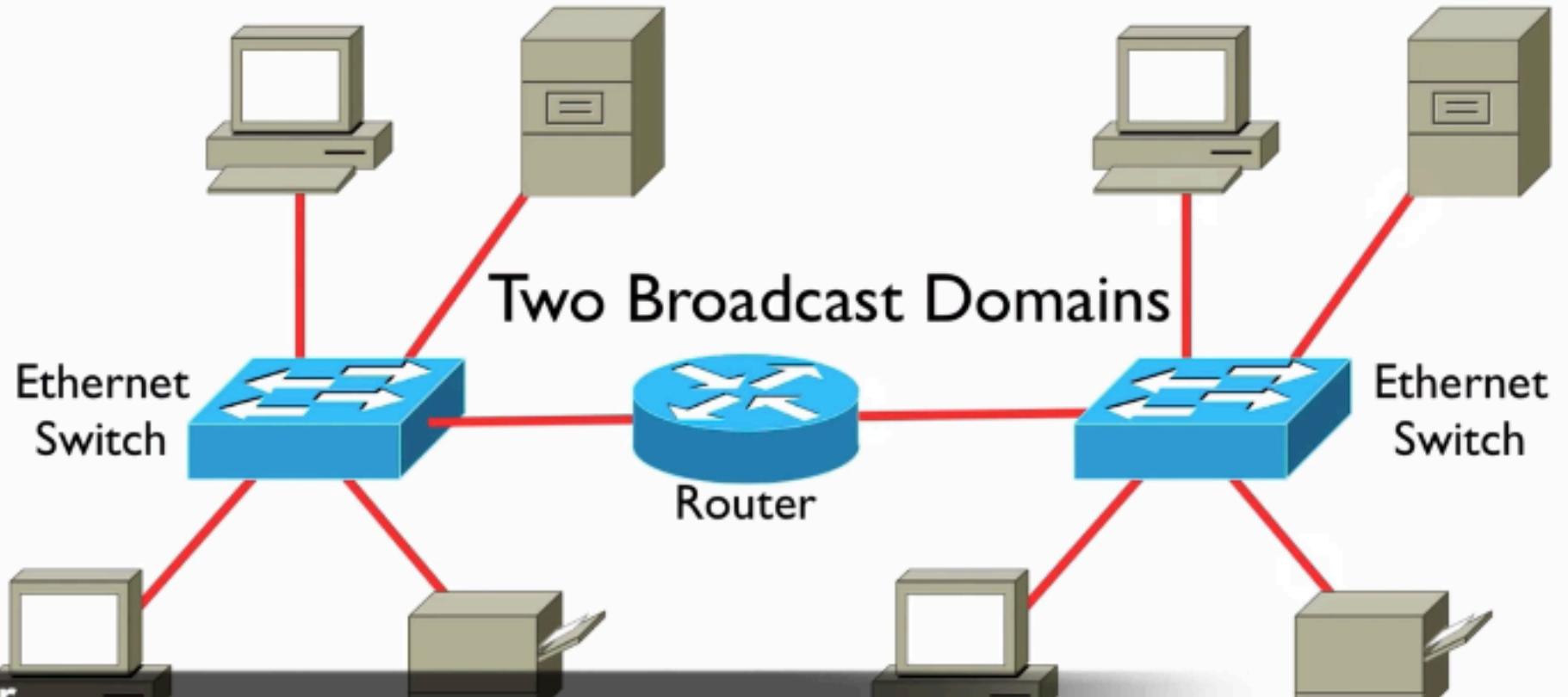






Ethernet Switch

All ports belong to separate collision domains but to the same broadcast domain.



Router

Each port (also called an interface) can belong to a separate collision domain and a separate broadcast domain.

Wireless Access Points

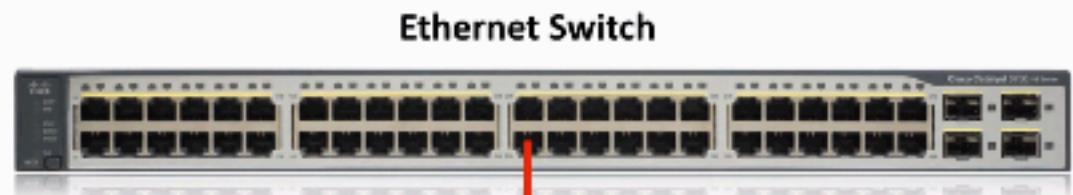
Wireless Access Points (APs)



Wireless Access Points (APs)



Laptop



Ethernet Switch



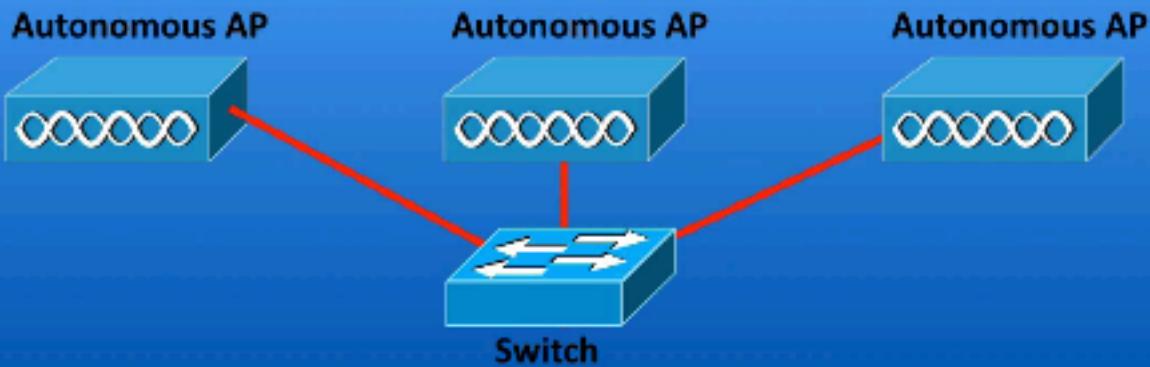
Wireless Access Point

Wireless Ad Hoc Network

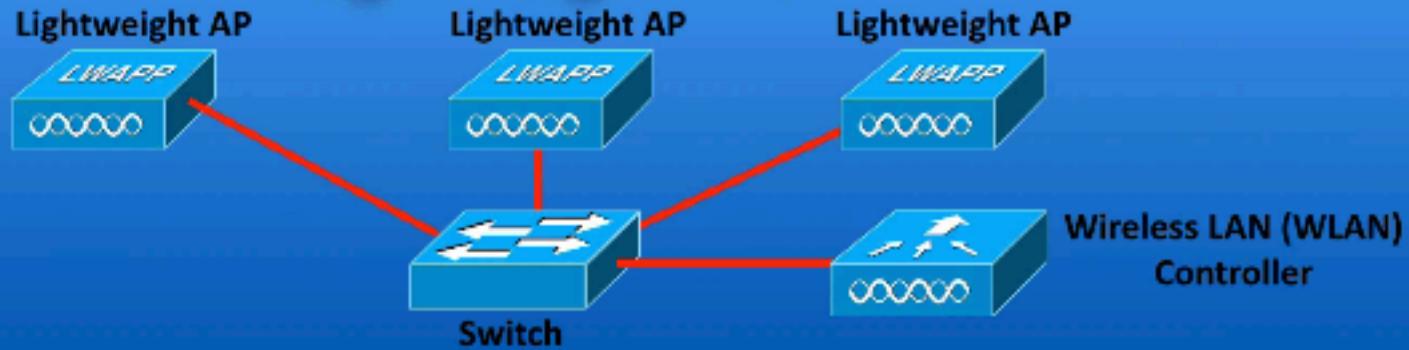
Allows wireless devices to communicate with one another without using a network infrastructure.

Wireless Access Points (APs)

Autonomous APs

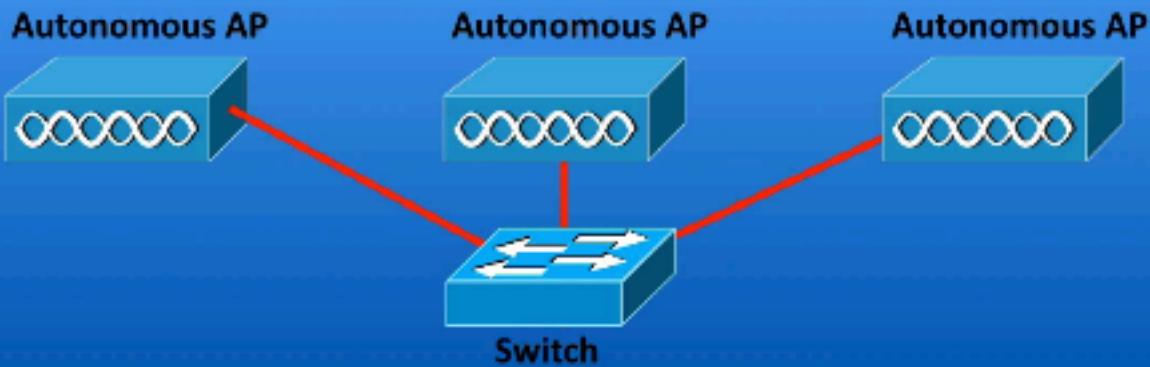


Lightweight APs

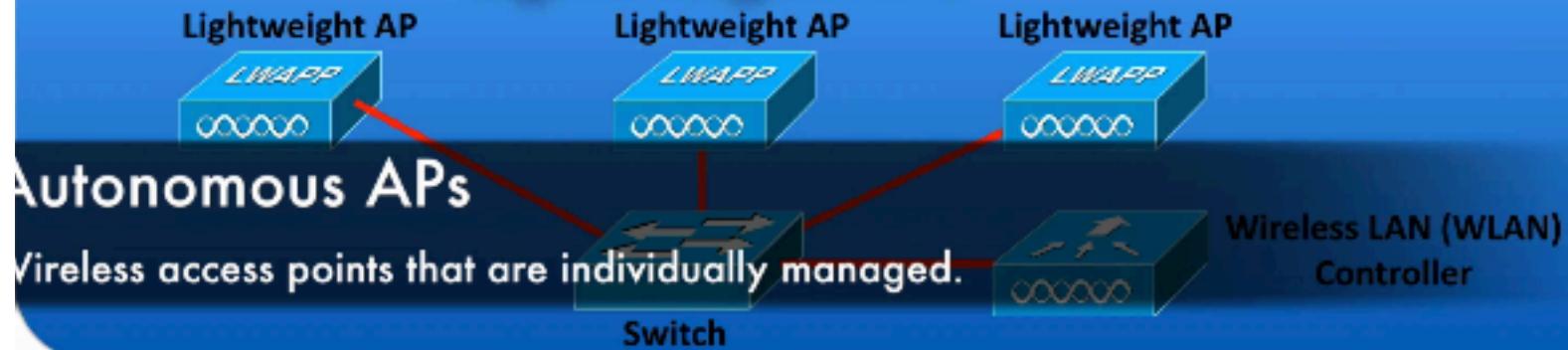


Wireless Access Points (APs)

Autonomous APs

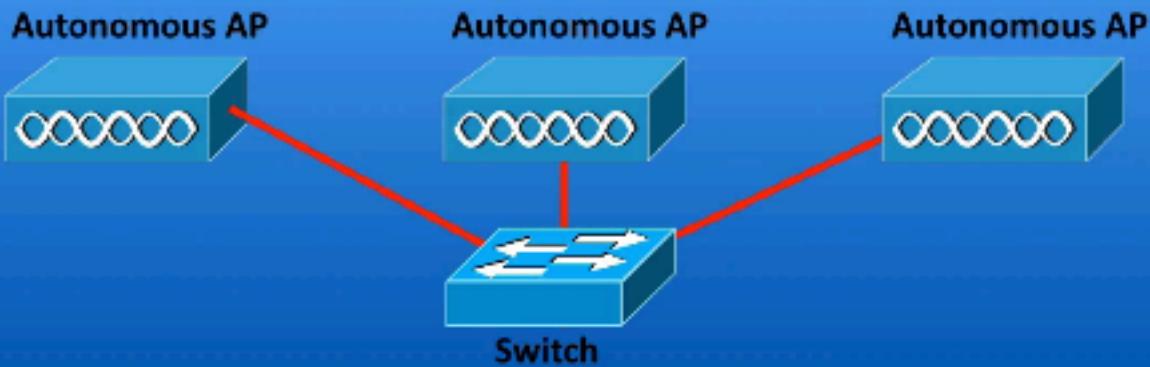


Lightweight APs

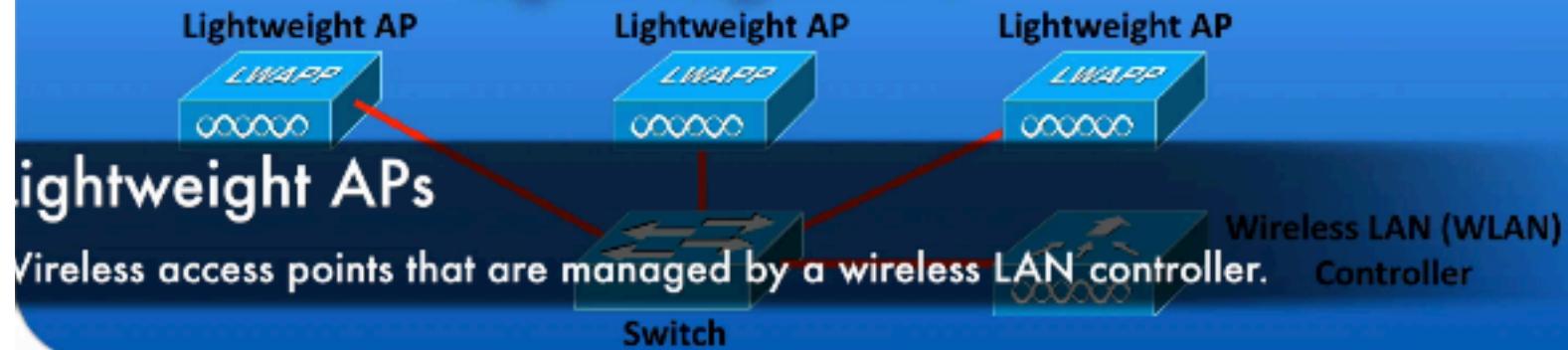


Wireless Access Points (APs)

Autonomous APs

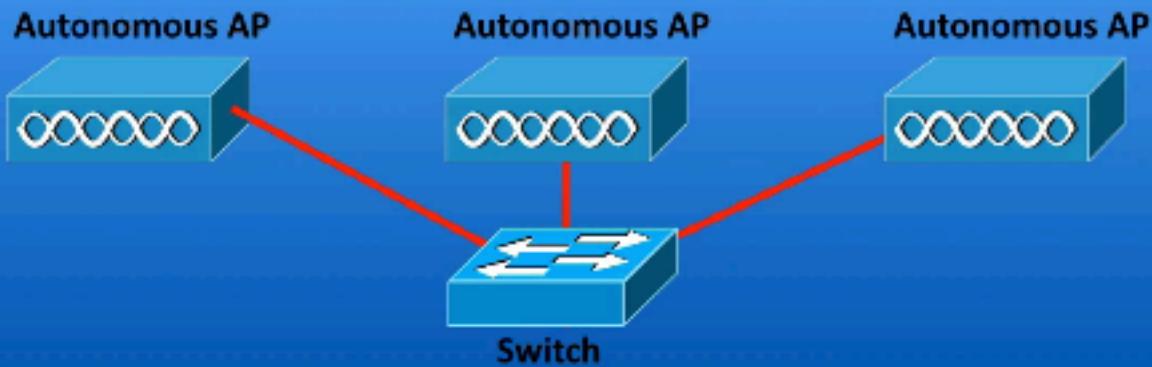


Lightweight APs

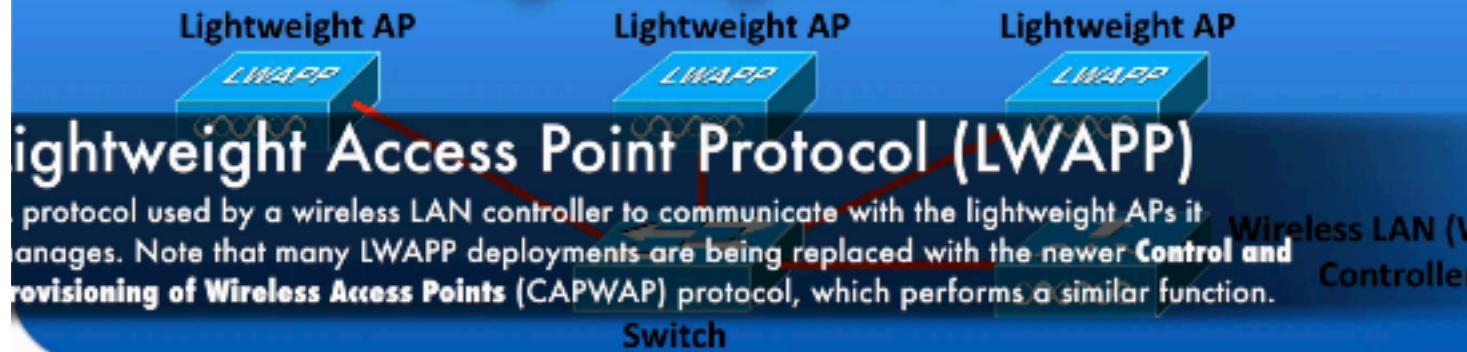


Wireless Access Points (APs)

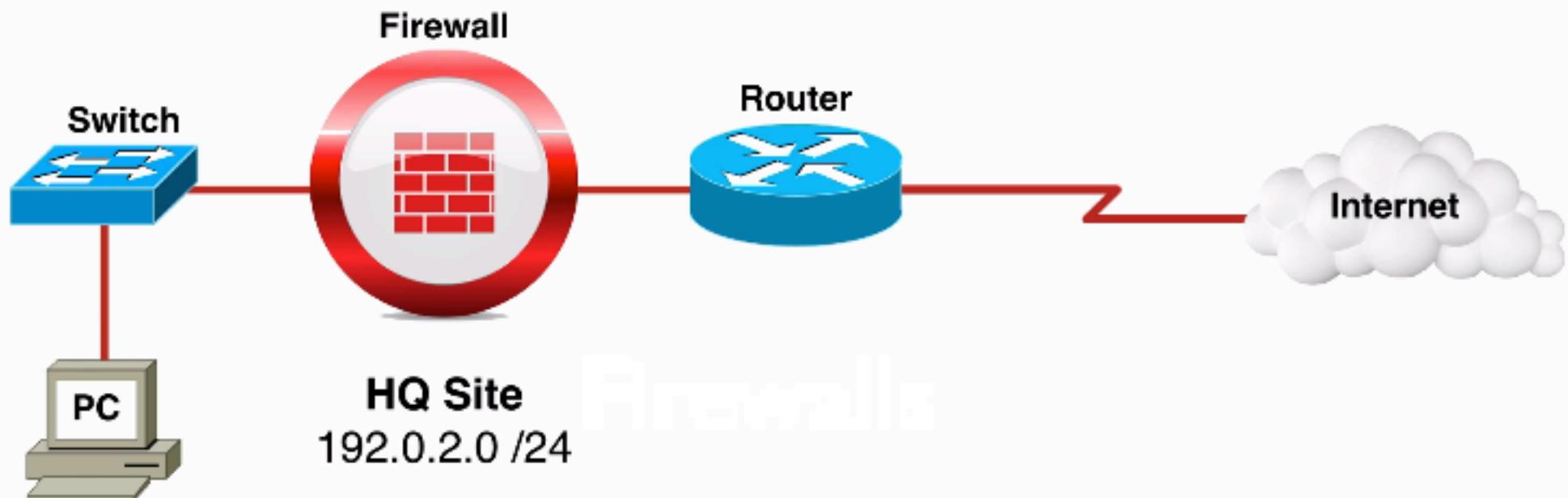
Autonomous APs



Lightweight APs

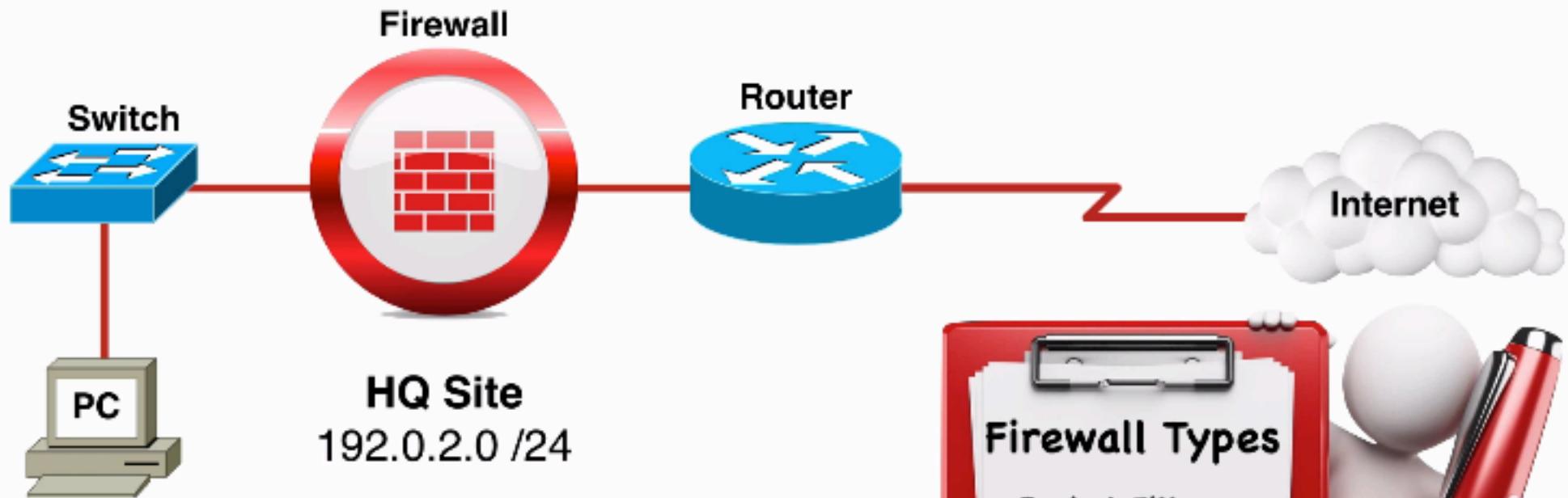


Firewalls



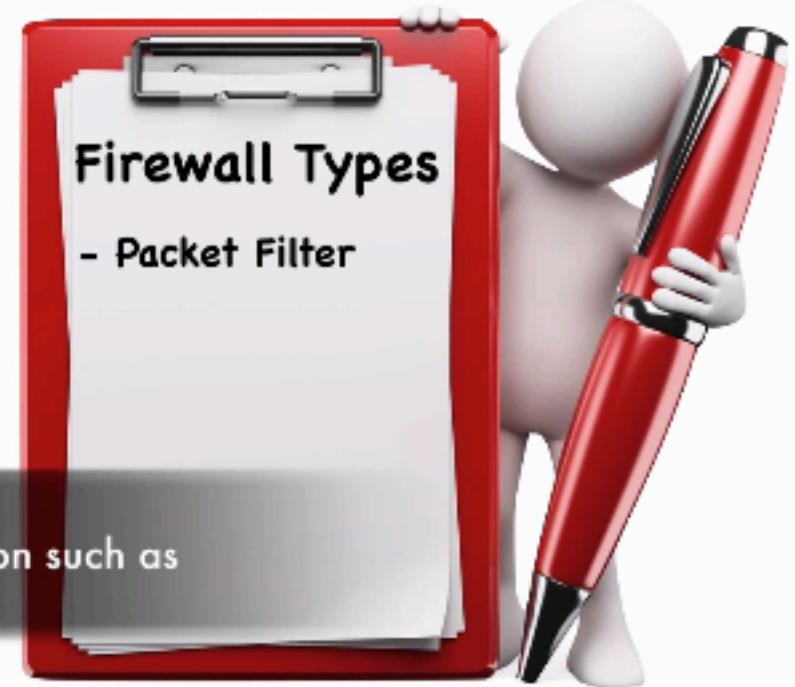
firewall

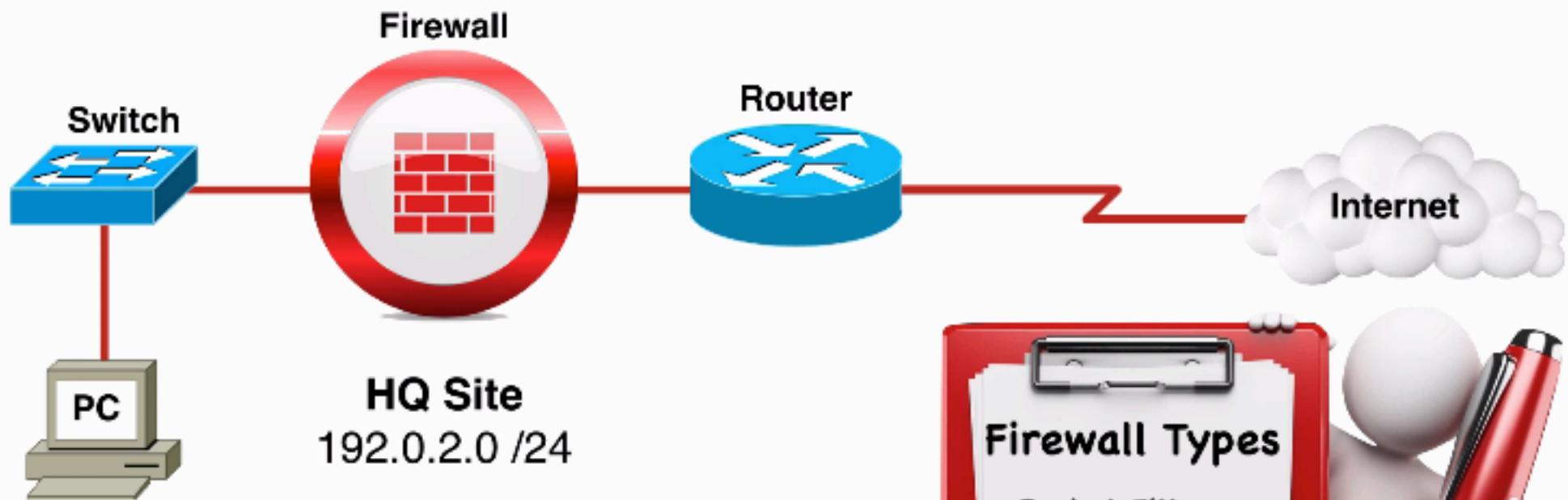
A network device (or software) that can help prevent malicious traffic from spreading into a secured area of a network, through the use of rule sets.



Packet Filter

A type of firewall that can permit or deny traffic based on information such as source and/or destination IP addresses and port numbers.

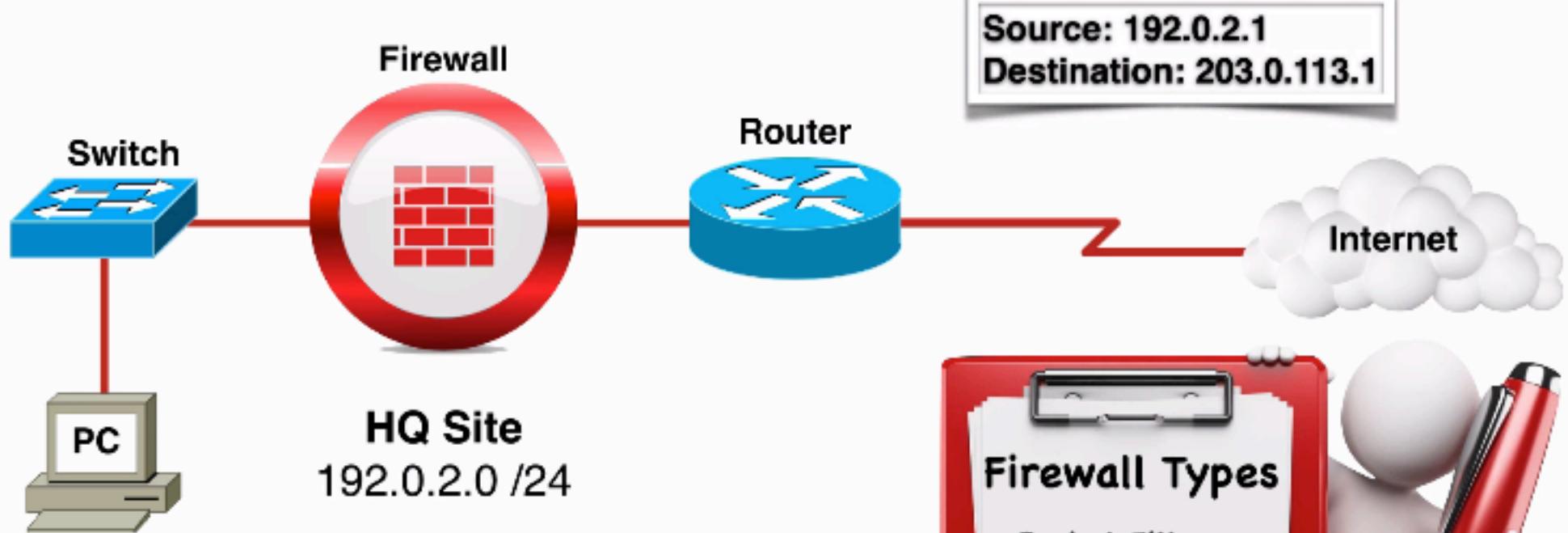




Rules

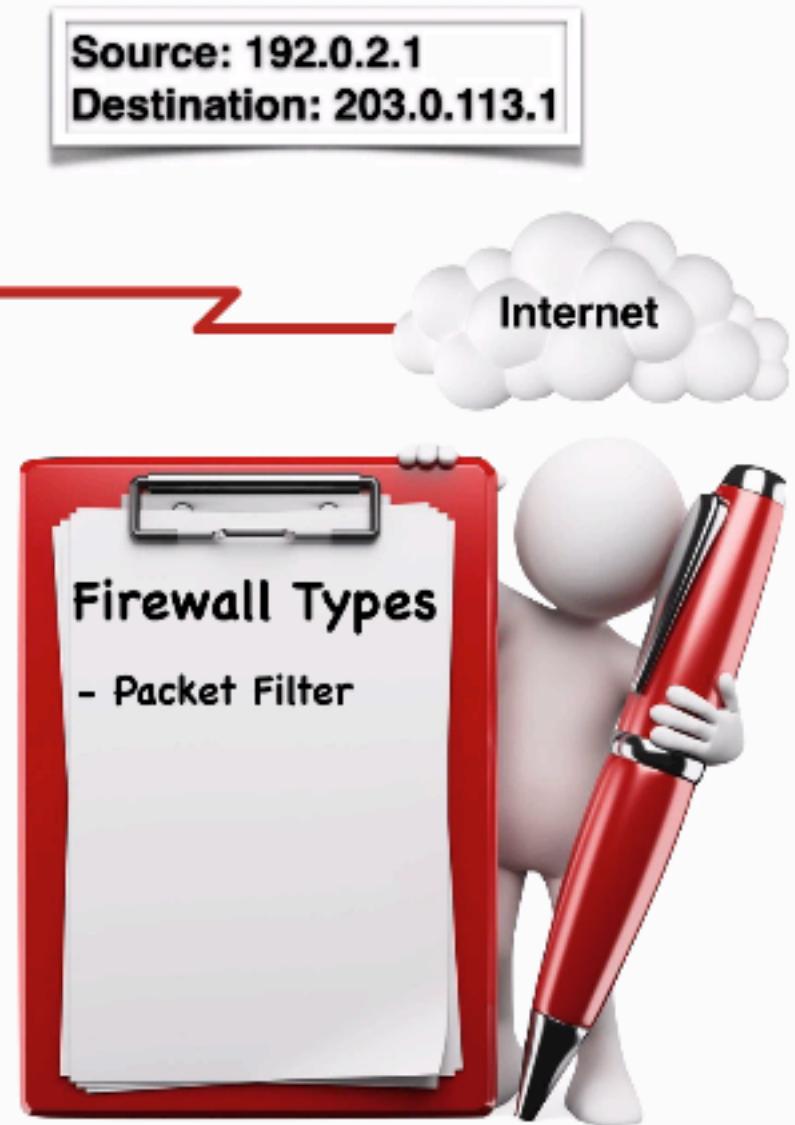
Source	Destination	Action
192.0.2.0 /24	Any	Permit
203.0.113.0 /24	192.0.2.0 /24	Permit
Any	Any	Deny

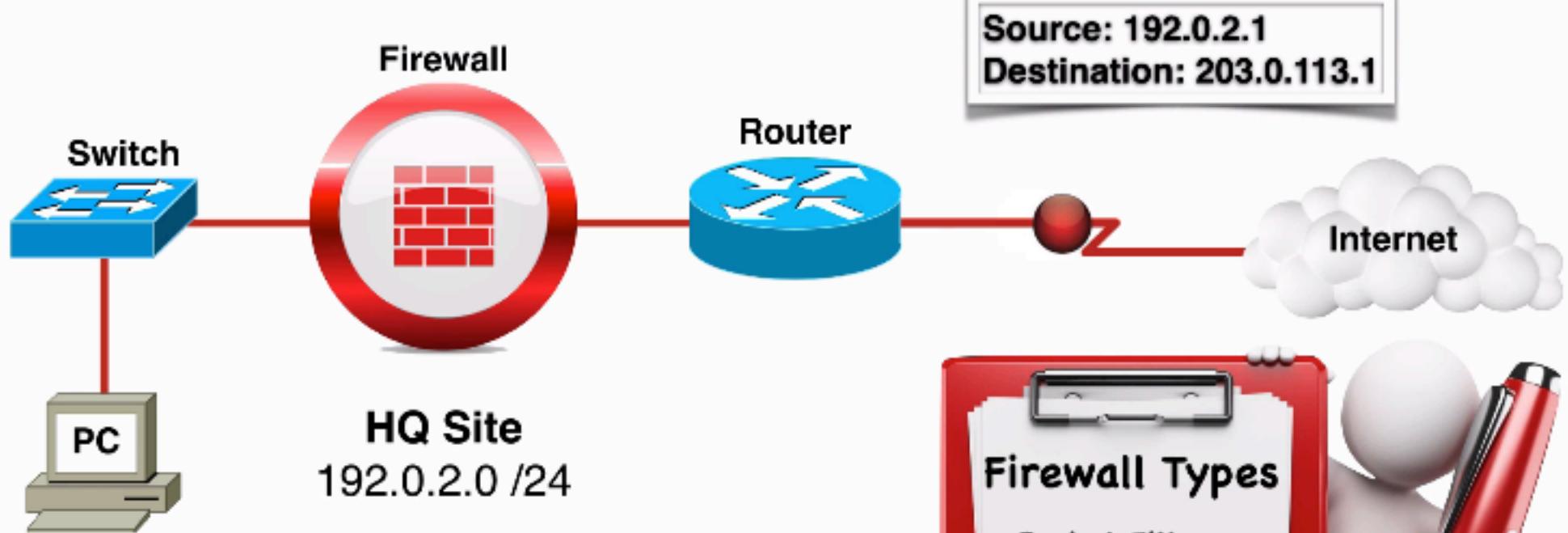




Rules

Source	Destination	Action
192.0.2.0 /24	Any	Permit
203.0.113.0 /24	192.0.2.0 /24	Permit
Any	Any	Deny

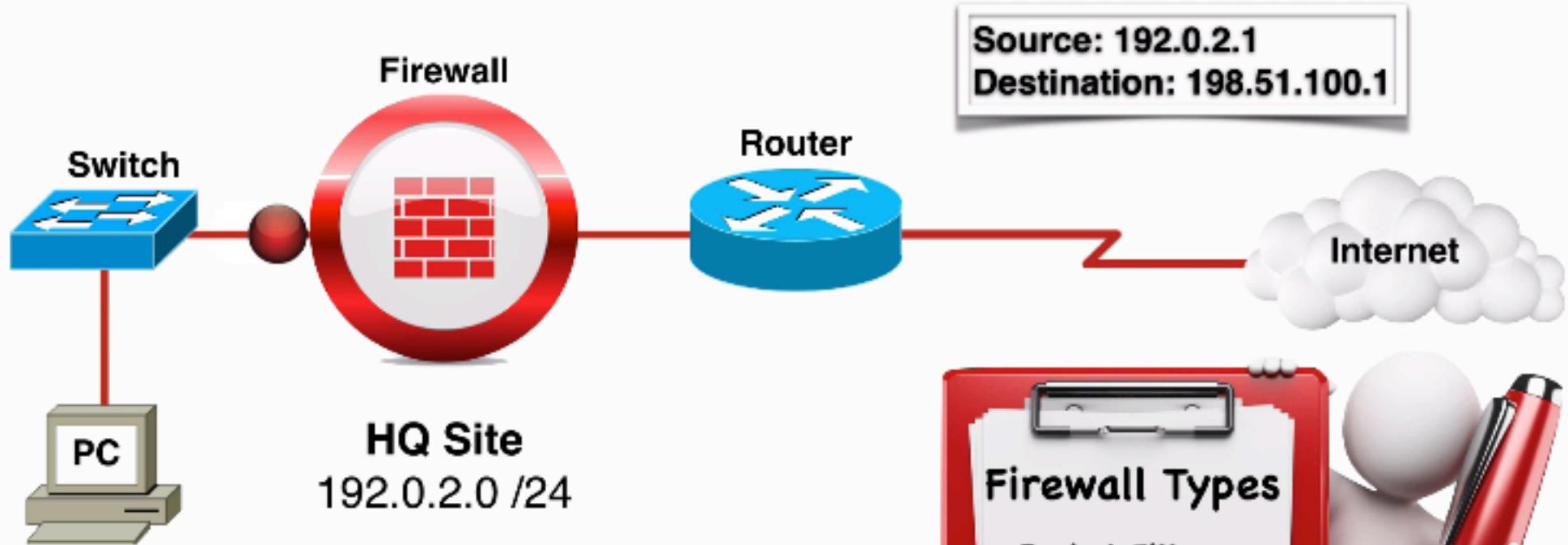




Rules

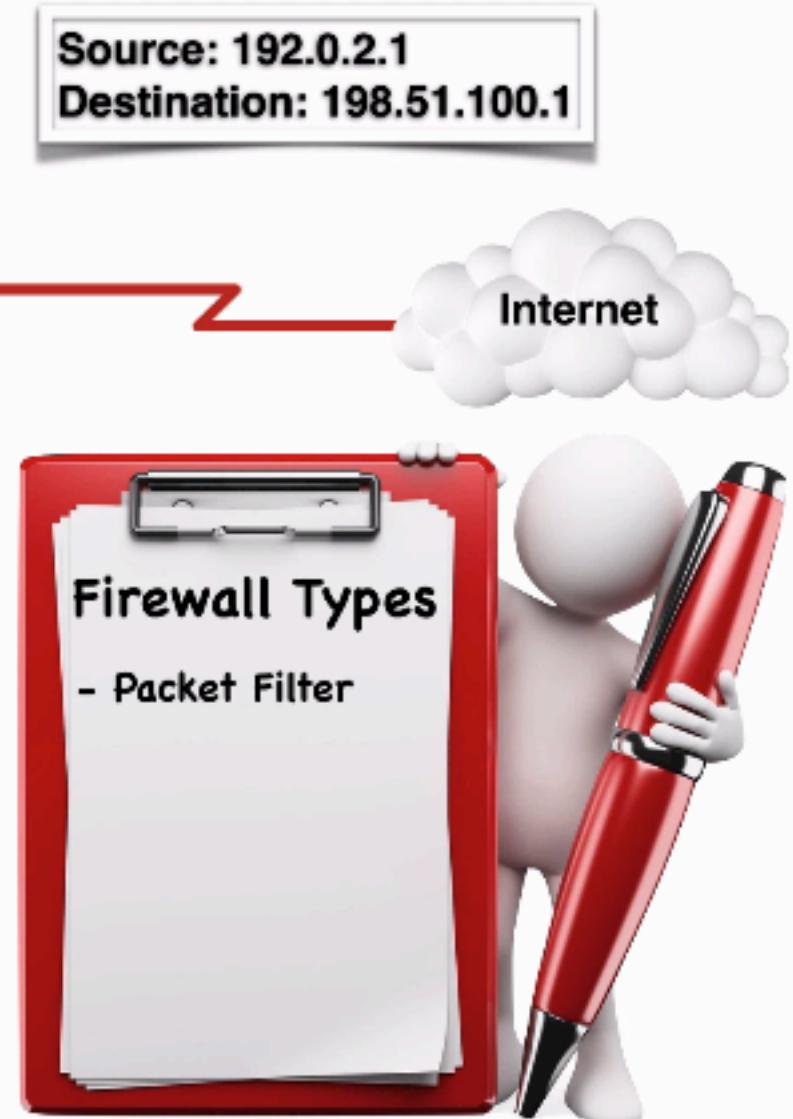
Source	Destination	Action
192.0.2.0 /24	Any	Permit
203.0.113.0 /24	192.0.2.0 /24	Permit
Any	Any	Deny

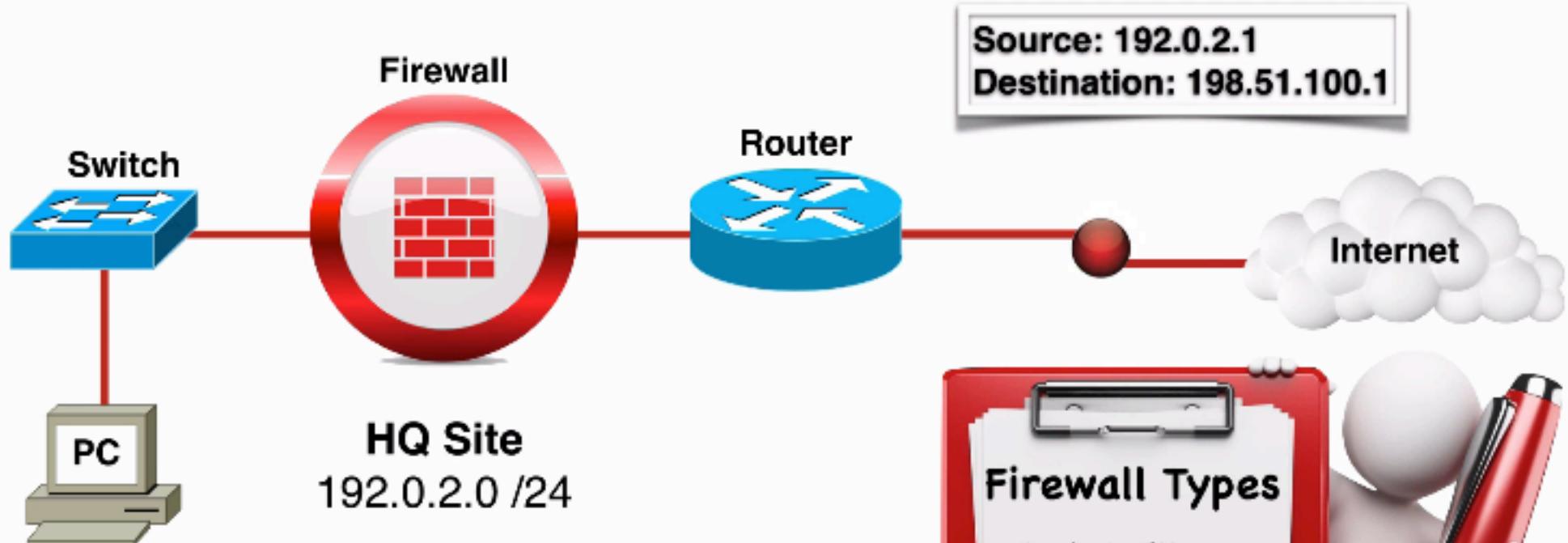




Rules

Source	Destination	Action
192.0.2.0 /24	Any	Permit
203.0.113.0 /24	192.0.2.0 /24	Permit
Any	Any	Deny

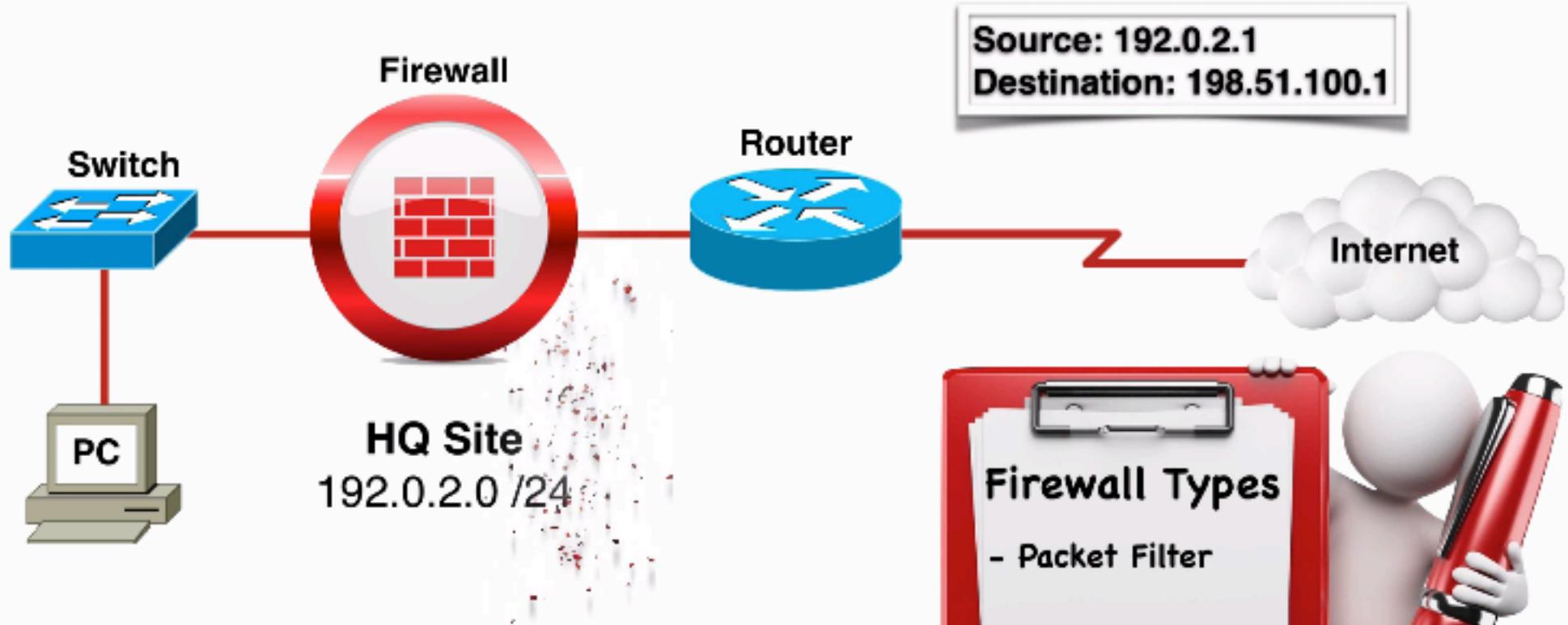




Rules

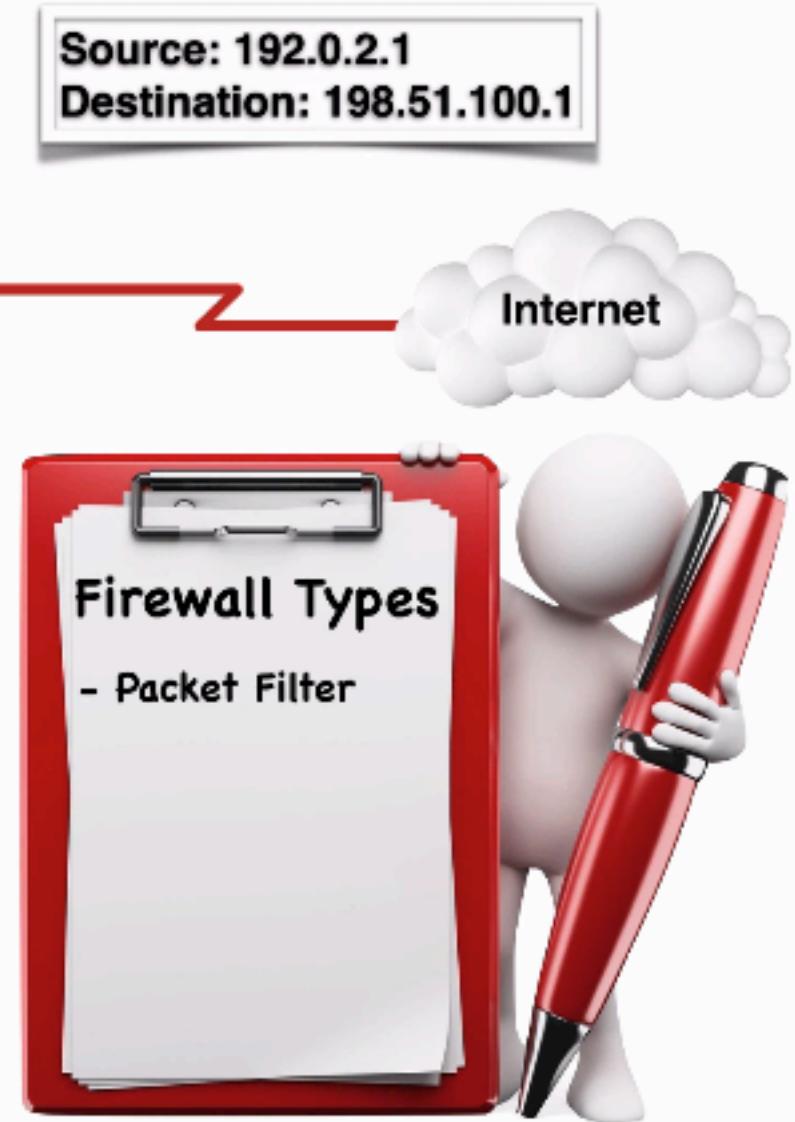
Source	Destination	Action
192.0.2.0 /24	Any	Permit
203.0.113.0 /24	192.0.2.0 /24	Permit
Any	Any	Deny

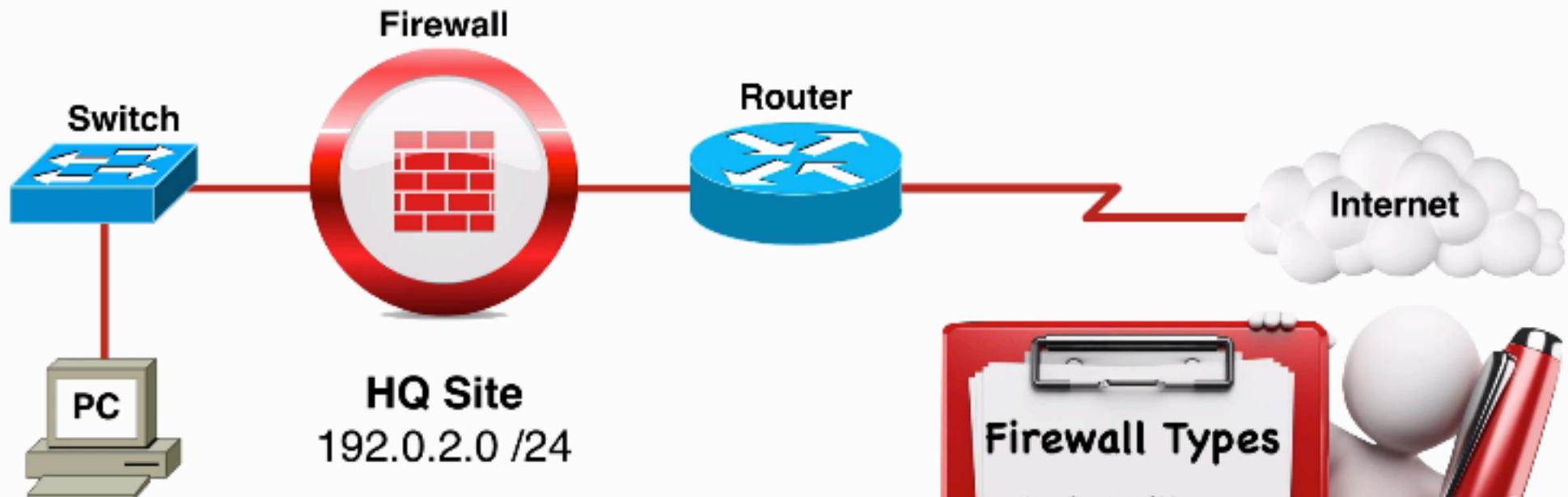




Rules

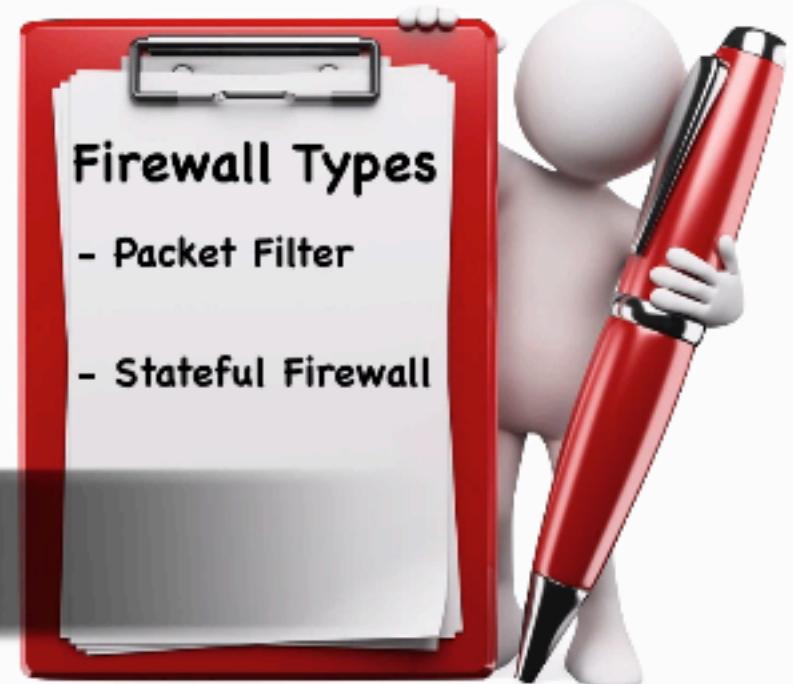
Source	Destination	Action
192.0.2.0 /24	Any	Permit
203.0.113.0 /24	192.0.2.0 /24	Permit
Any	Any	Deny

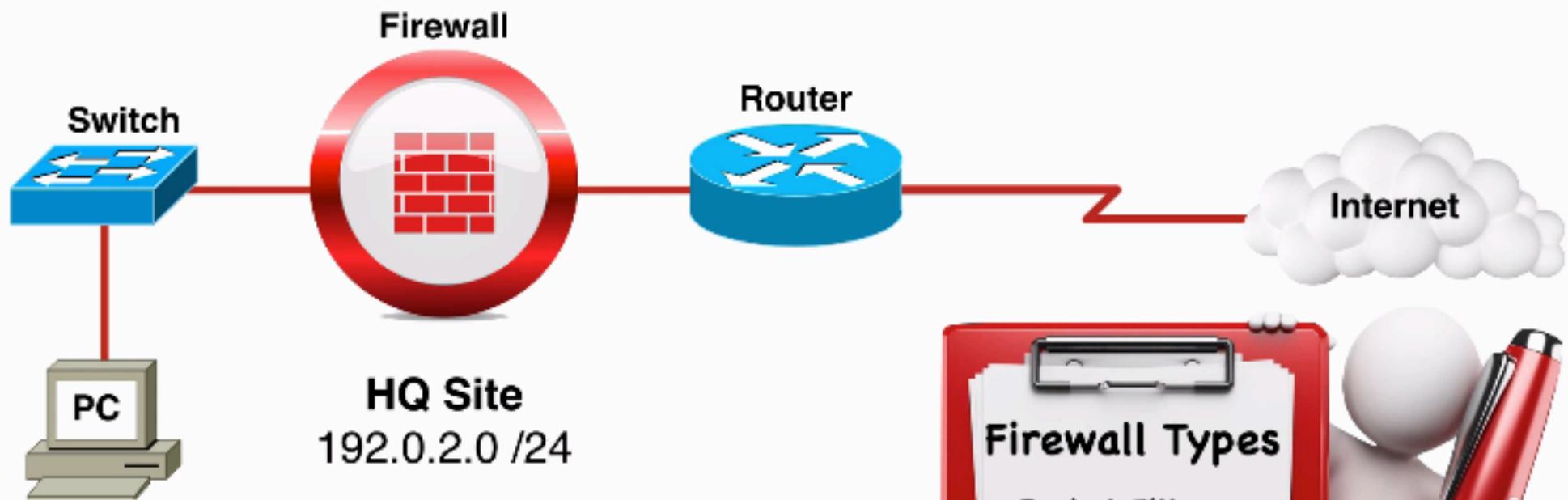




Stateful Firewall

A type of firewall that, in addition to permitting or denying traffic based on IP address and/or port number information, can inspect sessions and recognize return traffic for a session that was initiated from a trusted network.

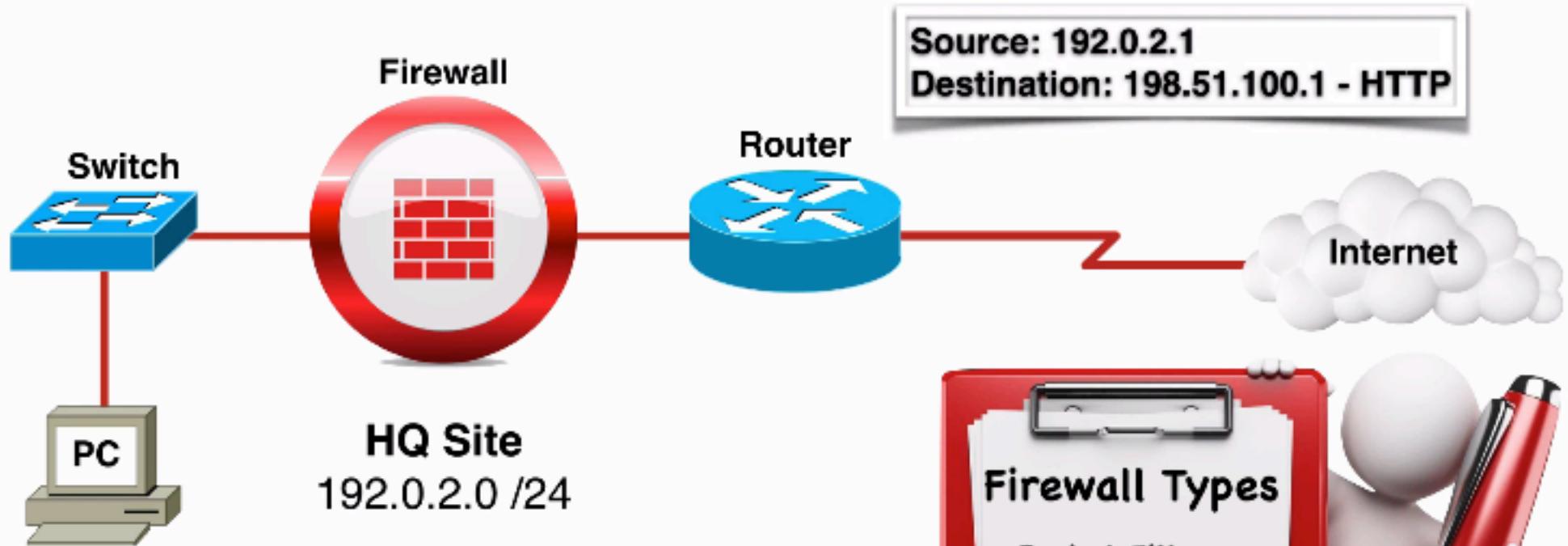




Rules

Source	Destination	Action
192.0.2.0 /24	Any - TCP Port 80	Permit
Any	Any	Deny

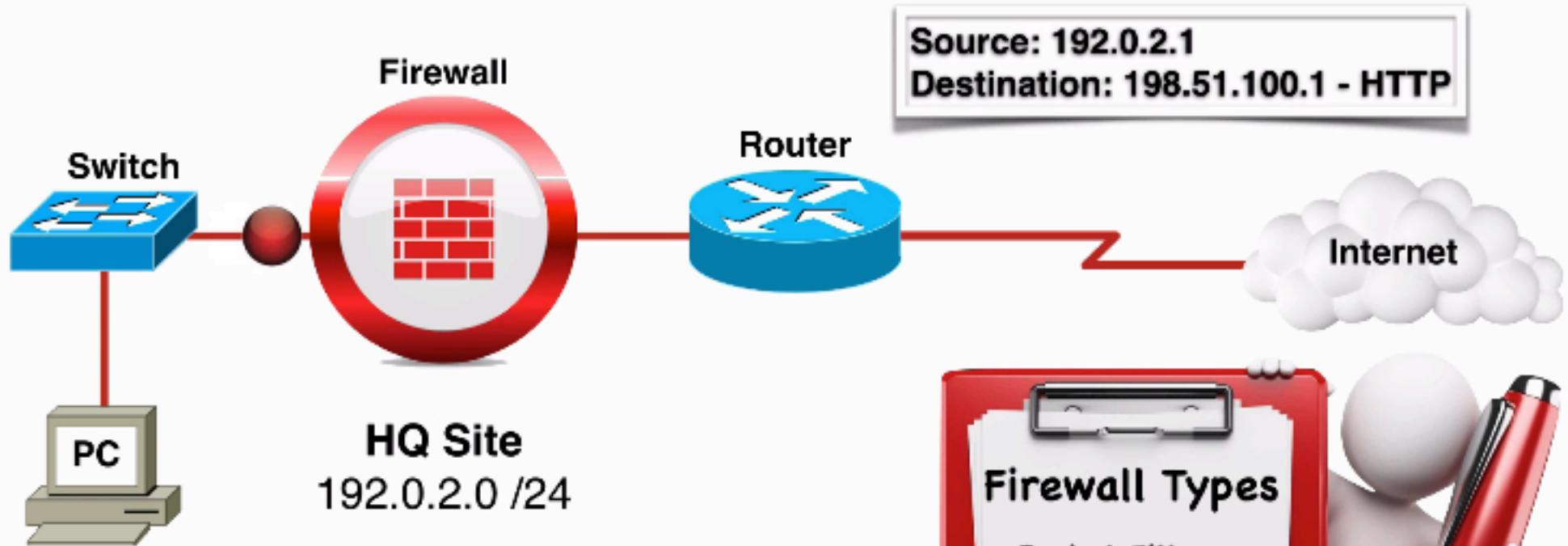




Rules

Source	Destination	Action
192.0.2.0 /24	Any - TCP Port 80	Permit
Any	Any	Deny

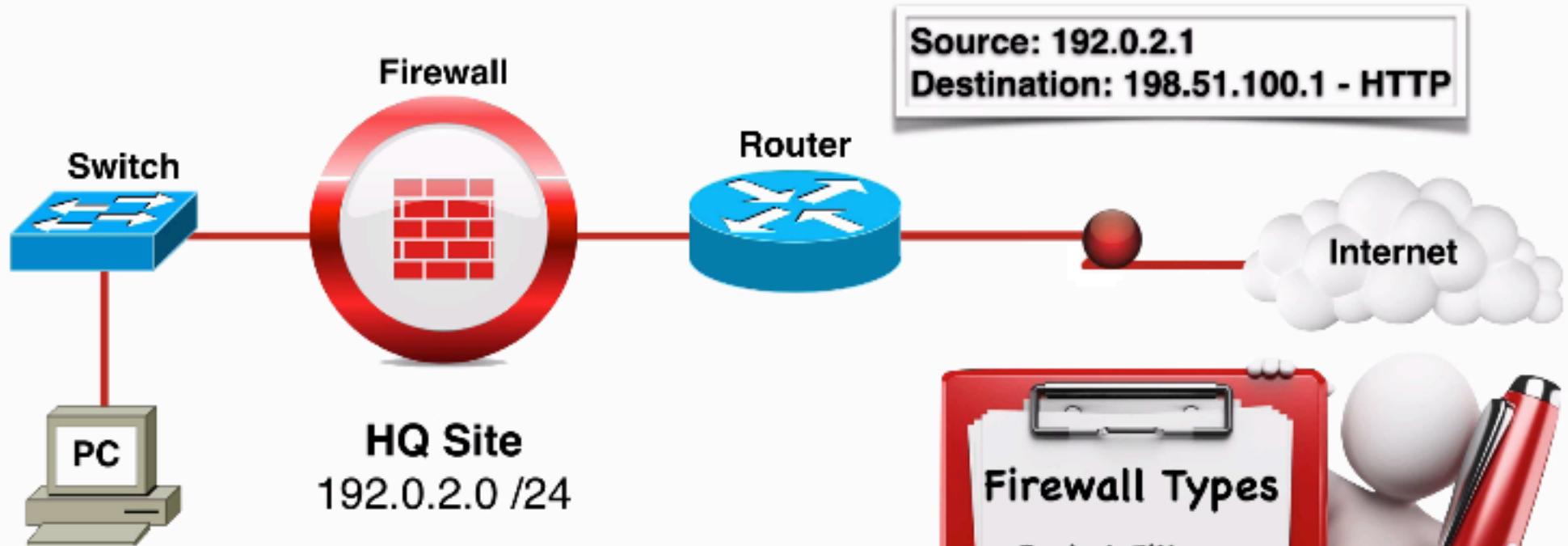




Rules

Source	Destination	Action
192.0.2.0 /24	Any - TCP Port 80	Permit
Any	Any	Deny

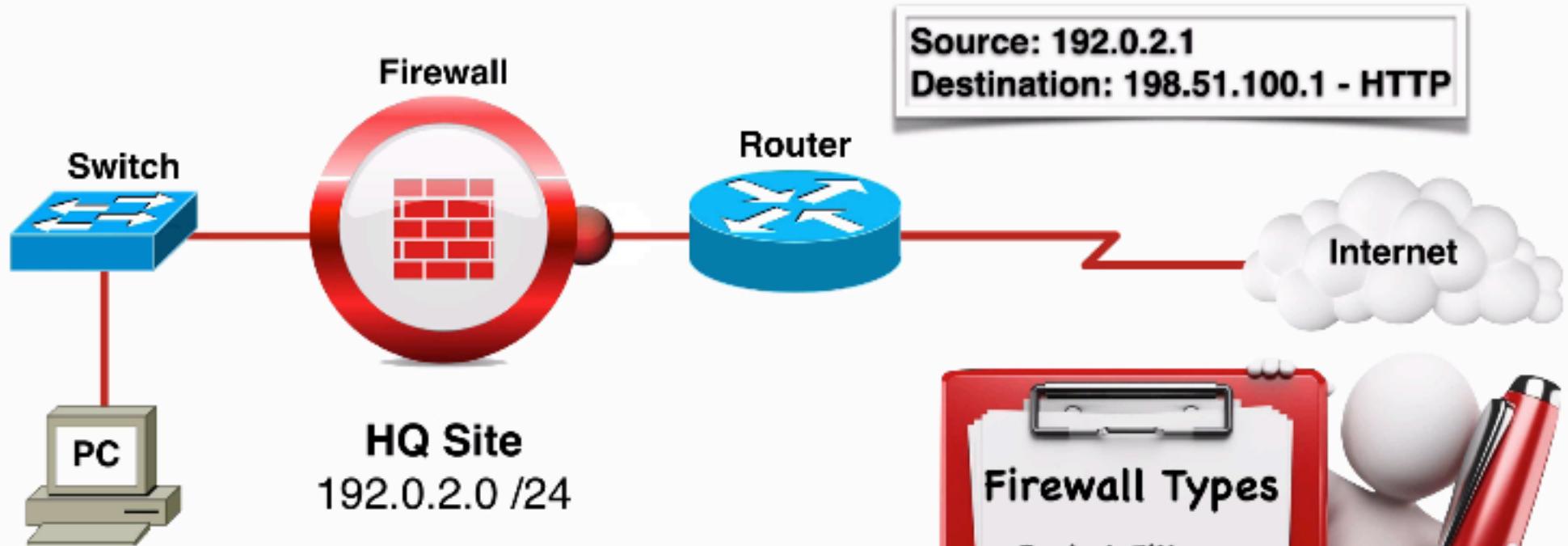




Rules

Source	Destination	Action
192.0.2.0 /24	Any - TCP Port 80	Permit
Any	Any	Deny



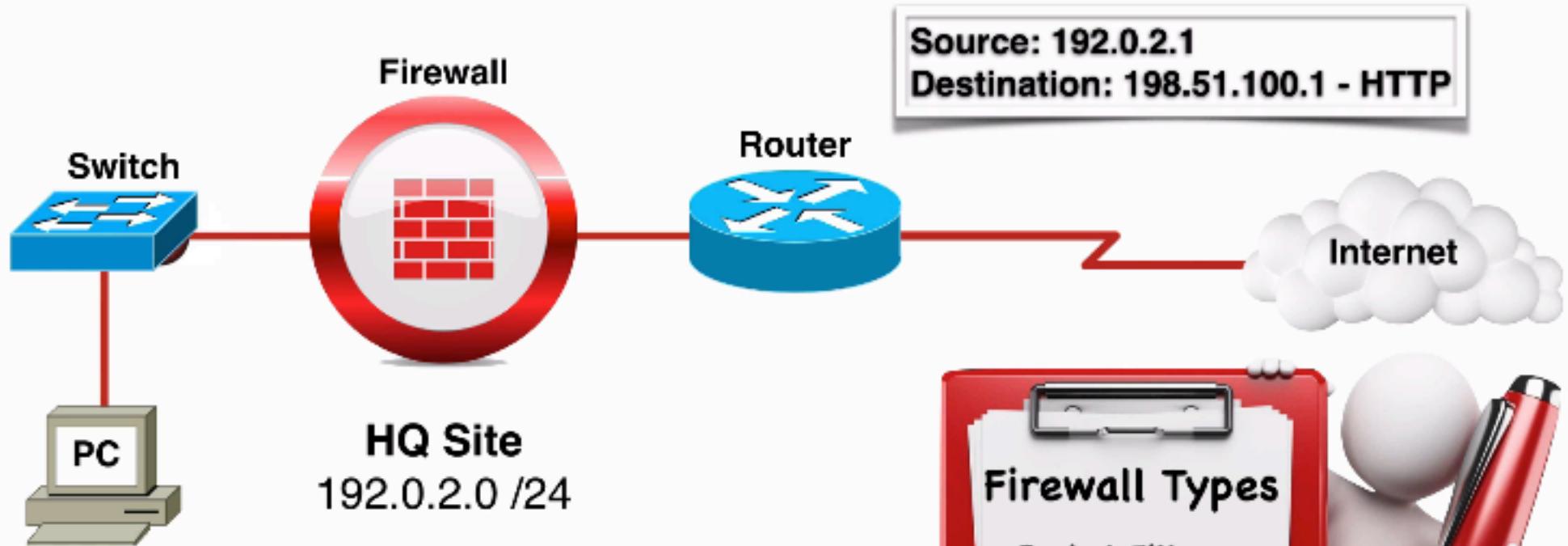


Rules

Source	Destination	Action
192.0.2.0 /24	Any - TCP Port 80	Permit
Any	Any	Deny

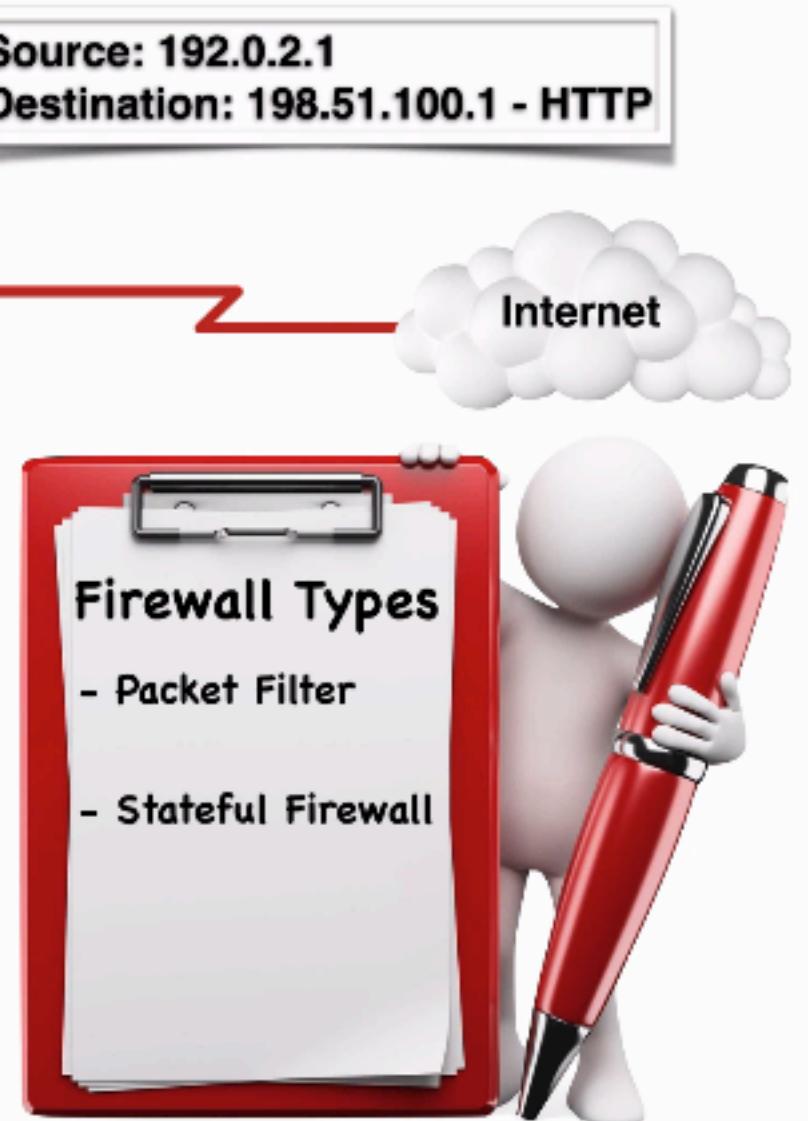
Source: 192.0.2.1
Destination: 198.51.100.1 - HTTP

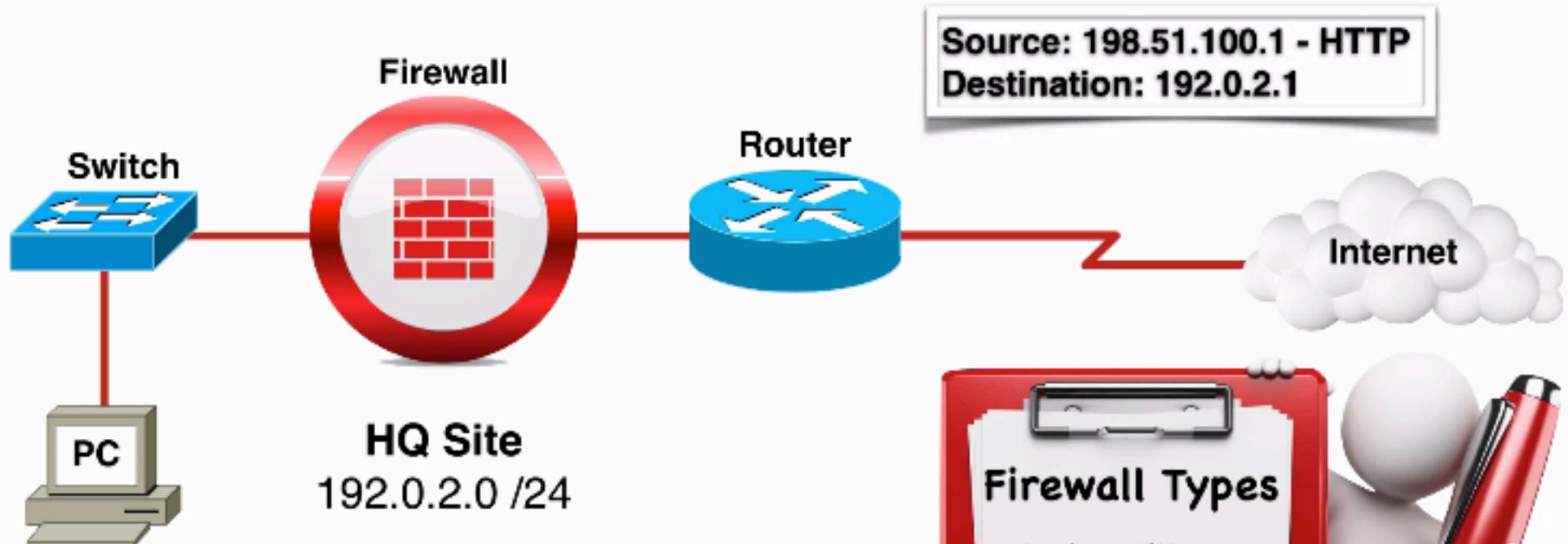




Rules

Source	Destination	Action
192.0.2.0 /24	Any - TCP Port 80	Permit
Any	Any	Deny

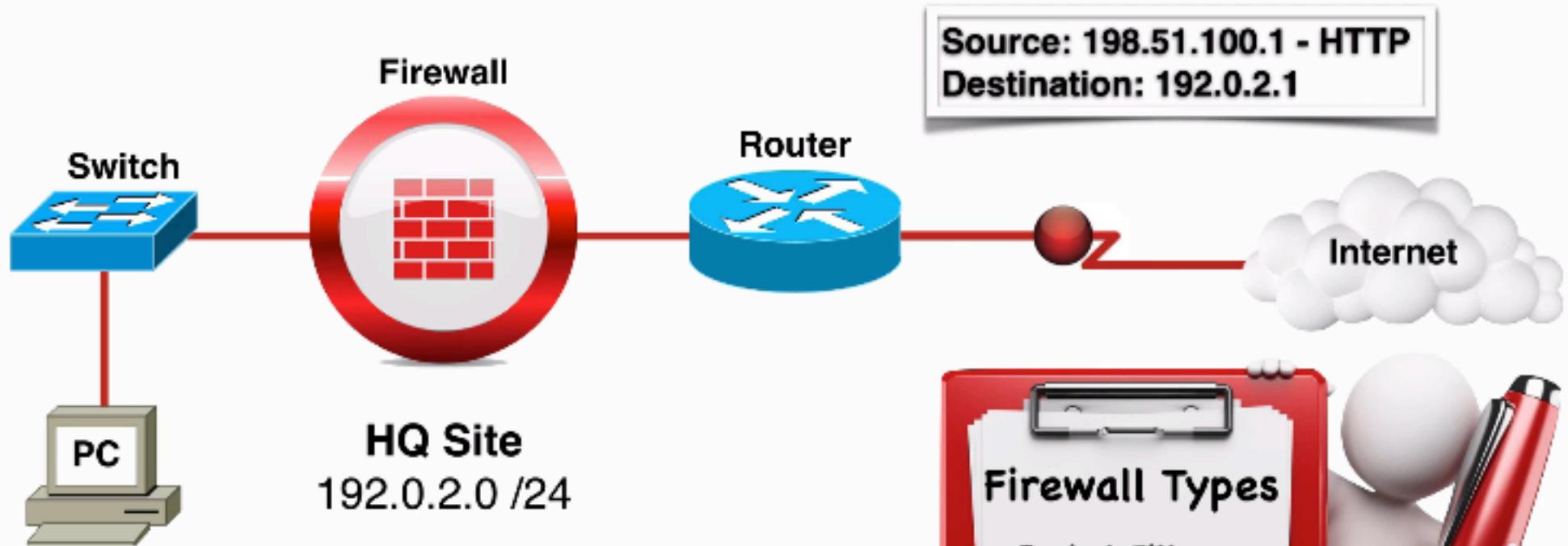




Rules

Source	Destination	Action
192.0.2.0 /24	Any - TCP Port 80	Permit
Any	Any	Deny

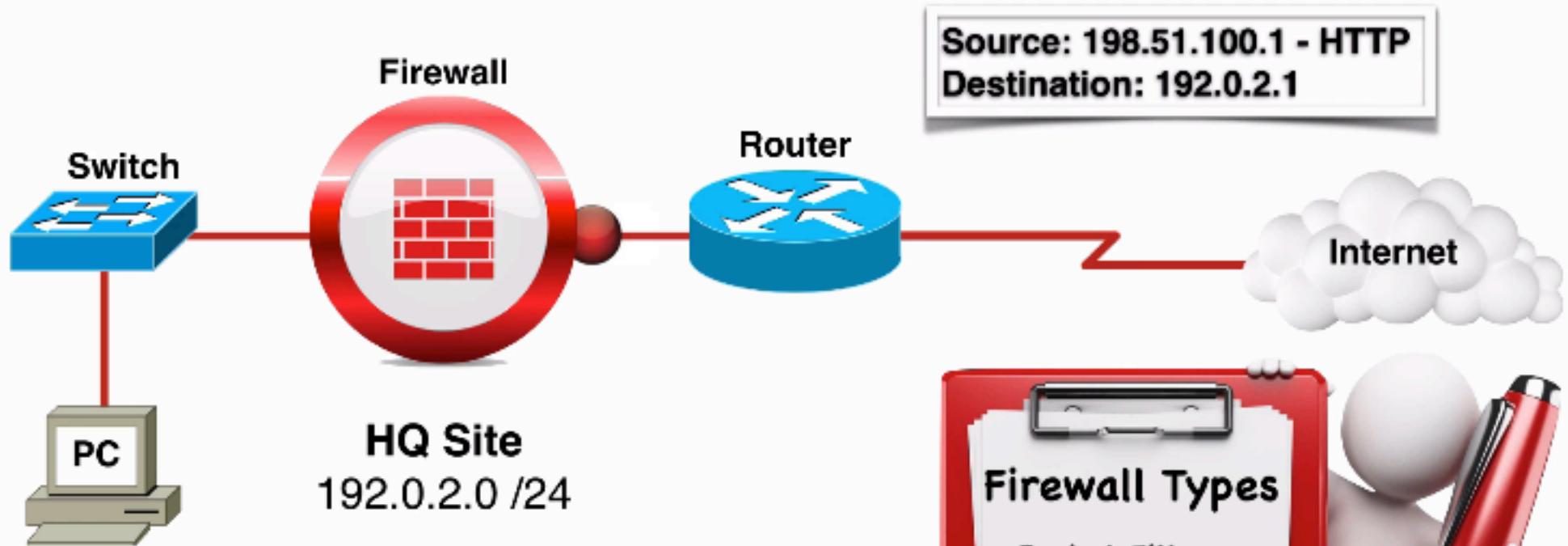




Rules

Source	Destination	Action
192.0.2.0 /24	Any - TCP Port 80	Permit
Any	Any	Deny

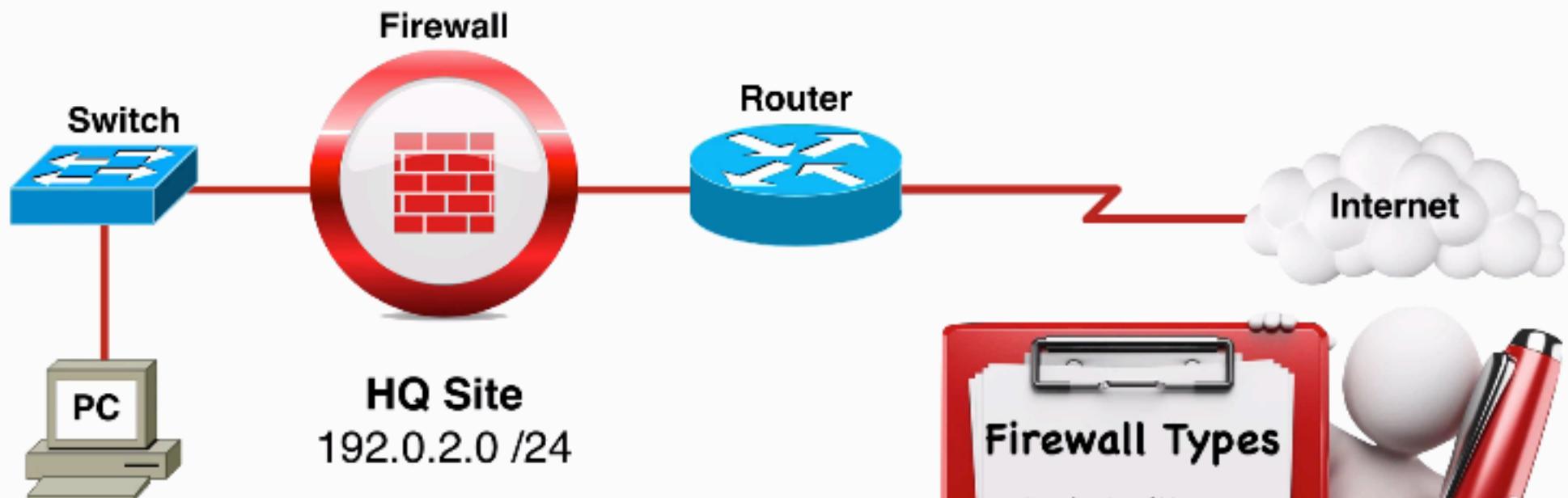




Rules

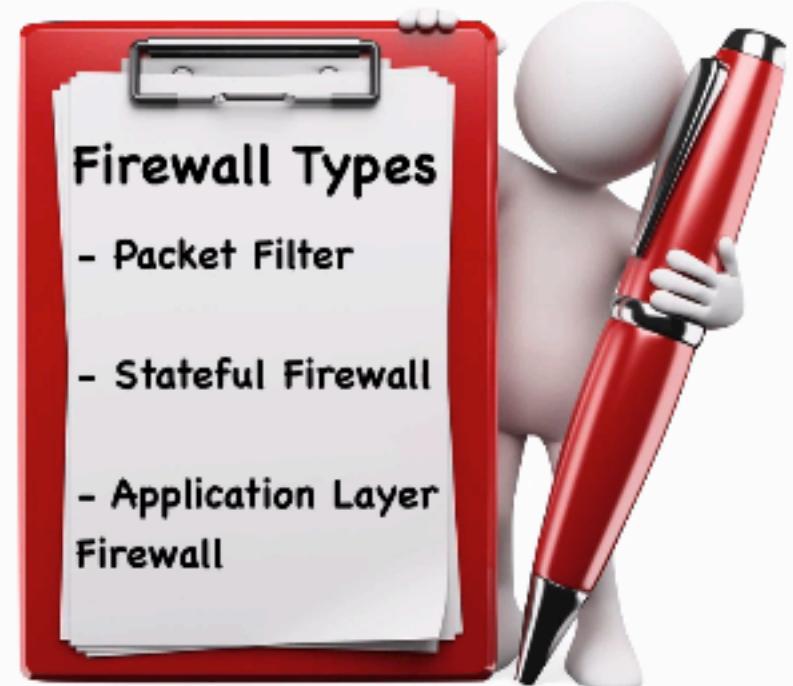
Source	Destination	Action
192.0.2.0 /24	Any - TCP Port 80	Permit
Any	Any	Deny

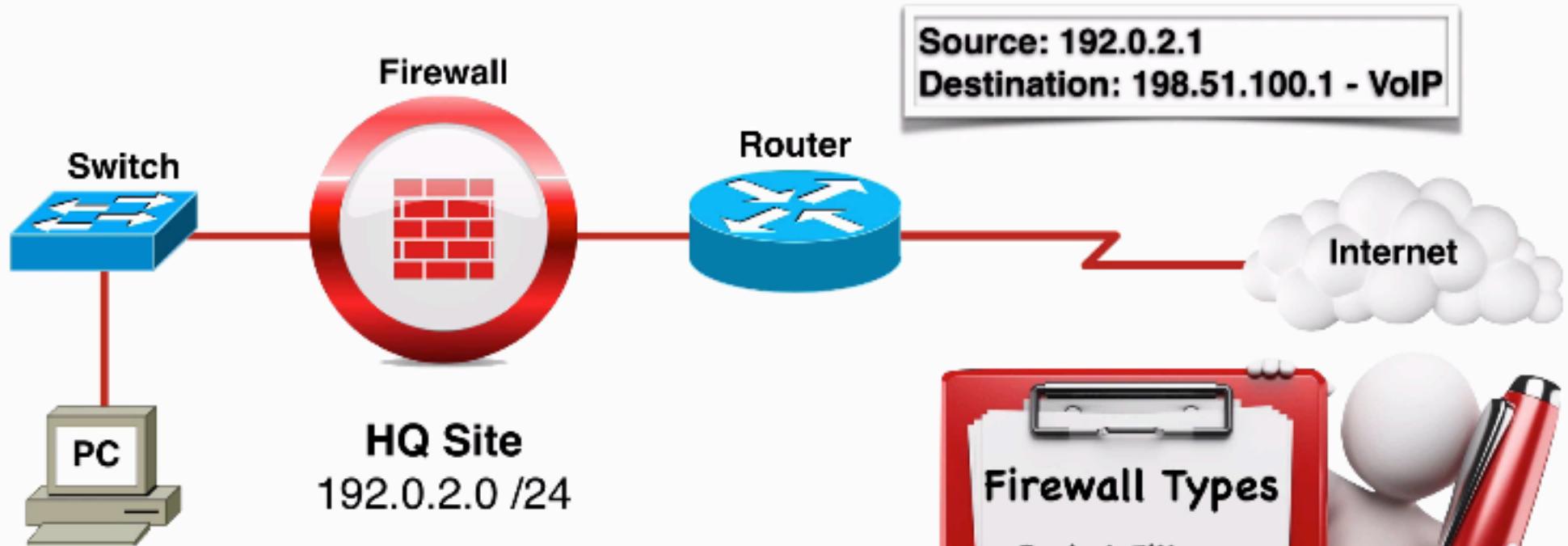




Rules

Source	Destination	Action
192.0.2.0 /24	Any - VoIP	Permit
Any	Any	Deny



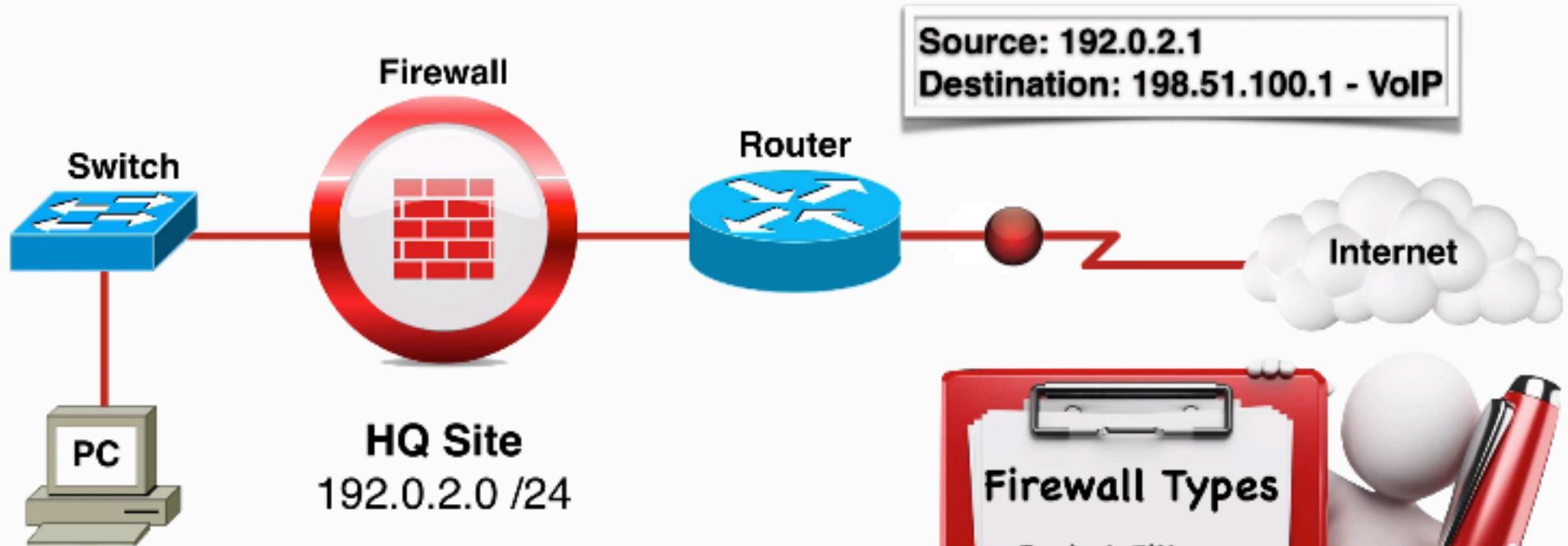


Rules

Source	Destination	Action
192.0.2.0 /24	Any - VoIP	Permit
Any	Any	Deny

**Source: 192.0.2.1
Destination: 198.51.100.1 - VoIP**



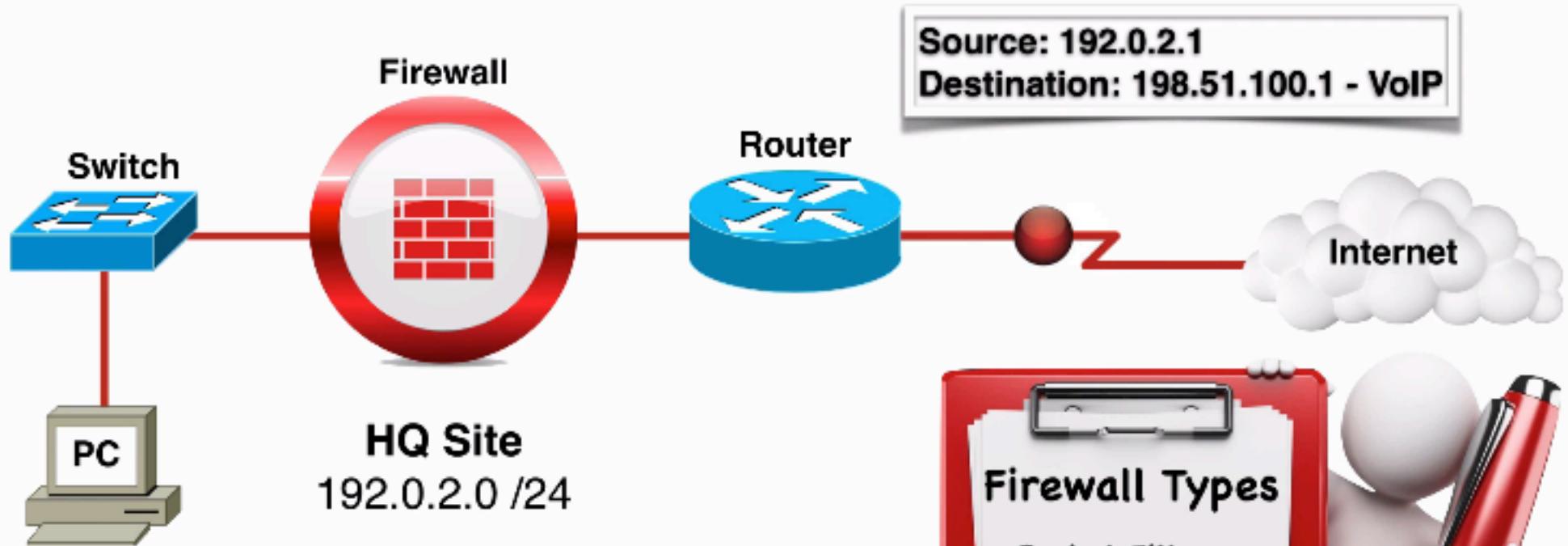


Rules

Source	Destination	Action
192.0.2.0 /24	Any - VoIP	Permit
Any	Any	Deny

Source: 192.0.2.1
Destination: 198.51.100.1 - VoIP



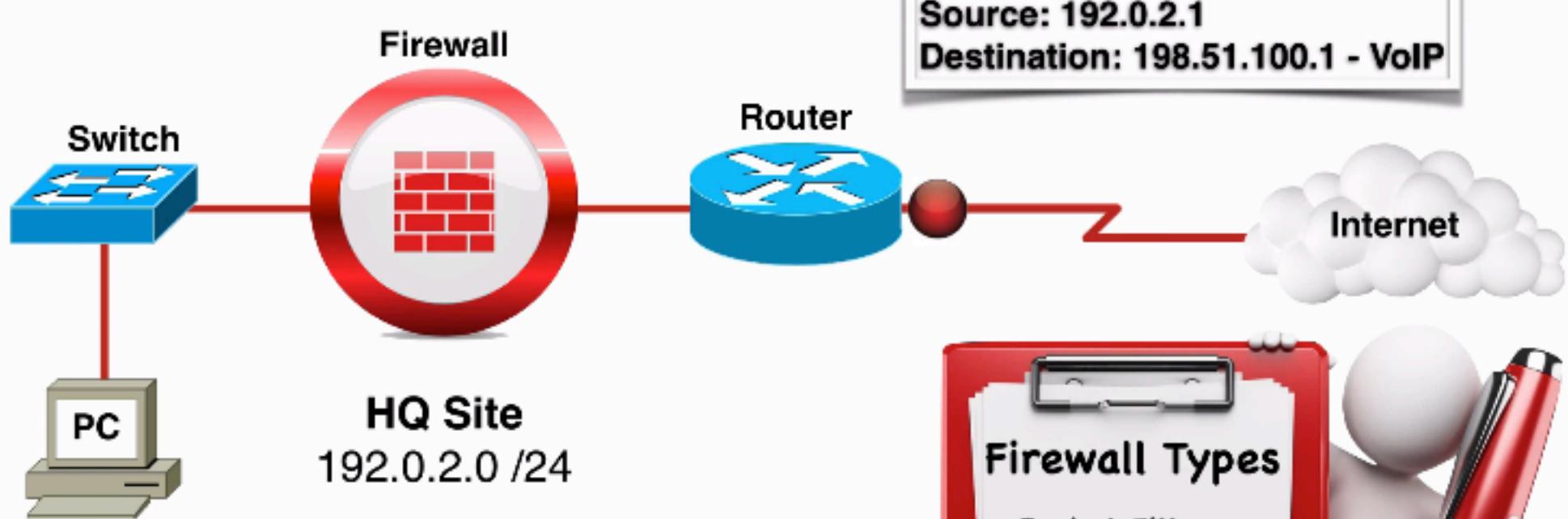


Rules

Source	Destination	Action
192.0.2.0 /24	Any - VoIP	Permit
Any	Any	Deny

Source: 192.0.2.1
Destination: 198.51.100.1 - VoIP



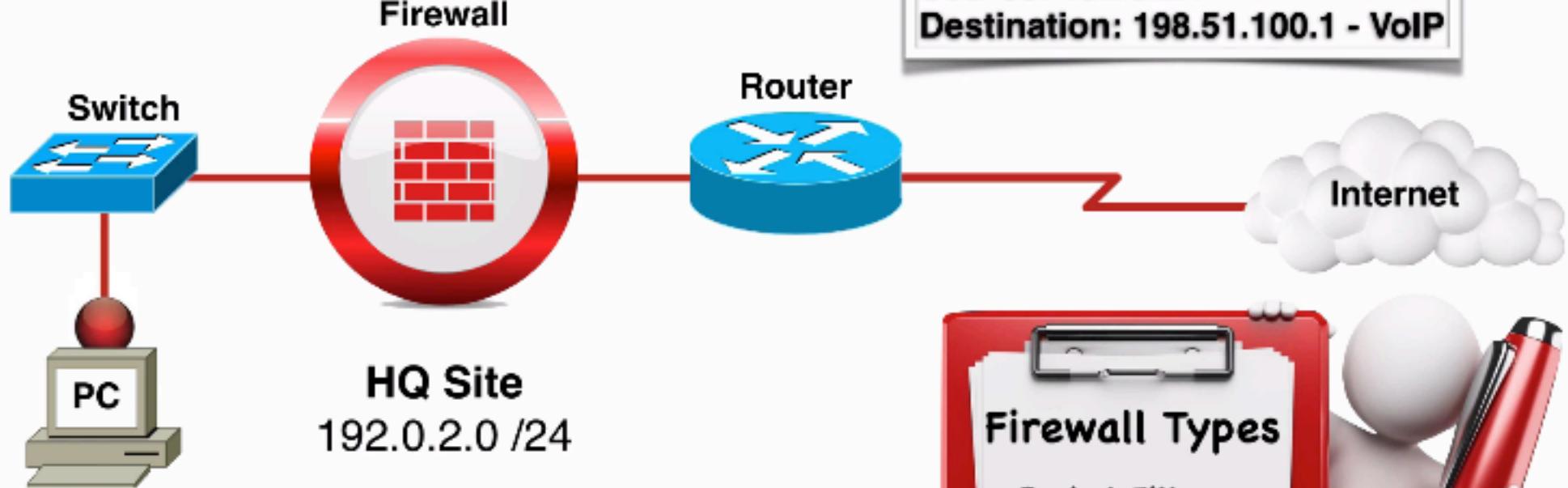


Rules

Source	Destination	Action
192.0.2.0 /24	Any - VoIP	Permit
Any	Any	Deny

**Source: 192.0.2.1
Destination: 198.51.100.1 - VoIP**

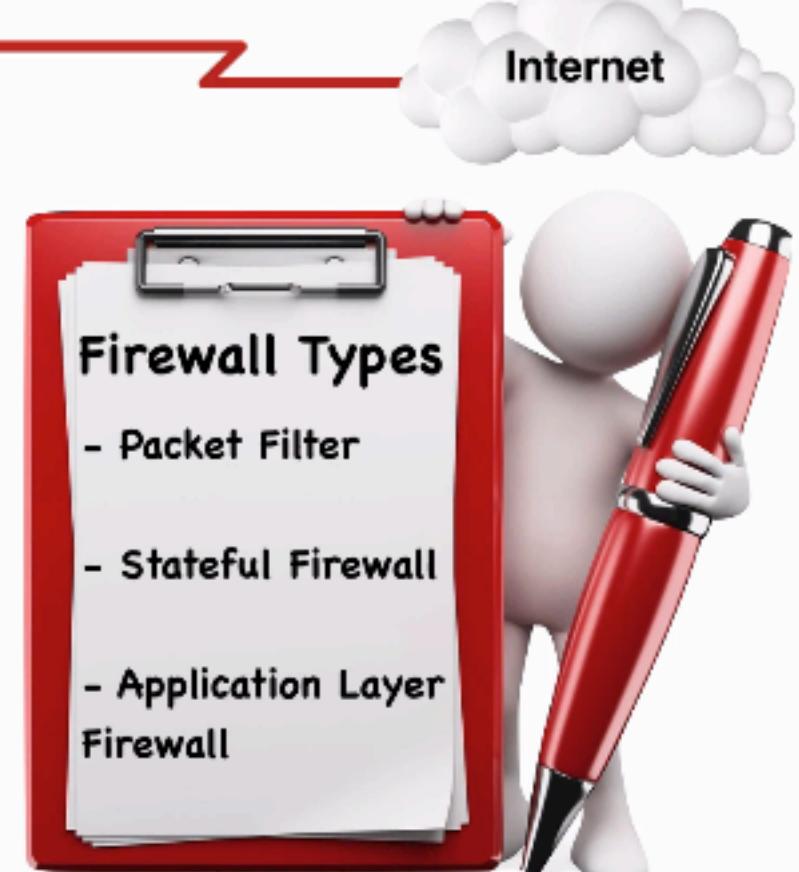


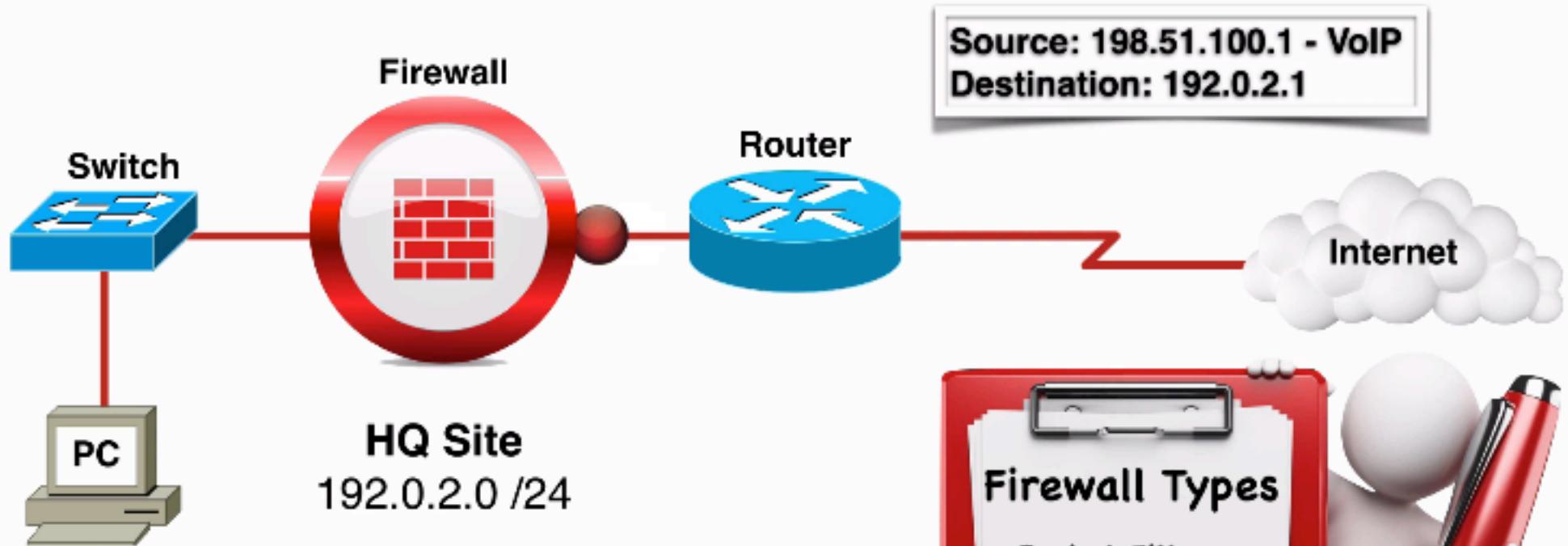


Rules

Source	Destination	Action
192.0.2.0 /24	Any - VoIP	Permit
Any	Any	Deny

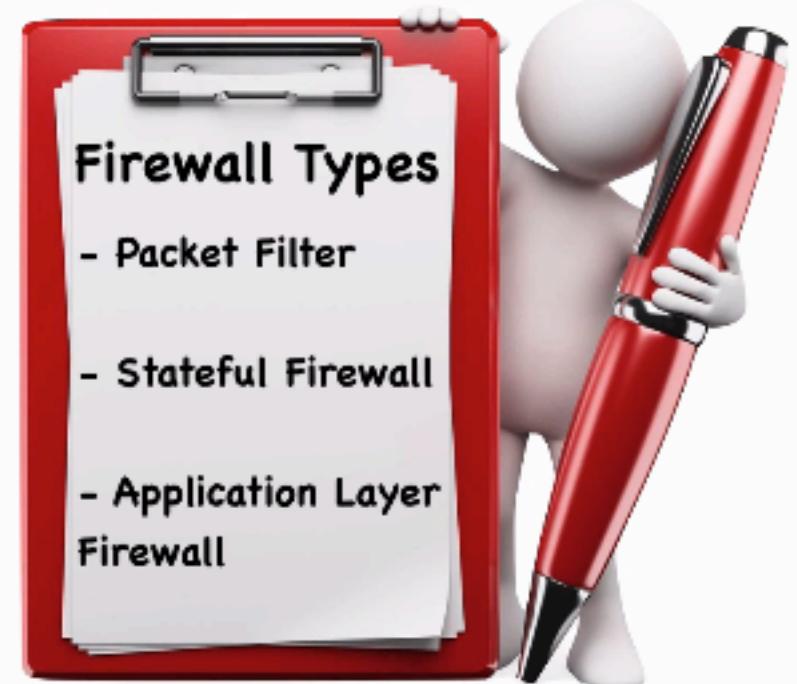
**Source: 192.0.2.1
Destination: 198.51.100.1 - VoIP**





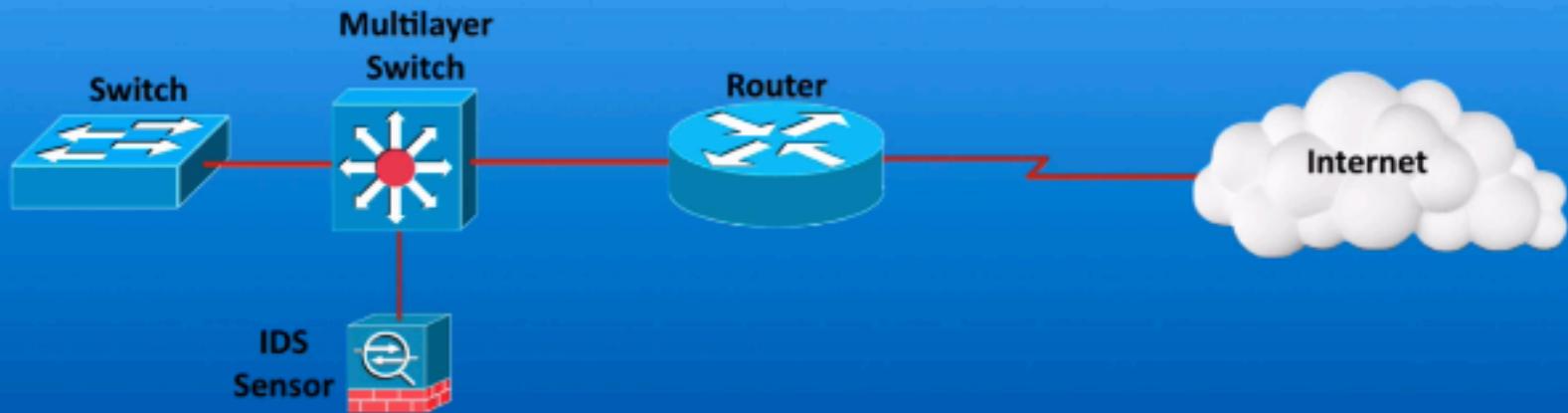
Rules

Source	Destination	Action
192.0.2.0 /24	Any - VoIP	Permit
Any	Any	Deny



Intrusion Detection Devices

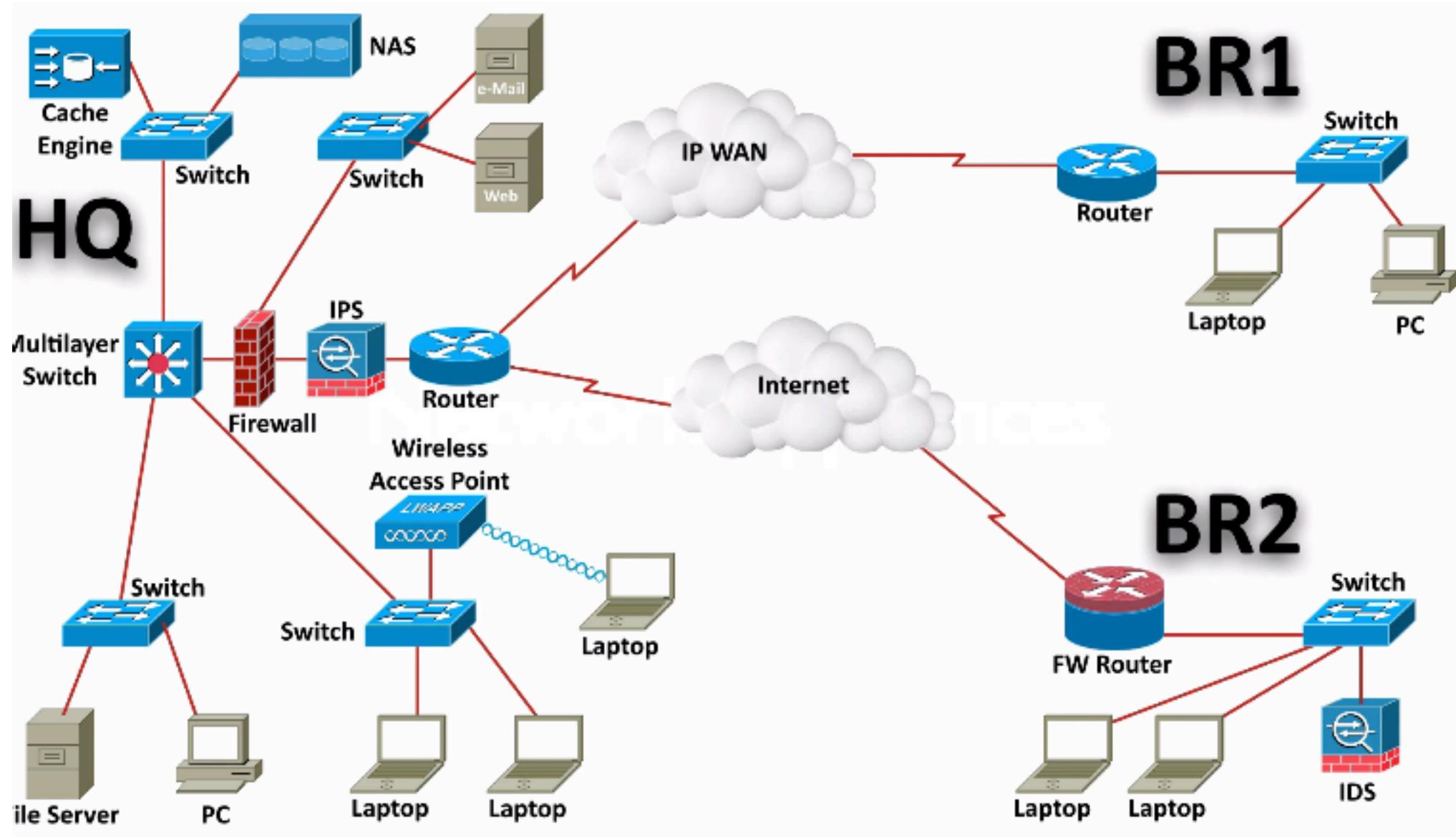
Intrusion Detection System (IDS) Sensor

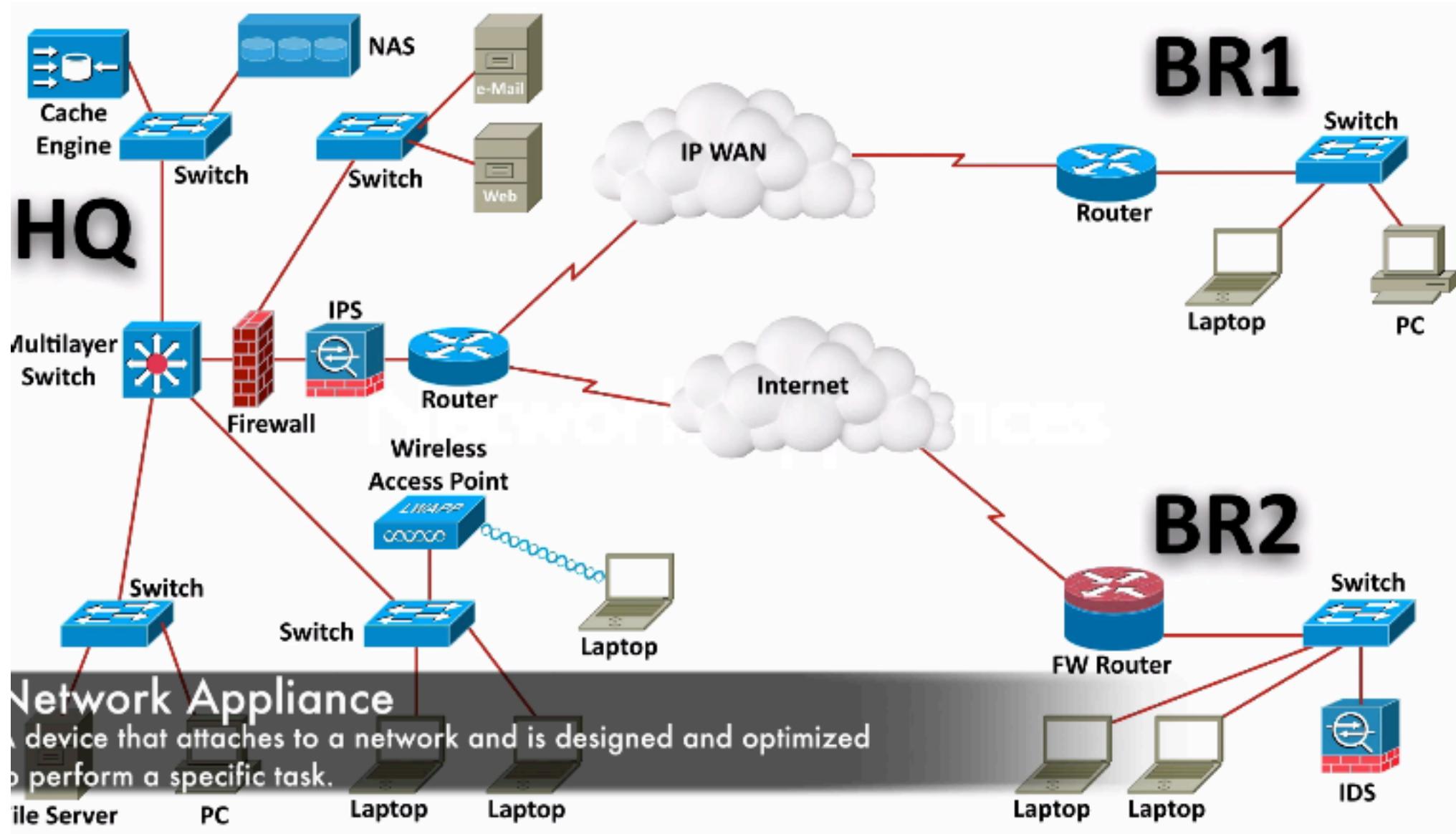


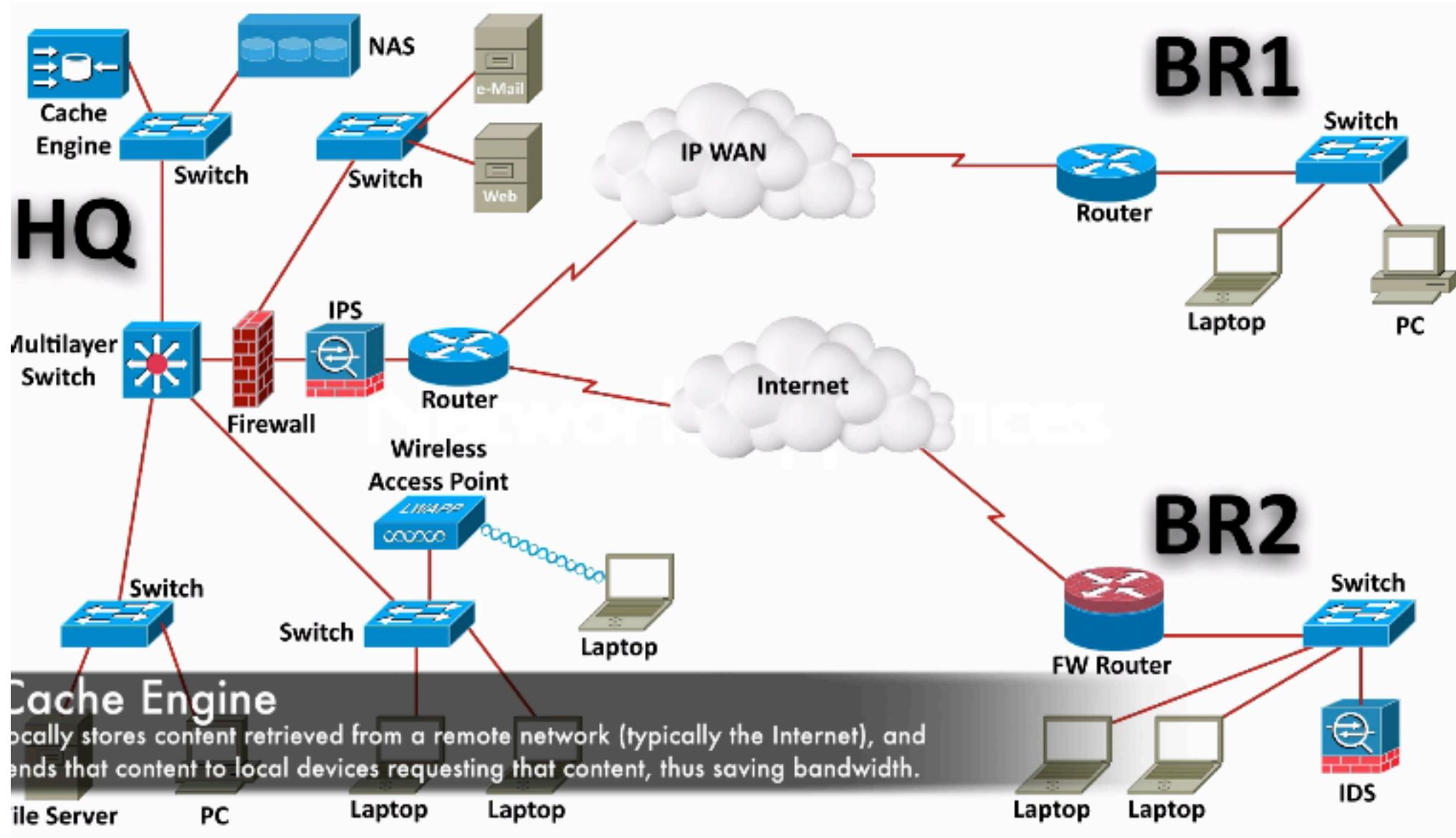
Intrusion Prevention System (IPS) Sensor

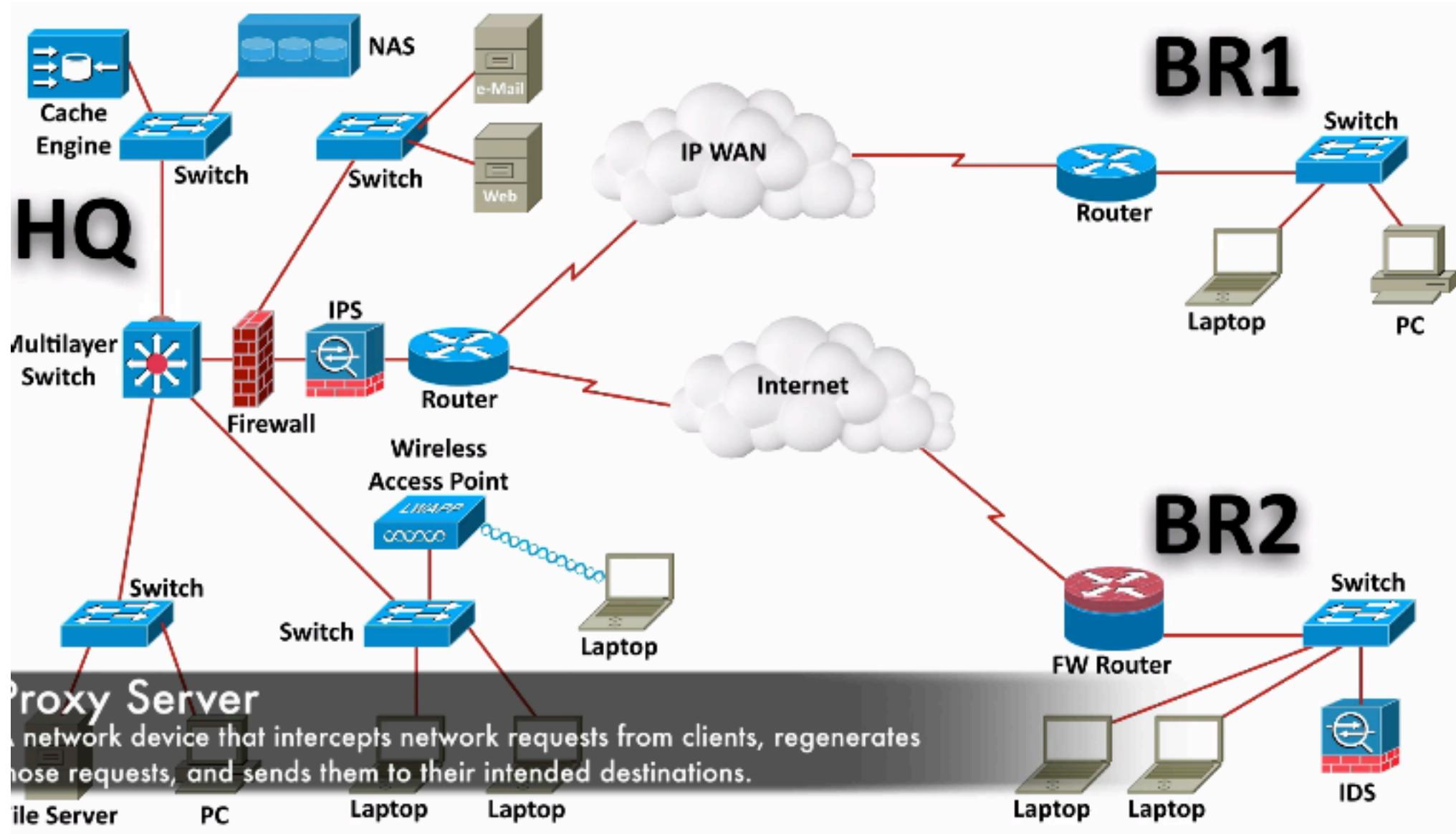


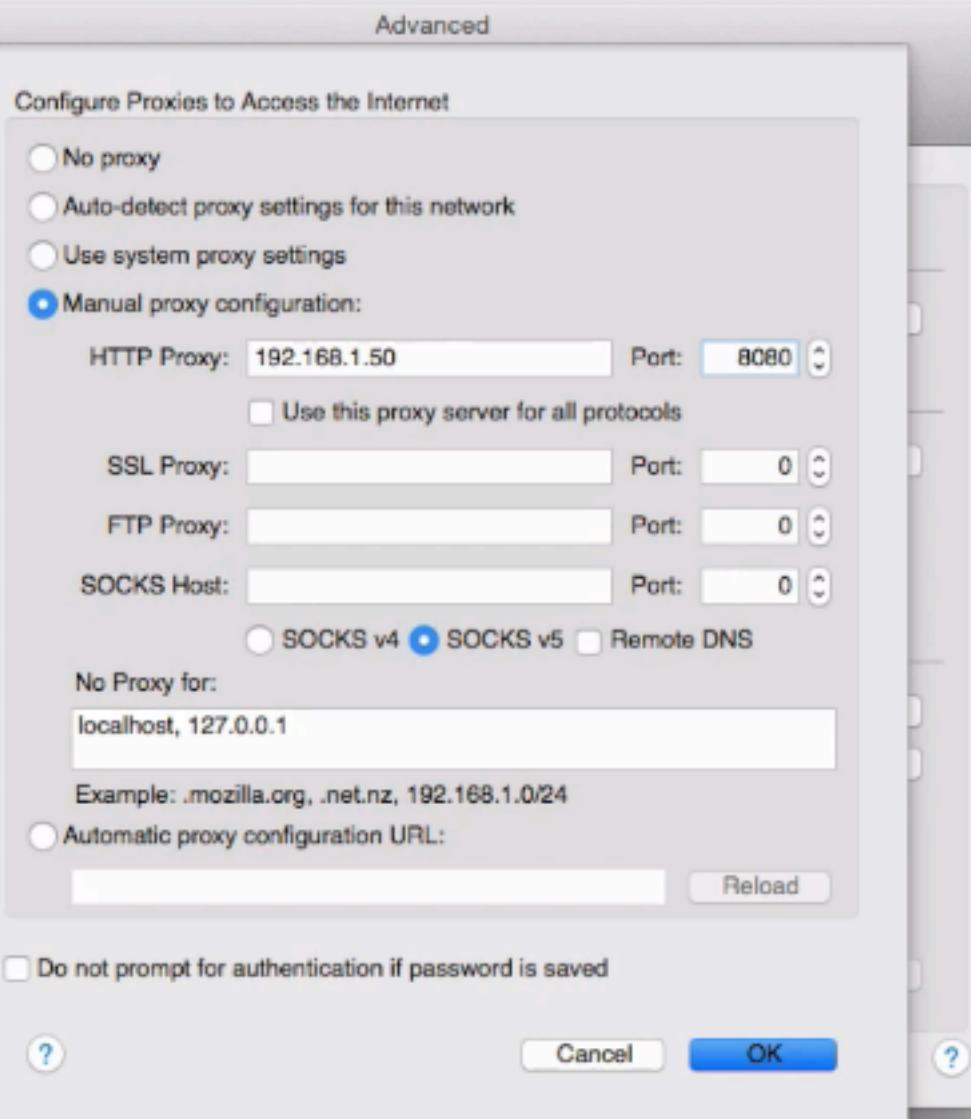
Network Appliances

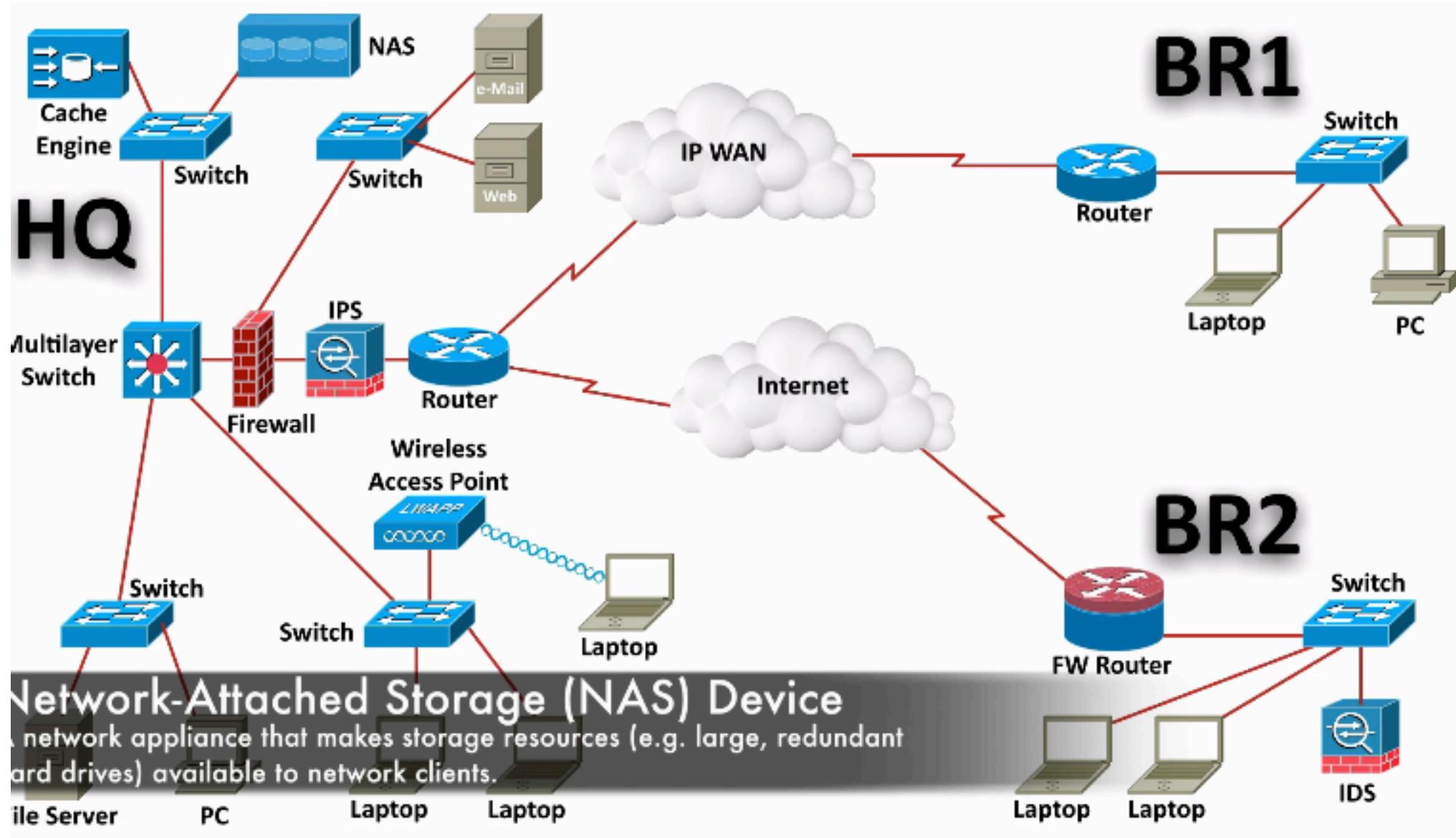


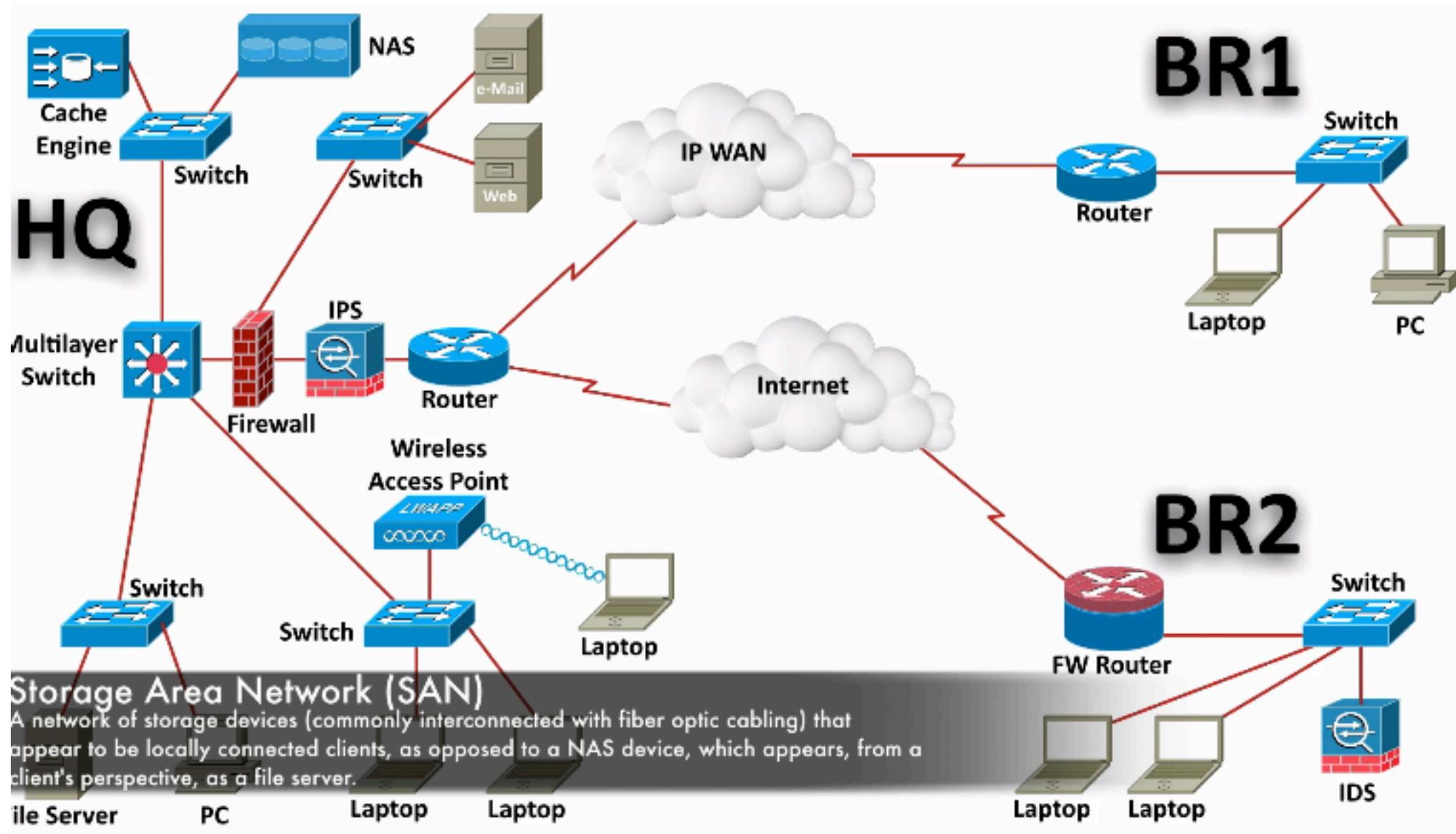












Module 2: Review