Networking Devices

DOMAIN 2.0

MODULE 6

Networking Devices Topics

Introductory Concepts

Repeaters and Hubs

Bridges and Switches

Routers and Multilayer Switches

Security Devices

Modems

Introductory Concepts

Network Interface

A network interface card (NIC) should have at least one address

- Typically a physical (MAC) address
- The MAC address is usually burned into the NIC's firmware
- Can be temporarily changed by the OS (usually for spoofing purposes)

Can also have a logical (IP) address assigned to it

Will be suited to a specific media type and Layer 2 framing

- On a LAN, usually Ethernet or Wi-Fi
- Includes the MTU of that segment

The interface will have a specific speed and duplex

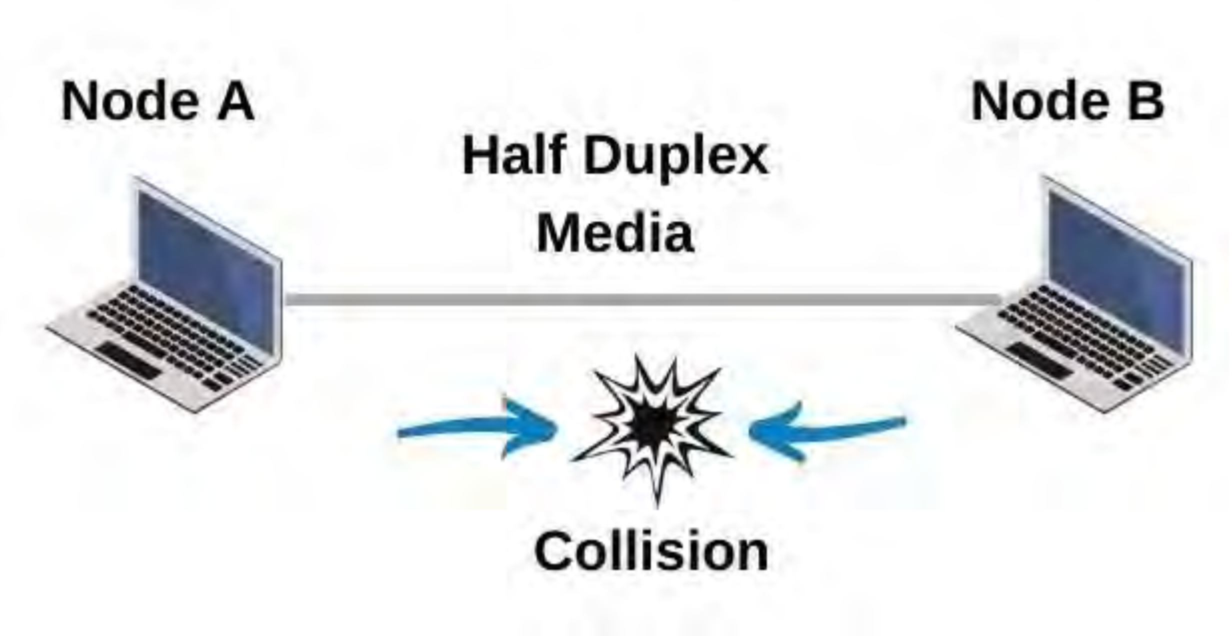
- Might have to be manually configured
- Usually can be auto-negotiated

What is Network Contention?

Multiple nodes try to use the network at the same time

Contention leads to collisions

Contention needs to be managed



CSMA/CD

Carrier Sense Multiple Access with Collision Detection

The LAN access method used in Ethernet networks

When a device wants to gain access to the network, it checks to see if the network is free

- Network is not free, the device waits a random amount of time before retrying
- Network is free and two devices access the line at exactly the same time, their signals collide and both stop and wait a random amount of time before retrying
- When the line is free that last transmission is resent

CSMA/CA

Carrier Sense Multiple Access with Collision Avoidance

Mostly used on Wi-Fi networks today

- Historically used on AppleTalk networks

Wireless Access Point polls each device (round robin) to see if it’s ready to transmit

If there is a collision, CSMA/CA does not deal with recovery, it waits for the line to be free

Network Segment

General term that describes one discrete part of a network where transmissions occur freely in an unmanaged way

- Hub
- Coax bus

Collisions can happen on a segment

The transmission media is usually the same

- Wired
- Wireless

Segments are usually connected together by:

- Bridge
- Switch
- Router

Collision Domain

A network segment where collisions can occur:

- Hub
- Coax bus

A *collision* occurs when two devices send a frame at the same time on the same network segment

If frames collide both devices must send the frames again

Very inefficient on a contention-based network like Ethernet

Switch ports divide the network segment into collision domains

- Each switchport is its own collision domain (if in half-duplex mode)
- Full duplex mode never has collisions (Tx and Rx are on physically separate wires)

Broadcast Domain

A network segment where Layer 2 (ARP) broadcasts are allowed to propagate

Includes all switch ports in a single VLAN

- Even across multiple switches
- Switchports in the same VLAN flood broadcasts out all ports
- Switches will propagate ARPs across trunk links and non-trunking simple uplinks

Routers and VLANs divide the segment into broadcast domains

Maximum Transmission Unit (MTU)

Largest size packet or frame that can be transmitted on a network segment

A router will fragment an IP packet if the MTU of the destination segment is smaller than the MTU of the source segment

TCP uses the MTU to determine the maximum size of each packet in any transmission

Most Layer 2 protocols have a default MTU

- Ethernet is 1500 bytes
- Dialup PPP is 296 bytes
- Most synchronous serial WAN protocols are 1500 bytes

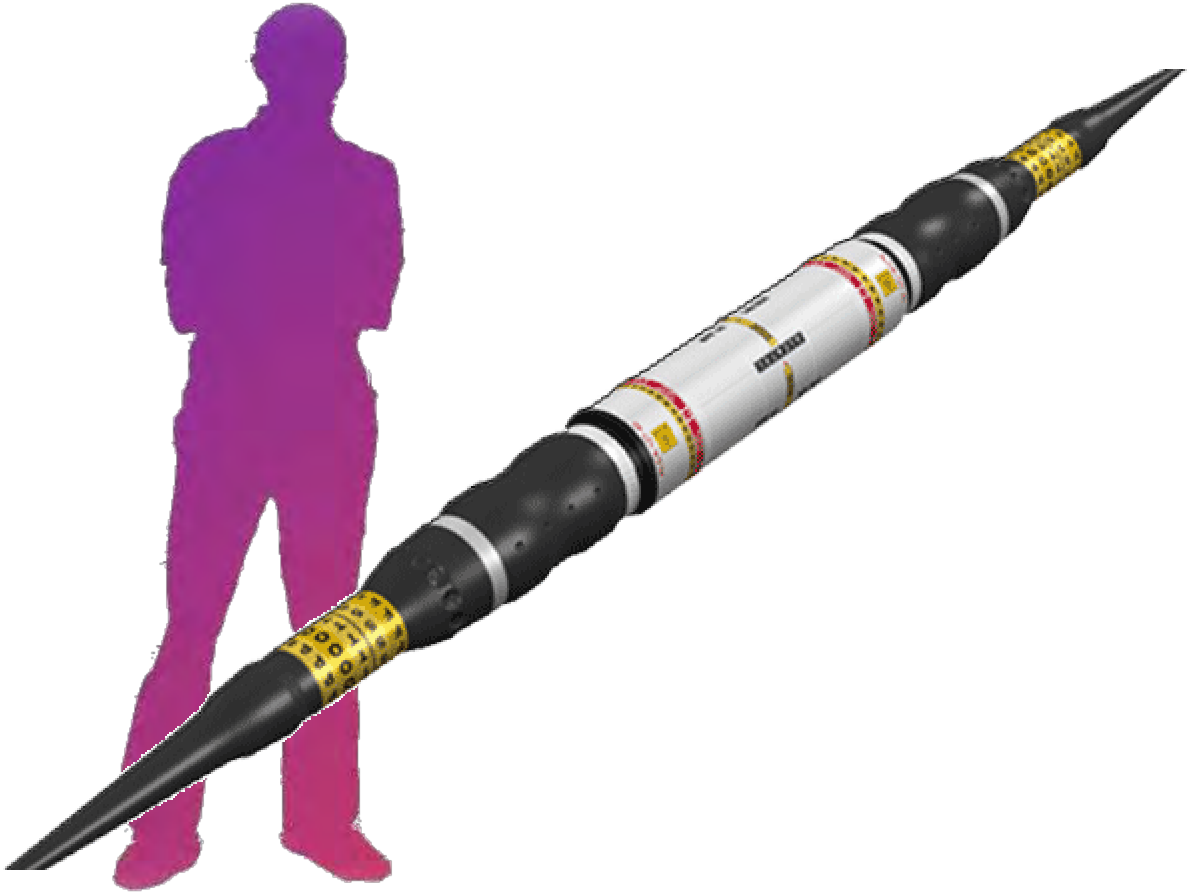
Repeaters and Hubs

Repeater

- Operates at the physical layer of OSI
- Used to extend cable length
- Amplifies or regenerates an incoming signal then retransmits it
- Has only a few ports (typically 2)
- Digital repeaters can reconstruct signals distorted by transmission loss.

LAN Repeater Examples

Submarine Fiber Optic Repeater Example



Hub

Multi-port repeater

Looks like a switch

Can be as simple as a splitter

Frames received on one port are flooded out all other ports

Half-duplex

- Only one node can transmit at a time

All ports belong to a single collision domain and a single broadcast domain

Hub (cont’d)

No processing or error checking is done

Considerably slower and far less efficient than a switch

Passive hub (splitter) – connects ports and passes frames without regenerating the signal

Active hub – regenerates signals

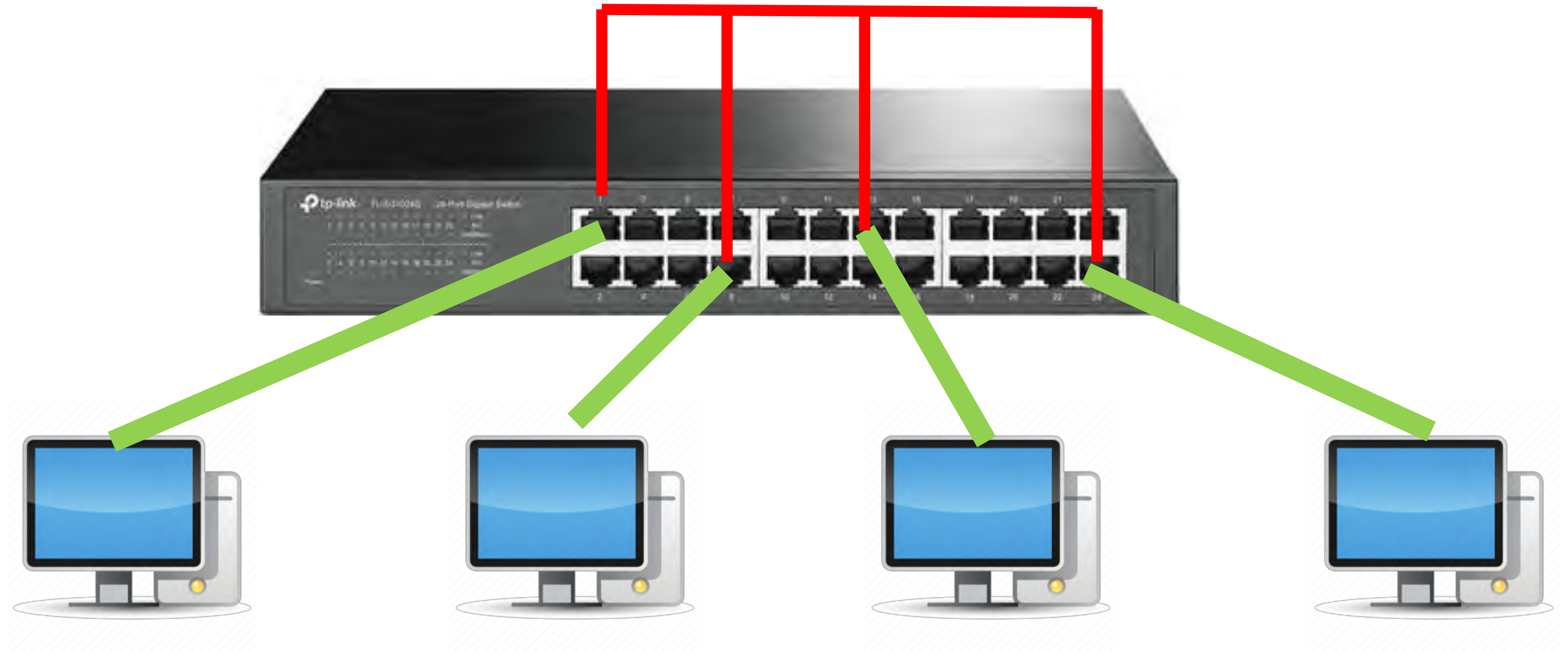
Note: the term “hub” can also refer to a device that connects and powers USB or other devices

Hub Examples

Active Hub

Passive Hub

Hub Traffic Flow Example



Bridges and Switches

Bridge

The term “bridge” can mean several things:

- An old software-based switch
- A device that connects network segments together

A point-to-point wireless extender

Usually L2 protocol is the same, but L1 protocols are different

Wireless access points/routers are also said to “bridge” Wi-Fi and Ethernet together

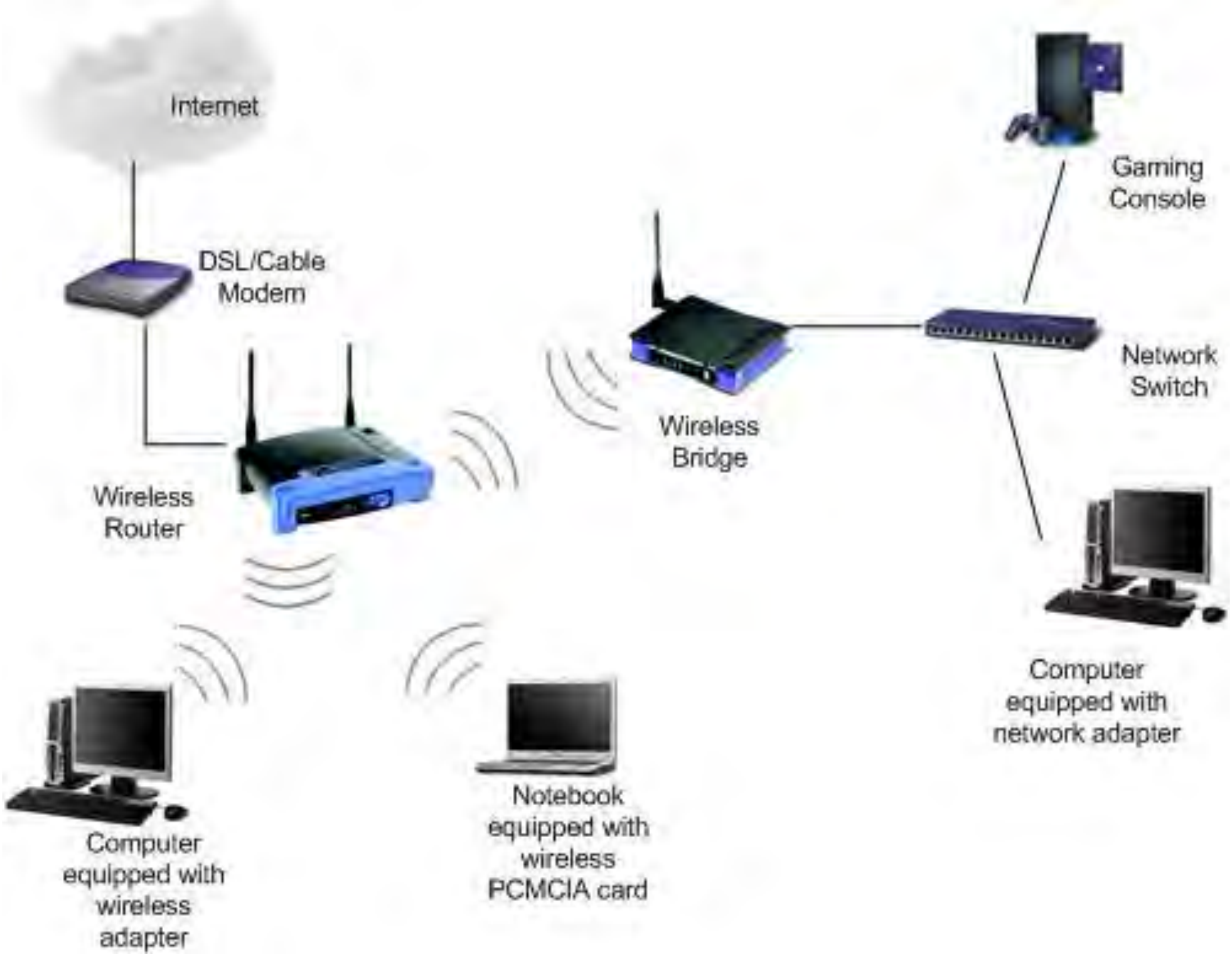
Bridge (traditional)

Originally, the term “bridge” referred to:

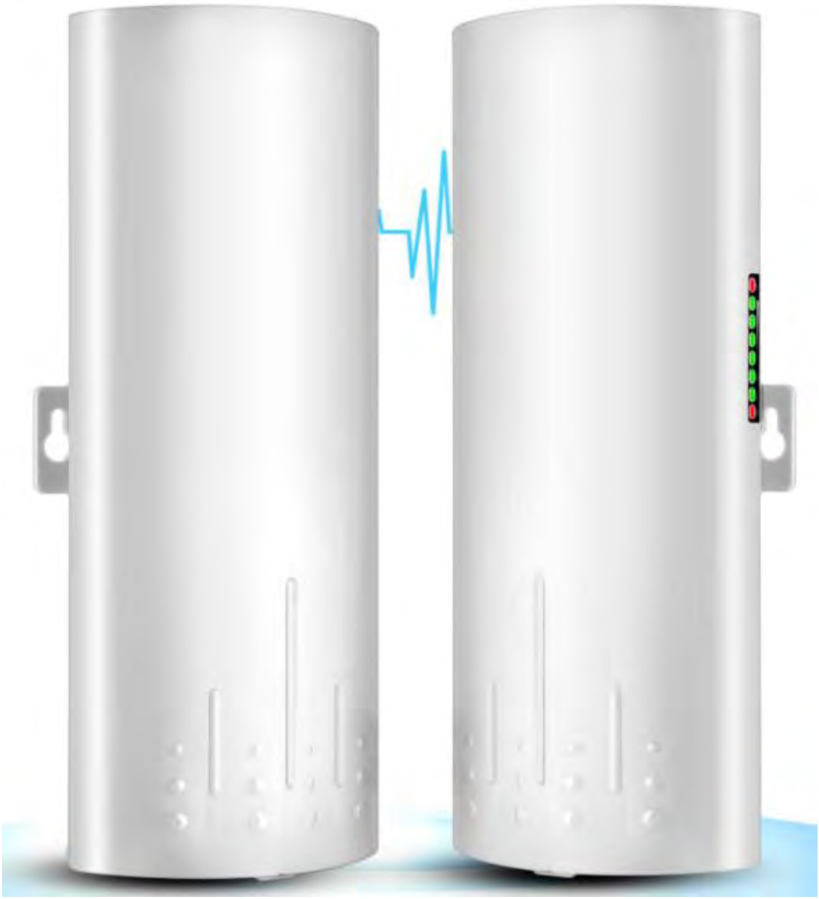
- Layer 2 device
- Makes forwarding decisions based on Layer 2 (MAC) addresses
- Predecessor to the common Layer 2 switch
- Typically has few ports
- Software-based logic
- Can connect different media types

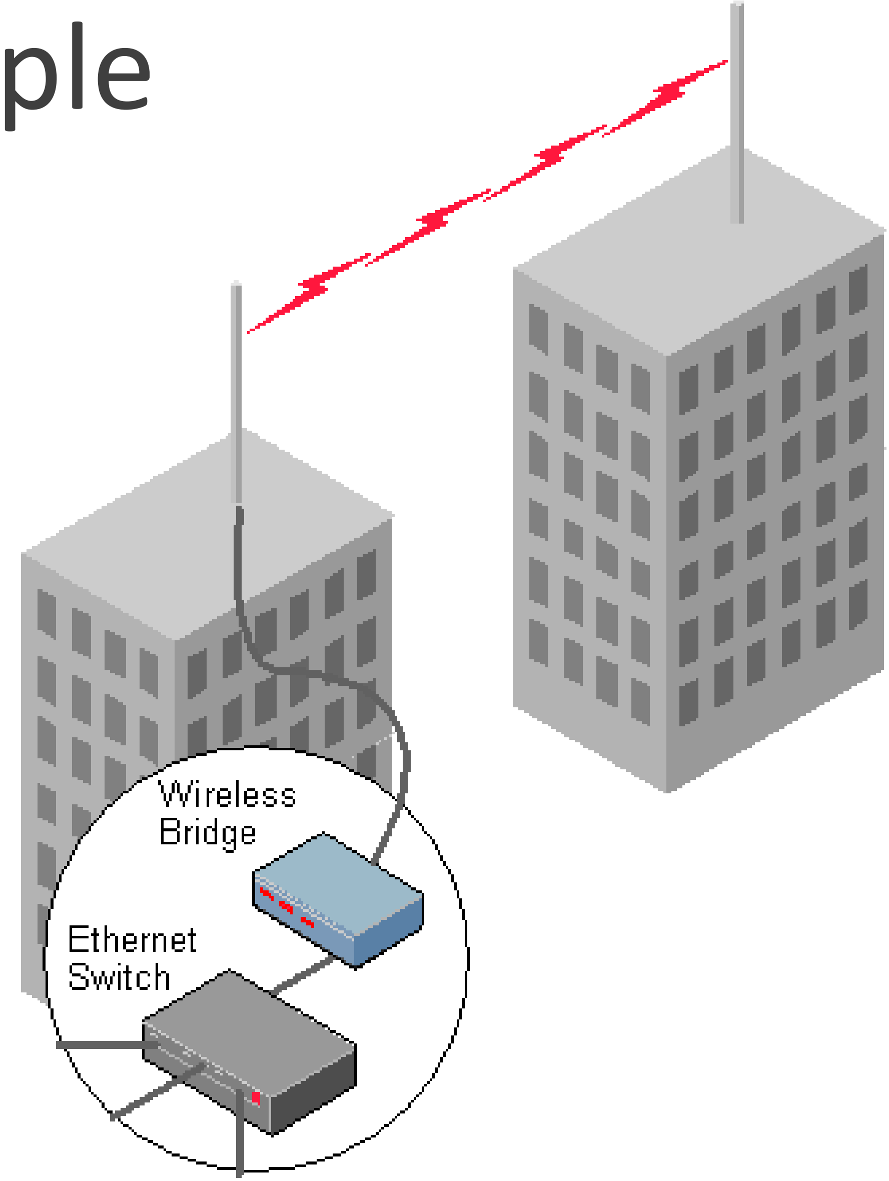
Traditional Bridge Examples

Home Wireless Bridge Example


Internet
DSL/Cable Modem
Wireless Router
Wireless Bridge
Gaming Console
Network Switch
Computer equipped with network adapter
Computer equipped with wireless adapter
Notebook equipped with wireless PCMCIA card

Site Wireless Bridge Example





Switch

Connects individual devices on a LAN

Hardware device that makes forwarding decisions based on Layer 2 addresses (MAC addresses)

- Uses application-specific integrated circuit (ASIC) chips to make forwarding decisions in hardware
- Considered to have "high port density"

The switch learns what MAC addresses are connected to it and builds a temporary table

Only forwards a frame out the necessary port

- A 48-port switch could have 24 conversations happening at once

Switch (cont'd)

Will flood the frame out all ports (except the port it came in on) if it receives:

- Unknown unicast (not in the MAC table)
- Broadcast
- Multicast

Micro-segments a basic segment

- Each switch port becomes its own segment and collision domain
- No collisions if the port is in full-duplex mode
  - And only one device on that port

Ports negotiate or can be configured for speed, duplex

- Ports can be half- or full-duplex

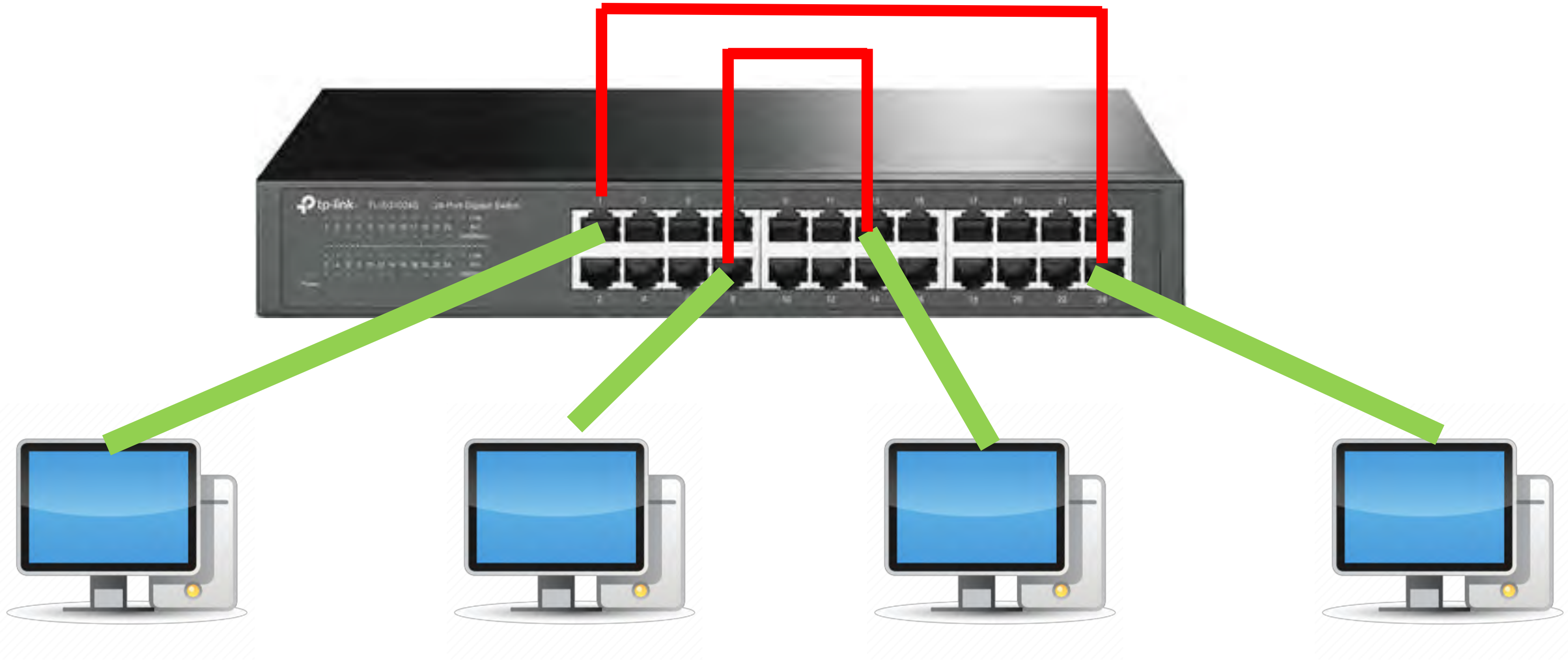
Switch Examples

Stacked Switches

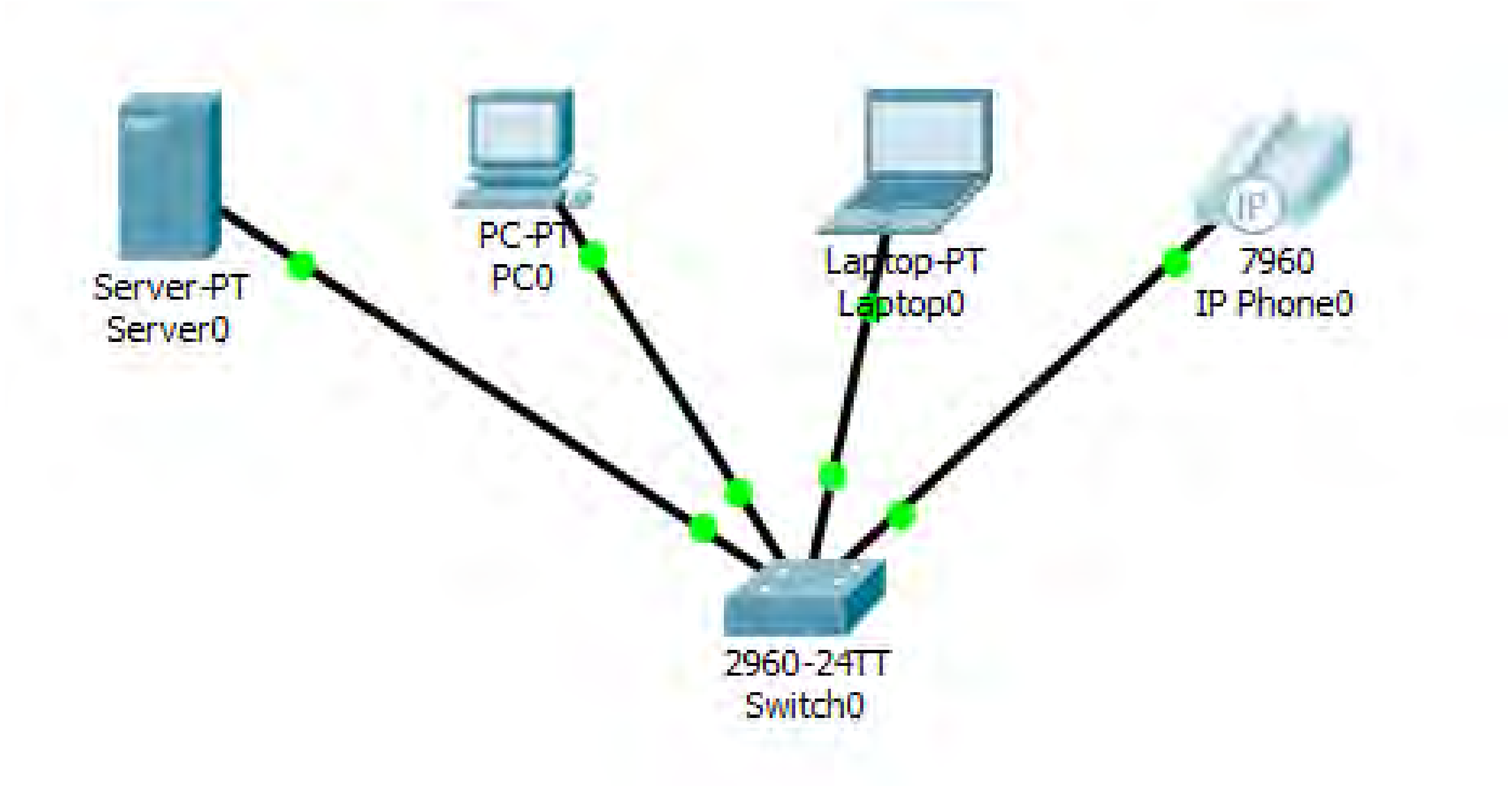
Switches connected together in back to create a single logical switch

If backplane of one switch fails, other members will take over its ports and service its connected clients

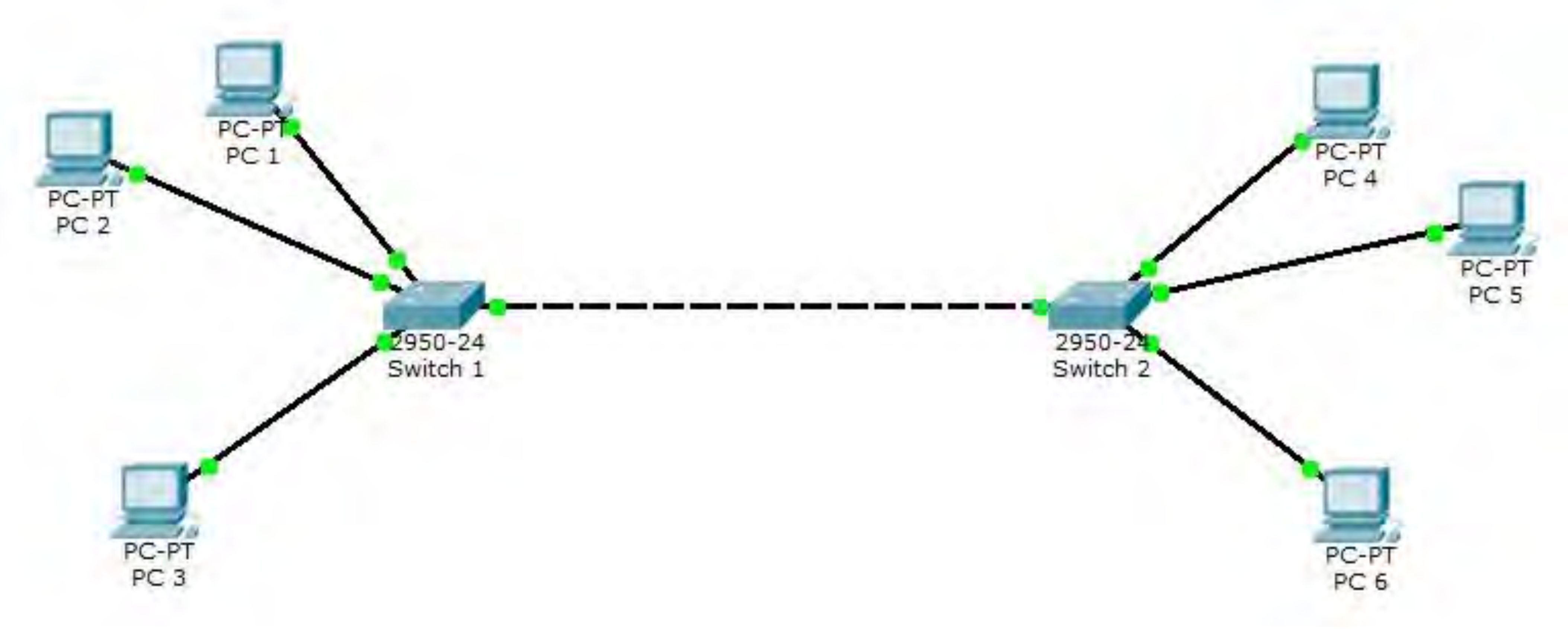
Switch Traffic Flow Example



Switch Connecting Multiple Devices Example



Two Switches Extending a Network Example



Power over Ethernet PoE and PoE+

Describes any of several standard or ad-hoc systems which pass electric power along with data on twisted pair Ethernet cabling

PoE can be built into a switchport or provided via a separate device

The main difference between the 802.3af (PoE) and 802.3at (PoE+) standards is the maximum amount of power they provide over Cat5 cabling

- 802.3af max = 15.4 watts
- 802.3at (PoE+) = 25.5 watts

Routers and Multilayer Switches

Router

Connects entire networks (LAN and WAN)

Forwards packets based on destination Layer 3 (IP) addresses

- Performs a route lookup
- "Switches" packet between interfaces
- Decisions are software-based

Reads its route table to determine which interface to send the packet out of

- If there is no entry in the route table, the router must send the packet to a default route or drop it
- Does not by default examine the source IP address

Interfaces can have different L1 connections and L2 protocols

- Generally 10x slower than switchports

Referred to as the "default gateway" for end clients

Router (cont’d)

Provides packets with new/updated L2 headers for the next segment

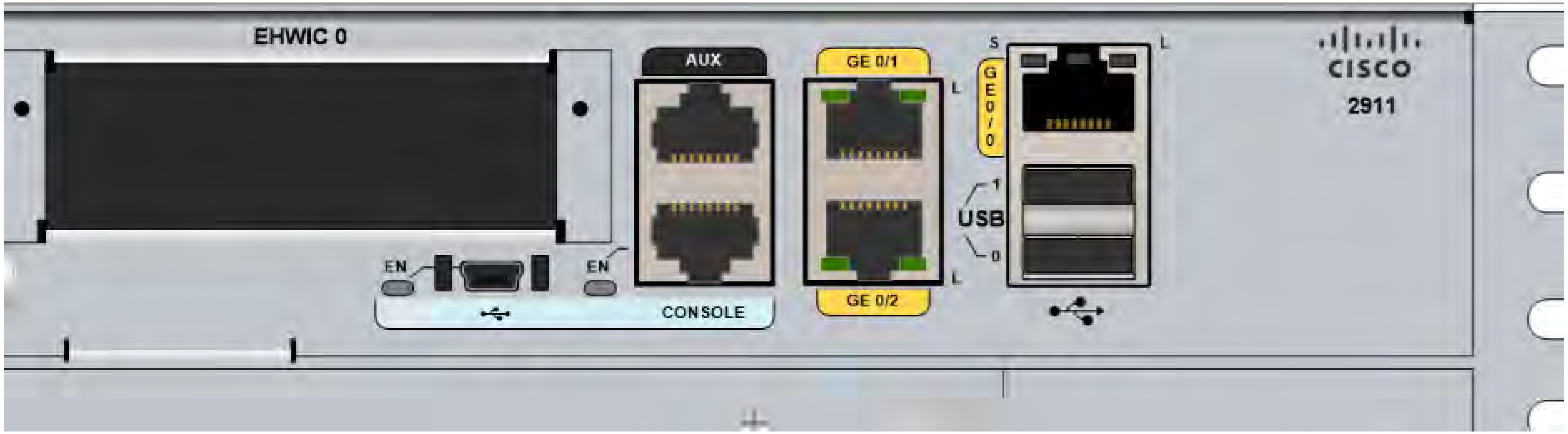
- If the L2 protocol is different between segments, the router strips off the old header and applies a new header

If the two segments use the same L2 protocol, the router simply does an inline rewrite of the source and destination addresses in the existing header

Blocks broadcasts and multicasts by default

- Each interface defines a broadcast domain
- Can be configured to forward multicast traffic

Router Examples



Small Office Home Office (SOHO) Router

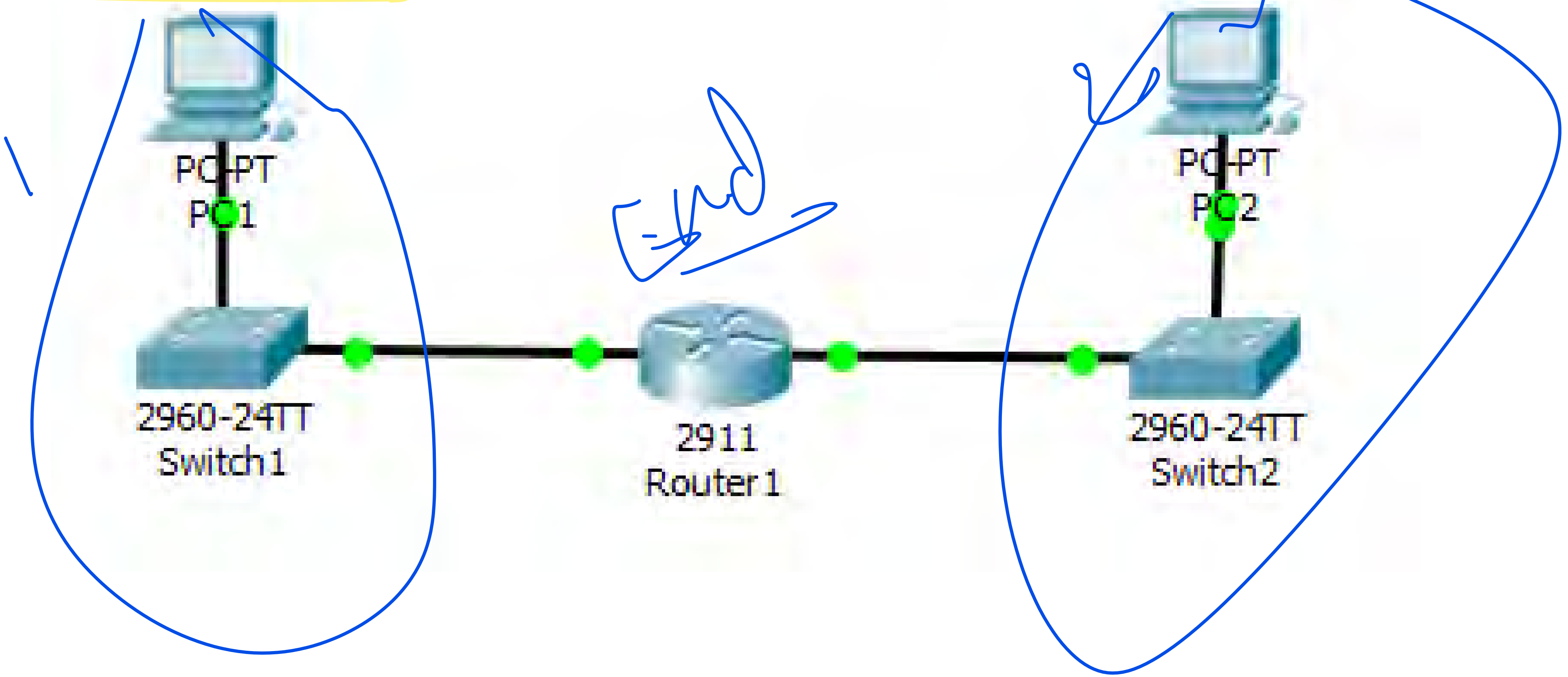
- Router with built-in switch ports and (usually) wireless access point
- Usually sufficient for just a few users/devices
- Usually has simple built-in firewall and management capabilities
- Connect the Internet (outside) network to its WAN/Internet port
- Connect internal clients to its switch ports or wireless transceiver

Basic Router and Switch Example

whenu see tehj router its means its the end of a brodacst

this isa A nrodacst doamin

this isa A nrodacst doamin



Layer 3 Switch

An Ethernet switch with routing capabilities

- Can switch or route

Looks like a L2 switch

Aka “multilayer switch” – works at Layer 2 and up

Typically has 24 or 48 ports, plus a few higher speed uplink ports

Multiple switches can be “stacked”

Has fiber optic or RJ-45 Ethernet ports (whatever the switch has)

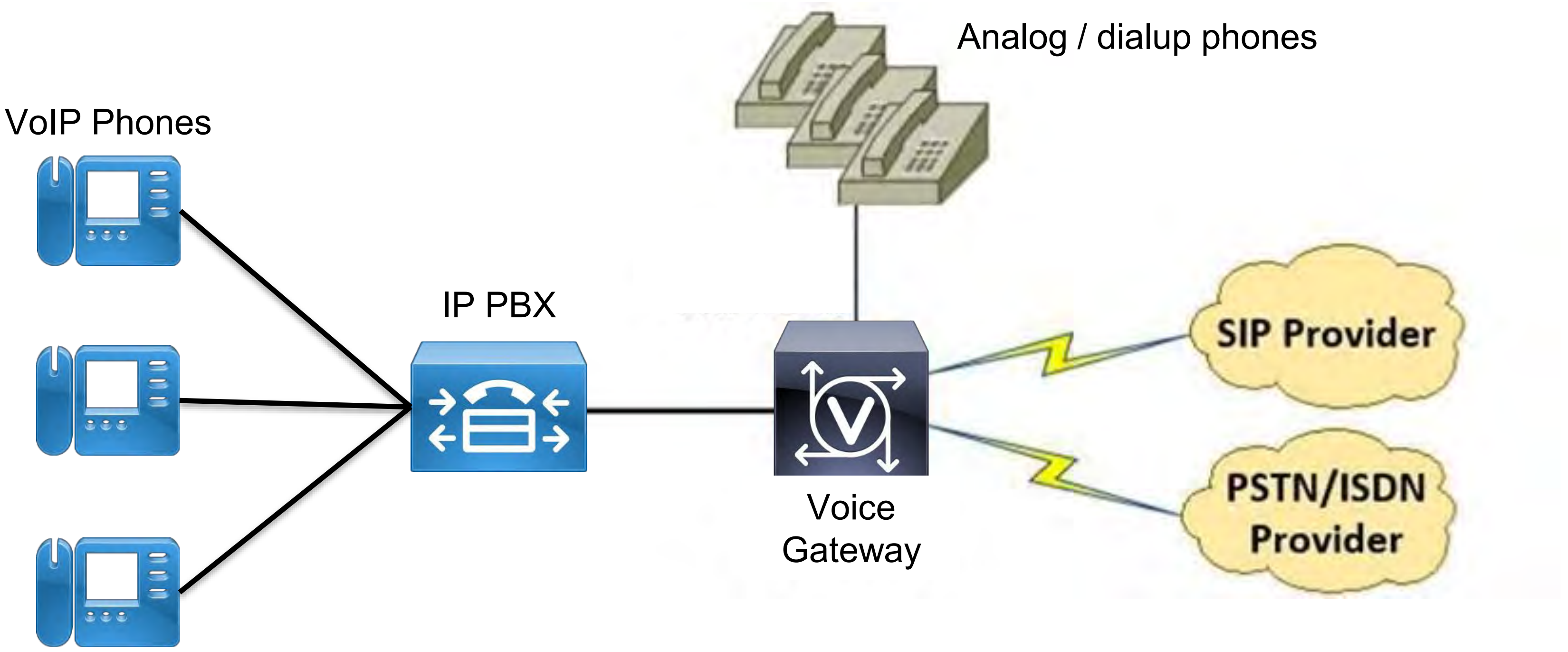
- Will not have serial, ISDN, or other ports found in a router

Best for routing VLANs

- Routing interfaces are virtual VLAN interfaces, not physical
- You assign physical ports to the VLAN that a VLAN interface services

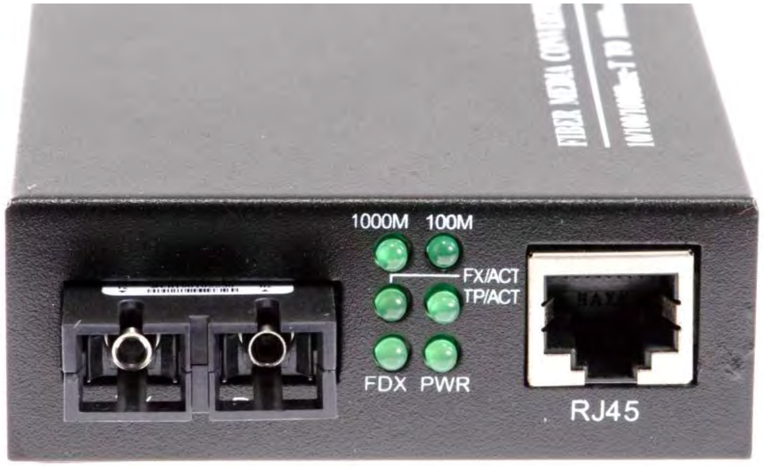
Voice Gateway

Connects the enterprise VoIP network to the telecommunications provider
Can use a number of different connectivity methods including the PSTN, ISDN and SIP



Media Converter

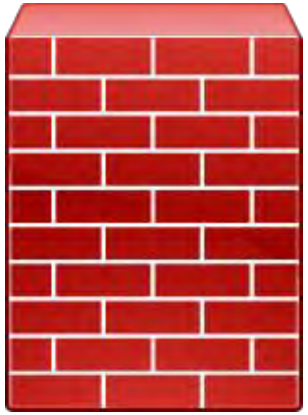
- Connects two cabling types
  - Typically fiber optic to twisted pair
  - Can also be multimode fiber to single mode fiber
  - Coax to twisted pair
- Often used when the router, firewall or voice gateway cannot accommodate the provider's incoming cable type



Security Devices

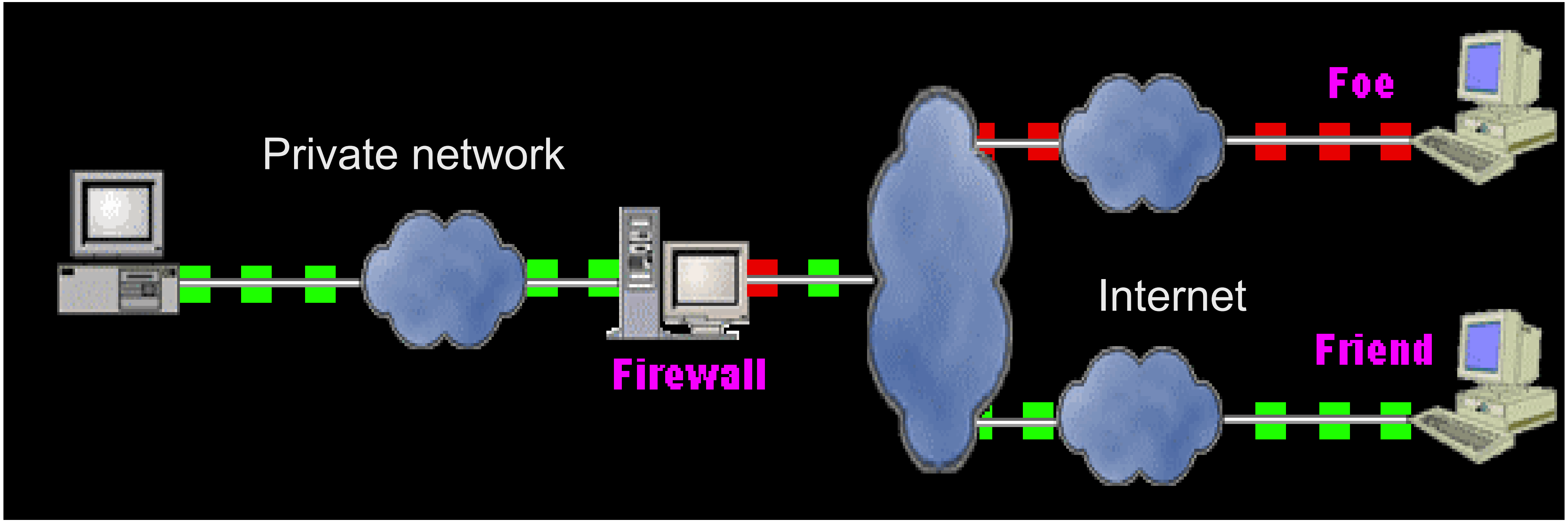
Firewall

- Software or hardware device (appliance) that separates the “untrusted” network from the “trusted” network
- Enforces rules to filter out unwanted traffic and protect the internal network
- Often provides NAT services
- Can work at Layers 2 – 7
- Might have a “subscription” from the vendor to download malware signatures for deep packet inspection



Firewall Example

Protects “trusted” private network from “untrusted” Internet



Controls both inbound and outbound traffic based on rules set by administrator

Demilitarized Zone (DMZ)

An untrusted network between two firewalls

Internet-facing hosts are placed here

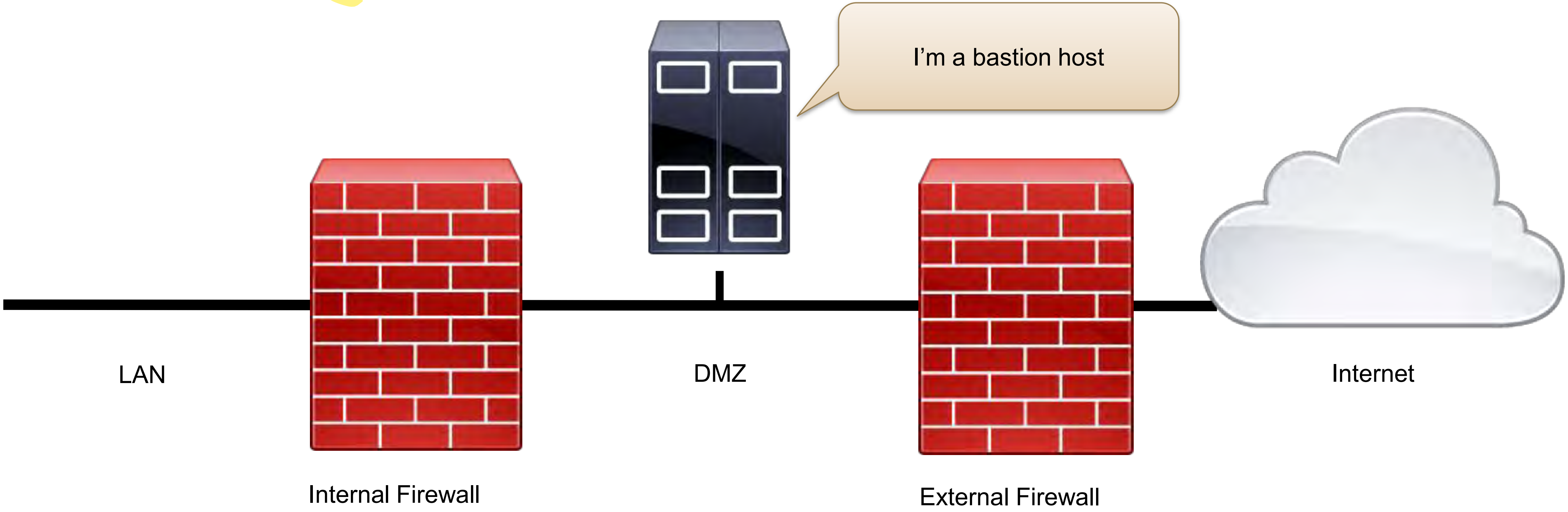
Typically used to isolate and (somewhat) protect public servers such as:

- DNS
- Web server
- MX (email relay)
- Spam and web traffic filtering appliances

Typical DMZ

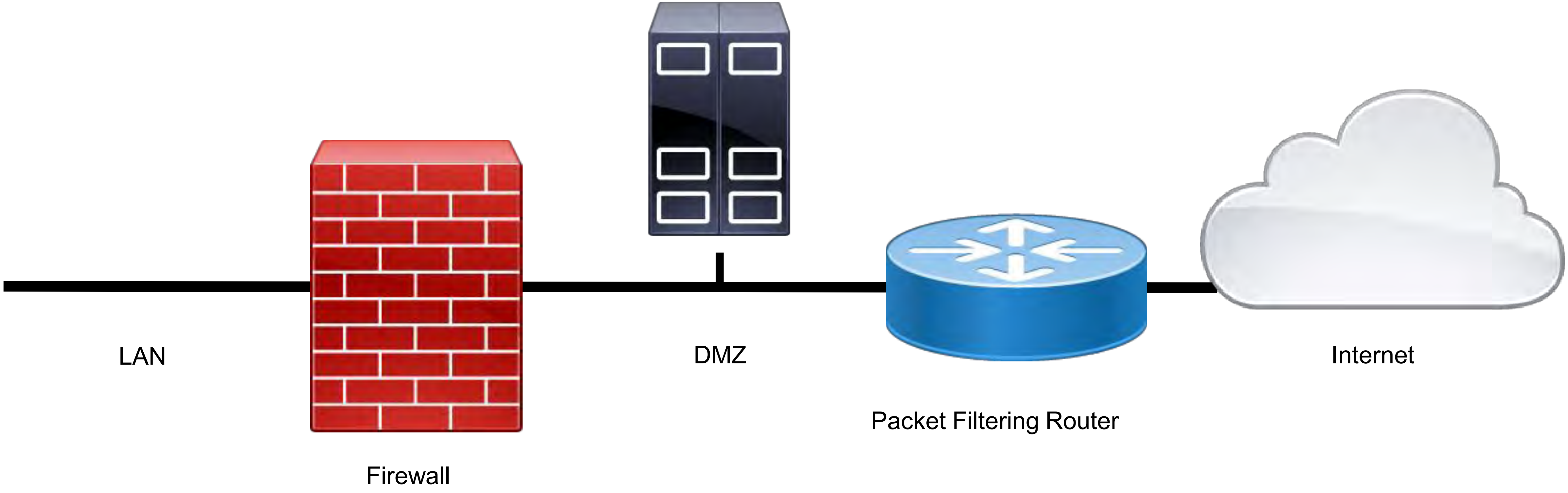
AKA “Screened Subnet”

IP addresses in DMZ can be public or private



“Dirty” DMZ

External “firewall” is a packet filtering router

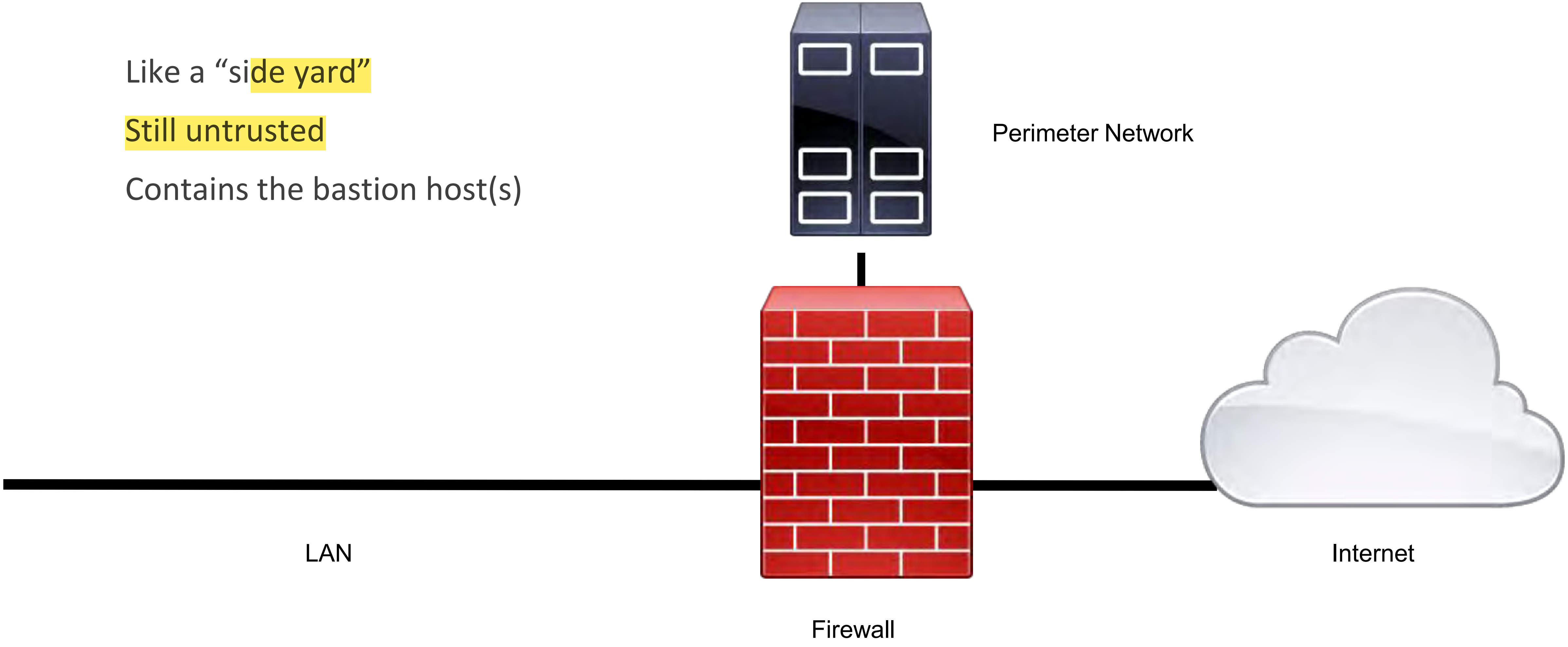


Perimeter Network

Like a “side yard”

Still untrusted

Contains the bastion host(s)



Access Control List

A set of rules used to control traffic in and out of a firewall, router, or multilayer switch

Each packet is compared to the rules in the ACL and processed accordingly

Rules can include:

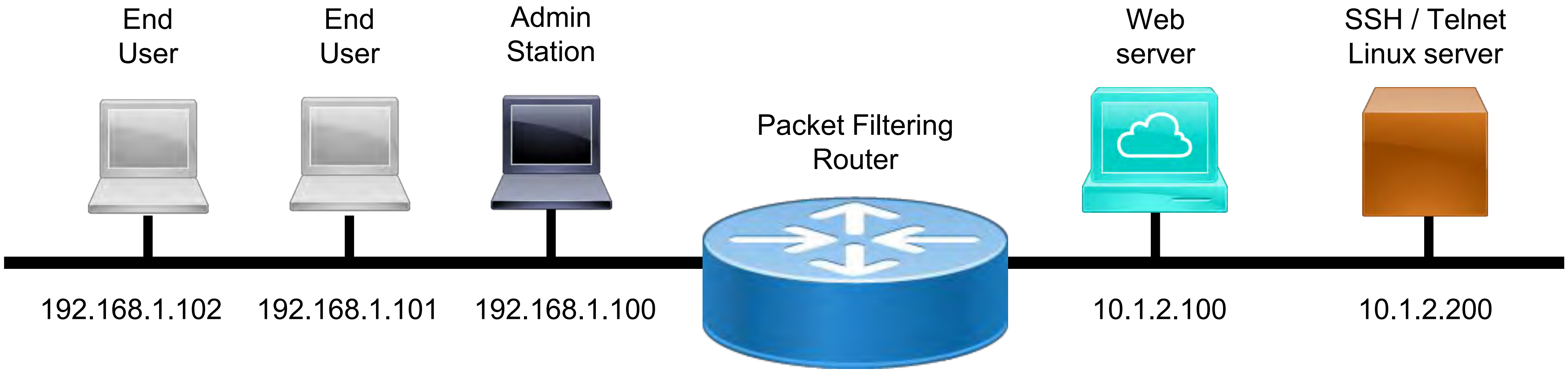
- Protocol
- Source IP address
- Destination IP address
- Source port
- Destination port

ACL actions are usually permit or deny

Most ACLs have an implicit “deny” at the end

- If you configure deny rules, you need to have a “permit all” rule at the end to allow all other traffic

ACL Example



source

destination

destination port/protocol

```
access-list 101 deny   tcp any                       any             eq 23
access-list 101 permit tcp 192.168.1.0 0.0.0.255 host 10.1.2.100 eq http
access-list 101 permit tcp host 192.168.1.100    host 10.1.2.200 eq ssh
access-list 101 permit ip  any                       any
```

Port Forwarding

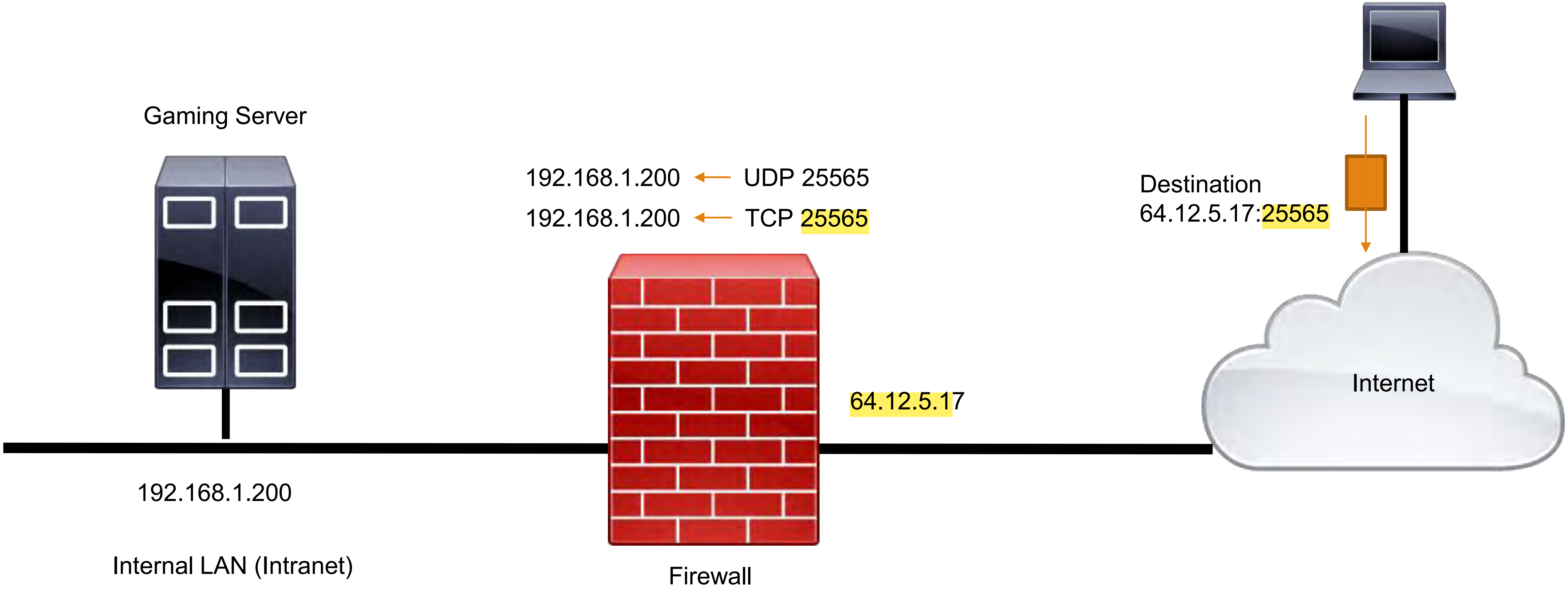
Aka “publishing”

A technique that allows external devices to access computers on a private networks

Uses an IP address plus port number to route network requests to specific internal devices

Typically configured on a firewall

Port Forwarding Example



Proxy Server

A service that fetches web content on behalf of clients

Client is not allowed to make a connection out on the Internet

The puts the client session “on hold”

- Creates a new session out to the Internet to fetch the requested content

Can run on a dedicated server on the internal network or the firewall

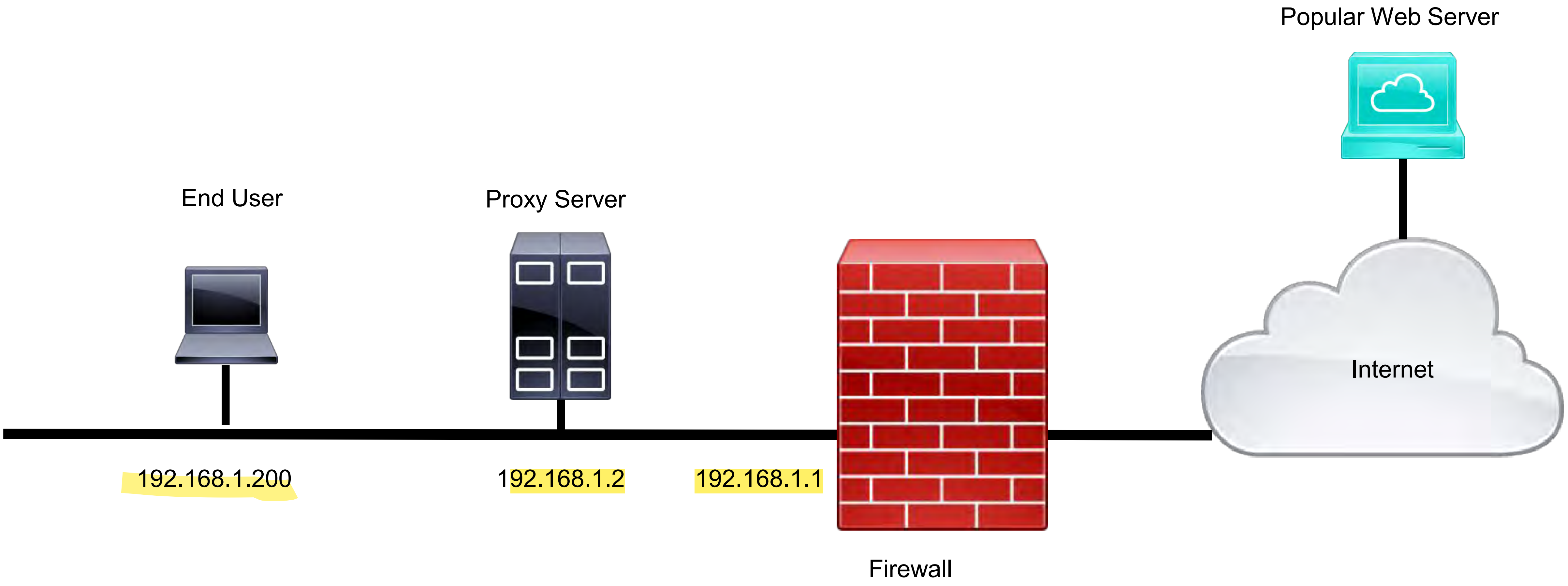
Works at Layer 7

Provides deep packet inspection

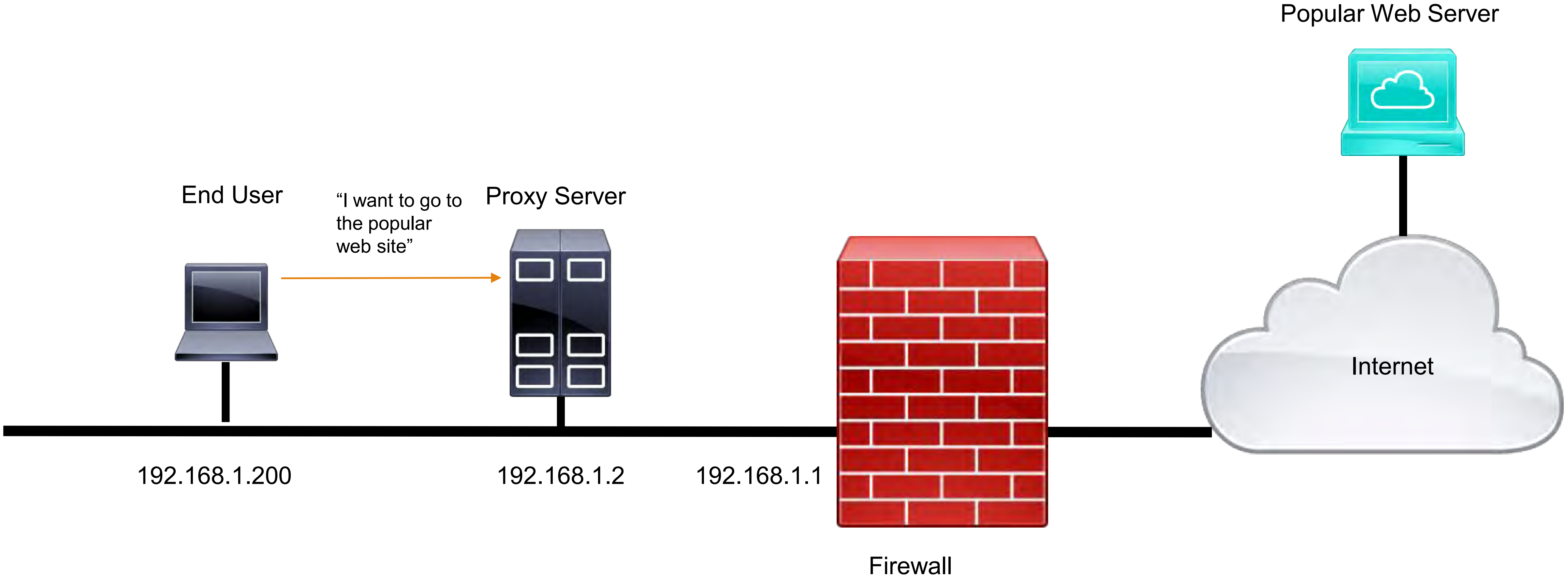
Commonly used for web clients

- The browser is configured with the IP address and port of the proxy server

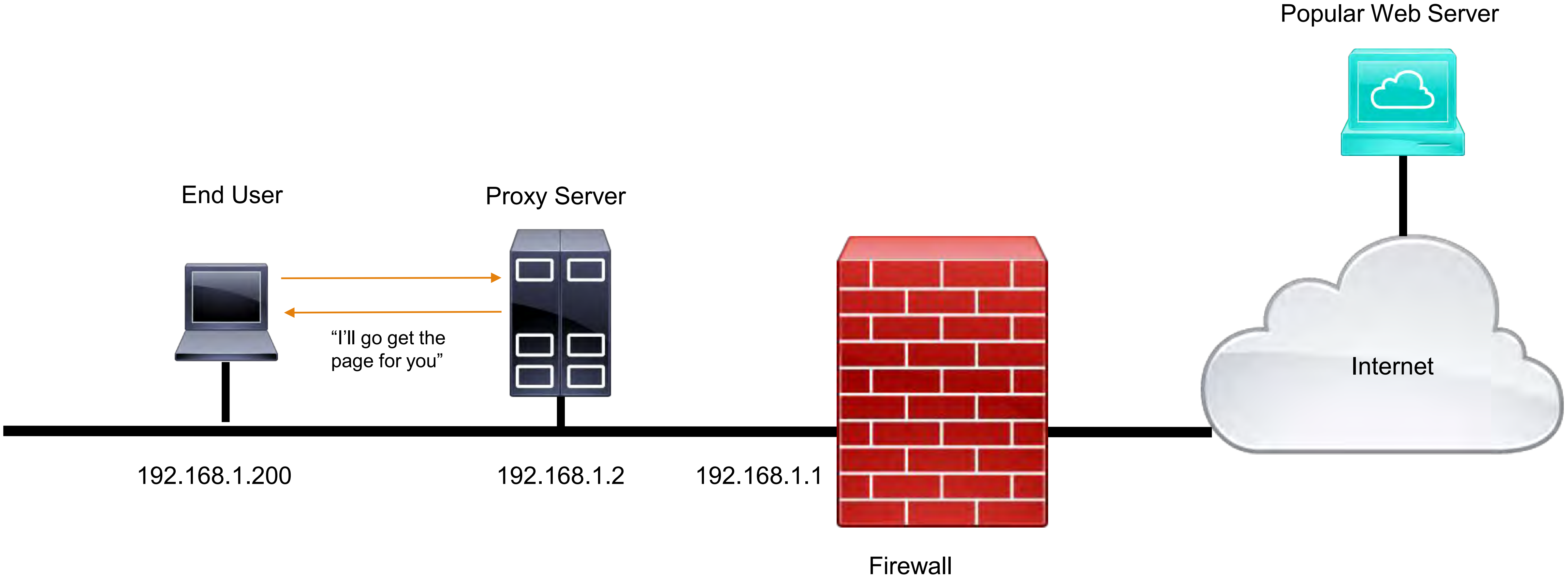
Proxy Server Example



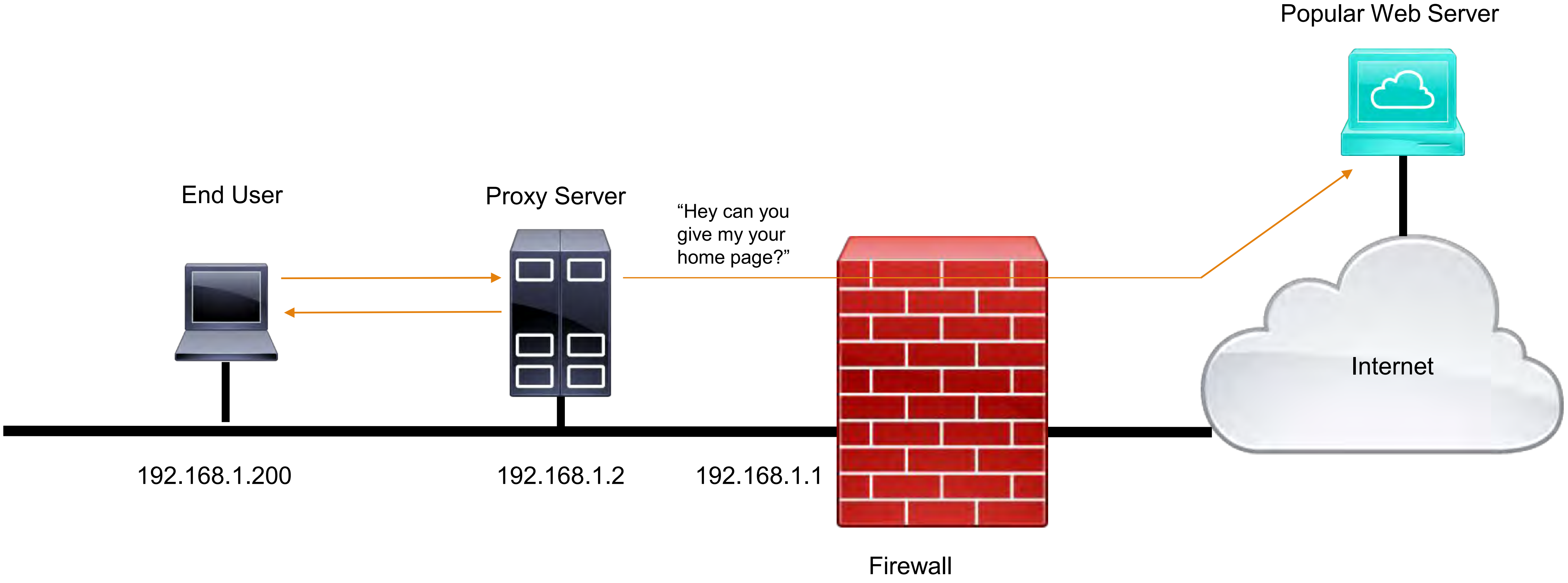
Proxy Server Example



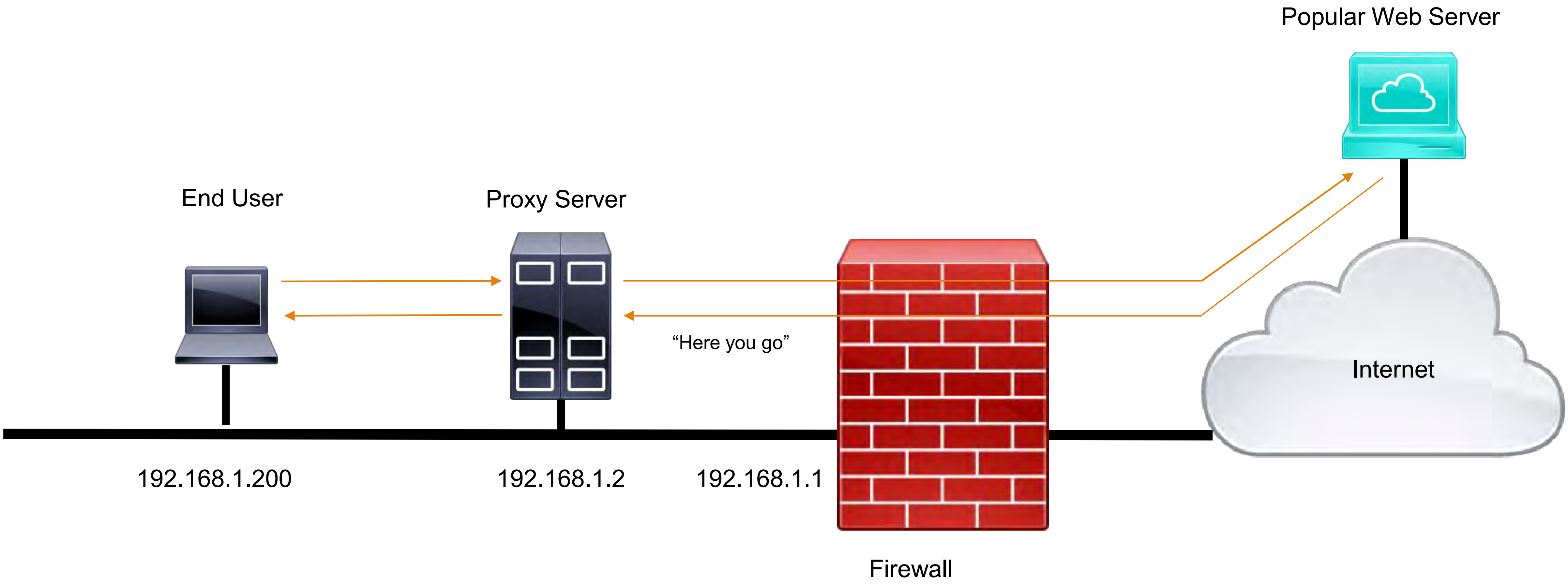
Proxy Server Example



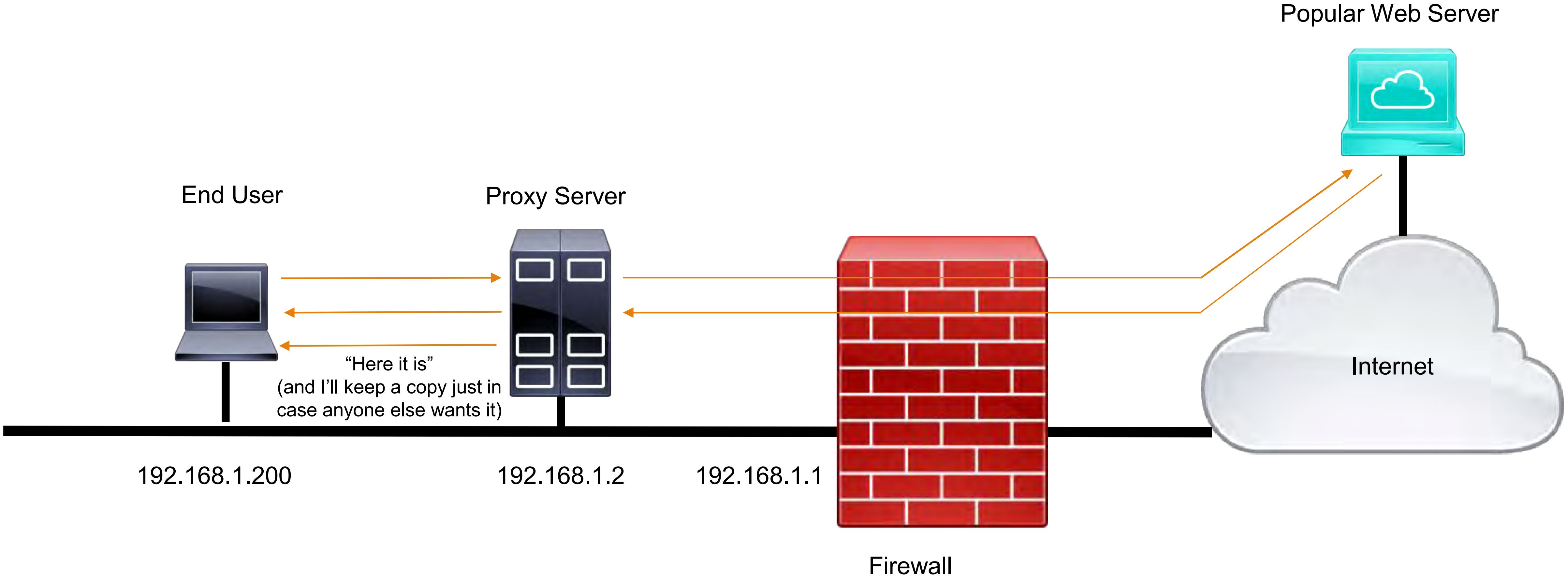
Proxy Server Example



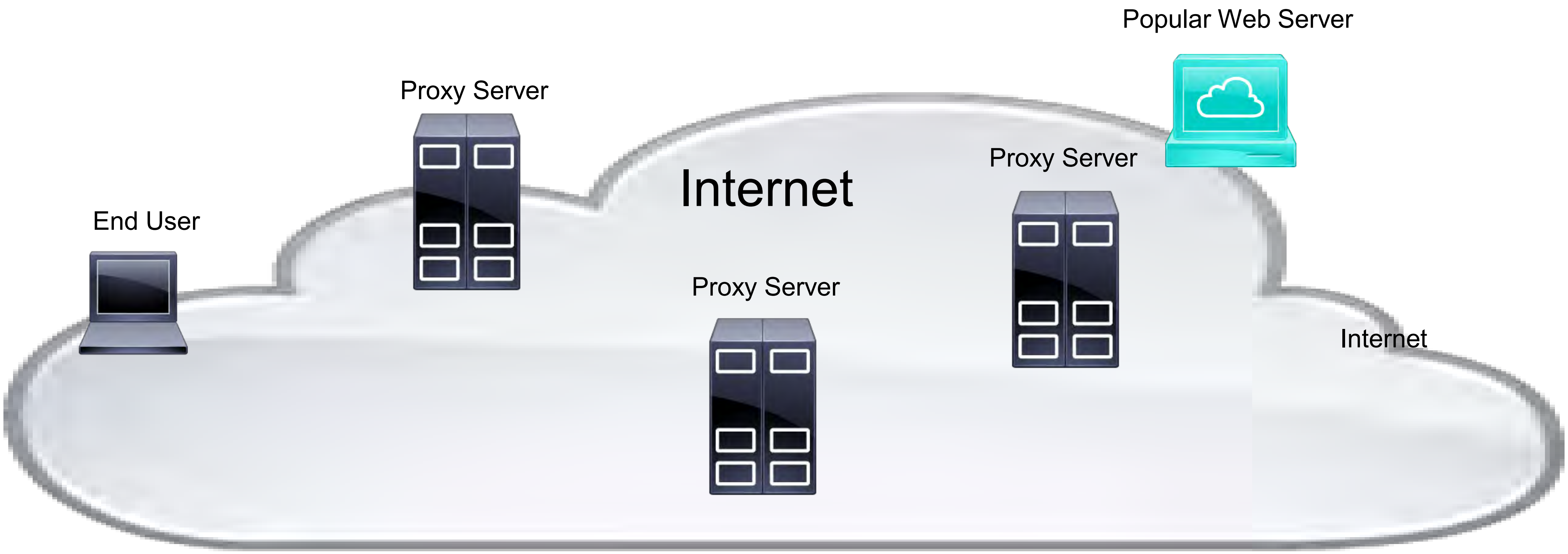
Proxy Server Example



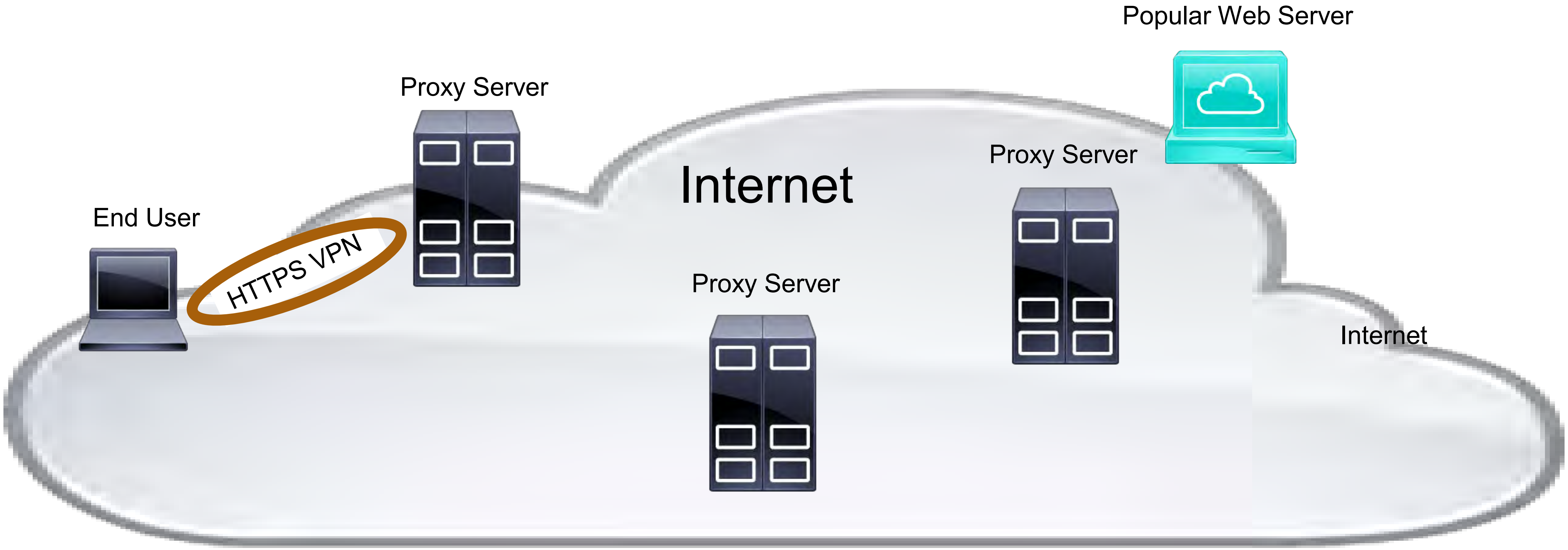
Proxy Server Example



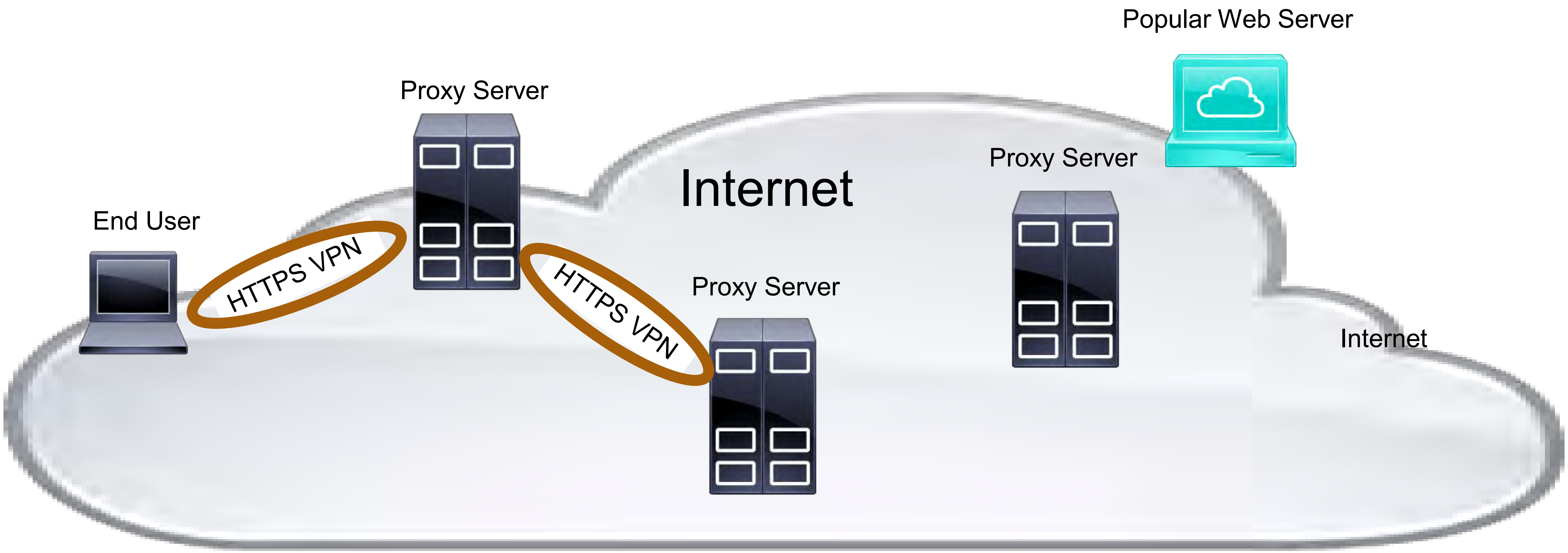
Anonymizers on the Internet Example



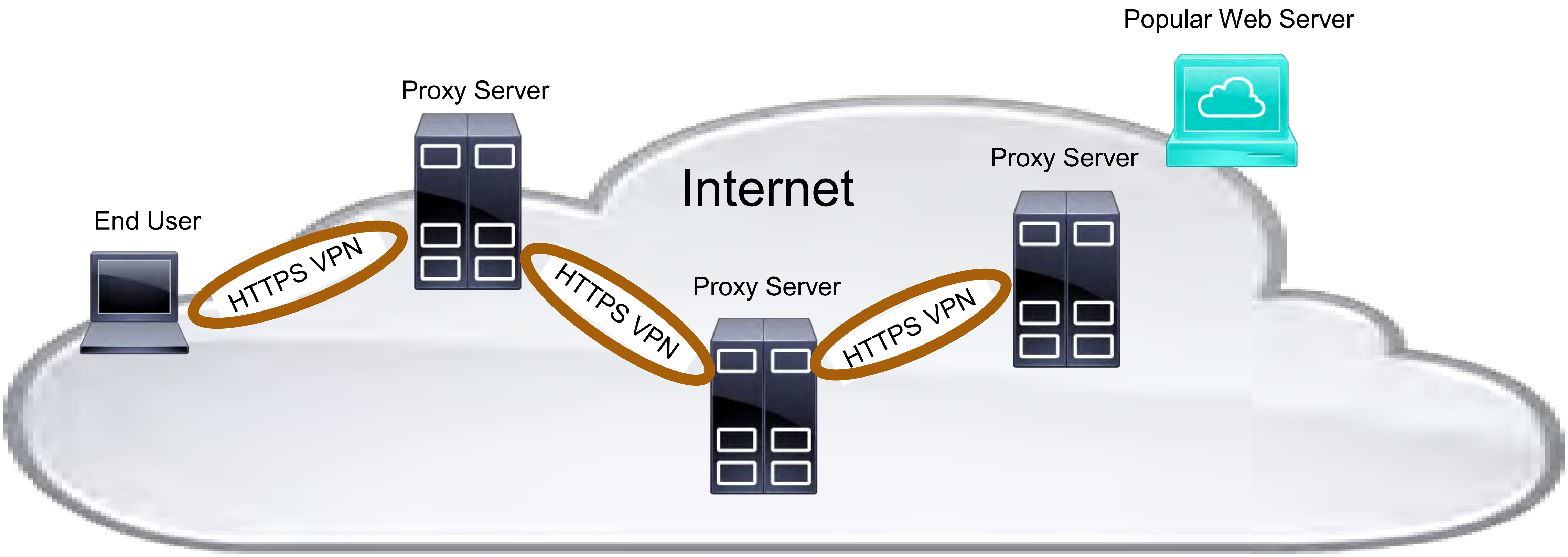
Anonymizers on the Internet Example



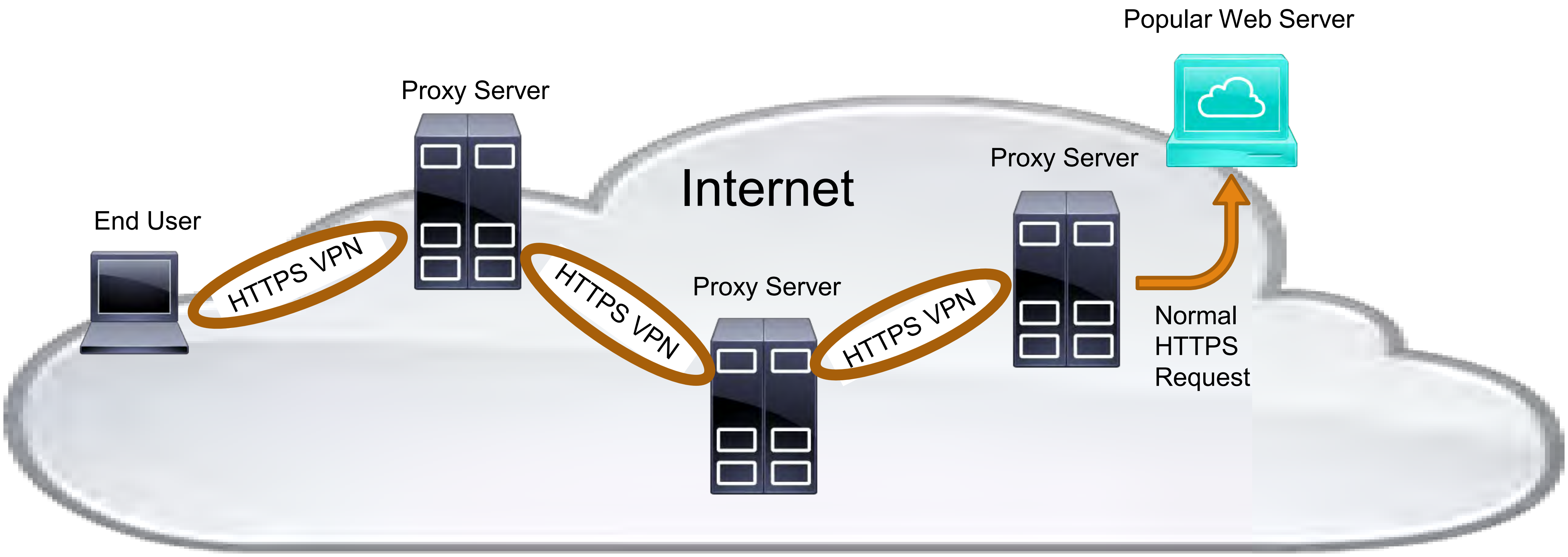
Anonymizers on the Internet Example



Anonymizers on the Internet Example

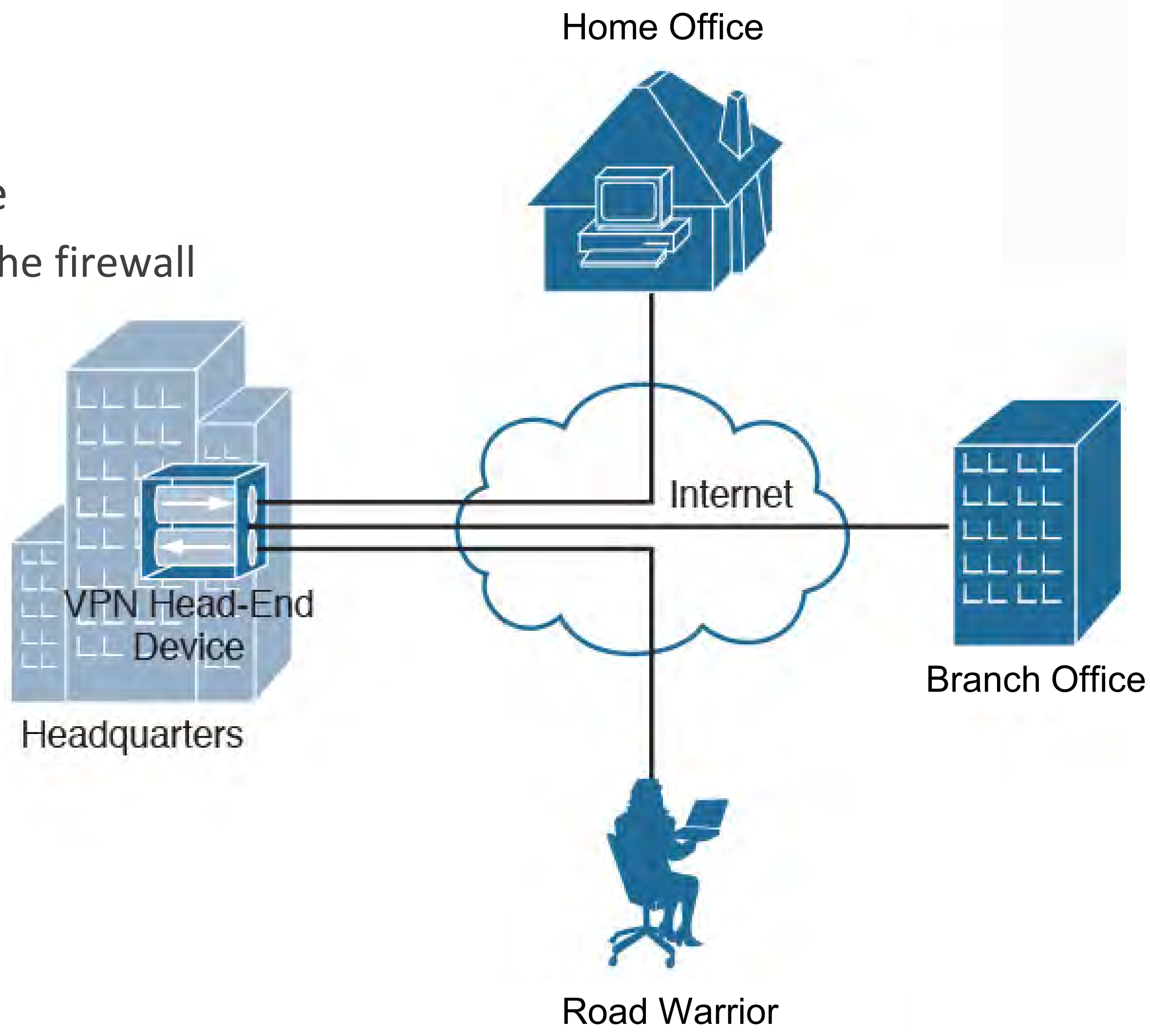


Anonymizers on the Internet Example



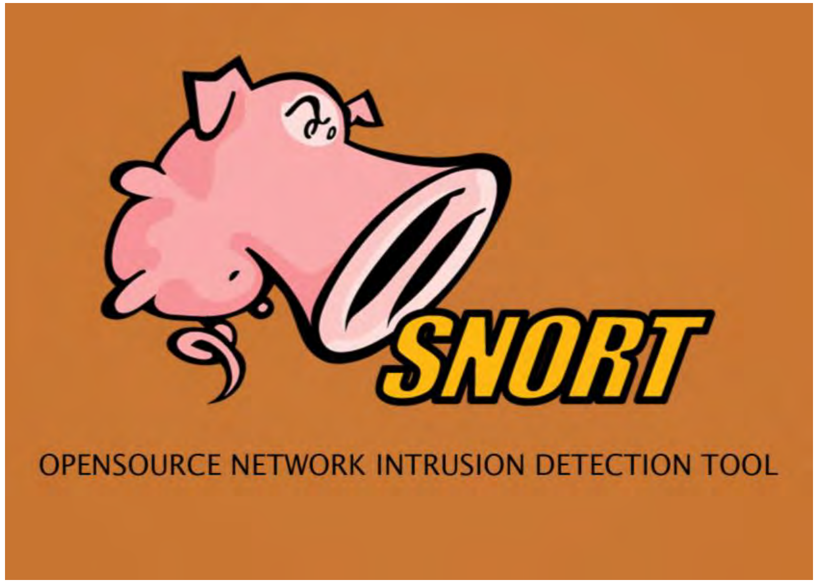
VPN Headend

- Terminates incoming client or site VPNs
- Can be a separate device or a firewall service
  - If a separate device, usually in parallel with the firewall
- Accepts multiple GRE or IPSEC connections



Intrusion Detection System (IDS)

- Analyzes network traffic for signatures that match known cyberattacks
- Must regularly update its signature database from the vendor
- Can be a network sensor or software on a device
- Logs findings to a dashboard
- Can send alerts to the administrator
- Risks include a signature database that is outdated
- Cannot detect zero day (as yet unknown) attacks



Intrusion Prevention System (IPS)

- Also analyzes packets
- Can instruct the router in real-time to block suspicious traffic
- Also logs findings to a dashboard and can alert the administrator
- Uses a signature database, but can also set a baseline of “normal” traffic and then watch for anomalies in real-time
- Can detect zero day attacks if they have an unusual traffic pattern
- Risks include:
  - false positives (system is configured to be too sensitive)
  - false negatives (if the baseline already included malicious traffic)
  - Could potentially cut off legitimate new protocols and traffic types

Modems

Modem

- **MO**dulator **DEM**odulator
- A Layer 1 device that translates signal types
- Used to connect your network to a provider
- Typically translates Ethernet (your network) to the Telco or ISP’s signal type

Cable Modem

- Connects your Ethernet LAN to a cable TV provider
- Provides you broadband Internet access via cable
- Typically has a built-in Wi-Fi router with some additional wired Ethernet ports
- Your data (transmit and receive) are treated as two premium TV channels
- Can be part of a larger service bundle that includes cable TV and VoIP telephone
- Some providers offer a free mobile app that allows you to manage the Wi-Fi part of your modem

Digital Subscriber Line (DSL) Modem

Provides broadband Internet over your phone system

Many DSL modem products are now combined with a Wi-Fi router into one unit

Connects your Ethernet LAN to a telco’s phone system

- Uses your existing phone line (with special signal conditioning)
- You use a DSL filter to separate low-frequency phone from high-frequency Internet signals

Translates Ethernet to Point-to-Point Protocol over Ethernet (PPPoE)

- PPP encapsulates Ethernet
- Provides classic PPP authentication

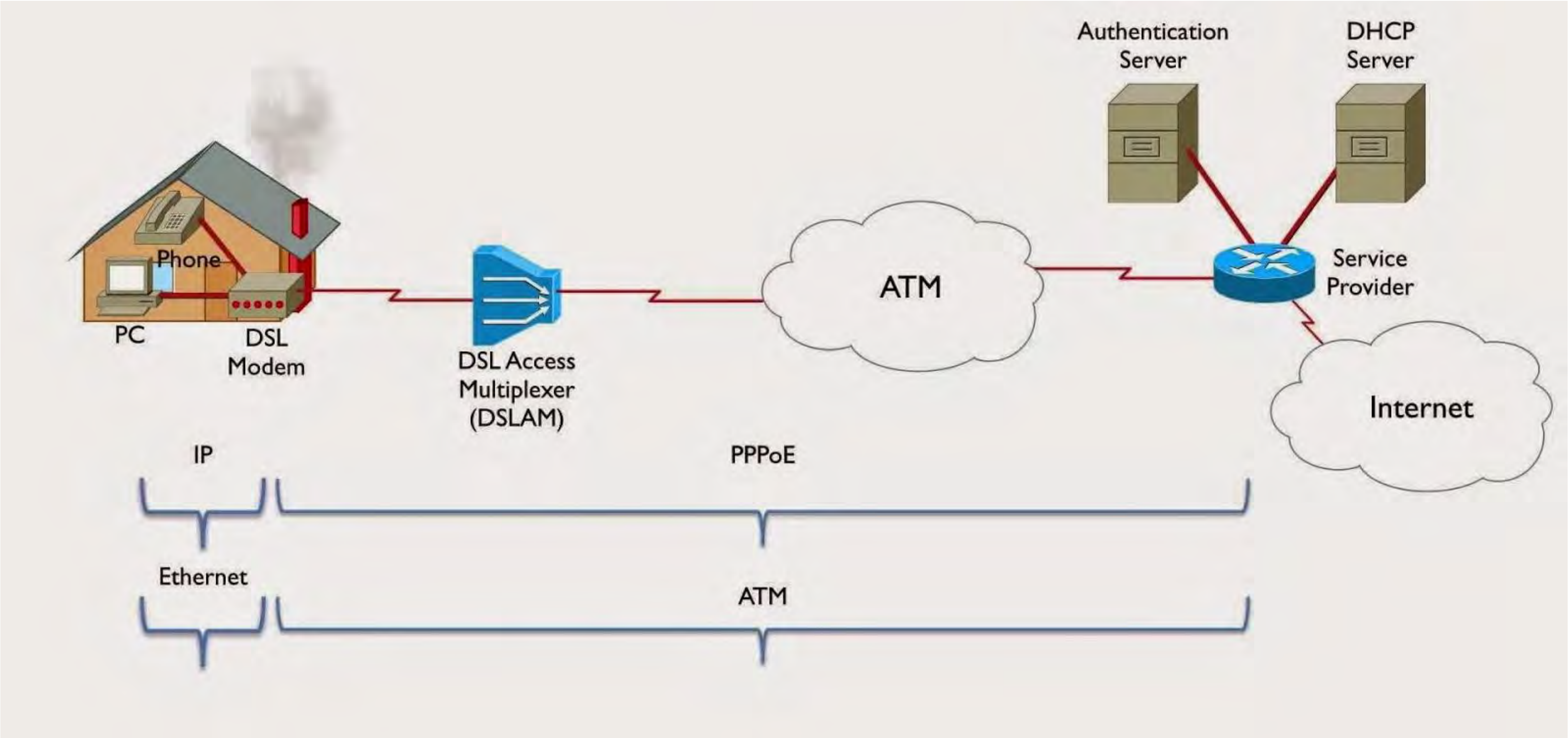
Customers are aggregated at a DSL Access Multiplexor (DSLAM)

- Located in the telephone exchange

Provider’s internal network is usually Asynchronous Transfer Mode (ATM)

DSL Modem and Filter Example

PPPoE Example



Cellular Modem

A compact device that acts as a mobile hotspot

Aka Mobile Wi-Fi (MiFi)

Connects Wi-Fi to cellular

Takes a SIM card / has a phone number

You can purchase data bundles and provide cellular broadband

Can also receive incoming calls for out-of-band management

Comes in a variety of forms including laptop dongle, expansion card, industrial device, consumer device

Some devices have jacks for external antennas

Cellular Modem Examples