Section 8:Routing

47. Introducing Routers

-A **Router** is a box that connects network IDs.

-Routers filter and forward based on IP address

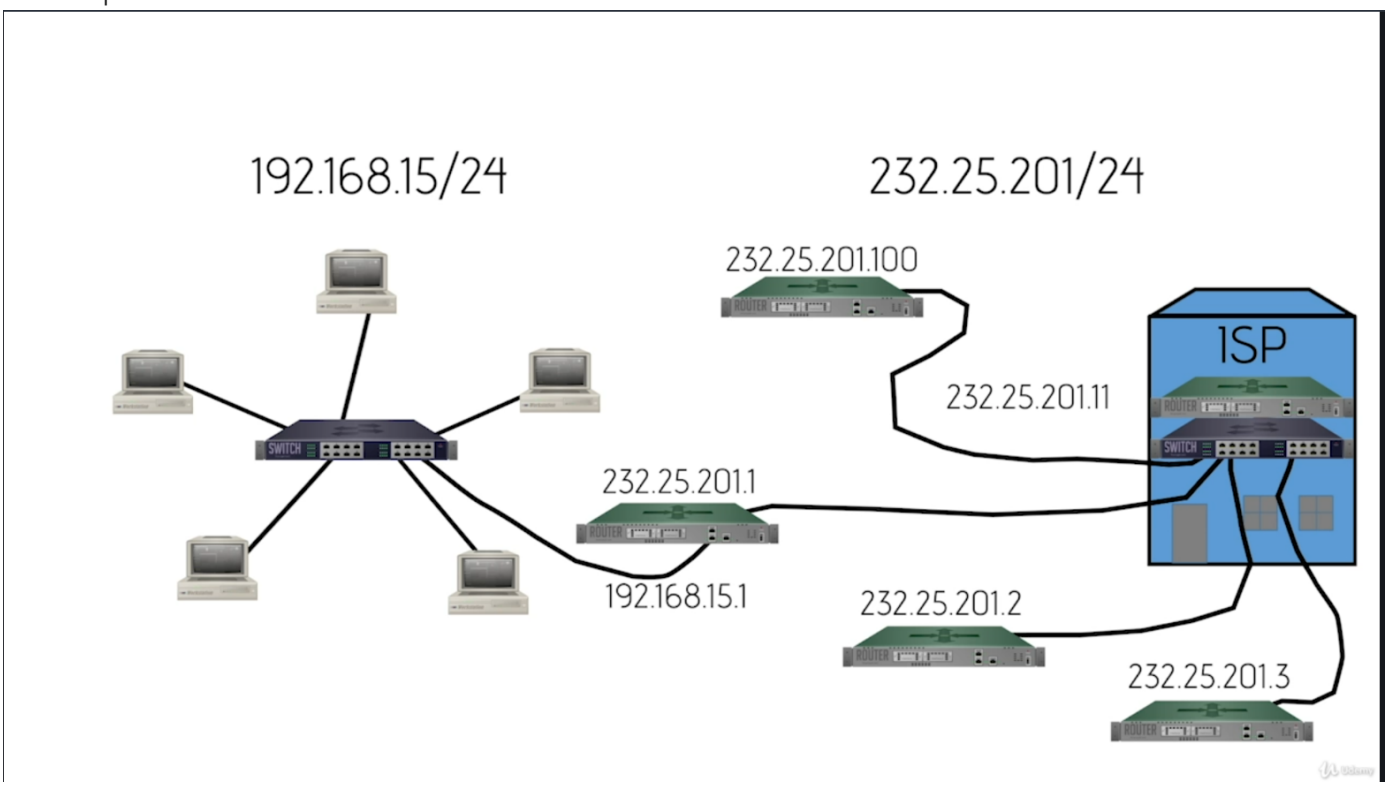
-A routing table is built into *every* router (Address, Subnet, Gateway, Interface)
Routing Tables are built automatically.

-A **Default Route** is built into every router.

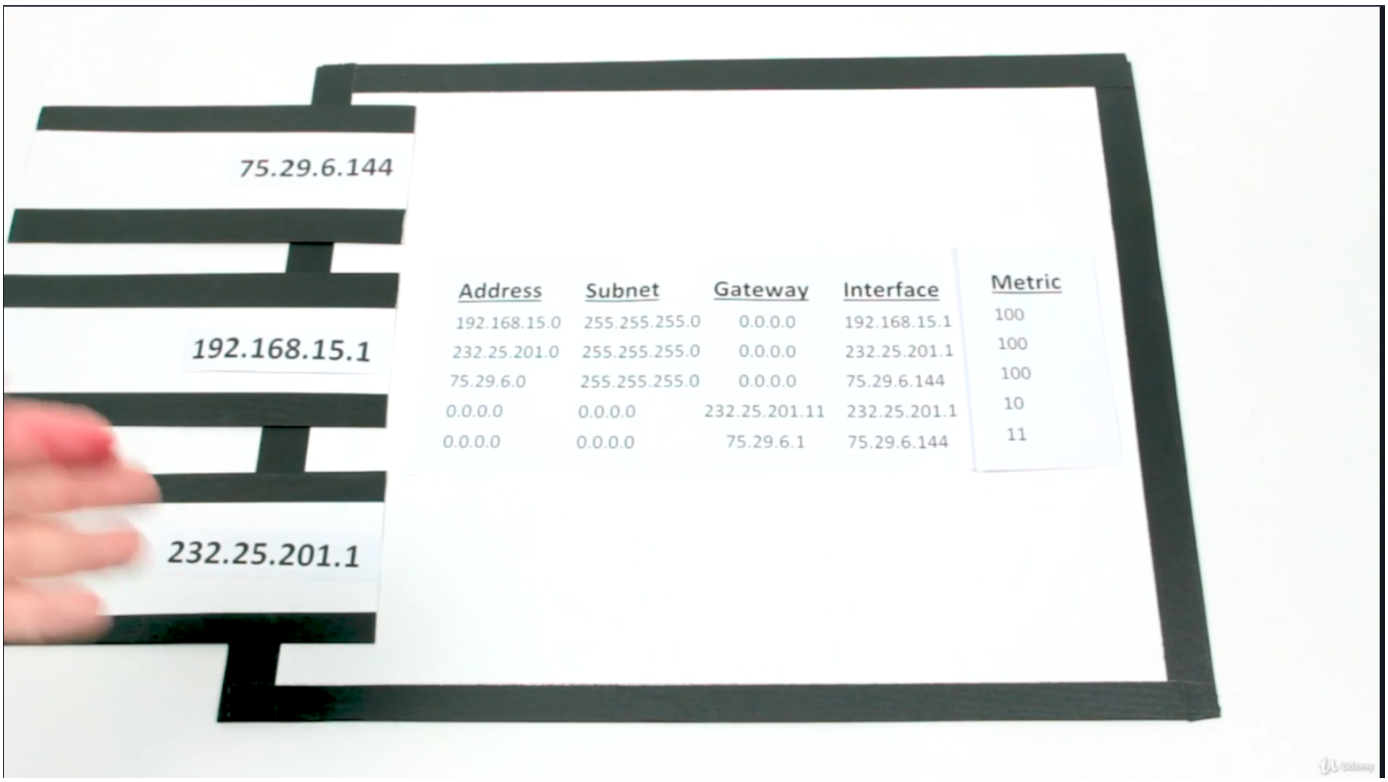
Address	Subnet	Gateway	Interface
192.168.15.0	255.255.255.0	0.0.0.0	192.168.15.1
232.25.201.0	255.255.255.0	0.0.0.0	232.25.201.1
0.0.0.0	0.0.0.0	232.25.201.11	232.25.201.1

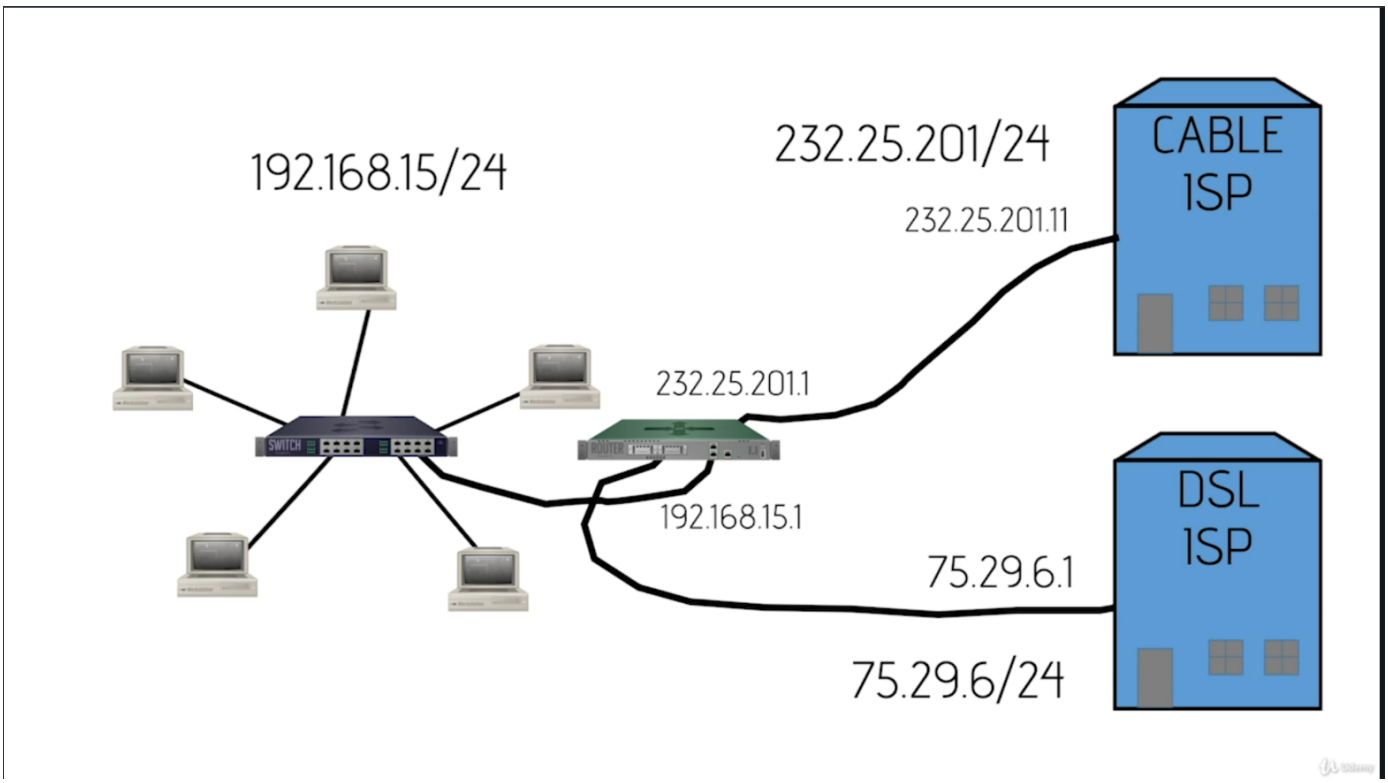
Default Gateway

ISP is Upstream router.



The metric is relative value that gives your router and Idea of which way to go if it has more than one choice.





1.Routers don't care where a packet came from, only where it's going
2.Routers are not tied to ethernet connections. It can have any kind of connections
3.Routers only care about the IP Packet.

48. Understanding Ports

Everytime a TCP packet is sent out there is a Destination port number and a source port number

1. The destination port # is set by the destination applicaton.
   -Ports 0-1024 are known as well known ports

2. Source Port (Ephemeral port) # is generated by your computer and it has to be a number well past 1023.

Web client must have the source port and the Web server must have the destination port.

Well Known Ports:

Description
1 TCP Port Service Multiplexer (TCPMUX)
5 Remote Job Entry (RJE)
7 ECHO
18 Message Send Protocol (MSP)
20 FTP -- Data
21 FTP -- Control
22 SSH Remote Login Protocol
23 Telnet
25 Simple Mail Transfer Protocol (SMTP)
29 MSG ICP
37 Time
42 Host Name Server (Nameserv)
43 WhoIs
49 Login Host Protocol (Login)
53 Domain Name System (DNS)
69 Trivial File Transfer Protocol (TFTP)
70 Gopher Services
79 Finger
80 HTTP
103 X.400 Standard
108 SNA Gateway Access Server
109 POP2
110 POP3
115 Simple File Transfer Protocol (SFTP)
118 SQL Services
119 Newsgroup (NNTP)
137 NetBIOS Name Service
139 NetBIOS Datagram Service
143 Interim Mail Access Protocol (IMAP)
150 NetBIOS Session Service
156 SQL Server
161 SNMP
179 Border Gateway Protocol (BGP)
190 Gateway Access Control Protocol (GACP)
194 Internet Relay Chat (IRC)
197 Directory Location Service (DLS)
389 Lightweight Directory Access Protocol (LDAP)

396 Novell Netware over IP
443 HTTPS
444 Simple Network Paging Protocol (SNPP)
445 Microsoft-DS
458 Apple QuickTime
546 DHCP Client
547 DHCP Server
563 SNEWS
569 MSN
1080 Socks

```
Well-known ports range from 0 through 1023.
Registered ports are 1024 to 49151.
Dynamic ports (also called private ports) are 49152 to 65535.

**for more info visit:** https://www.ietf.org/rfc/rfc1700.txt?number=1700
```

---

49. Network Address Translation

WAN - Wide area network

A **SOHO** router is a broadband router built and marketed for small offices and home offices. Since the workload for these types of businesses is primarily on the internet, they require a local area network (LAN), which means their network hardware is structured specifically for that purpose.

NAT - The router takes the local IP address, removes it and then attaches its own to send information out to the internet and vice versa.

Different versions - **Will see these on the exam**.

1. Port Address Translation (PAT)
2. Static NAT (SNAT) - I will assign one IP to one device on the network
3. Dynamic NAT (DNAT/Pooled NAT) - Router has two IPs

---

50. Implementing NAT

SOHO routers ship with NAT enabled

NAT ona SOHO router can be disabled from the routers configuration page

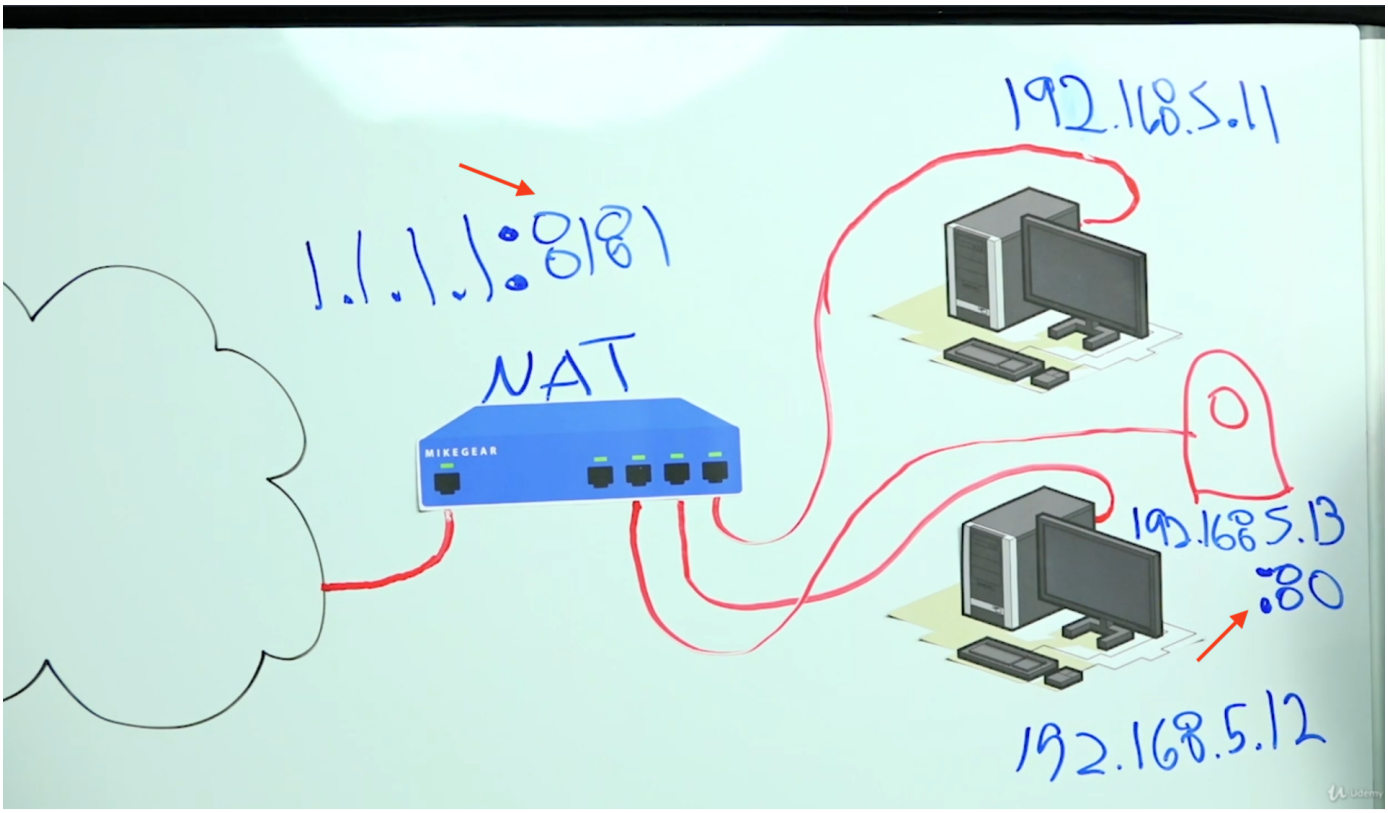
Some older routers call this setting gateway/router mode.

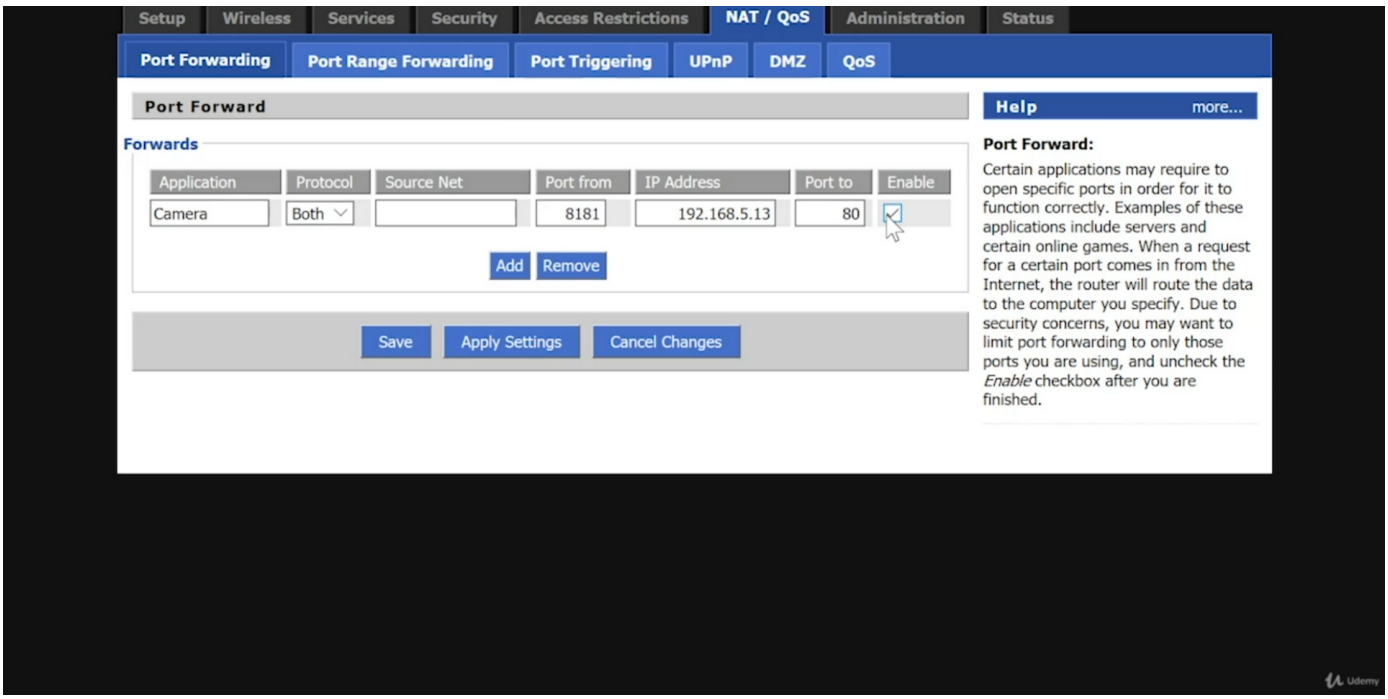
---

51. Forwarding Ports

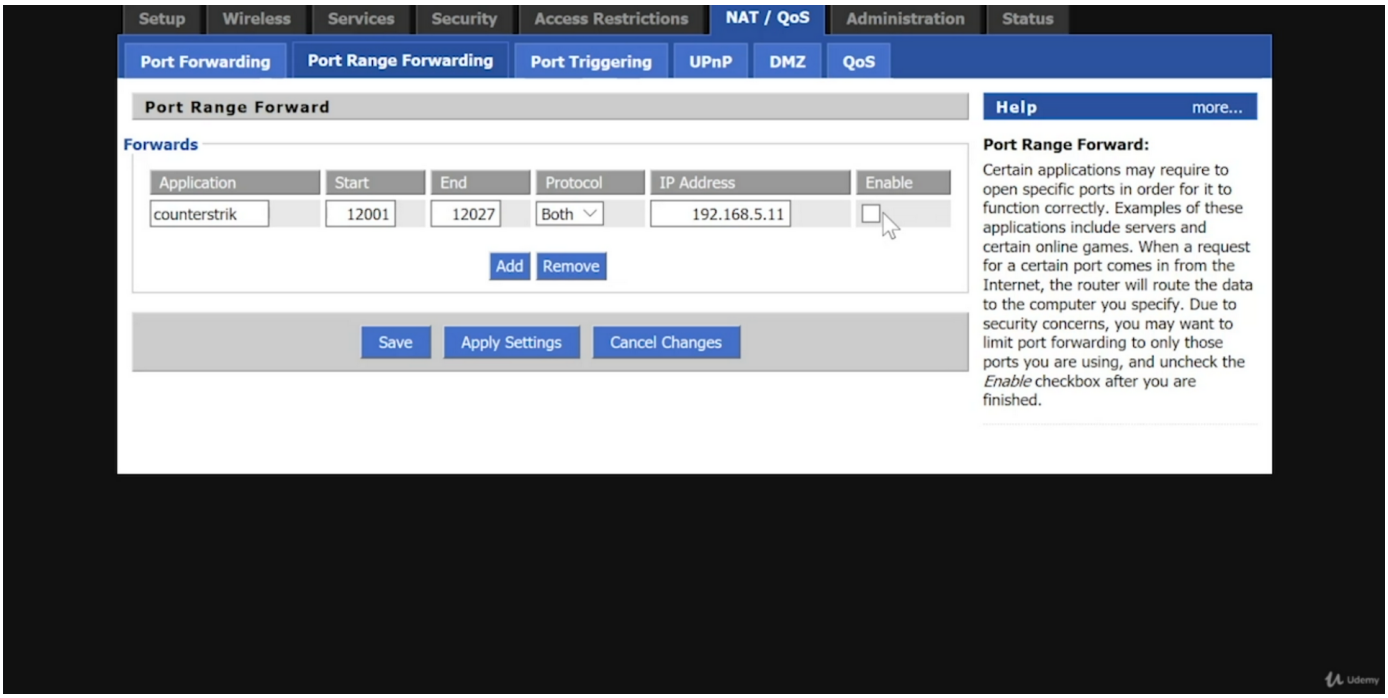
-Taking unsolicited information to let it pass through your router to get to a machine.

-Port Forwarding:





-Port Range Forwarding:

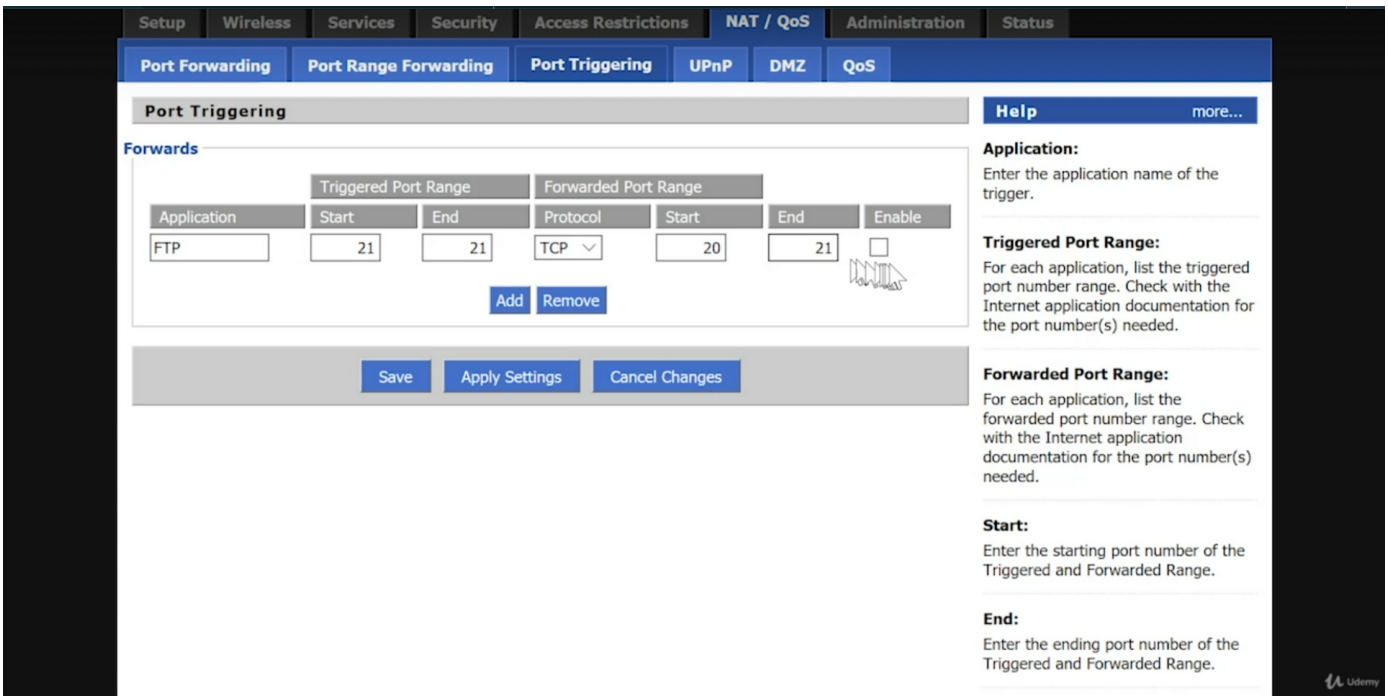


-Port Triggering:

FTP uses ports 20 & 21.

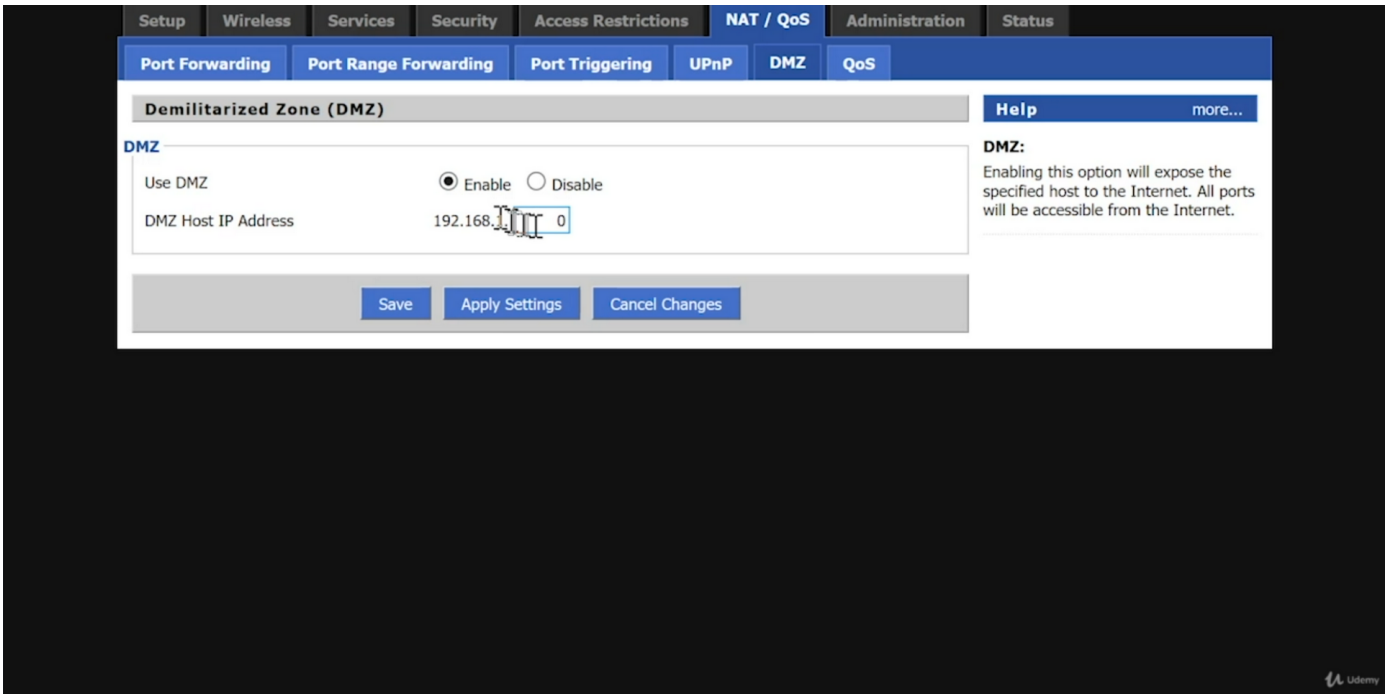
Machines will send information out on port 21, and the router is expecting a return of information on port 21 but ftp sends things back on port 20 so the information gets lost. what you can do is set the router to recognize that if something goes out on port 21, when the info comes back you can accept it from port 20 or 21.

FTP works better in active mode



-DMZ (Demilitarized Zone) or (SOHO DMZ)

Say to router "anything that comes through the router can send information to a certain computer" - Very scary. Anyone can access your computer.



Know these for the exam

---

52. Tour of a SOHO (Small Office/Home Office Router

-Router comes with documentation and Installation media:

Important info it comes with :

Default IP Address
Default UserName and Password

What can you expect to see on a typical router?

-A status
-WAN IP
-LAN IP

*30/30/30 rule for hard resettin routers.

1.Unplug all the network cables
2.Press in the reset buttion for thirty seconds with the power attached
3.unplug the power cable (while still holding the reset button) for thirty seconds
4.plug the power cable back in (while still holding the reset button) for thiry seconds

---

53. SOHO vs. Enterprise

*SOHO
-Gateway router (One connection to the isp, and a single connection to your network)
-Built in switch.
-Built in wireless access point 802.11
-can support 5-6 computers without slowdowns

-Customizable firewall
-Web interface

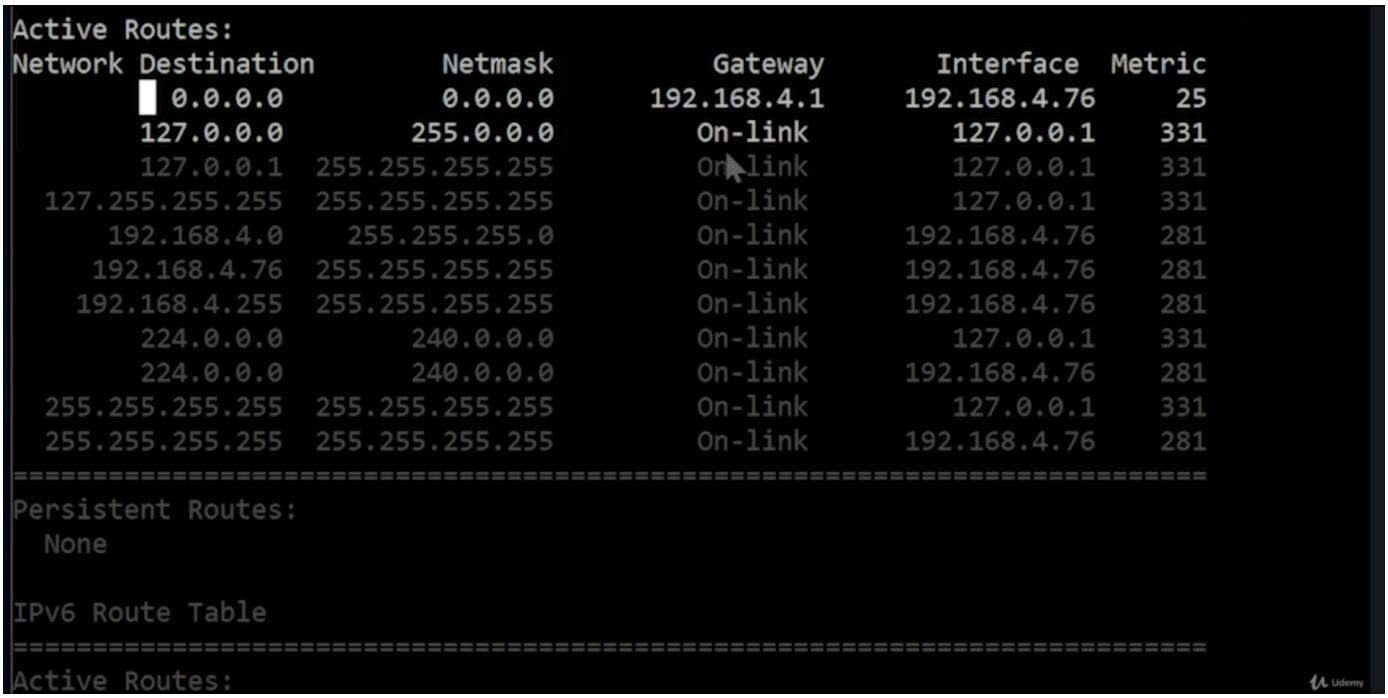
*Enterprise router
-Designed for more robust situations
-You put this on a rack and let it run without worry
-No wireless built in
-No switch built in
-100x bandwith (can support 200-300 computers without slow downs)
-Tend to not have web interfaces

---

54. Static Routers -Fixed route that is manually configured and persistent

-Every router has a routing table.
-Every computer on TCP/IP networks have a routing table

Routing table: (contain information for destination, subnet mask, gateway and NIC)



Multicast is a class D ip address

"netstat -r = route print"

55. Dynamic Routing

*Routers can dynamically change their routing tables.
*convergene is where all router tables reflect all routes

The **Metric** value can help us look at a lot of issues (arbitrary value)

Will see on exam
Considerations of metric values:

*MTU - maximum transmission unit (How much data can you haul in a frame)
-Ethernet can haul a max of 1500 bytes

*Bandwith

*Cost

*Latency - How long does it take a route to react to what you are trying to do

How to get info between routers

Dynamic routing protocols (two groups):

1. Distance vector - Sends entire routing table to all the neighbors. Neighbors look at them compare them to their own and determine the fastest route.
   -Old
   -Distance vector relies on hop count
   -They send things at a given interval so if one machine goes down we have to wait for the next interval to get back into convergence.
2. Link state:
   -Modern
   -Send out Hello/Link state advertisments (Basically a ping) and if there is a change the router will let others know when things have change.
   -get back to convergence much faster

*All dynamic routing protocols can be broken into two groups:

*IGP (interior gateway protocols)
*EGP (exterior gateway protocols) - anytime you want to talk outside of (a group of routers (one organization that has control of its particular routers is an "Autonomous system")) you used EGP.

-There is one EGP (Border Gateway Protocol (BGP) - ISPs get an autonomous number (ASN autonomous system number)

Need to know for Exam
Link state or distance vector
Uses metrics to get the routes
EGP (BGP) or IGP

56. RIP

"Routing information protocol"

1. RIP is an IGP (interior gateway Protocol)
2. Distance Vector Protocol

-Uses HOP counts
-Takes a while to get convergence
-RIP v1 only used classful networks
-RIP v2 can hand CIDR based networks
-RIP v2 can has security built in
-RIP has a max hop count of 15 hops.

57. OSPF (Open Shortest Path First)

1. Link state protocol
2. IGP (Interior Gateway Protocol)

-routers are plug together and then calculate their links
-they elect a designated router and a backup designated router
-Routers are configured/given an Area ID's
-Once this is set they start to tell each other who they are connected to by sending (Link advertisents/link states)
-convergence happens in seconds.

58. BGP

(Border Gateway protocol)

-Hybrid protol (aspects of Distance Vector and Link State)

-Breaks the internet into a little over 20000 autonomous systems

AS -group of one or more router networks under the control of a single entity
-those entities have direct or indirect control over every routers/networks/subnets within their own AS
-every AS has its own 32 bit ASN (AS Number)
-AS's are connected using BGP
-BGP routers only use ASNs to direct information.

```
**BGP is a hybrid protocol
**BGP is the primary protocol for the internet
**BGP is based around the concept of autonomous systems
```

QUIZ

1. What is the job of a routers?
   a. To assign IP addresses to hosts on the network
   b. To connect networks with different network IDs
   c. To map IP addresses against MAC addresses
   d. To allow outside hosts to initiate contact with hosts on the LAN side of a network.
2. What is the role of port numbers in IP headers?
   a. Port numbers identify the sending and receiving processes between two hosts
   b. Port numbers identify which interfaces on a router should receive data in and which interfaces should forward data out
   c. Port numbers identify which connectors on a swith that should receive data in and which should forward data out
   d. Port numbers identify the path of routers between any two hosts that need to communicate with each other.

3. Which statement is true of NAT router?
   a. NAT routers replace the source IP address with its own IP address
   b. NAT routers allow public addresses to exist on the LAN side of the router
   c. All hosts on the LAN side of a NAT router are assigned the same IP address as the public address in the router
   d. The NAT function is performed at the ISP facility
4. True or False: Most SOHO routers come with NAT enabled?
   a. True
   b. False
5. Port forwarding allows which of the following?
   a. Public addresses to be assigned to the LAN side of a NAT router
   b. One host on the LAN side of a NAT router to be assgned with the same public address of the router's WAN interface
   c. Registes a LAN side host with portable DNS address
   ** d. Outside access to hosts on the LAN side of a NAT router**
6. A tech has just installed a new SOHO router for a client. Which security task should the tech perform first?
   a. Change the administrator name and password
   b. Disable port forwarding
   c. Disable DHCP server
   d. Enable MAC address cloning
7. Which feature of a SOHO router is not typically found in a enterprise router?
   a. Two or routers interfaces
   b. Graphical or textual managment interface
   c. Each interface is the router much be configured
   d. Built-in switch
8. Which statement is not true of static routes?
   a. Routers can have static routes
   b. Hosts can have static routes
   c. Static routes are entered manually and must be manualy changed by a human
   d. Static routes are entered manually but can be automaticaly changed by the router.
9. Which of the following is not an element of a route metric?
   a.MTU
   b.Hop distance
   c.Cost
   d.Bandwith
10. Which of the following is not a characteristic of the RIP routing protocol?
    a. RIP is a distance vector protocol
    b. RIP is an interior gateway protocol
    c. RIP supports a maximum hop count of 127 hops
    d. The primary metric in RIP is hop count

11. Which of the following is not a characteristic of the OSPF routing protocol?
    a. OSPF is a link state protocol
    b. OSPF is a distance vector protocol
    c. OSPF routers are grouped into areas
    d. OSPF routers in an area elect a designated router and backup designated router
12. Which of the following is not a characteristic of the BGP routing protocol?
    a. BGP is a hybrid of distance vector and link state routing protocols b. BGP is broken up into divisions called Autonomous Systems (AS)
    c. The primary job of BGP is to route between ASes
    d. OSPF is the primary routing protocol between ASes