Routing and NAT

the transition from a simple to a complex wireless network

by: Ian Howard

purpose

- advanced routing techniques and NAT are two topics that I find that WISP operators encounter, but they are intimidating topics that are theoretical and not physical like other topics.
- in this session we will equip you to fix problems with NAT and routing to allow you to expand your network.

NAT

- NAT = Network Address Translation
- used for two reasons, one there is a limited number of IP addresses available
- two, ISPs often try to limit people's use of a connection by Ips, though “gateways” have for the most part nullified that feeble attempt.

there are two NATs

- Source NAT (SNAT)

  used to split one IP address among many machines behind a gateway

- Destination NAT (DNAT), sometimes referred to as port forwarding

  used to re-direct an outside connection to a system on the inside

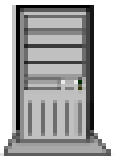
  also used by “captive portals” to send users to login pages

note: public vs. private IPs

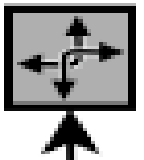
- public IP: an internet routable IP address, assigned by the Internet Numbering Authority
- private IP: a private IP address that is only used on an internal network and is not accessible by the internet, their ranges are:
  - 192.168.x.y
  - 10.x.y.z
  - 172.16.x.y

SNAT

- SNAT, also referred to as “masquerading” allows you to split a single “public” ip address to many internal “private” ip addresses

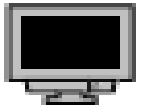


router has the only "real" ip address

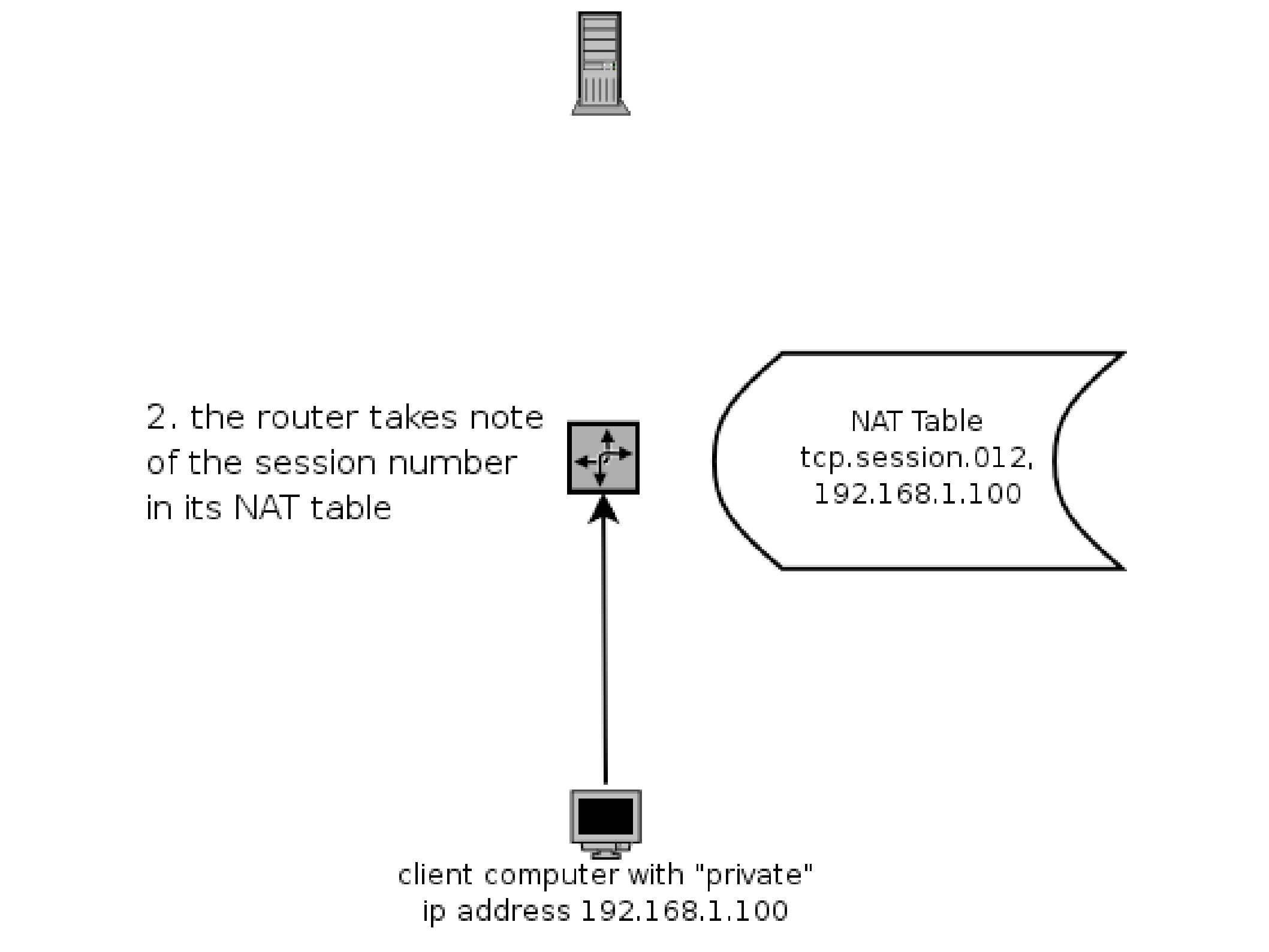


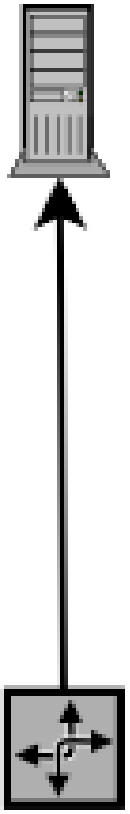
router on the internal side has a private ip address 192.168.1.1

client goes to a webpage



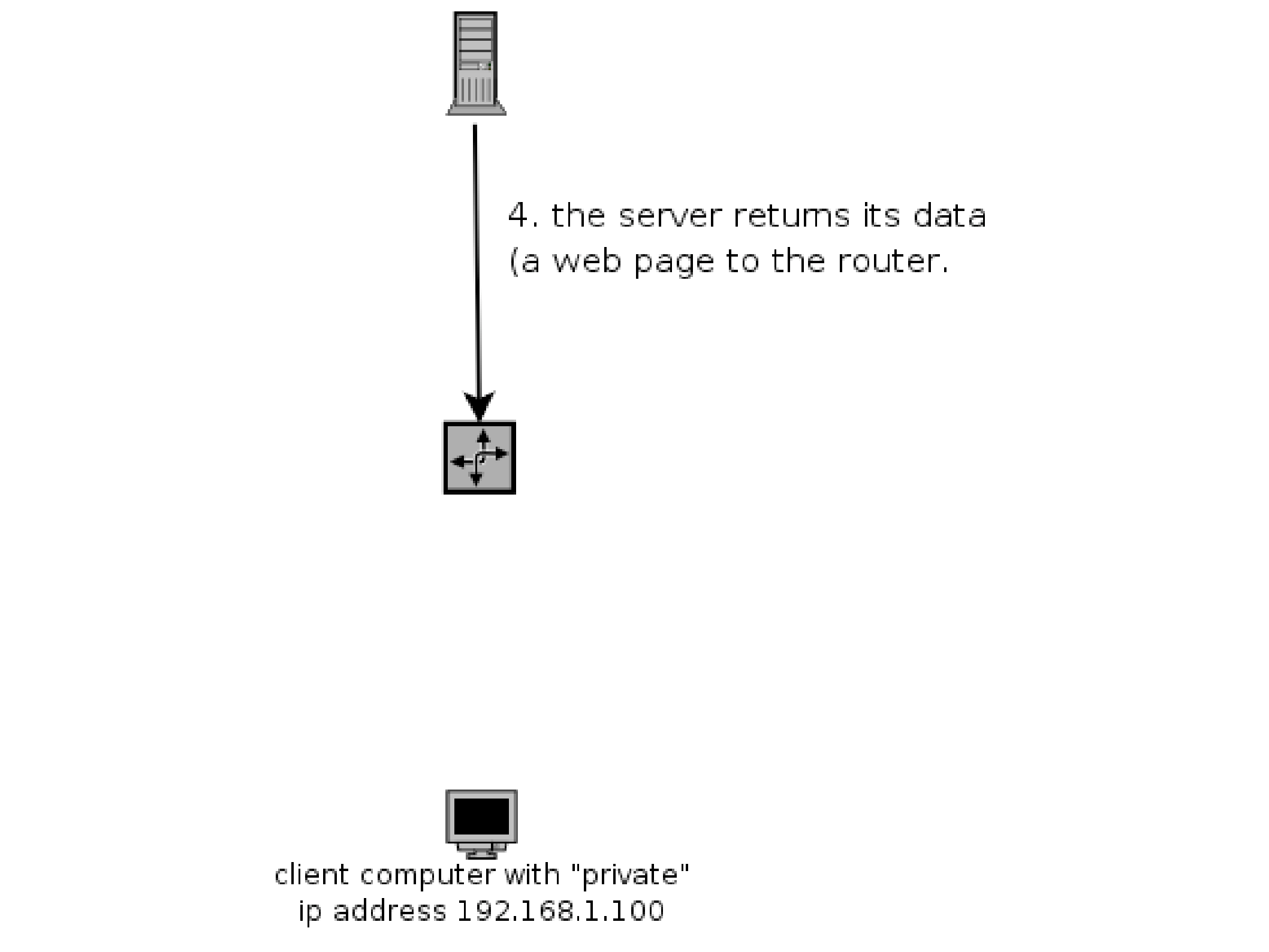
client computer with "private" ip address 192.168.1.100

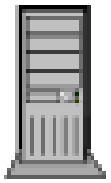

2. the router takes note
of the session number
in its NAT table
NAT Table
tcp.session.012,
192.168.1.100
client computer with "private"
ip address 192.168.1.100

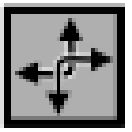


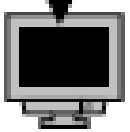
3. the router re-writes the source address to that of itself, then forwards the request to the internet

client computer with "private" ip address 192.168.1.100


4. the server retums its data
(a web page to the router.
client computer with "private"
ip address 192.168.1.100





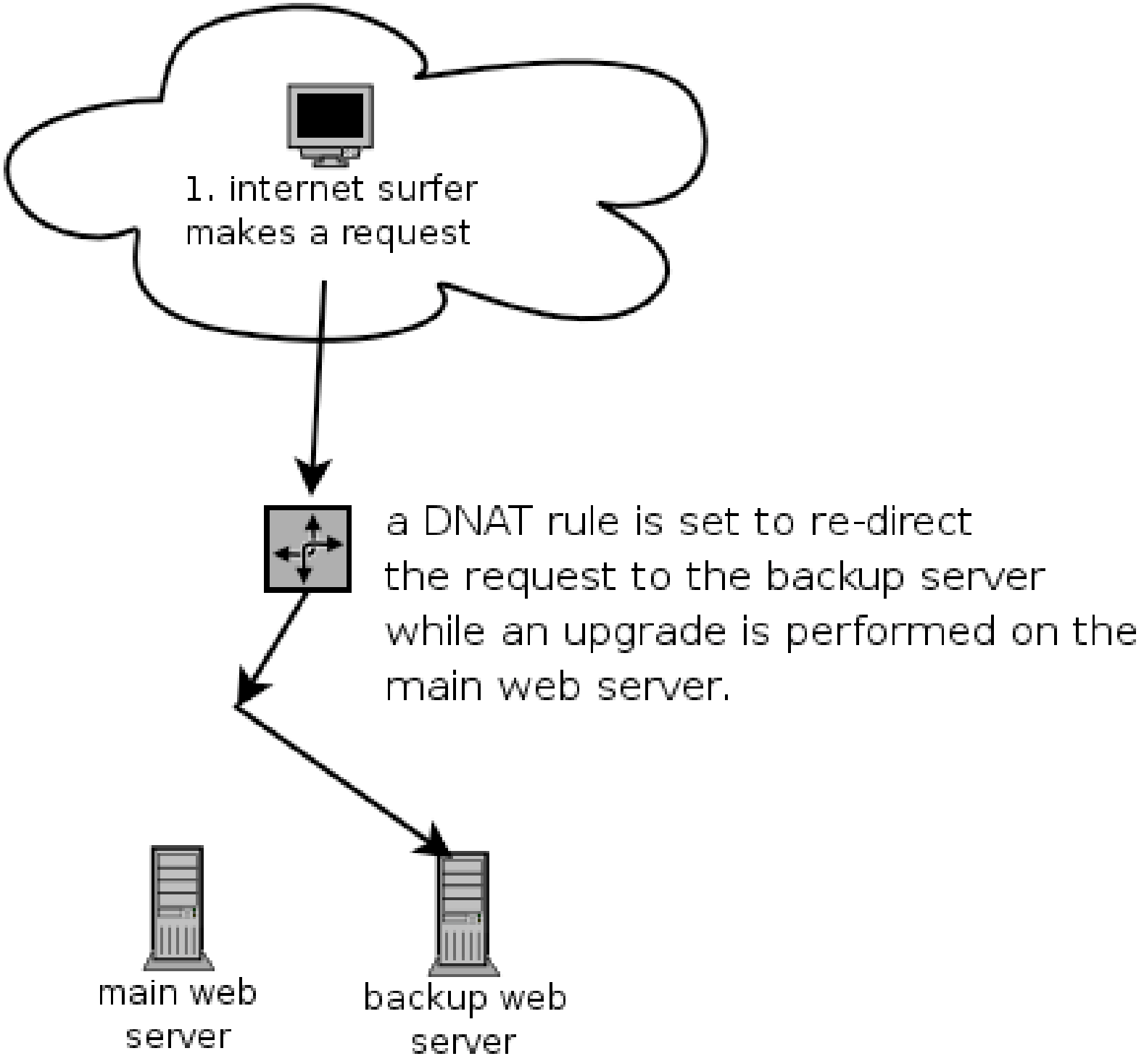


5. the router checks its NAT table,
finds the corresponding "tcp session"
then forwards the packet to the
original host.

client computer with "private"
ip address 192.168.1.100

DNAT

- most often used to allow administrators to access their servers from outside of the network
- also used for captive portals, login pages for hotspots.


1. internet surfer
makes a request
a DNAT rule is set to re-direct
the request to the backup server
while an upgrade is performed on the
main web server.
main web
server
backup web
server

how does SNAT work?

- NAT makes use of a characteristic of TCP, when a connection is made there is a tcp session with a unique number
- when a client connects to the internet, the gateway records the session number and the corresponding host's ip address, i.e. session X belongs to computer Y
- the source address in the packet is then re-written, changed to the public ip of the gateway

then,

- the packet is sent to its destination, such as a web server. The server receives the packet then sends it back to the public ip address.
- when the session arrives, the gateway checks its “NAT table”, looks up the corresponding session, then sends that packet back to the originating host.

and DNAT?

- this works in a similar way, a packet from the Internet is received by the gateway, if a DNAT rule exists, such as a “re-direct” to another system then the gateway with re-write the destination address of that packet to the server and also set the source address to itself. It records that session and the originating host.

then,

- when the server replies, the packet is sent back to gateway, where the gateway looks in its NAT table to find the session then returns the packet to the originating computer.

so what are the problems with NAT?

- little really, except it does give the originator some anonymity (that can be good or bad)
- does introduce a slight delay, as the gateway must do all of this re-writing, this is more acute on a busy gateway
- it can cause certain applications to not function well (VoIP, peer-to-peer, sharing)
- best to avoid when possible especially for busy machines, like servers.

a few hints

- servers that serve internal clients should be before the NAT gateway and visa versa, servers that serve the Internet should have a real IP.

repeaters, bridges

- a repeater = bridge
- it takes a signal and re-sends it
- it has no intelligence, it ignores TCP/IP, it simply takes packets and duplicates them
- used to extend a network, but to make that extension transparent
- the need for repeaters has been replaced by “virtual LANs”

the subnet

- gone but not forgotten
- the subnet has been made irrelevant by network switches on wired networks, but they are still very useful to wireless networks

broadcast domain

- wireless networks are shared mediums, access points cannot logically separate the signals because all radios in the broadcast range of a signal will receive it.
- when a repeater is used, the basic network packets, overhead, is also repeated.

why to not use a repeater at the client site?

- i.e. Bekka Valley Insurance Co. has 10 computers connected to your network.
- Pcs send out a lot of broadcast messages, “browsing” for other networks, seeking printers and other packets. With a repeater all of those packets are sent to the wireless network.

reason 2: why not as a relay?

- one-radio problem
- a radio can either send or receive, but not both at one time
- wireless repeaters have limited “buffer” space
- clogs the link
- ok for low-bandwidth links with few customers.

advanced routing

- so, to limit “broadcast” domains and to expand our network we need to route
- “route” in networking means to put in a device that can intelligently decide where to send a packet based on that packets destination address.

routing protocols

- routing protocols are used to inform a routers about routes on a distant router
- each router knows about the subnets directly connected to it, but not those that are connected to other routers, thus they need to be informed:
- static routes
- RIP
- Vector based protocols

the static route

- the simplest way to add a route to a distant subnet
- to go here, first go here. i.e. to get to the Cedars, first to to Tripoli
- you add this “statically” or manually
- it is called static because it will not change by itself.

RIP

- RIP = Routing Information Protocol
- is a very basic protocol that simply broadcasts to other routers what routes are connected to itself.
- the Tripoli router announces, “I have routes to Cedars, Beirut and El-Mina”, while the Baalbek router states, “I have routes to Zahle and Laboue”
- it is “dynamic”

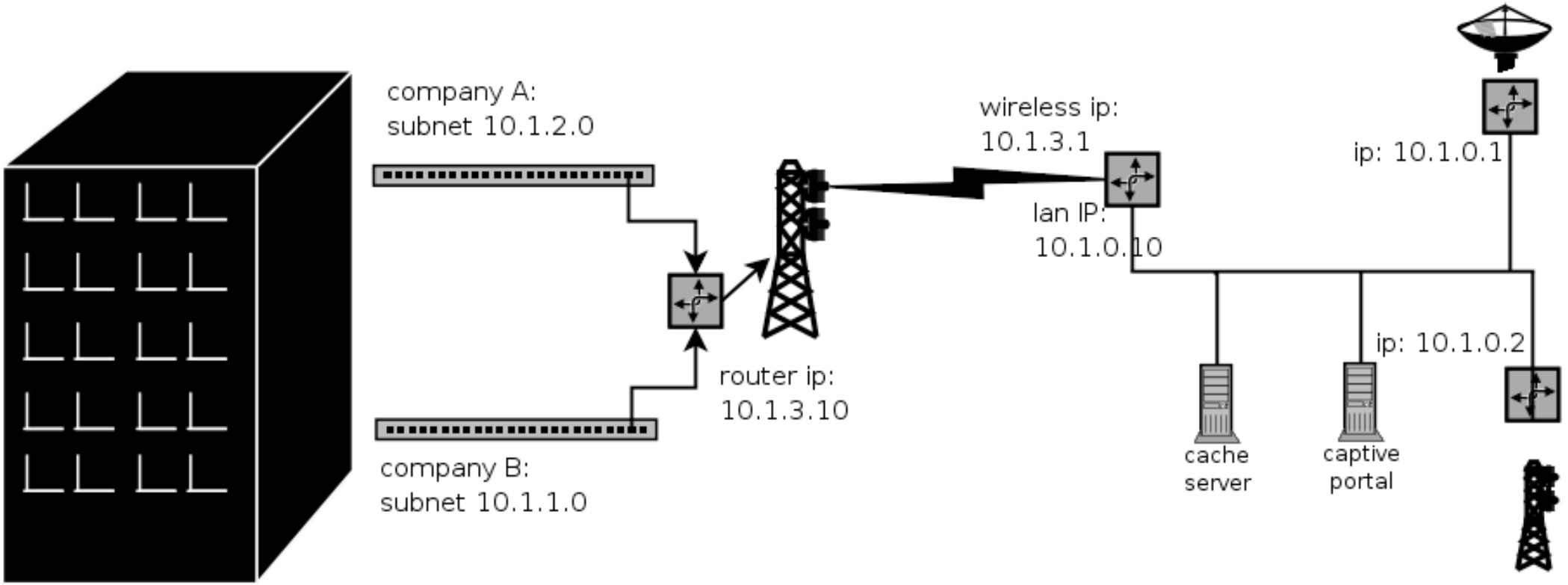
Vector based routing

- there are more advanced routing protocols referred to as “vector” based as they will calculate the shortest or best paths.
- they are more complex and can sometimes make routes a bit of a mystery.
- we will go into more detail in the “Mesh” networks seminar.

the two routers deep problem

- a common problem, where a subnet exists below another subnet. Perhaps there are two companies in the same building connected internally via Ethernet sharing a link but you do not want them to receive each other's traffic, so you add a router to each client's network.

the two routers deep problem



a VSAT problem

- up via microwave down via VSAT
- why won't this work?