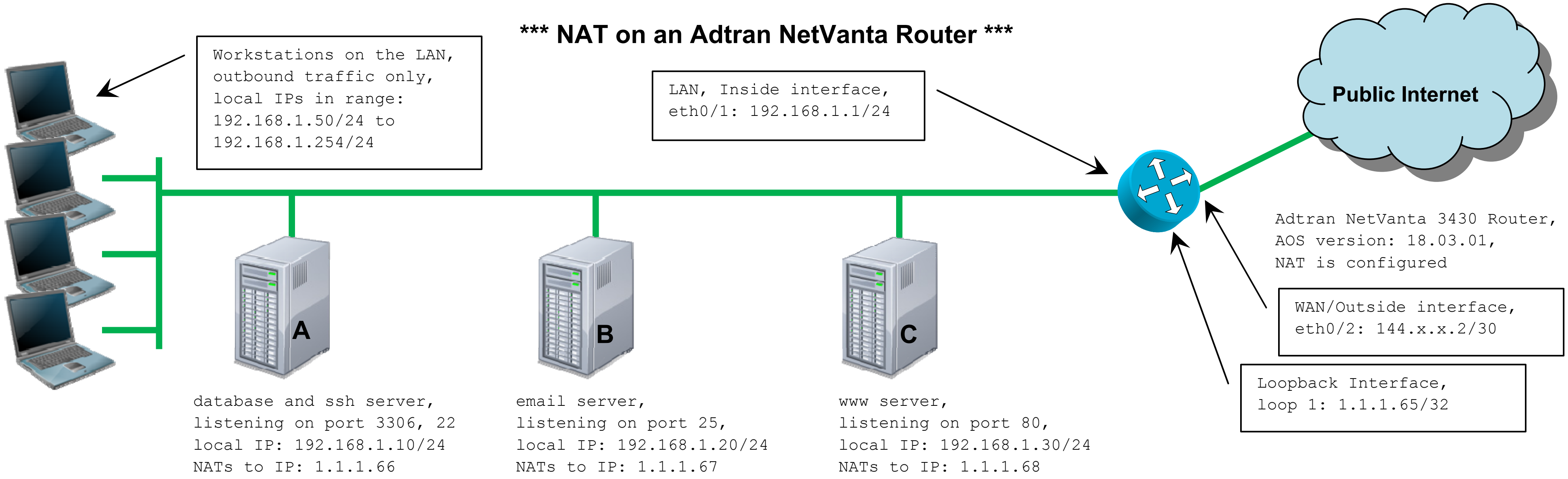
*** NAT on an Adtran NetVanta Router ***



```
Workstations on the LAN,
outbound traffic only,
local IPs in range:
192.168.1.50/24 to
192.168.1.254/24
```

```
LAN, Inside interface,
eth0/1: 192.168.1.1/24
```

```
Adtran NetVanta 3430 Router,
AOS version: 18.03.01,
NAT is configured
```

```
WAN/Outside interface,
eth0/2: 144.x.x.2/30
```

```
Loopback Interface,
loop 1: 1.1.1.65/32
```

```
database and ssh server,
listening on port 3306, 22
local IP: 192.168.1.10/24
NATs to IP: 1.1.1.66
```

```
email server,
listening on port 25,
local IP: 192.168.1.20/24
NATs to IP: 1.1.1.67
```

```
www server,
listening on port 80,
local IP: 192.168.1.30/24
NATs to IP: 1.1.1.68
```

Name	Private IP	Listening Ports	NATs To This IP	Comments
Server A	192.168.1.10	3306, 22	1.1.1.66	NAT for inbound & outbound traffic
Server B	192.168.1.20	25	1.1.1.67	NAT for inbound & outbound traffic
Server C	192.168.1.30	80	1.1.1.68	NAT for inbound & outbound traffic
Workstations	Range: 192.168.1.50 to .254	N/A	1.1.1.65	NAT for outbound traffic only

Summary

1. Servers A, B, and C are accessible from the public Internet and each server statically NATs to their own, unique, single public IP
    a. Each server NATs to the same public IP for both inbound *and* outbound traffic
2. All other workstations on the LAN statically NAT (outbound) to a single public IP address (1.1.1.65) (referred to as "NAT overload")
3. Examples
    a. Example 1: Server A sends a packet to the Internet; on the Internet, that packet has a source IP of 1.1.1.66
    b. Example 2: Server C sends a packet to the Internet; on the Internet, that packet has a source IP of 1.1.1.68
    c. Example 3: A workstation sends a packet to the Internet; on the Internet, that packet has a source IP of 1.1.1.65
    d. Example 4: A second workstation sends a packet to the Internet; on the Internet, that packet has a source IP of 1.1.1.65
    e. Example 5: A packet coming from the Internet has a destination of 1.1.1.68, the router will NAT this packet with a destination address of 192.168.1.30 (Server C)

filename: adtran_netvanta_nat_how_to
creation date: 22 june 2012

```
! ~~~ Note: only the NAT-required part of the configuration is listed here ~~~
!
ip firewall                                          <------ enable firewall (required in this case)
!
ip access-list extended ACL_1-1-1-66                 <------ ACL for server (outside to inside) NAT
  remark 1:1 outside-to-inside NAT/PAT 1.1.1.66 > 192.168.1.10
  permit tcp any host 1.1.1.66 eq 3306
  permit tcp any host 1.1.1.66 eq 22
!
ip access-list extended ACL_1-1-1-67
  remark 1:1 outside-to-inside NAT/PAT 1.1.1.67 > 192.168.1.20
  permit tcp any host 1.1.1.67 eq 25
!
ip access-list extended ACL_1-1-1-68
  remark 1:1 outside-to-inside NAT/PAT 1.1.1.68 > 192.168.1.30
  permit tcp any host 1.1.1.68 eq 80
!
ip access-list standard NAT-LAN-ACL                  <------ ACL for workstations to NAT to a single IP
  remark list used for inside-to-outside NAT for workstations
  permit 192.168.1.0 0.0.0.255
!
ip access-list extended HOST_192-168-1-10            <------ ACL for server (inside to outside) NAT
  remark 1:1 inside-to-outside NAT/PAT 192.168.1.10 > 1.1.1.66
  permit ip host 192.168.1.10 any
!
ip access-list extended HOST_192-168-1-20
  remark 1:1 inside-to-outside NAT/PAT 192.168.1.20 > 1.1.1.67
  permit ip host 192.168.1.20 any
!
ip access-list extended HOST_192-168-1-30
  remark 1:1 inside-to-outside NAT/PAT 192.168.1.30 > 1.1.1.68
  permit ip host 192.168.1.30 any
!
ip route 1.1.1.66 255.255.255.255 null 0            <------ null route required, otherwise router will send
ip route 1.1.1.67 255.255.255.255 null 0                    packets (destined for the server's NAT'd public
ip route 1.1.1.68 255.255.255.255 null 0                    IP) to the default route. Without the null route,
ip route 0.0.0.0 0.0.0.0 144.x.x.1                          the router does not have an explicit route for
!                                                           1.1.1.x in its routing table
!
ip policy-class UNTRUSTED
  nat destination list ACL_1-1-1-66 address 192.168.1.10        <------ outside to inside NAT statement
  nat destination list ACL_1-1-1-67 address 192.168.1.20        <------ observe you should list NAT
  nat destination list ACL_1-1-1-68 address 192.168.1.30                statements *before* any "allow"
!                                                                       or "discard" lists in the policy-
!                                                                       class
ip policy-class TRUSTED
  nat source list HOST_192-168-1-10 address 1.1.1.66 overload   <------ inside to outside NAT statement
  nat source list HOST_192-168-1-20 address 1.1.1.67 overload   <------ observe "overload" is required
  nat source list HOST_192-168-1-30 address 1.1.1.68 overload   <------ observe server NAT lines listed first
  nat source list NAT-LAN-ACL interface loop 1 overload         <------ workstations NAT to a single IP,
!                                                                       observe workstations NAT line listed
!                                                                       last but before any "allow" or
interface loop 1                                                        "discard" lists
  description NAT overload interface for workstations
  ip address 1.1.1.65 255.255.255.255
!
interface eth 0/1
  description LAN/inside interface
  ip address 192.168.1.1 255.255.255.0
  ip access-policy TRUSTED                   <------ apply TRUSTED policy-class to LAN/inside interface
!
interface eth 0/2
  description WAN/outside interface
  ip address 144.x.x.2 255.255.255.252
  ip access-policy UNTRUSTED                 <------ apply UNTRUSTED policy-class to WAN/outside interface
!
end
```