Technical Tip

TT-0411404a -- Information -- 22-Nov-2004

NORTEL

Alteon NAT

Contents:

Introduction: 1
Associated Products: 1
Sample Configurations....2
- Static one-to-one NAT 2
  - Setup 2
  - Configuring PC1 2
  - Configuring PC2 3
  - Configuring Alteon 3
  - Testing the configuration 10
- Static many-to-many NAT 11
  - Setup 11
  - Configuring PC1, PC2 11
  - Configuring PC3 12
  - Configuring Alteon 12
  - Testing the configuration 14
- Dynamic NAT 21
  - Setup 21
  - Configuring PC1, PC3 22
  - Configuring PC2 22
  - Configuring Alteon 26
  - Testing the configuration 31
- FTP and dynamic NAT 36
  - Setup 37
  - Configuring PC1 37
  - Configuring PC2 37
  - Configuring Alteon 40
  - Testing the configuration 41

Appendix A. Static one-to-one NAT configuration 46
Appendix B. Static many-to-many NAT configuration 47

Introduction:

Shows sample configurations of Network Address Translation (NAT) on Alteon switches.

Associated Products:

The information in this document is intended to be used with the following product(s) with the indicated software or hardware revisions:

Product Name or Order Number	Revision Information	
	Potentially Affected	*Corrected*
Alteon WebOS and Application switches: 180e, 180 Plus, 184, AD2, AD2, AD4, 2224, 2424, 2208, 2216, 3408	All	N/A

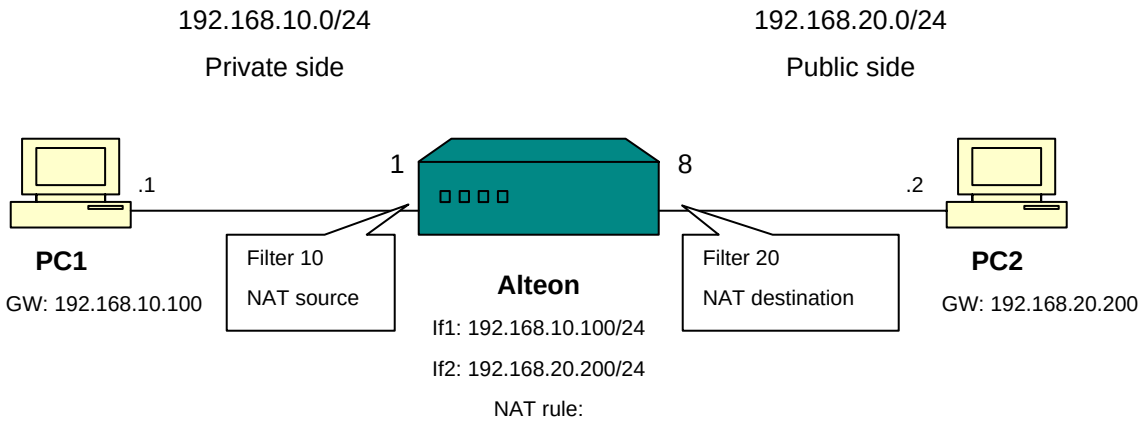
©2005 Nortel Networks Limited. All Rights Reserved

Sample Configurations

Four samples are shown: static one-to-one NAT, static many-to-many NAT, dynamic NAT, and FTP and dynamic NAT

Static one-to-one NAT

Setup



PC1 – Windows 2000 workstation with Ethereal packet capturing software installed, IP address 192.168.10.1/24;
PC2 – Windows 2000 workstation with Ethereal packet capturing software installed, IP address 192.168.20.2/24;
Alteon – Alteon AD3, code version 10.0.3.7, interface 1 IP 192.168.10.100/24, interface 2 IP 192.168.20.200/24.

The goal of the configuration is to set up a static one-to-one NAT rule translating PC1 private IP (192.168.10.1) address into public IP (192.168.20.150) address.

Configuring PC1

Configure IP address (192.168.10.1/24) on PC1 with Alteon interface 1 (192.168.10.100) as a default gateway:

```
C:\>ipconfig

Windows 2000 IP Configuration
Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.10.1
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.10.100
```

©2005 Nortel Networks Limited. All Rights Reserved

Configuring PC2

Configure IP address (192.168.20.2/24) on PC2 with Alteon interface 2 (192.168.20.200) as a default gateway:

```
C:\>ipconfig

Windows 2000 IP Configuration
Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.20.2
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.20.200
```

Configuring Alteon

Note: This sample configuration is started from factory default settings.

1. Log in to the switch.

```
Enter password:
System Information at 11:05:11 Wed Apr 21, 2004
Alteon AD3
sysName:
sysLocation:
. . .
```

2. Select **n** to not run the setup script:

```
The switch is booted with factory default configuration.
  To ease the configuration of the switch, a "Set Up" facility which
  will prompt you with those configuration items that are essential
  to the operation of the switch is provided.
Would you like to run "Set Up" to configure the switch? [y/n] n
```

Configuring interfaces

1. Configure Interface 1.
    a) Enter interface 1 configuration menu:

```
>> Main# /cfg/ip/if 1
------------------------------------------------------------
[IP Interface 1 Menu]
      addr    - Set IP address
      mask    - Set subnet mask
      broad   - Set broadcast address
      vlan    - Set VLAN number
      relay   - Enable/disable BOOTP relay
      ena     - Enable IP interface
      dis     - Disable IP interface
      del     - Delete IP interface
      cur     - Display current interface configuration
```

©2005 Nortel Networks Limited. All Rights Reserved

b) Set mask (255.255.255.0), address (192.168.10.100) and enable the interface.

Note: If address is specified before the mask, a broadcast address must be entered using **broad** command.

```
>> IP Interface 1# mask 255.255.255.0/addr 192.168.10.100/ena
Current subnet mask:     0.0.0.0
New pending subnet mask: 255.255.255.0
Current IP address:     0.0.0.0
New pending IP address: 192.168.10.100
Pending new broadcast address:  192.168.10.255
Current status: disabled
New status:     enabled
```

2. Configure interface 2.
   a) Enter interface 2 configuration menu:

```
>> IP Interface 1# /cfg/ip/if 2
------------------------------------------------------------
[IP Interface 2 Menu]
      addr    - Set IP address
      mask    - Set subnet mask
      broad   - Set broadcast address
      vlan    - Set VLAN number
      relay   - Enable/disable BOOTP relay
      ena     - Enable IP interface
      dis     - Disable IP interface
      del     - Delete IP interface
      cur     - Display current interface configuration
```

   b) Set the mask (255.255.255.0) and address (192.168.20.200) for the interface. Enable the interface:

```
>> IP Interface 2# mask 255.255.255.0/addr 192.168.20.200/ena
Current subnet mask:     0.0.0.0
New pending subnet mask: 255.255.255.0
Current IP address:     0.0.0.0
New pending IP address: 192.168.20.200
Pending new broadcast address:  192.168.20.255
Current status: disabled
New status:     enabled
```

3. Apply and save the changes:

```
>> IP Interface 2# apply/save
------------------------------------------------------------------
Apply complete; don't forget to "save" updated configuration.
Request will first copy the FLASH "active" config to "backup",
 then overlay FLASH "active" with new config.
Confirm saving to FLASH [y/n]: y
New config successfully saved to FLASH.
Switch is currently set to use factory default config block on next boot.
Do you want to change that to the active config block? [y/n] y
Next boot will use active config block.
```

©2005 Nortel Networks Limited. All Rights Reserved

4. Verify connectivity to PC1 and PC2 using ping:

```
>> IP Interface 2# ping 192.168.10.1
[host 192.168.10.1, max tries 5, delay 1000 msec]
192.168.10.1: #1 ok, RTT 1 msec.
192.168.10.1: #2 ok, RTT 0 msec.
192.168.10.1: #3 ok, RTT 1 msec.
192.168.10.1: #4 ok, RTT 1 msec.
192.168.10.1: #5 ok, RTT 1 msec.
Ping finished.
```

```
>> IP Interface 2# ping 192.168.20.2
[host 192.168.20.2, max tries 5, delay 1000 msec]
192.168.20.2: #1 ok, RTT 1 msec.
192.168.20.2: #2 ok, RTT 1 msec.
192.168.20.2: #3 ok, RTT 1 msec.
192.168.20.2: #4 ok, RTT 1 msec.
192.168.20.2: #5 ok, RTT 1 msec.
Ping finished.
```

Configuring NAT filters

1. Create NAT source rule. Filter 10 is created to define source address translation.

    a) Create filter 10:

```
>> IP Interface 2# /cfg/slb/filt 10
------------------------------------------------------------
[Filter 10   Menu]
      adv     - Filter Advanced Menu
      name    - Set filter name
      smac    - Set source MAC address
      dmac    - Set destination MAC address
      sip     - Set source IP address
      smask   - Set source IP mask
      dip     - Set destination IP address
      dmask   - Set destination IP mask
      proto   - Set IP protocol
      sport   - Set source TCP/UDP port or range
      dport   - Set destination TCP/UDP port or range
      action  - Set action
      group   - Set real server group for redirection
      rport   - Set real server port for redirection
      nat     - Set which addresses are network address translated
      invert  - Enable/disable filter inversion
      ena     - Enable filter
      dis     - Disable filter
      del     - Delete filter
      cur     - Display current filter configuration
```

    b) Set NAT action for the filter:

```
>> Filter 10  # action nat
Current action: allow
Pending new action:     nat
```

©2005 Nortel Networks Limited. All Rights Reserved

c) Set NAT filter to translate source address:

```
>> Filter 10  # nat source
Current NAT addresses:  dest
Pending new NAT addresses:      source
```

d) Set source IP address to 192.168.10.1:

```
>> Filter 10  # sip 192.168.10.1
Current source address:     any
New pending source address: 192.168.10.1
```

e) Set source address mask to 255.255.255.255 (this will translate only one address):

```
>> Filter 10  # smask 255.255.255.255
Current source mask:     0.0.0.0
New pending source mask: 255.255.255.255
```

f) Set destination IP address to 192.168.20.150 (address to translate the source to):

```
>> Filter 10  # dip 192.168.20.150
Current destination address:     any
New pending destination address: 192.168.20.150
```

g) Set the destination mask to 255.255.255.255:

```
>> Filter 10  # dmask 255.255.255.255
Current destination mask:     0.0.0.0
New pending destination mask: 255.255.255.255
```

h) Enable the filter:

```
>> Filter 10  # ena
Current status: disabled
New status:     enabled
```

i) Disable proxy and optionally enable logging of this filter:

```
>> Filter 10  # adv/proxy d
Current client proxy: enabled
New client proxy:     disabled
```

```
>> Filter 10 Advanced# log e
Current logging: disabled
New logging:     enabled
```

©2005 Nortel Networks Limited. All Rights Reserved

2. Create NAT destination rule. Filter 20 is created to configure destination address translation.

    a) Create filter 20:

```
>> Filter 10 Advanced# /cfg/slb/filt 20
------------------------------------------------------------
[Filter 20   Menu]
      adv     - Filter Advanced Menu
      name    - Set filter name
      smac    - Set source MAC address
      dmac    - Set destination MAC address
      sip     - Set source IP address
      smask   - Set source IP mask
      dip     - Set destination IP address
      dmask   - Set destination IP mask
      proto   - Set IP protocol
      sport   - Set source TCP/UDP port or range
      dport   - Set destination TCP/UDP port or range
      action  - Set action
      group   - Set real server group for redirection
      rport   - Set real server port for redirection
      nat     - Set which addresses are network address translated
      invert  - Enable/disable filter inversion
      ena     - Enable filter
      dis     - Disable filter
      del     - Delete filter
      cur     - Display current filter configuration
```

    b) Set NAT action for the filter:

```
>> Filter 20  # action nat
Current action: allow
Pending new action:     nat
```

    c) Set NAT filter to translate destination address:

```
>> Filter 20  # nat dest
Current NAT addresses:  dest
Pending new NAT addresses:      dest
```

    d) Set source IP address to 192.168.10.1:

```
>> Filter 20  # sip 192.168.10.1
Current source address:     any
New pending source address: 192.168.10.1
```

    e) Set source address mask to 255.255.255.255 (this will translate only one address):

```
>> Filter 20  # smask 255.255.255.255
Current source mask:     0.0.0.0
New pending source mask: 255.255.255.255
```

©2005 Nortel Networks Limited. All Rights Reserved

f) Set destination IP address to 192.168.20.150 (address to translate the source to):

```
>> Filter 20  # dip 192.168.20.150
Current destination address:     any
New pending destination address: 192.168.20.150
```

g) Set the destination mask to 255.255.255.255:

```
>> Filter 20  # dmask 255.255.255.255
Current destination mask:     0.0.0.0
New pending destination mask: 255.255.255.255
```

h) Enable the filter:

```
>> Filter 20  # ena
Current status: disabled
New status:     enabled
```

i) Disable proxy and optionally enable logging of this filter:

```
>> Filter 20  # adv/proxy d
Current client proxy: enabled
New client proxy:     disabled
```

```
>> Filter 20 Advanced# log e
Current logging: disabled
New logging:     enabled
```

3. Apply and save the changes:

```
>> Filter 20  # apply/save
------------------------------------------------------------------
Apply complete; don't forget to "save" updated configuration.
Request will first copy the FLASH "active" config to "backup",
 then overlay FLASH "active" with new config.
Confirm saving to FLASH [y/n]: y
New config successfully saved to FLASH.
```

Note: The only difference between the source (filter 10) and destination (filter 20) filters is the NAT direction setting – source (filter 10) or destination (filter 20).

Applying filters to ports

Apply the configured filters to appropriate ports.
PC1 (private side) is connected to the port 1 of the switch, so source filter is applied to port 1.

1. Enter SLB port configuration menu:

```
>> Filter 20 Advanced# /cfg/slb/port 1
------------------------------------------------------------
[SLB port 1 Menu]
      client  - Enable/disable client processing
      server  - Enable/disable server processing
      rts     - Enable/disable RTS processing
      hotstan - Enable/disable hot-standby processing
      intersw - Enable/disable inter-switch processing
      proxy   - Enable/disable use of PIP for ingress traffic
      pip     - Set Proxy IP address for port
      filt    - Enable/disable filtering
      add     - Add filter to port
      rem     - Remove filter from port
```

©2005 Nortel Networks Limited. All Rights Reserved

```
      idslb   - Enable/disable intrusion detection server load balancing
      cur     - Display current port configuration
```

2. Add filter 10 to the port:

```
>> SLB port 1# add 10
Filter 10 added to port 1.
```

3. Enable filtering on the port:

```
>> SLB port 1# filt en
Current port 1 filtering: disabled
New port 1 filtering:     enabled
```

PC2 (public side) is connected to port 8, so destination filter is applied to port 8.

4. Enter SLB port 8 configuration menu:

```
>> SLB port 1# /cfg/slb/port 8
------------------------------------------------------------
[SLB port 8 Menu]
      client  - Enable/disable client processing
      server  - Enable/disable server processing
      rts     - Enable/disable RTS processing
      hotstan - Enable/disable hot-standby processing
      intersw - Enable/disable inter-switch processing
      proxy   - Enable/disable use of PIP for ingress traffic
      pip     - Set Proxy IP address for port
      filt    - Enable/disable filtering
      add     - Add filter to port
      rem     - Remove filter from port
      idslb   - Enable/disable intrusion detection server load balancing
      cur     - Display current port configuration
```

5. Add filter 20 to the port:

```
>> SLB port 8# add 20
Filter 20 added to port 8.
```

6. Enable filtering on the port:

```
>> SLB port 8# filt e
Current port 8 filtering: disabled
New port 8 filtering:     enabled
```

Enabling SLB

1. Enable SLB globally:

```
>> SLB port 8# /cfg/slb/on
Current status: OFF
New status:     ON
```

2. Apply and save the changes:

```
>> Layer 4# apply/save
------------------------------------------------------------------
Apply complete; don't forget to "save" updated configuration.
Request will first copy the FLASH "active" config to "backup",
 then overlay FLASH "active" with new config.
Confirm saving to FLASH [y/n]: y
New config successfully saved to FLASH.
```

©2005 Nortel Networks Limited. All Rights Reserved

Testing the configuration

1. Clear the log on Alteon:

```
>> Layer 4# /info/clrlog
```

2. Start a capture on PC1 and PC2 using, for example, Ethereal and ping from PC1 to PC2:

```
C:\>ping 192.168.20.2

Pinging 192.168.20.2 with 32 bytes of data:

Reply from 192.168.20.2: bytes=32 time<10ms TTL=63
Reply from 192.168.20.2: bytes=32 time<10ms TTL=63
Reply from 192.168.20.2: bytes=32 time<10ms TTL=63
Reply from 192.168.20.2: bytes=32 time<10ms TTL=63

Ping statistics for 192.168.20.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms
```

PC1 was able to ping PC2.

3. Check the captured on PC1 and PC2 traffic.

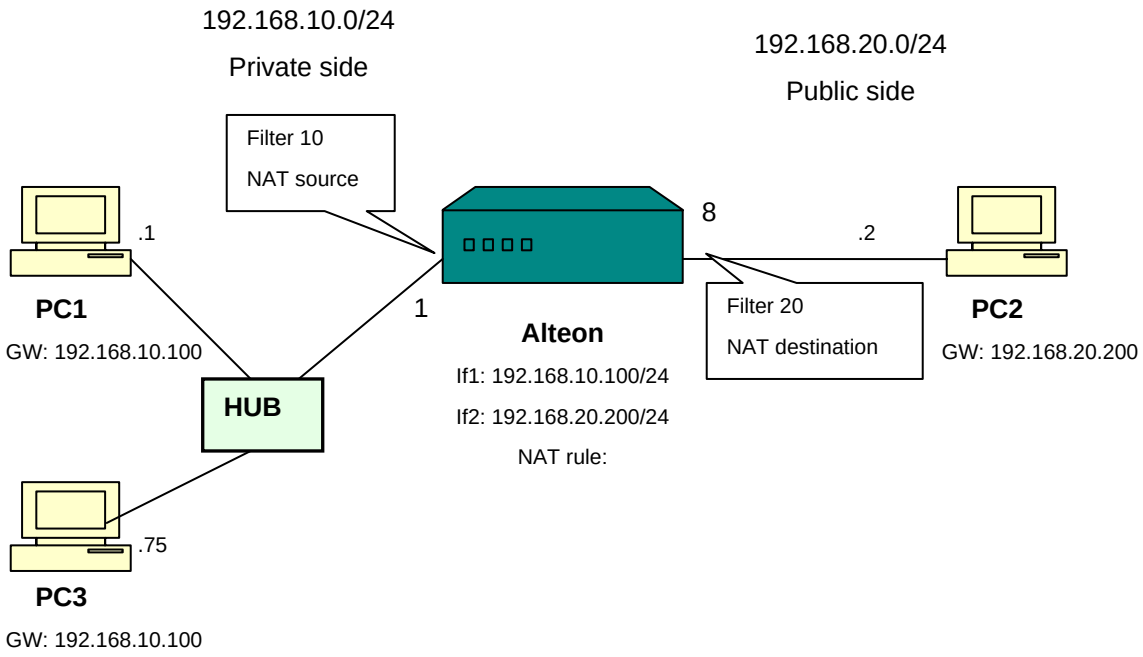
PC1 sends ARP request to resolve default gateway's IP address (192.168.10.100) to MAC address:

```
Frame 1 (42 bytes on wire, 42 bytes captured)
Ethernet II, Src: 00:08:74:9a:e5:85, Dst: ff:ff:ff:ff:ff:ff
Address Resolution Protocol (request)
    Hardware type: Ethernet (0x0001)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (0x0001)
    Sender MAC address: 00:08:74:9a:e5:85 (DellComp_9a:e5:85)
    Sender IP address: 192.168.10.1 (192.168.10.1)
    Target MAC address: 00:00:00:00:00:00 (00:00:00_00:00:00)
    Target IP address: 192.168.10.100 (192.168.10.100)
```

©2005 Nortel Networks Limited. All Rights Reserved

Static many-to-many NAT

Setup



PC1 – Windows 2000 workstation with Ethereal packet capturing software installed, IP address 192.168.10.1/24;
PC2 – Windows 2000 workstation with Ethereal packet capturing software installed, IP address 192.168.20.2/24;
PC3 - Windows 2000 workstation with Ethereal packet capturing software installed, IP address 192.168.10.75/24;
Alteon – Alteon AD3, code version 10.0.3.7, interface 1 IP 192.168.10.100/24, interface 2 IP 192.168.20.200/24;
HUB – Ethernet HUB.

The goal of the configuration is to set up a static many-to-many NAT rule translating private addresses from 192.168.10.0/24 network to public addresses from 192.168.20.0/24 network.

Configuring PC1, PC2

PC1 and PC2 are configured exactly as they were configured in the previous example. Please refer to PC1 and PC2 configuration in the previous example.

©2005 Nortel Networks Limited. All Rights Reserved

Configuring PC3

Configure IP address (192.168.10.75/24) on PC3 with Alteon interface 1 (192.168.10.100) as a default gateway:

```
C:\>ipconfig

Windows 2000 IP Configuration
Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.10.75
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.10.100
```

Configuring Alteon

Configuration is based on the configuration of Alteon in the previous example. Please refer to configuration of Alteon in the previous example. Only the differences are noted.

1. Enter the source filter 10 configuration menu from the previous example:

```
>> Main# /cfg/slb/filt 10
------------------------------------------------------------
[Filter 10   Menu]
      adv     - Filter Advanced Menu
      name    - Set filter name
      smac    - Set source MAC address
      dmac    - Set destination MAC address
      sip     - Set source IP address
      smask   - Set source IP mask
      dip     - Set destination IP address
      dmask   - Set destination IP mask
      proto   - Set IP protocol
      sport   - Set source TCP/UDP port or range
      dport   - Set destination TCP/UDP port or range
      action  - Set action
      group   - Set real server group for redirection
      rport   - Set real server port for redirection
      nat     - Set which addresses are network address translated
      invert  - Enable/disable filter inversion
      ena     - Enable filter
      dis     - Disable filter
      del     - Delete filter
      cur     - Display current filter configuration
```

2. Change the source IP to 192.168.10.0:

```
>> Filter 10  # sip 192.168.10.0
Current source address:     192.168.10.1
New pending source address: 192.168.10.0
```

3. Set the source mask to 255.255.255.0:

```
>> Filter 10  # smask 255.255.255.0
Current source mask:     255.255.255.255
New pending source mask: 255.255.255.0
```

4. Set the destination address to 192.168.20.0:

```
>> Filter 10  # dip 192.168.20.0
```

©2005 Nortel Networks Limited. All Rights Reserved

```
Current destination address:     192.168.20.150
New pending destination address: 192.168.20.0
```

5. Set the destination mask to 255.255.255.0:

```
>> Filter 10  # dmask 255.255.255.0
Current destination mask:     255.255.255.0
New pending destination mask: 255.255.255.0
```

6. Enter destination filter 20 configuration menu:

```
>> Filter 10  # /cfg/slb/filt 20
------------------------------------------------------------
[Filter 20   Menu]
      adv     - Filter Advanced Menu
      name    - Set filter name
      smac    - Set source MAC address
      dmac    - Set destination MAC address
      sip     - Set source IP address
      smask   - Set source IP mask
      dip     - Set destination IP address
      dmask   - Set destination IP mask
      proto   - Set IP protocol
      sport   - Set source TCP/UDP port or range
      dport   - Set destination TCP/UDP port or range
      action  - Set action
      group   - Set real server group for redirection
      rport   - Set real server port for redirection
      nat     - Set which addresses are network address translated
      invert  - Enable/disable filter inversion
      ena     - Enable filter
      dis     - Disable filter
      del     - Delete filter
      cur     - Display current filter configuration
```

7. Apply to filter 20 the same changes that were applied to filter 10:

```
>> Filter 20  # sip 192.168.10.0
Current source address:     192.168.10.1
New pending source address: 192.168.10.0
```

```
>> Filter 20  # smask 255.255.255.0
Current source mask:     255.255.255.255
New pending source mask: 255.255.255.0
```

```
>> Filter 20  # dip 192.168.20.0
Current destination address:     192.168.20.150
New pending destination address: 192.168.20.0
```

```
>> Filter 20  # dmask 255.255.255.0
Current destination mask:     255.255.255.255
New pending destination mask: 255.255.255.0
```

©2005 Nortel Networks Limited. All Rights Reserved

8. Apply and save the changes:

```
>> Filter 20  # apply/save
------------------------------------------------------------------
Apply complete; don't forget to "save" updated configuration.
Request will first copy the FLASH "active" config to "backup",
 then overlay FLASH "active" with new config.
Confirm saving to FLASH [y/n]: y
New config successfully saved to FLASH.
```

Testing the configuration

1. Clear the log on Alteon:

```
>> Filter 20  # /info/clrlog
```

2. Start a capture on PC1, PC2 and PC3 using for example Ethereal.

3. Ping from PC1 (192.168.10.1) to PC2 (192.168.20.2):

```
C:\>ping 192.168.20.2

Pinging 192.168.20.2 with 32 bytes of data:

Reply from 192.168.20.2: bytes=32 time=10ms TTL=63
Reply from 192.168.20.2: bytes=32 time<10ms TTL=63
Reply from 192.168.20.2: bytes=32 time<10ms TTL=63
Reply from 192.168.20.2: bytes=32 time<10ms TTL=63

Ping statistics for 192.168.20.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  10ms, Average =  2ms
```

4. Ping from PC3 (192.168.10.75) to PC2 (192.168.20.2):

```
C:\>ping 192.168.20.2

Pinging 192.168.20.2 with 32 bytes of data:

Reply from 192.168.20.2: bytes=32 time=10ms TTL=63
Reply from 192.168.20.2: bytes=32 time<10ms TTL=63
Reply from 192.168.20.2: bytes=32 time<10ms TTL=63
Reply from 192.168.20.2: bytes=32 time<10ms TTL=63

Ping statistics for 192.168.20.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  10ms, Average =  2ms
```

©2005 Nortel Networks Limited. All Rights Reserved

5. Check the log on Alteon.

Note: Filter 10 fired upon receiving ICMP traffic from 192.168.10.1 (PC1 private IP) to 192.168.20.2 (PC2) and upon receiving ICMP traffic from 192.168.10.75 (PC3 private side) to 192.168.20.2 (PC2).
Filter 20 fired upon receiving ICMP traffic from 192.168.20.2 (PC2) to 192.168.20.1 (PC1 public IP) and upon receiving ICMP traffic from 192.168.20.2 (PC2) to 192.168.20.75 (PC3 public IP):

```
>> Information# log
May  7 14:50:11 WARNING slb: filter 10 fired on port 1, icmp 192.168.10.1 ->
192.168.20.2, type 8
May  7 14:50:11 WARNING slb: filter 20 fired on port 8, icmp 192.168.20.2 ->
192.168.20.1, type 0
May  7 14:50:18 WARNING slb: filter 10 fired on port 1, icmp 192.168.10.75 ->
192.168.20.2, type 8
May  7 14:50:18 WARNING slb: filter 20 fired on port 8, icmp 192.168.20.2 ->
192.168.20.75, type 0
```

6. Check the captured traffic.

PC1 (192.168.10.1) sends an ICMP request to PC2 (192.168.20.2):

```
Frame 10 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:e0:7b:04:fb:00, Dst: 00:60:cf:46:53:60
Internet Protocol, Src Addr: 192.168.20.2 (192.168.20.2), Dst Addr: 192.168.20.1
(192.168.20.1)
Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x0b5c (correct)
    Identifier: 0x0300
    Sequence number: 0x4700
    Data (32 bytes)
```

Alteon receives a packet on its port 1, checks whether filter is enabled on the port. With NAT source filter 10 being enabled, Alteon compares packet to the filter defined criteria. With packet matching the filter, the configured NAT source translation action is applied and Alteon changes the private IP (192.168.10.1) source address to public IP (192.168.20.1) source address and forwards the request to PC2 (192.168.20.2):

```
Frame 9 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:60:cf:46:53:60, Dst: 00:e0:7b:04:fb:00
Internet Protocol, Src Addr: 192.168.20.1 (192.168.20.1), Dst Addr: 192.168.20.2
(192.168.20.2)
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x035c (correct)
    Identifier: 0x0300
    Sequence number: 0x4700
    Data (32 bytes)
```

©2005 Nortel Networks Limited. All Rights Reserved

PC2 receives an ICMP request and replies with ICMP reply:

```
Frame 10 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:e0:7b:04:fb:00, Dst: 00:60:cf:46:53:60
Internet Protocol, Src Addr: 192.168.20.2 (192.168.20.2), Dst Addr: 192.168.20.1
(192.168.20.1)
Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x0b5c (correct)
    Identifier: 0x0300
    Sequence number: 0x4700
    Data (32 bytes)
```

Alteon receives an ICMP reply from PC2 on its port 8. With filter 20 being enabled on port, Alteon compares the packet with filter criteria. With packet matching the criteria, Alteon performs the configured destination NAT translation action and changes the public destination address (192.168.20.1) to private destination address (192.168.10.1) and forwards the packet to PC1:

```
Frame 10 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:60:cf:46:53:60, Dst: 00:08:74:9a:e5:85
Internet Protocol, Src Addr: 192.168.20.2 (192.168.20.2), Dst Addr: 192.168.10.1
(192.168.10.1)
Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x0c5c (correct)
    Identifier: 0x0300
    Sequence number: 0x4600
    Data (32 bytes)
```

When PC3 pings PC2 the same procedure is applied to the packet.

PC3 (192.168.10.75) sends an ICMP request to PC2 (192.168.20.2):

```
Frame 21 (98 bytes on wire, 98 bytes captured)
Ethernet II, Src: 00:0c:29:4d:f9:8c, Dst: 00:60:cf:46:53:60
Internet Protocol, Src Addr: 192.168.10.75 (192.168.10.75), Dst Addr: 192.168.20.2
(192.168.20.2)
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x73c8 (correct)
    Identifier: 0xfb11
    Sequence number: 0x0100
    Data (56 bytes)
```

©2005 Nortel Networks Limited. All Rights Reserved

Alteon receives the packet on port 1, checks it against the filter enabled on the port and performs the configured action – translates private source IP address (192.168.10.75) to public IP address (192.168.20.75) and forwards the packet to PC2:

```
Frame 16 (98 bytes on wire, 98 bytes captured)
Ethernet II, Src: 00:60:cf:46:53:60, Dst: 00:e0:7b:04:fb:00
Internet Protocol, Src Addr: 192.168.20.75 (192.168.20.75), Dst Addr: 192.168.20.2
(192.168.20.2)
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x73c8 (correct)
    Identifier: 0xfb11
    Sequence number: 0x0100
    Data (56 bytes)
```

PC2 responds to ICMP request:

```
Frame 19 (98 bytes on wire, 98 bytes captured)
Ethernet II, Src: 00:e0:7b:04:fb:00, Dst: 00:60:cf:46:53:60
Internet Protocol, Src Addr: 192.168.20.2 (192.168.20.2), Dst Addr: 192.168.20.75
(192.168.20.75)
Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x7bc8 (correct)
    Identifier: 0xfb11
    Sequence number: 0x0100
    Data (56 bytes)
```

Alteon receives the reply on its port 8, checks whether filter is enabled on the port and performs the configured action – translates public destination address (192.168.20.75) to private destination address (192.168.10.75) and forwards the packet to PC3:

```
Frame 24 (98 bytes on wire, 98 bytes captured)
Ethernet II, Src: 00:60:cf:46:53:60, Dst: 00:0c:29:4d:f9:8c
Internet Protocol, Src Addr: 192.168.20.2 (192.168.20.2), Dst Addr: 192.168.10.75
(192.168.10.75)
Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x7bc8 (correct)
    Identifier: 0xfb11
    Sequence number: 0x0100
    Data (56 bytes)
```

©2005 Nortel Networks Limited. All Rights Reserved

As Alteon owns the 192.168.10.100 address, it responds to an ARP query with an ARP response and provides its MAC:

```
Frame 3 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: 00:60:cf:46:53:60, Dst: 00:08:74:9a:e5:85
Address Resolution Protocol (reply)
    Hardware type: Ethernet (0x0001)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (0x0002)
    Sender MAC address: 00:60:cf:46:53:60 (AlteonNe_46:53:60)
    Sender IP address: 192.168.10.100 (192.168.10.100)
    Target MAC address: 00:08:74:9a:e5:85 (DellComp_9a:e5:85)
    Target IP address: 192.168.10.1 (192.168.10.1)
```

Once PC1 has MAC address of the default gateway, it sends ICMP request to the 192.168.20.2:

```
Frame 4 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:08:74:9a:e5:85, Dst: 00:60:cf:46:53:60
Internet Protocol, Src Addr: 192.168.10.1 (192.168.10.1), Dst Addr: 192.168.20.2
(192.168.20.2)
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x0b5c (correct)
    Identifier: 0x0300
    Sequence number: 0x3f00
    Data (32 bytes)
```

Alteon receives an ICMP packet from source 192.168.10.1 on port 1. With filter 10 being enabled on this port, Alteon checks whether packet matches the criteria of the filter. With packet matching filter's criteria the configured filter action is applied, NAT source translation in this case.
Thus Alteon translates the private source address (192.168.10.1) of the ICMP packet to the public address (192.168.20.150) and forwards the packet to the PC2:

```
Frame 2 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:60:cf:46:53:60, Dst: 00:e0:7b:04:fb:00
Internet Protocol, Src Addr: 192.168.20.150 (192.168.20.150), Dst Addr: 192.168.20.2
(192.168.20.2)
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x0b5c (correct)
    Identifier: 0x0300
    Sequence number: 0x3f00
    Data (32 bytes)
```

©2005 Nortel Networks Limited. All Rights Reserved

PC2 receives an ICMP request from 192.168.20.150 (the translated address of PC1) and ARPs for MAC of 192.168.20.150:

```
Frame 3 (42 bytes on wire, 42 bytes captured)
Ethernet II, Src: 00:e0:7b:04:fb:00, Dst: ff:ff:ff:ff:ff:ff
Address Resolution Protocol (request)
    Hardware type: Ethernet (0x0001)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (0x0001)
    Sender MAC address: 00:e0:7b:04:fb:00 (BayNetwo_04:fb:00)
    Sender IP address: 192.168.20.2 (192.168.20.2)
    Target MAC address: 00:00:00:00:00:00 (00:00:00_00:00:00)
    Target IP address: 192.168.20.150 (192.168.20.150)
```

Alteon responds to the ARP:

```
Frame 4 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: 00:60:cf:46:53:60, Dst: 00:e0:7b:04:fb:00
Address Resolution Protocol (reply)
    Hardware type: Ethernet (0x0001)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (0x0002)
    Sender MAC address: 00:60:cf:46:53:60 (AlteonNe_46:53:60)
    Sender IP address: 192.168.20.150 (192.168.20.150)
    Target MAC address: 00:e0:7b:04:fb:00 (BayNetwo_04:fb:00)
    Target IP address: 192.168.20.2 (192.168.20.2)
```

PC2 receives the ARP response and replies to ICMP reply:

```
Frame 5 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:e0:7b:04:fb:00, Dst: 00:60:cf:46:53:60
Internet Protocol, Src Addr: 192.168.20.2 (192.168.20.2), Dst Addr: 192.168.20.150
(192.168.20.150)
Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x135c (correct)
    Identifier: 0x0300
    Sequence number: 0x3f00
    Data (32 bytes)
```

©2005 Nortel Networks Limited. All Rights Reserved

Alteon receives an ICMP reply from PC2 (192.168.20.1) on its port 8. With filter 20 (NAT destination translation) being enabled on port Alteon checks whether the received packet matches the criteria of the filter. With packet matching the criteria Alteon translates the public destination address (192.168.20.150) to private PC1 IP address (192.168.10.1) and forwards the reply to PC1:

```
Frame 6 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:60:cf:46:53:60, Dst: 00:08:74:9a:e5:85
Internet Protocol, Src Addr: 192.168.20.2 (192.168.20.2), Dst Addr: 192.168.10.1
(192.168.10.1)
Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x135c (correct)
    Identifier: 0x0300
    Sequence number: 0x3f00
    Data (32 bytes)
```

7. Check the log on Alteon.

Note: Filter 10 fired upon receiving ICMP packet from 192.168.10.1 (PC1 private IP) to 192.168.20.2 (PC2) and filter 20 fired upon receiving ICMP packet from 192.168.20.2 (PC2) to 192.168.20.150 (PC1 public IP):

```
>> Information# /info/log
May  7 13:45:31 WARNING slb: filter 10 fired on port 1, icmp 192.168.10.1 ->
192.168.20.2, type 8
May  7 13:45:31 WARNING slb: filter 20 fired on port 8, icmp 192.168.20.2 ->
192.168.20.150, type 0
```

8. Issue a continues ping on PC1 and check the session table on Alteon:

```
C:\>ping 192.168.20.2 -t

Pinging 192.168.20.2 with 32 bytes of data:
Reply from 192.168.20.2: bytes=32 time<10ms TTL=63
…
```

```
>> Session Table Information# /info/slb/sess/dump
 2,1:  192.168.10.1 1, 192.168.20.2 8  NAT  age 0
 2,2:  192.168.10.1 1, 192.168.20.2 8  NAT  age 4
 7,1:  192.168.20.2 icmp, 192.168.20.150  NAT  age 0
 7,2:  192.168.20.2 icmp, 192.168.20.150  NAT  age 4
```

Note: As one-to-one static NAT rule has been configured, the public address could be used from public side to initiate connections.

©2005 Nortel Networks Limited. All Rights Reserved

9. Ping from PC2 to PC1:

```
C:\>ping 192.168.20.150

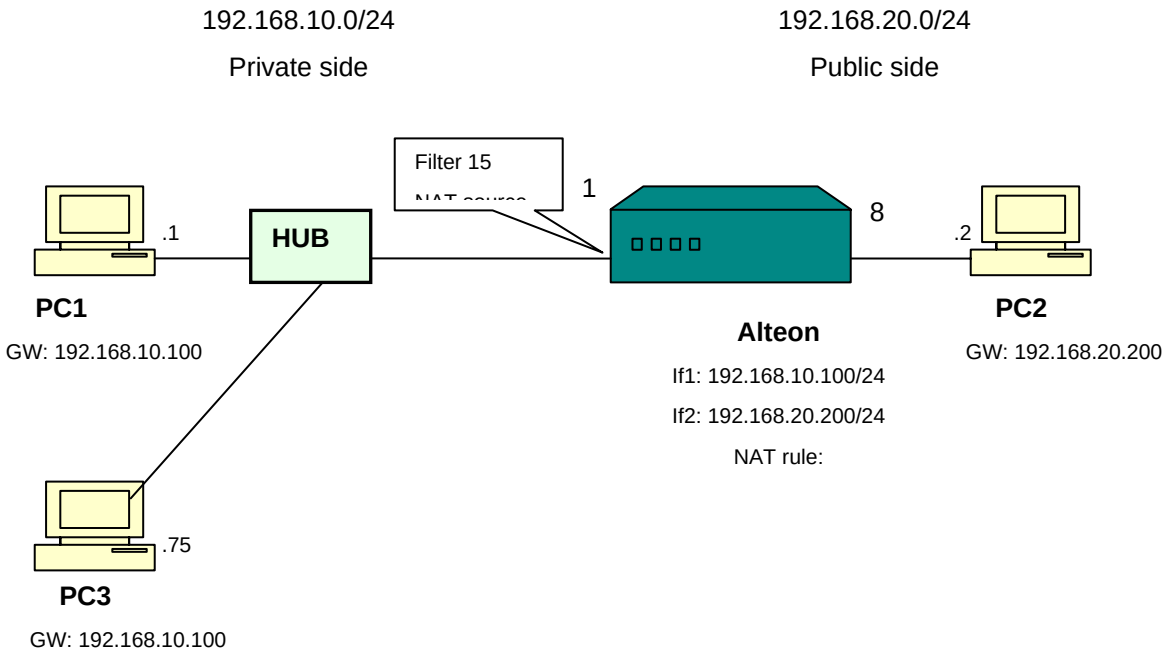
Pinging 192.168.20.150 with 32 bytes of data:

Reply from 192.168.20.150: bytes=32 time<10ms TTL=63
Reply from 192.168.20.150: bytes=32 time<10ms TTL=63
Reply from 192.168.20.150: bytes=32 time<10ms TTL=63
Reply from 192.168.20.150: bytes=32 time<10ms TTL=63

Ping statistics for 192.168.20.150:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms
```

Dynamic NAT

Setup



PC1 – Windows 2000 workstation with Ethereal packet capturing software installed, IP address 192.168.10.1/24;
PC2 – Windows 2000 workstation with Ethereal packet capturing software installed, IP address 192.168.20.2/24;
PC3 - Windows 2000 workstation with Ethereal packet capturing software installed, IP address 192.168.10.75/24;
Alteon – Alteon AD3, code version 10.0.3.7, interface 1 IP 192.168.10.100/24, interface 2 IP 192.168.20.200/24;
HUB – Ethernet HUB.

The goal of the configuration is to configure dynamic NAT translation to hide private network addresses (192.168.10.0/24) behind a single public IP address (192.168.20.150).

Note: Dynamic NAT solution applies to TCP/UDP traffic only and provides many-to-one translation.

©2005 Nortel Networks Limited. All Rights Reserved

Configuring PC1, PC3

PC1 and PC2 are configured exactly the same way they were configured in previous examples. Please refer to previous sample configurations.

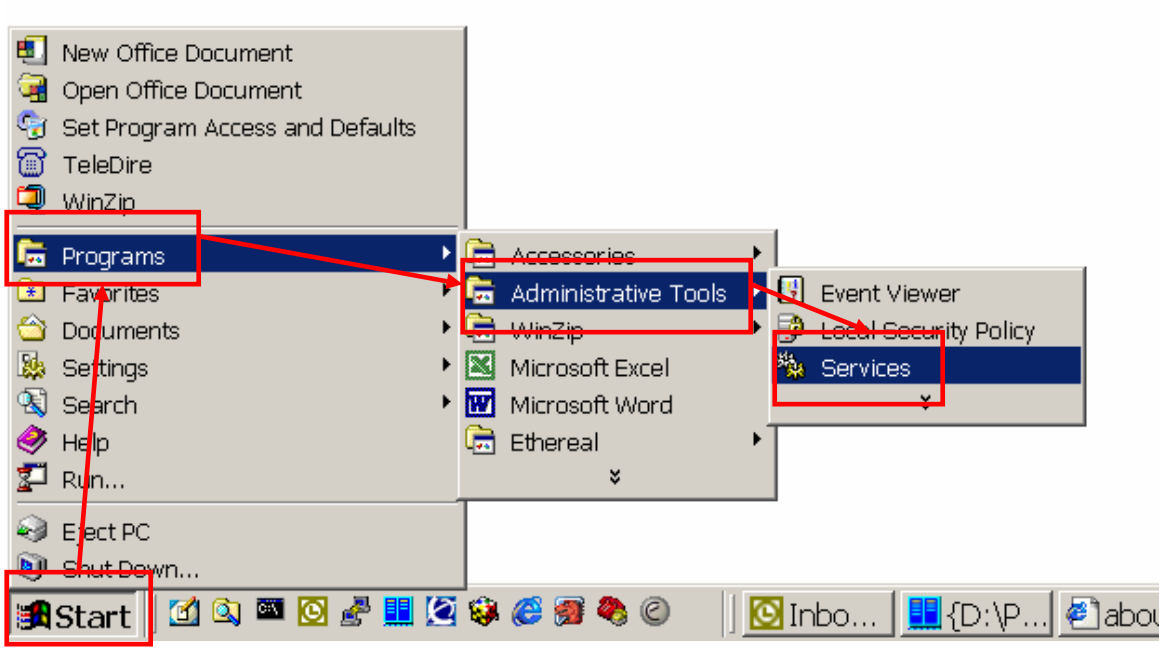
Configuring PC2

1. Configure IP address on PC2 the same way it was configured in the previous example.

As mentioned earlier, dynamic NAT can be used for applications that use TCP/UDP protocols, Telnet will be used to test the configuration in this example.

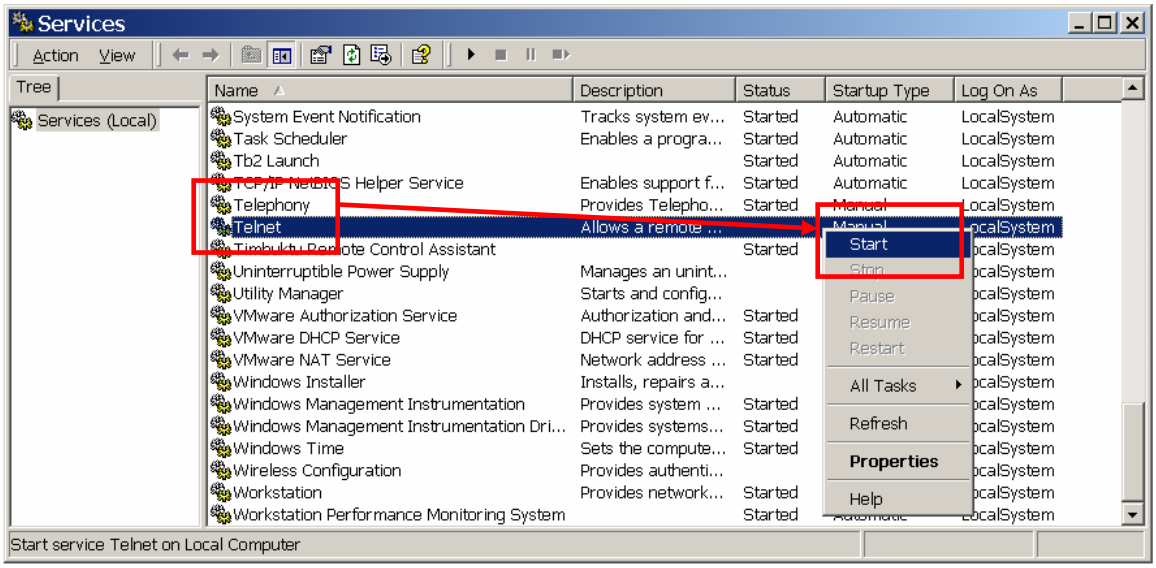
2. Enable Telnet on PC2.

    a) Navigate **Start→Programs→Administrative tools→Services**:

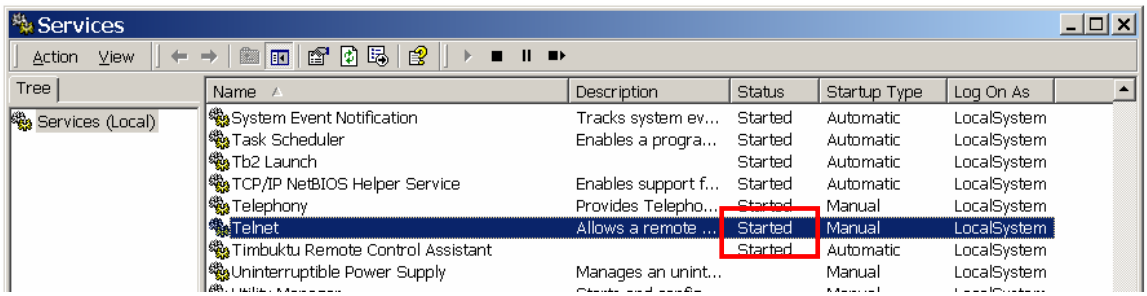


©2005 Nortel Networks Limited. All Rights Reserved

b) The **Services** window appears. Scroll down to the **Telnet** and right click on it.
c) A menu appears. Select **Start**:



Telnet service is started:



Note: Windows 2000 Telnet service has an NTLM (NT LAN Manager) authentication enabled by default preventing user credentials from being passed as clear text over the network. Telnet clients that do not use NTLM authentication will be denied access.

To allow access to users that do not support NTLM authentication, NTLM should be turned of or set to accept both NTLM and non-NTLM enabled users. Changing this setting requires administrator privileges.

To change NTLM authentication options, start Telnet Administration utility either by navigating **Start→Programs→Administrative Tools→Telnet Server Administration** or by running **`tlntadmn`** command from the DOS prompt:

```
C:\>tlntadmn
```

©2005 Nortel Networks Limited. All Rights Reserved

Telnet Administration utility starts. Select option **3**, to change Telnet settings:

```
Microsoft (R) Windows 2000 (TM) (Build 2195)
Telnet Server Admin (Build 5.00.99201.1)

Select one of the following options:


0) Quit this application
1) List the current users
2) Terminate a user session ...
3) Display / change registry settings ...
4) Start the service
5) Stop the service

Type an option number [0 - 5] to select that option: 3
```

Select option **7** for NTLM:

```
Select one of the following options:

0) Exit this menu
1) AllowTrustedDomain
2) AltKeyMapping
3) DefaultDomain
4) DefaultShell
5) LoginScript
6) MaxFailedLogins
7) NTLM
8) TelnetPort
Type an option number [0 - 8] to select that option: 7
```

The current value is displayed.
Enter **y** to change the value.
Enter **1** to allow both NTLM and non-NTLM enabled clients (server will probe NTLM first and if client does not support NTLM, server will revert to no NTLM) or **0** to completely disable NTLM:
Enter **y** to confirm new settings:

```
Current value of NTLM = 2
Do you want to change this value ? [y/n]y
NTLM [ current value = 2; acceptable values 0, 1 or 2 ] :0
Are you sure you want to set NTLM to : 0 ? [y/n]y

setting will take effect only when Telnet Service is re-started
```

©2005 Nortel Networks Limited. All Rights Reserved

Select option **0** to exit this menu:

```
Select one of the following options:

0) Exit this menu
1) AllowTrustedDomain
2) AltKeyMapping
3) DefaultDomain
4) DefaultShell
5) LoginScript
6) MaxFailedLogins
7) NTLM
8) TelnetPort
Type an option number [0 - 8] to select that option: 0
```

Telnet service must be restarted for the changes to take effect.
Select option **5** to stop Telnet service:

```
Select one of the following options:

0) Quit this application
1) List the current users
2) Terminate a user session ...
3) Display / change registry settings ...
4) Start the service
5) Stop the service

Type an option number [0 - 5] to select that option: 5
Stopping Microsoft Telnet Service ...
Microsoft Telnet Service stopped successfully
```

Select option **4** to start Telnet service:

```
Select one of the following options:

0) Quit this application
1) List the current users
2) Terminate a user session ...
3) Display / change registry settings ...
4) Start the service
5) Stop the service

Type an option number [0 - 5] to select that option: 4
Starting Microsoft Telnet Service ...
Microsoft Telnet Service started successfully
```

©2005 Nortel Networks Limited. All Rights Reserved

Select option **0** to quit Telnet Administration utility:

```
Select one of the following options:

0) Quit this application
1) List the current users
2) Terminate a user session ...
3) Display / change registry settings ...
4) Start the service
5) Stop the service

Type an option number [0 - 5] to select that option: 0

C:\>
```

Configuring Alteon

Note: This sample configuration is started from factory default settings.

1. Log in to the switch.

```
Enter password:
System Information at 11:05:11 Wed Apr 21, 2004
Alteon AD3
sysName:
sysLocation:
. . .
```

2. Select **n** to not run the setup script:

```
The switch is booted with factory default configuration.
  To ease the configuration of the switch, a "Set Up" facility which
  will prompt you with those configuration items that are essential
  to the operation of the switch is provided.
Would you like to run "Set Up" to configure the switch? [y/n] n
```

Configuring interfaces

1. Configure Interface 1.
    a) Enter interface 1 configuration menu:

```
>> Main# /cfg/ip/if 1
------------------------------------------------------------
[IP Interface 1 Menu]
      addr    - Set IP address
      mask    - Set subnet mask
      broad   - Set broadcast address
      vlan    - Set VLAN number
      relay   - Enable/disable BOOTP relay
      ena     - Enable IP interface
      dis     - Disable IP interface
      del     - Delete IP interface
      cur     - Display current interface configuration
```

©2005 Nortel Networks Limited. All Rights Reserved

b) Set mask (255.255.255.0), address (192.168.10.100) and enable the interface.

Note: If address is specified before the mask, a broadcast address must be entered using **broad** command.

```
>> IP Interface 1# mask 255.255.255.0/addr 192.168.10.100/ena
Current subnet mask:     0.0.0.0
New pending subnet mask: 255.255.255.0
Current IP address:     0.0.0.0
New pending IP address: 192.168.10.100
Pending new broadcast address:  192.168.10.255
Current status: disabled
New status:     enabled
```

2. Configure interface 2.
   a) Enter interface 2 configuration menu:

```
>> IP Interface 1# /cfg/ip/if 2
------------------------------------------------------------
[IP Interface 2 Menu]
      addr    - Set IP address
      mask    - Set subnet mask
      broad   - Set broadcast address
      vlan    - Set VLAN number
      relay   - Enable/disable BOOTP relay
      ena     - Enable IP interface
      dis     - Disable IP interface
      del     - Delete IP interface
      cur     - Display current interface configuration
```

   b) Set the mask (255.255.255.0) and address (192.168.20.200) for the interface.
   c) Enable the interface:

```
>> IP Interface 2# mask 255.255.255.0/addr 192.168.20.200/ena
Current subnet mask:     0.0.0.0
New pending subnet mask: 255.255.255.0
Current IP address:     0.0.0.0
New pending IP address: 192.168.20.200
Pending new broadcast address:  192.168.20.255
Current status: disabled
New status:     enabled
```

3. Apply and save the changes:

```
>> IP Interface 2# apply/save
------------------------------------------------------------------
Apply complete; don't forget to "save" updated configuration.
Request will first copy the FLASH "active" config to "backup",
 then overlay FLASH "active" with new config.
Confirm saving to FLASH [y/n]: y
New config successfully saved to FLASH.
Switch is currently set to use factory default config block on next boot.
Do you want to change that to the active config block? [y/n] y
Next boot will use active config block.
```

©2005 Nortel Networks Limited. All Rights Reserved

4. Verify connectivity to PC1 and PC2, PC3:

```
>> IP Interface 2# ping 192.168.10.1
[host 192.168.10.1, max tries 5, delay 1000 msec]
192.168.10.1: #1 ok, RTT 1 msec.
192.168.10.1: #2 ok, RTT 0 msec.
192.168.10.1: #3 ok, RTT 1 msec.
192.168.10.1: #4 ok, RTT 1 msec.
192.168.10.1: #5 ok, RTT 1 msec.
Ping finished.
```

```
>> IP Interface 2# ping 192.168.20.2
[host 192.168.20.2, max tries 5, delay 1000 msec]
192.168.20.2: #1 ok, RTT 1 msec.
192.168.20.2: #2 ok, RTT 1 msec.
192.168.20.2: #3 ok, RTT 1 msec.
192.168.20.2: #4 ok, RTT 1 msec.
192.168.20.2: #5 ok, RTT 1 msec.
Ping finished.
```

```
>> IP Interface 2# ping 192.168.10.75
[host 192.168.10.75, max tries 5, delay 1000 msec]
192.168.10.75: #1 ok, RTT 1 msec.
192.168.10.75: #2 ok, RTT 1 msec.
192.168.10.75: #3 ok, RTT 1 msec.
192.168.10.75: #4 ok, RTT 1 msec.
192.168.10.75: #5 ok, RTT 1 msec.
Ping finished.
```

Configuring NAT filters

Configure filters to perform dynamic NAT.

1. Filter 15 is created to perform NAT translation.
   Create filter 15 and enter filter's configuration menu:

```
>> IP Interface 2# /cfg/slb/filt 15
------------------------------------------------------------
[Filter 15   Menu]
      adv     - Filter Advanced Menu
      name    - Set filter name
      smac    - Set source MAC address
      dmac    - Set destination MAC address
      sip     - Set source IP address
      smask   - Set source IP mask
      dip     - Set destination IP address
      dmask   - Set destination IP mask
      proto   - Set IP protocol
      sport   - Set source TCP/UDP port or range
      dport   - Set destination TCP/UDP port or range
      action  - Set action
      group   - Set real server group for redirection
      rport   - Set real server port for redirection
      nat     - Set which addresses are network address translated
      invert  - Enable/disable filter inversion
      ena     - Enable filter
      dis     - Disable filter
      del     - Delete filter
      cur     - Display current filter configuration
```

2. In this example, a filter using an inverse logic is created.
   Note: Using inverse logic is not required for dynamic NAT to operate and is used only as an example. For example configuration without inverse logic, consult Appendix C of this document. Enable inverse logic:

```
>> Filter 15  # invert e
Current inversion: disabled
```

©2005 Nortel Networks Limited. All Rights Reserved

```
New inversion:     enabled
```

3. Set destination IP to private network 192.168.10.0:

```
>> Filter 15  # dip 192.168.10.0
Current destination address:     any
New pending destination address: 192.168.10.0
```

4. Set destination mask to 255.255.255.0 (mask of the private network in our example):

```
>> Filter 15  # dmask 255.255.255.0
Current destination mask:     0.0.0.0
New pending destination mask: 255.255.255.0
```

5. Set source IP to any:

```
>> Filter 15  # sip any
Current source address:     any
New pending source address: any
```

6. Set filter's action to NAT:

```
>> Filter 15  # action nat
Current action: allow
Pending new action:     nat
```

7. Set NAT direction to source:

```
>> Filter 15  # nat source
Current NAT addresses:  dest
Pending new NAT addresses:      source
```

8. Enable filter:

```
>> Filter 15  # ena
Current status: disabled
New status:     enabled
```

9. Enter filter's advanced configuration mode and enable proxy:

```
>> Filter 15  # adv/proxy e
Current client proxy: enabled
New client proxy:     enabled
```

10. Optionally enable logging for the filter:

```
>> Filter 15 Advanced# log e
Current logging: disabled
New logging:     enabled
```

11. Enter SLB port configuration menu for the port connected to private network, port 1 in this example:

```
>> Filter 15 Advanced# /cfg/slb/port 1
------------------------------------------------------------
[SLB port 1 Menu]
      client  - Enable/disable client processing
      server  - Enable/disable server processing
      rts     - Enable/disable RTS processing
      hotstan - Enable/disable hot-standby processing
      intersw - Enable/disable inter-switch processing
      proxy   - Enable/disable use of PIP for ingress traffic
```

©2005 Nortel Networks Limited. All Rights Reserved

```
      pip     - Set Proxy IP address for port
      filt    - Enable/disable filtering
      add     - Add filter to port
      rem     - Remove filter from port
      idslb   - Enable/disable intrusion detection server load balancing
      cur     - Display current port configuration
```

12. Add the create filter to the port:

```
>> SLB port 1# add 15
Filter 15 added to port 1.
```

13. Enable filtering on the port:

```
>> SLB port 1# filt e
Current port 1 filtering: disabled
New port 1 filtering:     enabled
```

14. Enable proxy on a port:

```
>> SLB port 1# proxy en
Current using proxy IP address: disabled
New using proxy IP address:     enabled
```

15. Assign proxy IP (PIP) that will server as a public IP (192.168.20.150) to a port (`/cfg/slb/pip` menu on the Alteon Application switch):

```
>> SLB port 1# pip 192.168.20.150
Current proxy IP address:     0.0.0.0
New pending proxy IP address: 192.168.20.150
```

Note: If VMA (Virtual Matrix Architecture) is enabled, PIP should be assigned to every port of the switch. It is not recommended to disable VMA on the switch as it will degrade switch performance and limit switch functionality. If VMA is enabled a pool of proxy addresses assigned to ports will be used for NAT translations, therefore a care must be taken to provide enough routable addresses.

16. In this sample configuration, VMA is disabled as performance is not an issue for this sample setup. Disable VMA:

```
>> SLB port 1# /cfg/slb/adv/matrix d
Current Virtual Matrix Architecture: enabled
New Virtual Matrix Architecture:     disabled
```

©2005 Nortel Networks Limited. All Rights Reserved

Enabling SLB globally

1. Enable SLB globally:

```
>> Layer 4 Advanced# /cfg/slb/on
Current status: OFF
New status:     ON
```

2. Apply and save the changes:

```
>> Layer 4# apply/save
------------------------------------------------------------------
Apply complete; don't forget to "save" updated configuration.
Request will first copy the FLASH "active" config to "backup",
 then overlay FLASH "active" with new config.
Confirm saving to FLASH [y/n]: y
New config successfully saved to FLASH.
```

Testing the configuration

1. Clear log on Alteon:

```
>> Layer 4# /info/clrlog
```

2. Start traffic capture on PC1, PC2 and PC3 using, for example, Ethereal.

3. Telnet from PC1 (192.168.10.1) to PC2 (192.168.20.2) and enter the appropriate credentials:

```
C:\>telnet 192.168.20.2
Trying 192.168.20.2...
Connected to 192.168.20.2.
Escape character is '^]'.
Microsoft (R) Windows (TM) Version 5.00 (Build 2195)
Welcome to Microsoft Telnet Service
Telnet Server Build 5.00.99206.1
login: Administrator
password: ********
*===============================================================
Welcome to Microsoft Telnet Server.
*===============================================================
C:\>
```

4. Check session table on Alteon:

```
>> Information# /info/slb/sess/dump
 1,3:  192.168.10.1 4241, 192.168.20.2 23  NAT  age 4  E
```

5. Close the telnet session:

```
C:\>exit
Connection to host lost.
C:\>
```

6. Telnet from PC3 (192.168.10.75) to PC2 (192.168.20.2).

©2005 Nortel Networks Limited. All Rights Reserved

7. Check session table on Alteon:

```
>> Information# /info/slb/sess/dump
 1,3:  192.168.10.75 1033, 192.168.20.2 23  NAT  age 4  E
```

8. Close the Telnet connection between PC3 and PC2.

9. Check the log on Alteon. Note that the configured filter fired upon receiving TCP traffic from PC1 (192.168.10.1) and PC3 (192.168.10.75) to PC2 (192.168.20.2):

```
>> Information# /info/log
May 10 11:31:59 WARNING slb: filter 15 fired on port 1, tcp 192.168.10.1:4241 ->
192.168.20.2:23, flags 02
May 10 11:34:01 WARNING slb: filter 15 fired on port 1, tcp 192.168.10.75:1033 ->
192.168.20.2:23, flags 02
```

10. Check the captured traffic.

PC1 (192.168.10.1) sends a SYN to PC2 (192.168.20.2) Telnet TCP port 23:

```
Frame 10 (62 bytes on wire, 62 bytes captured)
Ethernet II, Src: 00:08:74:9a:e5:85, Dst: 00:60:cf:46:53:60
Internet Protocol, Src Addr: 192.168.10.1 (192.168.10.1), Dst Addr: 192.168.20.2
(192.168.20.2)
Transmission Control Protocol, Src Port: 4241 (4241), Dst Port: telnet (23), Seq:
2272729190, Ack: 0, Len: 0
    Source port: 4241 (4241)
    Destination port: telnet (23)
    Sequence number: 2272729190
    Header length: 28 bytes
    Flags: 0x0002 (SYN)
    Window size: 65535
    Checksum: 0x3346 (correct)
    Options: (8 bytes)
```

Alteon receives SYN on its port 1, checks whether filter is enabled on this port. With NAT filter being enabled, Alteon compares the packet with the filter criteria. With packet matching the criteria, Alteon applies the configured NAT filter action by translating private source IP (192.168.10.1) into public proxy IP (192.168.20.150) and changing private source port (4241 in this example) to public proxy port (4130 in this example). Once the packet is translated, it's forwarded to PC2:

```
Frame 2 (62 bytes on wire, 62 bytes captured)
Ethernet II, Src: 00:60:cf:46:53:60, Dst: 00:e0:7b:04:fb:00
Internet Protocol, Src Addr: 192.168.20.150 (192.168.20.150), Dst Addr: 192.168.20.2
(192.168.20.2)
Transmission Control Protocol, Src Port: 4130 (4130), Dst Port: telnet (23), Seq:
2272729190, Ack: 0, Len: 0
    Source port: 4130 (4130)
    Destination port: telnet (23)
    Sequence number: 2272729190
    Header length: 28 bytes
    Flags: 0x0002 (SYN)
    Window size: 65535
    Checksum: 0x2920 (correct)
    Options: (8 bytes)
```

PC2 receives SYN from 192.168.20.150 (PC1 public IP) responds with SYN ACK:

©2005 Nortel Networks Limited. All Rights Reserved

```
Frame 5 (58 bytes on wire, 58 bytes captured)
Ethernet II, Src: 00:e0:7b:04:fb:00, Dst: 00:60:cf:46:53:61
Internet Protocol, Src Addr: 192.168.20.2 (192.168.20.2), Dst Addr: 192.168.20.150
(192.168.20.150)
Transmission Control Protocol, Src Port: telnet (23), Dst Port: 4130 (4130), Seq:
2269416528, Ack: 2272729191, Len: 0
    Source port: telnet (23)
    Destination port: 4130 (4130)
    Sequence number: 2269416528
    Acknowledgement number: 2272729191
    Header length: 24 bytes
    Flags: 0x0012 (SYN, ACK)
    Window size: 8760
    Checksum: 0x0849 (correct)
    Options: (4 bytes)
```

Alteon receives SYN ACK, translates it back to private IP address of PC1 (192.168.10.1), changes port back to the original and forwards SYN ACK to PC1:

```
Frame 13 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: 00:60:cf:46:53:60, Dst: 00:08:74:9a:e5:85
Internet Protocol, Src Addr: 192.168.20.2 (192.168.20.2), Dst Addr: 192.168.10.1
(192.168.10.1)
Transmission Control Protocol, Src Port: telnet (23), Dst Port: 4241 (4241), Seq:
2269416528, Ack: 2272729191, Len: 0
    Source port: telnet (23)
    Destination port: 4241 (4241)
    Sequence number: 2269416528
    Acknowledgement number: 2272729191
    Header length: 24 bytes
    Flags: 0x0012 (SYN, ACK)
    Window size: 8760
    Checksum: 0x126f (correct)
    Options: (4 bytes)
```

PC1 responds with ACK:

```
Frame 14 (54 bytes on wire, 54 bytes captured)
Ethernet II, Src: 00:08:74:9a:e5:85, Dst: 00:60:cf:46:53:60
Internet Protocol, Src Addr: 192.168.10.1 (192.168.10.1), Dst Addr: 192.168.20.2
(192.168.20.2)
Transmission Control Protocol, Src Port: 4241 (4241), Dst Port: telnet (23), Seq:
2272729191, Ack: 2269416529, Len: 0
    Source port: 4241 (4241)
    Destination port: telnet (23)
    Sequence number: 2272729191
    Acknowledgement number: 2269416529
    Header length: 20 bytes
    Flags: 0x0010 (ACK)
    Window size: 65535
    Checksum: 0x4c64 (correct)
```

©2005 Nortel Networks Limited. All Rights Reserved

Alteon receives it, translates to public IP/port and forwards to PC2:

```
Frame 6 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: 00:60:cf:46:53:60, Dst: 00:e0:7b:04:fb:00
Internet Protocol, Src Addr: 192.168.20.150 (192.168.20.150), Dst Addr: 192.168.20.2
(192.168.20.2)
Transmission Control Protocol, Src Port: 4130 (4130), Dst Port: telnet (23), Seq:
2272729191, Ack: 2269416529, Len: 0
    Source port: 4130 (4130)
    Destination port: telnet (23)
    Sequence number: 2272729191
    Acknowledgement number: 2269416529
    Header length: 20 bytes
    Flags: 0x0010 (ACK)
    Window size: 65535
    Checksum: 0x423e (correct)
```

Thus a three-way TCP handshake is complete and Telnet traffic can be sent:

src	**dst**		**src**	**dst**
192.168.10.1,	192.168.20.2 Telnet data	→Alteon→	192.168.20.150,	192.168.20.2 Telnet data
192.168.20.2,	192.168.10.1 Telnet data	←Alteon←	192.168.20.2,	192.168.20.150 Telnet data

Note: PC2 has no knowledge of PC1 private address. From PC2 point of view it has an open Telnet connection from the client at 192.169.20.150 port 4130.

When PC3 telnets to PC2, virtually the same procedure is performed by Alteon.

PC3 (192.168.10.75) sends SYN to PC2 (192.168.20.2) telnet port 23:

```
Frame 4 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:0c:29:4d:f9:8c, Dst: 00:60:cf:46:53:60
Internet Protocol, Src Addr: 192.168.10.75 (192.168.10.75), Dst Addr: 192.168.20.2
(192.168.20.2)
Transmission Control Protocol, Src Port: 1033 (1033), Dst Port: telnet (23), Seq:
4277648054, Ack: 0, Len: 0
    Source port: 1033 (1033)
    Destination port: telnet (23)
    Sequence number: 4277648054
    Header length: 40 bytes
    Flags: 0x0002 (SYN)
    Window size: 5840
    Checksum: 0xe0c0 (correct)
    Options: (20 bytes)
```

Alteon gets the SYN on its port 1 and checks the packet against the filter enabled on port. With packet matching filters criteria a configured NAT action is applied. Alteon changes private IP (192.168.10.75) and client's private port (1033 in this example) to public proxy IP (192.168.20.150) and public port (4131 in this example). Once packet has been translated, Alteon forwards it to PC2:

```
Frame 69 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:60:cf:46:53:60, Dst: 00:e0:7b:04:fb:00
Internet Protocol, Src Addr: 192.168.20.150 (192.168.20.150), Dst Addr: 192.168.20.2
(192.168.20.2)
```

©2005 Nortel Networks Limited. All Rights Reserved

```
Transmission Control Protocol, Src Port: 4131 (4131), Dst Port: telnet (23), Seq:
4277648054, Ack: 0, Len: 0
    Source port: 4131 (4131)
    Destination port: telnet (23)
    Sequence number: 4277648054
    Header length: 40 bytes
    Flags: 0x0002 (SYN)
    Window size: 5840
    Checksum: 0xca5b (correct)
    Options: (20 bytes)
```

PC2 receives SYN and responds with SYN ACK:

```
Frame 70 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:e0:7b:04:fb:00, Dst: 00:60:cf:46:53:61
Internet Protocol, Src Addr: 192.168.20.2 (192.168.20.2), Dst Addr: 192.168.20.150
(192.168.20.150)
Transmission Control Protocol, Src Port: telnet (23), Dst Port: 4131 (4131), Seq:
2274407198, Ack: 4277648055, Len: 0
    Source port: telnet (23)
    Destination port: 4131 (4131)
    Sequence number: 2274407198
    Acknowledgement number: 4277648055
    Header length: 40 bytes
    Flags: 0x0012 (SYN, ACK)
    Window size: 8760
    Checksum: 0xe3c2 (correct)
    Options: (20 bytes)
```

Alteon receives SYN ACK, translates public IP (192.168.20.150) and port (4131) back to private IP (192.168.10.1) and port (1033) and forwards packet to PC3:

```
Frame 5 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:60:cf:46:53:60, Dst: 00:0c:29:4d:f9:8c
Internet Protocol, Src Addr: 192.168.20.2 (192.168.20.2), Dst Addr: 192.168.10.75
(192.168.10.75)
Transmission Control Protocol, Src Port: telnet (23), Dst Port: 1033 (1033), Seq:
2274407198, Ack: 4277648055, Len: 0
    Source port: telnet (23)
    Destination port: 1033 (1033)
    Sequence number: 2274407198
    Acknowledgement number: 4277648055
    Header length: 40 bytes
    Flags: 0x0012 (SYN, ACK)
    Window size: 8760
    Checksum: 0xfa27 (correct)
    Options: (20 bytes)
```

PC3 receives the SYN ACK and responds with an ACK:

```
Frame 6 (66 bytes on wire, 66 bytes captured)
Ethernet II, Src: 00:0c:29:4d:f9:8c, Dst: 00:60:cf:46:53:60
Internet Protocol, Src Addr: 192.168.10.75 (192.168.10.75), Dst Addr: 192.168.20.2
(192.168.20.2)
Transmission Control Protocol, Src Port: 1033 (1033), Dst Port: telnet (23), Seq:
4277648055, Ack: 2274407199, Len: 0
    Source port: 1033 (1033)
    Destination port: telnet (23)
```

©2005 Nortel Networks Limited. All Rights Reserved

```
    Sequence number: 4277648055
    Acknowledgement number: 2274407199
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
    Window size: 5840
    Checksum: 0x3154 (correct)
    Options: (12 bytes)
```

Alteon receives ACK, translates it to public and forwards to PC2:

```
Frame 71 (66 bytes on wire, 66 bytes captured)
Ethernet II, Src: 00:60:cf:46:53:60, Dst: 00:e0:7b:04:fb:00
Internet Protocol, Src Addr: 192.168.20.150 (192.168.20.150), Dst Addr: 192.168.20.2
(192.168.20.2)
Transmission Control Protocol, Src Port: 4131 (4131), Dst Port: telnet (23), Seq:
4277648055, Ack: 2274407199, Len: 0
    Source port: 4131 (4131)
    Destination port: telnet (23)
    Sequence number: 4277648055
    Acknowledgement number: 2274407199
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
    Window size: 5840
    Checksum: 0x1aef (correct)
    Options: (12 bytes)
```

Thus a three-way TCP handshake is complete and Telnet connection is opened.

192.168.10.75,192.168.20.2 Telnet data →Alteon→ 192.168.20.150, 192.168.20.2 Telnet data
src dst src dst
192.168.20.2, 192.168.10.75 Telnet data ←Alteon← 192.168.20.2, 192.168.20.150 Telnet data

Note: PC2 has no knowledge of PC3 private address. From PC2 point of view it has an open Telnet connection from the client at 192.169.20.150 port 4131.

FTP and dynamic NAT

When FTP client operates in active mode, it sends its IP and port information on control channel. When dynamic NAT is enabled, Alteon performs NAT translation on TCP/IP header only and does not look at the data part of the frame. Therefore, client's private IP is revealed to the public that prevents active FTP from operating successfully. This does not cause any issues with passive FTP because in passive FTP server sends the data port information to the client.

Alteon could be configured to look in the data portion of the frame for FTP sessions. With FTP monitoring Alteon replaces the private IP sent by the client in the port request FTP command to the configured proxy IP (PIP) and changes the client's private port to a proxy port.

©2005 Nortel Networks Limited. All Rights Reserved

Setup

The setup from the previous example is used.

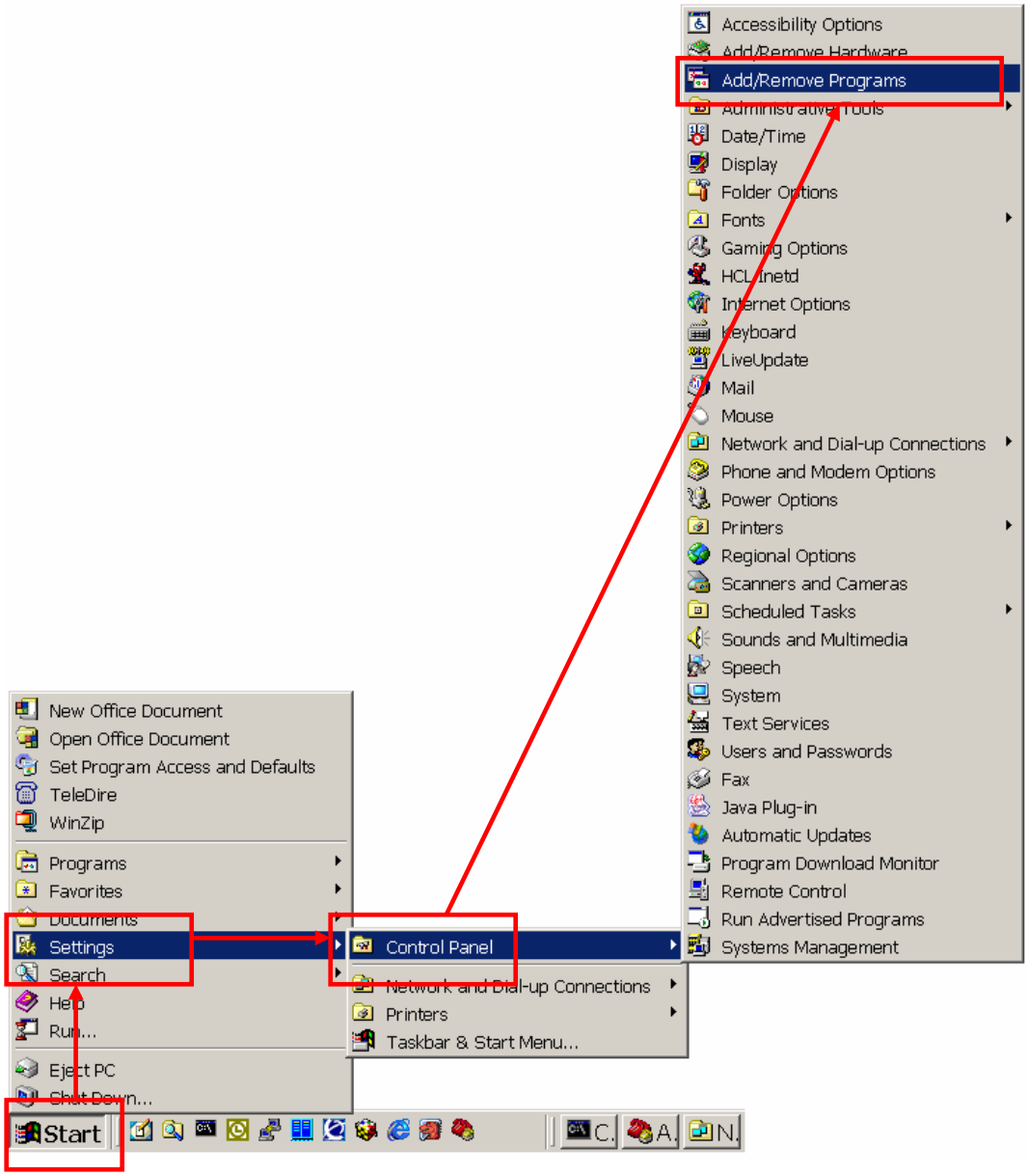
The goal of the configuration is to enable Alteon to perform dynamic NAT on active FTP sessions.

Configuring PC1

The configuration of PC1 is done exactly the same as shown for PC1 in the previous example.

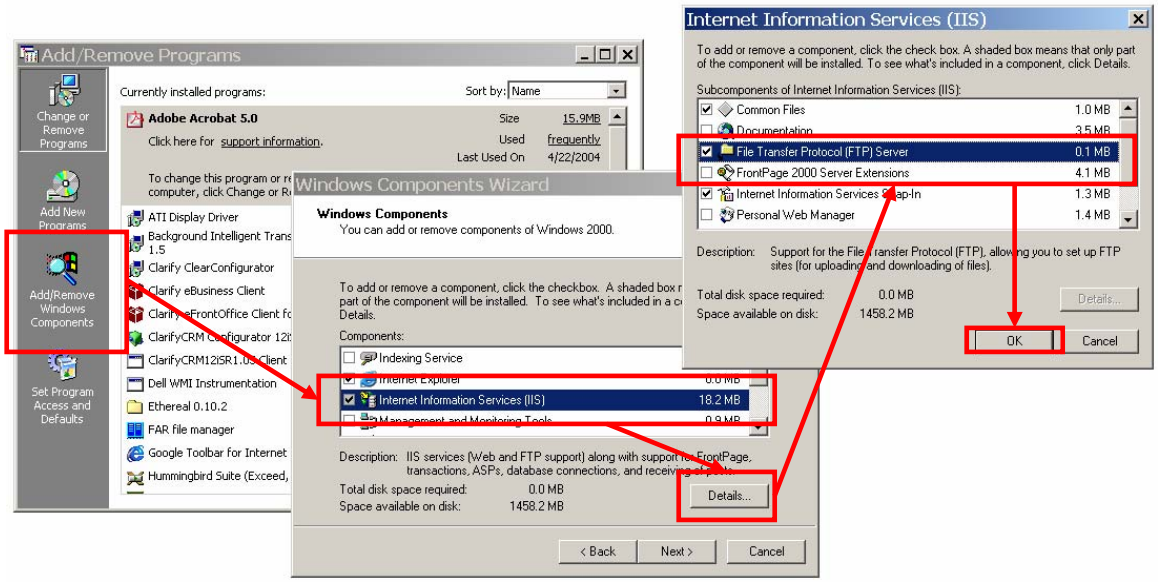
Configuring PC2

1. Configure IP address and default gateway exactly as they were configured in the previous example.
2. Enable FTP service on PC2.
   a) Make sure FTP service is globally enabled on PC2.
   Navigate **Start→Settings→Control Panel→Add Remove Programs**:



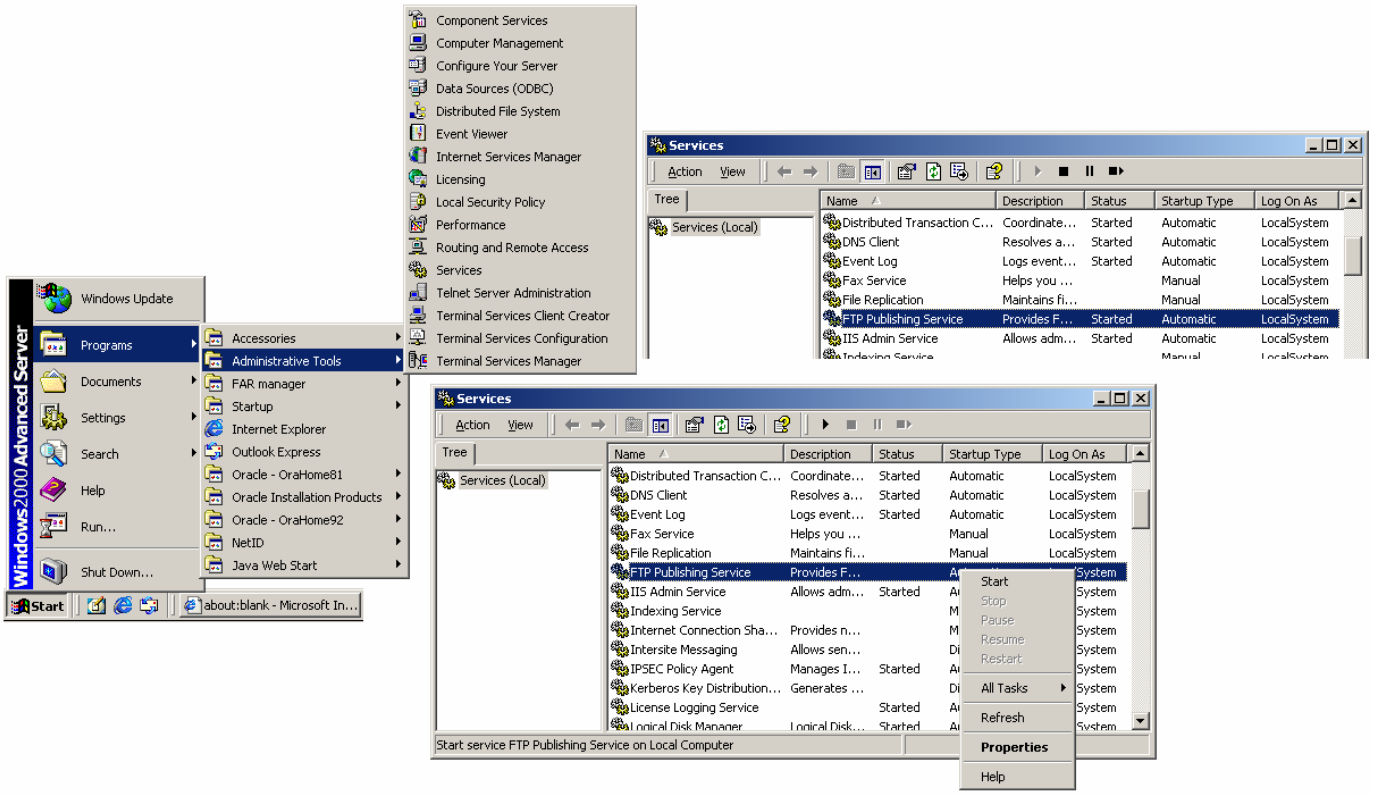
©2005 Nortel Networks Limited. All Rights Reserved

b) The **Add/Remove Programs** window appears.
c) Click on **Add/Remove Windows Components** in the panel on the left.
d) The **Windows Components Wizard** appears.
e) Select **Internet Information Services (IIS)**.
f) Click **Details**.
g) The **Internet Information Services (IIS)** window appears.
h) Make sure **File Transfer Protocol (FTP) Server** is enabled globally (checked).
i) Click **OK**.
j) If FTP service was not installed, install it.
k) Close Windows components and Add/Remove Programs windows.



©2005 Nortel Networks Limited. All Rights Reserved

l) Start an FTP server.
m) Navigate **Start→Programs→Administrative Tools→Services**.
n) The **Services** screen appears. Select the **FTP Publishing Service**, right-click on it and select **Start**:



©2005 Nortel Networks Limited. All Rights Reserved

Configuring Alteon

Configuration of the Alteon for active FTP is based on configuration of Alteon in Dynamic NAT sample configuration, only the differences are noted.

1. Enter filter configuration menu, filter 15 in this example:

```
>> Configuration# /cfg/slb/filt 15
------------------------------------------------------------
[Filter 15   Menu]
      adv     - Filter Advanced Menu
      name    - Set filter name
      smac    - Set source MAC address
      dmac    - Set destination MAC address
      sip     - Set source IP address
      smask   - Set source IP mask
      dip     - Set destination IP address
      dmask   - Set destination IP mask
      proto   - Set IP protocol
      sport   - Set source TCP/UDP port or range
      dport   - Set destination TCP/UDP port or range
      action  - Set action
      group   - Set real server group for redirection
      rport   - Set real server port for redirection
      nat     - Set which addresses are network address translated
      invert  - Enable/disable filter inversion
      ena     - Enable filter
      dis     - Disable filter
      del     - Delete filter
      cur     - Display current filter configuration
```

2. Enable active FTP processing in the advanced menu:

```
>> Filter 15  # adv/ftpa e
Current active FTP NAT: disabled
New active FTP NAT:     enabled
```

3. Apply and save the changes:

```
>> Filter 15 Advanced# apply/save
------------------------------------------------------------------
Apply complete; don't forget to "save" updated configuration.
Request will first copy the FLASH "active" config to "backup",
 then overlay FLASH "active" with new config.
Confirm saving to FLASH [y/n]: y
New config successfully saved to FLASH.
```

©2005 Nortel Networks Limited. All Rights Reserved

Testing the configuration

1. Start capture on PC1 and PC2, using for example Ethereal.

2. Initiate an FTP session from PC1 to PC2, provide proper credentials:

```
C:\>ftp 192.168.20.2
Connected to 192.168.20.2.
220 KRISTISE-1 Microsoft FTP Service (Version 5.0).
User (192.168.20.2:(none)): ftp
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 Anonymous user logged in.
ftp>
```

3. Check session table on Alteon:

```
>> Session Table Information# /info/slb/sess/dump
 1,8:  192.168.10.1 1057, 192.168.20.2 21  NAT  age 4  E
```

4. While FTP'd issue a **dir** command.
   Note: Native Windows FTP client uses active FTP for data transferring, if non-Windows or non-native FTP client is used switch to active mode prior to issuing a dir command.

```
ftp> dir
200 PORT command successful.
150 Opening ASCII mode data connection for /bin/ls.
02-05-04  03:21PM               175008 cepsetup.exe
226 Transfer complete.
ftp: 53 bytes received in 0.00Seconds 53000.00Kbytes/sec.
```

5. Check the session table again:

```
>> Session Table Information# /info/slb/sess/dump
1,8:  192.168.10.1 1057, 192.168.20.2 21  NAT  age 4  E
1,9:  192.168.10.1 1058, 192.168.20.2 20  NAT  age 0
```

6. Exit FTP session:

```
ftp> quit
221
```

©2005 Nortel Networks Limited. All Rights Reserved

7. Check the captured traffic on PC1 and PC2.

PC1 (192.168.10.1) sends SYN to PC2 (192.168.20.2) FTP port 21:

```
Frame 8 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:0c:29:4d:f9:8c, Dst: 00:60:cf:46:53:60
Internet Protocol, Src Addr: 192.168.10.1 (192.168.10.1), Dst Addr: 192.168.20.2
(192.168.20.2)
Transmission Control Protocol, Src Port: 1057 (1057), Dst Port: ftp (21), Seq:
3649787722, Ack: 0, Len: 0
    Source port: 1057 (1057)
    Destination port: ftp (21)
    Sequence number: 3649787722
    Header length: 40 bytes
    Flags: 0x0002 (SYN)
    Window size: 5840
    Checksum: 0x50b0 (correct)
    Options: (20 bytes)
```

Alteon receives SYN on its port, applies a NAT filter, changes private IP (192.168.10.1) to public IP (192.168.20.150), changes private port (1057) to public port (4104) and forwards the packet to PC2:

```
Frame 9 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 00:60:cf:46:53:60, Dst: 00:08:74:9a:e5:85
Internet Protocol, Src Addr: 192.168.20.150 (192.168.20.150), Dst Addr: 192.168.20.2
(192.168.20.2)
Transmission Control Protocol, Src Port: 4104 (4104), Dst Port: ftp (21), Seq:
3649787722, Ack: 0, Len: 0
    Source port: 4104 (4104)
    Destination port: ftp (21)
    Sequence number: 3649787722
    Header length: 40 bytes
    Flags: 0x0002 (SYN)
    Window size: 5840
    Checksum: 0x3a7e (correct)
    Options: (20 bytes)
```

PC2 receives SYN and replies with SYN ACK:

```
Frame 10 (78 bytes on wire, 78 bytes captured)
Ethernet II, Src: 00:08:74:9a:e5:85, Dst: 00:60:cf:46:53:61
Internet Protocol, Src Addr: 192.168.20.2 (192.168.20.2), Dst Addr: 192.168.20.150
(192.168.20.150)
Transmission Control Protocol, Src Port: ftp (21), Dst Port: 4104 (4104), Seq:
2868195030, Ack: 3649787723, Len: 0
    Source port: ftp (21)
    Destination port: 4104 (4104)
    Sequence number: 2868195030
    Acknowledgement number: 3649787723
    Header length: 44 bytes
    Flags: 0x0012 (SYN, ACK)
    Window size: 65535
    Checksum: 0x7149 (correct)
    Options: (24 bytes)
```

©2005 Nortel Networks Limited. All Rights Reserved

Alteon receives SYN ACK on its port, translates the packet's public address and port back to the private address and port and forwards the packet to PC1:

```
Frame 11 (78 bytes on wire, 78 bytes captured)
Ethernet II, Src: 00:60:cf:46:53:60, Dst: 00:0c:29:4d:f9:8c
Internet Protocol, Src Addr: 192.168.20.2 (192.168.20.2), Dst Addr: 192.168.10.1
(192.168.10.1)
Transmission Control Protocol, Src Port: ftp (21), Dst Port: 1057 (1057), Seq:
2868195030, Ack: 3649787723, Len: 0
    Source port: ftp (21)
    Destination port: 1057 (1057)
    Sequence number: 2868195030
    Acknowledgement number: 3649787723
    Header length: 44 bytes
    Flags: 0x0012 (SYN, ACK)
    Window size: 65535
    Checksum: 0x877b (correct)
    Options: (24 bytes)
```

PC1 receives SYN ACK and acknowledges it with ACK:

```
Frame 12 (66 bytes on wire, 66 bytes captured)
Ethernet II, Src: 00:0c:29:4d:f9:8c, Dst: 00:60:cf:46:53:60
Internet Protocol, Src Addr: 192.168.10.1 (192.168.10.1), Dst Addr: 192.168.20.2
(192.168.20.2)
Transmission Control Protocol, Src Port: 1057 (1057), Dst Port: ftp (21), Seq:
3649787723, Ack: 2868195031, Len: 0
    Source port: 1057 (1057)
    Destination port: ftp (21)
    Sequence number: 3649787723
    Acknowledgement number: 2868195031
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
    Window size: 5840
    Checksum: 0xa598 (correct)
    Options: (12 bytes)
```

Alteon once again translates private into public and forwards ACK to PC2:

```
Frame 13 (66 bytes on wire, 66 bytes captured)
Ethernet II, Src: 00:60:cf:46:53:60, Dst: 00:08:74:9a:e5:85
Internet Protocol, Src Addr: 192.168.20.150 (192.168.20.150), Dst Addr: 192.168.20.2
(192.168.20.2)
Transmission Control Protocol, Src Port: 4104 (4104), Dst Port: ftp (21), Seq:
3649787723, Ack: 2868195031, Len: 0
    Source port: 4104 (4104)
    Destination port: ftp (21)
    Sequence number: 3649787723
    Acknowledgement number: 2868195031
    Header length: 32 bytes
    Flags: 0x0010 (ACK)
    Window size: 5840
    Checksum: 0x8f66 (correct)
    Options: (12 bytes)
```

©2005 Nortel Networks Limited. All Rights Reserved

TCP three-way handshake is established and FTP connection is opened.
Client and server exchange information in the same manner TCP is negotiated, through the Alteon.

Once user on PC1 issues a dir command, FTP client starts active FTP session by sending a port request FTP command to FTP server, requesting port 1058 to be used for data:

```
Frame 51 (91 bytes on wire, 91 bytes captured)
Ethernet II, Src: 00:0c:29:4d:f9:8c, Dst: 00:60:cf:46:53:60
Internet Protocol, Src Addr: 192.168.10.1 (192.168.10.1), Dst Addr: 192.168.20.2
(192.168.20.2)
Transmission Control Protocol, Src Port: 1057 (1057), Dst Port: ftp (21), Seq:
3649787749, Ack: 2868195215, Len: 25
    Source port: 1057 (1057)
    Destination port: ftp (21)
    Sequence number: 3649787749
    Next sequence number: 3649787774
    Acknowledgement number: 2868195215
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
    Window size: 5840
    Checksum: 0x0d7a (correct)
    Options: (12 bytes)
File Transfer Protocol (FTP)
    PORT 192,168,10,1,4,34\r\n
        Request command: PORT
        Request arg: 192,168,10,1,4,34
        Active IP address: 192.168.10.1 (192.168.10.1)
        Active port: 1058
```

Alteon receives the packet on its port and with active FTP processing being enabled translates the requested by FTP client port (1058 in this example) to proxy port (4105 in this example), and changes client's Active IP address (192.168.10.1) to the proxy address (192.168.20.150). Once translation is done, Alteon forwards the packet to PC2:

```
Frame 52 (92 bytes on wire, 92 bytes captured)
Ethernet II, Src: 00:60:cf:46:53:60, Dst: 00:08:74:9a:e5:85
Internet Protocol, Src Addr: 192.168.20.150 (192.168.20.150), Dst Addr: 192.168.20.2
(192.168.20.2)
Transmission Control Protocol, Src Port: 4104 (4104), Dst Port: ftp (21), Seq:
3649787749, Ack: 2868195215, Len: 26
    Source port: 4104 (4104)
    Destination port: ftp (21)
    Sequence number: 3649787749
    Next sequence number: 3649787775
    Acknowledgement number: 2868195215
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
    Window size: 5840
    Checksum: 0xf914 (correct)
    Options: (12 bytes)
File Transfer Protocol (FTP)
    PORT 192,168,20,150,16,9\r\n
        Request command: PORT
        Request arg: 192,168,20,150,16,9
        Active IP address: 192.168.20.150 (192.168.20.150)
        Active port: 4105
```

©2005 Nortel Networks Limited. All Rights Reserved

PC2 receives the modified by Alteon request and accepts client's proposal for a data port:

```
Frame 53 (96 bytes on wire, 96 bytes captured)
Ethernet II, Src: 00:08:74:9a:e5:85, Dst: 00:60:cf:46:53:61
Internet Protocol, Src Addr: 192.168.20.2 (192.168.20.2), Dst Addr: 192.168.20.150
(192.168.20.150)
Transmission Control Protocol, Src Port: ftp (21), Dst Port: 4104 (4104), Seq:
2868195215, Ack: 3649787775, Len: 30
    Source port: ftp (21)
    Destination port: 4104 (4104)
    Sequence number: 2868195215
    Next sequence number: 2868195245
    Acknowledgement number: 3649787775
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
    Window size: 65483
    Checksum: 0xd8d0 (correct)
    Options: (12 bytes)
File Transfer Protocol (FTP)
    200 PORT command successful.\r\n
        Response code: Command okay (200)
        Response arg: PORT command successful.
```

Alteon performs a public to private translation and forwards packet to PC1:

```
Frame 54 (96 bytes on wire, 96 bytes captured)
Ethernet II, Src: 00:60:cf:46:53:60, Dst: 00:0c:29:4d:f9:8c
Internet Protocol, Src Addr: 192.168.20.2 (192.168.20.2), Dst Addr: 192.168.10.1
(192.168.10.1)
Transmission Control Protocol, Src Port: ftp (21), Dst Port: 1057 (1057), Seq:
2868195215, Ack: 3649787774, Len: 30
    Source port: ftp (21)
    Destination port: 1057 (1057)
    Sequence number: 2868195215
    Next sequence number: 2868195245
    Acknowledgement number: 3649787774
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
    Window size: 65483
    Checksum: 0xef03 (correct)
    Options: (12 bytes)
File Transfer Protocol (FTP)
    200 PORT command successful.\r\n
        Response code: Command okay (200)
        Response arg: PORT command successful.
```

Thus an active FTP data session is successfully opened.

©2005 Nortel Networks Limited. All Rights Reserved

Appendix A. Static one-to-one NAT configuration

```
script start "Alteon AD3" 4  /**** DO NOT EDIT THIS LINE!
/* Configuration dump taken 14:16:36 Fri May  7, 2004
/* Version 10.0.30.7,  Base MAC address 00:60:cf:46:53:60
/c/sys
        idle 60
        tnet ena
/c/ip/if 1
        ena
        addr 192.168.10.100
/c/ip/if 2
        ena
        addr 192.168.20.200
/c/slb
        on
/c/slb/filt 10
        ena
        action nat
        sip 192.168.10.1
        smask 255.255.255.255
        dip 192.168.20.150
        dmask 255.255.255.255
        nat source
/c/slb/filt 10/adv
        log ena
        proxy dis
/c/slb/filt 20
        ena
        action nat
        sip 192.168.10.1
        smask 255.255.255.255
        dip 192.168.20.150
        dmask 255.255.255.255
/c/slb/filt 20/adv
        log ena
        proxy dis
/c/slb/port 1
        filt ena
        add 10
/c/slb/port 8
        filt ena
        add 20
/
script end  /**** DO NOT EDIT THIS LINE!
```

©2005 Nortel Networks Limited. All Rights Reserved

Appendix B. Static many-to-many NAT configuration

```
script start "Alteon AD3" 4  /**** DO NOT EDIT THIS LINE!
/* Configuration dump taken 16:12:46 Fri May  7, 2004
/* Version 10.0.30.7,  Base MAC address 00:60:cf:46:53:60
/c/sys
        idle 60
        tnet ena
/c/ip/if 1
        ena
        addr 192.168.10.100
/c/ip/if 2
        ena
        addr 192.168.20.200
/c/slb
        on
/c/slb/filt 10
        ena
        action nat
        sip 192.168.10.0
        smask 255.255.255.0
        dip 192.168.20.0
        dmask 255.255.255.0
        nat source
/c/slb/filt 10/adv
        log ena
        proxy dis
/c/slb/filt 20
        ena
        action nat
        sip 192.168.10.0
        smask 255.255.255.0
        dip 192.168.20.0
        dmask 255.255.255.0
/c/slb/filt 20/adv
        log ena
        proxy dis
/c/slb/port 1
        filt ena
        add 10
/c/slb/port 8
        filt ena
        add 20
/
script end  /**** DO NOT EDIT THIS LINE!
```

©2005 Nortel Networks Limited. All Rights Reserved

Copyright © 2004 Nortel Networks Limited - All Rights Reserved. Nortel, Nortel Networks, the Nortel logo, Globemark, and Alteon are trademarks of Nortel Networks Limited.

Windows is a trademark of Microsoft Corporation.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks Limited.

To access more technical documentation, search our knowledge base, or open a service request online, please visit Nortel Networks Technical Support on the web at: http://www.nortel.com/support

If after following this guide you are still having problems, please ensure you have carried out the steps exactly as in this document. If problems still persist, please contact Nortel Networks Technical Support (contact information is available online at: http://www.nortel.com/cgi-bin/comments/comments.cgi?key=techsupport_cu).

We welcome your comments and suggestions on the quality and usefulness of this document. If you would like to leave a feedback please send your comments to: CRALT@nortel.com