# Esercizi sulle VPN Site-To-Site e Remote Access

# **VPN Site-To-Site**

 Un'azienda sottoscrive alcuni contratti presso un ISP per fornire connettività Internet alle sue tre filiali. Si suppone che l'infrastruttura dell'ISP sia composta da un router centrale a cui sono collegati tre router periferici utilizzati dalle filiali. Ogni router periferico è collegato a quello centrale attraverso un collegamento punto-punto; ogni collegamento dispone di una rete IP pubblica \30. Al router centrale è inoltre collegato il server web dell'ISP, anch'esso raggiungibile mediante un collegamento punto-punto e indirizzo pubblico.

Svolgere le seguenti attività:

- a) Realizzare in Packet Tracer l'infrastruttura di rete dell'ISP, configurando in particolare il router centrale, i router periferici e il server web utilizzando le seguenti reti IP: 200.1.2.0/30; 200.1.6.64/30; 200.1.8.192/30; 200.1.11.48/30 (utilizzare quest'ultima per il collegamento al server web, al quale deve essere assegnato l'indirizzo 200.1.11.49);
- b) Realizzare tre reti locali rappresentanti le filiali dell'azienda: ciascuna rete, di tipo *switch-based*, dovrà includere quattro client di tipo diverso (obbligatorio) e un web server (ogni filiale ne ha uno interno).
   Gli indirizzi IP da utilizzare per configurare le filiali sono indicati in figura.



- 2. A partire dall'infrastruttura creata al punto precedente, si realizzi una VPN site-to-site tra le filiali 1 e 2 avente le seguenti caratteristiche:
  - a) Policy per la creazione della *Security Association*: cifratura AES 256; algoritmo di hash di tipo SHA; autenticazione *pre-shared*; gruppo DH 5.
  - b) Chiave condivisa "SEGRETO12".
  - c) Set di trasformazione: ESP-AES 192; ESP-SHA-HMAC.

Verificare il corretto funzionamento accedendo al sito web della filiale n. 2 mediante un PC della filiale n. 1.

3. Realizzare le VPN *site-to-site* necessarie a garantire il collegamento sicuro tra tutte le filiali dell'azienda.

### **VPN Remote Access**

4. L'azienda permette ad alcuni lavoratori della prima filiale di operare in smart working. Per questo motivo, i telelavoratori hanno bisogno di collegarsi ai server della LAN di filiale utilizzando il proprio computer da casa.

Svolgere le seguenti attività:

- a) Estendere la rete realizzata in Packet Tracer negli esercizi precedenti aggiungendo un router domestico collegato a una nuova interfaccia del router centrale dell'ISP con un collegamento punto-punto da configurare a partire dalla rete IP 200.1.15.192/30. Collegare al router domestico il PC del telelavoratore a indirizzo IP dinamico (il servizio DHCP deve essere abilitato sul router del telelavoratore, i dettagli della rete LAN domestica e del servizio DHCP sono riportati in figura).
- 5. Realizzare una VPN Remote Access sul router della filiale n. 1 avente le seguenti caratteristiche:
  - a) Policy per la creazione della Security Association: cifratura AES 256; algoritmo di hash di tipo SHA; autenticazione pre-shared; gruppo DH 5 (se questa policy è già presente nel router R1, non deve essere creata nuovamente)
  - b) Pool DHCP per utenti remoti: da 10.0.0.100 a 10.0.0.150
  - c) Configurazione del client ISAKMP
    - Gruppo filiale1
    - Chiave del gruppo: **abc**
    - Associazione del pool DHCP creato precedentemente
  - d) Set di trasformazione: ESP-AES 192; ESP-SHA-HMAC (anche questa trasformazione può essere omessa se già presente sul router con le stesse impostazioni)
  - e) Mappa dinamica per le *Security Association* automatiche dei telelavoratori: la mappa utilizza il set di trasformazione creato al punto precedente e supporta il *reverse route* per l'inserimento automatico delle regole di routing necessarie
  - f) Autenticazione degli utenti tramite database locale. Le credenziali degli utenti sono memorizzate all'interno del router (lista **telelavoratori**)
  - g) Autorizzazione all'accesso alla rete per il gruppo filiale1
  - h) Definizione della mappa statica (si può integrare la mappa già presente nel router R1) contenente le seguenti informazioni:
    - Lista per l'autenticazione degli utenti
    - Lista per l'autorizzazione ISAKMP al gruppo
    - Configurazione client di tipo *address respond*
    - Collegamento alla mappa dinamica creata precedentemente
  - i) Aggiornamento delle ACL del processo NAT per evitare che gli indirizzi del traffico VPN siano modificati con quello del router

- j) Applicazione della mappa statica all'interfaccia seriale del router R1 (questa operazione non è richiesta se la mappa è già stata applicata negli esercizi precedenti).
- k) Creazione, all'interno del router, dell'utente **worker1** e password **123**



# Soluzioni

# Esercizio n. 1

### Configurazione router centrale (Router CISCO 1841 con quattro interfacce seriali e due Fast Ethernet)

```
enable
configure terminal
      interface serial 0/0/0
           ip address 200.1.2.2 255.255.255.252
           no shutdown
           exit
      interface serial 0/0/1
           ip address 200.1.6.66 255.255.255.252
           no shutdown
           exit
      interface serial 0/1/0
           ip address 200.1.8.194 255.255.255.252
           no shutdown
           exit
      interface fastEthernet 0/0
           ip address 200.1.11.50 255.255.255.252
           no shutdown
           exit
      exit
copy running-config startup-config
exit
```

### Configurazione router di filiale R1 (Router CISCO 1841 con due interfacce seriali e due Fast Ethernet)

```
enable
configure terminal
      interface serial 0/0/0
          ip address 200.1.2.1 255.255.255.252
          ip nat outside
          no shutdown
          exit
     interface fastEthernet 0/0
          ip address 10.255.255.254 255.0.0.0
          ip nat inside
          no shutdown
          exit
     ip route 0.0.0.0 0.0.0.0 200.1.2.2
     ip access-list extended NAT-RETE-LOCALE
           permit ip 10.0.0.0 0.255.255.255 any
           exit
     ip nat inside source list NAT-RETE-LOCALE interface Serial0/0/0 overload
     exit
copy running-config startup-config
exit
```

#### Configurazione router di filiale R2

```
(Router CISCO 1841 con due interfacce seriali e due Fast Ethernet)
```

```
enable
configure terminal
      interface serial 0/0/0
           ip address 200.1.6.65 255.255.255.252
           ip nat outside
          no shutdown
           exit
      interface fastEthernet 0/0
           ip address 172.16.255.254 255.255.0.0
           ip nat inside
          no shutdown
          exit
      ip route 0.0.0.0 0.0.0.0 200.1.6.66
      ip access-list extended NAT-RETE-LOCALE
            permit ip 172.16.0.0 0.0.255.255 any
            exit
      ip nat inside source list NAT-RETE-LOCALE interface Serial0/0/0 overload
      exit
copy running-config startup-config
exit
```

### Configurazione router di filiale R3 (Router CISCO 1841 con due interfacce seriali e due Fast Ethernet)

```
enable
configure terminal
      interface serial 0/0/0
          ip address 200.1.8.193 255.255.255.252
          ip nat outside
          no shutdown
          exit
     interface fastEthernet 0/0
          ip address 192.168.0.254 255.255.255.0
          ip nat inside
          no shutdown
          exit
     ip route 0.0.0.0 0.0.0.0 200.1.8.194
     ip access-list extended NAT-RETE-LOCALE
           permit ip 192.168.0.0 0.0.0.255 any
           exit
     ip nat inside source list NAT-RETE-LOCALE interface Serial0/0/0 overload
     exit
copy running-config startup-config
exit
```

### Configurazione della VPN LAN1-LAN2 sul router R1

```
enable
configure terminal
      crypto isakmp policy 1
           encryption aes 256
           hash sha
           authentication pre-share
           group 5
           exit
      crypto isakmp key SEGRET012 address 200.1.6.65
      ip access-list extended TRAFFICO-VPN12
           permit ip 10.0.0.0 0.255.255.255
                                               172.16.0.0 0.0.255.255
           exit
      crypto ipsec transform-set TRASFORMAZIONE esp-aes 192 esp-sha-hmac
      crypto map MAPPA-VPN 10 ipsec-isakmp
           set peer 200.1.6.65
           set transform-set TRASFORMAZIONE
           match address TRAFFICO-VPN12
           exit
      interface serial 0/0/0
           crypto map MAPPA-VPN
           exit
      ip access-list extended NAT-RETE-LOCALE
           no permit ip 10.0.0.0 0.255.255.255 any
           deny ip 10.0.0.0 0.255.255.255 172.16.0.0 0.0.255.255
           permit ip 10.0.0.0 0.255.255.255 any
           exit
      exit
copy running-config startup-config
exit
Configurazione della VPN LAN1-LAN2 sul router R2
enable
configure terminal
```

```
crypto isakmp policy 1
encryption aes 256
hash sha
authentication pre-share
group 5
exit
crypto isakmp key SEGRET012 address 200.1.2.1
ip access-list extended TRAFFICO-VPN12
permit ip 172.16.0.0 0.0.255.255 10.0.0.0 0.255.255.255
exit
```

exit

crypto ipsec transform-set TRASFORMAZIONE esp-aes 192 esp-sha-hmac crypto map MAPPA-VPN 10 ipsec-isakmp set peer 200.1.2.1 set transform-set TRASFORMAZIONE match address TRAFFICO-VPN12 exit interface serial 0/0/0 crypto map MAPPA-VPN exit ip access-list extended NAT-RETE-LOCALE no permit ip 172.16.0.0 0.0.255.255 any deny ip 172.16.0.0 0.0.255.255 10.0.0.0 0.255.255.255 permit ip 172.16.0.0 0.0.255.255 any exit exit copy running-config startup-config

#### Configurazione della VPN LAN1-LAN3 sul router R1

```
! Si suppone che il router sia già configurato con i dati della VPN 1-2
enable
configure terminal
      crypto isakmp key SEGRET013 address 200.1.8.193
      ip access-list extended TRAFFICO-VPN13
           permit ip 10.0.0.0 0.255.255.255 192.168.0.0 0.0.0.255
           exit
      ! Uso della mappa multi-entry.
      ! Si inserisce una nuova entry (la numero 20) all'interno della mappa
      ! creata nell'esercizio precedente
      crypto map MAPPA-VPN 20 ipsec-isakmp
           set peer 200.1.8.193
            set transform-set TRASFORMAZIONE
           match address TRAFFICO-VPN13
           exit
      ip access-list extended NAT-RETE-LOCALE
           no permit ip 10.0.0.0 0.255.255.255 any
           deny ip 10.0.0.0 0.255.255.255
                                            192.168.0.0 0.0.0.255
           permit ip 10.0.0.0 0.255.255.255 any
           exit
      exit
copy running-config startup-config
exit
```

#### Configurazione della VPN LAN1-LAN3 sul router R3

```
! Prima configurazione del router R3
enable
configure terminal
     crypto isakmp policy 1
           encryption aes 256
           hash sha
           authentication pre-share
           group 5
           exit
     crypto isakmp key SEGRET013 address 200.1.2.1
     ip access-list extended TRAFFICO-VPN13
           permit ip 192.168.0.0 0.0.0.255
                                              10.0.0.0 0.255.255.255
           exit
     crypto ipsec transform-set TRASFORMAZIONE esp-aes 192 esp-sha-hmac
     crypto map MAPPA-VPN 10 ipsec-isakmp
           set peer 200.1.2.1
```

```
set transform-set TRASFORMAZIONE
match address TRAFFICO-VPN13
exit
interface serial 0/0/0
    crypto map MAPPA-VPN
    exit
ip access-list extended NAT-RETE-LOCALE
    no permit ip 192.168.0.0 0.0.0.255 any
    deny ip 192.168.0.0 0.0.0.255 10.0.0.0 0.255.255.255
    permit ip 192.168.0.0 0.0.0.255 any
    exit
exit
copy running-config startup-config
exit
```

#### Configurazione della VPN LAN2-LAN3 sul router R2

```
! Si suppone che il router sia già configurato con i dati della VPN 1-2
enable
configure terminal
     crypto isakmp key SEGRET023 address 200.1.8.193
     ip access-list extended TRAFFICO-VPN23
           permit ip 172.16.0.0 0.0.255.255 192.168.0.0 0.0.0.255
           exit
      ! Uso della mappa multi-entry.
      ! Si inserisce una nuova entry (la numero 20) all'interno della mappa
      ! creata nell'esercizio precedente
     crypto map MAPPA-VPN 20 ipsec-isakmp
           set peer 200.1.8.193
           set transform-set TRASFORMAZIONE
           match address TRAFFICO-VPN23
           exit
     ip access-list extended NAT-RETE-LOCALE
           no permit ip 172.16.0.0 0.0.255.255 any
           deny ip 172.16.0.0 0.0.255.255 192.168.0.0 0.0.0.255
           permit ip 172.16.0.0 0.0.255.255 any
           exit
      exit
copy running-config startup-config
exit
```

#### Configurazione della VPN LAN2-LAN3 sul router R3

```
! Si suppone che il router sia già configurato con i dati della VPN 1-3
enable
configure terminal
    crypto isakmp key SEGRET023 address 200.1.6.65
    ip access-list extended TRAFFICO-VPN23
```

exit

permit ip 192.168.0.0 0.0.0.255 172.16.0.0 0.0.255.255 exit ! Uso della mappa multi-entry. ! Si inserisce una nuova entry (la numero 20) all'interno della mappa ! creata nell'esercizio precedente crypto map MAPPA-VPN 20 ipsec-isakmp set peer 200.1.6.65 set transform-set TRASFORMAZIONE match address TRAFFICO-VPN23 exit ip access-list extended NAT-RETE-LOCALE no permit ip 192.168.0.0 0.0.0.255 any deny ip 192.168.0.0 0.0.0.255 172.16.0.0 0.0.255.255 permit ip 192.168.0.0 0.0.0.255 any exit exit copy running-config startup-config

### Configurazione nuova interfaccia router centrale per collegamento a router domestico (Router CISCO 1841 con quattro interfacce seriali e due Fast Ethernet)

```
enable
configure terminal
    interface fastEthernet 0/1
        ip address 200.1.15.194 255.255.255.252
        no shutdown
        exit
        exit
        copy running-config startup-config
exit
```

					_		55 H broadballa Roater	
Setup	Setup Basia Sat	Wireless	Securit	V Re	Access	Applications & Gaming	Administration	Stat
	Dasic Sett	up	DDNS		MAC Addre	ess cione	Advanced Rou	ung
Internet Setup								
Internet	Static IP		$\sim$				Help	
Connection type								
-		000		45	402			
	Internet IP Address:	200	] . <u>1</u>	. 15	. 193			
	Subnet Mask:	255	. 255	. 255	. 252			
	Default Gateway:	200	. 1	. 15	. 194			
	DNS 1:	0	. 0	. 0	. 0			
	DNS 2 (Optional):	0	. 0	. 0	. 0			
	DNS 3 (Optional):	0	. 0	. 0	. 0			
Ontional Settings	Host Name:							
required by some	Domain Name:							
(required by some internet service providers)	Domain Name: MTU:	Size: 15	00					
(required by some internet service providers)	Domain Name: MTU:	Size: 15	00					
(required by some internet service providers)	Domain Name: MTU:	Size: 15	00				_	
required by some internet service providers) Network Setup Bouter IP	Domain Name: MTU:	Size: 15	. 168	. 10	. 254		_	
Router IP	Domain Name: MTU: IP Address: Subnet Mask:	<ul> <li>Size: 15</li> <li>192</li> <li>255.255.2</li> </ul>	. 168 255.252	. 10	. 254	~		
Router IP	Domain Name: MTU: MTU: MTU: MTU: MTU: MTU: MTU: MTU	Size: 15	. 168	. 10	. 254			
required by some internet service providers) Network Setup Router IP DHCP Server Settings	Domain Name: MTU: IP Address: Subnet Mask: DHCP Server:	Size: 15	00 . 168	Disablec	. 254	DHCP Reservation	n	
Router IP DHCP Server Settings	Domain Name: MTU: IP Address: Subnet Mask: DHCP Server: Start IP Address: 19	Size: 15	00 . <u>168</u> 255.252	Disabled	. 254	DHCP Reservation	n	
required by some internet service providers) Network Setup Router IP DHCP Server Settings	Domain Name: MTU: IP Address: Subnet Mask: DHCP Server: Start IP Address: 19 Maximum number of Users:	<ul> <li>Size: 15</li> <li>192</li> <li>255.255.2</li> <li>Enabled</li> <li>32.168.10. 1</li> <li>20</li> </ul>	00 . 168	Disablec	. 254	DHCP Reservation	n	
required by some internet service providers) Network Setup Router IP DHCP Server Settings	Domain Name: MTU: IP Address: Subnet Mask: DHCP Server: Start IP Address: 19 Maximum number of Users: IP Address Range: 1	<ul> <li>Size: 15</li> <li>192</li> <li>255.255.2</li> <li>Enabled</li> <li>92.168.10.</li> <li>192.168.10.</li> </ul>	00 . <u>168</u> 255.252 101 . 120	Disabled	. 254	DHCP Reservation	n	
Network Setup Router IP DHCP Server Settings	Domain Name: MTU: IP Address: Subnet Mask: DHCP Server: Start IP Address: 19 Maximum number of Users: IP Address Range: Client Lease Time:	Size: 15	00 . 168 255.252 101 101 - 120	Disablec	. <u>254</u>	DHCP Reservation	n	
Router IP DHCP Server Settings	Domain Name: MTU: IP Address: Subnet Mask: DHCP Server: Start IP Address: 19 Maximum number of Users: IP Address Range: 1 Client Lease Time: Static DNS 1: 0	Size: 15	00 . 168 255.252 101 101 - 120 . 0	Disablec	. <u>254</u>	DHCP Reservation minutes (0 means	n	
required by some internet service providers) Network Setup Router IP DHCP Server Settings	Domain Name: MTU: IP Address: Subnet Mask: DHCP Server: Start IP Address: 19 Maximum number of Users: IP Address Range: IP Address Range: Client Lease Time: Static DNS 1: O Static DNS 2: O	Size: 15	00 . 168 255.252 101 . 101 . 0 . 0 . 0	Disabled	. <u>254</u>	DHCP Reservation minutes (0 means . 0 . 0	ns one day)	
Router IP DHCP Server Settings	Domain Name: MTU: IP Address: Subnet Mask: DHCP Server: Start IP Address: IP Address: IP Address Range: Client Lease Time: Static DNS 1: Static DNS 2: O Static DNS 3: O	Size: 15	00 . 168 255.252 101 101 - 120 . 0 . 0 . 0	Disablec	. <u>254</u> d . <u>0</u> . <u>0</u>	DHCP Reservation	n	

# Configurazione router domestico (Router Wireless WRT300N)

#### Configurazione della VPN Remote Access sul router R1

```
! Si suppone che il router sia già configurato con i dati delle VPN Site-To-Site
enable
configure terminal
ļ
     crypto isakmp policy 1
ļ
           encryption aes 256
ļ
           hash sha
ļ
           authentication pre-share
Į.
           group 5
ļ
           exit
     ip local pool POOL-VPN 10.0.0.100 10.0.0.150
     crypto isakmp client configuration group filiale1
           key abc
           pool POOL-VPN
           exit
ļ
     crypto ipsec transform-set TRASFORMAZIONE esp-aes 192 esp-sha-hmac
     crypto dynamic-map MAPPA-VPN-DINAMICA 100
           set transform-set TRASFORMAZIONE
           reverse-route
           exit
     aaa new-model
     aaa authentication login telelavoratori local
     aaa authorization network filiale1 local
     crypto map MAPPA-VPN client authentication list telelavoratori
     crypto map MAPPA-VPN client configuration address respond
     crypto map MAPPA-VPN isakmp authorization list filiale1
     crypto map MAPPA-VPN 30 ipsec-isakmp dynamic MAPPA-VPN-DINAMICA
     ip access-list extended NAT-RETE-LOCALE
           no permit ip 10.0.0.0 0.255.255.255 any
           deny ip 10.0.0.0 0.255.255.255 10.0.0.0 0.255.255.255
           permit ip 10.0.0.0 0.255.255.255 any
           exit
ļ
     interface serial 0/0/0
           crypto map MAPPA-VPN
L
           exit
ļ
     username worker1 password 123
     exit
copy running-config startup-config
exit
```

# Configurazione del client VPN sul laptop del telelavoratore

(	≷ Laptop0							—		×
	Physical	Config	Desktop	Programming	Attributes					
	VPN Config	uration								х
	VPN									
	GroupNar	ne:	filiale1							
	Group Ke	y:	abc							
	Host IP (S	Server IP):	200.1.2.1							
	Username	e	worker1							
	Password	I	123							
									Conne	ct

## Conferma della connessione alla LAN della filiale mediante VPN Remote Access

(	Laptop(	D					—		×
	Physical	Config	Desktop	Programming	Attributes				
	VPN Conf	iguration							Х
	Client IP:					10.0.0.101			
								Disconr	nect

# Test di raggiungibilità del server di filiale dal computer del telelavoratore

Physical Config Desktop Programming Attributes         Command Prompt       X         Cisco Packet Tracer PC Command Line 1.0          C:\>ping 10.0.0.1       Pinging 10.0.0.1         Pinging 10.0.0.1 with 32 bytes of data:          Request timed out.          Reply from 10.0.0.1: bytes=32 time=2ms TTL=127          Reply from 10.0.0.1: bytes=32 time=2ms TTL=127          Reply from 10.0.0.1: bytes=32 time=2ms TTL=127          Ping statistics for 10.0.0.1:          Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),         Approximate round trip times in milli-seconds:         Minimum = 2ms, Maximum = 2ms, Average = 2ms         C:\>	R Laptop0	-	-	×
Command Prompt Cisco Packet Tracer PC Command Line 1.0 C:\>ping 10.0.0.1 Pinging 10.0.0.1 with 32 bytes of data: Request timed out. Reply from 10.0.0.1: bytes=32 time=2ms TTL=127 Reply from 10.0.0.1: bytes=32 time=2ms TTL=127 Reply from 10.0.0.1: bytes=32 time=2ms TTL=127 Ping statistics for 10.0.0.1: Packets: Sent = 4, Received = 3, Lost = 1 (25% loss), Approximate round trip times in milli-seconds: Minimum = 2ms, Maximum = 2ms, Average = 2ms C:\>	Physical Config Desktop Programming Attributes			
Cisco Packet Tracer PC Command Line 1.0 C:\>ping 10.0.0.1 Pinging 10.0.0.1 with 32 bytes of data: Request timed out. Reply from 10.0.0.1: bytes=32 time=2ms TTL=127 Reply from 10.0.0.1: bytes=32 time=2ms TTL=127 Reply from 10.0.0.1: bytes=32 time=2ms TTL=127 Ping statistics for 10.0.0.1: Packets: Sent = 4, Received = 3, Lost = 1 (25% loss), Approximate round trip times in milli-seconds: Minimum = 2ms, Maximum = 2ms, Average = 2ms C:\>	Command Prompt			Х
<pre>Request timed out. Reply from 10.0.0.1: bytes=32 time=2ms TTL=127 Reply from 10.0.0.1: bytes=32 time=2ms TTL=127 Reply from 10.0.0.1: bytes=32 time=2ms TTL=127 Ping statistics for 10.0.0.1: Packets: Sent = 4, Received = 3, Lost = 1 (25% loss), Approximate round trip times in milli-seconds: Minimum = 2ms, Maximum = 2ms, Average = 2ms C:\&gt;</pre>	Cisco Packet Tracer PC Command Line 1.0 C:\>ping 10.0.0.1 Pinging 10.0.0.1 with 32 bytes of data:			
<pre>Reply from 10:0:0:1: bytes=32 time=2ms TIL=127 Reply from 10:0:0:1: bytes=32 time=2ms TIL=127 Ping statistics for 10:0:0:1:     Packets: Sent = 4, Received = 3, Lost = 1 (25% loss), Approximate round trip times in milli-seconds:     Minimum = 2ms, Maximum = 2ms, Average = 2ms C:\&gt;</pre>	Request timed out.			
<pre>Reply from 10.0.0.1: bytes=32 time=2ms TTL=127 Ping statistics for 10.0.0.1:     Packets: Sent = 4, Received = 3, Lost = 1 (25% loss), Approximate round trip times in milli-seconds:     Minimum = 2ms, Maximum = 2ms, Average = 2ms C:\&gt;</pre>	Reply from 10.0.0.1: bytes=32 time=2ms TTL=127 Reply from 10.0.0.1: bytes=32 time=2ms TTL=127			
<pre>Ping statistics for 10.0.0.1: Packets: Sent = 4, Received = 3, Lost = 1 (25% loss), Approximate round trip times in milli-seconds: Minimum = 2ms, Maximum = 2ms, Average = 2ms C:\&gt;</pre>	Reply from 10.0.0.1: bytes=32 time=2ms TTL=127			
	<pre>Ping statistics for 10.0.0.1: Packets: Sent = 4, Received = 3, Lost = 1 (25% loss), Approximate round trip times in milli-seconds: Minimum = 2ms, Maximum = 2ms, Average = 2ms C:\&gt;</pre>			