

Tecnologias de Redes de Computadores - 90398

Apresentação 11 – Network Address Translation

Pedro Gonçalves - pasg@ua.pt

Sumário

- Network Address Translation:

- motivação do aparecimento
- funcionamento básico
- limitações do processo.
- Tipos de NAT típicos
- Configuração NAT

- Stateful NAT

- Necessidade e configuração




NAT – Network Address Translation

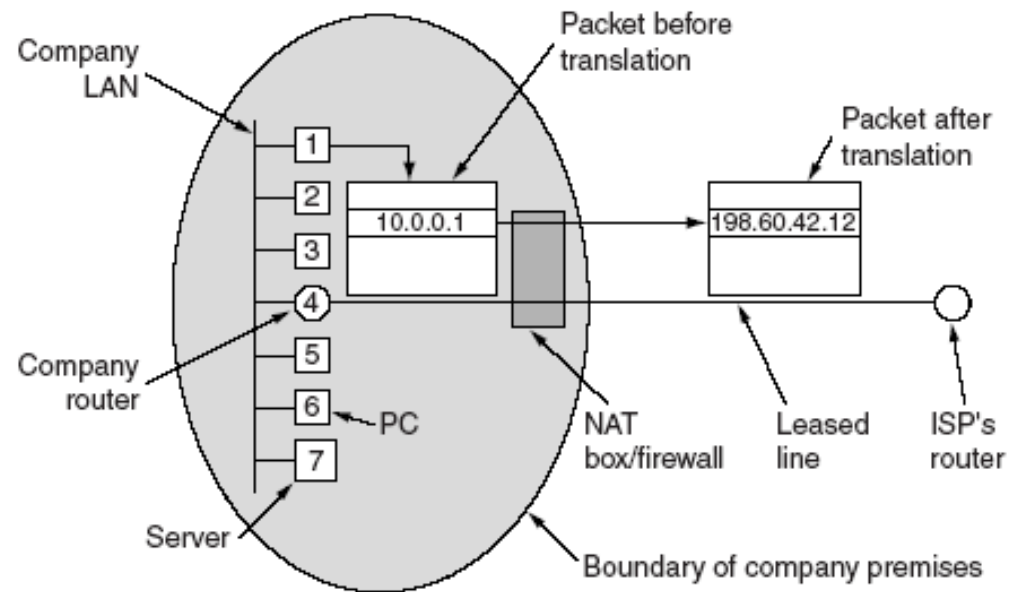
- Definido na RFC 1631 de 1994.
 - <http://www.rfc-base.org/rfc-1631.html>
 - Usado devido à falta de endereços.
- Vulgar em ISP para poupar nos preços do aluguer de endereços.
- Usado em empresas para ligar todas as maquinas da rede usando um endereço publico.
- Funciona traduzindo endereços dos pacotes na extremidade de uma rede.
- Transparente à rede (desde que seja configurado na *default gateway*)
- Uma medida de segurança: esconde a rede privada da rede pública



Endereços Privados Reservados

- 10.0.0.0 – 10.255.255.255 – 10.0.0.0/8
 - 172.16.0.0 – 172.16.255.255 – 172.16.0.0/12
 - 192.168.0.0 – 192.168.255.255 – 192.168.0.0/16
- 
- São cerca de 17,000,000 endereços privados
 - PRIVATE significa que não são endereçáveis da Internet.

Network Address Translators



Vantagens do NAT

- Minimiza a utilização de endereços IP
- Conserva o esquema de endereçamento interno das intranets;
- ***Aumenta a flexibilidade da ligação à rede pública*** – Permite várias ligações, ligações de backup e balanceamento de carga das ligações.
- Permite que o esquema de endereçamento interno seja alterado de uma forma transparente para o exterior.



Problemas do NAT

- Quebra a regra de 1 máquina – 1 endereço.
- Implementações mais básicas não suportam FTP nem H323.
Implementações mais complexas obrigam à leitura de informação nas camadas superiores.
- Não suporta algo que não seja TCP ou UDP.
 - há implementações que acabam por resolver o problema ao custo de desempenho
- Viola a regra de uma camada só falar com as adjacentes.
- Aumenta o atraso.
- Razão de não se usar IPv6 hoje



NAT - Funcionamento

- Quando um pacote chega ao router vindo da **rede privada**, este vai retirar o **IP-ORIGEM** do cabeçalho IP, e colocar lá o seu **IP-PUBLICO-DE-SAÍDA**
 - Portos origem/destino também podem ser mudados
- Esta tradução fica armazenada na **tabela de NAT** do router
 - Todas as conexões (rede pública<->rede privada) são registadas
 - Quando as ligações são fechadas, o registo é apagado da tabela
 - A operação da tabela depende do modo de NAT usado
- Quando chegar a resposta a esse pacote, o router analisa a **tabela de NAT**, e executa a operação inversa
 - Neste caso, o endereço de **DESTINO** é alterado para o endereço privado



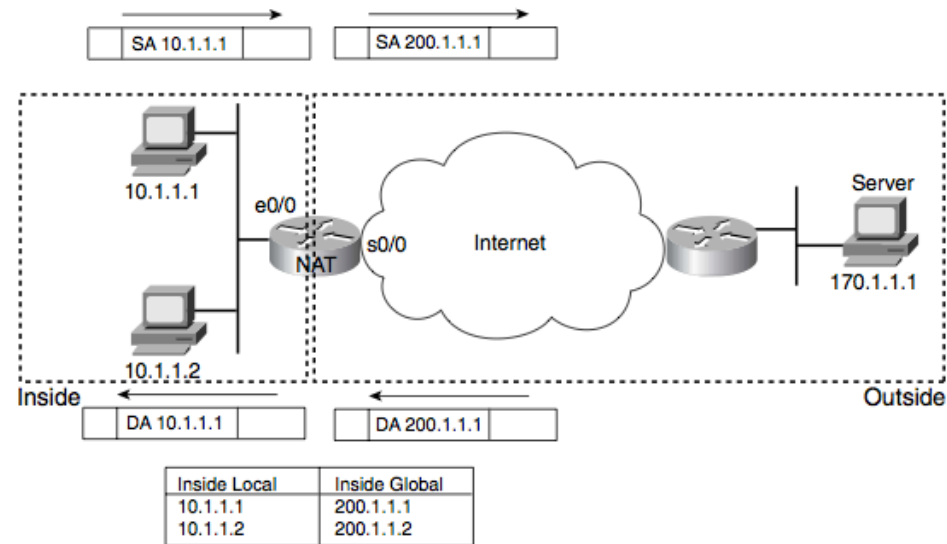
- Pedidos feitos à rede referentes às 2 primeiras linhas da tabela
- (IPP_NAT, 14003, 128.10.19.20, 80)
- (IPP_NAT, 140010, 128.10.19.20, 80)

Private Address	Private Port	External Address	External Port	NAT Port	Protocol Used
10.0.0.5	21023	128.10.19.20	80	14003	tcp
10.0.0.1	386	128.10.19.20	80	14010	tcp
10.0.2.6	26600	207.200.75.200	21	14012	tcp
10.0.0.3	1274	128.210.1.5	80	14007	tcp



Tipos de NAT

NAT estático

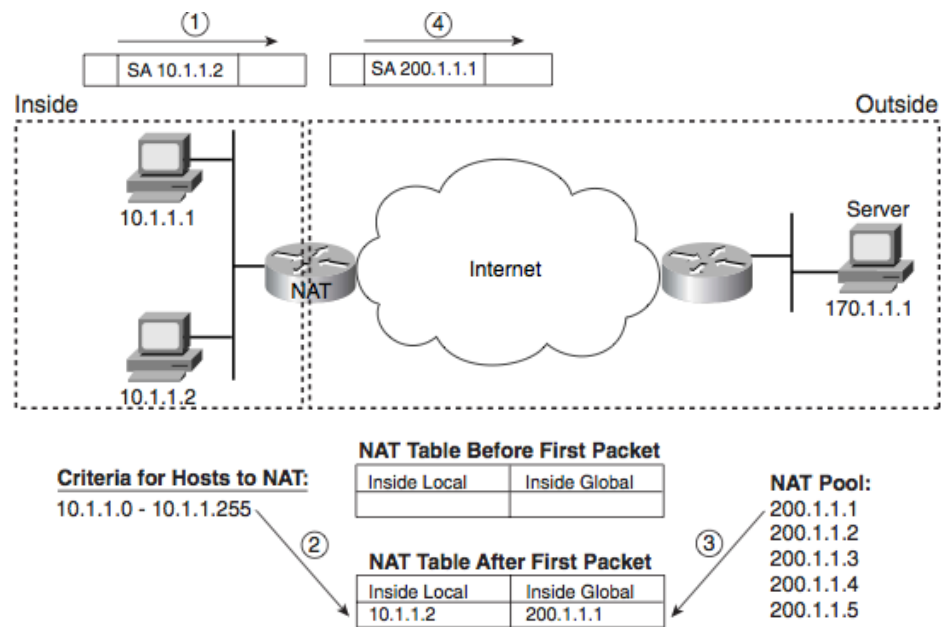


NAT Estático

- Mapeamento direto de máquinas da rede interna, para um endereço público
- Pouco usado em redes pequenas
- Usado para dar IP público a hosts dentro da rede privada de forma transparente
- Cada IP privado precisa de um IP público respetivo
 - Mapeamento máquina-a-máquina, entre endereço privado e público
 - Fica uma “regra” estática registada no router
- Perigoso: má configuração pode levar à exposição total da máquina, na Internet
- Exemplo: DMZ ZONE
 - Podemos expor à Internet máquinas tanto da DMZ como da rede privada, fazendo NAT estático



NAT dinâmico, sem Port Translation



NAT Dinâmico

- Também não é comumente usado em redes pequenas
- Mas encontra-se facilmente em empresas grandes com redes complexas
- Faz o mapeamento usando um grupo (pool ? reserva) de endereços públicos disponíveis
 - O mapeamento (escolha de qual o endereço público) é aleatório e vai-se manter enquanto a conexão estiver ativa
- Não fica nenhuma regra “estática” registada no router
- As regras ativam-se dinamicamente quando chega um pacote
- Após um timeout sem tráfego, as regras ativas desaparecem
- Exemplo:
 - Quando os utilizadores da rede privada estão a usar DHCP, e os seus endereços variam dinamicamente



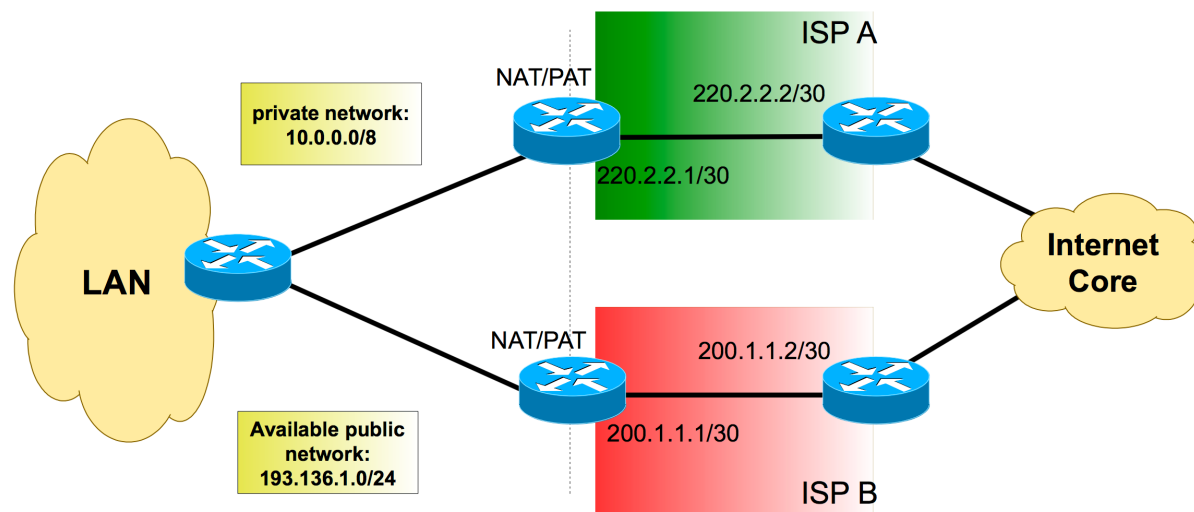
NAT Overload

- Também conhecido por NAPT (Network Address Port Translation), IP Masquerading e NAT-PAT (Port Address Translation)
- Forma mais comum de utilização de NAT
 - Permite todas as máquinas de uma rede privada de acederem à Internet através de uma conexão, e usando um endereço IP único
 - Usa portos para identificar/diferenciar a sessão de cada máquina privada
- A tabela NAT também regista o **porto de origem** (para além do **porto de destino**).
- Desta forma, é possível distinguir pedidos diferentes feitos a partir de máquinas diferentes na rede privada, para o mesmo servidor na rede pública
- Exemplo:
 - 2 máquinas da rede privada acedem a um servidor web na Int
- Pedidos feitos à rede referentes às 2 primeiras
 - (IPP_NAT, 14003, 128.10.19.20, 80)
 - (IPP_NAT, 140010, 128.10.19.20, 80)

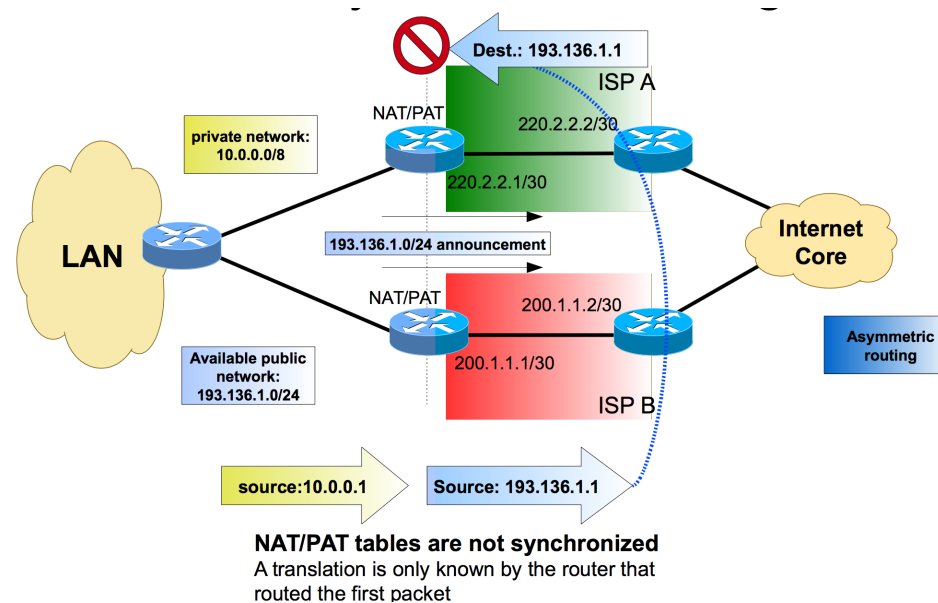


Private Address	Private Port	External Address	External Port	NAT Port	Protocol Used
10.0.0.5	21023	128.10.19.20	80	14003	tcp
10.0.0.1	386	128.10.19.20	80	14010	tcp
10.0.2.6	26600	207.200.75.200	21	14012	tcp
10.0.0.3	1274	128.210.1.5	80	14007	tcp

NAT/PAT com Múltiplos ISP



NAT/PAT com múltiplos ISP e encaminhamento simétrico

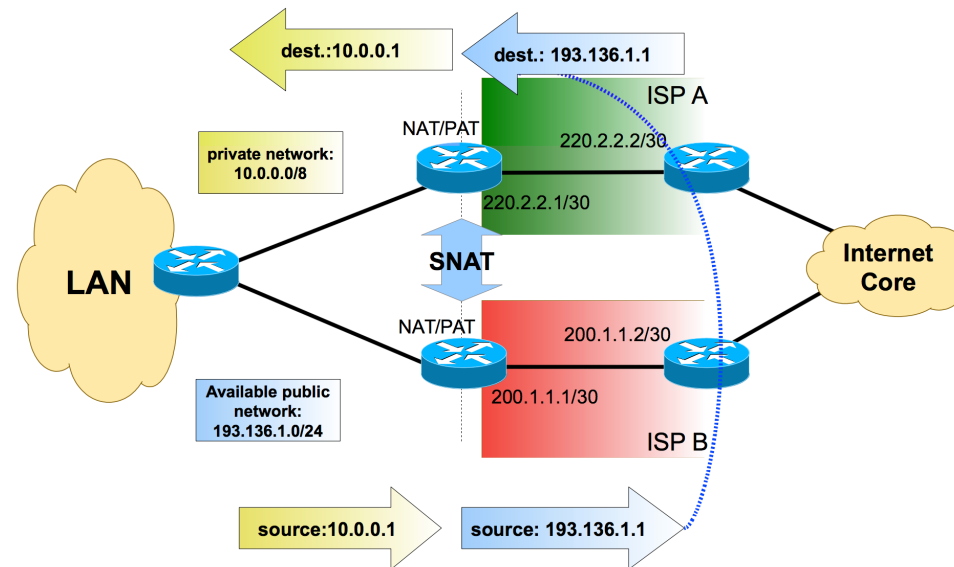


NAT State Synchronization

- Internet Draft proposals
 - NAT State Synchronization Using SCSP
 - Server Cache Synchronization Protocol (SCSP)
 - Framework de Redundância e Load Balancing para Stateful Network Address Translators (NAT)
- Solução Cisco (já em equipamentos Cisco's) Stateful NAT
 - Solução Proprietária, detalhes não conhecidos
 - Sincronização de dados em em TCP
 - Necessário to definir a primary server (outros são os backup servers)



Stateful NAT





Configuração do NAT em equipamentos Cisco

Static NAT

```
interface Ethernet0/0
```

```
    ip address 10.1.1.3 255.255.255.0
```

```
    ip nat inside
```

Definição do interface interno

```
interface Serial0/0
```

```
    ip address 200.1.1.251 255.255.255.0
```

Definição de interface externo

```
    ip nat outside
```

Definição máquina a máquina da tradução

```
ip nat inside source static 10.1.1.2 200.1.1.2
```

```
ip nat inside source static 10.1.1.1 200.1.1.1
```



Dynamic NAT com pool

```
interface Ethernet0/0
    ip address 10.1.1.3 255.255.255.0
    ip nat inside
interface Serial0/0
    ip address 200.1.1.251 255.255.255.0
    ip nat outside
```

!

```
ip nat pool fred 200.1.1.1 200.1.1.2 netmask 255.255.255.252
ip nat inside source list 1 pool fred [overload]
```

!

```
access-list 1 permit 10.1.1.0 0.0.0.255
```


Pool de endereços para os quais é feita a tradução

Definição de processo de tradução

Lista de acesso que define que endereços são traduzidos

Nota: overload permite utilização dos portos para poder reutilizar mesmo endereço da pool por vários fluxos da rede privada

Dynamic NAT com endereço externo

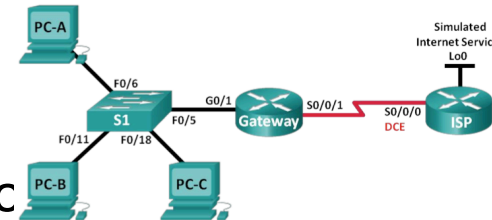


```
interface Ethernet0/0
    ip address 10.1.1.3 255.255.255.0
    ip nat inside
interface Serial0/0
    ip address dhcp
    ip nat outside
!
ip nat inside source list 1 interface s0/0
!
access-list 1 permit 10.1.1.0 0.0.0.255
```

Definição de processo de tradução

Lista de acesso que define que endereços são traduzidos

NAT overloading



- Definição de ACL que deixe passar tráfego

```
Gateway(config)# access-list 1 permit 192.168.1.0 0.0.0.255
```

- Associar a lista interna com o interface exterior:

```
Gateway(config)# ip nat inside source list 1  
interface serial 0/0
```

- Identificar os interfaces NAT interno e externo:

```
Gateway(config)# interface g0/1  
Gateway(config-if)# ip nat inside  
Gateway(config-if)# interface s0/0/1  
Gateway(config-if)# ip nat outside
```



NAT pool (c/ ou s/) overloading

- Definição de ACL (Access Control List) que deixe passar tráfego:

```
Gateway(config)# access-list 1 permit 192.168.1.0 0.0.0.255
```

- Definição de pool de endereços públicos:

```
Gateway(config)# ip nat pool public access 209.165.200.225  
209.165.200.230 netmask 255.255.255.248
```

- Aplicação de NAT à porta exterior:

```
Gateway(config)# ip nat inside source list 1 pool  
public_access overload
```

- Identificar os interfaces NAT interno e externo:

```
Gateway(config)# interface g0/1  
Gateway(config-if)# ip nat inside  
Gateway(config-if)# interface s0/0/1  
Gateway(config-if)# ip nat outside
```



Port NAT

```
interface ethernet 0
ip address 10.1.1.1 255.255.255.0
ip nat inside
```

!--- Defines Ethernet 0 with an IP address and as a NAT inside interface.

```
interface serial 0
ip address 193.135.66.44
ip nat outside
```

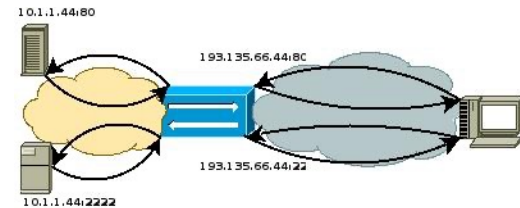
!--- Defines serial 0 with an IP address and as a NAT outside interface.

```
ip nat inside source static tcp 10.1.1.44 80 193.135.66.44 80 extendable
```

!--- Comando Port NAT que indica que pedido ao interface externo do NAT

!--- porto 80 de 193.135.66.44

!--- é reencaminhado para o porto 80 de 193.135.66.44



Stateful NAT

- #SNAT configuration

```
Router2(config)# ip nat Stateful id 2
```

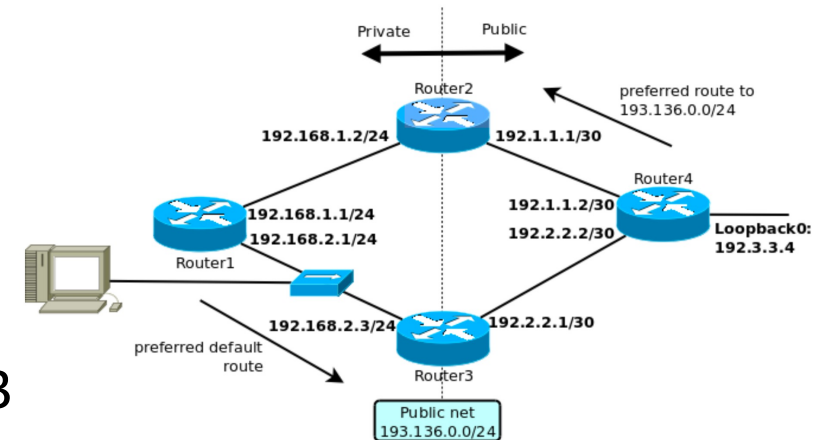
```
Router2(config-ipnat-snat)# backup 192.168.1.2
```

```
Router2(config-ipnat-snat-bkp)# peer  
192.168.2.3
```

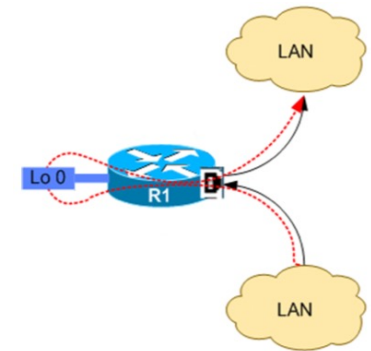
```
Router3(config)# ip nat Stateful id 3
```

```
Router3(config-ipnat-snat)# primary 192.168.2.3
```

```
Router3(config-ipnat-snat-bkp)# peer  
192.168.1.2
```



Interfaces de Loopback/lógicas



- Uma interface de loopback/lógica é uma interface virtual que esta sempre ativa (enquanto o router também estiver)
- Permite fazer conexões router-a-router independentemente das interfaces físicas
 - Ideal para terminações de Túneis
 - Ligações ponto-a-ponto aos nós vizinhos (e.g., protocolo de encaminhamento BGP).
- Também são usados como identificador base em vários mecanismos de rede.
- Configurado da mesma forma que as outras interfaces de layer 3.





NAT em Linux

NAT em Linux

- Implementado através de iptables
- Fica a dica, trataremos disso mais tarde.

- Sintaxe



```
iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to-source  
yourserverpublicIPAddress
```

- Exemplo:

```
iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to-source 192.168.229.115
```

Mais informação

- Fernandes B., Bernardes M., "TCP/IP Teoria e Prática", FCA, 2012
- Kurose J., Ross K., "Computer Networking: a Top-Down Approach", 5th edition, Addison Wesley, 2009
- Internetworking with TCP-IP, Douglas E. Comer



E é tudo...

- Questões?
- Comentários?

