

INSTITUTO FEDERAL
PIAUÍ
Campus Parnaíba

Equipamentos de Rede

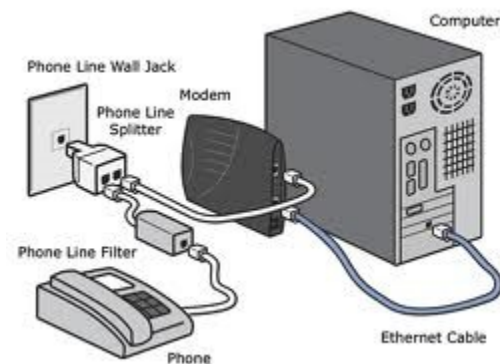
Prof. Msc Denival A. dos Santos

INTRODUÇÃO

- Hoje não faz muito sentido criar uma LAN isolada do resto do mundo. A necessidade de transferência de dados fruto da redução de custos e da dinamicidade do mundo moderno praticamente impõe esta conexão.
- Para que uma rede de computadores possa funcionar é necessário que existam, além do cabeamento propriamente dito, dispositivos de hardware e software cuja função é controlar a comunicação entre os diversos componentes da rede.
- Vários dispositivos são usados em uma rede, cada um deles possuindo funções específicas. Como exemplos de equipamentos dedicados podemos citar as placas de rede, os hubs, switches, bridges, routers, etc. que tem a finalidade de interpretar os sinais digitais processados na rede e encaminhá-los ao destino; ou seja, são o coração da rede permitindo que todos os pontos da rede comuniquem entre si.
- Essa interação entre dispositivos permite o compartilhamento das informações entre todos os usuários da rede.

MODEM

- O Modem é um dispositivo conversor de sinais que faz a comunicação entre computadores através de uma linha dedicada para esse fim. Seu nome é a contração das palavras MOdulador e DEModulador, pois essas são suas principais funções.



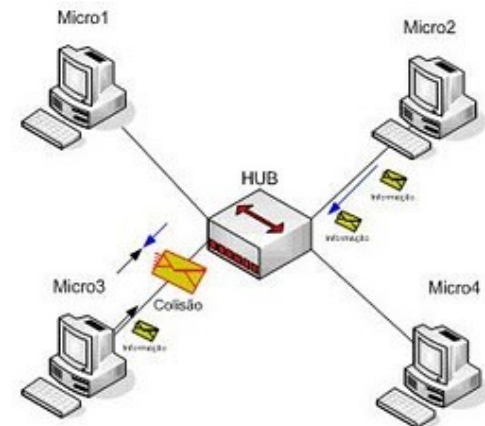
PLACA DE REDE

- A placa de rede ou adaptador de LAN ou ainda NIC (Network Interface Card), juntamente com o SO, trabalha para poder transmitir e receber mensagens a partir da rede. Funciona como uma interface entre o computador e o cabeamento da rede e suas funções básicas são gerar o sinal elétrico que trafega através do cabo da rede e controlar o fluxo de dados no sistema de cabeamento da rede.
- Especificações que devem ser levadas em consideração:
 - **Tipo de Barramento** - Ex: ISA, EISA, PCI, MCA, etc.;
 - **Conector da Placa** - Ex: RJ, BNC, ST, RJ/BNC, RJ/ST, MIC, etc;
 - **Padrão** - Ex: Ethernet, Fast-Ethernet, Token-Ring, FDDI, ATM, etc.;
 - **Velocidade de Transmissão** - 10 Mbps, 100 Mbps, 1Gbps, 10Gbps, etc.



HUB

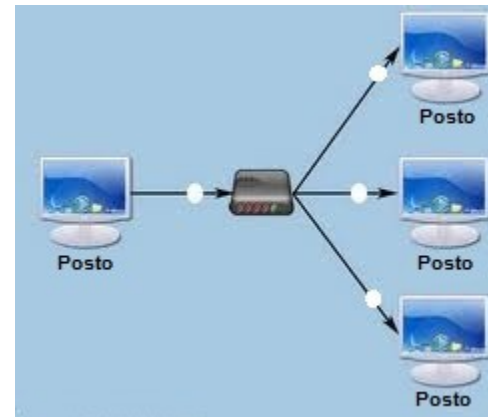
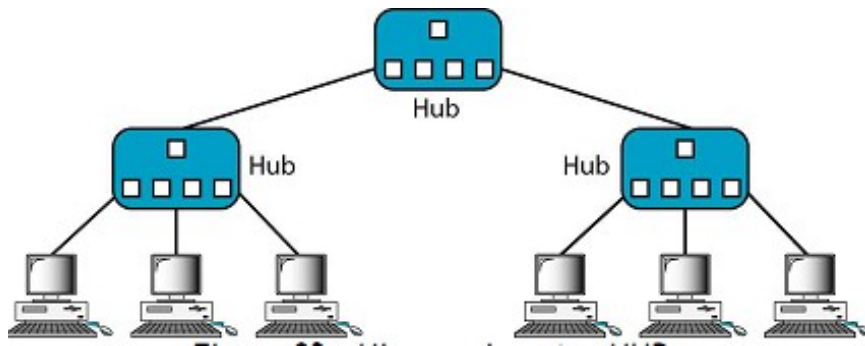
- Um hub consiste num repetidor multiportas, ou seja, ao receber a informação de uma porta, ele distribui por todas as outras. O Hub é basicamente um pólo concentrador de fiação e cada equipamento conectado a ele fica em um seguimento próprio.
- Todos os usuários conectados a um único hub ou uma pilha de hubs, compartilham o mesmo segmento e a mesma largura de banda.
- Um Hub permite apenas que os utilizadores compartilhem Ethernet e todos os nós do segmento Ethernet irão partilhar o mesmo domínio de colisão. À medida que uma rede composta por hubs, cresce muito passamos a ter problemas de performance.



HUB

▪ Domínio de colisão

- É uma área lógica onde os pacotes podem *colidir* uns contra os outros. A utilização de *hubs* faz propagar o domínio de colisão a todos os segmentos da rede. Em redes Ethernet, ao utilizar um hub, temos uma topologia lógica de barramento e as estações comportam-se com se estivessem todas ligadas a um único meio físico. O protocolo de comunicação CSMA/CD que controla o acesso ao meio em redes Ethernet minimiza este problema.
- **Observação:** Switches e Bridges são utilizados para separar domínios de colisão que são demasiado grandes de forma a melhorar a performance e a estabilidade da rede.



PONTE (BRIDGE)

- Com a bridge é possível fazer uma filtragem de entrega, pois ao verificar o MAC address, ela determina que interface receba o frame enviado.
 - Filtragem é a capacidade de um dispositivo determinar se um frame (quadro ou pacote) deve ser repassado para alguma interface ou deve ser descartado. A filtragem e o repasse são feitos através de uma tabela de comutação.
- As Bridges (ou pontes) são equipamentos que possuem a capacidade de segmentar uma rede local em várias sub-redes (domínios de colisão), e com isto conseguem diminuir o fluxo de dados (o tráfego).
- A ponte basicamente é composta de duas portas que conectam os segmentos de uma rede. O tráfego gerado por um segmento fica confinado no mesmo evitando assim que haja interferência no tráfego do outro segmento. O tráfego só atravessará para o outro segmento, se a estações origem e destino não estiverem no mesmo segmento.



PONTE (BRIDGE)

▪ Endereço MAC

- Cada estação numa rede Ethernet possui seu próprio adaptador de rede que contém um identificador único para o endereço físico, denominado endereço MAC (do inglês Media Access Control).
- No MAC address, os três primeiros octetos são destinados à identificação do fabricante, os 3 posteriores são fornecidos pelo fabricante.
- É um endereço universal, i.e., não existe, em todo o mundo, duas placas com o mesmo endereço.

06 : 01 : 02 : 01 : 2C : 4B

6 bytes = 12 hex digits = 48 bits

Relação MAC x Empresas

00-00-0C (hex) CISCO SYSTEMS INC
00-01-41 (hex) CISCO SYSTEMS INC
00-01-63 (hex) CISCO SYSTEMS INC
00-01-02 (hex) 3COM Corporation
00-01-03 (hex) 3COM Corporation
00-E0-4C (hex) REALTEK CORP.

Observe que uma empresa pode possuir mais que um grupo de MAC não contínuo.

Descrição : VIA Rhine II Fast Ethernet Adapter
Endereço físico : 00-1A-4D-A4-6A-E5

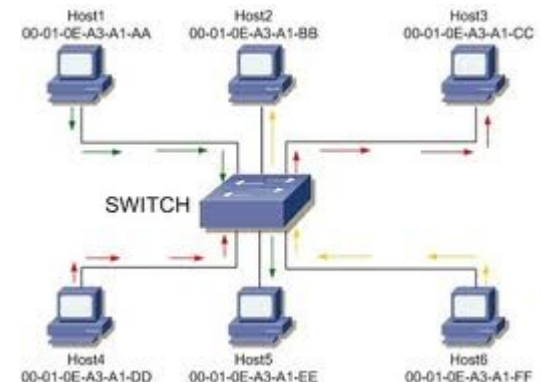
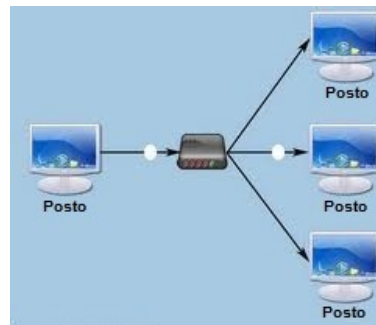
PONTE (BRIDGE)

▪ Segmentação de tráfego

- Dizemos que a ponte segmenta o tráfego, porque ela impede que o tráfego gerado entre computadores do mesmo segmento, passem para o outro segmento. A ponte possui um grau de inteligência baseado na sua tabela de roteamento (tabela SAT); é capaz de filtrar o tráfego que passa por ela, não protocolos. Uma grande rede pode ser segmentada em redes menores usando várias pontes. Essa segmentação aumenta a performance da rede já que teremos menos computadores competindo pelo acesso ao cabo no mesmo segmento.
- Atualmente as pontes encontradas no mercado constroem, automaticamente, as tabelas internas de endereços (self-learning), observando por algum tempo o tráfego de quadros na rede. Além disso, as pontes atualizam, automaticamente, as tabelas de endereços, recuperação sincronismo e amplificam sinal.
- O ideal é que as estações não tomem conhecimento da existência da bridge para que as configurações de rede se tornem mais simples. Para isso foi criado o conceito da bridge transparente (IEEE 802.1d) que deve obedecer aos critérios (como o compartilhamento de internet do Windows):
 - Os frames devem ser enviados diretamente entre as estações;
 - A tabela de encaminhamento deve ser aprendida e atualizada pela bridge ;
 - O sistema não deve conter loop.

SWITCH

- Um Switch Ethernet como o próprio nome já diz é um chaveador, ou seja, ele “chavea” o encaminhamento de quadros através de suas portas utilizando o MAC Address para este fim.
- Ele funciona de maneira semelhante a ponte também opera na camada de enlace do modelo OSI, porém possui um número maior de portas e lógica mais otimizada.
- O maior vantagem do switch perante a ponte é que a competição entre as máquinas conectadas as suas portas é eliminada definitivamente. O switch faz uma comutação virtual entre as máquinas origem e destino, isolando as demais portas desse processo. Essa característica permite que a comunicação ocorra em modo full-duplex diferentemente do que acontecia com hubs e pontes.
- O switch além de eliminar a colisão entre as suas portas, aumenta o número de domínios de colisão que é equivalente ao número de portas que ele possui.



SWITCH

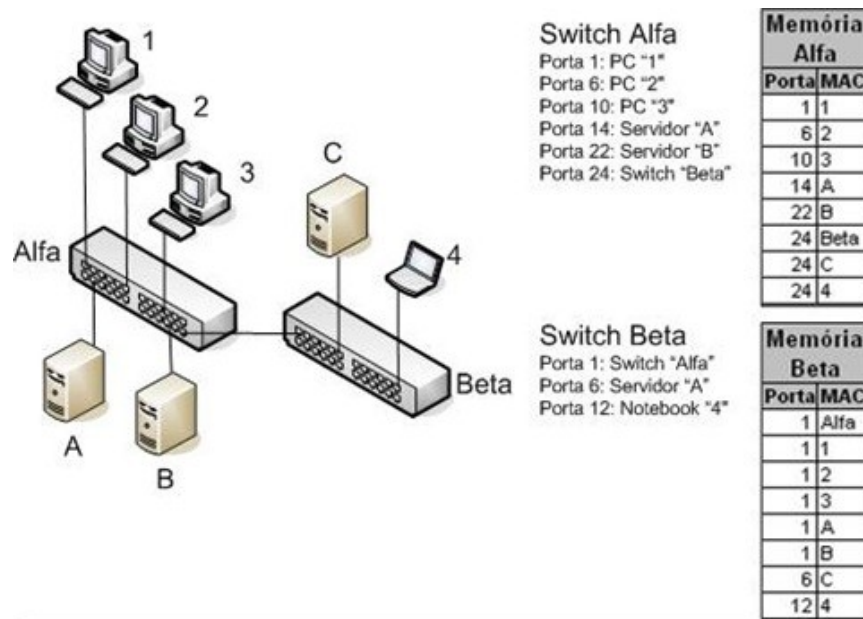
▪ O Switch pode operar em quatro modos distintos, que são:

- **Armazenar e encaminha (store-and-forward)** - os quadros recebidos são armazenados numa área temporária e é feita uma verificação e correção de erros antes de repassar os quadros para o segmento de destino. Este modo pode comprometer a performance de uma rede com vários conectados em série, devido ao retardo acumulado dos tempos de latência;
- **Direto (cut-through)** - assim que o endereço de destino é recebido, o quadro é imediatamente repassado ao segmento de destino. Este modo é o que oferece o menor tempo de latência, apresentando como desvantagem, a propagação de erros para os outros segmentos;
- **Direto modificado (modified cut-through)** - a diferença do direto é que neste o switch chaveia a operação de acordo com o tamanho do quadro. Ele opera no modo direto para quadros maiores que 64 octetos e no modo armazena e encaminha para quadros de até 64 octetos. Esta técnica filtra fragmentos de colisão e evita a maioria dos erros de quadros, já que um quadro com erros é, geralmente, detectado no primeiros 64 octetos;
- **Adaptativo (error sensing)** - o switch inicia a operação de modo direto, monitorando o ECS dos quadros. Se o número de quadros com erros se tornar elevado, segundo um limite preestabelecido, o switch, automaticamente, comuta para o modo armazena e encaminha. Assim que a “tempestade” de quadros errados passar, o switch retorna ao modo direto com monitoração de ECS. Este modo apresenta o melhor compromisso entre performance e velocidade.

SWITCH

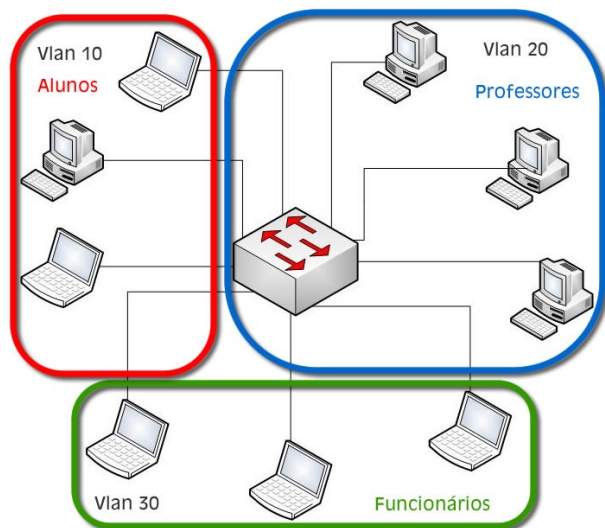
■ Forma de atuação dos switches:

- O switch armazena em memória os endereços MAC de todos os computadores conectados a ele, relacionando cada endereço MAC a uma de suas portas. É importante notar também que cada switch tem seu próprio endereço MAC. Para melhor entendimento, veja exemplo abaixo.
- No exemplo abaixo, os switches asseguram que o PC "1" pode enviar dados para o servidor "B" ao mesmo tempo que o PC "2" envia dados ao PC "3", isto evita qualquer tipo de colisão. É como se os switches buscassem criar "linhas diretas" entre cada computador.



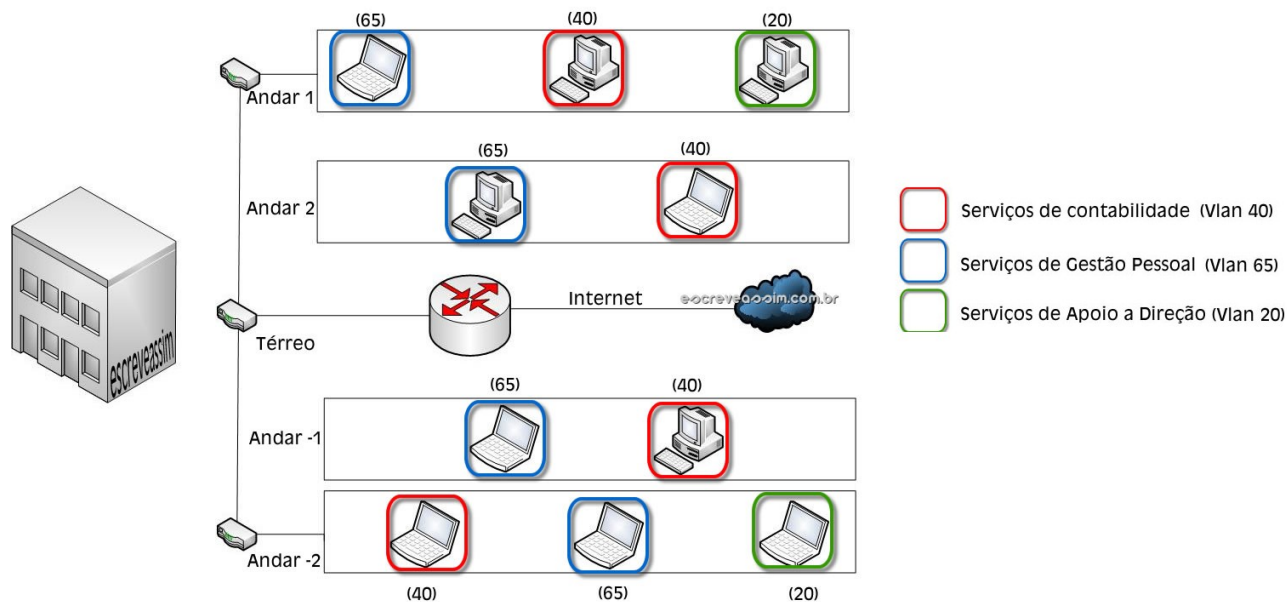
VLAN

- Devido ao crescimento e complexidade das redes de computadores, é muito comum nos dias de hoje as redes físicas serem constituídas por várias redes lógicas, denominadas de VLANs. Uma VLAN é basicamente uma rede lógica onde podemos agrupar várias máquinas de acordo com vários critérios (ex. grupos de usuários, departamentos, tráfego e etc).
- As VLANs permitem a segmentação das redes físicas, sendo que a comunicação entre máquinas de VLANs diferentes terá de passar obrigatoriamente por um roteador ou outro equipamento capaz de realizar o encaminhamento, que será responsável por encaminhar o tráfego entre redes (VLANs) distintas.



VLAN

- A constituição de VLANs numa rede física, pode dever-se a questões de:
 - **Organização** - Diferentes departamentos/serviços podem ter a sua própria VLAN. De referir que a mesma VLAN pode ser configurada ao longo de vários switches, permitindo assim que usuários do mesmo departamento/serviço estejam em locais físicos distintos;
 - **Segurança** - Pelas questões que já foram referidas acima, ou por exemplo para que os usuários de uma rede não tenham acesso a determinados servidores;
 - **Segmentação** - Permite dividir a rede física, em redes lógicas mais pequenas e assim tem um melhor controle/gestão a nível de utilização/tráfego.



VLAN - Exemplo de configuração

☒ IEEE 802.1Q VLAN ☐ Port-Based VLAN

VLAN Management: ☐ Remove VLAN

Port 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16
 T T T T U U U U U U U U U U U U

☐ Not member ☒ Tag egress packets ☐ Untag egress packets

VLAN Setting

ID	02											
Description	<input type="text" value="VLAN2"/>											
Port	01	02	03	04	05	06	07	08	09	10	11	12
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	13	14	15	16								
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>								

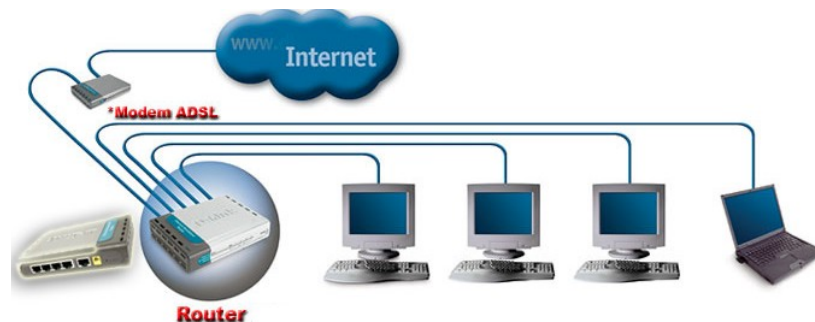
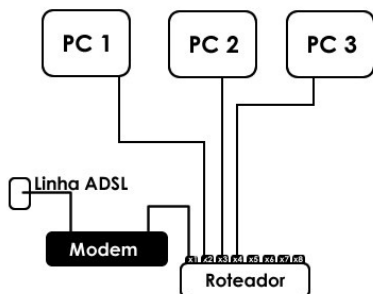
Configuração de VLANs na interface de gerenciamento de um Netgear GS716T.

ROTEADOR

- Um roteador é um dispositivo que opera na camada de rede do modelo OSI e sua principal função é selecionar o caminho mais apropriado entre as redes e repassar os pacotes recebidos. Ou seja, encaminhar os pacotes para o melhor caminho disponível para um determinado destino baseados em endereços IP.
- Cada vez que o dado é transmitido de um roteador para outro, temos um "hop".
- Os roteadores são inteligentes o suficiente para determinar o melhor caminho a seguir. Inicialmente, o roteador procurará o caminho com o menor número de hops: o caminho mais curto. Mas se por acaso perceber que um dos roteadores desta rota está ocupado demais (o que pode ser medido pelo tempo de resposta), ele procurará caminhos alternativos para desviar do trecho de lentidão, mesmo que para isso o sinal tenha que passar por mais roteadores. No final, apesar do sinal ter percorrido o caminho mais longo, chegará mais rápido, pois não precisará ficar esperando na fila do roteador congestionado.
- Os roteadores podem ser desde PCs comuns, com duas ou mais placas de rede, até supercomputadores capazes de gerenciar centenas de links de alta velocidade. O mesmo acontece ao configurar seu modem ADSL como roteador.

ROTEADOR

- A aparência física mais comum de um roteador é a de um equipamento semelhante aos hubs e switches, com duas ou mais portas de interface de rede.
- Juntamente com essas portas de interface de rede é comum encontrarmos uma porta serial para a conexão de outros equipamentos, normalmente com a finalidade de gerenciamento e configuração. Essa interface específica permite aos administradores de rede configurarem o roteador de uma forma segura, evitando um tráfego desnecessário de informações por toda a rede.
- Um roteador também pode executar funções como firewall, ou seja, a filtragem de pacotes e sua eliminação, sempre baseado em regras de gerenciamento predefinidas. Por exemplo, pacotes podem ser bloqueados e eliminados se não pertencerem à faixa de números IP especificada pelo administrador da rede ou no caso de estarem direcionados para aplicações que não estão autorizadas e/ou previstas.



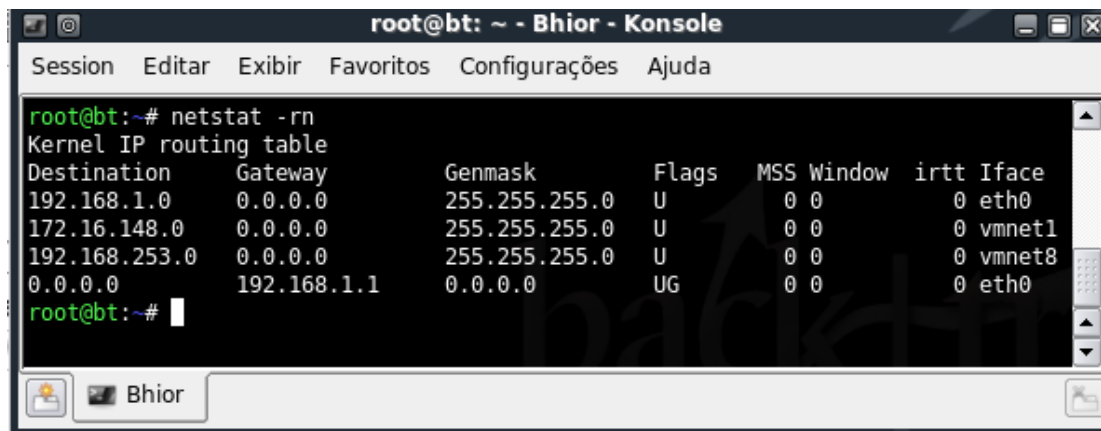
ROTEADOR

▪ Roteamento

- É a ação realizada por um roteador e consiste em encaminhar pacotes, baseado em seus destinos, para interfaces de rede ou outros roteadores.

▪ Tabela de roteamento

- Todo computador conectado a uma rede, como a Internet, por exemplo, possui uma tabela de roteamento. Esta tabela consiste em uma lista de destinos com seus respectivos caminhos, sendo consultada sempre que um dado vai ser enviado através da rede.
- Cada roteador da rede utiliza uma tabela de roteamento relacionando os destinos e caminhos que poderão ser seguidos pelos pacotes.

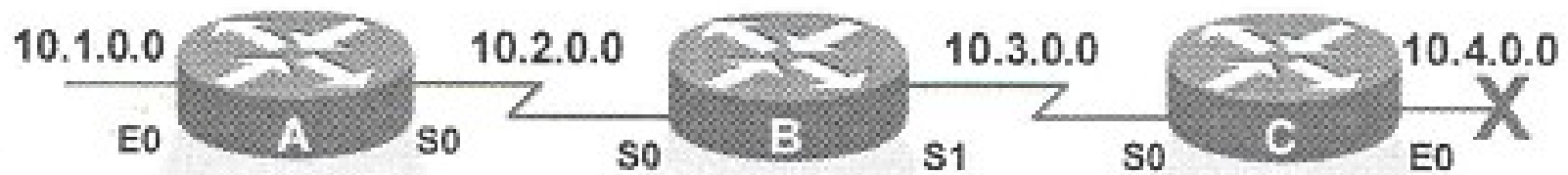


```
root@bt: ~ - Bhior - Konsole
Session  Editar  Exibir  Favoritos  Configurações  Ajuda

root@bt:~# netstat -rn
Kernel IP routing table
Destination      Gateway         Genmask         Flags   MSS Window  irtt Iface
192.168.1.0      0.0.0.0         255.255.255.0   U        0  0           0 eth0
172.16.148.0     0.0.0.0         255.255.255.0   U        0  0           0 vmnet1
192.168.253.0    0.0.0.0         255.255.255.0   U        0  0           0 vmnet8
0.0.0.0          192.168.1.1     0.0.0.0         UG        0  0           0 eth0

root@bt:~#
```

ROTEADOR



Routing Table		
10.1.0.0	E0	0
10.2.0.0	S0	0
10.3.0.0	S0	1
10.4.0.0	S0	2

Routing Table		
10.2.0.0	S0	0
10.3.0.0	S1	0
10.4.0.0	S1	1
10.1.0.0	S0	1

Routing Table		
10.3.0.0	S0	0
10.4.0.0	E0	Down
10.2.0.0	S0	1
10.1.0.0	S0	2

GATEWAY

- Gateways habilitam a comunicação entre diferentes arquiteturas e ambientes. Opera em todas as camadas do modelo OSI.
- Pode ser traduzido como "portão de entrada". O gateway pode ser um PC com duas (ou mais) placas de rede, ou um dispositivo dedicado, utilizado para unir duas redes. Existem vários usos possíveis, desde interligar duas redes que utilizam protocolos diferentes, até compartilhar a conexão com a Internet entre várias estações.
- Quando você se conecta à internet através de um provedor de acesso, você recebe apenas um endereço IP válido. A princípio, isso permitiria que apenas um micro acessasse a web, mas é possível compartilhar a conexão entre vários micros via NAT, opção disponível tanto no Windows quanto no Linux. Quando você compartilha a conexão entre vários micros, apenas o servidor que está compartilhando a conexão possui um endereço IP válido, só ele "existe" na internet. Todos os demais acessam através dele.
- O default gateway ou gateway padrão é justamente o micro da rede que tem a conexão, é ele que os outros consultarão quando precisarem acessar qualquer coisa na internet.

NAT

- A Tradução do Endereço de Rede (NAT - "Network Address Translation") é uma forma de mapear toda uma rede (ou redes) para apenas um endereço IP. NAT é necessária quando o número de endereços IP atribuídos a você pelo seu Provedor de Serviços de Internet é menor que o número total de computadores para os quais você quer prover acesso à Internet. NAT está descrita na RFC 1631, "The IP Network Address Translator (NAT)".
- O NAT é um mecanismo que visa economizar endereços IP públicos e simplificar as tarefas de gerenciamento do endereçamento IP. Quando um pacote é roteado através de um dispositivo de rede, geralmente um firewall ou um roteador de borda, o endereço IP interno (privado) é traduzido para um endereço IP externo (público). Isso permite que o pacote seja transportado por redes públicas como a Internet. Em seguida, o endereço IP externo de resposta é retraduzido para o endereço IP interno que originou o pacote, para ser entregue dentro da rede interna.
- NAT permite que você faça uso dos blocos de endereços reservados descritos na RFC 1918, "Address Allocation for Private Internets". São eles: 10.0.0.0/8 (10.0.0.0 - 10.255.255.255) , 172.16.0.0/16 (172.16.0.0 - 172.31.255.255) e 192.168.0.0/24 (192.168.0.0 - 192.168.255.255).

NAT - Exemplo

