

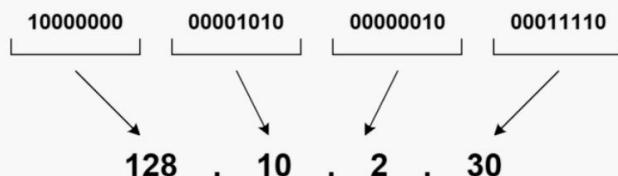


Redes IP

Redes de Comunicações 1

**Licenciatura em Engenharia de Computadores e
Informática**
DETI-UA, 2022/2023

Notação decimal dos endereços IP



Classe	menor endereço	maior endereço
A	1.0.0.0	126.0.0.0
B	128.0.0.0	191.255.0.0
C	192.0.0.0	223.255.255.0
D	224.0.0.0	239.255.255.255
E	240.0.0.0	255.255.255.254

notação de endereço IP

Um endereço IP é representado por quatro números, separados por pontos. Cada número é a representação decimal do byte correspondente.

Levando em consideração os endereços IP especiais (apresentados no último slide) e a representação em notação decimal, a tabela acima mostra o menor e o maior endereço de cada classe de endereço IP.

Máscaras

- Inicialmente os endereços IP tinham fronteiras fixas, sendo a fronteira definida a partir dos primeiros bits do campo de endereço; é o caso dos endereços de classe A, B e C
- Depois passaram a ter fronteiras flexíveis, sendo estas definidas a partir de uma máscara
- A máscara é utilizada para separar a parte de rede da parte de host dos endereços

		decimal		binário	
endereço IP	10.	0.0.1		00001010	00000000 00000000 00000001
máscara	255.	0.0.0		11111111	00000000 00000000 00000000
		← →		← →	→
		rede	host	rede	host

Máscaras de endereço IP (ou máscaras de rede)

Inicialmente, os tamanhos das partes netid e hostid de um endereço unicast foram fixados e fornecidos pela definição de sua classe. Logo percebeu-se que o número de endereços das sub-redes classe A era muito grande e o número de endereços das sub-redes classe C era muito pequeno (pelo menos para muitas situações).

Enquanto isso, uma forma mais flexível foi adotada para definir as partes netid e hostid de um endereço unicast, que é baseado em uma máscara (ou máscara de rede) composta também por quatro bytes e representada também em notação decimal. A máscara de rede é sempre composta por uma sequência de 1 bits e, em seguida, uma sequência de 0 bits. Os bits 1 definem a parte netid do endereço e os bits 0 definem a parte hostid do endereço.

IMPORTANTE: Além de permitir a escolha do tamanho apropriado das partes netid e hostid, cada host usa a máscara de rede para determinar o endereço IP da sub-rede à qual está conectado, fazendo uma operação 'and' bit a bit entre seu endereço IP e a máscara de rede.

Endereçamento IP - classes de endereços

	0	7	15	23	31
Classe A	0	netid		hostid	
Classe B	1 0		netid		hostid
Classe C	1 1 0		netid		hostid
Classe D	1 1 1 0		endereço multicast		
Classe E	1 1 1 1		reservado para utilização futura		

endereçamento IP

Para se comunicar, cada host de terminal executando o protocolo IP deve ter um endereço IP. Os endereços IP (na versão IP 4, ou IPv4 abreviado) são compostos por 4 bytes e são classificados em 5 classes diferentes.

Os endereços que podem ser atribuídos aos hosts terminais são classificados nas classes A, B e C. Esses endereços são chamados de endereços unicast, pois são usados para comunicações unicast (comunicações destinadas a um único host). Os endereços Unicast são estruturados em duas partes: (i) uma parte netid, que identifica a sub-rede IP e (ii) uma parte hostid, que identifica o host dentro da sub-rede IP.

Se o primeiro bit (o bit mais significativo) for 0, o endereço IP pertence à classe A e a parte netid é definida pelo primeiro byte do endereço. Se os dois primeiros bits forem 10, o endereço IP pertence à classe B e a parte netid é definida pelos dois primeiros bytes do endereço. Se os três primeiros bits forem 110, o endereço IP pertence à classe C e a parte netid é definida pelos três primeiros bytes do endereço.

Além das classes de endereços unicast, existem duas classes adicionais. Os endereços de classe D começam com os primeiros quatro bits 1110 e são usados para comunicações multicast (comunicações destinadas a vários hosts). Finalmente, os endereços de classe E começam com os primeiros quatro bits 1111 e são reservados para utilização futura.

Divisão do espaço de endereçamento unicast

Classe	# bits no prefixo	# máximo de redes	# bits no sufixo	# máximo de hosts por rede
A	7	128	24	16,777,216
B	14	16,384	16	65,536
C	21	2,097,152	8	256

NOTA: Nem todos os possíveis endereços podem ser usados!

Divisão de espaço de endereçamento unicast

O número de bits em cada parte dos endereços unicast define o número total de combinações para sub-redes e hosts em cada sub-rede.

Um endereço classe A tem 7 bits para definir o netid (resultando em um número total de 128 combinações) e 24 bits para definir o hostid (resultando em um total de 16777216 combinações).

Um endereço classe B tem 14 bits para definir o netid (resultando em um número total de 16.384 combinações) e 16 bits para definir o hostid (resultando em um total de 65.536 combinações).

Um endereço classe C tem 21 bits para definir o netid (resultando em um número total de 2097152 combinações) e 8 bits para definir o hostid (resultando em um total de 256 combinações).

NOTA: Nem todas as combinações estão disponíveis para definir netid e hostid, pois algumas combinações têm significados especiais (algumas delas mostradas no próximo slide).

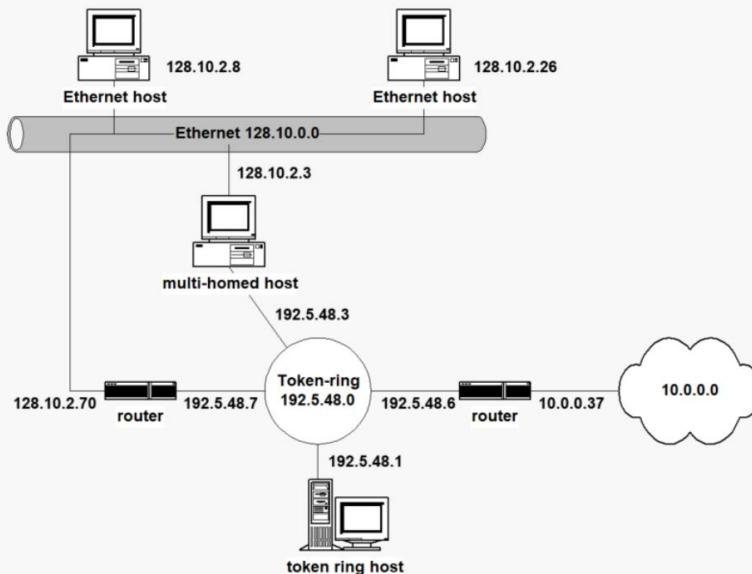
Endereços IP especiais	
tudo 0s	ESTE HOST ¹
tudo 0s	host NESTA REDE ¹
tudo 1s	BROADCAST LOCAL ²
net	BROADCAST DIRIGIDO PARA net ²
127	qualquer (em geral 1) LOOPBACK ³
net	ESTA net ⁴

¹ Permitido apenas na inicialização; nunca é endereço destino válido
² Nunca é endereço origem válido
³ Nunca deve aparecer na rede
⁴ Reservado para designar a rede

Endereços IP especiais

- O endereço composto por todos os bits iguais a 0 representa o host que o está utilizando. É permitido apenas na inicialização do host e não pode ser usado como endereço de destino.
- O endereço com a parte netid composta por todos os bits iguais a 0 representa o host (definido pela parte hostid) na sub-rede local. Não pode ser usado como endereço de destino.
- O endereço composto por todos os bits iguais a 1 representa a transmissão local Morada. Ele é usado como endereço de destino para enviar informações a todos os hosts da sub-rede local e não pode ser usado como endereço de origem.
- O endereço com a parte hostid composta por todos os bits iguais a 1 representa o endereço de broadcast da sub-rede definida pela parte netid. Ele é usado como endereço de destino para enviar informações a todos os hosts de uma sub-rede remota e não pode ser usado como endereço de origem.
- Qualquer endereço classe A que comece por 01111111 (em notação decimal, 127) é um endereço de loopback. Ele é usado como endereço de destino por um host para enviar informações para sua própria interface (ou seja, para comunicação interna do host) e não pode ser usado para enviar informações para a rede.
- O endereço com a parte hostid composta por todos os bits iguais a 0 representa o sub-rede definida pela parte netid.

Exemplo – endereçamento IP



Atribuição de endereço IP - exemplo

Considere o exemplo acima de uma rede composta por redes físicas (baseadas em diferentes tecnologias) e hosts conectados a elas. Ao atribuir endereços IP a cada interface de rede, as seguintes regras devem ser obedecidas:

- Todas as interfaces de rede conectadas à mesma rede física devem ter a mesma parte netid e diferentes partes hostid.
- Todas as interfaces de rede conectadas a diferentes redes físicas devem ter partes net.

Dessa forma, cada host tem uma maneira muito simples de determinar se um host de destino (definido por um endereço IP) está ou não em sua própria rede física: se a parte netid do endereço IP de destino for igual à parte netid de seu próprio endereço IP, o host de destino está na mesma rede física e o host de origem pode enviar as informações diretamente para o host de destino.

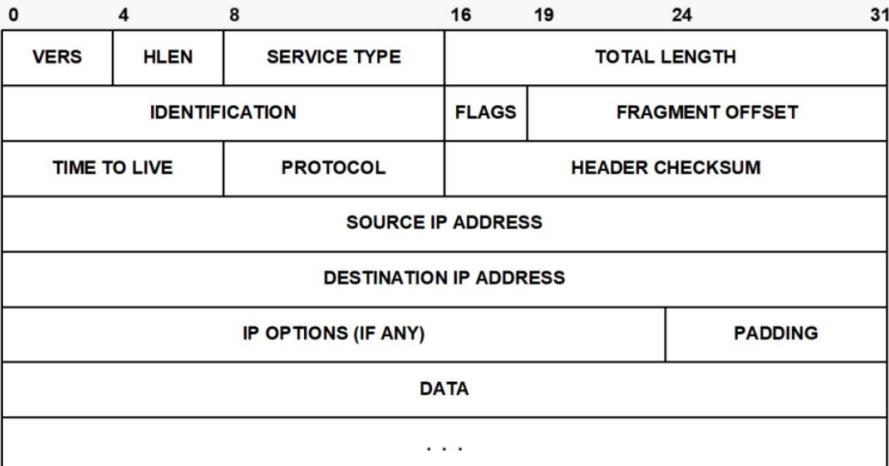
No exemplo acima, podemos distinguir três tipos de hosts:

Hosts de hospedagem única – hosts com uma única interface de rede.

Hosts multi-homed – hosts com mais de uma interface de rede; hosts multihomed não encaminham informações recebidas de uma interface de rede de entrada para uma interface de rede de saída.

Roteadores – como hosts multi-homed, roteadores são hosts com mais de uma interface de rede; ao contrário de hosts multi-homed, os roteadores podem encaminhar informações recebidas de uma interface de rede de entrada para uma interface de rede de saída.

Formato do datagrama IP



formato de datagrama IP

Um datagrama IP é composto por um campo de cabeçalho IP e um campo de dados (onde os dados são transportados). O cabeçalho IP possui vários campos obrigatórios com tamanho total de 20 bytes.

Os dois últimos campos obrigatórios são os endereços IP de origem e destino (obviamente, cada um com 4 bytes de tamanho). O significado dos demais campos obrigatórios é explicado nos próximos slides.

O cabeçalho IP pode ter campos de opção. Se houver campos de opção, o tamanho do cabeçalho deve ser um múltiplo de 4 bytes (bytes de preenchimento são inseridos, se necessário). Portanto, o tamanho do cabeçalho IP pode ser 20, 24, 28, 32 e assim por diante...

Campos do Datagrama IPv4

- **Version** (4 bits) – versão do protocolo IP (atualmente a versão mais comum é a versão 4)
- **Header Length** (4 bits) – tamanho do cabeçalho em blocos de 4 octetos
 - quando não tem opções, o cabeçalho ocupa 5 blocos de 4 octetos e o primeiro octeto do cabeçalho IP assume o valor 0x45
- **Service Type** (1 byte) – tipo de serviço ao qual o pacote pertence
 - Identifica o tipo de serviço e o objetivo é diferenciar o tratamento dos pacotes pelos routers com base na qualidade do serviço pretendida (por defeito, este campo tem o valor 0x00)
- **Total Length** (2 bytes) – tamanho do datagrama IP em octetos, incluindo o cabeçalho.
 - o tamanho máximo do datagrama IP é 65 535 octetos
 - no entanto este tamanho está restringido pelo *Maximum Transmission Unit* (MTU) da rede (mecanismo de fragmentação e reagrupamento)

Descrição do cabeçalho IP versão 4

Versão (4 bits) – versão do protocolo IP (atualmente, a versão 4 é a versão mais utilizada)

Header Length (4 bits) – tamanho do cabeçalho IP em múltiplos de 4 bytes (por exemplo, se o tamanho do cabeçalho for 20 bytes, o conteúdo deste campo será 0x5).

Tipo de Serviço (1 byte) – tipo de serviço do datagrama IP (utilizado em arquiteturas de qualidade de serviço); o valor padrão é 0x00

Comprimento total (2 bytes) – tamanho do datagrama IP (cabeçalho + dados); o tamanho máximo de um datagrama IP é 65535 bytes; no entanto, as redes físicas têm valores de MTU muito mais baixos; um mecanismo de fragmentação e remontagem está incluído no protocolo IP para resolver esse problema.

MTU (Maximum Transmission Unit) de uma rede física – o tamanho máximo do campo de dados de seus quadros da camada MAC (por exemplo, o MTU da Ethernet é 1500 bytes).

Campos do Datagrama IPv4 (continuação)

- **Identification** (2 bytes) – identificador atribuído pela estação que gerou o datagrama
 - este campo é mantido durante o processo de fragmentação permitindo o destinatário identificar os vários fragmentos de um mesmo pacote
- **Flags** (3 bits)
 - o primeiro bit está reservado para uso futuro (assume sempre o valor 0)
 - o segundo bit assume o valor 0 se o datagrama puder ser fragmentado e o valor 1 caso contrário
 - o terceiro bit assume o valor 0 se for o último fragmento e 1 se não for
- **Fragment Offset** (13 bits) – posição (em múltiplos de 8 bytes) do fragmento no datagrama original (o primeiro fragmento tem o valor 0x00)

Descrição do cabeçalho IP versão 4 (continuação)

Identificação (2 bytes) – um valor atribuído pelo host de origem ao datagrama IP; este valor é diferente para cada novo datagrama IP; esse valor é copiado para todos os datagramas de fragmentos IP na fragmentação de um datagrama IP original (desta forma, o host de destino pode identificar os datagramas de fragmentos IP de cada datagrama IP original).

Sinalizadores (3 bits):

- o primeiro bit é reservado para uso futuro (o valor padrão é 0)
- o segundo bit é o “**não fragmentar bit**”: é 1 se a origem não permite que o datagrama IP seja fragmentado e 0 caso contrário (se um datagrama IP requer fragmentação para ser transmitido por uma rede física e este bit é 1, o datagrama IP é descartado)
- o terceiro bit é o “**last fragment bit**”: é 0 se o datagrama IP for o último fragmento do datagrama IP original ou 1, caso contrário

Fragment Offset (13 bits) – posição (em múltiplos de 8 bytes) deste fragmento no datagrama IP original; o valor Fragment Offset indica quantos bytes estão em todos os datagramas anteriores (o primeiro fragmento tem o valor 0x00)

NOTA: um datagrama IP não fragmentado chega ao host de destino com Fragment Offset = 0x00 e o “last fragment bit” = 0.

Campos do Datagrama IPv4 (continuação)

- **Time to Live** (1 byte) - o máximo tempo que o datagrama pode permanecer na rede
 - é alterado em cada roteador e quando atinge o valor 0 o datagrama é eliminado
 - cada roteador decrementa este campo em 1 unidade ou no número de segundos que demorou a processar o datagrama
- **Protocol** (1 byte) - especifica o protocolo de nível superior
 - exemplos: 1 - ICMP, 6 - TCP e 17 - UDP
- **Header Checksum** (2 bytes) - resultado da soma (em palavras de 16 bits) dos outros campos do cabeçalho
 - como o header é alterado em cada roteador, este valor é também recalculado
 - permite detectar erros de transmissão que alterem o cabeçalho do datagrama

Descrição do cabeçalho IP versão 4 (continuação)

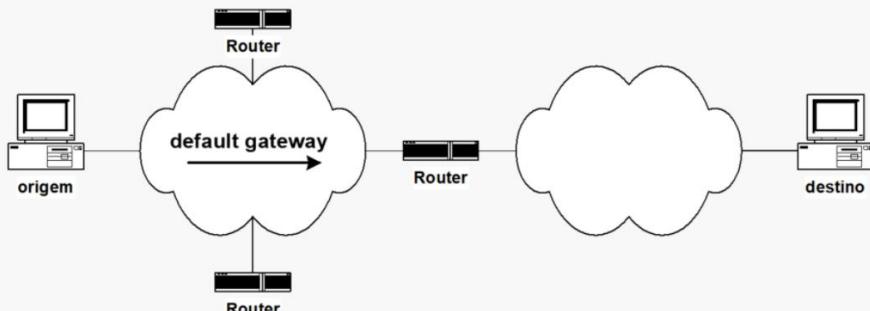
Time to Live ou TTL (1 byte) – o tempo máximo que o datagrama IP pode estar em trânsito antes de chegar ao host de destino; cada roteador subtrai a este valor o número de segundos que leva para processá-lo (este valor é decrementado pelo menos em 1); se o valor chegar a 0, o roteador descarta o datagrama IP

Protocolo (1 byte) – código que especifica o protocolo da camada superior ao qual o campo de dados pertence; exemplos: 1 - ICMP, 6 - TCP e 17 - UDP

Header Checksum (2 bytes) – resultado da soma (em palavras de 16 bits) dos demais campos do cabeçalho; permite que cada receptor (roteadores intermediários e host de destino) detecte erros de transmissão no cabeçalho IP (se um erro de transmissão for detectado, o datagrama IP será descartado); uma vez que o campo TTL é alterado por cada roteador, o cabeçalho

A soma de verificação também é alterada em cada roteador

Da estação ao 1º router



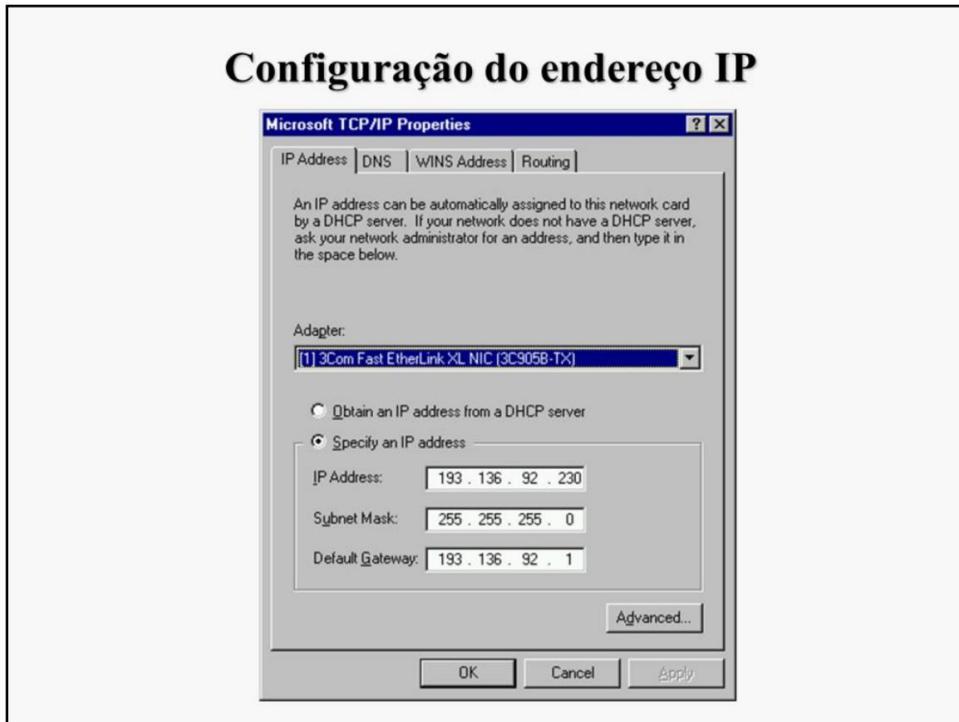
- Quando uma estação pretende enviar um pacote IP para uma rede IP que não a sua, o primeiro salto é para o **default gateway**
- O default gateway é configurado pelo utilizador – corresponde ao endereço IP da interface de um dos routers que pertence à rede da estação

Do host IP de origem ao primeiro roteador

Quando um host IP tem um datagrama IP para um endereço IP de destino, o host compara a parte netid do endereço IP de destino com a parte netid de seu próprio endereço IP.

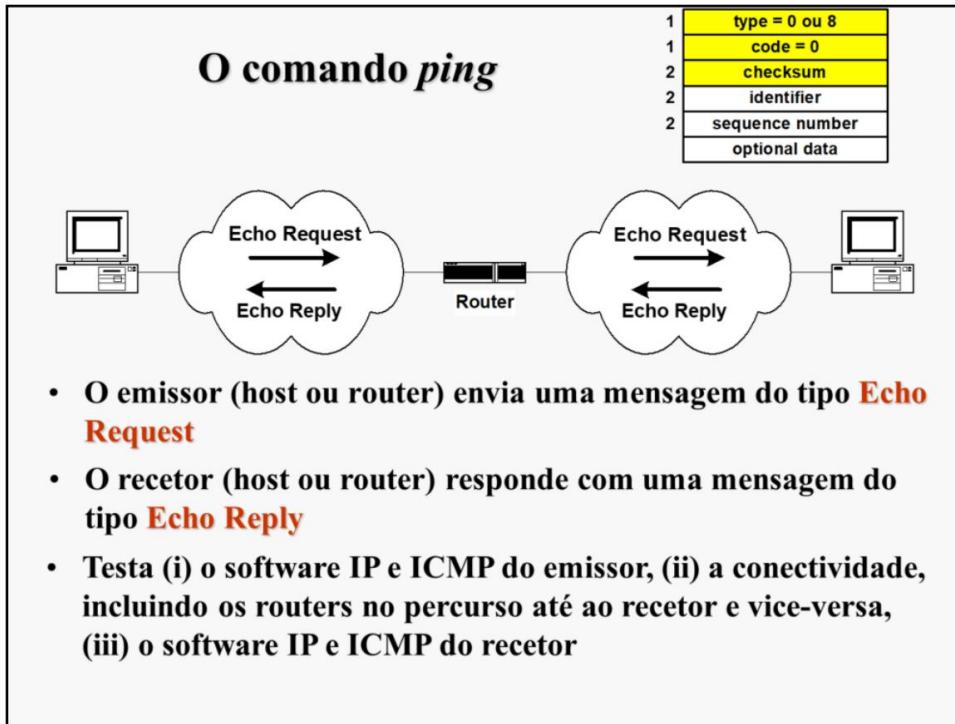
Se não forem iguais, significa que o host de destino não está conectado à sua rede física. Neste caso, o host envia o pacote para o Default Gateway.

Para ter conectividade global, um host IP deve ser configurado com o endereço IP de seu Gateway Padrão. Este endereço deve ser um endereço IP atribuído a uma interface de rede de um roteador conectado à sua própria rede física.



Configuração do host IP

A figura acima mostra um exemplo de janela de configuração de um host IP (no sistema operacional Windows) onde as informações básicas são solicitadas: o endereço IP do host, a máscara de rede e o endereço IP de seu Gateway Padrão.



comando ping

O comando *ping* usa as mensagens ICMP Echo Request e ICMP Echo Reply.

Quando um comando ping é executado em um host de origem para um endereço IP remoto, algumas mensagens ICMP Echo Request são enviadas pelo host de origem para o endereço IP remoto. Quando um host remoto recebe uma mensagem de solicitação ICMP de um endereço IP de origem, ele envia de volta uma mensagem de resposta de eco ICMP.

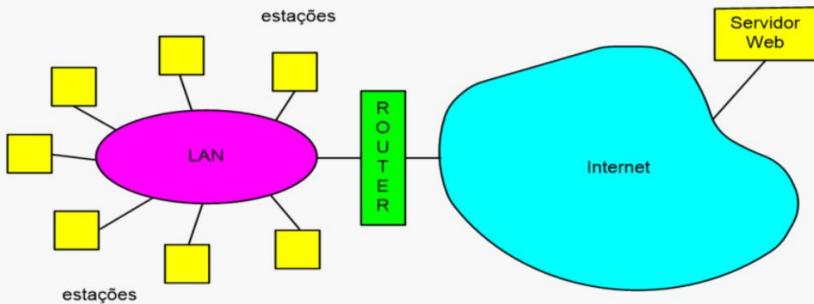
O campo de tipo é 8 (ICMP Echo Request) ou 0 (ICMP Echo Reply) e o campo de código é sempre zero. Ambas as mensagens têm dois campos adicionais: o campo **identificador** (2 bytes) e o campo de **número de sequência** (2 bytes). O conteúdo desses dois campos nas mensagens ICMP Echo Request é copiado para as mensagens ICMP Echo Reply enviadas de volta ao host de origem.

No final da mensagem, dados opcionais podem ser inseridos para gerar mensagens ICMP de tamanhos diferentes (por exemplo, para testar o mau funcionamento da fragmentação e remontagem). As mensagens ICMP Echo Reply são definidas com o mesmo tamanho de dados opcional das mensagens ICMP Echo Request recebidas.

Uma execução bem-sucedida do comando ping ocorre quando uma resposta de eco é recebida para cada mensagem de solicitação de eco enviada. Este comando testa a operação correta da pilha de protocolos TCP/IP no host de origem, a conectividade de rede entre os hosts de origem e destino e a pilha de protocolos TCP/IP no host de destino.

LANs – Redes de área local

- Permite a comunicação direta entre estações próximas através de ligações partilhadas
- Tecnologias
 - IEEE 802.3 Ethernet, IEEE 802.11 WiFi, IEEE 802.5 Token Ring, ...



LANs - Rede Local

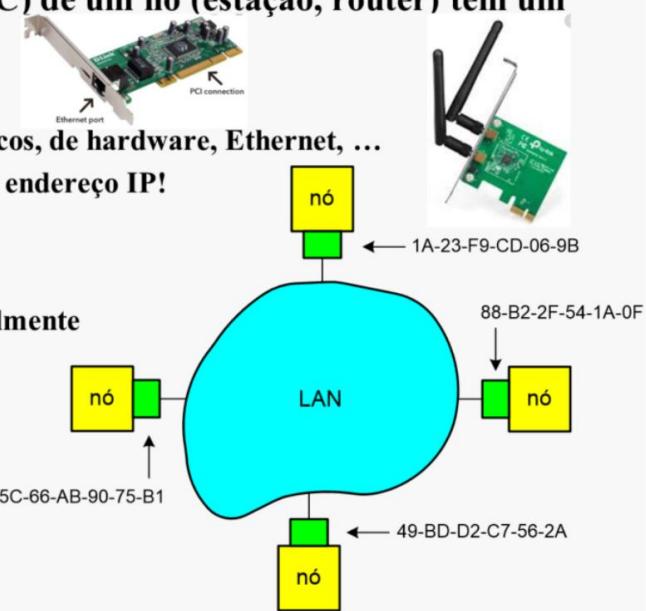
As redes locais (LANs) são sistemas de telecomunicações que permitem comunicações diretas entre estações terminais por meio de um meio de transmissão compartilhado.

Exemplos de LANs são as tecnologias padronizadas pelo IEEE como: Ethernet (IEEE 802.3), WiFi (IEEE 802.11), Token Ring (IEEE 802.5), ...

Na figura acima, uma rede LAN fornece os meios para que todas as estações se comuniquem diretamente entre elas e o roteador é o elemento de rede usado pelas estações locais para se comunicar com estações em outras redes.

Endereçamento LANs

- Cada adaptador (NIC) de um nó (estação, router) tem um endereço único
- Várias designações
 - Endereços MAC, físicos, de hardware, Ethernet, ...
 - Não é o mesmo que o endereço IP!
- Endereços IEEE
 - 48 bits
 - Administrados globalmente pelo IEEE
- Tipos de endereços:
 - Unicast
 - Multicast
 - Broadcast



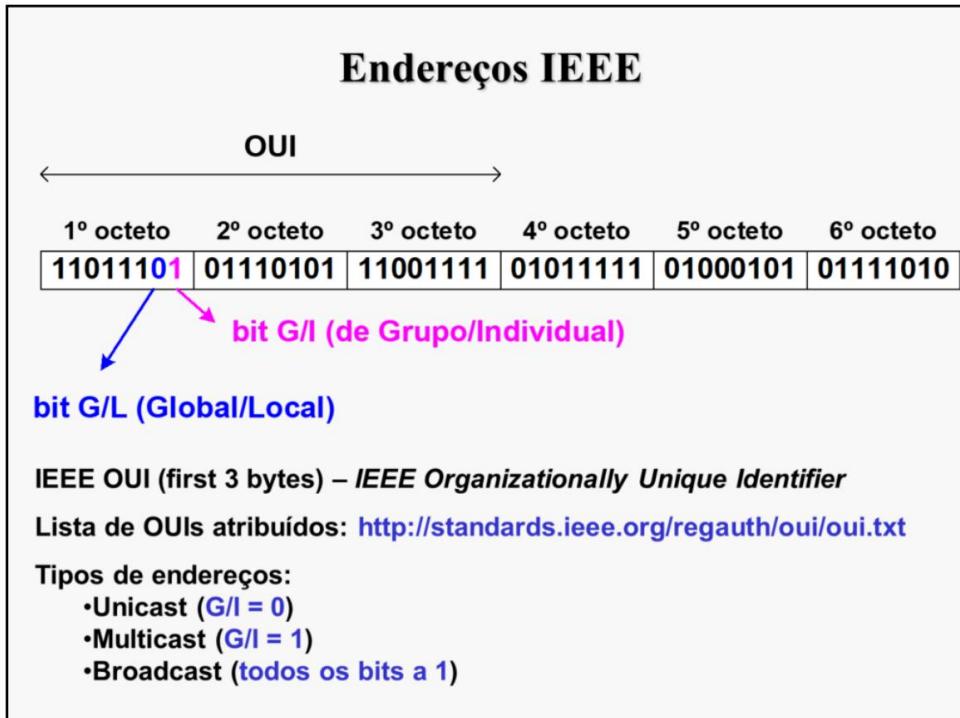
Endereçamento em LANs

As LANs são implementadas no hardware. Uma placa de interface de rede (NIC) é um dispositivo de hardware conectado a uma estação terminal ou a um roteador e que implementa todos os meios para se comunicar com as outras estações na mesma LAN.

Cada NIC tem um endereço. Este endereço é referido por vários nomes: endereço de hardware, endereço MAC, endereço físico, etc...

Todas as tecnologias IEEE têm o mesmo esquema de endereçamento: são 48 bits e são administradas globalmente pelo IEEE. Esses endereços são codificados pelos fabricantes em NICs e são garantidos como exclusivos. Ao contrário dos endereços IP, os endereços físicos são representados em notação hexadecimal.

Existem três tipos de endereços: endereços unicast (um endereço unicast identifica uma placa de rede), endereços multicast (usados para comunicações multicast) e o endereço de broadcast (um endereço especial usado como endereço de destino quando uma estação de origem deseja enviar um quadro para todas as outras estações terminais conectadas à mesma LAN).



Endereços IEEE

IEEE é a autoridade global responsável por atribuir blocos de endereços IEEE aos fabricantes de NIC. Os 3 primeiros bytes são usados para esta atribuição e são denominados IEEE Organizationally Unique Identifier (OUI). Quando um bloco é atribuído a um fabricante, ele usa os 3 últimos bytes para atribuir diferentes endereços a diferentes NICs. Observe que um fabricante pode receber mais de um bloco, dependendo de suas necessidades.

Os dois últimos bits do primeiro byte têm significados especiais:

- O 7º bit é 0 se for um endereço atribuído globalmente ou 1 se for um endereço administrado localmente (blocos atribuídos IEEE têm sempre este bit definido como 0).
- O 8º bit é 0 se for um endereço unicast ou 1 se for um endereço multicast (blocos atribuídos IEEE têm sempre este bit definido como 0).

O endereço de broadcast especial é definido por todos os bits iguais a 1: o endereço FF-FF-FF FF-FF-FF.

A lista de blocos atribuídos IEEE é pública
(<http://standards.ieee.org/regauth/oui/oui.txt>, por exemplo).

Encapsulamento de datagramas IP

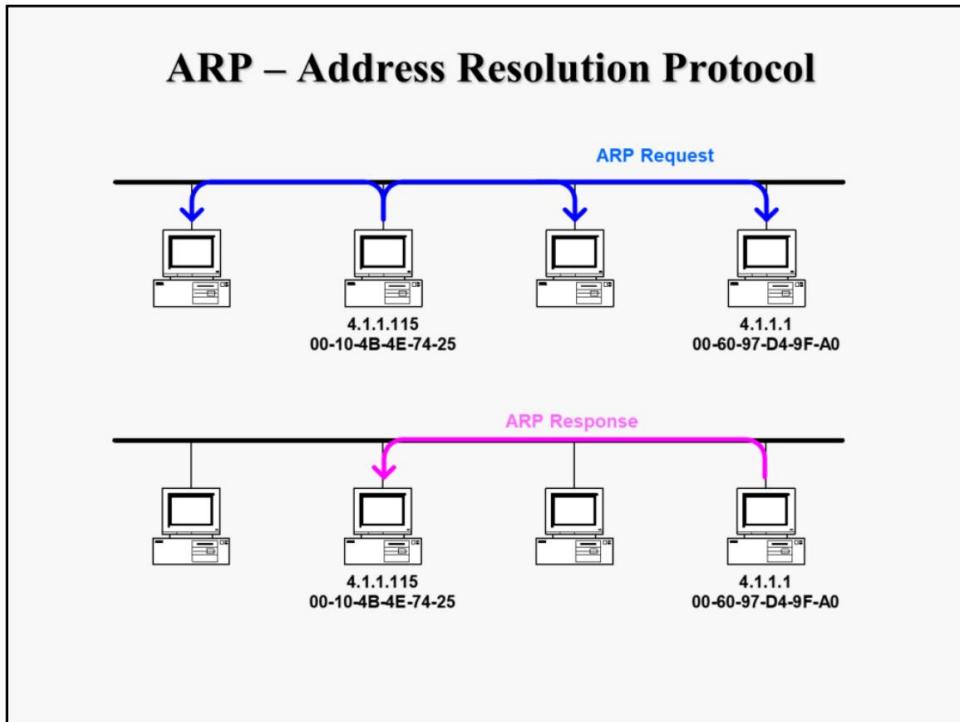


Encapsulamento de datagramas IP

O protocolo IP envia informações na forma de datagramas. Para cada bloco de bytes entregue pelo protocolo acima, o protocolo IP adiciona um cabeçalho formando assim um datagrama IP. Cada datagrama IP (composto por um campo de cabeçalho IP e um campo de dados) é entregue à camada MAC inferior para ser enviado à rede.

Em cada rede física, um quadro da camada MAC é composto por um campo de cabeçalho MAC e um campo de dados. Em cada rede física, cada datagrama IP é transmitido no campo de dados de um quadro da camada MAC (processo conhecido como encapsulamento).

MAC (Medium Access Control) – é o protocolo executado na rede física que gerencia a maneira como o meio de transmissão é usado por cada host conectado para enviar quadros da camada MAC para outros hosts.



ARP – Protocolo de Resolução de Endereço

Cada tecnologia de rede física tem seus próprios endereços. As tecnologias padronizadas pelo IEEE (por exemplo, Ethernet, Token Ring, WiFi ou WiMax), utilizam o mesmo esquema de endereçamento: cada endereço tem um tamanho de 6 bytes. Esses endereços são codificados pelos fabricantes em NICs (Network Interface Cards) e são garantidos como exclusivos (ao contrário dos endereços IP, os endereços físicos são representados em notação hexadecimal).

Na figura acima, se o host 4.1.1.115 possui um datagrama IP para enviar ao host 4.1.1.1, o datagrama IP deve ser encapsulado em um quadro de camada MAC onde o cabeçalho do quadro deve especificar os endereços MAC de origem e destino. Antes de fazer isso, o host 4.1.1.115 deve primeiro saber qual é o endereço MAC do host cujo endereço IP é 4.1.1.1.

Isso é feito através do Protocolo de Resolução de Endereço (ARP). Primeiro, o host 4.1.1.115 envia um pacote de solicitação ARP para todos os hosts solicitando o endereço MAC do host cujo endereço IP é 4.1.1.1. Se tal host estiver ativo, ele envia um pacote de resposta ARP, apenas para o host solicitante, com as informações solicitadas.

ARP Request

No.	St.	Source Address	Dest.Address	Layer	Summary	Len
1	Ok	This station	Broadcast	ARP	Op=ARP Request,	46
2	Ok	006097D49FA0	This station	ARP	Op=ARP Response	64
3	Ok	This station	Broadcast	ARP	Op=ARP Request,	46

- [-] Ethernet Version II
 - [+] Address: 00-10-4B-4E-74-25 --->FF-FF-FF-FF-FF-FF
 - [+] Ethernet II Protocol Type: ARP
- [-] Address Resolution Protocol
 - [+] Hardware Type: 1 (Ethernet)
 - [+] Protocol Type: 800
 - [+] Hardware Address Length: 6
 - [+] Protocol Address Length: 4
 - [+] Operations: ARP Request
 - [+] Source Hardware Address: 00-10-4B-4E-74-25
 - [+] IP Source Address: 4.1.1.115
 - [+] Destination Hardware Address: 00-00-00-00-00-00
 - [+] IP Destination Address: 4.1.1.1
 - [+] Calculate CRC: 0x27621e3b

**ARP Request enviado pela estação 4.1.1.115 para
saber o endereço MAC da estação 4.1.1.1.**

Solicitação ARP

Os pacotes ARP são encapsulados em quadros da camada MAC. O acima é o conteúdo de um pacote de solicitação ARP encapsulado em um quadro Ethernet. No cabeçalho do quadro Ethernet, o endereço de origem é o endereço MAC do host 4.1.1.115 e o endereço de destino é o endereço de broadcast MAC FF-FF-FF-FF-FF-FF (um endereço com todos os bits iguais a 1). O pacote ARP Request especifica os endereços MAC e IP de origem, o endereço IP de destino e um endereço MAC de destino vazio.

ARP Reply

No.	St.	Source Address	Dest Address	Layer	Summary	Len	Rel. Time
<input type="checkbox"/>	1	Ok This station	Broadcast	ARP	Op=ARP Request,	46	0:00:07
<input checked="" type="checkbox"/>	2	Ok 006097D49FA0	This station	ARP	Op=ARP Response	64	0:00:07
<input type="checkbox"/>	3	Ok This station	Broadcast	ARP	Op=ARP Request,	46	0:00:07

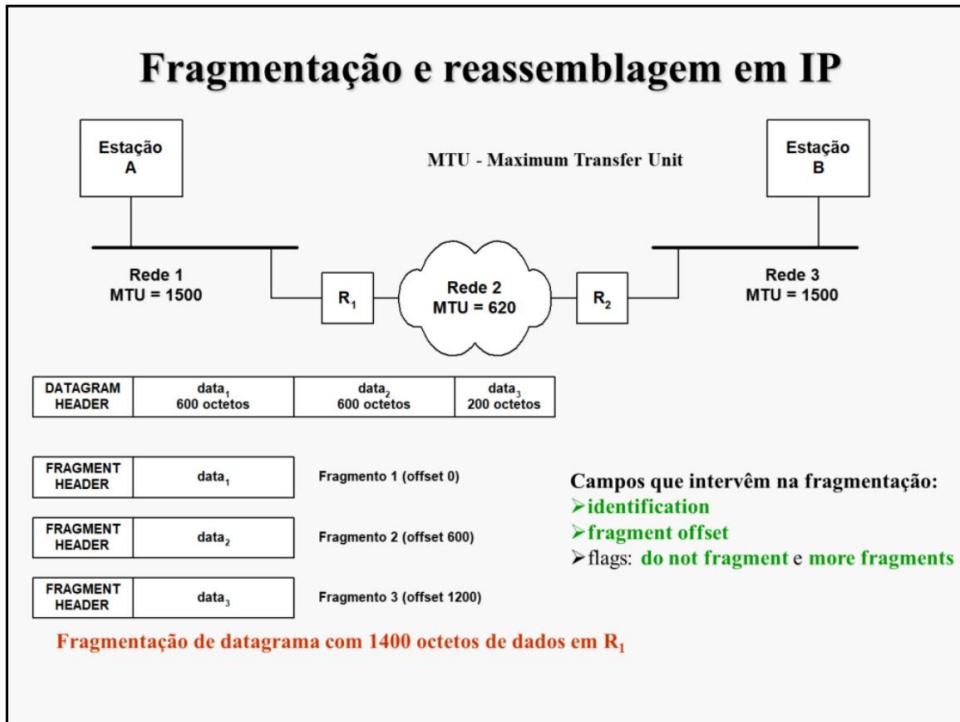
Ethernet Version II
 Address: 00-60-97-D4-9F-A0 --->00-10-4B-4E-74-25
 Ethernet II Protocol Type: ARP
 Address Resolution Protocol
 Hardware Type: 1 (Ethernet)
 Protocol Type: 800
 Hardware Address Length: 6
 Protocol Address Length: 4
 Operations: ARP Response
 Source Hardware Address: 00-60-97-D4-9F-A0
 IP Source Address: 4.1.1.1
 Destination Hardware Address: 00-10-4B-4E-74-25
 IP Destination Address: 4.1.1.115
 Data 0000: 01 73 01 73 01 73 01 73 01 73 01 73 |
 0010: 01 73 |
 Calculate CRC: 0x20255ec0

Resposta da estação 4.1.1.1 enviada através de ARP Response:
o endereço MAC é 00-60-97-d4-9f-a0

Resposta ARP

O acima é o conteúdo de um pacote ARP Reply encapsulado em um quadro Ethernet. No cabeçalho do quadro Ethernet, o endereço de origem é o endereço MAC do host 4.1.1.1 e o endereço de destino é o endereço MAC do host 4.1.1.115 (que é o solicitante).

A resposta ARP especifica seus endereços MAC e IP e os endereços MAC e IP de destino.



Processo de fragmentação e remontagem

Quando um datagrama IP é maior que o MTU da rede física, o host de envio deve fragmentá-lo em vários datagramas IP menores cujo tamanho não seja maior que o MTU. A operação de fragmentação pode ser feita pelo host de origem ou por qualquer roteador.

NOTA IMPORTANTE: Todos os datagramas de fragmentos IP são encaminhados individualmente para o host de destino. A operação de remontagem (isto é, a operação de juntar todos os fragmentos para recuperar o datagrama IP original) é realizada apenas pelo host de destino.

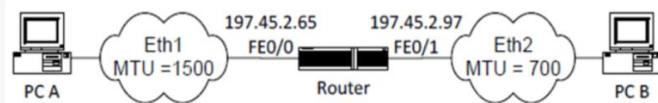
O processo de fragmentação de IP é o seguinte:

1. O campo de dados é segmentado em um conjunto ordenado de blocos de forma que cada bloco mais o cabeçalho não seja maior que o MTU. Cada bloco com seu cabeçalho forma um datagrama IP fragmentado.
2. O campo Identificação de todos os fragmentos é definido com o campo Identificação do datagrama IP original (desta forma, o host de destino pode identificar todos os fragmentos de um datagrama IP).
3. O campo Fragment Offset do fragmento n é definido com o número total de bytes de dados enviados por todos os fragmentos anteriores de 1 a $n - 1$ (dessa forma, o host de destino pode identificar fragmentos ausentes e pode ordenar os fragmentos se forem recebidos fora de serviço).
4. O sinalizador 'mais fragmentos' é definido com 0 no último fragmento e 1 em todos os fragmentos anteriores (desta forma, o host de destino pode saber qual é o último fragmento e, portanto, verificar se todos os fragmentos foram recebidos).

Na figura acima, o roteador R1 possui um pacote IP com 1400 bytes de dados para o host B. O pacote é fragmentado em três pacotes IP fragmentados. Como a MTU da rede de encaminhamento é de 620 bytes, os dois primeiros fragmentos possuem blocos de dados de 600 bytes e o terceiro fragmento possui os 200 bytes restantes. O Fragment Offset é 600 no segundo fragmento (os dados do primeiro fragmento) e é 1200 no terceiro fragmento (os dados totais do primeiro e do segundo fragmentos).

Exemplo

- Num ping do PC A para o PC B, o PC A envia uma mensagem ICMP de 900 bytes. Os pacotes IP que transportam esta mensagem têm o campo IDENTIFICATION com o valor 385. Indique justificadamente quantos fragmentos IP são recebidos pelo PC B, quem gera os fragmentos IP e qual o tamanho (em Bytes) de cada fragmento IP (incluindo o cabeçalho).

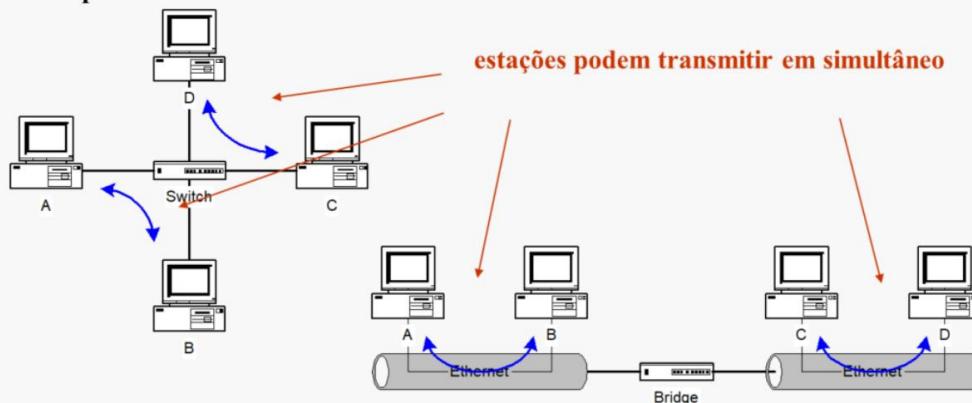


Switching

Bridges/switches versus repetidores/hubs (II)

- Consequências (II):

- As colisões deixam de ser um problema
- A largura de banda agregada não é limitada pela taxa de transmissão das portas



Pontes/Switches versus Repetidores/Hubs (II)

Outras consequências positivas são:

- As colisões são eliminadas (pontes / switches podem receber simultaneamente quadros e envio de quadros em portas diferentes)
- A taxa de transmissão total do equipamento não é restrita ao taxa de transmissão de uma única porta, mas, em vez disso, é dada pela soma das taxas de transmissão de todas as portas

Em uma rede 10BaseT, quando um hub é substituído por um switch (imagem à esquerda acima), todas as estações terminais conectadas podem transmitir e receber quadros simultaneamente (não é necessário CSMA/CD e as interfaces podem operar em modo full duplex).

Em uma rede 10Base2 (ou 10Base5), quando um repetidor é substituído por uma ponte (figura à direita acima), quadros simultâneos podem ser transmitidos nos diferentes segmentos conectados. Observe, no entanto, que neste caso o CSMA/CD ainda é necessário em cada segmento (por quê?).

Tabela de Encaminhamento do Switch

- **Pergunta:** como é que o switch sabe que A' é atingido via 4, por exemplo?
- **Resposta:** cada switch tem uma tabela de encaminhamento, em que cada entrada é da forma:
 - (endereço MAC, interface, tempo de vida)
- **Pergunta:** como é que estas entradas são criadas e mantidas?

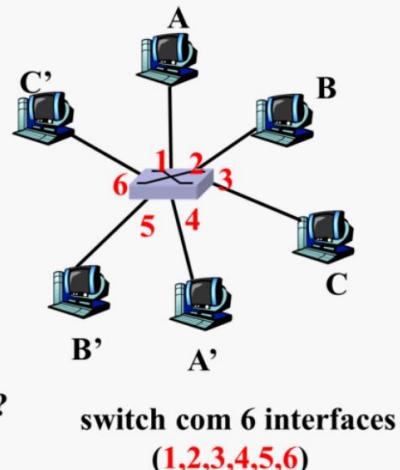


Tabela de endereços MAC de um switch

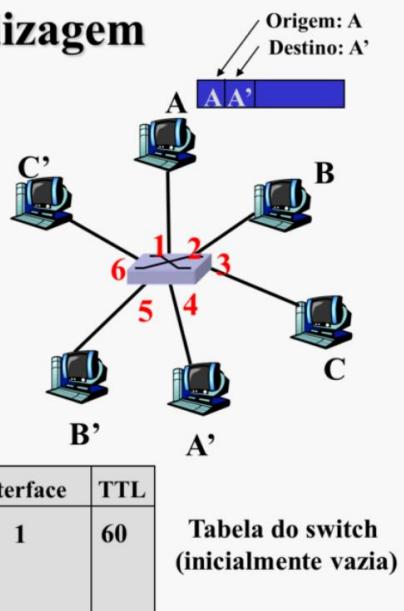
Como os switches podem realizar a função de filtragem, ou seja, como os switches sabem “onde” está a estação de destino de cada quadro de entrada? Primeiro, os switches atribuem um valor de ID de porta a cada uma de suas portas. Na figura acima, se o switch recebe um quadro destinado ao host A', como ele sabe que o quadro deve ser encaminhado pela porta 4?

Para realizar esta tarefa, os switches possuem uma tabela de roteamento (comumente denominada MAC Address Table) onde cada entrada possui: (i) um endereço MAC, (ii) um número de porta (iii) e um valor de tempo de vida (TTL).

Como a tabela de endereços MAC é gerenciada? Veja o próximo slide.

Switch: auto-aprendizagem

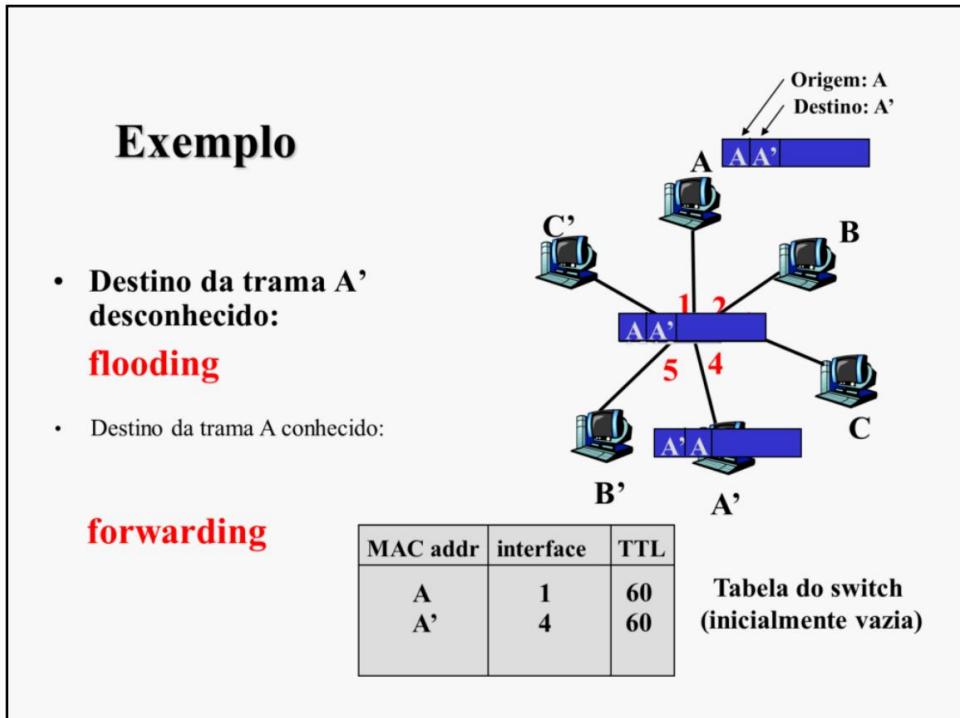
- O switch **aprende** que estações podem ser atingidas por cada uma das suas interfaces
 - quando uma trama é recebida numa interface, o switch regista na tabela de encaminhamento uma entrada com o endereço MAC origem da trama e a interface de entrada



Switch: processo de autoaprendizagem

Os switches aprendem quais estações terminais podem ser alcançadas através de quais portas: quando um quadro é recebido em uma porta de entrada, o switch inclui na tabela de endereços MAC uma entrada com o endereço de origem MAC do quadro, a porta de entrada e um valor TTL predefinido.

No exemplo acima, o host A envia um quadro com o endereço MAC de origem de A e o endereço MAC de destino de A'. Na recepção deste quadro na porta 1, uma entrada é inserida na Tabela de Endereços MAC associando o endereço MAC de A à porta 1.



Exemplo

Considere o exemplo acima onde no início a tabela de endereços MAC está vazia.

- Primeiro, a estação A envia um quadro com o endereço MAC de origem de A e destino Endereço MAC de A'.
- Ao receber este quadro na porta 1, uma entrada é inserida no endereço MAC Tabela associando o endereço MAC de A com a porta 1.
- Este quadro é inundado para as portas 2, 3, 4, 5 e 6 porque a tabela de endereços MAC não tem qualquer entrada com o endereço MAC de A'.
- Em seguida, a estação A' envia um quadro com o endereço MAC de origem de A' e endereço MAC de destino de A.
- Ao receber este quadro na porta 4, uma entrada é inserida no endereço MAC Tabela associando o endereço MAC de A' à porta 4.
- Este quadro é encaminhado para a porta 1 porque a tabela de endereços MAC possui uma entrada especificando que o endereço MAC de A é alcançável através da porta 1.

Switch: filtragem/forwarding

Quando uma trama é recebida por um switch:

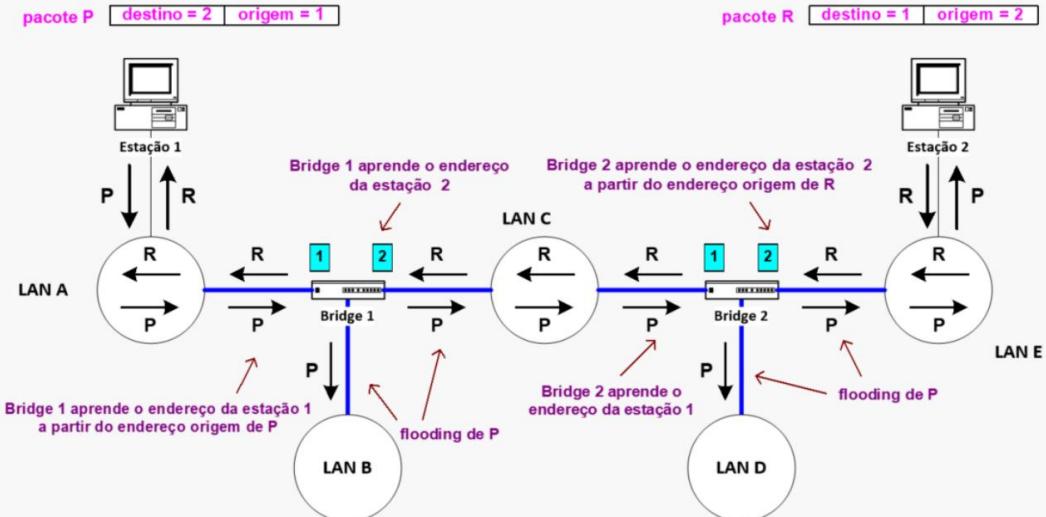
1. regista na tabela de encaminhamento a interface do emissor da trama
2. procura na tabela de encaminhamento uma entrada com o endereço MAC destino
3. if entrada encontrada
 then {
 if destino na mesma interface em que a trama foi recebida
 then descarta a trama
 else encaminha a trama pela interface indicada
 (forwarding)
 }
 else envia para todas as interfaces exceto a de entrada (flooding)

Switch: processo de filtragem/encaminhamento

Quando um quadro é recebido em uma interface de entrada, o switch executa as seguintes operações:

1. ele registra na Tabela de Endereços MAC o endereço MAC de origem do quadro com o porta
2. ele procura na tabela de endereços MAC uma entrada com o endereço MAC de destino do quadro
3. se houver entrada
 então {
 se a porta de destino for igual à porta de entrada do quadro
 em seguida, descarta o quadro
 senão encaminha o quadro pela porta de saída (processo de encaminhamento)
 }
 senão encaminha o quadro para todas as portas, exceto sua porta de entrada (processo de inundação)}

Aprendizagem de endereços



30

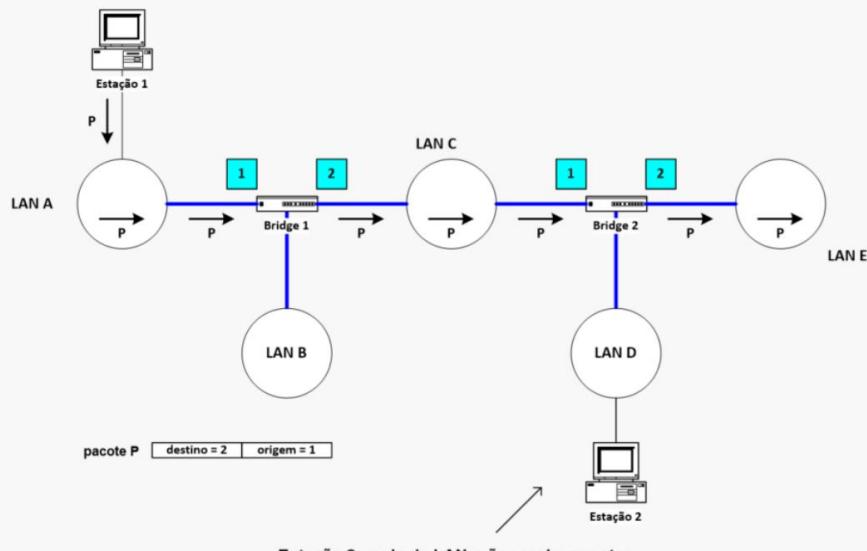
Processo de Aprendizagem de Endereço MAC

O que acontece quando uma rede é composta por vários switches/pontes? Os processos de autoaprendizagem e encaminhamento funcionam exatamente da mesma forma que no caso de elemento único.

A imagem acima ilustra estes processos recorrendo a uma rede de bridges (o mesmo acontece com uma rede de switches):

- Primeiro, a estação 1 envia um quadro para a estação 2
- A ponte 1 descobre que a estação 1 pode ser acessada por meio de sua porta conectada à LAN A e inunda o quadro para LAN B e LAN C.
- A ponte 2 aprende que a estação 1 é alcançável através de sua porta conectada à LAN C e inunda o quadro para LAN D e LAN E.
- Em seguida, a estação 2 envia um quadro para a estação 1
- A ponte 2 descobre que a estação 2 é alcançável através de sua porta conectada à LAN E e encaminha o quadro para a LAN C.
- A ponte 1 descobre que a estação 2 pode ser alcançada através de sua porta conectada à LAN C e encaminha o quadro para a LAN A.

Tempo de vida das entradas das tabelas de encaminhamento



31

TTL das entradas da tabela de endereços MAC

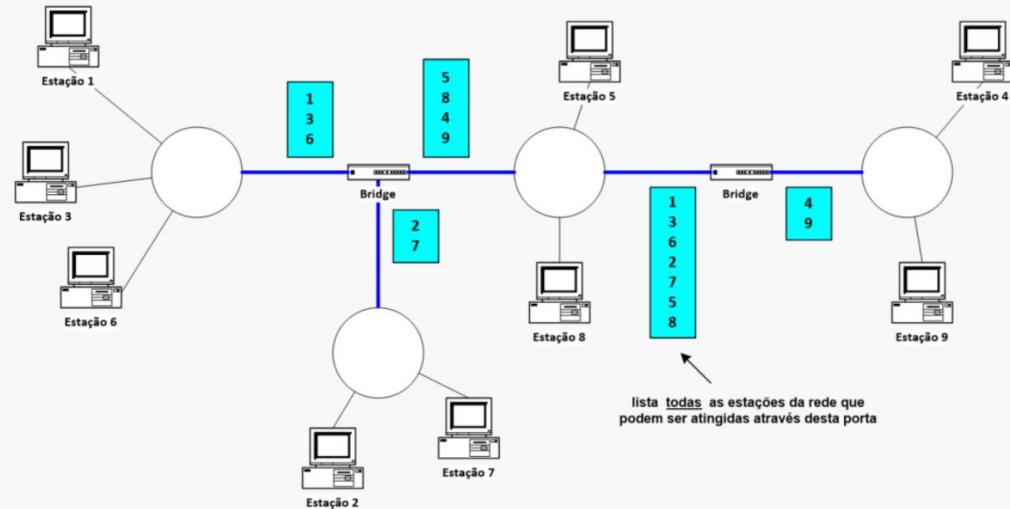
Lembre-se de que cada entrada da tabela de endereços MAC tem um valor de tempo de vida (TTL) associado. Este valor é ajustado para um valor pré-definido toda vez que o switch recebe um quadro da estação terminal de origem. Em seguida, a entrada é excluída se nenhum quadro for recebido da estação de origem durante os segundos TTL (dizemos que o tempo da entrada expirou).

Considere o exemplo do slide anterior onde, enquanto isso, a estação 2 muda seu ponto de conexão de LAN E para LAN D (figura acima). Neste caso, a tabela de endereços MAC da ponte 2 fica errada e os quadros enviados pela estação 1 para a estação 2 não chegarão ao seu destino (causando perda de conectividade).

Se, entretanto, a estação 2 enviar um quadro para a rede, ela permitirá que a ponte 2 atualize sua tabela de endereços MAC associando o endereço MAC da estação 2 à nova porta e a conectividade seja recuperada.

Caso contrário, a conectividade será recuperada quando expirar a entrada da ponte 2 na Tabela de Endereços MAC, o que ocasionará o flooding de quadros para a estação 2.

Encaminhamento em bridges



32

Roteamento em Bridges/Switches

As pontes/switches usam quadros de dados para saber quais estações terminais podem ser alcançadas por cada uma de suas próprias portas.

Exercício

- Considere a seguinte tabela de encaminhamento de um Switch com 8 portas:

00:01:42:b5:45:f1 – port 4

00:0e:0c:3e:45:c3 - port 1

00:11:52:a5:45:f2 - port 4

00:1F:02:1e:34:B1 - port 2

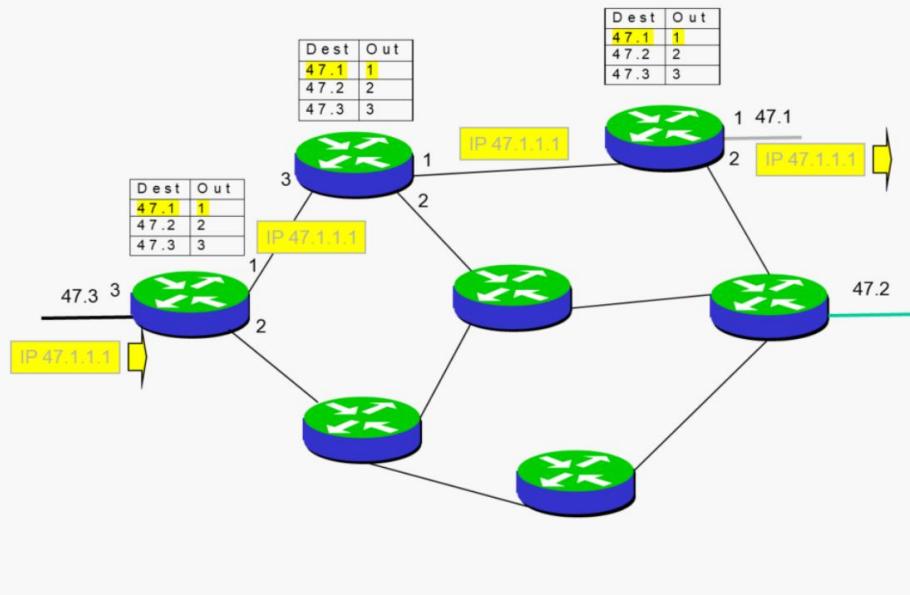
Das afirmações que se seguem, assinale as afirmações verdadeiras e as falsas:

- a) Se na porta 1 do Switch chegar uma trama Ethernet com endereço MAC de destino 00:00:00:00:AA:AA esta será reenviada por todas as portas do Switch
- b) Se na porta 5 do Switch chegar uma trama Ethernet com endereço MAC de destino 00:00:00:00:AA:AA será adicionada à tabela de encaminhamento a entrada “00:00:00:00:AA:AA port 5”
- c) Se na porta 4 do Switch chegar uma trama Ethernet com endereço MAC de origem 00:00:00:00:AA:AA será adicionada à tabela de encaminhamento a entrada “00:00:00:00:AA:AA port 4”
- d) Se na porta 8 do Switch chegar uma trama Ethernet com endereço MAC de origem 00:1F:02:1e:34:B1, a 4ª entrada da tabela será substituída por “00:1F:02:1e:34:B1 port 8”
- e) Se na porta 1 do Switch chegar uma trama Ethernet com endereço MAC de destino 00:11:52:a5:45:f2 esta será reenviada apenas pela porta 4 do switch

33

Routing

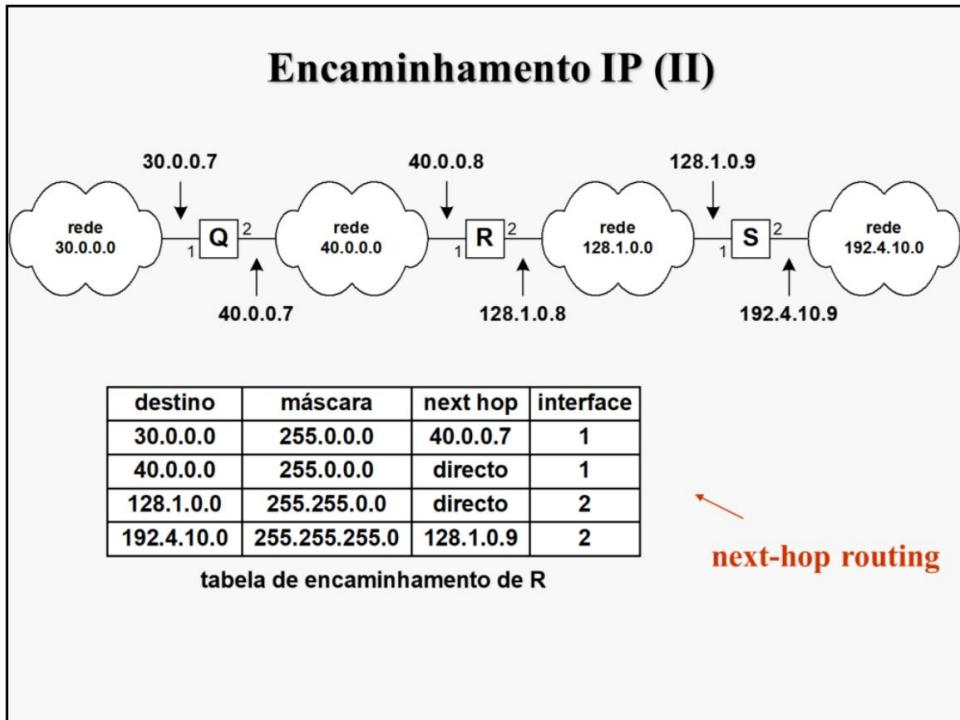
Encaminhamento IP (I)



Roteamento IP (I)

Os roteadores são os elementos de rede responsáveis por encaminhar cada datagrama IP para seu host de destino. Para cumprir essa tarefa, cada roteador possui uma tabela de roteamento que define a porta de saída a ser utilizada para cada destino possível.

Na figura acima, esta tarefa é ilustrada de forma bastante simplificada. O primeiro roteador recebe na porta 3 um datagrama IP do host de origem para o host IP de destino 47.1.1.1. O roteador verifica sua tabela de roteamento e encontra uma entrada informando que datagramas para endereços IP iniciados por 47.1 devem ser transmitidos pela porta de saída 1 e, portanto, ele encaminha esse datagrama por essa porta. O processo é repetido no segundo e no terceiro roteador.



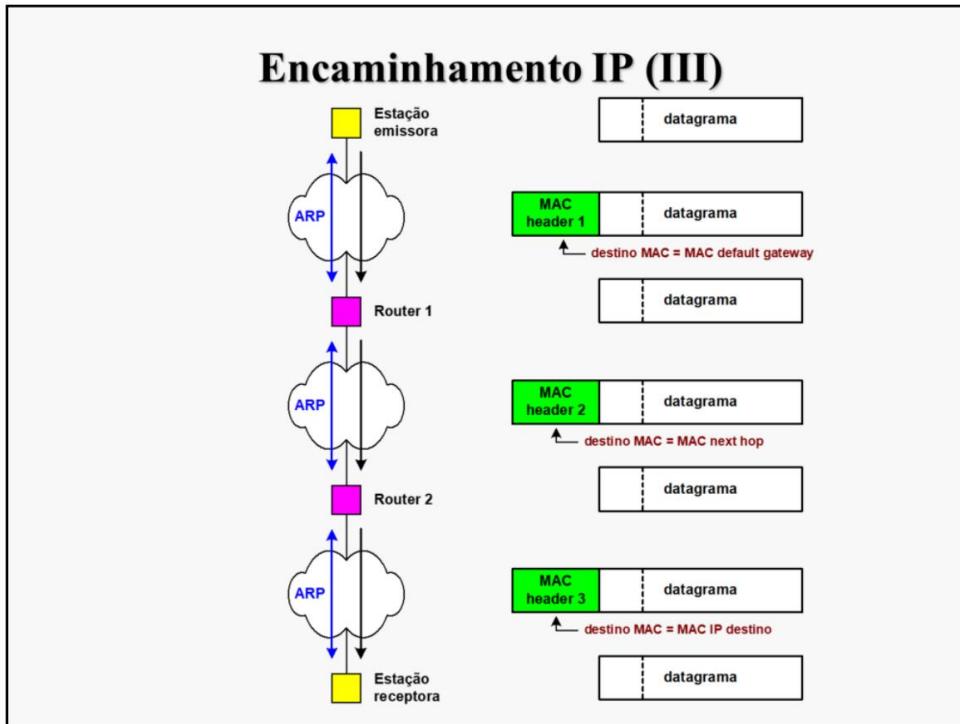
Roteamento IP (II)

No exemplo acima, são mostrados mais alguns detalhes sobre as tabelas de roteamento. Mostra a tabela de roteamento do roteador R na rede mostrada. Cada entrada da tabela de roteamento identifica:

- uma rede de destino (especificada por seu endereço de rede IP e máscara de rede),
- a porta de saída para encaminhar os datagramas para a rede de destino,
- o endereço IP da próxima interface de rede do roteador no caminho para a rede de destino.

O roteamento em redes IP às vezes também é chamado de “roteamento do próximo salto”, pois cada roteador encaminha cada datagrama com base na identificação do roteador do próximo salto no caminho para o destino.

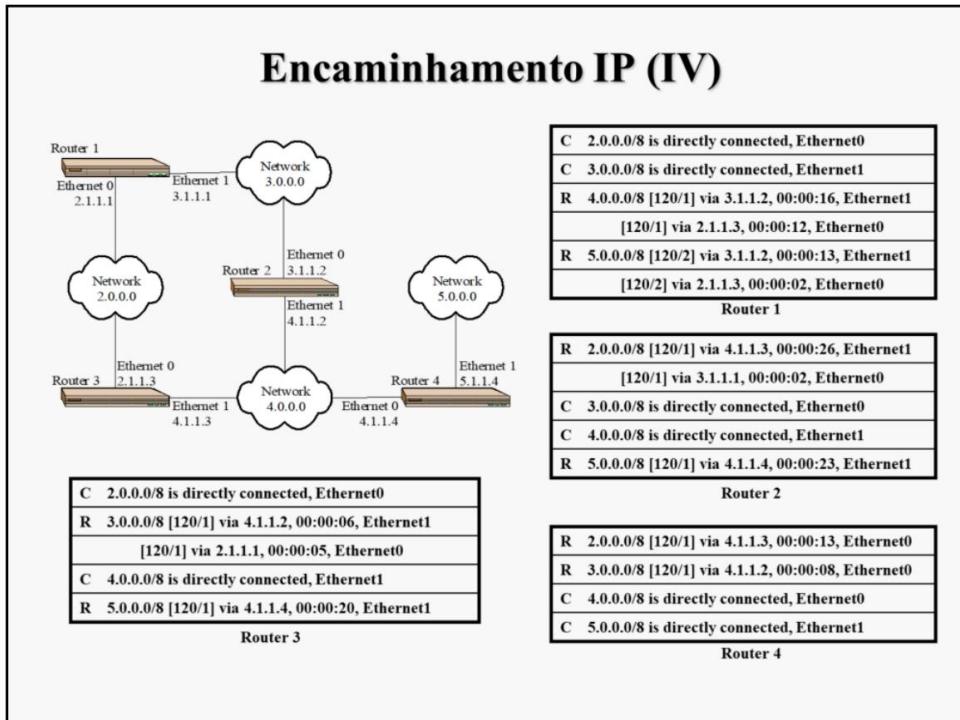
Observe que se a rede de destino estiver conectada diretamente ao roteador, o endereço IP do roteador do próximo salto está ausente (na tabela de roteamento), pois, nesse caso, o roteador deve enviar o datagrama diretamente ao host de destino.



Roteamento IP (III)

Em geral, a transmissão de um datagrama IP de um host de origem para um host de destino envolve as seguintes etapas:

1. Se necessário, o host de origem descobre (através do ARP) o endereço MAC de seu gateway padrão.
2. O datagrama IP é encapsulado em um quadro de camada MAC (com seu endereço MAC como endereço de origem e o endereço MAC do Gateway Padrão como endereço de destino) e é enviado à rede.
3. Em cada roteador antes do último no caminho para o host de destino:
 - 3.1. O roteador desencapsula o datagrama IP do quadro da camada MAC de entrada.
 - 3.2. De sua tabela de roteamento, obtém a porta de saída a ser usada e o endereço IP do próximo salto para a rede de destino.
 - 3.3. Se necessário, descobre (através do ARP) o endereço MAC do endereço IP do próximo salto.
 - 3.4. O datagrama IP é encapsulado em um quadro da camada MAC (com o endereço MAC da porta de saída como endereço de origem e o endereço MAC do roteador do próximo salto como endereço de destino) e é enviado pela porta de saída.
4. No último roteador no caminho para o host de destino:
 - 4.1. O roteador desencapsula o datagrama IP do quadro de entrada da camada MAC.
 - 4.2. A partir de sua tabela de roteamento, obtém a porta de saída a ser utilizada e a informação de que o host de destino está na rede diretamente conectada.
 - 4.3. Se necessário, descobre (através do ARP) o endereço MAC do endereço IP de destino.
 - 4.4. O datagrama IP é encapsulado em um quadro da camada MAC (com o endereço MAC da porta de saída como endereço de origem e o endereço MAC do host de destino como endereço de destino) e é enviado pela porta de saída.



Roteamento IP (IV)

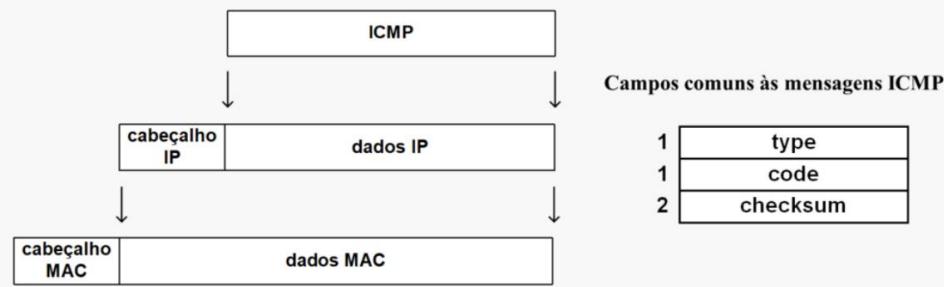
Para a rede mostrada acima, composta por quatro roteadores interligando quatro redes Ethernet, são apresentadas as tabelas de roteamento observadas nos roteadores.

Nesse caso, o protocolo de roteamento RIP está ativo em todos os roteadores para computar as tabelas de roteamento. Este protocolo de roteamento compõe as tabelas de roteamento com os roteadores de próximo salto que fornecem o número mínimo de saltos até a rede de destino (entradas iniciadas com a letra 'R').

Observe que um roteador pode ter mais de uma entrada para cada destino (se houver vários caminhos de roteamento com o mesmo número mínimo de saltos). Quando isso acontece, os roteadores implementam o balanceamento de carga: eles usam todas as entradas de forma a equilibrar igualmente o uso de todos os caminhos de roteamento.

ICMP – Internet Control Message Protocol

- Permite a troca de mensagens de controle e diagnóstico
- Os pacotes ICMP são encapsulados nos pacotes IP
- O campo *Checksum* é determinado com base em toda a mensagem (deteção de erros de transmissão em toda a mensagem)



Protocolo de mensagens de controle da Internet (ICMP)

O Internet Control Message Protocol (ICMP) faz parte do Internet Protocol Suite. As mensagens ICMP são geradas em resposta a erros em datagramas IP ou para fins de diagnóstico ou roteamento. No caso de resposta a erros, as mensagens ICMP são sempre enviadas para o endereço IP do host de origem do datagrama IP.

As mensagens ICMP são encapsuladas em datagramas IP. Os três primeiros campos de uma mensagem ICMP são comuns a todas as mensagens ICMP: **tipo** (1 byte), **código** (1 byte) e **soma de verificação** (2 bytes).

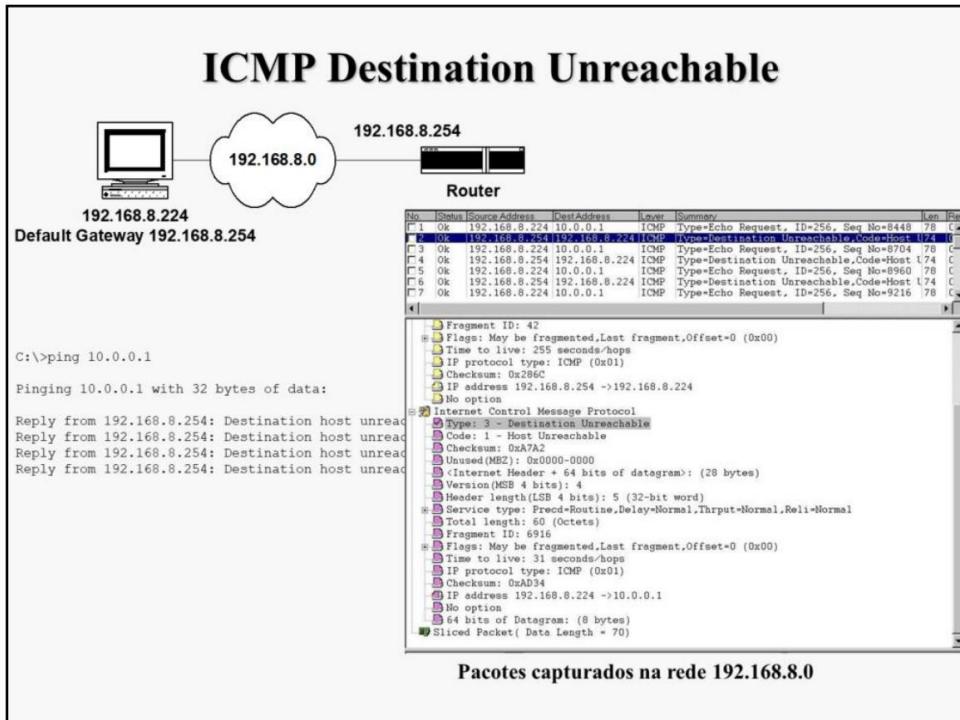
O campo de soma de verificação é calculado com base no conteúdo da mensagem completa e permite que o host de destino verifique erros de transmissão na mensagem completa.

Tipos de mensagens ICMP

Campo type	Significado
0	Echo Reply
3	Destination unreachable
4	Source quench
5	Redirect
8	Echo request
11	Time exceeded
12	Parameter problem
13	Timestamp request
14	Timestamp reply

Tipos de mensagens ICMP

O campo type (o primeiro campo de uma mensagem ICMP) define o tipo de mensagem ICMP. Acima, alguns tipos de mensagem ICMP são identificados junto com seus valores de tipo atribuídos. Nos slides a seguir, alguns desses tipos de mensagens são abordados com mais detalhes.



Mensagem de destino inacessível ICMP

A mensagem ICMP Destination Unreachable (campo tipo é 3) é usada quando o destino de um datagrama IP não pode ser alcançado.

Existem 6 valores possíveis para o campo de código:

Código 0 - Net Unreachable - enviado por um roteador caso não conheça uma rota para a rede solicitada.

Código 1 - Host inacessível - enviado por um roteador se souber uma rota para a rede solicitada, mas não puder alcançar o host de destino.

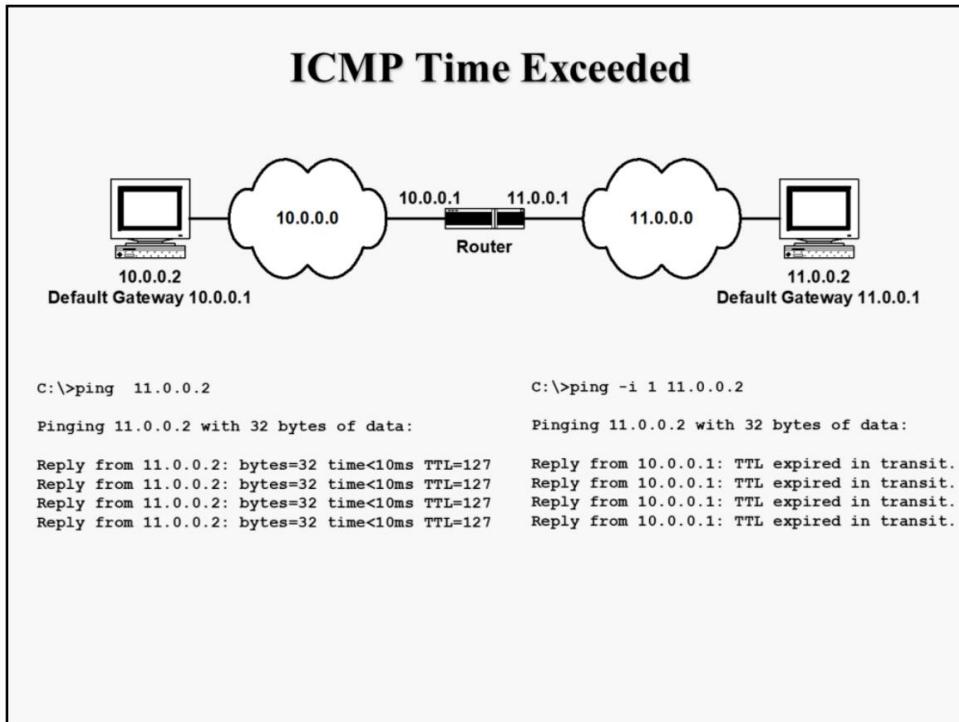
Código 2 - Protocolo inacessível – enviado pelo host de destino se o protocolo de destino não estiver em execução.

Código 3 - Port Unreachable – enviado pelo host de destino se nenhum aplicativo estiver ativo no número da porta de destino.

Código 4 - Não é possível fragmentar - enviado por um roteador se ele precisar fragmentar um datagrama IP, mas o bit 'não fragmentar' for 1 no cabeçalho IP.

Código 5 - Falha na rota de origem - O roteamento de origem IP é uma das opções de cabeçalho IP.

No exemplo acima, ao executar o comando ping no host para o endereço IP 192.168.8.254, as mensagens ICMP Echo Request chegam ao roteador que não sabe como chegar ao host de destino. As Solicitações de Eco ICMP são descartadas e o Roteador envia ao host de origem uma mensagem ICMP Destination Unreachable com o código Host Unreachable. O resultado do comando ping indica o endereço IP do roteador que relata a situação.



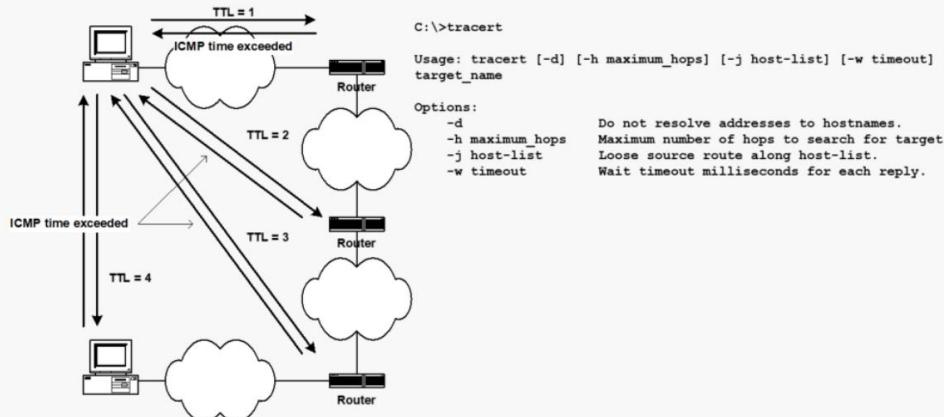
Mensagem de tempo excedido ICMP

A mensagem ICMP Time Exceeded (campo do tipo é 11) é enviada por um roteador para o host de origem de um datagrama IP de entrada quando é descartado devido ao fato de seu valor TTL atingir zero.

No exemplo acima, se o ping for definido com um TTL de origem igual a 1, o primeiro roteador descarta a mensagem e responde com uma mensagem ICMP Time Exceeded (indicada na saída do comando ping).

Comando *tracert*

- Permite descobrir o percurso utilizado no encaminhamento dos pacotes
- Recorre ao campo TTL e a mensagens ICMP Time Exceeded



comando *tracert*

O comando *tracert* é uma ferramenta de diagnóstico para exibir caminhos de roteamento e medir atrasos de trânsito de datagramas IP na rede IP.

Ao executar o comando *tracert* em um host de origem para um endereço IP de destino, o host de origem começa a enviar 3 mensagens ICMP Echo Request com TTL = 1. Para cada uma dessas mensagens, o primeiro roteador responde com uma mensagem ICMP Time Exceeded (as três mensagens dê três medidas do tempo de ida e volta para o primeiro roteador). Em seguida, o host de origem repete o processo com valores crescentes de TTL até receber respostas de eco ICMP do host de destino. Para cada valor de TTL, um novo roteador do caminho de roteamento é descoberto e três medidas do tempo de ida e volta são obtidas para esse roteador.

Exemplo – *tracert*

```
C:\>tracert -d 193.136.173.30
Tracing route to 193.136.173.30 over a maximum of 30 hops
```

```
1 <10 ms <10 ms <10 ms 193.136.92.1
2 <10 ms <10 ms <10 ms 193.137.172.254
3 <10 ms <10 ms <10 ms 193.136.173.30
```

Trace complete.

No.	Source Address	Dest Address	Summary
1	[193.136.92.243]	[193.136.173.30]	ICMP: Echo
2	[193.136.92.1]	[193.136.92.243]	ICMP: Time exceeded
3	[193.136.92.243]	[193.136.173.30]	ICMP: Echo
4	[193.136.92.1]	[193.136.92.243]	ICMP: Time exceeded
5	[193.136.92.243]	[193.136.173.30]	ICMP: Echo
6	[193.136.92.1]	[193.136.92.243]	ICMP: Time exceeded
7	[193.136.92.243]	[193.136.173.30]	ICMP: Echo
8	[193.137.172.254]	[193.136.92.243]	ICMP: Time exceeded
9	[193.136.92.243]	[193.136.173.30]	ICMP: Echo
10	[193.137.172.254]	[193.136.92.243]	ICMP: Time exceeded
11	[193.136.92.243]	[193.136.173.30]	ICMP: Echo
12	[193.137.172.254]	[193.136.92.243]	ICMP: Time exceeded
13	[193.136.92.243]	[193.136.173.30]	ICMP: Echo
14	[193.136.173.30]	[193.136.92.243]	ICMP: Echo reply
15	[193.136.92.243]	[193.136.173.30]	ICMP: Echo
16	[193.136.173.30]	[193.136.92.243]	ICMP: Echo reply
17	[193.136.92.243]	[193.136.173.30]	ICMP: Echo
18	[193.136.173.30]	[193.136.92.243]	ICMP: Echo reply

exemplo de *tracert*

Na captura acima, podemos verificar se a exibição do comando *tracert* está de acordo com os endereços IP dos roteadores que responderam com mensagens ICMP Time Exceeded.

ICMP Redirect

- Quando um router deteta que uma estação está a usar uma rota que não é a melhor envia-lhe um mensagem ICMP Redirect para que ele mude de rota
- O router inicial, para além do ICMP Redirect, envia também o datagrama original para o destino
- Não possibilita mudanças de rotas entre routers; apenas entre um host e um router ligados à mesma rede

1	type = 5
1	code = 0...3
2	checksum
4	better router IP address
	IP header + first 8 octets of datagram

← gateway proposto

Mensagem de redirecionamento ICMP

A mensagem ICMP Redirect é usada quando um roteador recebe um datagrama IP de um host e detecta que não é o Gateway Padrão apropriado a ser usado para aquele datagrama IP, ou seja, o roteador verifica sua tabela de roteamento e vê que existe outro roteador no mesmo rede física com uma rota mais direta.

Nesta situação, o roteador: (i) encaminha o datagrama IP para o destino e (ii) envia ao host de origem uma mensagem ICMP Redirect com o endereço IP do outro roteador.

A mensagem de redirecionamento ICMP não permite alterar rotas entre roteadores.

O campo de tipo de uma mensagem de redirecionamento ICMP é 5.

O campo de código é usado para fornecer mais informações sobre quais datagramas IP devem ser "redirecionados":

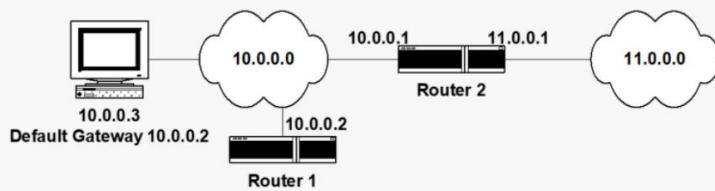
Código 0 - Redirecionar datagramas para a rede

Código 1 - Redirecionar datagramas para o host

Código 2 - Redirecionar datagramas para o Tipo de Serviço e a rede

Código 3 - Redirecionar datagramas para o Tipo de Serviço e o host

Exemplo – ICMP Redirect (I)



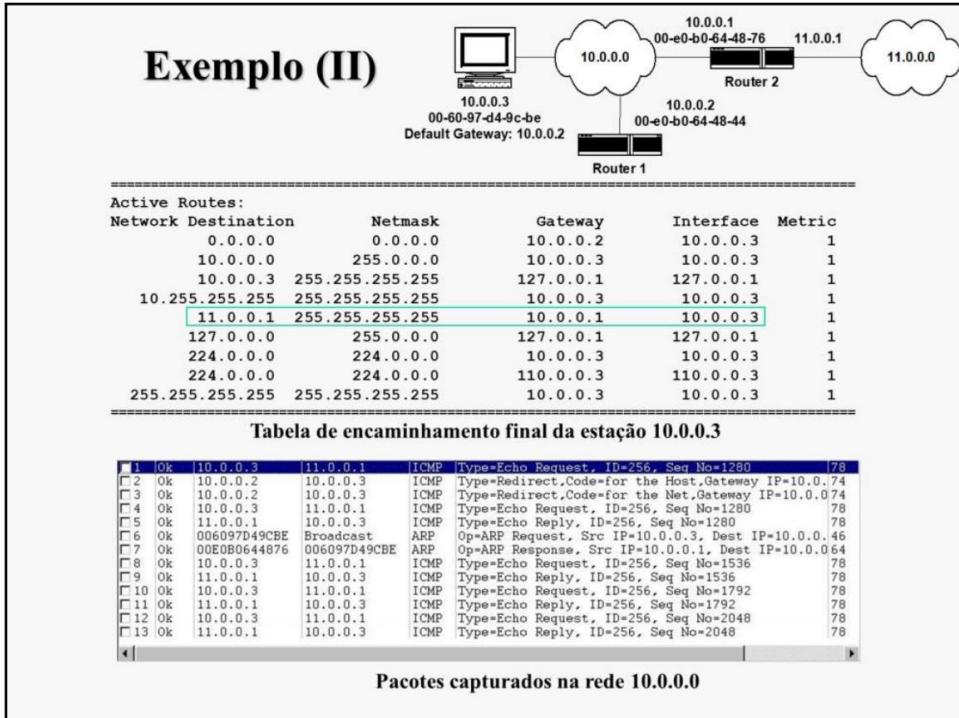
=====					
Active Routes:					
Network Destination	Netmask	Gateway	Interface	Metric	
0.0.0.0	0.0.0.0	10.0.0.2	10.0.0.3	1	
10.0.0.0	255.0.0.0	10.0.0.3	10.0.0.3	1	
10.0.0.3	255.255.255.255	127.0.0.1	127.0.0.1	1	
10.255.255.255	255.255.255.255	10.0.0.3	10.0.0.3	1	
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1	
224.0.0.0	224.0.0.0	10.0.0.3	10.0.0.3	1	
224.0.0.0	224.0.0.0	110.0.0.3	110.0.0.3	1	
255.255.255.255	255.255.255.255	10.0.0.3	10.0.0.3	1	

Tabela de encaminhamento inicial da estação 10.0.0.3

Exemplo de redirecionamento ICMP (I)

Considere o exemplo acima. Executando o comando 'route print' em uma janela DOS (no sistema operacional Windows) do host 10.0.0.3, podemos verificar a tabela de roteamento do host. A tabela de roteamento acima é possível para a rede mostrada.

Observe que, se nenhuma outra linha corresponder a um endereço IP de destino, a primeira linha informa que o Gateway Padrão é o host com endereço 10.0.0.2 (Roteador 1) que pode ser alcançado através da interface de saída 10.0.0.3 (sua própria interface de rede).



Exemplo de redirecionamento ICMP (II)

Após executar um comando ping no host 10.0.0.3 para o endereço remoto 11.0.0.1, a tabela de roteamento do host 10.0.0.3 agora possui uma linha adicional informando que o gateway a ser usado para o endereço de destino 11.0.0.1 é 10.0.0.1.

Analizando os pacotes capturados na rede 10.0.0.0, vemos que o primeiro ICMP Echo Request é enviado para o Roteador 1, este roteador envia uma mensagem ICMP Redirect para o host 10.0.0.3 e encaminha o ICMP Echo Request para o Roteador 2. Na próxima Solicitações de eco ICMP , elas agora são enviadas diretamente para o roteador 2.

O roteador 1 detectou que o endereço IP 10.0.0.1 é uma rota melhor para o endereço de destino 11.0.0.1 porque: (i) a interface de saída para encaminhar o datagrama IP é sua interface de entrada e (ii) sua tabela de roteamento indica 10.0.0.1 como o endereço do roteador de próximo salto para a rede de destino.

Observe que se nenhum redirecionamento ICMP foi emitido pelo roteador 1, todos os datagramas IP enviados do host 10.0.0.3 para outras redes seriam transmitidos duas vezes na rede 10.0.0.0.

Subredes

- Uma subrede (subnet) é um subconjunto de uma rede de classe A, B ou C
- A utilização de máscaras, permite que uma rede seja dividida em subredes estendendo a parte de rede à parte de host do endereço IP; esta técnica aumenta o número de redes e reduz o número de hosts

	decimal	binário	
endereço IP	10.32.0.1	00001010	
máscara	255.224.0.0	11111111 00000000 00000000 00000000	← → rede subrede host

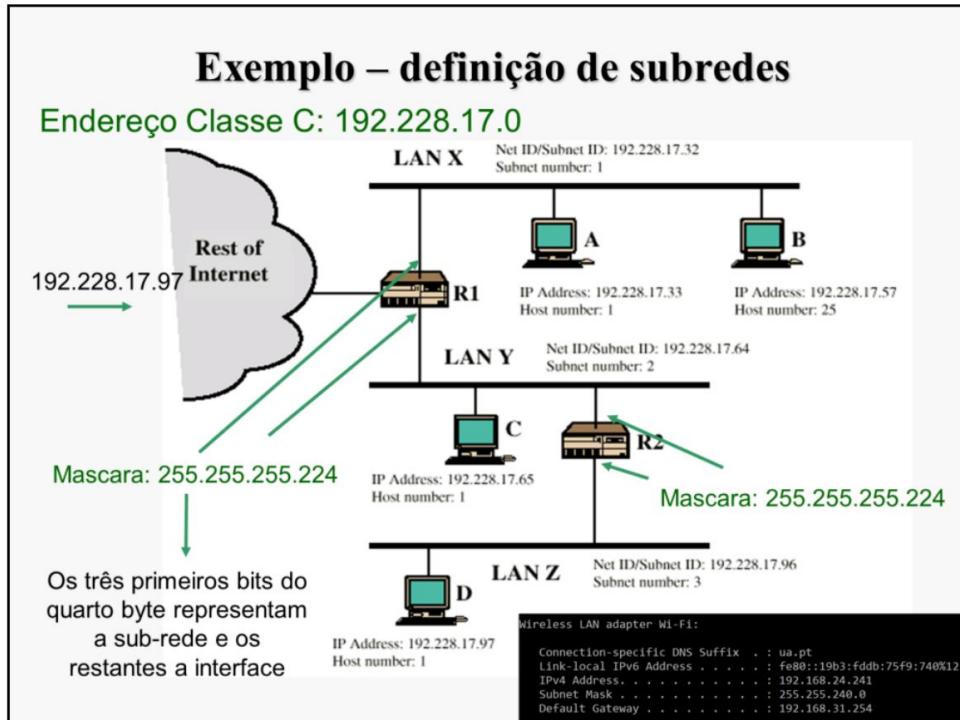
sub-redes IP

As máscaras de rede dão mais flexibilidade aos gerentes de rede no uso do espaço de endereçamento. Uma sub-rede de um endereço de rede original é definida quando alguns bits da parte hostid original são usados para definir a parte netid do endereço.

No exemplo acima, o endereço IP 10.32.0.1, definido com netmask 255.224.0.0, usa os primeiros onze bits para definir a parte netid e 21 bits para definir a parte hostid.

É um endereço definido em uma sub-rede do endereço de rede classe A 10.0.0.0, pois usa os três bits mais significativos (atribuídos com 001) de sua parte hostid para definir a sub-rede.

Dessa forma, um único endereço de rede classe A pode ser organizado em sub-redes menores para serem atribuídas a diferentes redes físicas.



Exemplo de sub-redes IP

No exemplo acima, o endereço de rede classe C 192.228.17.0 (máscara de rede 255.255.255.0) foi atribuído a um cliente por seu provedor de serviços de Internet (ISP). O cliente deve atribuir endereços aos hosts, mas sua rede é composta por três redes locais (LAN X, LAN Y e LAN Z) separadas por 2 roteadores (R1 e R2). Uma vez que tem de atribuir diferentes partes netid a diferentes LANs, deve recorrer à segmentação do endereço de rede atribuído em várias sub-redes.

Usando a máscara de rede 255.255.255.224, três bits adicionais estão disponíveis para definição de netid (em um total de 27 bits). No exemplo acima, os endereços de rede usados são 192.228.17.32 (na LAN X), 192.228.17.64 (na LAN Y) e 192.228.17.96 (na LAN Z). Cada host recebe um endereço IP cujos 27 primeiros bits (sua parte netid) são iguais aos 27 primeiros bits de seu endereço de rede. Como existem 5 bits para identificar hosts, cada host pode ser identificado por um número entre 1 e 30 (lembre-se porque 0 e 31 não podem ser usados). O endereço IP de cada host é obtido adicionando o número atribuído ao endereço IP da rede (por exemplo, o host B tem o endereço IP 192.228.17.57 que resulta da adição do número 25 atribuído ao endereço de rede 192.228.17.32).

Questões sobre Máscaras de rede e sub-rede

1. Qual o endereço de broadcast das redes:

- 200.3.27.128/25
- 200.3.27.0 e 200.3.27.128 máscara 255.255.248.0?

2. Qual a primeira máquina das redes que têm uma máquina com o endereço:

- 175.0.92.191/23
- 175.0.92.190/26
- 175.0.92.18/28?

3. Qual a última máquina das redes:

- 175.0.32.0 máscara 255.255.248.0
- 175.0.0.0 máscara 255.255.224.0
- 175.0.16.0 máscara 255.255.248.0

4. Quais as redes da máquina:

- 175.0.22.79/25
- 175.0.117.215/23
- 175.0.117.215/27?

Questões sobre Máscaras de rede e sub-rede

5. Quantas redes e com quantas máquinas se obtêm nas redes particionadas como:

- 175.0.4.0 máscara 255.255.255.252
- 175.0.114.0 255.255.255.240?

6. Considere que tem o conjunto de endereços IPv4 de classe C 200.123.189.0/24, que tem de ser usado para as diferentes sub-redes:

- 55 PCs no Networks1 Lab
- 48 PCs no Networks2 Lab
- 45 servidores no Internal Datacenter
- 5 PCs no Professors Lab
- 9 PCs na Administration room.

Define o esquema de endereçamento para as diferentes sub-redes usando os endereços disponíveis.